

TECHNOLOGY TRANSFER CONTROL PLAN DEVELOPMENT GUIDELINES

Revision 3.4

28 August 2013

Defense Technology Security Administration

Record of Changes

<u>Revision</u>	<u>Reason for Change</u>	<u>Revision Date</u>
3.0	Complete Update from Previous Version.	31 Jan 11
3.1	Moved Section 4.2, Foreign Persons, and Section 8, Third Party Foreign Nationals & Dual Citizen Employees to Section 2, Scope; Combined Sublicensing, Non-Disclosure Agreements, and Authorized Countries of Citizenship for Dual/Third Country Foreign Nationals into new paragraph as Section 2.5 named Authorized Areas for Transfer (ITAR 124.7 (4)) with major changes; Added new last sentence to Section 3, DTSA Monitoring Provisos; Minor update and examples of ITAR markings added to Section 5.1.3, Documentation Markings; Changed "export control official" to "Activity Chair throughout Section 6, Technical Interchange; Updated Section 6.6.2, Teleconferences/Videoconferences; Updated Section 6.6.3, Joint Operations, and Section 7.7, Access for DTSA Monitors; Complete rewrite of Section 7.5, Foreign Person Residence; Minor grammatical updates to Section 8.1 and 8.2, Authorization and Physical Location (formerly Section 9.1 and 9.2); Update to Section 8.5, Technical Interchanges (formerly 9.5); and minor grammatical changes to Section 9, Annexes to the TTCP (formerly Section 10).	28 Apr 11
3.2	Added Section 2.4.1 describing U.S. Persons working for a foreign company; Added Section 2.5.1, Territories Approved for Export Activities; Renumbered Section 2.5; Deleted Section 2.6 Re-export and/or Retransfer Authority; added common definitions to Section 6.8 to aid in TTCP consistency for non-reimbursable programs; and changed due date of documents in Section 6.6.3.	27 Jun 11
3.3	DTSA POC Phone Numbers Updated; Updated Section 2.1 to advise companies that they should indicate any DoS limitations in their authorized export description; Made minor changes to Section 2.4 to enhance clarity; Updated Section 4.2.1, Description of Training, to add "TAA" which had been inadvertently left out, added language under "ITAR Awareness" that employees should not discuss technical data or defense services performed in common areas, and added the requirement for companies to add how to ask proper questions of foreign signatories to their training; Updated Section 5.1.2 to include a required statement from the applicant regarding technical provisos and limitations in the technical review process; Clarified technical data DTSA is not required to review in Section 5.3.3; Updated 6.6.2, third sentence, to include instances of TAAs where the USG reserves the right to monitor; Added word	6 Sep 12

	<p>“operations” to line 4 of Section 6.6.3 as it had been inadvertently left out; Updated Section 6.7 to clarify DTSA Data Review in the field; Clarified that only technical meeting minutes are required for a company’s library in Section 6.8.2 (5); Added requirement in Section 7.6 for companies to explain how they protect computer at TIMs.</p>	
3.4	Updated POC for Non-Reimbursable Programs	28 Aug13

TECHNOLOGY TRANSFER CONTROL PLAN DEVELOPMENT GUIDELINES

DTSA Points of Contact (POC)

<u>Reimbursable Programs</u>	<u>Non-Reimbursable Programs</u>
Mr. Juan Paz 571-372-2469 juan.paz@dtsa.mil	Maj Steven Zollars 571-372-2536 steven.zollars@dtsa.mil
None	Mr. Brian Glancy 571-372-2539 brian.glancy@dtsa.mil
<u>Administrative POC for All Programs</u> Ms. Sheila Rhett 571-372-2472 sheila.rhett@dtsa.mil	

REQUIREMENT

Per the Arms Export Control Act implemented in accordance with 22 CFR 120-130 (International Traffic in Arms Regulations), certain defense articles require special export controls.

REFERENCES

DoD Monitoring Program - for information and details, refer to the following:

1. PL 105-261, Title XV, Sections 1511-1516
2. PL 106-65, Title XIV, Section 1409
3. 22 CFR 124.15

PURPOSE

The purpose of this document is to provide guidelines on the content of TTCPs. The main communication tool for submitting licenses, TTCPs, data, and monitoring requests is Spacelink. Please contact the DTSA Administrative POC (see above) to initiate Spacelink company and user accounts. For further details, refer to the *Spacelink Industry Software User Manual*. All required documentation will be submitted via Spacelink.

