TECHNOLOGY TRANSFER CONTROL PLAN
GUIDELINES

REVISION 4.3

31 August 2021

DEFENSE TECHNOLOGY SECURITY ADMINISTRATION

RECORD OF CHANGES

REVISION	REASON FOR CHANGE	REVISION DATE
4.0	Complete re-baselined to Revision 4.0. Significant changes throughout the whole document.	11 June 2015
4.1	Reflects the incorporation of Department of Commerce licenses and technology. Updates the reorganization of the Space Directorate into the Technology Directorate. Requires more details when submitting a Monitor Request in support of a Telecon. Other administrative changes.	1 November 2018
4.2	Changes incorporated relate to the Technology Directorate reorganization to the Export Control Directorate. Requires companies to submit Minutes and Attendance Rosters into Spacelink for selected TIMs and Telecons. Increases the level of detail required for Telecon agendas.	1 July 2020
4.3	Detailed documents to submit as a license. Changed requirement on meeting minutes. Expanded security measures descriptions to address digital media and devices. Expanded security measures applicable to foreign visitors and personal electronic devices.	31 August 2021

TECHNOLOGY TRANSFER CONTROL PLAN GUIDELINES

Introduction – A Technology Transfer Control Plan (TTCP) defines the procedures, controls, and processes a company intends to implement to satisfy the approved Department of State (DoS), or Department of Commerce (DoC) export license and their related provisos in order to prevent unauthorized transfer of controlled defense articles, defense services or technology. Your TTCP also delineates your plan to prevent the unauthorized transfer of information that could be used by a foreign country to improve its spacecraft, missile, or space launch capabilities.

All DoS/DoC export authorizations that include the TTCP requirement proviso requires a TTCP that has been approved by Defense Technology Security Administration, Export Control Directorate (DTSA/ECD), Missiles/UAVs/Space Division (MUS) prior to exporting defense articles, defense services or technology.

These Guidelines were created to assist companies in developing a thorough TTCP. TTCP's are company prepared documents developed to meet your specific needs. Although MUS does not require you to follow these Guidelines, using them is suggested for companies with little or no previous TTCP preparation experience.

Your TTCP is a working document and should be updated as the program matures from start to finish, i.e., marketing through post-launch reviews. If your TTCP inadvertently conflicts with the limits and conditions of the DoS/DoC license or export authorization, the DoS/DoC license takes precedence.

The following pages contain outline samples and section descriptions of a: TTCP, including a Launch Campaign Security Plan (LCSP). Other documents sometimes attached to the TTCP are the: Transportation Plan, Debris Recovery Plan, Storage Plan, etc. The TTCP is treated as the main document with other documents attach to it if needed. TTCP issues should be addressed to MUS at dtsa.mc-alex.ecd.mbx.ttcp-request@mail.mil or 571-372-2522

TTCP Approval – Companies are required to get a Spacelink account for those export licenses with a TTCP proviso. Spacelink is a web-based program used by DTSA/MUS and Industry to facilitate interactions on: licenses, TTCPs, data, defense services and technology. Once your company opens a Spacelink account, the license, the Technology Assistance Agreement (TAA), and the Statement of Work (SOW) must be uploaded into Spacelink as a single searchable document, (Word and Acrobat formats are recommended to the maximum extent possible). The TTCP is then reviewed and accepted by DTSA/MUS.

Procedure for TTCP Review and Approval:

1. Load the license files (DSP-5, TAA & SOW) into Spacelink; DTSA/MUS accepts the license files into Spacelink.

    a. DoS/DoC license files consist of the license and TAA with attachments, one of them being the Statement of Work.
    b. Sample naming format: 4567-11A

2. Load the draft TTCP into Spacelink; DTSA/MUS approves the draft TTCP into Spacelink.

    a. Draft TTCP updates should be uploaded with tracked-changes.

    b. Sample naming format: 4567-11A_TTCP_DRAFT.

    c. To upload an updated TTCP not driven by a license change into Spacelink, or an administrative change, call DTSA/MUS.

3. Load the final TTCP into Spacelink; DTSA/MUS approves the final TTCP into Spacelink.

    a. Sample naming format: 4567-11A_TTCP_FINAL.
    b. The TTCP name must track with the latest license version, e.g., an A version of the TTCP is associated to A version of the license.

SAMPLE TTCP OUTLINE AND SECTION DESCRIPTIONS

Title Page

Include the following: Technology Transfer Control Plan for your program name, you export license number or DoS/DoC identifying number, your company name and address, TTCP version and approval date.

