FINAL REPORT

LOS ALAMOS NATIONAL LABORATORY SUBCONTRACT

9-X38-1032U-1

Provide Technical Analysis of US Army Weapons Systems and Related Advanced Technologies of Military Interest, Along With Quick Response Technical Support

ABSTRACT: This report summarizes the activities and accomplishments of an US Army technology security project designed to identify and develop effective policy guidelines for militarily critical technologies in specific Army systems and in broad generic technology areas of military interest. Individual systems analyses are documented in separate Weapons Systems Technical Assessments (WSTAs) and the general generic technology areas are evaluated in the Advanced Technology Assessment Reports (ATARs). However, specific details of these assessments are not addressed here, only recommendations regarding aspects of the defined approach, methodology, and format are provided and discussed.

Prepared for:

International Technology Division
IT-3
Los Alamos National Laboratory
Los Alamos, NM 87544
Mr. Truel West, Project Technical Director

Prepared by:

Orion Enterprises, Incorporated
P.O. Box 62
Fredericksburg, VA 22404

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

LA-SUB--93-183

FINAL REPORT

LOS ALAMOS NATIONAL LABORATORY SUBCONTRACT

9-X38-1032U-1

Provide Technical Analysis of US Army Weapons Systems and Related Advanced Technologies of Military Interest, Along With Quick Response Technical Support

ABSTRACT: This report summarizes the activities and accomplishments of an US Army technology security project designed to identify and develop effective policy guidelines for militarily critical technologies in specific Army systems and in broad generic technology areas of military interest. Individual systems analyses are documented in separate Weapons Systems Technical Assessments (WSTAs) and the general generic technology areas are evaluated in the Advanced Technology Assessment Reports (ATARs). However, specific details of these assessments are not addressed here, only recommendations regarding aspects of the defined approach, methodology, and format are provided and discussed.

Prepared for:

International Technology Division
IT-3
Los Alamos National Laboratory
Los Alamos, NM 87544
Mr. Truel West, Project Technical Director

Prepared by:

Orion Enterprises, Incorporated
P.O. Box 62
Fredericksburg, VA 22404

LIST OF RELATED DOCUMENTS FOUND IN THE ATTACHMENT

1. Security Arrangements for Multinational Armament Cooperation Program--MLRS
2. Point Paper--International Participation in LHX Program
3. An Industry Briefing Paper for the LH Program
4. Usage of Commercial Microprocessors in Tactical US Army Equipment
5. Analysis of Weapon System Technical Assessment Questionnaire
6. Guidelines for Preparing Munitions License Applications
7. Requirements of the Foreign Disclosure Plan (FDP)
8. Language for Interim Changes to AR-70-1
9. US-Canada Joint Certification Program Documentation; US/Canada Joint Certification Program; The US/Canada Joint Certification Program for Directly Arranged Visits (DAV); and a Briefing Paper--US/Canada Technology Security under the Joint Certification Program
10. Visits Involving Access to Unclassified Technical Data by Canadian Government Officials and Certified Canadian Contractors
11. DoDD 5230.20--International Visits and Personnel Exchanges

DISCLAIMER

INTRODUCTION

Overview of Work

Effective management of militarily critical technology--that is, technology that could make a significant contribution to the military capability of a potential adversary to the detriment of US national security--is a primary concern in defense policy. Maintaining the technological superiority is a cornerstone of Western military planning. The US technology security program plays a fundamental role by ensuring that technology is properly identified as a valuable resource and prudently invested in the mutual defense of our allies, while being protected from exploitation by potential adversaries.

Within the US Army, the Army Materiel Command, Assistant Chief of Staff for Intelligence (AMC/ACSI) has broad responsibilities for implementing DoD technology security policy. Specifically, ACSI is responsible for identifying militarily critical technologies in US Army systems and for recommending appropriate technology security guidelines for those technologies.

Orion Enterprises, Inc.'s (OEI) broad background and involvement in technology security has given the program an ability to identify and adapt to rapidly changing requirements. This ability has allowed us to anticipate the project's needs and respond to those needs in a timely way. As a result, the AMC/LANL/OEI work has become an important factor in, and a model for, a number of initiatives in technology security and export control policy development and program implementation in international arms cooperative efforts.

In the 1980's the acquisition by the Soviet Bloc of US militarily critical technology was the principle focus for the Army's Technology Security Program. However, recent global political changes are leading the United States to reconsider and extend its scope of coverage. These new concerns encompass not only West-to-East trade but also a North-to-South transfer and trade with Third World countries. The recent Persian Gulf crisis, in particular, underlies the importance of effective technology security to control critical technologies. The US Army technology security program, by identifying and providing explicit guidance for the protection of critical technologies, is an essential element in impeding the flow of technology that could be damaging to Allied Forces in such conflicts.

Statement of Work

The Statement of Work tasked OEI to provide subcontractor support for Los Alamos National Laboratory, International Technology Division's effort on the Army Technology Security Program (ATSP). To meet the programs stringent delivery rates

and deadlines requires personnel with broad technical backgrounds and detailed familiarity with the MCTL. The project further demands understanding of current technology security issues, foreign military sales (FMS)/exports, technology transfer mechanisms, and the ability to provide rapid response to travel schedules and reporting requirements. In addition, OEI was responsible for providing general project administrative and technical support to Los Alamos and AMC for the tasks described below.

This effort was divided into four areas of support. These being:

- Task 1--Weapon System Technical Assessments (WSTAs),
- Task 2--Advanced Technology Assessment Reports (ATARs),
- Task 3--Quick Response, and
- Task 4--Information Systems (report previously submitted).

Scope of Report

This report summarizes the performance of the Army's Technology Security Program over the span of the contract period (1 August 1988 to 28 February 1991). It covers the results and accomplishments of the first three tasks identified in the Statement of Work. The major effort on Task 4 Information Systems was terminated because of funding limitations. Work was completed and the final report on Task 4 was provided separately. This report addresses only Tasks 1 through 3.

RESULTS AND ACCOMPLISHMENTS

Overview/Context of Changing Requirements

New Directions in Technology Security

CoCom and US Export Controls

One of the primary external factors effecting the ATSP will be the political changes in Eastern Europe, and the resulting liberalization of world trade. Many technologies and products that were previously controlled to all destinations for national security reasons have been, or within months will be, entirely free from embargo. For example, many 16-bit microprocessors and multilayered printed circuit boards were released for transfer to the Soviets. These are technologies that were previously recommended in the WSTA's for release only to allies. US Army guidance for FMS and technology transfer must now be updated to be consistent with our overall national export control and trade policy.

Another rapidly changing aspect of US policy is revision of the Missile Technology Control Regime (MTCR), which will form the basis for a new set of North-South oriented control of products and technologies for nuclear and CBW delivery systems. These too, must be reflected in future Army assessments.

International Armament Cooperative Programs (IACP)

Over the life of this project, we also saw a dramatic increase in the emphasis placed on technology sharing and international cooperation.

IACP involves a broad range of activities supporting development and implementation of technology security policy. The major effort included development and documentation of the process for negotiating and concluding international agreements (the Technology Assessment and Control Plan (TA/CP)); procedures for visits and accreditations of foreign defense professionals and exchange personnel; and policy for disclosure of classified and controlled unclassified defense technical information under a wide range of exchange mechanisms.

For the past several years OEI has been directly involved in work in these areas. In addition to development of the TA/CP, and visits procedures, OEI personnel provided the primary support for the Canadian Joint Certification Program and implementation procedures.

Defense Critical Technologies Plan

A third change has been the legislatively mandated emphasis on more comprehensive R&D planning, as reflected in the Defense Critical Technologies Plan (DCTP). (The DCTP uses the term "critical" in a different context than the MCTL--i.e., it identifies the twenty areas of technology that are most critical from an R&D investment perspective.) This provides insights useful for assessing the importance of the developing, sharing, and protecting technologies critical to future military systems. At the same time the ATSP (and especially the WSTA's on programs in advanced development and the ATARs) provide key information regarding real-world military development activities.

MCTL

Finally, the MCTL itself is evolving. The organization of the MCTL is changing to reflect that of the new export controls. The supporting analysis and documentation is being expanded to include more detailed discussion of military systems, foreign capabilities, and related technologies. The WSTA's and ATAR's should serve as an important source of information for developing both the MCTL itself, and the supplemental information.

TASK 1 AND 2--WSTAs and ATARs

General

WSTAs

Orion performed technology security analysis of selected US Army weapons systems and provided draft WSTAs to LANL in the approved format. In this task OEI:

Reviewed detailed technical documentation supplied by LANL, the Army, and Army contractors on selected weapons systems.

Acquired additional weapon system descriptions and documentation from written sources and verbal interviews as necessary. Interviewed the prime contractor and subcontractor personnel and, in some cases, Army laboratory and intelligence personnel. Accordingly, travelled to numerous locations across the United States to complete these evaluations.

OEI used its in-depth background knowledge of the Department of Defense's MCTL, the Department of Commerce's Commodity List (CL), and the State Department's International Traffic In Arms Regulations (ITAR). Orion analyzed and compared critical items within AMC-specified weapons (at the

subsystem, component, or technology level) that are identified by the MCTL, CL, and ITAR, and categorized them according to their levels of concern.

Reviewed and incorporated AMC comments into WSTAs at draft, final draft, and final stages. Addressed comments and concerns raised by LANL technical reviews at all document stages.

Updated and revised existing WSTAs to reflect weapon program improvements or changes in technology.

ATARs

OEI also generated draft ATARs for LANL in the approved format. In this task OEI:

Conducted technology security analyses and prepared assessment reports in selected advanced technology areas.

Integrated technical analyses performed by LANL into the format approved by AMC, including the addition of technology security guidelines.

Evolution of Studies, Content and Format

WSTA's and ATAR's changed greatly over the life of the project. The coverage and detail of material/analysis increased significantly. The use and policy exposure of these products also increased. These reports are used by Headquarters, Department of the Army, Office of the Deputy Chief of Staff for Intelligence, Technology Transfer and Foreign Disclosure Division (DAMI-CIT) and Defense Technology Security Agency (DTSA) as references in export control decisions. They will be a major asset for DoD's Technical Review Groups in the revision of the MCTL and in formulating guidance for the CoCom Core List.

OEI anticipated the impact that the liberalization of controls would have on technology security due to the rapid political/economic changes occurring in the world today. This was reflected in the evolution of the ASTP's products. These changes have made the WSTAs/ATARs a vital and important asset for international technology security and export control. The program has evolved, and continues to evolve, with greater emphasis on identifying opportunities in the cooperative R&D exchange/ arrangements in the international arms industry. Our studies now address time-phase release of technology in a manner that allows cooperation, while protecting against premature and/or unnecessary release or disclosure of militarily critical technologies.

In addition, the overall readability of the WSTA was improved. Primary changes included a more concise Executive Summary containing basic information necessary to convey an overview of the program and the system. We added several graphics presentations which helped simplify the Executive Summary. A breakout graphic was introduced (see Figures 1, 2, and 3 for examples) showing the relationship of the system's subsystems and their critical elements. This change increased the understandability of the weapon system and its components by identifying pertinent critical technologies indigenous to each subsystem in an easily interpreted graphic format.

Originally, weapon systems transfer guidelines were provided in text. This was replaced by the Summary Guidelines Chart (see Figure 4). This graphic provides a very clear, understandable, overview of the transfer guidelines that explain the general level of technology security concerns involved with different possible transfer mechanisms. We also developed new definitions that addressed the latest status quo in the export control regulations. These new definitions pertained to the criticality of concern of the transfer (e.g., LOW, MODERATE, SIGNIFICANT, AND EXTREME) to candidate destination areas (friendly nations, allies, and closest allies). The guidelines were expanded to address the impact of unauthorized disclosure of technical information, data packages, or reverse engineering potential for the critical elements imbedded in a system. This analysis of the potential negative impact of the technologies released aided decisionmakers in formulating an informed export transfer/control action.

The MCTL has been the primary reference of the WSTA/ATAR program. Because of the rapid advancement in technology, changes in the control arena and the fact that the MCTL is only updated every two years, it became evident that to be technically current more narrative text explaining the technology's criticality was needed. OEI suggested that the document could be made less dependent on the MCTL with a few simple changes. The notes and tables in Section IV.C Controlled Technologies were reversed (originally, the MCTL-referenced tables appeared first) and the narrative analysis was expanded. Placing greater emphasis on the substance of the technology improved the documents currency and technical validity and provides the audience with a more complete and easily assimilated discussion of critical technologies and rationale for control.

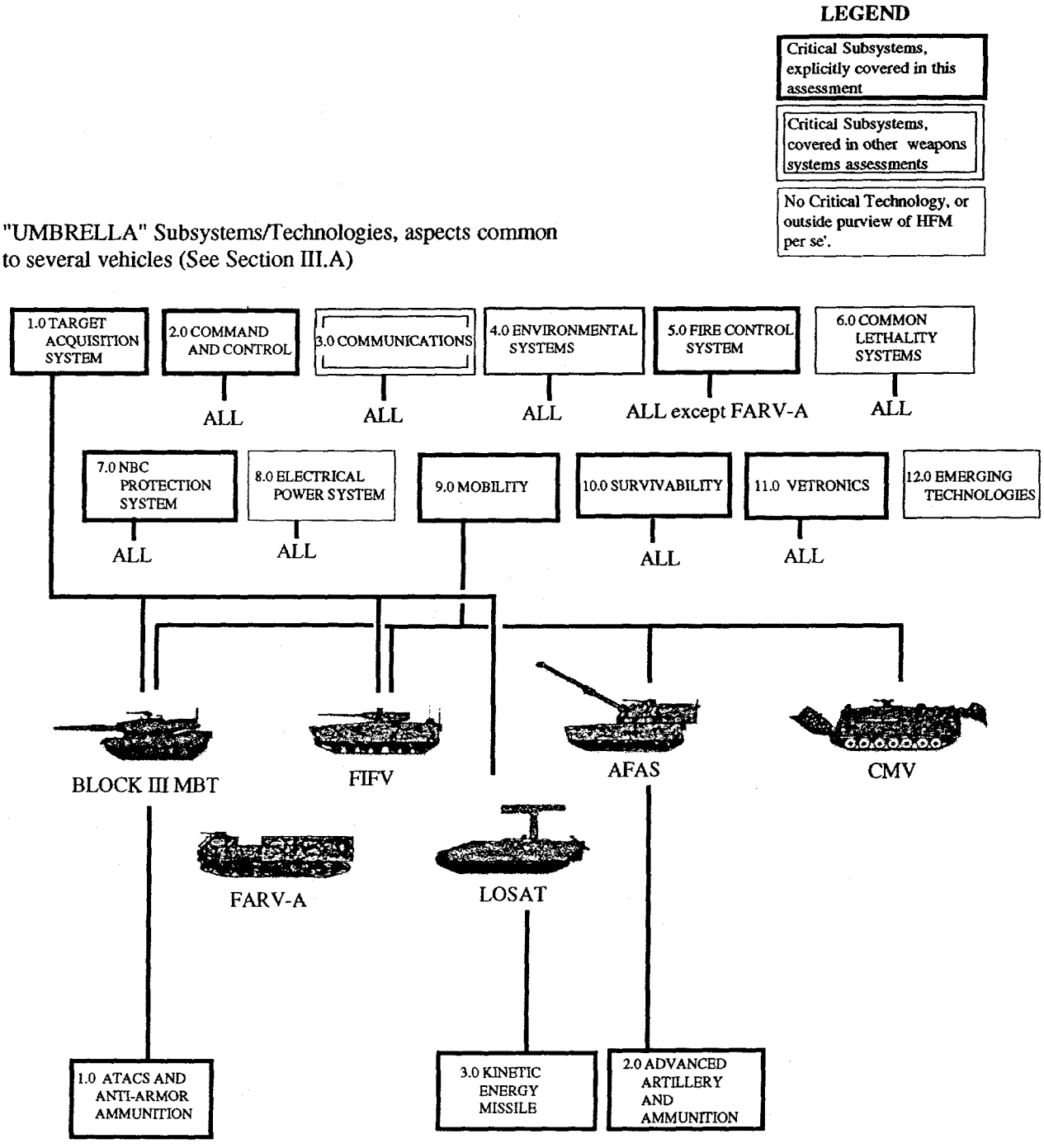


FIGURE 1. Heavy Force Modernization Family of Vehicles, Primary Subsystem Areas

9-X38-1032U-1

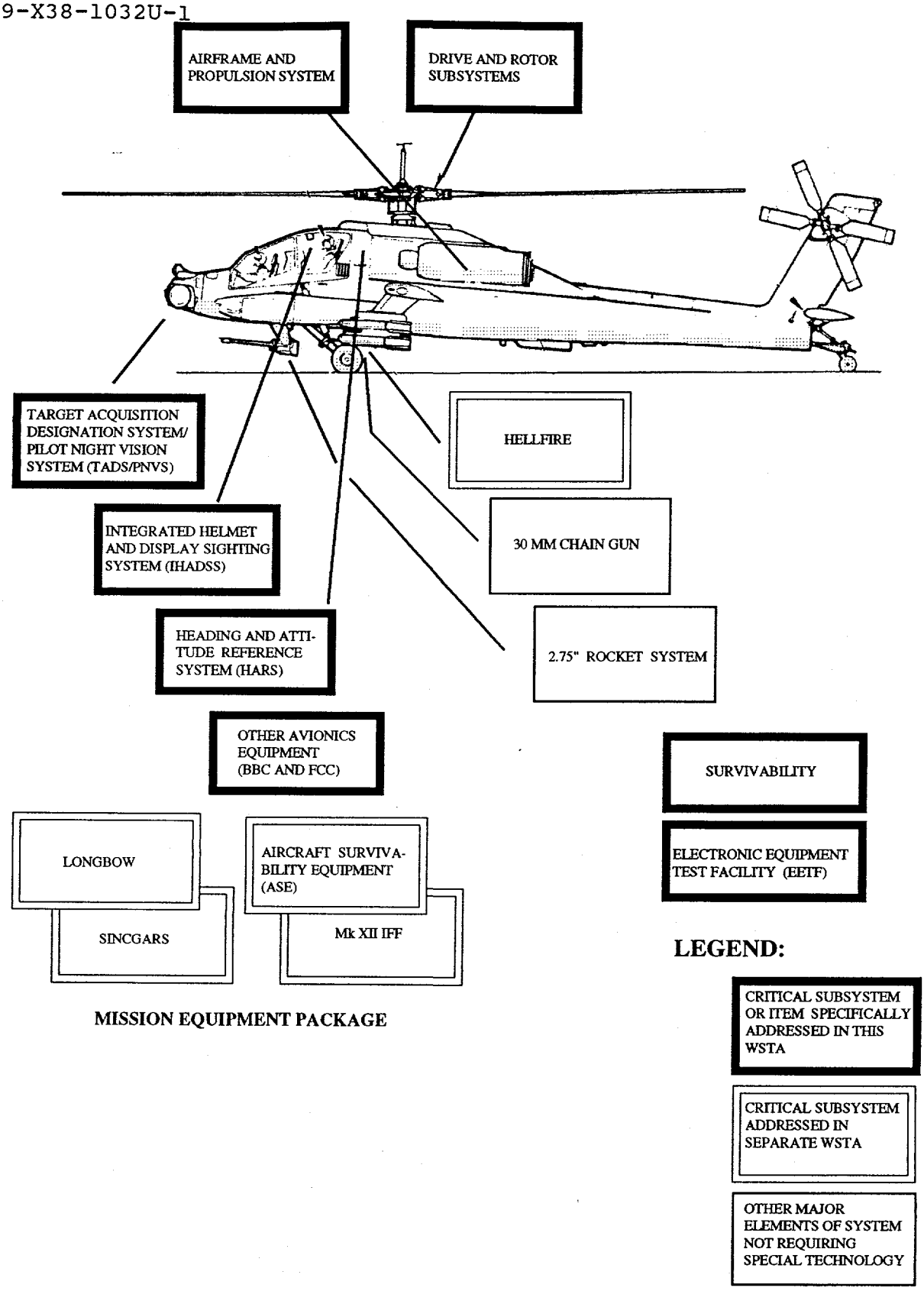
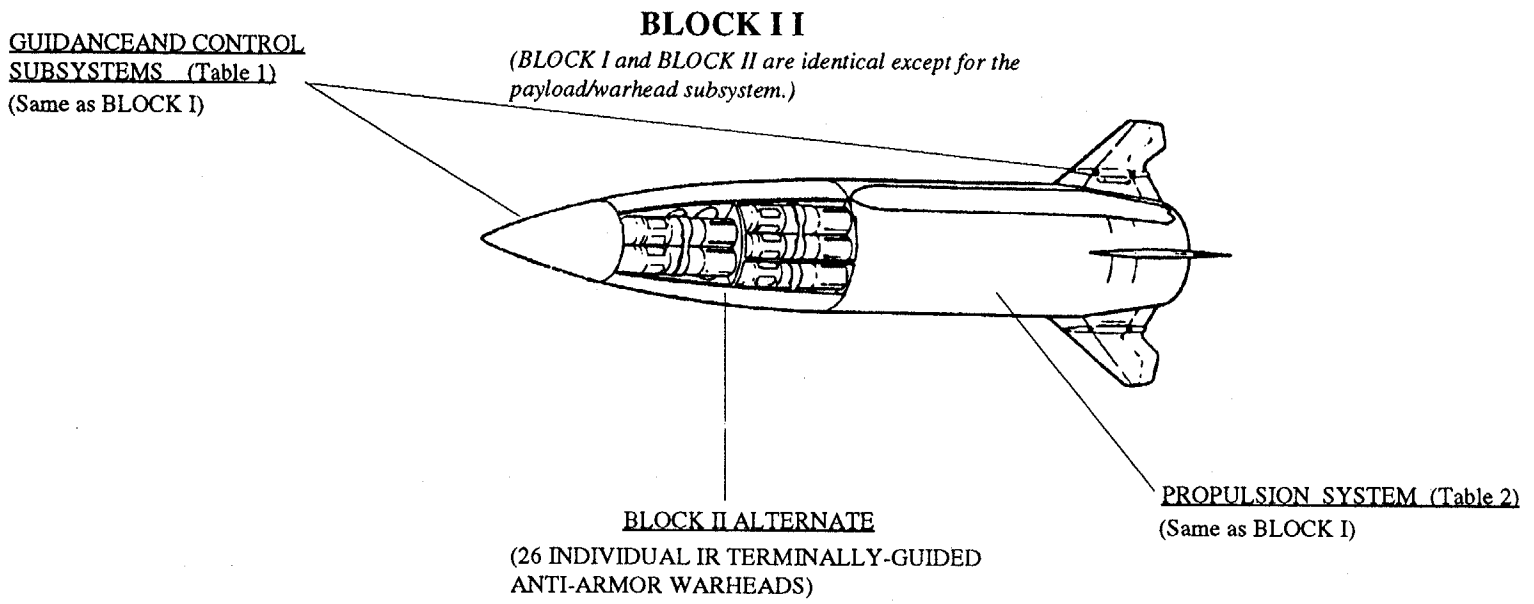


