TECHNOLOGY TRANSFER CONTROL PLAN
GUIDELINES

REVISION 4.0

11 JUNE 2015

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

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), Directorate of Defense Trade Controls (DDTC) export license and its related provisos, in order to prevent unauthorized transfer of controlled defense articles and defense services. Your TTCP 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 export authorizations that include the TTCP requirement per proviso from DDTC, require a TTCP that has been approved by Defense Technology Security Administration, Space Directorate (DTSA/SD) prior to exporting defense articles and defense services.

These Guidelines were created to assist companies in developing a thorough TTCP. TTCP's are company prepared and owned documents developed to meet your specific needs. Although DTSA/SD 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 DDTC export authorization, the DDTC license takes precedence.

Points of Contact (POCs) – Below are the DTSA/SD POCs for TTCP related issues.

Administrative Matters 571-372-2472
E-mail: dtsa.mc-alex.sd.mbx.sd-admin@mail.mil

Reimbursable Programs*, 571-372-2540/2469
E-mail: dtsa.mc-alex.sd.mbx.reimbursable@mail.mil

Discretionary (Non-Reimbursable) Programs*, 571-372-2539/2541
E-mail: dtsa.mc-alex.sd.mbx.discretionary@mail.mil

***** *Reimbursable and discretionary programs are designated by the appropriate DTSA monitoring proviso within your license. This proviso will dictate that DTSA "MUST monitor" (indicating a reimbursable program), or that DTSA has a "right to monitor" (indicating a discretionary program).*

TTCP Approval – For those export licenses with the TTCP proviso, companies are required to get a Spacelink account. Spacelink is a web-based program used by DTSA/SD and Industry to facilitate interactions on: licenses, TTCPs, data, and technical assistance. Once your company opens a Spacelink account (Opening a Spacelink Account), both the license and the Technology Assistance Agreement (TAA) must be loaded into Spacelink as searchable Word or Adobe documents (to the extent possible), and accepted by DTSA/SD.

Procedure for TTCP Review and Approval:

1. Load license files into Spacelink; DTSA accepts license files into Spacelink.
    a. License files should consist of license (DSP-5), and TAA with attachments (e.g., Statement of Work).
2. Load the draft TTCP into Spacelink; DTSA approves the draft TTCP into Spacelink.
    a. Sample name: 4567-11A_TTCP_DRAFT.
    b. TTCP updates should be uploaded with tracked-changes.
    c. To upload an updated TTCP not driven by a license change into Spacelink, call DTSA/SD.
3. Load the final TTCP into Spacelink; DTSA approves the final TTCP into Spacelink.
    a. Sample name: 4567-11A_TTCP_FINAL.

General Instructions – Attachment A provides a sample TTCP outline, detailed section descriptions, and wording to aid in the development of your document. Attachment B provides a suggested outline and section descriptions for the Launch Campaign Security Plan (LCSP). The LCSP is usually treated as an attachment to your TTCP that is due for review and approval 60 days prior to the shipment of ITAR hardware. Reiterating, to the maximum extent possible, upload your documents into Spacelink as searchable Word or Adobe documents.

SAMPLE TTCP OUTLINE AND SECTION DESCRIPTIONS

(Attachment A to the TTCP Guidelines)

Title Page

Include the following Technology Transfer Control Plan for your program name, you license or DTC case number, your company name and address, and TTCP 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 DTC Case TA (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, normally following the "NOW, THEREFORE" clause in your latest license submission, and copy the DDTC authorization provisos.

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 DTC approval dates for each. This allows the reader to follow the evolution of the agreement. The DTSA/SD requires that 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 (xxxxxxxxx), approved 12 Dec 01, marketing TAA for Super Spacecraft XT.

- 1234-00A (xxxxxxxxx), approved 30 Mar 03, added scope, to include satellite (aka spacecraft or SC) build, manufacture, and delivery.
- 1234-00B (xxxxxxxxx), Returned Without Action (RWA'd).
- 1234-00C (Revised) (xxxxxxxxx), 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 DTC Approval, the DTC Approval takes 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 all foreign persons who will have access to ITAR controlled defense articles (hardware or ITAR controlled data) or defense services 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 CFR 124.16 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 ITAR controlled defense articles or defense services. By definition, there cannot be foreign person passive attendees.