LICENSE FILES

1. License Files (agreements) are file copies of the export authorization. This includes the executed copy, along with any attachments, and the DTC Approval Letter; any amendments thereto (again, complete with any attachments and its DTC Approval Letter).

2. License Files must be in Adobe PDF and be in a format that enables electronic scanning for specific words.
3. License Files must be submitted via Spacelink before any TTCP, technical data or monitor request submission against the export authorization can be accepted for review.
4. Uploading License Files is designed to be a “one-time” action that will place all export authorizations into Spacelink, DTSA’s central repository.

SUBMITTING TTCPs TO DTSA

1. Any TTCP requiring DTSA approval, whether newly developed or revised (beyond clarifications and edit corrections), must first be submitted into Spacelink as a draft. Once *Approved* (or *Approved with Conditions*), the final TTCP must be submitted. Only then, after the final TTCP is approved, may technical assistance, defense services, and the transfer of technical data under the license be allowed. If desired, advance copies may be submitted to the TTCP POC for review and comment prior to being submitted as a draft in order to expedite the process. To expedite approval, it is recommended that companies use track changes in the document to enable faster review.
2. In order to upload TTCPs that do not require subsequent DTSA approval (i.e., administrative updates such as adding signatories or countries), companies must first contact the appropriate POC so that the existing TTCP can be deleted from Spacelink (assuming the new document is taking the place of an already-existing final TTCP). After this deletion, companies may then upload the updated TTCP into Spacelink as a final submission.

GENERAL INSTRUCTIONS

1. DTSA has identified sections that must be addressed and be included, at a minimum, in any TTCP. If a section does not apply, simply state that. Companies are free to add sections and provide as much information, with as much detail in order to fully explain policies, procedures, and/or processes used to maintain technology transfer controls.
2. Required sections and required statements, and additional discussion points on the requirements of each section are presented in this guideline. Required statements are in **bold** text here, but would not be bold in the actual TTCP. Each section contains the necessary requirements that the TTCP must address.
3. All pages must be numbered. This includes all annexes and any other attachments. Companies may use a local page numbering scheme for annexes as long as the respective annexes are identified. For example, if Appendix D has a total of 26 pages, it would number the pages D-1 through D-26. It would not be acceptable to simply number them 1-26.

TTCP TABLE OF CONTENTS WITH SECTION DESCRIPTIONS

TITLE PAGE:

The title page must include: **Technology Transfer Control Plan (TTCP)**
[DTC Case]
[Company Name]
[Company Address]
[Date of the TTCP]

RECORD OF CHANGES:

Summarize the evolution of the TTCP, from initial approval through the latest approval. A tabular format has proven to be effective. 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; etc.)

1.0 INTRODUCTION:

1.1 Purpose. Identify the purpose of the TTCP. For instance, "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. At a minimum, identify a point of contact(s) for the TTCP (this may be an office or an individual), providing phone and fax numbers and email address(es) for each.

2.0 SCOPE:

2.1 Authorized Export. Summarize the scope of the export authorization. DTSA recommends re-stating from the license the exact authorization (e.g. the statement(s) following the "NOW, THEREFORE" clause); however, if applicable, companies must acknowledge and incorporate any limitations to scope levied by the USG in the export authorization(s) into this paragraph. If there are Exhibits, Attachments, or Appendices, instead of copying and pasting large amounts of data into the TTCP, simply point the reader to its location in the license.

2.2 Summary of Export Authorizations. If there are amendments to the base agreement, add a one- to two-sentence/phrase 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. It is also required that both the 9-digit DSP application number be referenced along with any final TAA number issued by the Department of State.

Example:

- 1234-00 (xxxxxxxxx), approved 12 Dec 01, is a marketing TAA for Super Spacecraft XT.
- 1234-00A (xxxxxxxxx), approved 30 Mar 03, added scope, to include satellite build, manufacture, and delivery.
- 1234-00B (xxxxxxxxx) was 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.
- 1234-00D, (xxxxxxxxx), approved 13 Dec 03, includes launch services (minus on-orbit support); adds eight foreign signatories, drops one, corrects name of another; superseding provisos.