Record of Changes

Summarize the evolution of the TTCP, from initial approval through the latest approval. A tabular format similar to that shown in the second page of the TTCP Guidelines is suggested. If it is the initial approval, state just that; otherwise, at a minimum, include the revision number, submittal/approval dates, and reason for the latest submission (*e.g.,* required by latest amendment; changes to internal procedures)

Table of Contents

The Table of Contents should contain the following sections and annexes. Use the section numbering system suggested below. If a section is not used, state that it is "Not Applicable".

1.0 INTRODUCTION

1.1 Purpose

Identify the purpose of the TTCP, e.g., "This TTCP has been prepared by (company name) to ensure that U.S. technology associated with [program name] is restricted and protected in accordance with the approval letter for DoS/DoC identifying number, dated (date)."

1.2 Contact Information

Identify a point of contact(s) for the TTCP, Launch Campaign, or Export Control Official (this may be an office or an individual), providing phone, job title, and email address for each.

2.0 SCOPE

2.1 Authorized Export

Summarize the scope of the export authorization, and copy the DoS/DoC license export authorization provisos.

2.1.1 Retransfers

Describe any retransfer authority, or lack of it.

2.2 Summary of Export Authorizations

If there are amendments to the base agreement, add a summary of those amendments, starting with the base (or initial approval). Include the DoS/DoC approval dates for each. This allows the reader to follow the evolution of the agreement. The DTSA/MUS requires that for DoS export licenses both the 9-digit DSP application number be referenced and the final TAA number issued by the Department of State be listed; see the following examples:

- 1234-00 (019345289), approved 12 Dec 01, Marketing TAA for Super Spacecraft
- 1234-00A (019345288), approved 30 Mar 03, added scope, to include satellite (aka spacecraft or SC) build, manufacture, and delivery.
- 1234-00B (019345287), Returned Without Action (RWA'd).
- 1234-00C (Revised) (019345272), approved 29 Aug 03, added three foreign and one U.S. signatories with no expansion in scope

.

The following statement must be added under this TTCP section:

"If this TTCP inadvertently conflicts with the limitations and conditions of the DoS/DoC License Export Approval, the DoS/DoC License Export Approval limitations and conditions take precedence."

2.3 Signatories/End-Users

Include the names and countries of all the signatories to the agreement, U.S. and foreign alike, with a brief description of roles and responsibilities of each.

2.4 Foreign Persons

Companies should acknowledge their responsibility for ensuring that all foreign persons with access to controlled defense articles, defense services or technology are authorized under an appropriate export authorization (as employees or embedded contractors of a foreign licensee). If an employee is a dual/ third country national, he must have the appropriate authorization under 22 CFR 124.8(5) or 22 CFR124.16 to include a valid non-disclosure agreement on file (as appropriate). Foreign persons that are not representing foreign signatories are not allowed access to any controlled defense articles, defense services or technology. By definition, there cannot be any passive foreign person attendees.

2.4.1 Foreign Persons Working for U.S. Companies (Employment DSP-5)

List all foreign personnel with a DoS DSP-5 license associated with this agreement, and attach the corresponding licenses to the TTCP.

2.4.2 U.S. Persons Working for Foreign Companies

The following statement must be added under this TTCP section:

"**Any U.S. Person working for a foreign company is treated as a Foreign Person for export purposes."**

2.5 Authorized Areas for Transfer

2.5.1 Territories Approved for Export Activities

State the countries or areas in which the transfer of controlled data, defense services or technology is authorized.

2.5.2 Dual/Third Country National Employees and Non-Disclosure Agreements

State the countries or areas from which dual/third country national employees are authorized by the Technical Assistance Agreement (i.e., ITAR 124.8 (5) and ITAR124.16). Further, describe when and for which countries Non-Disclosure Agreements are required, if any.

2.5.3 Sublicensing

State whether sublicensing is authorized. If authorized, identify the sub-licensees. If there are a large number of sub-licensees, you may direct the reader to the specific portion of the license where they are listed.

2.6 Separate or Independent Export Authority

Identify whether this is authorized and if so, by whom (they all would have to be U.S. persons).

3.0 DTSA MONITORING PROVISOS

Identify all applicable provisos verbatim (by # and amendment, as applicable) related to DTSA/MUS monitoring. These are: TTCP; ITAR controlled (technical) data review or technology; monitoring of ITAR controlled meetings; reimbursement procedure; and any other provisos related to DTSA/MUS monitoring.

4.0 EXPORT COMPLIANCE TRAINING

4.1 U.S. Persons

In this subsection, companies should acknowledge their responsibility for ensuring all U.S. persons who represent U.S. signatories or end-users to the agreement or license, respectively, are trained on the limitations and conditions of the export authorization. The company should also indicate who will provide this training and how it will be documented.

