TECHNOLOGY TRANSFER CONTROL PLAN GUIDELINES

REVISION 4.4

06 July 2026

DEFENSE TECHNOLOGY SECURITY ADMINISTRATION
Office of the Under Secretary of War
Acquisition and Sustainment (A&S)
International Armaments Cooperation

REVISION	REASON FOR CHANGE	REVISION DATE
4.0	Complete re-baselined to Revision 4.0. Significant changes throughout the whole document.	11 Jun 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.	01 Nov 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.	01 Jul 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 Aug 2021
4.4	Update includes: 1. Titles/Dates Administrative section updates 2. Incorporation of EAR/CCL terms 3. Incorporation of TSA requirements	06 Jul 2026

TECHNOLOGY TRANSFER CONTROL PLAN GUIDELINES

Introduction:

This Technology Transfer Control Plan (TTCP) is prepared and submitted to Defense Technology Security Administration, Export Control Directorate (DTSA/ECD), Missiles/UAVs/Spacecraft Division (MUS) to meet the requirements of ITAR/EAR export control authorizations.

This TTCP defines the process and procedures to be implemented to ensure defense articles, defense services, technical data and technology approved for export will be transferred only to the authorized parties on the license. The TTCP is NOT a substitute for or interchangeable with a company specific Technology Control Plan (TCP). Although sections of a TCP may be used to fulfil TTCP requirements, the TTCP should focus only on the activities and scope of the individual export license and the parties identified on the license.

These guidelines are intended to assist applicants in developing a comprehensive TTCP. Although not mandatory, it is recommended applicants follow this guideline to obtain a TTCP approval in the minimum amount of time.

DTSA/MUS Point of Contact for this guideline:
Email: dtsa.mc-alex.ecd.mbx.ttcp-request@mail.mil
Phone: 571-372-2541 or (571) 372-2312

Procedure for submitting TTCP for DTSA Review:

A Spacelink account is *required* to submit TTCP. Spacelink is a web-based program used by DTSA and Industry to facilitate interactions on TTCPs, technical data review, and technical monitoring requests.

1. Contact DTSA/MUS POC to request a Spacelink account.

2. Upload the license (DSP-5, Technical Assistance Agreement (TAA), and Statement of Work (SOW) as a single searchable Word or Acrobat format document into Spacelink.
   - DTSA accepts the license files into Spacelink.

3. Upload the draft TTCP (in Word/Acrobat) into Spacelink. TTCP file name must track with the license authorization, e.g., 1234_00A should be associated with TA-1234-00A. Use naming format: 1234-00_TTCP_DRAFT.
   - DTSA will Approve or Reject with Comments.

4. Upload the final TTCP into Spacelink. Use naming format: 1234-00_TTCP_FINAL.
   - DTSA approves the final version.

TTCP OUTLINE

Sample

Title Page

Include program name, export license number, company name and address, TTCP version and submittal date.

Record of Changes

Summarize the evolution of the TTCP from initial through the latest approval in tabular format, include the revision number, TAA amendment, and reason for the submission, (*e.g.,* required by latest amendment), and approved date.

Table of Contents

Should contain the following sections and annexes. If a section is not used, state "Not Applicable".

1. 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 at least one point of contact(s) for the TTCP, Launch Campaign, and Export Control Official. Include job title, phone number, and email address for each. Multiple POCs are recommended; both technical and administrative.

2. Scope

2.1. Authorized Export

Summarize the scope of the export authorization and list the DOS/DOC license provisos.

2.1.1. Hardware Summary

List any/all ITAR/USML categories/sub-categories and ECCNs, if authorized.

2.1.2. Technical Data/Technology and Defense Service Summaries

Summarize in a few sentences from your license submittal to State or Commerce.

2.2. Summary of Export Authorizations

List chronologically the license authorizations and amendments. Include approval date and a summary. For examples:

- 1234-20 (050123456), approved 12 Dec 21, Marketing TAA for 'X1' Spacecraft
- 1234-20A (050234567), approved 30 Mar 22, added scope, to include satellite build, manufacture, and delivery.