The following statement must be added:

If the 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.** (Insert applicant name) acknowledges their responsibility for ensuring all foreign persons who will have access to ITAR controlled defense articles (hardware or technical data) or defense services are authorized under an appropriate export authorization (as employees or embedded contractors of a foreign licensee). Additionally, if the employee is a dual/ third country national, they 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 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 (ITAR 124.7 (4)).**
- 2.5.1 Territories Approved for Export Activities.** State the countries or areas in which the transfer of Technical Data or Defense Services is licensed.
- 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 per 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, it is permissible to 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 monitoring. This includes requirements for: a TTCP; technical data reviews; monitoring of technical interchanges; and reimbursement procedure, if required. This will serve to let the reader know the extent of DTSA's involvement in the subject export authorization. The proviso for a library of technical data transferred is not a DTSA monitoring proviso.

4.0 EXPORT COMPLIANCE TRAINING:

4.1 U.S. Persons. In this subsection, companies shall acknowledge their responsibility (as the applicant) 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 is documented.

This includes providing an awareness briefing to Non-Signatory Attendees. Non-signatories are U.S. persons allowed to attend technical interchanges, but only as non-participants (i.e. passive 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, citing: 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 technical data or defense services performed 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 An explanation of how to properly ask questions of a foreign signatory. For example, leading or suggestive questions (“Have you considered...?”) could lead to a potential export violation. Instead, questions should be of a more general nature, such as, “How are you meeting my requirement?”

4.2.3 Frequency of training (DTSA recommends semi-annual training), who provides the training, if not by name, at least by office symbol or title;

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

4.2.5 Out of cycle training for special circumstances such as: a change in the scope of work in the TAA that has been approved by DDTTC, change in the law affecting procedures, if there is a violation, etc.

4.2.6 Companies are free to add any additional material.

5.0 TECHNICAL DATA:

5.1 Documentation Control.

5.1.1 Unique Data Identifier. Technical 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 technical data exports are to have the same identifier or "number" (which could be alphanumeric). Not only must each export be uniquely identifiable, they must be recorded and tracked. At the minimum, records must be able to show what has been exported, when, and to whom.

It is not sufficient to just state that a naming convention is in place, an example must be provided in the TTCP.

Spacelink does give the opportunity to enter these identifiers, or *Industry ID*, as they are referred to in Spacelink, during the technical data upload process.

5.1.2 Internal Processes. Describe the internal process for documentation control, from the moment the technical data is generated to the time it is exported, to include procedures for how it is tracked and maintained. This should include the processes for the maintenance of a library of exported technical data. In the end, the following questions should be answered: Who makes the determination on whether data marked for export is technical or non-technical? If technical, how are documents routed and approved internally and then sent to DTSA, if applicable. How are data exports tracked? Who is the POC for documentation control? Are the technical data packages for the library archived electronically or in hard copy format?

Prior to release, (insert company name) will ensure all technical 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. DTSA does not prescribe the method or format, but the purpose is to verify that technical data delivery is only as authorized by appropriate export control and DTSA, if necessary, approvals.

5.1.3 Documentation Markings. All technical data for release should be marked with the following: 1) DTC Case Number (the export authorization, this includes identifying the correct and current amendment); 2) the Unique Data Identifier; and 3) 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, please contact DTSA for approval. Markings should be added prior to DTSA review.

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

“This document contains ITAR controlled technical data (ITAR 120.10) that is 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 technical data is shown below:

“Contains ITAR data subject to U.S. Export Control, TA xxxx-xx (Doc no. xxxx)”

These are provided as examples only.

5.2 DTSA Review. State whether this is a requirement or not, and if so, cite the proviso; if not, say "Not Applicable". If DTSA review of technical data is required, include the following statement: **[Company name] acknowledges that DTSA has up to 10 business days to review technical data submitted for approval. The first full normal business day after DTSA's receipt of the submission is counted as Day 1 (of the 10).**

5.3 Request for Waiver/Exemption Process. The technical data review proviso contains circumstances where companies may request DTSA review of technical data be waived. These are:

5.3.1. New technical data that is similar to that already approved by DTSA. [Company name] must specifically request such a waiver in accordance with TTCP guidelines.

5.3.2. Technical data defined in the applicant's approved TTCP that is determined by DTSA as not requiring review based upon subject matter or scope.

5.3.3. Test Results are exempted from the technical data requirement. Reports including test analysis, procedures, or derived conclusions **MUST** still be reviewed as stated above.

The company must specifically request such a waiver in writing using Spacelink, certifying that the currently submitted technical data is similar to that previously approved for release. Companies must reference the previous approval in Spacelink.