This includes providing awareness briefings to Non-Signatory Attendees. Non-signatories are U.S. persons allowed to attend controlled meetings, but only as non-participants (i.e. passive or silent attendees). Non-Signatory Attendees are not covered by an export authorization, and therefore, have no export authorization whatsoever. Use this subsection to identify potential Non-Signatory Attendees, cite who they are or might be, their relationship to the agreement or license, and a brief description as to why they might be attending.

4.2 Description of Training for U.S. Persons

This training must provide instruction on the following:

4.2.1 The contents of the export license and TTCP, general ITAR awareness (to include an emphasis on not discussing ITAR controlled data, perform defense services or transfer technology in common areas such as hotel lobbies, taxis, and restaurants), company policies pertaining to exports, and consequences of violations of export law and regulations.

4.2.2 The difference between ITAR controlled data and other types of data or technology.

4.2.3 An explanation of how to properly ask questions to a foreign signatory. Leading or suggestive questions (e.g., "Have you considered…?") that could lead to a potential export violation cannot be asked. Questions should be of a more general nature, such as, "How are you meeting my requirement?"

4.2.4 Frequency of training (semi-annual training is recommended), who provides the training, if not by name, at least by office symbol or title;

4.2.5 State that all individuals shall be trained prior to their participation in any export activity and how training records will be maintained and tracked;

4.2.6 Describe your plan to handle out-of-cycle training for special circumstances such as: an approved export license change in the scope of work, change in the law affecting procedures, if there is a violation, etc.

4.2.7 Describe the rules for escorting foreign visitors, restricted areas, etc.

5.0 ITAR CONTROLLED DATA

5.1 Documentation Control

5.1.1 Unique Data Identifier

ITAR controlled data or Commerce controlled technology tagged for export must have a unique identifier; *i.e.,* a document control number. Each export be uniquely identifiable, recorded and tracked. As a minimum, records must be able to show what has been exported, when, and to whom.

Provide an example of your naming convention.

Spacelink provides the opportunity to enter these identifiers, or Industry ID, as they are referred to in Spacelink, during the controlled data upload process.

5.1.2 Internal Processes

Describe your internal process for documentation control, from the moment the controlled data or technology is generated until the time it is exported. Include procedures for how it is tracked and maintained. This should include:

- The process for the maintenance of a library of exported controlled data independent of Spacelink.
- Who makes the determination on whether data marked for export is ITAR-controlled or non-ITAR controlled?
- How are documents routed and approved internally prior to DTSA/MUS review?
- How are data exports tracked?
- Who is the point of contact for documentation control?
- How is ITAR/EAR controlled data archived?

The following statement must be added under this TTCP section:

"Prior to release, (company name) will ensure all ITAR/EAR controlled data is in compliance with any technical limitations/provisos from the DoS/DoC license export authorization(s)."

DTSA/MUS expects companies to document and have available a cross-referencing log that associates each corporate Unique Data Identifier with the Spacelink approval reference identifier(s) and the signatories and countries authorized to receive that specific document. The purpose is to verify that ITAR/EAR controlled data delivery is only as authorized by the appropriate export license and DTSA/MUS approvals.

Submitting your documents for inclusion into Spacelink does not relieve your company of the obligation to maintain their own records of transactions involving ITAR/EAR items.

5.1.3 Documentation Markings

All ITAR controlled data for release should be marked with the following:

- DoS/DoC Identifying Number (the export authorization, this includes identifying the correct and current amendment);
- The Unique Data Identifier; and
- An ITAR/EAR warning (disclaimer) against unauthorized re-export or third-party transfer of the controlled data.

Provide an example of documentation markings. If there is a specific company process that differs from this, contact DTSA/MUS for approval. Markings should be added prior to the DTSA/MUS review.

An example ITAR marking that would be appropriate for the first page of ITAR controlled data is shown below:

> "This document contains ITAR controlled data (ITAR 120.10) being transmitted under License (#). Retransfer of this data by any means to any other end-user or for any other end-use is prohibited without the written approval of the U.S. Department of State. 22 CFR 125.4 (b) (2) applies."

An example of information that should be placed in the footer of each page of ITAR controlled data is shown below:

> "Contains ITAR data subject to U.S. Export Control, License (3) (Doc no. xx)"

5.2 DTSA Review

State whether this is a requirement or not, and if so, cite the proviso. If DTSA/MUS review of ITAR controlled data is required, include the following statement in this section:

"(Company name) acknowledges that DTSA/MUS has up to 10 business days to review **ITAR/EAR controlled data submitted for approval. The first full normal business day after DTSA/MUS' receipt of the submission is counted as Day 1."**

5.3 Request for Waiver/Exemption Process

The ITAR/EAR controlled data review proviso contains circumstances when companies may request that DTSA/MUS review of ITAR controlled (technical) data may be waived.