The following statement (or a very similar one) 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

List all the Signatories (U.S and foreign), with a brief description of roles and responsibilities.

2.4. Foreign Persons

Companies should acknowledge their responsibility for ensuring all foreign persons with access to controlled defense articles, defense services, technical data or technology are authorized under an appropriate export authorization (as employees or embedded contractors of a foreign licensee) or exemption 22CFR126.5 (Canadian) or 126.7 (AUKUS). If an employee is a dual/ third country national, he/she should have the appropriate authorization 22 CFR 124.8(5) or 22 CFR126.18 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. There cannot be any passive foreign person attendees.

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

List all foreign personnel with a DOS/DOC license associated with this agreement and attach the corresponding licenses to the TTCP as an Appendix/Exhibit.

2.4.2. U.S. Persons Working for Foreign Companies

The following statement (or a very similar one) must be added under this TTCP section:

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

2.5. Authorized Areas for Transfer

2.5.1. Territories Approved for Export Activities

Identify countries or other specific locations where exports are authorized to take place per your license.

2.5.2. Dual/Third Country National Employees and Non-Disclosure Agreements (NDA)

State the countries from which dual/third country national employees are authorized by the export license. Describe when and for which countries Non-Disclosure Agreements (NDA) are used, if any.

2.5.3. Sublicensing

If sub-licensing is authorized, identify the authorized entities. If there are many sub-licensees, refer to the specific portion of the license where they are listed.

2.6. Separate or Independent Export Authority

Identify any other U.S. entities authorized to perform exports without your direct approval.

2.7 Other Relative Agreements

If the export activity involves any country-to-country based agreements, such as Technology Safeguards Agreements (TSA), for MTCR Cat I launch vehicles. Identify the TSA by name and attach a copy of the TSA and any side arrangements as an Appendix/Exhibit. Identify unique license provisos or limitations imposed for the TSA in this section.

3. DTSA Monitoring Provisos

Identify all applicable provisos related to DoD/DTSA monitoring. This includes TTCP review, ITAR controlled technical data review, monitoring of ITAR controlled technical meetings and launch activities, and reimbursement procedure (if applicable).

4. Export Compliance Training

4.1. U.S. Persons Training

Companies should acknowledge that all U.S. persons who represent U.S. signatories or end-users must have completed export compliance training prior to interface with foreign parties. Indicate who (e.g. U.S signatory/POC) will provide the training, frequency of training (semi-annual training is recommended), and how training records will be maintained.

Training must also be provided to Non-Signatory Attendees. Non-signatories are U.S. persons allowed by the applicant to attend controlled meetings, but only as non-participants (passive or silent attendees). Non-Signatory Attendees are not covered by an export authorization, and therefore, have no export authorization. Identify potential Non-Signatory Attendees (like

consultants or legal entities), their relationship to the licensees, and a brief description of their role.

Describe your plan to conduct out-of-cycle training for special circumstances such as a change in the scope in the TAA, new hires, change in the law affecting regulations/procedures, or if there is a violation (consent decree) or compliance directive.

4.2. Details of Training

This section may closely align with a company TCP, and sections may be copied in whole from that document here, but emphasis should be on unique training being conducted for this license activity and not just general export control training. At the minimum, training must provide instruction on the following:

- The contents (to include scope, limitation, and conditions) of the export authorization and TTCP, general ITAR awareness (e.g. not discussing ITAR-controlled data, perform defense services or transfer technology in common areas), company policies pertaining to exports, and consequences of violations of export law and regulations.
- The difference between ITAR-controlled data and other types of EAR controlled, sensitive, or proprietary data or technology.
- Who and how to protect ITAR-controlled technical data at technical interchange and joint operations at U.S. locations and at foreign signatories' facilities.
- Procedure to protect access to controlled technical data on IT networks and to transfer electronically controlled technical data.
- Identify the U.S. Only areas, including those designated for U.S. Launch Vehicles, U.S. Spacecraft, U.S.-Related Equipment, and U.S. Technical Data. Indicate how entry into U.S. only areas be restricted and monitored, and who is responsible. What happens if there is a breach?
- If the license authorization requires all activities must be in accordance with a Technology Safeguards Agreement (TSA), include the pertinent sections.
  - The pertinent sections of the TSA, related to definitions of "Controlled Areas" and "Segregated Areas" or U.S. only areas.
  - Pertinent sections of the TSA, General Provisions.
  - Pertinent sections of the TSA, Control of U.S. Launch Vehicles, U.S. Spacecraft, U.S.-Related Equipment, and U.S. Technical Data.
- Rules for escorting foreign parties to restricted and U.S. only areas.
- 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 should not be asked.