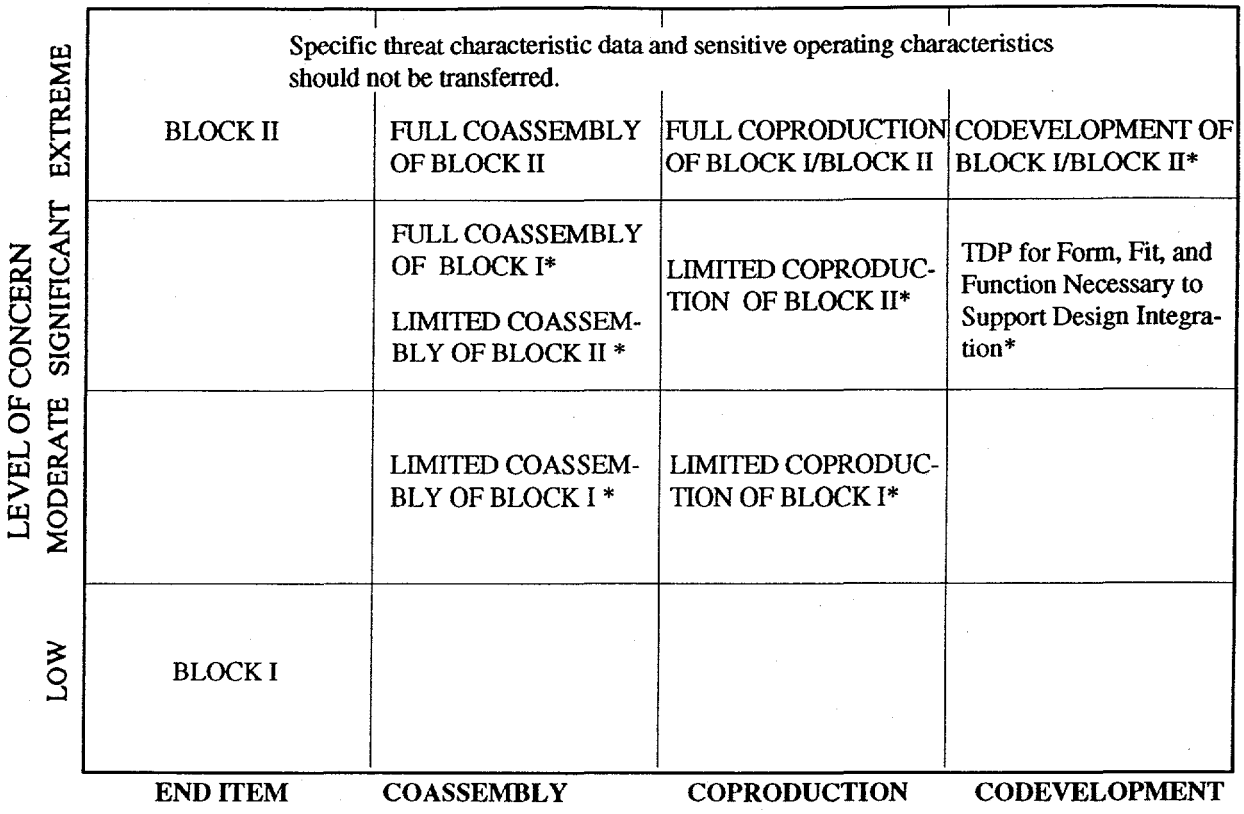
Figure 2. Apache System Overview



WARHEADS (Table 4)	TERMINAL GUIDANCE ELECTRONICS (Table 5)	TERMINAL GUIDANCE SENSOR (Table 6)
Organic Explosives Compounds Production (MCTL 20.1.2)	Signal Processing (MCTL 1.2.4)	Microcircuits (MCTL 7.1)
Energetic Materials (MCTL 20.2, 20.3, and 20.4)	Hybrid Microcircuits (MCTL 7.3.2)	Semiconductor Detectors (MCTL 7.2.4)
Warhead Components and Systems (MCTL 20.5.1)	Target Classification, Recognition, Identification (MCTL 10.4)	Preparation and Purification of Detector Materials (MCTL 7.4.1)
Safing-and-Arming, Fuzes, Detonators (MCTL 20.5.6)	Primary and Reserve Battery (MCTL 19.1.2)	IR Band Sensor (MCTL 14.1.3)

UNCLASSIFIED

Figure 3. Breakout of Critical Elements in the Army TACMS BLOCK II



* See appropriate part of Section III.B for more detailed guidelines.

DEFINITIONS OF LEVELS OF CONCERN:

EXTREME: Items whose performance or extractable technologies support unique US operational advantages in primary mission areas. (Typically, items whose inspection or use will reveal critical system vulnerabilities or susceptibilities, or technologies wherein the US enjoys a significant worldwide lead in military applications.) *Items in this category will not normally be approved for release.*

MODERATE: Other items whose acquisition and exploitation by potential adversaries could significantly impact US Army mission capabilities.

LOW: Hardware, software, or technical data whose acquisition and exploitation by potential adversaries would have marginal impact on US Army operational capabilities.

(See Section III.A for more complete definitions.)

Figure 4. Summary Guidelines for the Army TACMS

Studies Completed

List of WSTAs/ATARs successfully completed from 1 August 1988 through 1 March 1991.

Initial Draft

Optical Improvements Program (OIP) ATAR
Single Channel Ground Airborne Radio System (SINCGARS)
Improved Guardrail
Short Range Thermal Sight (SRTS)
Lightweight Manportable Radio Direction Finding System (LMRDFS)
ASE-Volume I--Radar Countermeasures
ASE-Volume II--Infrared Countermeasures
ASE-Volume III--Electrooptical Countermeasures and Decoys
J-STARS
LHX Technology Security Risk Assessment
LHX ATAR
FOG-M (Non-Line-of-Sight-Missile)
OIP ATAR (Draft #2)
HFM
MSE
Longbow
AN/TRC-173/-174 Radio Terminal Set
Thermal Weapon Sight (TWS)
HFM (Draft #2)
HFM (Draft #3)
Autonomous Precision Guided Munitions (APGM) ATAR
Avenger
FOG-M (Draft #2)
Longbow (Draft #2)
OIP ATAR (Draft #2)
Army Tactical Missile System (ATACMS)
Tunable Laser ATAR
Anti-Armor ATAR (update)
ATACMS (Draft #2)
OIP ATAR (Draft #3)
SINCGARS (Draft #2)
LH WSTA
Avenger (Draft #2)
MSE (Draft #2)
MMIC ATAR
AAWS-M
Corps-SAM
FAAD-C^2
Common Hardware/Software
Multipurpose Individual Munition

Final Draft

Quickfix
PLRS/EPLRS
Stingray
REMBASS (Remotely Monitored Battlefield Sensor System)
SINCGARS
Regency Net
Apache AH-64
Stinger
Cobra/TOW
Patriot
TOW 2
Improved Guardrail

TASK 3--Quick Response Tasks

General

Orion provided on-site response and technical support to AMC resolving specific issues arising from the Army's review and use of WSTAs/ATARs, and topics of interest in the technology security/export control areas. Quick responses included tasks in several basic areas, these being:

- Policy-related studies and analysis, and
- Specific technical analysis.

Also, additional support included attendance at meetings, phone discussions and preparation of point papers to assist AMC in their role as security experts.

AMC Support

OEI completed several major projects between October 1989 and March 1991 supporting primarily three offices: Headquarters, Army Materiel Command (AMC); Headquarters, Department of the Army, Office of the Deputy Chief of Staff for Intelligence, Technology Transfer and Foreign Disclosure Division (DAMI-CIT); and the Office of the Deputy Under Secretary of Defense for Security Policy (ODUSD(SP)).

Support to AMC included:

- Multiple Launch Rocket System-Terminally Guided Warhead (MLRS-TGW) program pamphlet of security procedures (see Attachment #1),
- Point paper for AMC on international participation in the Light Helicopter (LH) Program (see Attachment #2),

- An industry briefing for the LH program (see Attachment #3),
- White papers on microprocessors used in US Army systems (see Attachment #4),
- Analysis and documentation of results from an AMC questionnaire pertaining to WSTAs (see Attachment #5),
- Briefing material for an AMC Technology Security presentation,
- Summary analyses and briefing charts on the relationships between TA/CP and WSTA/Foreign Disclosure Plan (FDP),
- Guidelines for Preparing Munitions License Applications (see Attachment #6),
- Requirements of the Foreign Disclosure Plan (FDP) (see Attachment #7),
- Language for Interim Changes to AR-70-1 (see Attachment #8),
- North American security initiative, and
- Army Tactical Missile System (TACMS) congressional briefing paper.

DAMI-CIT Support

OEI assisted DAMI-CIT in a variety of quick response tasks, including:

- Preparation of a short talking paper on technology security considerations in the Army Acquisitions process;
- Development of an MOU between the Services, DIA and DTIC to streamline DTIC document requests from certain embassies; and
- Development of preliminary draft changes for a re-write of Army Regulation 380-10 Policy for Disclosure of Military Information to Foreign Governments.

OEI also supported DAMI-CIT in its role as designated lead service activity for certain international programs for ODUSD(SP). Support to ODUSD(SP) included:

- Documentation for the U.S.-Canada Technology Sharing and Security Subcommittee and development of the US-Canada Joint Certification Program pamphlet (see Attachment #9);

- Assistance for developing DoD Policy for US Contractors on Unclassified Canadian Visits to DoD installations or DoD Contractor facilities (see Attachment #10);

- A study examining the possible relocation of the Joint Certification Office;

- Examination of the legal weight of Canadian "PROTECTED" information in US security procedures; and

- Review of DoD Directives 5230.24, Distribution Statements on Technical Documents and 5230.25, Withholding of Unclassified Technical Data from Public Disclosure with suggested additional changes to acknowledge incorporation of Canadian contractors into the term "qualified contractor."

Further support for ODUSD(SP) also included the development of four draft DoD Directives (later combined into two) - draft DoD Directive 5230.20 (see Attachment #11), Control of Foreign Representatives (to include the previously separate directive, DoDD 5230.xx on personnel exchanges) and draft DoD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations (which combined DoD Directive 11 and Instruction 17, Procedures and Standards for Disclosure of Military Information to Foreign Activities). "Quick response" support also was provided for the TA/CP, previously developed by Orion, as it underwent several minor revisions. Numerous other small "quick response" tasks performed for ODUSD(SP) involved preparation for, and support for, review and coordination of these documents and analysis and revisions of directives to incorporate results of inter-service review.

LESSONS LEARNED AND RECOMMENDATIONS

The crisis in the Persian Gulf, the rapidity of recent changes in Eastern Europe, the continuing instability of the Soviet Union, and the increasingly advanced technological progress made by Third World countries have all reinforced the urgent need for more flexible and responsive technology security analysis. Subsequently, WSTAs/ATARs will need to become more responsive because of their integral part in formulating FDPs, TA/CPs, and International Armaments Control Plans (IACPs). Scheduling priorities and deliveries must respond to real world situations/scenarios if the ATSP is to remain a driving force in technology security and export control.

Because of the development and subsequent review process these documents presently take anywhere from nine to eighteen months to become final approved documents. (See Figure 5 for the WSTA Development Process and Figure 6 for the ATAR Development Process.) When major systems with AMC urgency are needed and the review process has been reduced by direct interaction between OEI and the Army PMs and PEOs response time has improved. Examples of these successes are LH, CORPS-SAM, Army TACMS, and Heavy Forces Modernization (HFM) all of which needed WSTAs to respond to milestones and/or to seek international cooperation. Lessons learned in these programs should be incorporated into the standard operating procedure for all WSTAs/ATARs.

The program should continue to focus on the needs of the users in the technology transfer/export control community. Technology security is dynamic by nature and we should endeavor to seek increased audience exposure/review, even if this necessitates further changes to the format and content of the documents.

The WSTA/ATAR documents provide a wealth of information if used with the understanding that they are guidance documents and with some intuitive reasoning/analysis they coupled with the technology security classification guide can provide the necessary information to formulate the Foreign Disclosure Guidelines.

Every effort should be made to continuing a refining process to enhance the documents usefulness.

WSTA DEVELOPMENT PROCESS

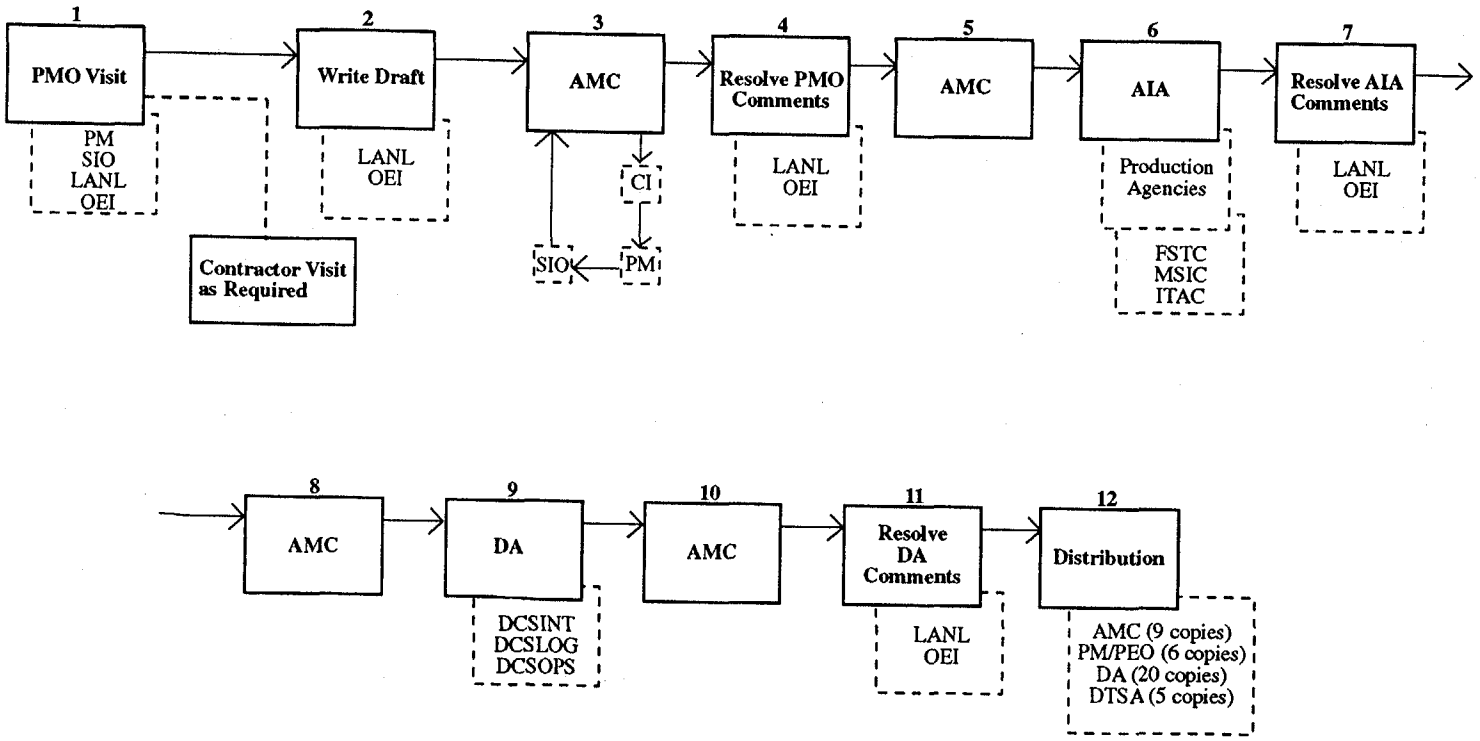


Figure 5. WSTA Development Process

ATAR DEVELOPMENT PROCESS

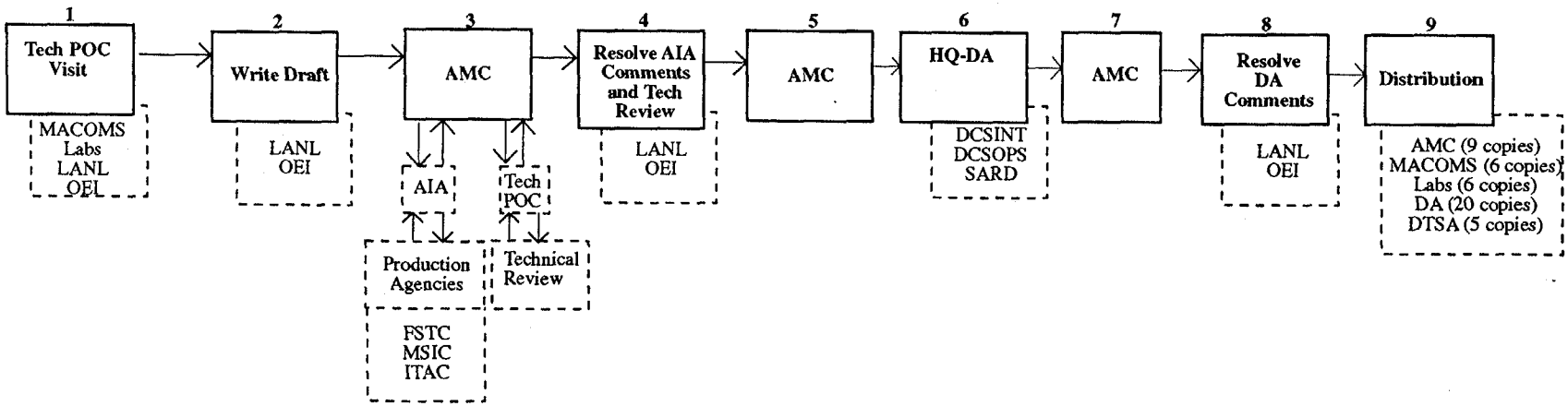


Figure 6. ATAR Development Process

9-X38-1032U-1

ATTACHMENT 1

Security Arrangements for Multinational Armament Cooperation Program--MLRS

SECURITY ARRANGEMENTS

FOR

MULTINATIONAL ARMAMENT COOPERATION PROGRAM

MLRS-TGW

SECURITY AND TECHNOLOGY TRANSFER

WORKING GROUP

(STTWG)

TABLE OF CONTENTS

INTRODUCTION

The Multiple Launch Rocket System/Terminal Guidance Warhead (MLRS/TGW) Program is a multinational cooperative program involving the United States, Great Britain, France and Germany. The Program is sponsored by U.S. Army Missile Command (MICOM) and is a joint venture special security agreement between Martin Marietta, Diehl GmbH, Thomson CSF and Thorn EMI. Together, these four corporations have formed a joint venture, U.S. company, called MDTT, Inc., to work on the MLRS/TGW Program.

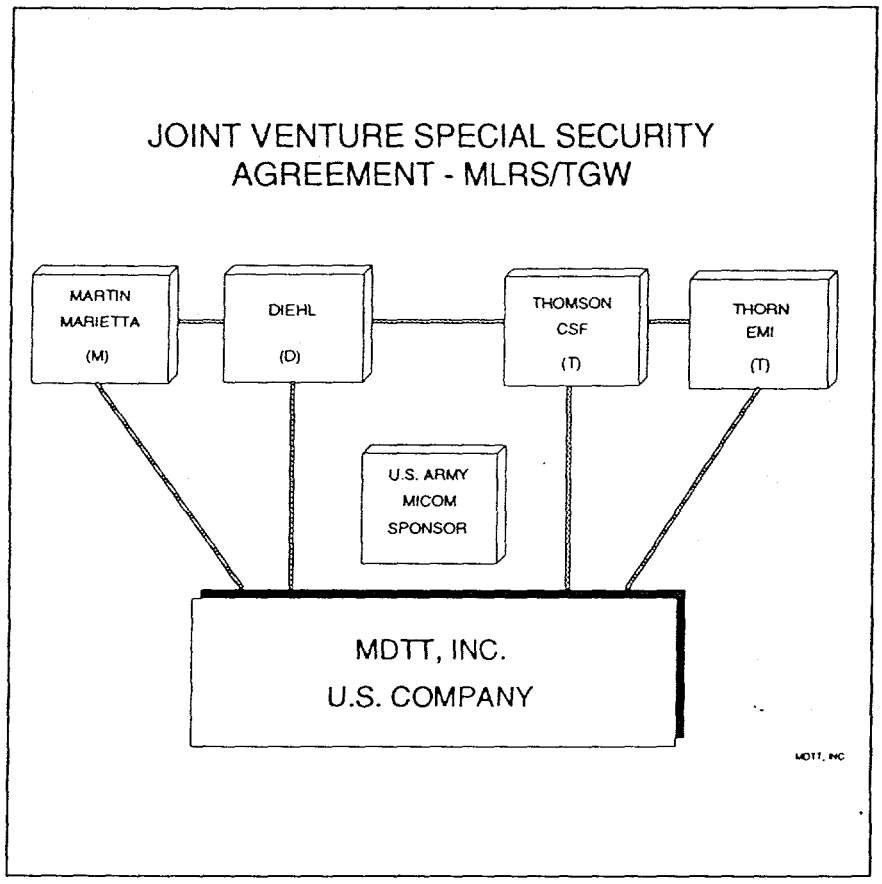


Figure 1

The MLRS/TGW Program requires the release of classified military equipment and information and controlled unclassified technical data. This security plan describes the procedures

that have been developed and adopted by the National Security Authorities (NSA) for the MLRS/TGW Program to ensure the proper protection of information shared in the program. It covers all aspects of transfer of material and information including physical release and oral and visual disclosure via visits of foreign personnel. The following procedures also are addressed in this pamphlet:

* Procedures and documentation required for the hand carriage of classified information and material, including procedures for approval and use of contractor courier personnel.