5.3.1 Types of Data that can be Waived

- Repetitive data/documents that might fall within the definition of requiring review. Identification of this data is subjective, and must be agreed upon, in writing, with DTSA/MUS. A list of such document/data may be listed within the waiver section of the TTCP, or added as an attachment.

- Test results are exempted from the ITAR controlled data review requirement. Reports including test analysis, procedures, or derived conclusions must still be reviewed as stated above.

- ITAR/EAR controlled data that is similar to that already approved by DTSA/MUS.

5.3.2 Waiver Requests via TTCP

Companies may list (in this section or in an appendix) ITAR/EAR controlled data that they believe is authorized for export without prior DTSA/MUS review. DTSA/MUS will review this list, and negotiate the final list prior to TTCP approval.

DTSA/MUS review of documents is not required in the following instances so long as the applicant has not made any technical modifications that change the technical meaning or content of the document:

- Documents originated by a foreign signatory to be exported to a different foreign signatory.
- Export-approved U.S. origin data that has been translated into a foreign language for a foreign signatory.

5.3.3 Waiver Requests via Spacelink

After the TTCP has been approved additional waivers/exemptions can be requested using Spacelink. All waivers/exemptions will be granted on a case-to-case basis. DTSA/MUS will negotiate the waiver details through the approval process. The following must be included in order for a waiver to be approved.

- The company must certify that the currently submitted ITAR/EAR controlled data is similar to that previously approved for release.
- The company must reference the previous approval of the data in Spacelink, if requesting waiver for future similar data submittals within a program.

- The request must include the scope of data to be waived.
- The waiver must have an expiration date (companies may utilize dates or milestones as the expiration date).

5.4 Definition of Terms

Define terms; if using ITAR definitions you may reference the ITAR paragraph number.

6.0 ITAR CONTROLLED/TECHNICAL INTERCHANGE MEETINGS

The terms “ITAR Controlled Meeting” and “Technical Interchange Meeting” (TIM) are used interchangeably for this document. This section assumes that all technical interchanges are ITAR-controlled and that all controlled meetings are technical—even though this may not always be industry’s view.

6.1 General Requirements

Meetings, teleconferences, videoconferences, and joint operations are technical interchanges. These are events where technical data is exported and/or defense services or technology are provided. Operations also involve hardware (i.e., defense articles). The minimum technology transfer controls required for technical interchanges that must be addressed in any TTCP are listed below. Companies should indicate in this paragraph the individual (e.g., Activity Chair or designee, export control official) attending the technical interchange that will ensure compliance with technology transfer controls; this person will be referred to as the “Activity Chair” or “Chair”. The Chair must start each TIM or Telecon/Videoconference with a statement similar to:

“”Company Name” is conducting this Technical Interchange Meeting (or Telecon) under the auspices of DoS license (license #). All the participants must be trained under this license to be allowed in this meeting. All license provisos apply.”

As with all aspects of the TTCP, the controls established apply whether or not a DTSA/MUS Monitor is present. The applicant must insert the applicable Conduct of Technical Interchanges wording suggested below into the TTCP:

Conduct of Technical Interchanges. “All technical interchanges will be held under license number (company export license #) and will only include signatories to the agreement and applicant approved passive attendees.”

Conduct of Technical Interchanges. “Technical interchanges may be held under multiple licenses. Prior to any technical interchange of this type, the Empowered Official and Activity Chair will ensure that the content discussed during the technical interchange is within the scope of all active agreements and the foreign parties involved are signatories of all agreements. They will also ensure that the most stringent provisos be implemented. The Activity Chair’s company hereby acknowledges that they are ultimately responsible for all activities/actions that occur during the subject meeting.”

In this situation, the Monitor Request must include information on the other agreements that

will be used. Copies of these agreements will be uploaded to the Monitor Request under the "Document Upload" tab.

The following statement must be added to this section of the TTCP:

"The licensee hereby acknowledges that they are ultimately responsible for all activities/actions that occur during the subject meeting."

6.2 Attendance Roster

An Attendance Roster is required for all ITAR-related activities. The attendance roster must be filled out by all participants at the beginning of every technical interchange. There may be some who do not sign right away, but the Activity Chair must follow-up to ensure each individual signs the roster as soon as possible. The DTSA/MUS Monitor (if present) will review the roster for compliance and be provided an electronic copy after the event. The attendance roster must include, at a minimum: full name, nationality, company, and signatory (contractors hired by a signatory company should list the signatory company as their signatory, unless they are a signatory to the license themselves). Non-signatories (U.S. person passive attendees) need to list the applicant that invited them to attend and be approved by the Activity Chair. This paragraph is also a good place to discuss anyone who is exempt from signing the roster (e.g., janitors, cafeteria workers) and the procedures used when these need access to the conference room where technical discussions are on-going.