Companies may list technical data that they believe is authorized for export without prior review to DTSA. This will be granted on a case-to-case basis. DTSA will contact or place in review comments any issues they have with any item(s) on the list.

DTSA review of documents IS NOT required in the following instances so long as the applicant has NOT made any technical changes: documents created by a foreign signatory to be exported to a different foreign signatory, foreign-language origin data translated into English, and export-approved U.S. origin data that has been translated into a foreign language.

State “Not Applicable” if data review does not apply to the export authorization.

5.4 Definition of Terms. Define terms; e.g., system, subsystem, part, component, assembly, test results, etc., especially as it relates to terms used in the provisos. If you do not intend on using this subsection, then you may delete it or state "Not Applicable".

6.0 TECHNICAL INTERCHANGE:

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 the remainder of this document, this person will be referred to as "Activity Chair" for simplicity.

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

6.2 Attendance Roster. This is required for all activities. To the greatest extent possible, the attendance roster must be filled out by all participants at the beginning of every technical interchange. DTSA understands 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 a copy electronically after the event. The attendance roster must include, at a minimum: full name, nationality, company, and signatory (contractors hired by the applicant should list the applicant as their signatory). Non-signatories (passive attendees) need to list the applicant that invited them to attend. 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 (also 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. Most importantly, 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.

6.6.2 Teleconferences/Videoconferences. Teleconferences/Videoconferences are similar to meetings 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 USG reserves the right to monitor, companies are not allowed to have both U.S. and foreign persons in the same room. When U.S. and foreign persons are in the same room, a teleconference/videoconference becomes a meeting. Discuss any nuances or differences in the way you handle telecons/videoconferences from meetings. Much of the controls will be the same, but there might be differences from company to company.

6.6.3 Joint Operations. The purpose of this subsection is to discuss controls used for joint operations with foreign parties which are not specifically called out elsewhere. Ensure it is stated that an Activity Chair will monitor all joint operations. An exception to this policy is that during any hazardous operations, the Activity Chair is not required to be in the area for export compliance reasons. They are required to 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.

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, and a Debris Recovery Plan. 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. **Annexes must be provided to DTSA no later than sixty (60) days prior to shipment of any hardware. Non-reimbursable programs may contact DTSA to negotiate a shorter timeline.**

6.7 DTSA Monitors. If monitoring is required, or if the USG reserves the right to monitor, the following text must be included in this subsection (tailor to license): Attending DTSA Monitors at typical Technical Interchange Meetings (TIM) will not, unless previously coordinated, review data on-site. They will, however, review change-pages to technical data previously approved for export. The Monitor will also review and approve meeting minutes for immediate release via signature (not Spacelink). During major operations (i.e., sine vibe tests, fit checks) or launch operations, Monitors will review data on-site in real-time. If there is no proviso for monitoring in the license, state “Not applicable.”

6.8 Notification Requirements.

6.8.1 Reimbursable Programs. Reimbursable programs are those where the company reimburses the USG per Public Law. All technical 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).

1. Timelines. Notification timelines for reimbursable monitoring support are forty (40) days in advance of overseas technical meetings in support of the agreement; fifteen (15) days when meetings are held in the continental U.S.; and five (5) business days for telecons/videoconferences.

2. The 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. Realize, a positive disposition to a Request only means DTSA has approved the Request itself. Actual support by Monitors is subject to personnel availability.

6.8.2 Non-Reimbursable Programs. Non-reimbursable programs are those where DTSA reserves the right to monitor activities per Proviso, but companies DO NOT reimburse the USG. Monitoring Requests (MR) will be submitted in accordance with the below guidelines.

1. Timelines. Notification timelines for non-reimbursable programs 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 for DTSA clearance to foreign facilities); seven (7) calendar days for meetings in the US; and five (5) calendar days for telecons/videoconferences. Minutes for all waived meetings shall be uploaded to the original waived MR for that activity within five (5) calendar days. 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 an MR only means DTSA has approved the MR itself. Actual support by Monitors is subject to personnel availability.

2. The Request. (The company) shall submit requests for monitoring support for Technical Interchange Meetings with the foreign parties. These requests for, and any changes to, DTSA monitoring support will be submitted via Spacelink as a Monitor Request (MR). In the MR, (the company) shall note "DTSA reserves the right to monitor per Proviso #XX of TA XXXX-XX."