* U.S. Customs procedures for importing foreign material.

* Security communications and related physical security, operating procedures, record keeping and time allocation for administrative and custodial duties.

* U.S. and foreign security classification procedures for MLRS/TGW information.

* Visit procedures for recurring visits and emergency visits.

* Responsibilities of the Designated U.S. Representative, and designated contractor personnel.

* International transportation and shipping plans for classified and high-value shipments.

* Operational security.

ACRONYMS

COMSEC	- Communications Security
COR	- Central Office of Recrod
DA	- Department of the Army
DCS	- Defense Courier Service
DD	- Department of Defense
DIS	- Defense Investigative Service
DISP	- Defense Industrial Security Program
DLA	- Defense Logistics Agency
DLSSO	- Defense Logistics Standard Systems Office
DoD	- Department of Defense
DSA	- Designated Security Authority
GFE	- Government Furnished Equipment
HTSUS	- Harmonized Tariff Schedules of the United States
ISM	- Industrial Security Manual
ISR	- Industrial Security Regulations
ITAR	- International Traffic in Arms Regulations
MAPAD	- Military Assistance Program Address Directory
MICOM	- (U.S. Army) Missile Command
MLRS/TGW	- Multiple Launch Rocket System/Terminal Guidance Warhead
MMMS	- Martin Marietta Missile Systems
MOD	- Ministry of Defense
MOU	- Memorandum of Understanding
NATO	- North Atlantic Treaty Organization
NPO	- National Program Office
NSA	- National Security Authority
OPSEC	- Operations Security
SOP	- Standard Operating Procedures
STU	- Secure Telephone Unit
TAC	- Type of Address Code
US	- United States
USG	- United States Government

CHAPTER 1
HAND CARRIAGE OF CLASSIFIED INFORMATION

CONTRACTOR COURIERS

The standard method of transmitting classified documents across international borders is through government-to-government channels. These are routes which have been certified by individual governments as being secure and involve constant physical control by government employees.

Except for NATO, there were no provisos in U.S. regulations for the use of U.S. contractor couriers to hand carry classified material outside of the U.S. mainland, its possessions or trust territories. In December 1986, the Defense Investigative Service (DIS) approved the use of U.S. contractor couriers acting on behalf of the U.S. Government (USG) to carry out the overseas transfer of classified material. European industrial couriers have been in place since the MLRS/TGW Program's inception. Contractor couriers are limited to documentation and hardware that can be carried in the aircraft cabin.

All MDTT, Inc. personnel and Martin Marietta Missile Systems (MMMS) personnel who undertake any international travel relating to the MLRS/TGW Program must have proper documentation and follow the correct procedures in accordance with the International Traffic in Arms Regulations (ITAR) (Title 22, CFR, Sections 120-130), Department of Defense (DoD) 5220.22-M, "The Industrial Security Manual For Safeguarding Classified Information," (short name: Industrial Security Manual (ISM)) and company security policies.

Contractor couriers may be used on a case-by-case basis with approval of the Designated Security Authority (DSA) when official government-to-government channels are not reasonably available or transfer through government-to-government channels would result in a delay that will adversely affect performance on the MLRS/TGW Program. The U.S. DSA for the MLRS/TGW Program, approved by U.S. national authorities to be responsible for the security aspects of the MLRS/TGW Program, is *U.S. Army MICOM.*

Hand carriage is permitted only by an appointed courier of classified documents. The courier must maintain personal control over them at all times. The highest classification must not exceed **"SECRET"** and the documents must have been authorized by the owning government for release in conjunction with the MLRS/TGW Program. (Participating governments may impose a lower maximum classification level on the documents to be hand carried).

A contractor courier must be a permanent employee of the dispatching or receiving company and possess a personnel security clearance to at least the level of the classified documents which are to be hand carried.

The courier must be provided with a "Courier Certificate," written in English and - on the reverse - in the national language of one or more of the participating countries. The "Courier Certificate" will be stamped and signed by the DSA and by the company Security Officer of the dispatching country. "Courier Certificates" will bear the date of the beginning of the journey and will be valid for one journey only (the journey may include more than one stop) and must be returned to the issuing DSA through the dispatching company's Security Officer immediately after the end of the journey. The Security Officer must ensure that the courier possesses a valid export license, or other appropriate government authorization, if required.

A copy of the "NOTE FOR THE COURIER," outlining the courier's responsibilities, will be attached to the Courier Certificate. The courier must be aware that the non-fulfillment of his or her obligation to safeguard the classified information contained in the consignment and/or any other negligent action chargeable to him or her that gives rise to a security breach, will constitute not only a matter of contractual obligation but also a matter of possible penal responsibility. In the event of a breach by the courier, the dispatching authority may request the authorities in the country in which the breach occurred to carry out an investigation and report their findings to the dispatching authority and take legal action as appropriate.

Before each used "Courier Certificate" is returned to the issuing DSA both the courier and the Security Officer will sign a declaration at the bottom of the "Courier Certificate" certifying that no situation occurred that might have compromised the security of the consignment during the journey.

The dispatching company Security Officer will make out three copies of a receipt, listing the classified documents to be hand carried by the appointed company courier. One copy will be retained by the dispatching company Security Officer and the other two copies will be packed with the classified documents. The documents will be wrapped and sealed and placed in a container approved by the courier's national security authorities, by or in the presence of, the company Security Officer or a designated Government Representative in accordance with national procedures. The addresses of the Security Officer of the receiving and dispatching company or designated Government Representative will be shown on the inner and outer envelope or wrapping.

The Security Officer of the dispatching company will instruct the courier in all of his or her duties and ensure that he or she understands them and completes the declaration shown below. The Security Officer of the dispatching company, or a designated Government Representative, also must obtain from the courier a receipt for the sealed package.

The courier will be responsible for the safe custody of the classified documents until they are handed over to the receiving company Security Officer or a designated Government Representative, and a receipt has been obtained as evidence of delivery.

The receiving company Security Officer or the designated Government Representative, will sign both copies of the receipt in the package. One copy will be returned to the courier.

On his return the courier will pass the completed receipt to the dispatching company Security Officer or to the designated Government Representative. The second copy of the receipt will be forwarded by the receiving company Security Officer or the designated Government Representative to his or her DSA who is responsible for ensuring that the classified documents are properly protected while they are in that country's custody.

The receipt, which is packed with the classified documents, must contain the following details:

1. Exact description of the classified documents (originating organization, date of issue, copy number, registry reference number and number of pages, including annexes).

2. Date and time of handing over of the package to the addressee.

3. Name and position/appointment of the individual that signed the receipt.

4. Stamp or official seal of recipient's organization.

5. Signature of the recipient.

The dispatching company Security Officer will notify the receiving company Security Officer or a designated Government Representative of the anticipated date and time of the courier's arrival. If the courier has not arrived within 24 hours of the expected time of arrival, the receiving company Security Officer or designated Government Representative, after investigation including consulting the dispatching company Security Officer, will notify their DSA, unless officially notified otherwise of a change to the courier's itinerary.

Throughout the journey the classified documents will remain under the direct personal control of the courier. In particular, they must not be left unattended at any time during the journey, either in the transport being used, in hotel rooms, cloakrooms, or other such locations, nor may they be deposited in hotel safes, luggage lockers, or in luggage offices. Envelopes or packages containing the classified documents must not be opened en route, unless required by the Customs or other designated public officials.

The courier will comply with official requests to open classified consignments by Customs or other public officials. When inspection is unavoidable, care should be taken to show only sufficient parts of the contents of the consignments to enable the officials to determine that the consignment does not contain any items other than those declared.

In cases where the consignment is opened, to comply with a request by Customs or other public officials, the courier will notify his company Security Officer who will notify his DSA. If the inspecting officials are not of the same country as the dispatching company, the responsible NSA whose officials inspected the consignment also shall be notified.

Under no circumstances will the classified consignment be handed over to Customs or other public officials for their custody.

When carrying classified documents, the courier will not travel:

1. By surface routes through countries that are not participating in this arrangement, except as agreed by the DSAs;

2. On carriers of, or by air routes over countries designated by NSAs. Further advice on this matter may be requested from the DSAs, if necessary.

In cases where documents classified RESTRICTED are being carried, national security regulations will apply.

HAND CARRIAGE OF CLASSIFIED EQUIPMENT AND COMPONENTS

The above procedures also govern the urgent hand carriage by couriers of equipment and/or components classified **"SECRET"** or below relative to the MLRS/TGW Program. Participating governments may impose a lower maximum classification level on the equipment or components to be hand carried. The consignment will be of such size, weight and configuration that it can be retained at all times in the personal possession of the courier or accompanying security escorts.

The following requirements, in addition to the requirements cited above, also govern the urgent hand carriage by couriers of equipment or components classified **"SECRET"** or below relative to the MLRS/TGW Program. Participating governments may impose a lower maximum classification level on the equipment or components to be hand carried. The consignment will be of such size, weight and configuration that it can be retained at all times in the personal possession of the courier or accompanying security escorts. Except as modified in this section, the provisions for hand carriage of classified documents apply.

1. The "Courier Certificate" is to be used only to verify the bona fide of the courier and to avoid direct inspections of the hand carried items or, if an inspection is unavoidable, to have it done under security conditions. It will not be used as an instrument to avoid obligations on the exportation, importation and/or transit of material subject to export or import laws and regulations.

2. The Security Officer of the dispatching company, in collaboration with the company export officer and a security cleared forwarding agent if necessary will:

a. Obtain approval for the urgent transfer of the classified consignment by the national program office (NPO) or MLRS Program Director, Contracting Officer and responsible DSAs; as required by national regulations;

b. Verify the content of the consignment against a receipt and/or shipping documentation;

c. Provide the courier with the consignment to be hand carried, packaged in accordance with the existing national security regulations, after having accomplished the necessary administrative and customs requirements for exportation;

d. Provide the courier with the documentation necessary to carry the consignment out of the exporting country, for transit through or stops in intermediate countries (if any) and to enter the destination country;

e. Provide the courier with the inventory of the consignment, if an inventory is not in the above described documentation; and

f. Arrange for customs and security officials at the port of embarkation and debarkation, as well as diplomatic and military authorities of intermediate and destination countries, to be notified of the shipment and request their support.

3. The courier also must receive from the dispatching company's Security Officer all the instructions necessary to fulfil the operations of legal introduction and secure final delivery of the consignment in the country of destination. Such instructions will provide for unforeseen difficulties that may hamper or make it temporarily impossible to deliver the consignment to its final destination. Therefore, they must contain appropriate addresses and telephone numbers of company and government officials in the countries to be transitted and entered, who may be contacted for assistance. They may be the addresses and telephone numbers of:

a. Diplomatic or consular authorities or defense attaches of the courier's country;

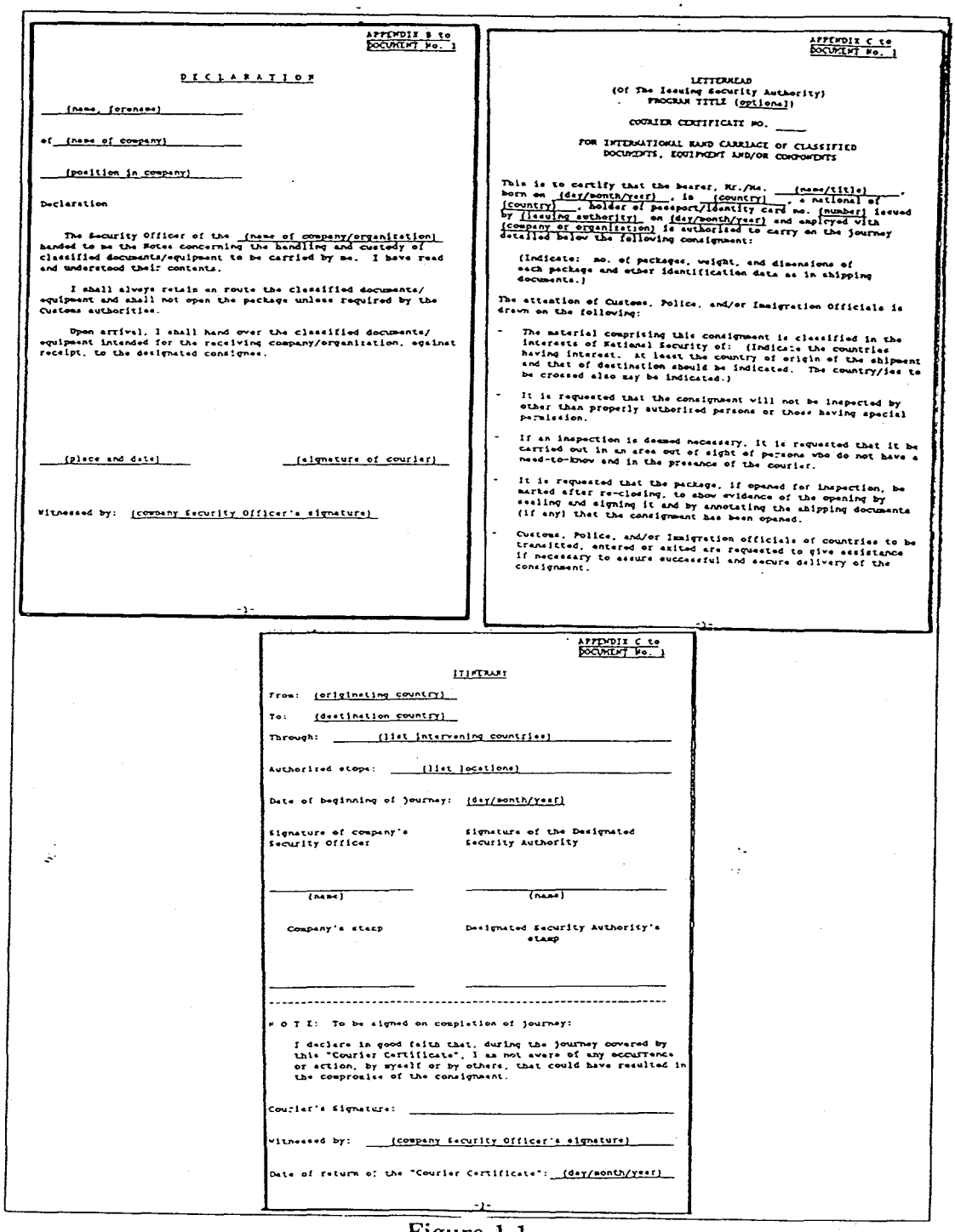
b. Police or other governmental authorities of the country where the courier has encountered difficulties;

c. The Security Officer of the receiving company.

4. In the event of difficulties, the courier will report only what is necessary to let the authorities understand the problem. Identification will be on the basis of the details of the "Courier Certificate", without revealing details concerning the consignment. The courier may reveal the number, weight, volume and dimensions of the consignment but not the nature of its

contents. In no case will the courier relinquish control of the consignment until it is delivered in accordance with the security instructions.

5. The Security Officer of the receiving company will inform the DSA of the anticipated classified consignment, and administrative formalities.



APPENDIX B to
DOCUMENT No. 1

DECLARATION

(name, forenames)

of (name of company)

(position in company)

Declaration

The Security Officer of the (name of company/organization) handed to me the Notes concerning the handling and custody of classified documents/equipment to be carried by me. I have read and understood their contents.

I shall always retain en route the classified documents/equipment and shall not open the package unless required by the Customs authorities.

Upon arrival, I shall hand over the classified documents/equipment intended for the receiving company/organization, against receipt, to the designated consignee.

(place and date) (signature of courier)

Witnessed by: (company Security Officer's signature)

-1-

APPENDIX C to
DOCUMENT No. 1

LETTERHEAD
(Of The Issuing Security Authority)
PROGRAM TITLE (optional)

COURIER CERTIFICATE NO. ____

FOR INTERNATIONAL HAND CARRIAGE OF CLASSIFIED DOCUMENTS, EQUIPMENT AND/OR COMPONENTS

This is to certify that the bearer, Mr./Ms. (name/title), born on (day/month/year), is (country), a national of (country), holder of passport/identity card no. (number) issued by (issuing authority) on (day/month/year) and employed with (company or organization) is authorized to carry on the journey detailed below the following consignment:

(Indicate: no. of packages, weight, and dimensions of each package and other identification data as in shipping documents.)

The attention of Customs, Police, and/or Immigration Officials is drawn on the following:

- The material comprising this consignment is classified in the interests of National Security of: (Indicate the countries having interest. At least the country of origin of the shipment and that of destination should be indicated. The country/ies to be crossed also may be indicated.)
- It is requested that the consignment will not be inspected by other than properly authorized persons or those having special permission.
- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not have a need-to-know and in the presence of the courier.
- It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.
- Customs, Police, and/or Immigration officials of countries to be transitted, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.

-2-

APPENDIX C to
DOCUMENT No. 1

ITINERARY

From: (originating country)

To: (destination country)

Through: (list intervening countries)

Authorized stops: (list locations)

Date of beginning of journey: (day/month/year)

Signature of company's Security Officer	Signature of the Designated Security Authority
(name)	(name)
Company's stamp	Designated Security Authority's stamp

N O T I: To be signed on completion of journey:

I declare in good faith that, during the journey covered by this "Courier Certificate", I am not aware of any occurrence or action, by myself or by others, that could have resulted in the compromise of the consignment.

Courier's signature:

Witnessed by: (company Security Officer's signature)

Date of return of the "Courier Certificate": (day/month/year)

-1-

Figure 1-1

CHAPTER 2
CUSTOMS PLAN (U.S.)

The Office of Defense Trade Controls, Department of State, requires the appropriate Temporary Import License for certain British, French and German Government-owned materials and components being sent for repair, assembly, or test in connection with the MLRS/TGW Program, that are imported temporarily into the United States under the auspices of a blanket duty-free authorization granted under subheading 9809.00.40, Harmonized Tariff Schedules of the United States (HTSUS).

All materials imported will remain the property of the British, French and German Governments while in the United States. All shipments will bear the code word "GRIDDLE".

CHAPTER 3
SECURE COMMUNICATIONS

STU II NETWORK

In October 1985, the idea of establishing a secure link between the MLRS/TGW Joint Venture partners, to communicate via encryption voice and facsimile, was presented to U.S. Army MICOM and to the Joint Venture partner governments. MICOM issued authorization for use of secure voice network communications equipment for the MLRS/TGW Program via the Department of Defense Contract Security Classification Specification (DD Form 254).

MDTT, Inc., the Joint Venture company for MLRS, developed standard operating procedures (SOP) to cover:

1. Physical security
2. Operating procedure
3. Record keeping
4. Time allocation

In May 1987 all governments approved the use of the STU II in a "close net" for MLRS/TGW data only. The net is comprised of the four Joint Venture partners and their governments. Delivery of keying material for the STU II equipment is performed by the Defense Courier Service (DCS) at the written request of the MICOM MLRS/TGW Program Contracting Officer. Previously, the contractor's DD 254 was accepted by DCS as contract officer's approval. This is no longer the case.

The STU II network is composed of the following companies and government offices:

1. MDTT, Inc. - Net Control (Orlando, Florida, U.S.A.);
2. Martin Marietta Missile Systems (Orlando, Florida, U.S.A.);
3. Diehl GmbH & Co. (Roethenbach, West Germany);
4. Thomson CSF (Malakoff, France);
5. THORN EMI Electronics, Ltd. (Feltham, United Kingdom);
6. MICOM MLRS/TGW Program Management Office (Huntsville, Alabama, U.S.A.);

7. Federal Republic of Germany MLRS/TGW Program Management Office (Bonn, Germany);

8. Republic of France MLRS/TGW Program Management Office (Paris, France);

9. United Kingdom MLRS/TGW Program Management Office (London, England).

MDTT, Inc. presently is seeking purchase approval for GFE Encryption Devices to transmit classified software data from flight test programs as well as timely software updates between the field test sites and MDTT, Inc, and among the Joint Venture partners.

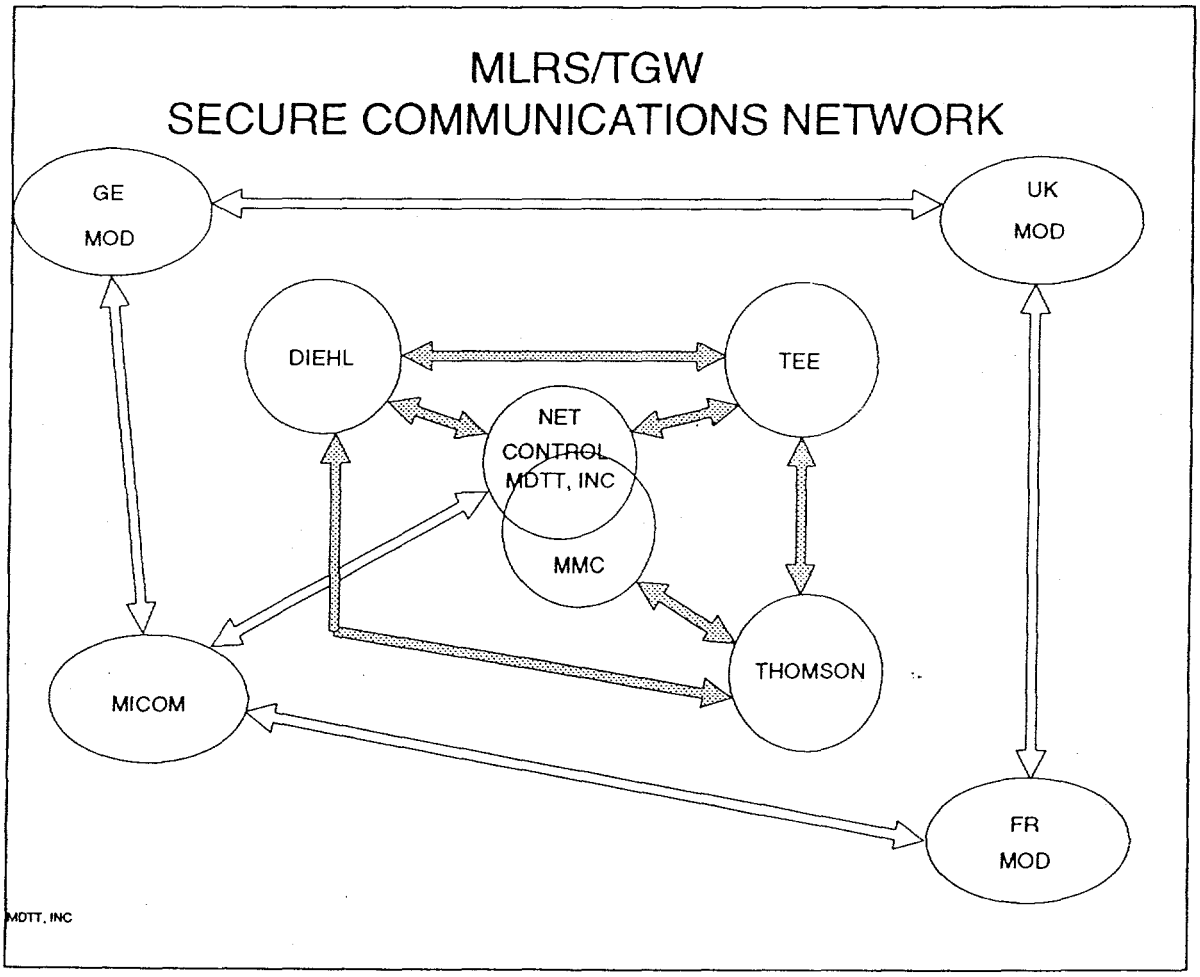


Figure 3-1

ADMINISTRATIVE REQUIREMENTS

Each station is required to provide Net Control (MDTT, Inc.) with written assurance that *their national* directives meet the following, minimum U.S. requirements:

1. Identification and location of the STU II equipment.

2. Identification and telephone numbers (office and home) of the primary and alternate persons responsible as COMSEC custodians.