6.3 Non-Signatory Attendees

The Activity Chair must be able to identify all Non-Signatory Attendees (sometimes referred to as passive attendees or non-participants). If a DTSA/MUS Monitor is present, they should be made aware of all such participants. Non-Signatory Attendees are U.S. persons who are not signatories to the agreement and are there, at your invitation. These U.S. persons have no export authority, and therefore, may not participate in any of the technical interchange. For this reason, it is important to know who these individuals are.

6.4 Walk-Ins

Companies need to describe their procedure or process to ensure that any person who arrives after a technical interchange has begun signs the attendance roster. The Activity Chair needs to know if they are authorized to be in attendance. The procedure needs to take this validation-of-the-individual process into account, because a company cannot export technical data or provide defense services when a foreign person who is not authorized to receive such data or services steps into an activity. Be particularly mindful of this when meetings or interchanges occur at foreign signatories' facilities.

6.5 Responsibilities of the Activity Chair (i.e., Export Control Official)

6.5.1 Copies of the Export Authorization

The Activity Chair must have in his/her possession copies of the complete export authorization. This includes the TTCP and a copy of the current license or executed agreement, to include any amendments, attachments, and corresponding DoS/DoC Approval(s).

6.5.2 Who is Who

The Activity Chair must also be able to identify and verify all participants and attendees and whether those who are U.S. persons have had their export compliance training or awareness briefing.

6.5.3 Technical Data

The Activity Chair must have, as the minimum, a list of the technical data approved for release. This should be consistent with the implementation of section 5.1.2 for the tracking of technical data release approval.

6.5.4 Change-Pages to Approved Technical Data

It is the Activity Chair's responsibility to notify the attending DTSA/MUS Monitor, if present, of any change-pages made to approved technical data prior to its discussion or presentation. The presumption is that changes are strictly editorial, as any other change involving the addition of technical content would require subsequent DTSA/MUS approval.

6.6 Specific Controls

Discuss any specific technology control procedures for meetings, telecons, and operations in this section. Describe how export control will be different if it is held in the company's facility versus one held in a foreign person's facility. Explain how positive control of technical data will be maintained, as well as any special procedures a company might have.

A TIM/Telecon/Videoconference agenda must be provided with the Monitor Request (see section 6.8.2 below). It must include a list of documents, **with the Spacelink reference number**, for those documents planned to be used in the discussions. If a detailed agenda is not available when the Monitor Request is submitted into Spacelink, provide a general agenda and 2 days prior to the TIM/Teleconference/Videoconference submit via email a detailed agenda to the assigned DTSA Monitor.

6.6.1 Meetings

A meeting is a face-to-face technical interchange. Defense services are provided and technical data exported. Discuss how control of the environment, control of technical data, and any other controls during meetings will protect technical data. It is not necessary to repeat information discussed previously, rather focus on peculiarities or nuances. Most of the discussion should revolve around physical controls or any limitations. Also, identify potential meeting locations in the U.S. and abroad. What are your procedures to transition a non-technical meeting into a technical meeting; and vice versa? Does this procedure include DTSA/MUS notification if a Monitor Request is required (not required if the authorization does not have a monitoring proviso)?

6.6.2 Teleconferences/Videoconferences

Teleconferences/Videoconferences are Technical Interchange Meetings (TIMs) except that they are not face-to-face. Each participating party, individually or as a whole, either calls a bridge line or a "personal" line with some kind of teleconferencing capability. Companies are not allowed to have TIMs where both U.S. and foreign signatories are in the same room without a DTSA/MUS Monitor present, unless waived.

Discuss any nuances or differences in the way you handle teleconferences/ videoconferences from meetings; many of the controls will be the same for both. In instances where groups dial in to the teleconference, a Point-of-Contact for each group will be responsible to announce all attendees to the Activity Chair and give assurance that no passive attendees or Non-Signatory attendees are present.

The following statement must be added to this section of the TTCP:

“When U.S. and foreign persons are in the same room, a teleconference/ videoconference become a Technical Interchange Meeting (TIM).”

6.6.3 Launch Campaigns and Joint Operations

The purpose of this subsection is to discuss controls used for launch campaigns and joint operations with foreign parties which are not specifically called out elsewhere. Ensure it is stated that an Activity Chair, or his delegated representative, will monitor all joint operations. An exception to this policy is that during any hazardous operations, personnel are not required to be in the area for export compliance reasons. In this case the Activity Chair is required to maintain positive control to the greatest extent possible (through attendance sheets, using remote monitoring, etc.) and participate in any planning sessions beforehand in order to understand what is being accomplished.