3. Exemptions. Non-technical meetings are exempt from notification. The following technical meetings may also be exempt from notification as long as the discussion is based on the level and scope of Technical Data approved IAW Section 5.0 and the applicant specifically addresses their 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 telecons/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.

4. 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, 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 spacecraft power or spacecraft 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/spacecraft 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.

5. Other Meetings. In cases where notification is not required for a technical meeting, companies should place a copy of technical meeting minutes in their library.

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).

7.2 Facility Layout. Provide a basic graphical overview of the facilities where technical interchanges 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 (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 satellite; there may be other commercial or USG satellites 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 facility(ies) 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 technical data and defense services foreign persons will have access to or receive during their residency. Further, describe what type of work they will observe and how close they will 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 authorized ITAR controlled areas and how the company will prevent unauthorized access to any USG 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. A discussion of how computer equipment will be protected at Technical Interchange Meetings at third-party facilities in the U.S. (i.e. a hotel conference room) and aboard is required. Encryption, password protections, networking, flash/thumb drive use, etc. are also appropriate in this subsection.

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, do not add):

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 technical data will be handled. Address how all technical 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.

8.5 Technical Interchanges. Describe how the U.S. person(s) will be involved in technical and non-technical interchanges. If DTSA monitoring is part of the export authorization, then this person may only participate in non-technical meetings with the Foreign Parties and may not provide defense services. All technical interchanges they will participate in 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 IAW the TAA and TTCP.

9. Annexes to the TTCP:

Companies are free to add their own annexes, as necessary.

A. Copies of License Files

B. Sample Outline for Annexes (again this is for launch campaigns). If a TTCP is required for a non-launch program, this would be "Not Applicable."

1. Document Description

1.1. Purpose of document

1.2. Revision History

1.3. Process for Modifications

2. Launch Campaign Overview

2.1. Program

2.2. Key Participants

2.3. Export Authorizations (TAAs, DSPs, etc)

2.4. Reference Documents

2.5. Summary of Defense Articles

3. Organizations, Participants, Names, Roles / Responsibilities

This section needs to provide enough detailed information to help the DTSA monitor know how the players interact, and especially to know who's who when looking for information or to discuss issues. This includes more than just the primary POC.

 - 3.1. Org Chart
 - 3.2. DTSA Interface
 - 3.3. Key Foreign Participants
 - 3.4. Include all 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. Building by building Number, Room-by-Room
 - 4.2.1. Description/Location
 - 4.2.2. Physical Layout
 - 4.2.3. Physical Security Measures
 - 4.3. Include any Contingency Facilities
 - 4.4. Include US-Only (and non-US)
 - 4.5. Facility Acceptance Process
5. General Functions (Common Processes)
 - 5.1. Overall Security Practices
 - 5.1.1. Guards (staffing plan in Appendix)
 - 5.1.2. Manned vs. Remote Monitoring
 - 5.1.3. Escorting
 - 5.1.4. Video/Photo Plan (or summary of plan)
 - 5.2. Badging & Access Control
 - 5.3. Training
 - 5.4. Networks/Communications
 - 5.5. Release of Technical Data
 - 5.6. Meeting Protocols / Technical Meetings
 - 5.7. Storage of ITAR data and equipment
6. Factory-to-Post-Launch Flow of Events
 - 6.1 Chronology of Events
 - 6.2 Nominal Timeline of Events
 - 6.3 Recurring Topics/Themes throughout
 - 6.3.1 Escort
 - 6.3.2 Public/VIP tours
 - 6.3.3 Security
 - 6.3.4 Transportation
 - 6.3.5 Joint Ops
 - 6.3.6 DTSA Requirements/Participation
 - 6.3.7 Briefings/Daily Meetings
 - 6.4 Include Post-Launch (facility close-out, pack-out, shipments home, etc)
7. Contingency Planning

- 7.1. Incident Reporting
 - 7.2. Launch Delays
 - 7.3. Debris Recovery
 - 7.4. Transportation Delays/Interruptions/Diversions
 - 7.5. Back-to-Back and Overlapping Campaigns
 - 7.6. Failures/Outages Contingency Plan (CCTV outage, emergency egress, etc)
8. Other
- 8.1. Incident Reporting Form
 - 8.2. Staffing Plan
 - 8.2.1. Security Staffing
 - 8.2.2. Work Tempo of Launch Campaign Ops
 - 8.3. Acronyms/Abbreviations/Definitions