3. Local procedures for denying access to COMSEC material and equipment by unauthorized persons.

4. Method to be used to account for COMSEC equipment and keying material.

5. Local procedures covering the removal, transfer, maintenance and repair of the COMSEC (STU II) equipment.

6. Local procedures for the destruction or return of COMSEC equipment and material.

7. Method used to receive and store the key.

8. Identification of the person(s) authorized to key and/or re-key the STU II.

9. Local procedures for reporting actual security violations regarding the STU II.

CUSTODIAL RESPONSIBILITIES

The U.S. requires that the COMSEC (STU II) Custodian, or Alternate(s), be responsible for the receipt, custody, issue, safeguarding, accounting,and disposition and destruction of COMSEC material. Each station is required to provide Net Control (MDTT, Inc.) with written assurance that their national directives meet the following, minimum U.S. requirements:

1. Protect COMSEC material and limit access to personnel with valid clearances and need-to-know for the classification level of the material.

2. Receive, receipt for, and ensure the safeguarding and accounting of all material issued to the COMSEC account.

3. Maintain appropriate COMSEC accounting and related records.

4. Conduct a semi-annual inventory, or an inventory upon the appointment of a new custodian, wherein all material in the account is physically sighted and records are annotated and reported to the appropriate Central Office of Record (COR).

5. Perform destruction of disposable keying tape within twelve (12) hours of supersession; if a weekend or holiday occurs, perform destruction during the first hour of the first work day after the weekend or holiday. Keep destruction records for three (3) years.

6. Establish procedures to ensure strict control of each item of keying material, being aware at all times of the location of each item of accountable material held by the account.

7. Report known or suspected COMSEC security incidents immediately to the COR and also to the National Prime's security investigative agency.

8. Prepare an Emergency Plan for safeguarding COMSEC material during emergency situations.

9. Verify need-to-know and security clearance of individuals requiring access to COMSEC material.

10. Provide initial COMSEC briefings, and annual re-indoctrinations, for all individuals who have access to COMSEC information.

11. Ensure that all accountable material shipped outside the facility is packed and shipped by authorized methods.

12. Establish a "Visitor Register" to record access given to persons whose names do not appear on the entrance list. This register should include:

    a. Date of access

    b. Signature of the visitor

    c. Printed name of the visitor

    d. Organization represented

    e. Purpose of the visit

    f. Signature of the authorizing authority

g. Time in and out

13. Establish a procedure to ensure that all locking devices are properly secured, that alarms are activated, and that other security measures are in force.

14. Prohibit the installation or use of telephones, other than the STU II, within the secure communications facility unless:

    a. Installation is fully justified by operational necessity.

    b. Approval has been obtained from the appropriate NSA with notification to MDTT, Inc.

    c. Installation is made in accordance with the appropriate NSA.

    d. If a telephone is installed, it cannot be used when the STU II instrument is being utilized; and vice-versa.

15. Prohibit the entrance of TVs, tape recorders, public address systems, or other electronic equipment into the secure communications facility except as required in the fulfillment of the contract.

CHAPTER 4
CLASSIFICATION OF DOCUMENTS

SECURITY CLASSIFICATION GUIDE

The MLRS/TGW Security Classification Guide, issued by the Program Coordinator for MLRS at MICOM, provides the foundation for security classification of information and material pertaining to the MLRS/TGW. Issued under the authority of Army Regulation (AR) 380-5, "Department of the Army Information Security Program," this security classification guide constitutes authority and may be cited as the basis for classification regrading, or declassification of information concerning the MLRS/TGW System.

Questions concerning the content and interpretations of the security classification guide for MLRS/TGW should be directed to the Program Coordinator for MLRS at MICOM. If the security classifications imposed by this guide are considered impractical, documented and justified recommendations should be made through appropriate channels to the Program Coordinator at MICOM. If current conditions, state of the art, or other factors indicate a need for changes, similar recommendations should be made. Pending a final decision, the information involved will be protected at either the currently assigned level or the recommended level, whichever is higher. Any over-classification or incorrect classification should be brought to the attention of MICOM.

UNCLASSIFIED INFORMATION

Certain details of information involved in the MLRS/TGW Program will be **"UNCLASSIFIED"**. However, the information is not automatically authorized for public release. Proposed public release of **"UNCLASSIFIED"** information must be processed through appropriate channels for approval for publication. Department of the Army (DA) activities will follow the procedures outlined in AR 360-5. Defense contractors will comply with the Industrial Security Manual (ISM) and other requirements. Other DoD activities will comply with DoD Directive 5230.9, "Clearance of DoD Information for Public Release," and applicable service regulations.

INFORMATION CLASSIFIED BY A FOREIGN GOVERNMENT

Information or data that previously has been classified by a foreign government will be classified at a level which will give the information or data at least the same degree of protection as provided by the foreign government classification. This procedure will be followed even though a higher classification than normally imposed by the U.S. for the same type of information may result.

Each government and contractor shall assure that classified and unclassified data is handled within the system at least to the comparable minimum security requirements contained in the MLRS/TGW Security Classification Guide. In addition, the following also should be considered when classifying such information:

1. The classification level assigned should be the highest anticipated. Security classification in any case must be determined by considering all applicable elements. When partial information relative to those subjects is presented, the lowest classification consistent with adequate protection of the information concerned will be assigned. Similarly, a higher classification may be assigned to compilations of information if the compilation provides an added factor which warrants higher classification than that of its component parts. Classification on this basis shall be fully supported by a written explanation that will be provided with the material so classified.

2. Data or information relating to the threat systems, or other intelligence derived from material, must bear the security markings of that threat or other intelligence material. The release of threat or other intelligence material may require the consent of the producer. All dissemination of threat or other intelligence information from MICOM is controlled by the Foreign Intelligence Division (FID), Intelligence and Security Directorate, U.S. Army MICOM. Threat information will not be reproduced or otherwise disseminated unless approved by the FID. Questions regarding any release of threat or other intelligence information shall be referred to the FID.

3. Reports, publications, drawings, schematics, photographs, models, markups, training aids, test data, hardware, etc., will be assigned a security classification commensurate with the information classified by the MLRS/TGW Security Classification Guide and other applicable security classification guides. External and internal views which may yield classified parameters, characteristics, and/or performance will be classified in accordance with the classification of those items revealed.

FRENCH CLASSIFICATION OF INFORMATION

There are differences between the French classification of classified material and the United States classification that need to be taken into consideration when shipping classified information or material overseas.

U.S. "**CONFIDENTIAL**" is equivalent to the French "**CONFIDENTIEL DEFENSE**". However, "**CONFIDENTIEL DEFENSE**" in and of itself extends beyond the U.S. "**CONFIDENTIAL**" level to the U.S. "**SECRET**" level. The French "**SECRET DEFENSE**" extends to the U.S. "**TOP SECRET**" level. Thus any document that has the "**SECRET DEFENSE**" stamp cannot be transmitted via high value service (which may be used to ship classified information

and material no higher than U.S. "**SECRET**") and must be sent by Diplomatic Pouch, or hand carried by courier.

In order to facilitate the timely transfer of information and maintain the program schedule, any MLRS/TGW material that is to be transmitted to France should be reviewed at MDTT, Inc. or MMMS by French engineers prior to shipment. If the material is determined to be "**CONFIDENTIEL DEFENSE**" than it should be so stamped instead of "**SECRET DEFENSE**".

EQUIVALENT SECURITY CLASSIFICATIONS AMONG THE MLRS/TGW PROGRAM PARTICIPATING GOVERNMENTS

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
FRANCE	(1)	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
GERMANY	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	VS-NUR FUR DEN DIENSTGEBRAUCH
UNITED KINGDOM	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
UNITED STATES	TOP SECRET	SECRET	CONFIDENTIAL	(NO EQUIVALENT)
	(1) ONLY FOR GOV-ERNMENT PRIORITIES			

Figure 4-1

PROTECTION OF PROGRAM CLASSIFIED INFORMATION

Prior to the MLRS/TGW Program, only U.S. citizens who were employees of a facility with a U.S. clearance could have the combination or access devices to classified containers and controlled areas.

In 1986, an exception was granted for all MDTT, Inc. participating personnel to have access to controlled areas and container custodianship providing the information is MLRS releasable and that the necessary clearances are on record.

Procedures also have been established for the protection of classified information overseas. A briefing has been developed which covers the requirements of the DoD ISM as it applies to cleared DoD contractor personnel stationed overseas. This briefing is given to all company employees who may require access to U.S. and/or foreign classified information and controlled areas pursuant to performance on their facility's contract(s) overseas.

CHAPTER 5
VISIT PROCEDURES

RECURRING INTERNATIONAL VISITS

In order to facilitate access to contractor and government facilities that are participating in the MLRS/TGW Program, the following visit procedures have been agreed to by the participating nations:

1. Each NPO has prepared a list of its government and contractor facilities that are directly involved in the MLRS/TGW Program. Each list includes the name, complete telephone number, mail and electronic message addresses of each government's DSA and the individuals at each listed facility who have responsibility for (a) Program management and (b) Program security. These lists are forwarded to the consortium manager for MLRS/TGW, which is MDTT, Inc., the joint venture company. The NPO's from each government have verified with their DSA that the facilities involved hold security clearance at the required level.

2. The consortium manager, MDTT, Inc., has prepared a consolidated list, known as the "Facilities List", of participating government and contractor facilities. These facilities are listed numerically by country and have been assigned a facility code (an example of a facility code would be if Martin-Marietta in Orlando, Florida is the first listed United States facility for the MLRS/TGW Program, it's facility code would be listed as US/MLRS #1). MDTT, Inc. has provided the Facilities List to the other participating program offices.

3. Each NPO requires the security officers of its participating government and contractor facilities to submit Block Lists for their representatives who require access to Program classified information and/or controlled sites and who will have an official need to make frequent visits to other participating facilities during the following 12 months. (See Appendix A for the suggested format of a Block List Request).

4. The NPO of each country verifies the need for access by facilities and personnel, and forwards the Facilities List and Block Lists to their national DSA office for verification of the facility and personnel security clearance data and final approval. On completion, copies of the approved Facilities List and Block Lists are forwarded to the DSAs of the other participating countries, the consortium manager, and the participating facilities, as required, under the jurisdiction of the dispatching DSA.

5. Individuals whose names appear on an approved Block List may visit a participating facility upon 72 hours (3 WORKING days) notice by their Security Officer to the Security Officer of the facility to be visited. These individuals may visit only the precisely designated areas of the facility.

6. Block Lists are reviewed and updated at least annually. Information concerning individuals or facilities derived from routine or emergency requests is added at this time, as appropriate.

U.S. GOVERNMENT FACILITIES INVOLVED IN MLRS/TGW

Several U.S. Government facilities are involved in the MLRS/TGW Program and are on the U.S. Facilities List. These include:

* White Sands Missile Range (WSMR)

* Holloman AFB

* Eglin AFB

* Ft. Drum

* Ft. Sill

* Aberdeen Proving Ground (APG)

EMERGENCY VISITS

When an emergency visit exists that cannot be accommodated by the normal application and amendment to the Block List, the following procedures will be used:

1. Amendments to Block Lists will be by electrical message from the company which submitted the original Block List. The subject of the message will be: **"Emergency Amendment to visit request number..."** (See Appendix A for the suggested format for Emergency Visit requests).

2. The message will be sent by priority precedence at least seven working days prior to the requested visit to the following addressees:

a. *If a contractor visit request*:

(1) The appropriate government security office(s) in the country of the originating company:

(2) The embassy of the originating company's government in the country to be visited;

(3) The specified government security offices in the country to be visited; and

(4) If visiting a company, the security office of the company to be visited.

b. *Government personnel visit request*:

(1) The central control point in the appropriate government security office of the country of the government employee;

(2) The embassy of the originating government in the country to be visited;

(3) The specified government security offices in the country to be visited; and

(4) If visiting a contractor location, the security office of the company to be visited.

3. The message will contain the name, rank or title, passport number, nationality, place of birth, date of birth, and security clearance level and number (if appropriate) of the individual(s) for whom the amendment is requested.

4. The message will specify the location to be visited, a point of contact at that location, the dates of the visit, the specific and detailed purpose of the visit if it differs from the purpose stated on the Block List, and the reason the visit could not be included in the Block List.

5. The message will included the statement: **"Request approval. Approval will be assumed unless disapproval is received at least two working days before the proposed visits."**

6. Any addressee may deny or disapprove the request, up until the time of visit in exceptional circumstances, in which case all other addressees will be notified.

7. Block Lists will continue to be submitted annually, but they will be updated in hard-copy on a quarterly basis only. Quarterly updates will included all emergency amendments.

APPROVED MDTT, INC. JOINT VENTURE SUBCONTRACTORS TO USE THE MLRS/TGW EMERGENCY VISIT PROCEDURES

PRIME CONTRACTOR	SUBCONTRACTOR
MDTT, Inc.	TRW Electronics System Group
Martin Marietta	None
Diehl GmbH & Co.	AEG Aktiegeselschaft Aero-Dienst GmbH SAC Technology Group Limited Technology Project Services (International), Ltd.
Thomson-CSF	Talley Defense Systems
THORN EMI	British Aerospace PLC

Figure 5-1

CHAPTER 6
DESIGNATED U.S. GOVERNMENT REPRESENTATIVE

GENERAL

A person designated as an official U.S. Government Representative is the USG authority responsible for the transfer or receipt of classified information between the USG and a foreign government. The primary responsibility of the Government Representative is to ensure that only classified information authorized for release to a foreign government is, in fact, the only information released. Designated Government Representatives must have a security clearance and a need-to-know. The appropriate DIS Office will brief the Government Representative of his or her responsibilities and furnish copies of the following:

1. Industrial Security Regulations (ISR), DoD 5220.22-R.

2. Industrial Security Manual (ISM), DoD 5220.22-M.

3. International Traffic in Arms Regulations (ITAR), Title 22, CFR, Sections 120 130.

4. DIS "Handout for Designated U.S. Representatives."

Government-to-government channels of transmission are used in the exchange of both U.S. and foreign classified information between countries.

There are four basic conditions under which classified information and material may be exchanged between governments. They are:

1. ***Classified information or material may be provided a foreign government under the Mutual Aid Program by a User Agency.***

2. ***The U.S. Government, through a User Agency, contracts for and acts as buyer for the foreign government (i.e., the User Agency issues a U.S. contract to cover the foreign purchase.***

In the case of both 1. and 2., above, the User Agency concerned is responsible for government-to-government transmission and a designated Government Representative is not required. An export authorization also is not required.

3. ***A foreign government or firm negotiates and awards a contract directly to U.S. industry.***

Under this condition, the appropriate DIS office is responsible for establishing the procedures for the classified transmissions between countries. A Government Representative, designated by the

DIS office, will be responsible for transferring any classified information authorized for release for the foreign government.

4. ***Co-production programs with foreign governments.***

Under this condition, one of the U.S. Military Departments is assigned the responsibility for acting as the executive agent for the major end item or weapons system. In such cases, the assigned military executive agent is responsible for monitoring all security aspects related thereto, including the responsibility for establishing government-to-government transmission channels. *The MLRS/TGW Program falls under this category. U.S. Army MICOM is the executive agent for the Program.*

GOVERNMENT CONTRACTORS

Under the MLRS/TGW Program, procedures have been established to allow U.S. Government contractors to be designated as government-to-government representatives. A contractor individual designated by the appropriate DIS Office as a U.S. Government Representative, and an alternate, must be U.S. citizens, have appropriate security clearances, and possess a "need to know". Both the Representative and his or her alternate will receive a security briefing by a DIS representative. A contractor will be designated as a U.S. Government Representative only for information or material relating to the MLRS/TGW Program. Any changes in the U.S. Government Representative must be made in writing to the appropriate DIS Field Office.

CHAPTER 7
INTERNATIONAL TRANSPORTATION AND SHIPPING PLANS

GENERAL

At the start of the MLRS/TGW Program, there were only two methods used for the transfer of classified hardware: the diplomatic pouch and military air. Cleared freight forwarders exist for most of the European countries and are generally national air carriers whose freight handling services are cleared by their national security agency. These freight forwarders are authorized to receive and deliver classified material on behalf of their governments. In some countries however, there are some restrictions dealing with the level of classified information. Up until recently the U.S. had no such capability.

In the fall of 1989, MDTT, Inc., the MLRS joint venture company, was tasked to develop a shipping plan for the transport of classified material using U.S. airline High Value Service. Final approval was received from the DoD in October 1989. This method was thought to be readily accepted by all governments in the joint venture partnership. However, after the first two successful shipments, the UK questioned the use of High Value for documents and France would not accept any material above "CONFIDENTIEL DEFENSE." The German Government voiced no problem.

Classified material shipped under these procedures must be classified no higher than US SECRET. They may be used only by companies and their subcontractors performing on prime contract DAAH01-85-C-A004.

All shipments are government-to-government via a cleared air carrier of one of the participating governments. Only premium "High Value" type air carrier service is used to ship classified information outside of diplomatic channels or by military air. Shipments must remain in the custody of the same carrier from air terminal point of origination to final air terminal destination. Prior to shipment, the shipping company (consignor) will obtain, in writing, the name, title, address, and phone number of the individual authorized by the receiving government to receive the shipment. This documentation is retained for two years.

PREPARATION FOR SHIPMENT:

Material will be packaged as prescribed in 17a(1), of the ISM. Outer markings will contain the name and phone number of the individual designated by the recipient government to receive the shipment, the return address of the US Government Representative processing the

outgoing shipment and the following notations in the language of both shipping and receiving countries:

ENGLISH

1. "DELIVER TO ADDRESSEE ONLY"
2. "PLEASE NOTIFY CONSIGNOR AND CONSIGNEE (telephone numbers) IMMEDIATELY IF SHIPMENT IS DELAYED BECAUSE OF ACCIDENT OR INCIDENT."

FRENCH

1. "REMETTRE SEULEMENT AU DESTINATAIRE"
2. "PRIERE D'INFORMER L'EXPENDITEUR ET LE DESTINATAIRE (numeros de telephone) IMMEDIATEMENT SI L'EXPEDITION EST RETARDEE QUELLE QUE SOIT LA CAUSE."

GERMAN

1. "NUR AN DEN EMPFANGER AUSLIEFERN"
2. "BITTE INFORMIEREN SIE ABSENDER UND EMPFANGER (Telephonnummern angeben) UNVERZUGLICH FALLS SICH DIE AUSLIEFERUNG WEGEN UNFALL ODER ANDEREN ZWISCHENFALLEN VERZOGERN SOLLTE."

An envelope containing a receipt for the signature of the consignee MAY be attached to the outside of the container if the shipment is not to be opened by the addressee on the outer wrapper. If so, the receipt will NOT describe or list the contents of the shipment, but be for a sealed package (container) and description.

METHOD OF SHIPMENT:

Prior to shipping, the consignor will obtain the scheduled departure and arrival times of the proposed transporting aircraft.

The consignor will notify the consignee of the carrier, of the approximate size of the package (shipment), the method of shipment (airlines/high value), and the scheduled arrival times. The consignee will be requested to notify the consignor immediately if the shipment is not received within 24 hours or if information is received that the shipment was delayed or lost due to an incident while in the carrier's possession.

A cleared employee of the consignor may be used to transport the shipment to the airline freight terminal after it has been sealed by the US Government Representative. It must be delivered no sooner than 3 hours prior to scheduled aircraft departure time. A signed receipt for

the shipment must be obtained. It is retained by the consignor until the detailed receipt inside the inner container is received from the ultimate addressees.

An inquiry will be initiated immediately on receipt of information that a shipment did not arrive within 24 hours of the scheduled arrival time, or of notice of delay due to accident or incident. In such a case, the DSA of the shipping and receiving company will be notified promptly.

FREIGHT FORWARDERS AND UNCLEARED FOREIGN OWNED/CONTROLLED FACILITIES

Paragraph 8-104, of DoD 5200.1-R, "Information Security Program Regulation", permits shipment of classified material which is authorized for release to a foreign government to:

1. a duly authorized representative of the recipient government at a point of departure from the U.S. (Freight Forwarder); or

2. a storage point owned or controlled by the recipient government for temporary storage pending availability of a carrier (Foreign Owned/Controlled Facility).

Foreign Owned/Controlled Facilities serve the same purpose as freight forwarders but are under the complete control of the foreign government. They cannot be cleared but can be approved by DIS to receive material, which is authorized for release to the controlling government, classified to the "**SECRET**" level .

Freight Forwarders

The establishment of freight forwarders allows for the commercial yet secure transportation of classified material between program destinations in the United States and Europe, thus relieving the pressure on the MOU countries' diplomatic channels and providing the Joint Venture with a mode of transportation which improves its ability to perform within the Program schedule.