Annexes to the TTCP will be required for launch campaigns and might include a Security Plan, a Joint Operations Plan, a Training Plan, a Transportation Plan, a Debris Recovery Plan, and/or any plans deemed necessary for a specific mission. Companies may provide these annexes as one document attached to the TTCP or as separate attachments so long as they allow DTSA/MUS to fully understand how the company will accomplish the topics addressed. A sample outline of a set of annexes is provided in Attachment A.

The following statement must be added to the TTCP:

“Attachments or Annexes to the TTCP must be provided to DTSA/MUS no later than sixty (60) business days prior to shipment of any ITAR/EAR-controlled hardware. Companies may contact DTSA/MUS to negotiate shorter timelines.”

6.6.4 Launch Failure Review Meetings

If this does not apply to your export authorization, state that it is “Not Applicable.”

Per 22 CFR 124.15(b) all launch failure discussions require a separate Department of State License, unless said discussions are within the scope of your authorization (e.g., heritage failure data). SC failures have similar restrictions. Reference your authorization’s provisos and the ITAR prior to any discussions. Identify all applicable provisos verbatim (by # and amendment, as applicable) related to the Launch Failure.

The following statement must be added under this TTCP section:

“All data and presentations developed and exported at Launch Failure Review meetings shall be uploaded to Spacelink by (company name), whether or not the data was approved by DTSA/MUS on site.

6.7 DTSA Monitors

The following text must be included in this subsection (tailor to your authorization):

“Attending DTSA/MUS Monitors will not, unless previously coordinated, review data on-site. They will, however, review change-pages to ITAR/EAR controlled data previously approved for export. The Monitor will also review and approve meeting minutes for immediate release via signature (not as data review within Spacelink).”

If there is no proviso for monitoring in the authorization, state that it is “Not applicable.”

6.8 Notification Requirements

Companies are required to alert DTSA/MUS of upcoming ITAR TIMs by requesting DTSA support through Monitor Requests. DTSA/MUS will then assign a monitor or waive the monitoring requirement. On every July companies that have reimbursable programs must provide a forecast of their TIMs and Launch Campaigns for the upcoming government fiscal year (October – Sept). This allows DTSA/MUS to provide an estimated cost of monitoring applicable to those companies with reimbursable programs.

6.8.1 Timelines

Notification timelines for monitoring are forty (40) business days in advance for launch activities; twenty-one (21) business days in advance for meetings overseas (unless more time is required by the licensee to obtain DTSA/MUS clearance to foreign facilities); seven (7) business days for meetings in the US; and five (5) business days for teleconferences/videoconferences.

6.8.2 The Monitor Request

All requests for DTSA/MUS monitoring must be submitted via Spacelink as a Monitor Request and include an agenda; see section 6.6 above. Follow-up questions may be addressed to the DTSA/MUS point of contact. Meetings between U.S. and foreign participants under an EAR license occurring at the launch site during a launch campaign require a DoS license and monitoring by DTSA/MUS. If your company allows other company licenses to be concurrently used for separate export, state this in your Monitor Request; after verifying with DTSA/MUS that this is allowed for your license.

6.8.3 Exceptions

Non-ITAR controlled meetings are exempt from the notification requirements.

6.9 Reimbursable Programs

Reimbursable programs are those where the company reimburses the U.S. Government per Public Law. All ITAR controlled meetings involving the foreign signatories must have a Department of Defense (DoD) Monitor present unless exempted by the DoD/Defense Technology Security Administration (DTSA/MUS). The following statement must be added for reimbursable programs under this TTCP section:

"(Company name) will upload Minutes and Attendance Roster for all meetings to the original Monitor Request for that activity within 5 business days after completion of the activity."

6.10 Non-Reimbursable Programs

Non-reimbursable programs are those where DTSA/MUS "reserves the right to monitor" activities per Proviso, but where companies DO NOT reimburse the U.S. Government.

The following statement must be added for non-reimbursable programs under this TTCP section:

"(Company name) will upload Minutes and Attendance Roster for all waived meetings, if required by the waiver wording, to the original waived Monitor Request for that activity within 5 business days after completion of the activity."

In the Monitor Request, for non-reimbursable programs, companies must state:

"DTSA reserves the right to monitor per Proviso #XX of Export License # XXXX."

6.10.1 Non-Reimbursable Program Exemptions

Along with non-ITAR controlled (or business) meetings, the following ITAR controlled meetings may also be exempt from notification, as long as the discussion is based on the scope of approved ITAR controlled data and the applicant adequately addresses their specific export controls during such interchanges:

- Informal discussions, daily activity meetings, and weekly program status meetings.
- Meetings below the system-level (unless it involves a major anomaly).
- Ad hoc teleconference/videoconferences, if applicable, relating to minor anomalies without going into detailed discussions with the foreign customer. Minor anomalies are defined as simple manufacturing defect discussions such as solder joint, component/subsystem/system/spacecraft test failures, etc.