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

List all foreign personnel with a DoS DSP-5 associated with this agreement, and attach the corresponding DSP-5s to Annex A.

2.4.2 U.S. Persons Working for Foreign Companies

Any U.S. Person working for a foreign company is treated as a Foreign Person.

2.5 Authorized Areas for Transfer

2.5.1 Territories Approved for Export Activities

State the countries or areas in which the transfer of ITAR controlled data or defense services 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 ITAR

124.16). 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 number and amendment, as applicable) related to DTSA/SD monitoring. These are: TTCP; ITAR controlled (technical) data review; monitoring of ITAR controlled meetings; reimbursement procedure; and any other provisos imposing DTSA/SD 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 an awareness briefing to Non-Signatory Attendees. Non-signatories are U.S. persons allowed to attend ITAR 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 TAA and TTCP, general ITAR awareness (to include an emphasis on not discussing ITAR controlled data or perform defense services in common areas such as hotel lobbies 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.

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 (DTSA/SD recommends semi-annual training), 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 how do you plan to handle out of cycle training for special circumstances such as: a change in the scope of work in the TAA that has been approved by DDTC, change in the law affecting procedures, if there is a violation, etc.

5.0 ITAR CONTROLLED DATA

5.1 Documentation Control

5.1.1 Unique Data Identifier

ITAR controlled data, sometimes referred to as documents or packages, tagged for export must have a unique identifier; *i.e.,* a document control number. This means no two ITAR controlled data exports can have the same identifier or "number" (which could be alphanumeric). Not only must each export be uniquely identifiable, they must be 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 ITAR controlled data upload process.

5.1.2 Internal Processes

Describe your internal process for documentation control, from the moment the ITAR controlled data 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 ITAR controlled data independent of Spacelink.
- Who makes the determination on whether data marked for export is ITAR controlled or non-ITAR controlled? (Not all ITAR controlled data is technical & not all technical data is ITAR controlled).
- How are documents routed and approved internally prior to DTSA/SD review?
- How are data exports tracked?
- Who is the POC for documentation control?
- How are ITAR controlled data packages archived?

The following statement must be added under this TTCP section:

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

DTSA 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 controlled data delivery is only as authorized by the appropriate export control and DTSA approvals.

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

5.1.3 Documentation Markings

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

- DTC Case Number (the export authorization, this includes identifying the correct and current amendment);
- The Unique Data Identifier; and
- An ITAR 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/SD for approval. Markings should be added prior to DTSA 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 TA xxxx-xx. 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, TA xxxx-xx (Doc no. xx)"

5.2 DTSA Review

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

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

5.3 Request for Waiver/Exemption Process

The ITAR controlled data review proviso contains circumstances where companies may request that DTSA/SD review of ITAR controlled (technical) data 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/SD. A list of such document/data may be listed within the waiver section of the TTCP, or added as an attachment.
- ITAR controlled data that is similar to that already approved by DTSA/SD.
- 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.

5.3.2 Waiver Requests via TTCP

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

DTSA 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 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 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, 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 ITAR 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 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 (Activity Chair or designee, export control official, etc.) at the technical interchange that will ensure compliance with technology transfer controls; for this document, this person will be referred to as “Activity Chair”.

The applicant must insert the applicable Conduct of Technical Interchanges wording below into the TTCP:

Conduct of Technical Interchanges. “All technical interchanges will be held under the subject TAA and will only include signatories to the agreement and applicant approved passive attendees.”

Conduct of Technical Interchanges. “Technical interchanges may be held under multiple TAAs. 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 agreements in use 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 said 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.”

As with all aspects of the TTCP, the controls established apply whether or not a DTSA monitor is present.

6.2 Attendance Roster

An Attendance Roster is required for all 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 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 (janitors, cafeteria workers, etc.) and why.