U.S. Freight Forwarders are U.S. agents designated by a foreign country to receive, process, and tranship security assistance program material between User Agencies and foreign governments. They are "duly authorized representatives" of that foreign government. Freight Forwarders are cleared in the Defense Industrial Security Program (DISP) on request of a foreign country or U.S. service representative. Requests for facility clearance are submitted through the

Defense Logistics Agency (DLA) and DIS. Freight Forwarders must have DIS-approved safeguarding capability no less than **"SECRET"**.

The MLRS/TGW Program uses Emory Air Freight as an established cleared U.S. Freight Forwarder. Emory Air Freight is authorized to accept and deliver classified material overseas to and from the following destinations:

1. Orlando, Florida

2. Los Angeles, California

3. El Paso, Texas

4. Dallas/Ft. Worth, Texas

These ports allow shipments to be made to and from Martin Marietta, TRW and the U.S. Government White Sands Missile Range (WSMR) test facility respectively.

The applicable ports in Europe are:

1. London (Gatwick), England

2. Paris (Orly), France

3. Frankfurt, West Germany

These ports allow shipments to be made to and from THORN EMI Electronic, Ltd., Thomson-CSF and Diehl GmbH and Co., respectively, who are the European Partners in the MDTT Joint Venture.

Foreign Owned/Controlled Facilities

Classified storage at Foreign Owned/ Controlled facilities must have DIS-approved safeguarding capability no less than **"SECRET"**. Foreign Owned/Controlled Facilities always must have guards.

Government-to-government transfer occurs on receipt at the Freight Forwarder or Foreign Owned/Controlled Facility. The shippers are USG User Agencies and the recipients either agents designated by the foreign government to represent it or personnel of the foreign government.

User Agencies do not verify storage capability of either type facility with DIS prior to shipping classified. They ship to an address listed in the Military Assistance Program Address

Directory (MAPAD). Each addressee in the MAPAD is coded to show the type and mode of shipments which can be made to that location. The codes indicate if shipment of classified is authorized. *If shipment of classified is authorized, that automatically certifies that the facility can store "SECRET".* (The coding is a "Type of Address Code" abbreviated as TAC. TAC's A and B indicate authorization for classified.) The MAPAD is published and updated monthly by the Defense Logistics Standard Systems Office (DLSSO) under DoD Directive 4000.25, "Expedited Address Changes".

HIGH VALUE GOVERNMENT-TO-GOVERNMENT SHIPMENTS:

U.S.

The following procedures, which were established by the previous freight forwarders, American Airlines, are representative of those that will be established for high value MLRS shipments on other approved carriers: (Bracketed figures indicated values that will be established with the carrier).

1. The size of the shipment can not be less than [12x12x12] with a declared stated value not to exceed [$500,000]. Shipments of more than the limit require special consideration with prior approval of [Mgr. Corporate Insurance Administration] and on the condition that customers make their own pick up and delivery arrangements.

2. High Value Shipments must be booked in advance by calling the [International overseas office]. High Value Shipments will be booked and can only be accepted during business hours and will be received at the point of destination during hours of business. Acceptance time frames will be limited at the point of origin so that the shipment will arrive at the point of destination between 0900 Monday and 1200 noon Friday. Holiday High Value Shipments must be avoided. Normal working hours will be considered to be 0800 to 1700 Monday through Friday.

3. For shipments valued at [$500,000] or more, the General Manager or appropriate station management at the final carrier's destination cities must authorize dispatch before it may be shipped from the point of origin. This authorization and advance approval are handled via Telephone contact only. Shipments valued at [$500,000] or more must have advance concurrence by both the carrier's destination management and the downline connecting carrier to be certain that the other carrier will accept transfer. For example: Emory Air Freight to France to Brinks (the approved carrier for Thomson CSF). The origin city will not accept a shipment from the shipper until the arrangements at the transfer city have been finalized and are acceptable to the other carrier. Arrangements must be made by telephone contact only.

4. All handlers for High Value Service (both in the United States and abroad) are required to have a Security check and must be closely supervised by the carrier's supervisory per-

sonnel. Due to the great liability potential high value shipments are monitored and accounted for from time of receipt by the carrier until time of delivery to consignee or authorized carrier.

FRENCH

French high value shipments are brought to Miami via Air France, the French established cleared Freight Forwarder. MMMS employees assigned as couriers pick up the shipments from Air France for the MLRS Program and transport the shipment to MMMS, secure it in a closed area, and make it available to the U.S. Government Representative for inspection and transfer as soon as practicable.

Although designated couriers pick up the material from Air France and transport it to MMMS, the formal government-to-government transfer does not take place until the cases are opened, the contents inspected and the proper paper work executed. The MMMS couriers only sign for the sealed shipment and transport it to MMMS. They do not function as official government representatives.

DIS has provided the French Government with a Security Assurance for the list of cleared MMMS personnel who are assigned as couriers to pick up packages from Air France for the MLRS/TGW Program.

BRITISH

The British Government uses British Airways as its established cleared freight forwarder. Classified hardware in moved via British Airways' Valued Cargo Services. The following procedures are used to transport classified hardware from the U.K. contractor THORN EMI to Martin Marietta in Orlando, Florida:

1. A THORN EMI company courier will deliver the material to British Airways at Gatwick to connect with a pre-determined flight to Orlando.

2. THORN then will inform Martin Marietta of the relevant details as soon as the information is available.

3. Martin Marietta will arrange collection by DIS-approved company couriers who will deliver the sealed container to the authorized Security Officer.

4. The point of physical transmittal will be Orlando Airport, at the British Airways Valued Cargo vaults, as agreed to by DIS. The British Government will cease to have responsibility over the shipment at that point and the U.S. Government will assume responsibility.

5. Martin Marietta will acknowledge safe receipt of the consignment.

These procedures will be used only to ship classified hardware to MLRS/TGW joint venture partners. The British Government has approved this system only for hardware and not for classified documents.

GERMAN

**** PROCEDURES TO BE ADDED ****

CHAPTER 8
OPERATIONS SECURITY

TO BE ADDED

APPENDICES

APPENDIX A

EMERGENCY AMENDMENT TO VISIT REQUEST NUMBER:_____

TO: DATE

INFO COPY:

BLOCK LIST NO.: _____

NAME: _____
(LAST, FIRST, MIDDLE)

TITLE: _____

LEVEL OF CLEARANCE: _____

DATE AND PLACE OF BIRTH: _____

SECURITY CERTIFICATE NO.: _____

CITIZENSHIP: _____

COMPANY: _____

PASSPORT NO.: _____

CONTRACT NO.: _____

LOCATION TO BE VISITED: _____

POINT OF CONTACT: _____

PURPOSE OF VISIT: _____

DATE OF VISIT: _____

REASON FOR EMERGENCY REQUEST: _____

Request approval. Approval will be assumed unless disapproval is received at least two days before the proposed visit.

Security Manager _____

Government Agency/Company _____

Phone/Telex Number _____

FORMAT FOR BLOCK LISTS

BLOCK LIST

ORIGINAL DATE: (The date the original request is prepared)

REVISED DATE: (Date of the latest amendment)

SUBJECT: Block List for MLRS/TGW Program

REQUESTING FACILITY: (Originator of list)

SECURITY OFFICER/CERTIFICATION: (Name, address, telephone number of facility security officer, followed by a certification that all security clearance and "need-to-know" have been verified.)

NAME/GRADE/TITLE DOB/POB CITIZENSHIP SC ID#PP#

(Provide the date of birth (day/month/year), place of birth, and country of citizenship.)
Example: 10.01.44, London UK, British

(Provide the level of personnel security clearance: C-Confidential, S-Secret, and TS-Top Secret.)

(Fill in either the individual's official identification card or passport number. The number is needed to verify the individual's identity upon arriving at one of the facilities.)

LOCATIONS: (List facilities to be visited according to code from consolidated Facilities List.)

APPENDIX B

GOVERNMENT SECURITY OFFICES INVOLVED IN THE MLRS/TGW PROGRAM

UNITED STATES	UNITED KINGDOM	FEDERAL REPUBLIC OF GERMANY	FRANCE
Mr. Stephan Lewis Director of Industrial Security, Defense Investigative Service, Southeastern Region, S4110	MOD Security, IVCO Metropole Building Northumberland Ave London, WC2N 5B1 England Telephone: 218 5773 Telex Address: Security 5C/IVCO Telex: 22241	Budesamt fuer Wehrtechnik und Beschaffung WM IV-5, Postfach 7360 5400 Koblenz, West Germany zu Haenden: Hr. Huefner/Hr. Wassenberg Telephone: 261-400-7638 Telex Address: BWB, WM IV/5, Prob. MLRSS Koblenz, ATTN: Hr. Huefner Telex: 862661, Fax: 261-400-7098	Delegation aux Relations Internationales (DRI) (LTC Roussel) B.S. 5 14 rue Saint Dominique 75997 Paris Armees, France Telephone: 45.55.95.20 Telex Address: DRI for LTC Roussel SDC/B.V.10 Telex: 270003+Delegram, Derelint Paris
Mr. Ronald E. Valimaki, Chairman Commander AMC 5001 Eisenhower Avenue Alexandria, VA 22333-001 Attn: AMCMI-CT Telephone: (202) 274-7016 Fax Only: (202) 274-0665		Bundesministerium fuer Wirtschaft Referat Z/5, Postfach 140260 5300 Bonn 1, West Germany zu Haenden: Ministerialrat T. Koenig Telephone: 228-6151 Telex Address: BMWi Z/5 Bonn - Attn: Hr. Koenig, Telex: 886 747	Direction des Armements Terrestres (DAT) (ASA/ART) (Mr. Du Parquet) 10 Place Georges Clemenceau 92211 Saint-Cloud Cedex, France Telephone: 47.71.42.32 Telex Address: DAT for Maj. Ceron & Mr. Du Parquet, Telex: 260010 Fax: (1) 46029226
Mr. Tom O'Malley U.S. Army Missile Command Security Directorate, Attn: AMSMI-SI-CI-SO Redstone Arsenal, AL 35898-5160 Tele: (205) 876-1345, Fax Only: (205) 876-0510			
Defense Investigative Service P.O. Box 2499-43216, 3990 E. Broad St., Bldg. 306, Upper Floor, Columbus, OH 43213 Attn: L. Harris, Telephone: (614) 238-2136 Telex Address: DISCO-ATTN: S0833 L. Harris Telex: 245-463			
Defense Investigative Service Industrial Security Field Office 3659 Maguire Blvd., Suite 190 Orlando, FL 32803-3726 Attn: William F. Shreve, Jr. (S41RL)			

APPENDIX B

MLRS/TGW PROGRAM
CONTRACTOR SECURITY OFFICES

UNITED STATES	UNITED KINGDOM	GERMANY	FRANCE
Martin Marietta Missile Systems P.O. Box 5837 Orlando, Florida 32855 ATTN: Security Officer Telephone: (407) 356-7161 Telex Address: Martin Marietta-Security Telex: 564414 Facsimile: (407) 356-1671	THORN EMI Electronics Ltd Victoria Road Feltham, Middlesex TW13 7DZ ATTN: Security Officer-John Camp Telephone: 441 890 3600 Telex Address: THORN EMI-Security Telex: 24325	Diehl GmbH & Co. Fischbachstrasse 16 8505 Roethenbach/Pegnitz Federal Republic of Germany ATTN: Security Officer - W. Hinkelmann/W. Sosic/Hr. Thierauf Telephone: 49 911 509 2643 Telex Address: Diehl-Security Telex: 622 591-0	Thomson Brandt Armements 45240 LaFerte-St. Aubin ATTN: Security Officer Telephone: Security Officer-Mr. Barot 38.51.65.86. Program Security-Mr. Perrin 38.51.63.53. Telex Address: Telex: ESBRANT 780375F
MDTT, Inc. 7200 Lake Ellenor Drive Suite 220 Orlando, Florida 32809 Telephone: (407) 850-5700 Telex Address: MDTT-Security Telex: 564414 Facsimile: (407) 851-8128			Thomson-CSF Division RCM-Malakof ATTN: Security Manager-Mr. De la Goutte Telephone: 33.1.465.544.22 Telex Address: X-3413 Telex: TCSF 204780F
TRW Electronics System Group Military Electronics Div. One Space Park Redondo Beach, CA 90278 ATTN: Security Officer Telephone: (213) 535-3115 Telex Address: Security Officer Telex: 674476			

APPENDIX C

DEFINITIONS

***** TO BE ADDED *****

Central Office of Record (COR)) -

Contractor Courier -

Designated Security Authority (DSA) -

Memorandum of Understanding (MOU) -

National Program Office (NPO) -

National Security Authority (NSA) -

Security Assurance -

User Agencies -

9-X38-1032U-1

ATTACHMENT 2

Point Paper--International Participation in LHX Program

POINT PAPER

INTERNATIONAL PARTICIPATION IN LHX PROGRAM

OVERVIEW OF CLIMATE FOR IACP

FAVORABLE CLIMATE FOR COOPERATION WITH ALLIES ON POLICY LEVEL.

TWO MODES OF PARTICIPATION AVAILABLE:

AS SUBCONTRACTORS/TEAM MEMBERS/PARTICIPANTS IN U.S. PROGRAMS (THE PRESENT STATUS IN LHX)

UNDER FORMAL INTERNATIONAL COOPERATIVE PROGRAMS

PROS AND CONS OF FORMAL PROGRAM

PROS:

FOREIGN CONTRIBUTION TO FUNDING

POTENTIALLY GREATER ACCESS TO SENSITIVE/ADVANCED FOREIGN TECHNOLOGIES

POTENTIALLY MORE EXPEDITIOUS PROCESSING OF CASES IF CONTRACTORS CAN CITE FORMAL MOU

FOREIGN COMMITMENT TO PROCUREMENT OF PRODUCTION ITEMS

CONS:

TIME--COMMON REQUIREMENTS AND AND MOU MUST BE NEGOTIATED

PROGRAM SUSCEPTIBILITY TO BUDGET PERTURBATIONS MULTIPLIED BY NUMBER OF PARTICIPATING GOVERNMENTS

NEGOTIATION AND ACCOUNTING OF WORK SHARE BECOMES MAJOR EFFORT

KEY QUESTIONS ARE:

IS FOREIGN FUNDING ESSENTIAL IN R&D PHASE?

ARE FOREIGN PURCHASES ESSENTIAL TO MEETING PRODUCTION UNIT COST GOALS?

WILL INFORMAL INDUSTRY TEAMING RESULT IN ADEQUATE ECONOMIC INCENTIVE FOR FOREIGN PURCHASES?

REGARDLESS OF HOW FOREIGN INDUSTRY PARTICIPATES, THE MAJORITY OF TRANSACTIONS WILL BE INDUSTRY-TO-INDUSTRY UNDER DEPARTMENT OF STATE, OFFICE OF MUNITIONS CONTROL. REGARDLESS OF APPROACH, DELAYS IN THE LICENSING PROCESS ARE LIKELY TO BE ENCOUNTERED. DAMI-CIT, AMC, AND THE PM HAVE, HOWEVER, INITIATED A NUMBER OF ACTIONS THAT WILL HELP TO REMOVE DELAY AND UNCERTAINTY FROM INTERATIONAL PARTICIPATION IN THE LHX PROGRAM.

OVERVIEW OF ARMY'S APPROACH TO RESOLVING PROBLEMS AND EXPEDITING IACP EFFORTS

PROACTIVE DEVELOPMENT OF FORMAL EXPORT AND TECHNOLOGY TRANSFER GUIDELINES AND DISCLOSURE GUIDANCE.

TECHNOLOGY SECURITY RISK ASSESSMENT

FOREIGN DISCLOSURE PLAN WEAPON SYSTEM TECHNICAL ASSESSMENT

DELEGATION OF DISCLOSURE AUTHORITY INFORMAL

PROGRAM TO INFORM/EDUCATE EXPORT LICENSING REVIEW COMMUNITY

EFFORTS UNDERWAY TO ESTABLISH DOD/USG-WIDE "STREAMLINING" PROCEDURES; PROGRAM TO PROVIDE NEEDED INFORMATION AND SUPPORT TO LHX CONTRACTORS PLANNED

WHITE PAPER PREPARED OUTLINING GENERAL SITUATION

BRIEFINGS PLANNED TO INFORM/EDUCATE CONTRACTORS ON:

SPECIFIC AREAS OF TECHNOLOGY THAT ARE OF CONCERN TO DOD/USG

CONDITIONS THAT SHOULD BE MET FOR TRANSFER OF TECHNOLOGIES IN THESE (AND LESS SENSITIVE) AREAS

DOCUMENTATION NEEDED WITH APPLICATION TO ASSIST/EXPEDITE CASE REVIEW PROCESS (HOW TO GUIDELINES)

MECHANISMS FOR OBTAINING INFORMAL GUIDANCE AND ASSISTANCE FROM PM IN EARLY PLANNING PHASE OF A TEAMING/SUBCONTRACTING NEGOTIATION

MECHANISMS FOR INDUSTRY TEAM INPUTS TO FORMULATION/REVISION OF FUTURE GUIDELINES

SCHEDULE OF MEETINGS:

BOEING/SIKORSKY TEAM—NOVEMBER 29, 1989, AT PHILADELPHIA

MDAC/BELL TEAM—NOVEMBER 30, 1989, AT PHOENIX

LHTEC—NOVEMBER 30, 1989, AT PHOENIX

OCF File

International Participation in LHX

1.0 Purpose and Scope

The following paper discusses potential international participation in the U.S. Army's Light Helicopter, Experimental (LHX) program. It discusses present plans for foreign involvement in the development, as well as the potential for formal international cooperation in LHX. The mechanisms for foreign involvement, and the DOD/DA requirements and procedures for implementing foreign involvement in the present U.S. program, as well as in a possible future international program are also presented and discussed.

2.0 Present Status

A. The LHX is presently a U.S. development program, in which foreign participation is officially encouraged. The U.K. has expressed some interest in the LHX program. A number of foreign concerns are expected to participate as subcontractors to the two U.S. development teams. However, at present no foreign government has committed to a jointly-funded codevelopment effort. Foreign involvement in subcontracting roles can, however, still provide several benefits:

1. Access to foreign technologies, and potential cost savings due to an increased competitive base;

2. Potential interest from foreign allies in future purchases of LHX, with attendant benefits in reduced unit cost, and enhanced interoperability and standardization.

B. The program office (PM-LHX) has drafted a Weapons Systems Technical Assessment (WSTA) and Technology Security Risk Assessment (TSRA) and Foreign Disclosure Plan (FDP) to guide foreign release of materiel and technical data. The WSTA and FDP identify specific areas to technology for which special protective measures are needed, and specify requirements and conditions for their release. These documents have been staffed through, and approved, by DA and OSD. Their recommendations have been implemented in detailed disclosure guidance provided by DA to the program office. These guidelines provide a stable and consistent basis for international involvement in LHX.

C. PH-LHX is delegated authority for release of classified and sensitive materiel and defense technical information. Release of information will be phased to be in consonance with the projected milestones of the contract, as follows, and as illustrated in figure 1:

1. During the Pre-Bid/Pre-Award Phase, the U.S. Army will be responsible for release of Classified and sensitive information, via appropriate government-to-government procedures for transfers of information to properly cleared and authorized foreign industrial activities.

2. Transfer of FOREGROUND information will be the responsibility of the contractors, under the licensing provisions of the International traffic in Arms Regulations, administered by Department of State, Office of Munitions Control (OMC). Figure 2 illustrates the review procedure involved in this process.

Figure 1. Release Responsibilties

Pre-Bid/Pre-Award Phase

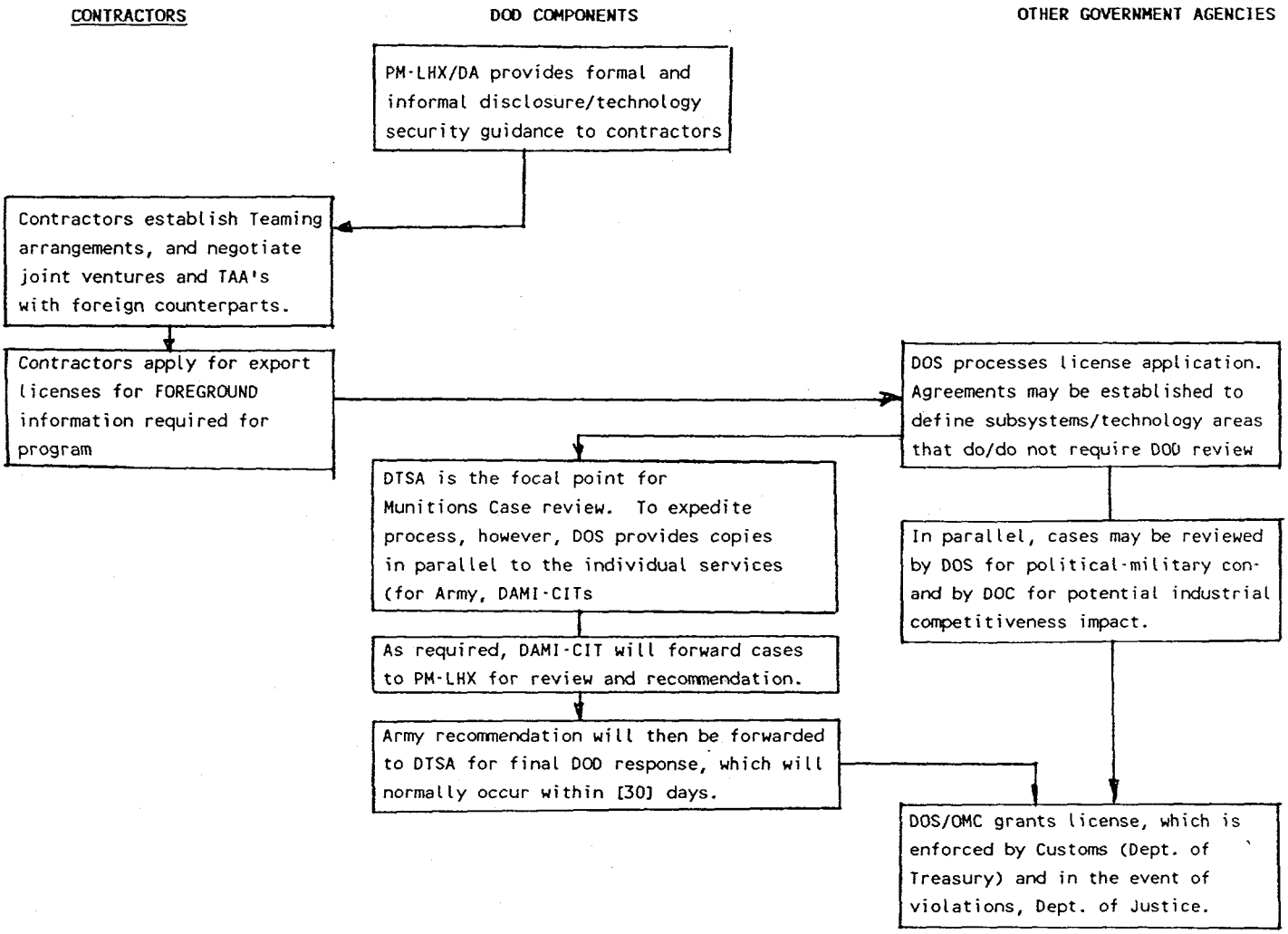
	Release Authority	Mechanism
BACKGROUND Information (Identified in FDP)	PM-LHX	Government-to-Government Transfer Foreign government is responsible for transfer to foreign industry.
ALL PHASES		
FOREGROUND Information Guidelines provided in FDP, expanded in WSTA	DOS/OMC	Munitions License Company-to-Company exports of data, Technical Assistance Agreements, or other commercial arrangements

D. The Munitions licensing process (See figure 2) involves a number of participants in different roles. Appropriate guidance, prepared by PM-LHX and DA, will be disseminated to U.S. prime contractors, and to the various DOD and other government agencies responsible for review, approval, or enforcement of munitions licences. In addition, the PM will provide prescreening of any proposed teaming arrangement or transfer that might involve export of more sensitive advanced technologies. These steps will further ensure a stable environment for both U.S. and foreign industry participants.