5. ITAR Controlled Data

5.1. Documentation Control

5.1.1. Unique Data Identifier

ITAR controlled technical data or Commerce controlled technology to be exported must have a unique identifier or a document control number. Each export must be uniquely identifiable, recorded and tracked.

Provide an example of your naming convention.

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

5.1.2. Internal Processes

Describe your internal process for documentation control, from the moment the controlled technical data is generated until the time it is exported. This should include:

- Process to determine whether the technical data marked for export is ITAR-controlled.
- How are technical data documents routed and approved prior to DTSA/MUS review?
- How is technical data exported tracked?
- Describe recordkeeping procedure. As a minimum, records must show what has been exported, to whom, and when.
- Who is the point of contact for documentation control?

The following statement (or a very similar one) 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 authorizations."**

Submitting your documents into Spacelink does not relieve your company of the obligation to maintain company records of transactions (22CFR122.5 or 15CFR762) involving ITAR/EAR items.

5.1.3. Documentation and Email Markings

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

- DOS/DOC Identifying Number (export authorization and/or 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. Markings should be on the document submitted on Spacelink for 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 technical data (ITAR 120.33) being transmitted under License (050xxxxxx). 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."**

Examples of information that should be placed in the footer of each page of ITAR/EAR controlled data is shown below:

> **"Contains ITAR technical data subject to U.S. Export Control."**
>
> **"Contains export-controlled data subject to U.S. Export Law."**

Please note: DTSA does not recommend applicant ever using the document marking **"Confidential"**. If the document is sensitive, proprietary for business/competition reasons use the marking **"Business Proprietary"** or **"Business Confidential**", as one may interpret it as a classified U.S.G. marking.

In addition, consider attaching export/privacy warnings to emails should an email be sent to incorrect parties. Sample:

Notice: This e-mail is intended solely for use of the individual or entity to which it is addressed and may contain information that is proprietary, privileged, and exempt from disclosure under applicable law. If the reader is not the intended recipient or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. This communication may also contain data subject to U.S. export and privacy laws. If so, that data subject to the Export Administration Regulation or International Traffic in Arms Regulation cannot be disseminated, distributed, or copied to foreign nationals, residing in the U.S. or abroad, absent the express prior approval of the U.S. Department of Commerce or Department of State. If you have received this communication in error, please notify the sender by reply e-mail and destroy the e-mail message and any physical copies made of the communication.

5.1.4. Electronic Transfer of Technical Data

Describe who has access to the controlled data and any limits. Are U.S. Employees, Foreign National employees, foreign signatories, and visitors treated the same?

Is IT access managed, monitored, and audited regularly? Are documents password protected?

Describe if/how the technical data will be transferred electronically to work sites/locations (U.S. and abroad). Are employees authorized to use USB drives to copy data?

Describe recordkeeping process of technical data exported electronically.

5.2. DTSA Review

If the license authorization includes a proviso that requires DTSA review of technical data, cite the proviso, and include the following statement:

> **"(*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's receipt of the submission is counted as Day 1."**

5.3. Request for Waiver/Exemption Process

There are certain circumstances when DTSA review may be waived. Please read the data review proviso for waiver conditions and address them here if you intend or do not intend to use them. Actual waiver requests can be submitted via Spacelink (See section 5.3.3).