6.10.2 Definitions

The text provided below serves as guidance only to companies in their application of the exemptions listed above for non-reimbursable programs.

- System. A system is an assembly of two or more subsystems. Typical systems are a spacecraft a launch vehicle (LV), or a ground segment.
- Subsystem. A subsystem is composed of related components that perform a set of functions grouped under a single description such as SC power or SC attitude and control. Examples for a Launch Vehicle are structure, telemetry, or instrumentation.
- Minor Anomaly. A simple manufacturing defect that does not require detailed discussions with a foreign customer such as solder joint, component/subsystem/system/SC test failures, etc.
- Major Anomaly. Any issue, problem or defect that does not fit the definition of a minor anomaly as described above.

7.0 PHYSICAL AND COMMUNICATIONS SECURITY

Without physical and computer networks/communications security considerations, there is no way to adequately protect controlled technologies. At a minimum, each of the following subsections (unless otherwise noted) must be addressed. Where appropriate, cite and paraphrase existing and/or standard security procedures that directly relate to this TTCP. If a particular subsection below does not apply, state that it is "Not Applicable."

7.1 Security Management

In this subsection, briefly introduce the "who" (*e.g.,* security management team/lead and key personnel, and the "what" (basic approach to security; for instance, whether standard and recognized industrial security practices or other published guidelines are used, etc. Explain procedures for handling any security-related problems or shortfalls that may arise (e.g., reporting of incidents, process change due to recently exposed vulnerabilities). Describe your plan of action if tamper-evident seals show signs of tampering or other discrepancies occur. Describe security measures taken to protect the computers and communications networks, and all digital information. Describe how you intend to control personal recording equipment (e.g., personal phones/cameras), and the recording of photographs and videos of equipment, or in controlled areas.

7.2 Facility Layout

Provide a basic graphical overview of the facilities where controlled meetings may take place. Identify or describe where the "common" areas are, if applicable, or areas in which even escort-required personnel do not need an escort like restrooms, cafeteria, etc. Provide a layout (charts/diagrams) of the facilities, highlighting program areas, entrance, "common" areas, location of card readers, cipher locks, emergency exits, etc.

7.3 Physical Barriers/Separators

It is necessary to address the use of physical barriers/separators, or the like, if plans include taking foreign persons into areas that afford visual access to defense articles not authorized for export under the current export authorization. For example, a large high bay or

with multiple cells may contain more than a foreign customer's SC; there may be other commercial or U.S. Government SC in work adjacent to that authorized for export. In this case, companies should discuss plans and procedures for ensuring foreign persons only have access to that which is authorized.

7.4 Badges and Badging

Discuss the different types of badges *e.g.,* visitor, U.S. versus foreign, escort-required, non- escort required, contractor, government reps, and the privileges for each (access areas); distinguishing characteristics that sets one type of access from another (*e.g.,* colors, borders, stripes); direction to wear badges between waist and shoulders; what happens if a person wearing an escort-required badge is found without an escort, etc. If a chart with examples of all the types of badges is not available, then describe them. If badges are not used, explain what controls are used, with discussions centering on the topics identified above (*e.g.,* how to differentiate a visitor from an employee, etc.).

7.5 Network, Telecommunications and User Controls

Describe types of controls for: computers, external drives and similar removable devices, mobile phone transmissions and remote access to networks and databases including encryption. Describe foreign visitors access to networks if provided and related controls.

LAUNCH CAMPAIGN SECURITY PLAN (LCSP)

SAMPLE OUTLINE AND SECTION DESCRIPTIONS

(Attachment A to the TTCP Guidelines)

Title Page
Include your license or DoS/DoC identifying number, your company name and address, and date. The Launch Campaign Security Plan (LCSP) is usually an attachment to the TTCP.

Record of Changes
Summarize the evolution of the LCSP, from initial approval through the latest approval. A tabular format similar to that shown in the second page of the TTCP Guidelines is suggested. If it is the initial approval, state just that; otherwise, at a minimum, include the revision number, submittal/approval dates, and reason for the latest submission (*e.g.,* required by latest amendment; changes to internal procedures)

Table of Contents

The Table of Contents should contain the following sections. Use the section numbering system suggested below. If a section is not used, state that it is "Not Applicable". Use as much or as few of these sections as needed to describe your security plan during the launch campaign.