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 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, ultimately, at your invitation. These U.S. persons have no export authority, and therefore, may not participate in any of the technical interchange. For that very 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 DTC 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, at 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 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 or technologies would require subsequent DTSA 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.

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 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 they are not face-to-face. Each participating party, individually or as a whole, either calls a bridge line or a "personal" line (*e.g.,* office, conference room, etc.), the latter of which normally has some kind of teleconferencing capability. For any TAA that requires DTSA monitoring or a TAA where the U.S. Government reserves the right to monitor, companies are not allowed to have both U.S. and foreign persons in the same room.

Discuss any nuances or differences in the way you handle teleconferences/ videoconferences from meetings; many of the controls will be the same for both.

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)."

An agenda should be provided with the Monitor Request (see section 6.8.2 below) for the teleconference/videoconference. The company will coordinate with the DTSA monitor regarding the supply of any supporting data or documents to be used during the meeting, such as briefing slides or faxes.

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. The Activity Chair is required to maintain positive control to the greatest extent possible (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 must 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 plan so long as they allow DTSA to fully understand how the company will accomplish the topics addressed. A sample outline of a set of annexes is provided in Section 10.

The following statement must be added to the TTCP:

"Annexes must be provided to DTSA no later than sixty (60) days prior to shipment of any ITAR-controlled hardware. Companies may contact DTSA 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 number 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 on site.

6.7 DTSA Monitors

If monitoring is required, or if the U.S. Government reserves the right to monitor, the following text must be included in this subsection (tailor to your authorization):

"Attending DTSA Monitors at ITAR controlled meetings will not, unless previously coordinated, review data on-site. They will, however, review change-pages to ITAR 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 "Not applicable."

6.8 Notification Requirements

6.8.1 Timelines

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

6.8.2 The Monitor Request

All requests for, and any changes to, DTSA monitoring must be submitted via Spacelink as a Monitor Request. Follow-up questions may be addressed by calling the DTSA Administrative POC. DTSA's objective is to provide a response (*i.e.,* disposition within Spacelink) within one business day. A positive disposition to a Request only means DTSA has approved the Request itself. Actual support by Monitors is subject to personnel availability.

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)/Space Directorate (SD).

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 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 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 TA 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. Minor anomalies are defined as simple manufacturing defect discussions such as solder joint, component/subsystem/system/spacecraft test failures, etc. without going into detailed discussions with the foreign customer.

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 such as solder joint, component/subsystem/system/SC test failures, etc. that does not require detailed discussions with a foreign customer.
- 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 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.

7.2 Facility Layout

Provide a basic graphical overview of the facilities where ITAR controlled meetings may take place. Identify or describe where the "common" areas are, if applicable (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 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, etc.) and the privileges for each (access areas, etc.); 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 tell a visitor from an employee, etc.).

7.5 Foreign Person Residence

If an export authorization allows foreign persons as residents in company facilities describe their activities as follows:

7.5.1 Facility Arrival

Foreign residents should be provided training specific to their residency at the U.S. facility prior to being granted any access. This would include a review of the relevant TAA and its Department of State provisos (details of 7.5.2 should be included or companies can provide the reference in their TAA if this topic is covered adequately in the agreement). Badging, building access and restrictions, computer access, escort and non-escort requirements and restrictions (work areas, cafeterias, etc.), facility layouts to include the location of office space(s), how to check in/out, and when they are authorized to be in the same facility (regular business hours versus off-duty hours) should also be addressed.

7.5.2 Foreign Person Access

If not covered in the applicable TAA, companies should provide specific details explaining the level and scope of the ITAR controlled data and defense services that foreign persons will have access to or receive during their residency. Further, describe what type of work they can observe and how close they can be when observing. An example would be the monitoring of any assembly, integration, or test activities. Will they play any role whatsoever beyond observation at any time? Also, address the procedures the company will have in place to properly control foreign persons when in ITAR controlled areas and how the company will prevent unauthorized access to any U.S. Government programs, if applicable.