5.3.1. Types of Data that can be Waived.

Repetitive data/documents or new technical data that is similar to that already approved by DTSA. A list of such data/document must be listed within the Waiver Request section or added as an Exhibit/Attachment.

EX: Testing results are exempted. However, reports including test analysis, procedures, or derived conclusions still require DTSA review.

5.3.2. Waiver Requests via TTCP

List the ITAR/EAR controlled data to be exported.

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

The following must be included with the waiver request:

- Scope of data requested to be waived.
- Statement that certifies the currently submitted ITAR/EAR controlled data is similar to that previously approved for release.

- Reference the previous approval of the data in Spacelink.
- Expiration date (companies may utilize dates or milestones as the expiration date).

5.4. Unique definitions, terms, or acronyms

Define unique company terminology used in the TTCP and identify if you are not using standard ITAR or EAR definitions as specifically defined by State or Commerce regulations.

6. Technical Interchange Meetings

Technical interchange may include meetings, teleconferences, videoconferences, and joint operations where technical data is exported and/or defense services are provided. The terms "ITAR Controlled Meeting" and "Technical Interchange Meeting" (TIM) are used interchangeably for this document. This section assumes the technical interchanges are ITAR-controlled and defense services are being performed.

6.1. General Requirements.

The minimum technology transfer controls required for technical interchanges that must be addressed in TTCP are listed below. Companies should indicate the individual (e.g., Activity Chair or designee, export control official) attending the technical interchange 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 export license (license 050xxxxxx). All the participants must be export control trained."**

As with all aspects of the TTCP, the controls established apply whether a DTSA/MUS Monitor is present. The applicant must insert the applicable Conduct of Technical Interchanges wording suggested below into the TTCP:

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

For Conduct of Technical Interchanges held under multiple licenses, if applicable:
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.

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 (or a very similar one) 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 Activity Chair must ensure all attendees and required information are recorded on the attendance roster. The DTSA/MUS Monitor (if present) will review the roster and be provided an electronic copy after the event. The attendance roster must include Full name, Company, Nationality, and Signatory Affiliation. Non-signatories (U.S. person passive attendees) must list U.S. signatories that invited them to attend.

6.3. Non-Signatory Attendees

The Activity Chair must be able to identify all Non-Signatory Attendees. 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 at your invitation. These U.S. persons have no export authority, and therefore, may not participate in any of the technical interchange.

6.4. Walk-Ins

Describe the procedure to ensure that any person who arrives after a technical interchange has begun are authorized to be in attendance. The Activity Chair needs to know if they are authorized to be in attendance. Companies 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.

Discuss how the Activity Chair will verify if a walk-in attendee is authorized when the technical interchange occurs at foreign signatories' facilities.

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

6.5.1. Copies of the Export Authorizations

The Activity Chair must have in his/her possession copies of export authorization and TTCP.

6.5.2. Participant Verification

The Activity Chair must ensure technical data or defense services transferred only to authorized Parties. The Activity Chair must be able to identify and verify all participants and whether those who are U.S. persons have had completed their export compliance training.

6.5.3. Technical Data

The Activity Chair must have, as the minimum, a list of the technical data approved for release.

6.5.4. Change-Pages to Approved Technical Data

The Activity Chair must notify the attending DTSA/MUS Monitor, if present, of any change-pages made to approved technical data prior to its discussion or presentation. Any change involving the addition of technical content will require DTSA/MUS approval.

6.6. Specific Controls

Describe the technology control procedures for meetings, telecons, and joint operations.

Describe procedure if the event were held in foreign person's facility or hosted by foreign signatories.

Describe how positive control of technical data will be maintained, along with any specific procedure you may have. All technical data and discussion will be limited to what already been approved for release.

6.6.1. Meetings

Discuss how control of the environment, control of technical data, and any other controls during meetings will protect technical data.

Identify potential meeting locations in the U.S. and at foreign signatories' facility. Describe the physical controls or any limitations for each location.

6.6.2. Teleconferences/Videoconferences

Discuss any differences in the way you conduct teleconferences/ videoconferences from meetings; many of the controls may 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.