3.0 Potential International Cooperation

A. There are ample opportunities for a formal international program. The technology base for helicopters in the class of LHX is by-and-large a resource shared with our NATO allies. In addition, our allies have identified requirements for advanced attack helicopters that LHX could fill. The draft WSTA developed by PM-LHX indicates that, with the exception of a few very narrow

Figure 2. Munitions License Review Process



areas of concern--i.e., VHSIC production processes, low observables, EOTADS/PNVS, certain algorithms embodying sensitive threat data or operating characteristics, and certain aspects of aircraft survivability,--all other aspects of the LHX are appropriate for international participation. (In addition to these, PM-LHX has encountered some reluctance within OSD to allow international participation in the jet engine area. The level of technology involved in the basic version of the T-800 engine is available within NATO, and DA is addressing this issue separately at present.)

B. DA experience with other international programs such as the Autonomous Precision Guided Munition (APGM) and Multiple Launch Rocket System/Terminally Guided Warhead (MLRS/TGW) indicates that a lengthy negotiating process will be required to reach accord on any international cooperative effort. Once an MOU has been negotiated, the prime contractors will face a complex task to develop teaming arrangements that meet the work-sharing requirements of the MOU. International program offices with special security procedures and facilities will also be required. The PM-LHX's intent, therefore, is to pursue efforts towards establishing LHX as a formal international arms cooperative program in parallel with the currently planned Demonstration/Validation phase. It is anticipated that encouraging foreign participation in the U.S. program, will lay the groundwork for this effort.

C. OUSD,P, with DAMI-CIT as the lead service agent, is in the process of updating and revising requirements and procedures for entering into international program agreements. The LHX program, although not formally an international program, was one of the primary models from which these new procedures were derived. The WSTA, FDP and disclosure guidance cited above, when augmented by a hostile intelligence threat assessment and an Industrial Base Factors Analysis, will meet all identified requirements for negotiating international program MOUs.

D. Under present regulations and procedures, the presence or absence of an MOU will not significantly affect the process for transferring foreground information. In either case, the vast majority of transfers can be expected to occur on a company-to-company basis, under the export licensing procedures shown in figure 2. As noted previously the available guidance should provide a sound and consistent basis for expediting the licensing process. (NOTE: OUSD,P is currently pursuing the possibility of establishing procedures whereby certain exceptions to ITAR licensing requirements might be granted for international programs under approved MOU's. However, these procedures are not currently in place. Should such procedures be instituted in the future, however, the existing guidelines will be adequate to establish the bounds for exceptions.)

9-X38-1032U-1

ATTACHMENT 3

An Industry Briefing Paper for the LH Program

US ARMY
AVIATION
SYSTEMS COMMAND

INTERNATIONAL PARTICIPATION IN LHX

LHX

US ARMY
AVIATION
SYSTEMS COMMAND

BRIEFING OVERVIEW

CLIMATE FOR INTERNATIONAL PARTICIPATION

MODES OF INTERNATIONAL PARTICIPATION

ARMY ROLE AND ACTIVITIES TO HELP U.S. CONTRACTORS IN PLANNING AND IMPLEMENTING INTERNATIONAL PARTICIPATION

TECHNOLOGY TRANSFER ISSUES AND AREAS OF CONCERN

PRACTICAL STEPS FOR INTERNATIONAL PARTICIPATION

LHX

US ARMY
AVIATION
SYSTEMS COMMAND

CLIMATE

OVERALL FAVORABLE CLIMATE FOR INTERNATIONAL PARTICIPATION

FOREIGN PARTICIPATION IN LHX ENCOURAGED BY PROGRAM OFFICE

INTERNATIONAL ARMS COOPERATIVE PROGRAMS ARE A NATIONAL PRIORITY

However, implementation will continue to require concentrated effort and attention to detail.

US ARMY
AVIATION
SYSTEMS COMMAND

MODES OF PARTICIPATION

AS SUBCONTRACTORS, TEAM MEMBERS, OR SUPPLIERS ON EXISTING U.S. PROGRAM

AS PARTICIPANTS IN A FORMAL INTERNATIONAL ARMS COOPERATIVE PROGRAM (IACP) UNDER A FORMAL GOVERNMENT-TO-GOVERNMENT MOU

LHX

US ARMY
AVIATION
SYSTEMS COMMAND

ARMY'S ROLE AND STATUS

DEVELOP AND DISSEMINATE POLICY GUIDANCE

EFFECT TRANSFERS OF BACKGROUND AND CLASSIFIED TECHNICAL DATA

INFORMAL CASE-BY-CASE ADVICE ON T^2 AND EXPORT CONTROL MATTERS

EXPEDITE CASE PROCESSING REVIEW AND DISPOSITION

LHX

US ARMY
AVIATION
SYSTEMS COMMAND

STATUS OF POLICY GUIDANCE

WEAPON SYSTEM TECHNICAL ASSESSMENT DRAFT COMPLETED, INCORPORATING INPUTS FROM INDUSTRY TEAMS

FOREIGN DISCLOSURE PLAN APPROVED

DELEGATION OF DISCLOSURE AUTHORITY LETTER HAS BEEN ISSUED BY DEPARTMENT OF ARMY TO PM-LHX

LHX

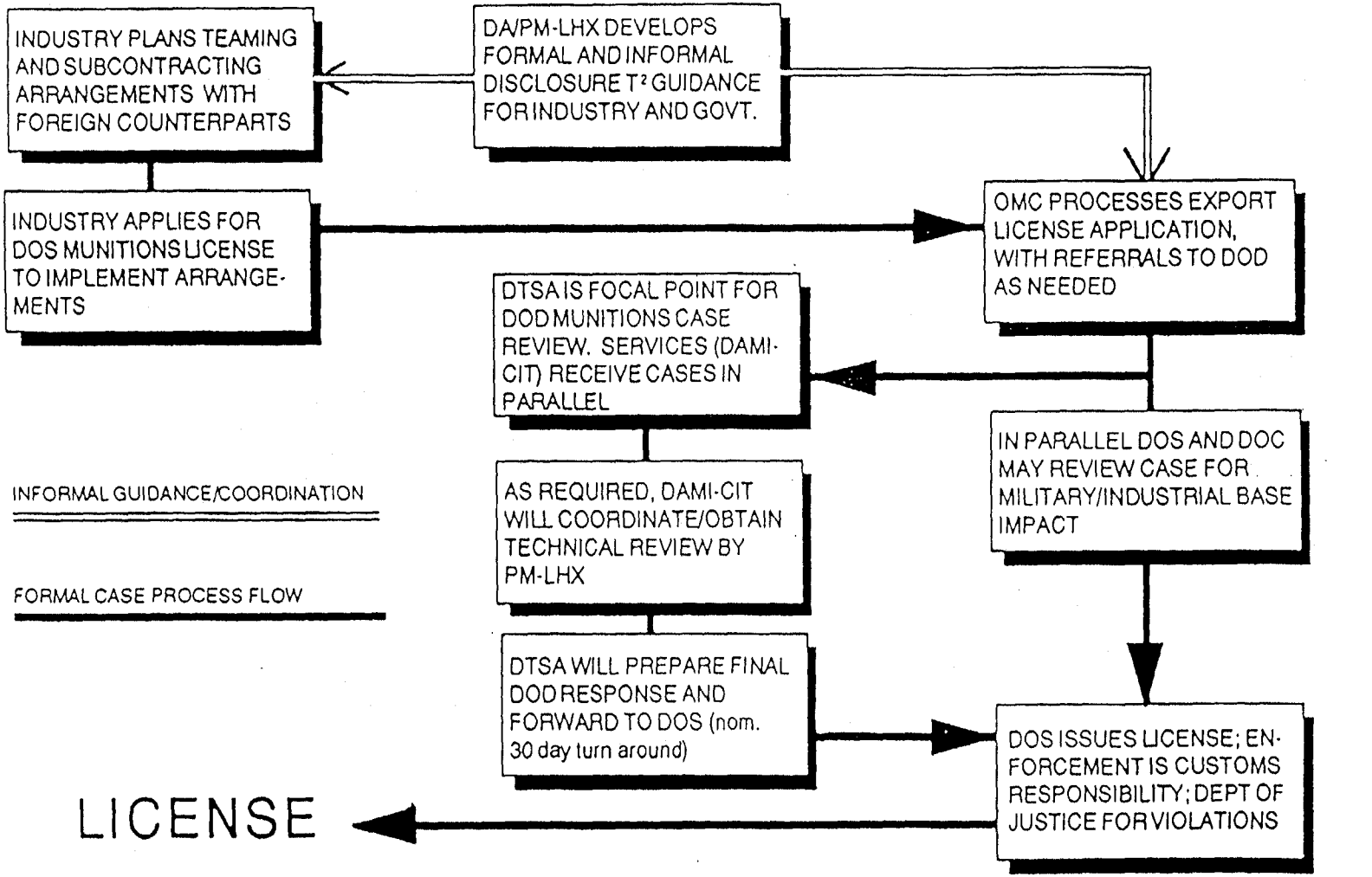
US ARMY
AVIATION
SYSTEMS COMMAND

RELEASE RESPONSIBILITIES

	RELEASE AUTHORITY	TRANSFER MECHANISM
PRE-BID/PRE-AWARD BACKGROUND INFORMATION (identified in Foreign Disclosure Plan)	PM-LHX	GOVT-TO-GOVT TRANSFER. FOREIGN GOVERNMENT IS RESPONSIBLE FOR TRANSFER TO FOREIGN INDUSTRY.
DURING ALL PHASES FOREGROUND INFORMATION (categories of concern defined in Foreign Disclosure Plan)	DOS/OMC	MUNITIONS LICENSE FOR COMPANY-TO-COMPANY EXPORTS OF DATA, TECHNICAL ASSISTANCE, OR OTHER COMMERCIAL ARRANGEMENTS (e.g., consulting, licensing of patent rights, etc.)

US ARMY AVIATION SYSTEMS COMMAND

MUNITIONS LICENSE OVERVIEW



LHX

US ARMY
AVIATION
SYSTEMS COMMAND

OTHER ARMY INITIATIVES

INDUSTRY BRIEFINGS

INFORMAL PROGRAM TO OBTAIN ADVANCE ACCEPTANCE AND UNDERSTANDING OF ARMY POSITION THROUGHOUT DOD/USG EXPORT LICENSING COMMUNITY

LONGER TERM INITIATIVES UNDERWAY TO ESTABLISH DOD/GOVERNMENT-WIDE "STREAMLINING " PROCEDURES

US ARMY
AVIATION
SYSTEMS COMMAND

INDUSTRY BRIEFINGS--OBJECTIVES

IDENTIFY TO INDUSTRY TECHNOLOGIES OF CONCERN TO DOD/USG

PROVIDE SPECIFIC GUIDANCE REGARDING CONDITIONS FOR T^2 THESE AND OTHER MILITARILY CRITICAL TECHNOLOGIES

IDENTIFY DOCUMENTATION NEEDED TO ASSIST/EXPEDITE THE GOVERNMENT'S CASE REVIEW (PRACTICAL NUTS AND BOLTS OF LICENSE APPLICATIONS)

ESTABLISH AND INFORM INDUSTRY OF MECHANISMS FOR

- OBTAINING INFORMAL GUIDANCE DURING EARLY PLANNING PHASES OF TEAMING/SUBCONTRACTING NEGOTIATIONS

- PARTICIPATING IN FUTURE REVISIONS OF TECHNOLOGY SECURITY GUIDELINES

LHX

US ARMY
AVIATION
SYSTEMS COMMAND

SENSITIVE TECHNOLOGIES/ISSUES

LOW OBSERVABLES (STEALTH)

VHSIC/MMIC

INEWS

EOTADS/NVPS

JET ENGINE HOT SECTION

PLUS A GENERAL CONCERN REGARDING EMBEDDED SOFTWARE OR TECHNICAL DATA REVEALING INHERENT SYSTEM LIMITATIONS OF CHARACTERISTICS THAT AN ADVERSARY MIGHT EXPLOIT TO DEVELOP COUNTERMEASURES, for example:

AIRCRAFT SURVIVABILITY EQUIPMENT (ASE)

COMSEC

LHX

US ARMY
AVIATION
SYSTEMS COMMAND

CONDITIONS FOR RELEASE OF CRITICAL TECHNOLOGY

THE ARMY WILL SUPPORT TRANSERS OF SENSITIVE CRITICAL TECHNOLOGY TO CLOSEST ALLIES IF, AND ONLY IF:

1. THERE IS A DOCUMENTED TECHNOLOGICAL QUID-PRO-QUO OF CLEAR OVERRIDING BENEFIT TO US NATIONAL SECURITY

2. THE TERMS OF THE TRANSACTION PROVIDE ADEQUATE LEGAL ASSURANCES AND/OR TECHNICAL SAVEGUARDS TO PRECLUDE DIVERSION OR COMPROMISE OF THE TECHNOLOGY.

THE ARMY WILL SUPPORT TRANSFERS OF OTHER MILITARILY CRITICAL TECHNOLOGIES TO ALLIES TO SUPPORT PROGRAM OBJECTIVES WITH ADEQUATE SAFEGUARDS AND ASSURANCES

(NOTE: BASED ON TECHNOLOGY TRANSFER CONCERNS ONLY. THERE MAY BE OTHER OVERRIDING CONSIDERATIONS RELATING TO INDUSTRIAL BASE IMPACT AND INTERNATIONAL COMPETITIVENESS, OR RELEASE OF CLASSIFIED/SENSITIVE INFORMATION)

LHX

US ARMY
AVIATION
SYSTEMS COMMAND

RISKS AND BENEFITS--EXAMPLES

RISKS

COMPROMISE OF SENSITIVE INFORMATION

LOSS OR DIVERSION OF TECHNOLOGY AFFECTING PRIMARY MISSION CAPABILITIES

UNNECESSARY EXPOSURE OF A UNIQUE U.S. CAPABILITY

POTENTIAL DIVERSION OR MISUSE OF TECHNOLOGY FOR OTHER PURPOSES

INDUSTRIAL BASE IMPACT

INTERNATIONAL COMPETITIVENESS

BENEFITS

INCREASED INTEROPERABILITY AND STANDARDIZATION

ENHANCEMENT OF SYSTEM PERFORMANCE / COST EFFECTIVENESS THROUGH ACCESS TO FOREIGN TECHNOLOGY

ENHANCEMENT OF U.S. TECHNOLOGY BASE THROUGH ACQUISITION OF FOREIGN TECHNOLOGY

GREATER QUANTITY PRODUCTION/ REDUCED UNIT COST

IN ASSESSING RISKS AND BENEFITS A FUNDAMENTAL CONSIDERATION IS THE INDIGENOUS CAPABILITY OF THE RECIPIENT AND/OR THE AVAILABILITY OF IDENTICAL OR EQUIVALENT TECHNOLOGY FROM NON-U.S. SOURCES.

LHX

ATTACHMENT 4

Usage of Commercial Microprocessors in Tactical US Army Equipment

USAGE OF COMMERCIAL MICROPROCESSORS IN TACTICAL U.S. ARMY EQUIPMENT

The Army makes extensive use of commercial microprocessors in its fielded equipment. The following is the result of a quick survey of the WSTA's and is not a comprehensive list. The uses cited do, however, indicate pervasive use.

We have listed a number of older microprocessors/families of microprocessors. These are significant in that they will almost certainly be replaced with their more advanced counterparts when as equipment is product-improved or replaced. This trend is, in fact, clear in a number of the entries.

Selected Communications Systems

AN/TRC-173/174 Radio--employs 8086 microprocessor

REGENCY NET--contains a number of 16-bit Intel 80186 microprocessors.

SINCGARS (the General Dynamics version)--presently uses Intel 80C196 microprocessors and it is anticipated that the next upgrade will involve the Intel 68000 series.

MSE--plans to replace proprietary microprocessor chips with 68030 chips in the near future.

Single Subscriber Terminal SST (UGC-144)--employs the 80386 microprocessor

Selected Electronic Warfare Systems

GUARDRAIL--contains a number of Motorola MC 68000 microprocessors

QUICKFIX--contains a number os Intel 68000 microprocessors

STINGRAY (EOCM)--employs 68020 microprocessors

TRAILBLAZER--employs a number of 68000 microprocessors and also uses the TMS 320 processing chip

Selected Sensor Systems

Short Range Thermal Sight (SRTS)--are unspecified presently but will almost certainly employ a 32-bit microprocessor, possibly in the 68000 series.

Selected Weapon Systems

M1A1--employs Motorola 68020 microprocessors

Heavy Force Modernization--will use commercial 32-bit microprocessors in its VETRONICS suite.

Longbow (APACHE)--Still in development, likely to use commercial microprocessors in radar processor and in weapons control interfaces.

LHX--Still in development, however, likely user of 32-bit systems, expecially commercial variants conforming to JAIWG or Pave Pillar architectural (VHSIC) interface standards.

Other Systems

QRMP (Non-impact printer)--uses custom IC's now but plans to replace with unspecified microprocessor in the future.

Tactical Computer Terminal (TCT)--uses the 68000 microprocessor

IFTE (Integrated Family of Test Equipment)--System will be developed around commercial microprocessors--probably that used in Sun work stations.

Joint Tactical Fusion--Uses the MicroVax II microprocessor-based PC-board computer.

In summary, we see a pattern of pervasive use and continuous upgrading of U.S. Army systems through the use of commecial microprocessors. As a general observation--radiation hardened circuits aside--the difference between a MILSPEC and a commercial circuit is often only the degree of testing. Commercial integrated circuits are inherently rugged and reliable and can, with proper screening and packaging be used with excellent results under most tactical conditions.

9-X38-1032U-1

ATTACHMENT 5

Analysis of Weapon System Technical Assessment Questionnaire

1 March 1990

Analysis of Weapon System Technical Assessment (WSTA) Questionnaire

The U.S. Army Materiel Command provided a Questionnaire to evaluate their Weapon System Technical Assessment (WSTA) program (Memorandum AMCMI-CIT (380-66) dated 5 December 1989). The Questionnaire was provided to all organizations who were on distribution for completed WSTAs or had been significantly involved in the development of a WSTA.

The attached provides an analyses of the responses received from the Questionnaire. The information is arranged as follows:

SUMMARY RESULTS OF WSTA QUESTIONNAIRE DISTRIBUTED BY AMC
Memorandum AMCMI-CIT (380-66) dated 5 December 1989

OVERALL ANALYSIS

NUMBER OF QUESTIONAIRES	65
NUMBER OF RESPONSES	38
RATE OF RESPONSE	58.46%

ANALYSIS OF USER NEED, RATE OF USE, AND IMPACT OF WSTA's

First we analyzed the types of users who responded and the functions they performed. The analysis of user need was based primarily on the number of functions designated. A very few cases (e.g., PM-CH-47) the need was assessed to be low because of the age and state of technology of the system.

LEGEND:

User Type A = DA/Command/Tech Security Specialist
B = PEO/PM
C = Field Activities/Laboratories

Use Need H = High Need
M = Moderate Need
L = Little Need
N = Negligible/No Need

Use Made Y = Yes
N = No

a, b, ..., j - Denotes organizations and functions/decisions from Item 2 of Questionnaire (see attached)

BASIC ASSESSMENT OF USER TYPE, NEED, AND FUNCTIONS PERFORMED

Organization	USER TYPE	UseNeed	UseMade	a.	b.	c.	d.	e.	f.	g.	h.	i.	j.
HQDA/DAMI-CIT	A	H	Y	X	X	X	X			X		X	
HQDA/DALO-SAA	A	H	Y	X	X	X		X				X	X
HQDA/DAPE-MRA	A	L	N									X	X
OTSG	A	N	N										
SAIS-PPT	A	L	N										
CORP OF ENGR.	C	N	N										
HQAMC-AMCDE-AQ	A	L	N										
HQAMC-AMC-PPD-P	A	N	N										
HQAMC-OICP	A	H	Y			X	X			X	X		
AMSAC-MI	A	H	Y	X	X	X		X					
HQAMC-ASAC/PPD	A	H	Y	X		X						X	X
AMC-STCEUR	C	L	Y									X	
COMAVSCOM	A	H	Y	X	X	X	X	X	X	X	X	X	
HQAMC-COM	C	M	Y								X	X	
ACRDEC, APG	C	M	Y			X		X	X	X	X	X	
CECOM AMSEL MI-I	A	H	Y	X	X		X	X	X		X	X	
MICOM-AMSMMI-SI	A	H	Y		X	X		X	X	X		X	X
TACOM-AMSTA-S	A	H	N										
PM SINCGARS	B	M	N		X			X	X	X		X	
MICOM AMCPM-PE	B	L	N										
CRDEC-SMCER-DDW	C	N	N										
PEO-AD	B	Y	N	X	X		X			X		X	
PM-STINGER	B	H	Y	X	X			X		X	X	X	X
PM-CHAPARRAL	B	L	N	X	X			X		X	X	X	
PM-CH-47M-T	B	L	N	X	X			X	X	X	X	X	
PM-SATCOM	B	M	N					X	X				
PM-HELLFIRE	B	H	N	X				X		X	X	X	
PM-CSTS	B	M	N	X	X	X		X		X	X	X	
AMC-PEO-IEW-RDR	B	H	Y	X	X			X			X	X	
AMCPM-AAH	B	M	N										

Organization	USER TYPE	UseNeed	UseMade	a.	b.	c.	d.	e.	f.	g.	h.	i.	j.	(cont'd)
AMCPEO-IEW-SW-TB	B	L	N											
AMCPEO-IEW-SW-TT	B	L	N											
AMCPEO-IEW-NVEO	B	L	N											
AMCPM-COBRA	B	M	N	X	X			X		X	X	X		
ARDEC-SMCAR	C	H	N	X			X	X		X		X		
AMCPM-MCD	B	H	N	X			X	X	X	X	X			
ARDEC-SMCAR-FSP-G	C	M	N			X		X		X	X			
ARDEC-SMCAR-FSP-G	C	M	Y	X			X	X		X	X	X	X	

The following provides a summary of the results of the questionnaire shown above.