7.6 Computer/Networked Systems

Describe procedures that are used to maintain positive control of company computer and networked systems. Clearly state what computer system access foreign persons will have on company systems. If foreign persons are to have access to company computer systems, address the issue of their access and what measures are employed to ensure foreign persons do not have access to unauthorized data of any kind. Describe how computer equipment will be protected at TIMs at third-party facilities in the U.S. (i.e. a hotel conference room) and abroad is required. Encryption, password protections, networking, flash/thumb drive use/exchange, etc. are also appropriate in this subsection.

Identify the facility's WIFI capabilities, and/or if the public or foreign parties have the capability to join a network (WIFI or hard wire) within your facility. Identify the firewalls or

safeguards that prevent a non-signatory from gaining access to ITAR controlled material via this “public” network.

7.7 Access for DTSA Monitors

Describe the process that allows Monitors to have full access from the time the Monitor arrives at your facility to the time the Monitor leaves. Companies should describe the badge in detail. If there are situations where an escort is required, explain in detail why and how you intend to satisfy the DTC proviso (this explanation should include a detailed procedure for both normal working and after hours); picture or no picture; etc. Describe the badging process itself and what, if anything, is needed from DTSA beforehand. DTSA monitors will not be present for any hazardous operations. Monitors will observe the Activity Chair as they maintain positive control to the greatest extent possible (i.e., attendance sheets, using remote monitoring, if available) and participate in any planning sessions beforehand in order to understand what is being accomplished.

8.0 U.S. PERSONS ASSIGNED TO FOREIGN PARTY FACILITIES

If not applicable insert in this section of the TTCP: “Not Applicable”.

8.1 Authorization

Identify the export authorization allowing the company to have a U.S. person(s) assigned to a Foreign Party facility. Also, describe the role of the assignee(s).

8.2 Physical Location

Describe where the U.S. person(s) will be assigned.

8.3 Documentation Control

Describe how releasable and non-releasable ITAR controlled data will be handled. Address how all ITAR controlled data will be controlled.

8.4 Computer/Networked Systems

Describe how computer and network security will be handled. Discussions of encryption, password protections, networking, flash/thumb drive use, etc. are appropriate in this subsection. Also identify the facility’s WIFI capabilities, and/or if the public or foreign parties have the capability to join a network (WIFI or hard wire) within your facility. Identify the firewalls or safeguards that prevent a non-signatory from gaining access to ITAR controlled material via this “public” network.

8.5 ITAR Controlled Meetings

Describe how U.S. person(s) will be involved in ITAR controlled and non-ITAR controlled meetings. If DTSA monitoring is part of the export authorization, then this person may only participate in non-ITAR controlled meetings with the Foreign Parties and may not provide defense services. All ITAR controlled interchanges in which they will participate must have

a DTSA monitor unless waived/exempted. For the U.S. person(s) to be an active participant in a teleconference, they must be in a different location than the Foreign Parties. If the U.S. person(s) remains in the same room, they must remain passive. In cases where DTSA monitoring is not required, company policy applies in accordance with the TAA and TTCP.

If a foreign facility contains a “U.S. only” controlled area, are there any procedures to allow a foreign person into that area for facility maintenance? How is the U.S. only data/hardware protected?

LAUNCH CAMPAIGN SECURITY PLAN (LCSP)

SAMPLE OUTLINE AND SECTION DESCRIPTIONS

(Attachment B to the TTCP Guidelines)

Title Page

Include your license or DTC case number, your company name and address, and date.

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 Export Authorizations (TAAs, DSPs, etc.)
   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 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 Interface
   3.3. Key Foreign Participants
   3.4. List of Companies, TAAs, 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)
5.1.2. Manned vs. Remote Monitoring
5.1.3. Escorting
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.
- 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 State Department. 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 (video surveillance, locks, tamper-evident seals, etc.)

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. Escort
6.3.2. Public/VIP Tours
6.3.3. 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).

6.3.4. 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.

6.3.5. Joint Operations Description
6.3.6. DTSA Requirements/Participation
6.3.7. Briefings/Daily Meetings

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 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.

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. Staffing Plan
8.2.1. Security and ITAR control Personnel Staffing
8.2.2. Work Tempo of Launch Campaign Operations
8.3. Acronyms/Abbreviations/Definitions