A TIM where both U.S. and foreign signatories are in attendance MUST have a DTSA/MUS Monitor present, unless waived.

6.6.3. Launch Campaigns and Joint Operations

Discuss controls used for launch campaigns and joint operations with foreign parties not specifically called out elsewhere. Ensure it is stated that an Activity Chair, or his delegated representative, will monitor all joint operations. An exception is hazardous operations where 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 to understand what is being accomplished.

Identify both controlled or segregated areas (or any area where U.S.-only operations are conducted. Describe who controls physical/electronic access and by what means. Describe security controls for these areas in detail. If a TSA contains specific language on access, security or controls, address each separately. A Launch Campaign Security Plan must be included as an Annexes to the TTCP. Other documents such as Joint Operations Plan, a Training Plan, a Transportation Plan, a Debris Recovery Plan, and/or any plans deemed necessary for a specific mission may also be required. These Annexes may be provided as one document with the TTCP or as separate Appendix/Exhibit.

The following statement (or a very similar one) must be added to the TTCP:

> **"Attachments, Exhibits, or Annexes to the TTCP will be provided to DTSA/MUS no later than forty-five (45) business days prior to shipment of any ITAR/EAR- controlled hardware"**

6.6.4. Launch Failure Review Meetings

If this does not apply to your export authorization, state "Not Applicable."

Per 22 CFR 124.15(b) all launch vehicle failures (crash) investigation discussions require a separate Department of State License, unless said discussions are within the scope of your authorization (e.g., heritage failure data). 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 (or a very similar one) must be added under this TTCP section:

> **"All data and presentations developed and exported during any Launch Failure, Oversight, or Investigation meetings shall be uploaded into Spacelink by (*company name*), including the data approved by DTSA on site within 72 hours."**

6.7. DTSA Monitors

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

> **"Attending DTSA/MUS Monitors will not be expected to, unless previously coordinated, review data on-site in real-time. 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 DTSA monitoring in the authorization, state that it is "Not applicable."

6.8. Notification Requirements

If your license authorization includes a DTSA monitoring proviso, you must notify DTSA/MUS in advance of TIMs with foreign persons. To request DTSA/MUS support of ITAR TIM, a Monitoring Request must be submitted into Spacelink.

If you have a reimbursable program, you must provide a forecast of TIMs and Launch Campaigns by Sep 1st for the upcoming government fiscal year (October – Sept). This allows DTSA/MUS to provide an estimated cost of DTSA monitoring.

6.8.1. Monitoring Request

A Monitoring Request must be submitted in Spacelink. It must include a detailed agenda and a list of documents to be discussed at the technical interchange. If a detailed agenda is not available when the Monitor Request is submitted, a detailed agenda must be provided via email to the assigned DTSA Monitor prior to the meeting.

6.8.2. Timelines

Monitoring Request must be submitted in Spacelink at least forty (40) business days in advance for launch activities; thirty (30) business days 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 U.S.; and five (5) business days for teleconferences/videoconferences.

6.8.3. Exceptions

Non-ITAR controlled meetings (EAR or business only) 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 War (DoW) Monitor present unless exempted by the DoW/Defense Technology Security Administration (DTSA/MUS). The following statement (or a very similar one) 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 on the export authorization, but where companies DO NOT reimburse the U.S. Government.

The following statement (or a very similar one) 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, if required by the waiver wording,"**

On the Monitor Request, include the following statement:

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

6.10.1. Non-Reimbursable Program Exemptions

The following ITAR controlled meetings may also be exempt from notification, if 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.

7. Physical & Information Security

For each facility and each location used for the scope of the activity (office spaces, manufacturing areas, integration facility, clean room, and launch sites), describe the Physical and Information security procedure. At a minimum, each of the following subsections (unless previously noted) must be addressed. Where appropriate, cite and paraphrase existing and/or standard security procedures that directly relate to this TTCP.

7.1. Security Management

Describe the site clearance levels if approved for classified, include any SCIFs or other restricted areas. Specifically address any foreign owned/operated/controlled facilities and what agency granted the clearance.