	TOTAL NO.	NOUSERS	NEED H/M	USED	H/M IMPACT
COMMAND/TECH SECURITY SPECIALTY	14	8	9	8	7
PEO/PM	16	2	9	2	2
FIELD ACTIVITIES AND LABORATORIES	8	4	5	3	3
TOTALS	38	14	23	13	12
PERCENT OF TOTAL RESPONDENTS	100.00%	36.84%	60.53%	34.21%	31.58%
PERCENTS OF RESPONDENTS W/ H/M NEED			60.53%	56.52%	92.31%

NO WITH H/M NEED NOT USING WSTAS	10	43.48%
COMMAND/TECH SECURITY SPECIALTY	1	7.14%
PEO/PM	7	43.75%
FIELD ACTIVITIES AND LABORATORIES	2	25.00%

USER FUNCTION ANALYSIS	a.	b.	c.	d.	e.	f.	g.	h.	i.	j.	
COMMAND/SEC SPEC	6	6	7	4	5	3	4	2	7	4	
PEO/PM	9	8	1	2	10	4	9	8	9	1	
FIELD ACTIVITIES	2	2	2	2	4	1	4	4	5	1	
TOTALS	17	16	10	8	19	8	17	14	21	6	0

FREQUENCY OF USE IN PAST 3 MO.	>10	5 to 9	1 to 4	None	NO RESP
COMMAND SECTY SPEC.	3	1	4	1	5
PEO/PM ORGANIZATIONS	0	0	1	11	4
FIELD/LABORATORY	0	1	2	3	2
TOTALS	3	2	7	15	11

OF THOSE WITH NO RESPONSE 10/11 WERE ASSESSED TO HAVE LITTLE OF NO NEED FOR THE WSTA's BASED IN THE FUNCTIONS PERFORMED.

LIST OF ORGANIZATIONS INDICATING LOW/NEGLIBILE NEED FOR WSTA'S

Organization	USER	TYPE	
HQDA/DAPE-MRA	A	L	
OTSG	A	N	
SAIS-PPT	A	L	
HQAMC-AMCDE-AQ	A	L	
HQAMC-AMC-PPD-P	A	N	
MICOM AMCPM-PE	B	L	(Based on Type of System (Pershing)
PM-CHAPARRAL	B	L	(Low need based on age of system)
PM-CH-47M-T	B	L	(Low need based on age of system)
AMCPEO-IEW-SW-TB	B	L	(Based on stated functions of office)
AMCPEO-IEW-SW-TT	B	L	(Based on stated functions of office)
AMCPEO-IEW-NVEO	B	L	(Based on stated functions of office)
AMC-STCEUR	C	L	(Based on stated functions of office)
CORP OF ENGR.	C	N	
CRDEC-SMCER-DDW	C	N	(Based on stated functions of office)

The overall picture here is:

1. Only about half of the people who could benefit from using the WSTA's are using them.

2. Those who do use them find them useful (92% of users responding indicated a H/M impact).

3. The WSTA's (properly) appear to be more useful to the DA/Command/Tech Security people than to the PM's who have direct access to expert technical support and experience.

FREQUENCY OF USE/NO. OF USERS/CLARITY

LEGEND:

User Type A = DA/Command/Tech Security Specialist
B = PEO/PM
C = Field Activities/Laboratories

Freq. - Use in last 3 months as follows:

A = 10+
B = 5-9
C = 1-4
D = Not used

Overall - Overall Clarity

Y = Yes
N = No

No. Filed - No. on file at responding organization

No. User - Number of other users (other than respondent) at activity.

DES - Extent of Dispersement of WSTA's Outside of Activity

Y = Respondent indicates dispersement but did not indicate extent.
M = Respondent indicated dispersement to a few other users
W = Respondent inidcates wide distribution with and outside of activity

Organization	USER TYPE	FREQ	NO.FILED	NO.USER	DES	OVERALL
HQDA/DAMI-CIT	A	A	30			Y
HQDA/DALO-SAA	A	C	30	3		Y
HQDA/DAPE-MRA	A					
OTSG	A					
SAIS-PPT	A					
CORP OF ENGR.	C					
HQAMC-AMCDE-AQ	A					
HQAMC-AMC-PPD-P	A					
HQAMC-OICP	A	C	20	1		Y
AMSAC-MI	A	A	36	7		Y
HQAMC-ASAC/PPD	A	A	25	3		
AMC-STCEUR	C	D	8	8		
COMAVSCOM	A	C	4	2		Y
HQAMC-COM	C	C	NS	0	Y	Y
ACRDEC, APG	C	B				Y
CECOM AMSEL MI-I	A	B	30	5	W	Y
MICOM-AMSMMI-SI	A	C	8	4	W	Y
TACOM-AMSTA-S	A	D	1	0	Y	N
PM SINCGARS	B	D	1	0		Y
MICOM AMCPM-PE	B	D	2	0		Y
CRDEC-SMCER-DDW	C					
PEO-AD	B	D	0			
PM-STINGER	B	C	2	3	M	Y
PM-CHAPARRAL	B	D	1	0	Y	
PM-CH-47M-T	B	D	1	0		
PM-SATCOM	B	D				
PM-HELLFIRE	B	D				
PM-CSTS	B	D				
AMC-PEO-IEW-RDR	B	D	2	1	Y	Y
AMCPM-AAH	B					
AMCPEO-IEW-SW-TB	B					
AMCPEO-IEW-SW-TT	B					

Organization	USER TYPE	FREQ	NO.FILED	NO.USER	DES	OVERALL (cont'd)
AMCPEO-IEW-NVEO	B					
AMCPM-COBRA	B	D	1	3		
ARDEC-SMCAR	C	D	1		W	Y
AMCPM-MCD	B	D	NS			
ARDEC-SMCAR-FSP-G	C	D	NS			
ARDEC-SMCAR-FSP-G	C	C	1	5		Y

The following provides a summary of these statistics:

NUMBER OF WSTA's ON FILE

TWENTY OR MORE	6
TEN-TO-NINETEEN	0
FIVE-TO-NINE	2
ONE-TO-FOUR	13
NO RESPONSE	17

AVG. OF RESPONDENTS 10.20

AVG NUMBER OF USERS INDICATED = 2.5

Dissemination outside of activity= 8/36

SECTION-BY-SECTION ANALYSIS

The following provides a detailed section-by-section break-out of how respondents rated various aspects of the WSTA's.

LEGEND:

X.U - Usefulness

A = Most Useful
B = Somewhat Useful
C = Seldom Used

X.C - Clarity (Generally Clear)

Y = Yes
N = No

X.D - Detail

M = Too Much
R = Right
L = Too Little

("X" denotes Section)

Organization	ESU	ESC	ESD	I.U	I.C	I.D	II.U	II.C	II.D	IIIA.U	IIIA.C	IIIA.D	IIIB.U	IIIB.C	IIIB.D	IV.U	IV.C	IV.D	V.U	V.C	V.D	HOISU	HOISC	HOISD
HQDA/DAMI-CIT	A	Y			Y					B			B			C	N		C	N		B	N	
HQDA/DALO-SAA	A	Y	R	A	Y	R	B	Y	R	A			B	Y	R	A	Y	R	A	Y	R	B	Y	R
HQDA/DAPE-MRA																								
OTSG																								
SAIS-PPT																								
CORP OF ENGR.																								
HQAMC-AMCDE-AQ																								
HQAMC-AMC-PPD-P																								
HQAMC-OICP	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	B	Y	R	B	Y	R
AMSAC-MI	B	Y	R	B	Y	R	C	Y	L	A	Y	R	A	Y	L	B	N	L	C	Y	R	C	N	L
HQAMC-ASAC/PPD				A			A			A			A			A			A			A		
AMC-STCEUR	B	Y	R	B	Y	R	B	Y	R	B	Y	R	B	Y	R	B	Y	R	B	Y	R	B	Y	R
COMAVSCOM	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R
HQAMC-COM	A	Y	R	B	Y	R	B	Y	R	C	Y	R	C	Y	R	A	Y	R	C	Y	R	C	Y	R
ACRDEC, APG				A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	L
CECOM AMSEL MI-I	C	Y	R	C	S	R	B	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R
MICOM-AMSMMI-SI	A			A			A			A			A			A			A			A		

Organization	ESU	ESC	ESD	I.U	I.C	I.D	II.U	II.C	II.D	IIIA.U	IIIA.C	IIIA.D	IIIB.U	IIIB.C	IIIB.D	IV.U	IV.C	IV.D	V.U	V.C	V.D	HOISU	HOISC	HOISD
TACOM-AMSTA-S	C	Y	Y	B	C	M	C	N	M	B	Y	R	B	Y	R	C	N	M	C	N	M			
PM SINCGARS	A	Y	R	A	S	R	B	Y	R	B	Y	R	B	Y	R	B	Y	R	B	Y	R	B	Y	R
MICOM AMCPM-PE	C	Y	R	C	Y	R	C	Y	R	C	Y	R	B	Y	R	C	Y	R	C	Y	R	C	Y	R
CRDEC-SMCER-DDW																								
PEO-AD																								
PM-STINGER	B	Y	R	B	Y	R	B	Y	L	A	Y	R	A	Y	R	B	Y	R	B	Y	L	B	Y	R
PM-CHAPARRAL																								
PM-CH-47M-T																								
PM-SATCOM																								
PM-HELLFIRE																								
PM-CSTS																								
AMC-PEO-IEW-RDR	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R	A	Y	R
AMCPM-AAH																								
AMCPEO-IEW-SW-TB																								
AMCPEO-IEW-SW-TT																								
AMCPEO-IEW-NVEO																								
AMCPM-COBRA																								
ARDEC-SMCAR																								
AMCPM-MCD																								
ARDEC-SMCAR-FSP-G																								
ARDEC-SMCAR-FSP-G	C		R	C		R	A	Y	R	C	Y		C	Y		A	Y	R	B	Y	R			

The overall result shows that the hierarchical structure of the WSTA's is functioning as designed, in that different users make greater or less use of different parts of the WSTA's, overall respondents felt that the WSTA's were clear and about the proper level.

RECOMMENDATIONS AND SUGGESTIONS

Suggestions for improvement/modification requested by:

HQDA/DAMI-CIT - A meaningful Intelligence Assessment that states the consequense of compromise.

HQDA/DAPE-MRA - Comparison with predecessor system; coordinate release with major decision point (M/S II)

AMSAC-MI - Include summary of fielding plan to Allies and Friendly Foreign Countries.

MICOM-AMSMI-SI - Make more readable; less technical in nature, write for broad, varied audience.

MICOM AMCPM-PE - INF Treaty complicance would limit any changes or suggestions to the PII WSTA.

PM-STINGER - Provide a technology matchup between US and foreign systems, and include more complete characteristics of foreign capabilities.

WEAPON SYSTEM TECHNICAL ASSESSMENT (WSTA)
USER QUESTIONNAIRE

PURPOSE: WSTAs are required by Department of Army Regulation (AR) 70-1 as part of the documentation for major milestones. They are also used to support technology transfer decision-making for a wide range of activities involving public or foreign release of U.S. Army and material, including security assistance, FMS, munitions case processing, exceptions to National Disclosure Policy, etc. The information requested below will increase our understanding of how the WSTAs are being used, and help us to make them better satisfy the user's needs.

NAME:	**DATE:**
ORGANIZATION AND ADDRESS:	**PHONE:** Commercial: AUTOVON:

1. Do you or your organization use the WSTAs? Yes ☐ No ☐

(If you do **NOT** use the WSTAs indicate if you or your organization perform any of the functions listed in 2. a.through j. below, and complete questions 8, 9, 10, and 17.)

2. For what functions/decisions do you use the WSTAs? (Check all that apply)

☐ a. Security Assistance/FMS programs	☐ b. Export License Case Processing
☐ c. National Disclosure Policy Exceptions	☐ d. International Arms Cooperative Program (IACP)
☐ e. Release of Army Technical Data Packages	☐ f. Foreign Participation in U.S. Procurements
☐ g. Foreign Visits	☐ h. Public Release of Technical Papers and Information
☐ i. General Technical Information	

☐ j. Other (Please specify)

3. How many times have you referred to WSTAs during the past three months?

☐ Ten times or more. ☐ Five-to-nine times. ☐ One-to-four times. ☐ Not used in last 3 months.

4. Approximately how many WSTAs do you have on file or available to you?	**5. Approximately how many other people in your immediate office use the WSTAs?**
6. Please list any WSTAs that have been particularly useful.	**7. List any other systems or programs for which you would like to see a WSTA.**

8. Who else in your organization uses the WSTAs?

Name: Office Symbol: Phone:

9. Who else should be added to the WSTA distribution (either within or outside your organization)?

Name: Office Symbol: Phone:

10. Do you provide the WSTA, or any extracted information as guidance to any other activities (e.g., to supporting laboratories, contractors, to assist them in developing foreign subcontracting or cooperative R&D efforts?) Please identify activities and purpose.

For those who use the WSTAs, the following questions solicit your evaluation and suggestions as to how well the WSTAs are meeting your specific needs. Offer any comments or criticisms. We understand that not all sections will be equally useful to every organization. If you find the space provided is insufficient, or if you have specific examples of things you would like to see incorporated, please add attachments. Our primary purpose is to make the WSTA process as useful as possible to the greatest number of users.

11. Is the overall WSTA format reasonably clear and easy to follow? Yes ☐ No ☐
How might it be improved?

12. Please give us your assessment of the information contained in the different elements of the WSTA as follows.

	This part of the WSTA is			The presentation is generally		The level of detail is		
	Most Useful	Somewhat Useful	Seldom Used	Clear	Confusing	Too Much	About Right	Too Little
EXECUTIVE SUMMARY								
I. System Description								
II. Weapon System Comparison with Foreign Capability								
III. Transfer Guidelines								
General Guidelines								
Specific Guidelines								
IV. Controlled Technologies (Notes and Tables)								
V. Critical Technologies Lead-Times (Charts)								
APPENDIX Intelligence Assessment								

13. Are the graphics, charts and tables an effective and useful supplement to the text?

	YES/NO	REMARKS
EXECUTIVE SUMMARY (e.g., summary guidelines, system photos)		
I. System Description (photos, block diagrams, charts)		
IV. Critical Technologies Notes and Tables		
V. Critical Technologies Lead-Time Charts		

Can you suggest any other graphics or charts that would enhance the presentation and use of information in the WSTA?

14. What other changes can you suggest to make the WSTAs more useful?

15. Please describe any savings in cost, time, or resources realized by your organization through use of the WSTAs

16. If production and/or distribution of the WSTAs to you organization stops, will it make your job more difficult?

☐ Yes ☐ No Comments

17. The Army point of contact for WSTA development and this questionnaire is Headquarters Army Materiel Command, ATTN: AMCMI-CT, Mr. Ron Vallmaki or Ms. Melodie Campbell, (202) 274-7016 or AUTOVON 284-7016. Would you like a follow-up telephone call from us regarding the WSTAs or this questionnaire? Yes ☐ No ☐

9-X38-1032U-1

ATTACHMENT 6

Guidelines for Preparing Munitions License Applications

Guidelines for Preparing Munitions License Applications

1. INTRODUCTION

Department of Defense's stated policy is to manage militarily critical technology as a national resource, to be invested in the enhancement of the capabilities of our allies and protected from exploitation that might be detrimental to our national security. For most transactions involving UNCLASSIFIED U.S. Army material and technology (including technical data in all forms), the basic control mechanism for implementing this policy is the Department of State Munitions License.

Increasingly, the U.S. is looking to foreign participation to help defray the growing costs of military systems development and acquisition. Whether this participation occurs pursuant to a formal MOU program or through allied industrial participation in commercial arrangements, both industry and government benefit when the munitions licensing process proceeds efficiently and with as little uncertainty as possible.

While the following guidelines reflect the approach developed for the Army's Light Helicopter (Experimental) LHX program, they can also be applied beneficially to other programs.

2. FUNDAMENTALS

The recommended guidelines focus on two fundamental elements of the technology security/export licensing process.

> Ensuring that proposed transfers of material and technology are, in fact, appropriate and beneficial to U.S. national security; and that US Army concerns are adequately addressed prior to the submission of the license and;
>
> That the application contains the information the government needs to verify these facts and process the case without undue delay.

NOTE

The suggested guidelines are designed to complement and support the formal Department of State Licensing process. They should not be construed as adding to, eliminating, or reducing any requirements of federal laws or regulations. Moreover, the guidelines are not intended to be universally applied to all licenses. Many exports involving more mundane and less sensitive material and technology will not require such detailed prescreening and documentation. Finally, all involved should recognize that there will be, for any program, a period of learning. As the program evolves and precedents become established, both industry and government will become more effective in evaluating technology security concerns and the level of documentation needed to resolve those concerns.

2.1 Dealing Effectively With National Security Concerns.

It is too late to address information and technology security concerns in the export licensing process. Questions of what information can be disclosed, and under what conditions, should be considered **before** serious discussions with potential foreign participants. Basic concerns derive from one of three closely related issues:

Military Capability--Does the material or technology pose a direct threat to U.S. forces, and do we have adequate defenses against the projected threat;

Compromise of Sensitive Information--Will access to the material or technology reveal (either directly, through operational use and evaluation, or reverse engineering):

> inherent systems weakness from which countermeasures to defeat or minimize the systems effectiveness could be developed; or
>
> U.S. intelligence information, sources, or methods?

Technology Transfer--Could the technological capabilities transferred be applied and exploited by another country either to replicate the system or extend their capabilities to design, produce, or operate another military system that would be detrimental to U.S. national security?

The first two concerns are dealt with primarily by classification and National Disclosure Policy. There will be, however, cases where transfers of UNCLASSIFIED hardware, software, or technical data can reveal systems performance limitations or vulnerabilities. In these cases the contractors ensure that the sensitive information is either not transferred or, if transferred, that acceptable security measures are implemented.

Most militarily critical technologies (as defined in the Omnibus Trade and Competetiveness Act of 1988, and listed in the DOD Militarily Critical Technologies List (MCTL)) can--with proper protective measures--be shared with our allies. Where the U.S. enjoys a significant technological lead in an area that enables or enhances an important U.S. operational advantage, technology transfer will generally be permitted only to closest allies to attain a specific **technological** quid-pro-quo of benefit to the U.S.

To assist both government and industry in evaluating proposed exports, a **Technology Security Risk Assessment** (or Weapons Systems Technical Assessment (WSTA)) for the LHX, identifying militarily critical technologies and areas of specific concern has been prepared. This evaluation, in which the Program Office and LHX contractors participated, formed the basis of the **Foreign Disclosure Plan** (FDP). The FDP provides disclosure guidance and specifies what information will be allowed for transfer during different phases of the program.

In addition to the formal guidance provided in these documents, U.S. Contractors can obtain informal assistance on specific export control and technology security matters through Aviation Systems Command, PM-LHX. This assistance can take a variety of forms, ranging from very informal advisory opinions on the general suitability of a particular transfer during early planning to pre-screening of specific export license applications against established foreign disclosure and technology transfer policies.

2.2 Structuring the Transaction.

In the vast majority of cases problems can be avoided and the essential objectives of the government and industry met with a little care and foresight in negotiating and structuring a sale, manufacturing license agreement (MLA), technical assistance agreement (TAA), joint venture, subcontract, etc. When considering transfers of sensitive information or militarily critical technologies, limit the scope of the exchange to what is necessary to achieve specific program objectives. Clearly define technical limits, limits on licensing of third country transfers and sales, and security measures employed to limit retransfer or diversion. From the case processors' perspective, the more specific the agreement, the easier it will be to process in a timely manner.

Common pitfalls to avoid in structuring the transaction include:

Transfer of critical technology in excess of that required for the program (for example, transfer of an empirically validated CAD/CAM database when build-to drawings and/or specific process control specifications would have been sufficient to allow the recipient to develop or produce an item;)

Premature transfer of critical technology (e.g., transfer of manufacturing process data for serial production during an early development phase before a requirement for the technology has been established;)

Unnecessary release of sensitive software in source code format when object code form will serve as well;

Release of critical manufacturing process data to participants who are not viable candidates to produce the end-items in question. (In these cases, transfers of the end items as finished, tested assemblies is preferred.)

The most careful coordination and attention to technology security can be wasted if the license application is poorly prepared. It is not enough to do the homework. The license application must satisfy the reviewers that it has been done and done adequately. The rest of this paper suggests specific steps for preparing a license application to meet this requirement.

3. PREPARING THE APPLICATION

An effective license application will have three primary elements, as illustrated and summarized on page 3. These are as follows:

The Cover Letter summarizing all of the information that the case processor needs to evaluate the case;

The Application (DSP-5) Form which is the legal instrument for munitions case licensing; and

Supporting Information as necessary to permit the reviewer to verify the statements made in the cover letter and application.

It is essential that these three items be organized as a package to present a complete, accurate and consistent picture and to allow the reviewer to access information in a systematic way. The following sections discuss the organization of each of these elements of the application in greater detail.

Again, these guidelines apply primarily to proposed exports involving material or technology identified in the FDP as containing militarily critical technology and/or sensitive UNCLASSIFIED defense technical information. Routine transfers not involving critical technology transfer will not need this level of documentation.