1. Document Description (Optional)
   1.1. Purpose of Document
   1.2. Revision History

2. Launch Campaign Overview
   2.1. Program
   2.2. Key Participants
   2.3. Reference to License Export Authorizations
   2.4. Other Reference Documents
   2.5. Summary of Defense Articles

3. Organizations, Participants, Names, Roles, and Responsibilities
   This section needs to provide enough details to help the DTSA/MUS monitor know how the players interact and who is who when looking for information or to discuss issues. This includes more than just the primary POC.
   3.1 Organizational Chart(s)
   3.2 DTSA/MUS Interface
   3.3 Key Foreign Participants
   3.4 List of Companies, licenses, etc.
   3.5 Sublicensing
   3.6 Technology Safeguards Agreement
   3.7 Non-Signatory Services

4. Launch Base Facilities
   4.1. Base-Level Pictures and Description
   4.2. Buildings & Rooms
      4.2.1. Description/Location/Numbers
      4.2.2. Physical Layout

4.2.3. Physical Security Measures
4.2.4. Contingency Facilities (e.g., Failure Debris Storage Building/Room)
4.3. US-Only vs. Foreign Controlled Areas
4.4. Facility Acceptance Process

5. General Functions
5.1. Overall Security Practices
5.1.1. Guards (Staffing Plan and unexpected workload situations)
5.1.2. Manned vs. Remote Monitoring
5.1.3. Escorting, and Public/VIP Tours 5.1.4. Video/Photo Plan (or summary of plan)
- State the frequency at which the security video will be reviewed. Describe how you are going to avoid missing an intrusion event (review speed). Describe for how long the video will be preserved, and if will the video will be overwritten/erased.
- Discuss who is allowed to use a camera and where. Describe how will your company control the use of personal phones cameras/video.
- Spacecraft videos or photos taken by any foreign party must comply with the spacecraft manufacturer distance and image resolution (pixels) limits.

5.2. Badging & Access Control
5.3. Training – in addition to that described in Section 4.2 of the TTCP
5.4. Networks/Communications
5.5. Release of ITAR Controlled Data
5.6. Meeting Protocols / ITAR Controlled Meetings
5.7. Storage of ITAR Data and Equipment
5.7.1. Storage of defense articles must be approved by DoS, either via your license authorization and/or amendment to your license, or via a letter from the DoS. If there is no written documentation approving storage of the defense article, it cannot be stored at a foreign location.
5.7.2. Include security measures to be used during storage (e.g., video surveillance, locks, and tamper-evident seals.)

6. Factory-to-Post-Launch Flow of Events
6.1. Chronology of Events
6.2. Nominal Timeline of Events
6.3. Recurring Topics/Themes
6.3.1. Security
- If the program has a detailed security plan that includes security during movements, you may reference it here, if not, include all security measures that will be taken during the movement
- Describe in detail your process if a security violation occurs (e.g., broken lock/seal; loss of video surveillance).

6.3.2. Transportation
- Describe your transportation plan. Team members must accompany the SC throughout its journey maintaining positive control.

- Identify times, if any, where positive control is lost, and what controls are utilized to maintain security. Positive control, meaning continuous line of sight.
- State when tamper-evident seals are used and how are often are these verified and logged. Describe any other protective measures used.
- Describe how your company will maintain positive control through foreign Customs and the team members that will be present (U.S. company, foreign company, and translator) while defense articles clear Customs.

6.3.3. Joint Operations Description
6.3.4. DTSA/MUS Requirements/Participation
6.3.5. Briefings/Daily Meetings

- Describe how you plan to manage ITAR technical discussions when other non-signatories are in a meeting; as in the case of multiple SCs manufacturers sharing a Launch Vehicle

6.4. Post-Launch
6.4.1. Describe your facility close-out, pack-out, shipments home, etc.

7. Contingency Planning
7.1. Incident Reporting
7.1.1. Describe in detail your process if a security violation or concern occurs, including investigation and reporting plans (e.g., broken tamper-evident seal/lock, loss of video surveillance).

7.2. Launch Delays
7.2.1. Describe how DTSA/MUS will be notified through Spacelink of changes in campaign plans.

7.3. Debris Recovery
7.3.1. Describe your plans for recovery of your spacecraft components. Include security issues, transportation of personnel to-and-from the wreckage location, debris storage, and identify a POC. Also, include your plans to document and report the status and outcome of the debris recovery efforts to DTSA/MUS.

7.4. Transportation Delays/Interruptions/Diversions
7.5. Back-to-Back/Overlapping Campaigns
7.6. Failures/Outages Backup Plan (e.g., security video outage, emergency egress)

8. Other
8.1. Incident Reporting Form(s)
8.2. Security Staffing Plan
8.2.1. Security and ITAR control Personnel Staffing
8.2.2. Work Tempo of Launch Campaign Operations
8.2.3 Plan to manage unexpected security related circumstances
8.3. Acronyms/Abbreviations/Definitions