Describe the security process, including the "who" (*e.g.,* security management team/lead and key personnel), and the "what" (e.g., the basic security approach, such as using standard industrial security practices or if other published guidelines are used, etc).

Explain procedures for handling security-related problems or shortfalls that may arise (e.g., reporting of incidents, process change due to recently exposed vulnerabilities).

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 in controlled areas.

7.2. Facility Layout

For each of the facilities where TIM or joint operations may occur, provide a layout (charts/diagrams) of the facilities, highlighting program areas, entrance, "common" areas, location of card readers, cipher locks, emergency exits, etc. Identify or describe building, facility, or areas that are designated for (1) the approved program, (2) U.S. only parties, (3) joint operation activities, and (4) foreign parties.

For processing/launch sites:

- Indicate where the SLV/payload/spacecraft processing, joint operations, and launch vehicle integration will take place. Clearly identify areas that are designated for U.S. only Launch Vehicles, U.S. Spacecraft, U.S.-Related Equipment, and U.S. Technical Data. Indicate how entry into U.S. only areas be restricted and monitored, and who is responsible.
- Indicate where non-U.S. persons will be working. Discuss (1) the physical barriers and (2) network security procedure to ensure the non-U.S. persons can access to only what is authorized according to their respective license (s).

If the license authorization requires all activities must be in accordance with the Technology Safeguards Agreement (TSA) include the pertinent sections. Clearly identify areas that are designated in the TSA as “Controlled Areas”, “Segregated Areas” for U.S. Launch Vehicles, U.S. Spacecraft, U.S.-Related Equipment, and U.S. Technical Data.

7.3. Physical Barriers/Separators

Address the use of physical barriers/separators, 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 may have other commercial or U.S. Government spacecraft in work. In this case, companies should discuss plans and procedures for ensuring foreign persons only have access to what they are 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.

Provide a sample. If not available, then describe them. Clearly identify what badge is allowed entry into the U.S only areas.

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. Information Security Controls

Describe procedure for verifying user's access request, monitoring access to network, and terminating user's access when needed.

Describe how the controlled technical data stored in the IT network be protected from unauthorized access. What happens if a breach is detected?

For non-U.S. person employee working in the U.S. – describe the procedure to allow access (both local and remote) to IT system with controlled technical data, how to ensure the non-U.S. persons can only access to authorized technology.

For non-U.S. person employee working remotely oversea - discuss any special controls.

If foreign visitors will be provided access to the network - discuss IT controls.

Remote access to IT system for U.S. person while on travel at foreign facilities, such as launch sites.

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

7.6. Access for DTSA Monitors

DTSA Monitor should be provided with non-escort badge and have full access to the facility, where technical discussions, satellite processing, and launch activities take place. Indicated areas where special access may be required due to security or hazardous operations.

The Activity Chair should be informed that DTSA monitors can observe technical interchange meetings and how the Activity Chair maintains positive control to the greatest extent possible (i.e., attendance sheets, using remote monitoring, if available).

The Activity Chair should be informed that DTSA monitors have the authority of stopping a TIM and requesting a caucus with the Chair to discuss concerns if the TIM discussions might be interpreted as violating technology transfer restriction.

LAUNCH CAMPAIGN SECURITY PLAN (LCSP)

OUTLINE AND SECTION DESCRIPTIONS

(Attachment A to the TTCP Guidelines if needed)

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 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 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
5.4 Release of ITAR/EAR Controlled Data
5.6 Meeting Protocols / ITAR/EAR Controlled Meetings
5.7 Storage of Technical Data and Related Equipment
5.7.1 Storage of defense articles and technical data 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.)
5.7.3 Include any measures to be proposed/used for the destruction of technical data or hardware when in a foreign territory. (e.g. use of burn barrels, industrial or commercial shredders, compactors, 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 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 spacecraft 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/U.S.G. 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.
6.4.2 Describe any hardware or related items to be left behind for successive missions and an accounting of any hardware destroyed in place and not returning to the U.S.

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