3.1 The Cover Letter

A properly written cover letter is the most important means a contractor possesses to ensure timely processing of an export license request. While the level of detail and content will be tailored to a specific export, the cover letter should generally disclose the following:

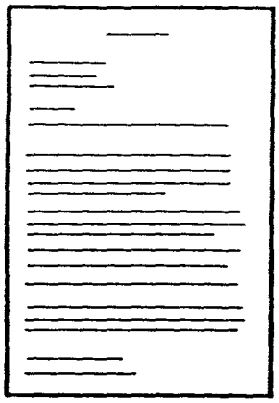
Administrative Information and Points of Contact

Identify the exporter, including division, parent company and PM/MC code, and cognizant points of contact. *For cases involving technology transfer, it is important that the contact either be technically cognizant, or have ready access to personnel who are;*

Include a statement that the proposed export is in support of the Army LHX program. Make note that the Army has encouraged international participation in the LHX program.

If work is to be performed abroad directly as a result of this export state where it will be performed and by whom, specifying the company(ies) receiving the export. Include the division, parent company and location.

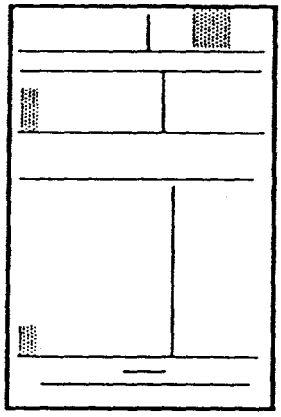
Identify any points of contact within the U.S. Army with whom the proposed license has been coordinated. *This information is vital for timely processing of the export license. The Army Program Manager (PM) at AVSCOM is the primary point of contact for LHX. The PM will coordinate technical concurrence with other Army technical POCs as required in pre-screening the license application and will further ensure that this fully coordinated Army position is provided to DTSA and OMC at State.*



COVER LETTER

The COVER LETTER should provide:

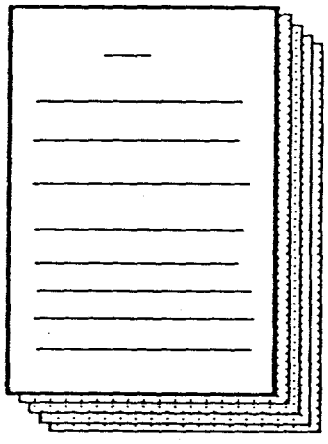
1. A clear and concise summary of the nature and purpose of the proposed transaction;
2. Assurances that important technology transfer and security concerns have been recognized and addressed;
3. Clear identification of cognizant offices and individuals from whom additional information can be obtained, especially any with whom the specific transaction has been coordinated;
4. If additional information has been provided to support the application, a summary overview of the contents and organization of the application package; and
5. Any other information regarding the transaction that may help the reviewers reach a timely decision.



DSP-5

The DSP-5 form should:

1. Be complete and accurate;
2. Be consistent with the cover letter;
3. Clearly identify the program for which the export is required; and
4. Be as specific as possible in the description of the material or technical data to be exported.



SUPPORTING INFORMATION

SUPPORTING INFORMATION should be:

1. Kept to the minimum needed to support the application and address government concerns;
2. Organized and indexed to aid the reviewer;
3. Clear, legible, and understandable; and
4. Described and referenced in the COVER LETTER and referenced appropriately in the DSP-5.

Technical Scope and Description

The cover letter should specifically identify the type of transaction, and the **technology** content of the material or technical information that will be provided. The following provides an exemplary list of distinctions that will be meaningful to the reviewing community:

End-item sales, without know-how;

End-item sales, with know-how for operation, maintenance, test, alignment, or calibration;

End-items or technical data (e.g., performance specification, interface control drawings) to permit design integration or system assembly;

End items with embedded software (specifying software form and whether or not software development/support technology will be provided;

Manufacturing license agreements (MLA). In these cases it is important to specify whether transfer of process know-how is required. The form of the Tech Data (e.g., Build-to-print, process control information, CAD/CAM software) and the extent to which the information can be exploited for other purposes should be explicitly addressed.

Technical Assistance Agreements (TAAs) are highly effective technology transfer mechanism and are, therefore, usually subjected to special scrutiny. In addition to the technical questions already discussed, the reviewer will be interested in a number of specific points, as follows:

The purpose of the TAA and the direction of the technology transfer. *(A surprising number of TAAs are delayed because the exporter has failed to make clear that the purpose of the transfer is to acquire foreign technology.)*

Specific hardware, technical data, or elements of U.S. technology that must be transferred or disclosed to achieve the stated purposes. *Specify what critical technologies (especially manufacturing information, or production data as identified in the foreign disclosure plan) are involved and how they will be protected.*

The extent (both in time and number of participants) of personal interaction envisioned, and where the exchanges will take place. *Where the TAA will involve foreign participation on-site at U.S. industrial facilities, the applicant should describe what security measures will be implemented to preclude foreign access to material and technical information related to other DOD work at the facilities in question.*

If the transfer is related to, or required to support an existing TAA or MLA, the relationship should be explained and the previous export license cross referenced, as necessary. It is important that the cover letter clearly identify the quid-pro-quo between your company and the foreign company(ies) (i.e., The net benefit to the U.S. anticipated as a result of this export). In the case of certain key technologies, wherein a U.S. lead supports a significant operational advantage of U.S. forces, an acceptable **technological** quid-pro-quo should be documented.

For these and other exports involving sensitive components or critical technology, pre-screening of the application and identification of PM LHX POC who can concur that it meets the technology security requirements of the Foreign Disclosure Plan will greatly expedite case processing.

Other Information

In addition to information on the specific transaction, information about comparable exports or availability of equivalent products or technologies from foreign sources is often an important consideration in evaluating a given license. It is important that information cited be accurate, referenced as specifically as possible, and well documented. *A marketing brochure alone, without further documentation or corroborating evidence is not sufficient to establish equivalent foreign availability.*

In citing related or similar (as opposed to identical) precedents, be as specific as possible. Give sufficient technical detail to allow the reviewer to see precisely how the transactions are related. *(An example, when considering an end item transfer, the reviewer should know if an MLA to allow offshore production of the item had been previously approved.)*

3.2 The Application Form (DSP-5)

The essential part of the entire export license request process is the State Department form (DSP-5). Incomplete or inaccurate information on the DSP-5 will result in costly delays to an export license request and to the program. The following is a list of suggestions for those sections of the DSP-5 that Army experience has shown cause problems:

Item 6. Names, agency and telephone numbers of USG personnel familiar with the commodity. This should be someone with technical knowledge, or a POC that has direct access to such technical expertise. *In the case of the LHX program this would be the PMO at AVSCOM.*

Item 7. Applicant's contact. Department of State prefers this be a Washington, D.C. POC if possible. This Washington POC should, however, know and have the ability to contact the company's technical POC.

Item 9. Commodity. Be as detailed, accurate, and specific as possible. Use specific nomenclatures, define the nature of the transaction (e.g., MLA, TAA, etc.) and (as appropriate) the character of the technical data provided.

Item 14. Specific Purpose. Be as specific as possible regarding the aspect of the program for which the export is intended. **Be sure to state that the export is required to support the LHX program.**

Item 21. **Licensing precedents.** Be sure that the precedents cited were for **identical** commodities, and not similar or related items. Other exports involving similar or related materials should be addressed in **supporting information** and in the **cover letter**.

3.3 Supporting Information.

While form and content of supporting information will be dictated by the requirements of the specific case, several general suggestions apply.

Minimize the amount of paper involved. Include only information that directly relates to the application. *A common error on the part of inexperienced applicants is to submit technical information on a family of equipments and assume that the reviewer will sort out which applies. This introduces confusion and delay, and can result in a case being returned without action.*

Organize the material, and provide a table of contents. Ideally the cover letter, license, and supporting information should be as parallel in structure as possible, the references concise and clear.

For example, consider a license for a TAA for a joint codevelopment. A cover letter might summarize the technical scope of the exhange, the security measures being instituted to preclude foreign access to other programs at their facility, and the quid-pro-quo in terms of anticipated technical contributions by the foreign partner. Supporting information in this case could include the TAA, itself, a copy of a security plan, and technical information on relevant work being done by the foreign partner to demonstrating their ability make the expected contribution. An effective cover letter will obviate the need for wading through extraneous boiler-plate by citing salient points in the supporting information by page and/or paragraph.

Examples of the types of information that may be incorporated into supporting documentation include:

Technical descriptions of products or technologies, including both those proposed for export and those available from foreign sources;

Descriptions of software (format and function;)

End-use/end user information and assurances (in addition to that required for the licensing process;)

Copies of MLAs/TAAs;

Listings of references to precedent cases involving similar or related products and/or technologies;

Copies of specific technical data (drawings, process control data, patents, etc.) proposed for export;

Security plans and procedures;

Resumes and descriptions of the anticipated contributions of foreign experts participating in the project;

As appropriate, copies of specific USG guidance, to document compliance.

4. PUTTING IT ALL TOGETHER

These suggested guidelines have one objective--to ensure that the licensing process as a whole (including the actual application, cover letter and any supporting information provided) will effectively communicate what the government needs to know to processs a case quickly and consistently. Communication should begin in the early planning stages, long before submission of an application for a munitions export license. The cover letter, the license, and the supporting information provided should be complementary, and should give a complete and accurate picture of the proposed transaction.

ATTACHMENT 7

Requirements of the Foreign Disclosure Plan (FDP)

REQUIREMENTS OF THE FOREIGN DISCLOSURE PLAN (FDP)

An FDP is required for any program subject to AR 70-1, which is either classified, or for which U.S. Army-owned technical data is controlled as unclassified Defense technical data under DoDD 5230.24 and 5230.25. The following programs do not require an FDP:

a. Programs which for reasons of classification are categorically excluded from all foreign disclosure or participation;

b. Unclassified NDI programs for which the U.S. Army has not acquired technical data for production;

c. Existing programs which were created pursuant to an international agreement, wherein the agreement serves as the FDP.

There will be presumption of denial for any other disclosure request not addressed by an approved FDP.

PURPOSE OF THE FDP

The FDP provides the policy guidance for release of U.S. Army material and information to foreign governments and their authorized representatives, including appropriately cleared foreign industry. The intent is to facilitate international cooperation within a framework that adequately protects classified information and militarily critical technologies. The FDP should, therefore, be based on and reflect an approved Security Classification Guide and a Weapons System Technology Assessment (WSTA).

The FDP serves as a management tool to identify and resolve foreign disclosure issues. It summarizes the assessment of foreign disclosure considerations upon which releases will be based. While the basic elements described below must appear in all cases, the level of detail may vary depending on specific program needs. The FDP is normally updated and augmented prior to Material Acquisition Decision Process reviews, or as technological developments or program changes occur. In all cases, the FDP must provide sufficient detail to be used as guidance for case-by-case disclosure decisions and delegations of disclosure authority. The following outlines the minimum requirements for elements of an FDP.

CONTENT OF THE FDP

I. PURPOSE AND SCOPE: Identify the program and overall intent of releases (e.g., to support codevelopment, FMS, etc.) any other guidance incorporated by reference (i.e., WSTAs and/or security classification guides).

II. BACKGROUND: Summarize the technical objectives of the program, and describe the present status of the program.

III. DISCLOSURE GUIDELINES:

A. Eligibility Requirements: Specify limits on disclosure based on NDP eligibility by classification and category of disclosure.

B. ***Level and Scope of Disclosure:*** This section must differentiate and provide guidance regarding:

1. The program phases for which international cooperation/participation is anticipated;

2. Highest classification of information releasable;

3. Any general limitation or conditions (e.g., foreign government sponsorship and legal assurances; FMS only; or limitations on information that can be licensed under ITAR);

4. FMS;

5. Coproduction;

6. Codevelopment;

7. Other exchanges of information or technical data (e.g., threat descriptions, tactics, training materials, etc.).

C. ***Specific Disclosure Guidance:*** The general guidelines provided in B. must be supported by the following details:

1. A program technology overview describing the program's key technology security issues (e.g., design and production of high-temperature structural composites.)

2. Current state of program development of those technologies (e.g., is the program in an early design/demonstration phase; has it developed unique production processes, etc.)

3. Disclosures permitted by program phase, including:

   a. Purpose of disclosure;

   b. Classification;

   c. Limitations on unclassified defense information based on level of technology transfer concern identified in WSTA;

   d. Any explicit conditions or restrictions--e.g., no release of manufacturing process data during preliminary design phase; and

   e. To the extent possible disclosure guidance for specific program documents.

4. Any other special security restrictions (e.g., COMSEC, special access restrictions, etc.); and

5. Data of next required update for the FDP.

9-X38-1032U-1

ATTACHMENT 8

Language for Interim Changes to AR-70-1

Language for Interim Change to AR 70-1

1. AR 70-1 is hereby modified to incorporate a requirement for a Technology Security Plan (TSP). The TSP meets the requirements for "full consideration of foreign disclosure and development of technology security plan as set forth in Action item 34 of Table D-1 in AR 70-1. The TSP supersedes and fulfills the requirements defined in AR 70-1 Table D-6 Items q. Foreign Disclosure Plan (FDP), and ao. Weapons System Technical Assessments.

2. The following provide interim language, superseding the two items cited in one above, pending the next update to AR 70-1

xx. Technology Security Plan (TSP)

(1) **Applicability**: All MDAPs, ADAPs subject to ASARC review, and Level I programs for which foreign disclosure of classified of unclassified defense technical information is projected. Requirements for a TSP for Level II, and III programs will be established on a case-by-case basis. (See references for guidance.)

(2) **Description:** Description, assessment, and disclosure guidance and plan for sharing and protecting all material and technical information required to support foreign participation either in a formal international cooperative program or as a participant in a U.S. acquisition program, or procurement of the system.

(3) **Responsibility:** MATDEV in conjunction with AMC and program sponsor.

(4) **Approval:** HQDA (DCSINT)

(5) **Reference:** AR 380-10, AR 380-66, and DODD 2040.2

Attachment A provides interim guidance regarding the format and content of the TSP. This guidance is hereby incorporated as an interim addendum to AR 380-10 and AR 380-66, and will be incorporated in the next update of those regulations.

ATTACHMENT A

INTERIM GUIDANCE FOR PREPARATION OF TECHNOLOGY SECURITY PLAN

The following provide general criteria and guidelines for the development of Technology Security Plans (FDP) for U.S. Army Systems. Under the interim change to AR 70-1 a TSP is required by AR 70-1 for certain programs, as a prerequisite for major milestones.

REQUIREMENTS FOR THE TSP

A TSP is required for all MDAPs, ADAPs subject to ASARC review, and any Level I program for which foreign disclosure of classified information or U.S. Army-owned technical data controlled as unclassified Defense technical data under DoDD 5530.24 and 5530.25 unclassified defense technical information is projected. Other the need for a TSP for other Army programs (Level II and III) will be determined on a case-by-case basis by the MACOMs in coordination with AMC, HQ ACSI, and approved by DAMI-CIT. Completion and approval of the TSP is a prerequisite for any disclosure to foreign entities of classified or unclassified defense technical information related to Army systems acquisition programs. Prior to approval of the TSP, foreign disclosure will be limited to unclassified information that has been approved for public release.

The following programs do not require an full TSP.

a. Programs which for reasons of classification are categorically excluded from all foreign disclosure or participation;

b. Unclassified NDI programs for which the U.S. Army has not acquired technical data for production.

PURPOSE OF THE TSP

The TSP provides a description and analysis of the militarily critical technologies and sensitive information contained in Army programs. It provides policy guidance and procedures for release of U.S. Army material and information to foreign governments and their authorized representatives, including appropriately cleared foreign industry. The intent is to facilitate international cooperation within a framework that adequately protects classified information and militarily critical technologies. The TSP should, therefore, be based on and reflect an approved Security Classification Guide and current National Disclosure Policy.

The TSP serves as a management tool to identify and resolve foreign military sales, technology transfer, foreign disclosure issues. It summarizes the assessment of foreign disclosure considerations upon which releases will be based. While the basic elements described below should appear in all cases, the level of detail may vary depending on specific program needs. The TSP is intended to be a "living document" that will be updated and augmented prior to Material Acquisition Decision Process reviews, or as technological developments or program changes occur. In all cases, the DSP should provide sufficient detail to be used as guidance for case-by-case decisions and delegations of disclosure authority. The following outlines the minimum requirements for elements of an acceptable TSP.

CONTENT OF THE TSP

The TSP has three major components as follows:

The technology assessment. This incorporates the elements of the current WSTA, and addresses the Army and DOD requirements for the risk assessments required as a prerequisite for international programs;

The foreign disclosure guidelines, incorporating the elements of the FDP;

An executive summary of outlining the general levels of concern for the different aspects of technology (end-item sale, coassembly, coproduction, codevelopment, and related information) involved in the program, and broad disclosure guidelines for each category of information.

The following is a general outline and description of the form and content of the TSP.

PREFACE PROVIDING STATEMENT OF PURPOSE AND SCOPE: Identify the program and overall intent of releases (e.g., to support codevelopment, FMS, etc.) any other guidance incorporated by reference (i.e., WSTAs and/or security classification guides). This should also summarize any Army and contractor activities involved, and the cognizant point(s) of contact for Army activities as appropriate.

EXECUTIVE SUMMARY

This should be a concise summary for senior level decision makers, typically three-to-four pages consisting of:

PROGRAM OVERVIEW--a brief summary of the program and major milestones, including projected operational dates, planned production rates, and the prime contractors (if known.)

SYSTEM DESCRIPTION--a concise paragraph giving the systems essential characteristics. Use of figures and photographs is appropriate.

TECHNOLOGY SECURITY ISSUES--identifies and summarizes:

Any material or information whose disclosure would reveal:

Inherent systems weaknesses from which countermeasures to defeat or degrade U.S. systems effectiveness could be derived; or

Threat data or other information that could compromise U.S. intelligence sources or methods;

and the impact of unauthorized disclosure or compromise;

The current and projected level of international interest and technological capabilities in the systems, or comparable systems; and

SUMMARY GUIDELINES--summarizes broad limits for disclosure of classified and unclassified information. A chart characterizing the level of concern for release of end items, and technical information for co-assembly, co-production, and codevelopment should be provided, together with the NDP category and highest classification of information involved in each category.

I. TECHNOLOGY ASSESSMENT

A. SYSTEM DESCRIPTION--Provide a description of the system identifying sensitive subsystems and components. The level of detail should be kept to the minimum needed to let the reader to understand the importance of information and technology for which control measures are recommended. (Depending on complexity this will typically range from 5-15 pages. Use of figures and diagrams is encouraged.)

B. FOREIGN CAPABILITIES AND COMPARABLE SYSTEMS--Describe any similar foreign systems, and related technological capabilities in sufficient detail to let the reader understand the relative risks and benefits of technology sharing/transfer.

C. TRANSFER GUIDELINES--Specific guidelines for sharing and protecting sensitive technologies with friendly and allied nations. Each aspect listed below should be addressed.

End item sales

Coassembly

Coproduction

Codevelopment

Other Technical Data/Information Exchanges

Technical Assessments Update Information

Other Special Security Considerations

D. **CONTROLLED TECHNOLOGY**--This section provides the technical rationale for the guidelines, identifying critical aspects of subsystems and components and unclassified defense technical information subject to export control. The following Department of Defense Militarily Critical Technologies List (MCTL), the Export Administration Regulations (EAR), and the International Traffic in Arms Regulations (ITAR) should be used and referenced as guidance.
This section also can provide additional background on foreign capabilities and specific technical characteristics and performance limits of concern.

III. DISCLOSURE GUIDELINES

A. **ELIGIBILITY REQUIREMENTS**: Specify limits on disclosure based on NDP eligibility by classification and category of disclosure.

B. **LEVEL AND SCOPE OF DISCLOSURE**: This section should discuss and provide guidance for:

1. The program phases for which international cooperation/participation is anticipated;

2. Highest classification of information releasable;

3. Any general limitation or conditions (e.g., foreign government sponsorship and legal assurances; FMS only; or limitations information that can be licensed under ITAR).

The FDP should differentiate and provide explicit guidance for disclosure under any of the following that apply. The FDP should provide (There will be presumption of denial for any disclosure not addressed in the FDP.)

4. FMS;

5. Coproduction;

6. Codevelopment;

7. Other Technical data (e.g., threat descriptions, tactics, training materials, etc.);

8. Any other special security restrictions (e.g., COMSEC, special access restrictions, etc.); and

9. Next required update for FDP.

C. SPECIFIC DISCLOSURE GUIDANCE: The general guidelines provided in B. should be supported by the following details:

1. A program technology overview describing the program's key technology security issues (e.g., design and production of high-temperature structural composites.)

2. Current state of program development of those technologies (e.g., is the program in an early design/demonstration phase; has it developed unique production processes, etc.)

3. Disclosures permitted by program phase, including:

   a. Purpose of disclosure;

   b. Classification;

   c. Limitations on unclassified defense information based on level of technology transfer concern identified in WSTA

   d. Any explicit conditions or restriction (e.g., no release of manufacturing process data during preliminary design phase.)

   e. To the extent possible disclosure guidance for specific program documents should be provided.

APPENDIX A. HOSTILE INTELLIGENCE SUMMARY ASSESSMENT (HOIS)

ATTACHMENT 9

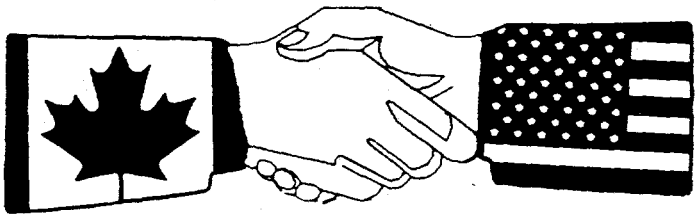
US-Canada Joint Certification Program Documentation:

US/Canada Joint Certification Program;

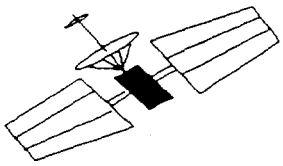
The US/Canada Joint Certification Program for Directly Arranged Visits (DAV); and

Briefing Paper--US/Canada Technology Security under the Joint Certification Program.

DEPARTMENT OF DEFENSE
U.S.-CANADA
JOINT CERTIFICATION PROGRAM



Control of Unclassified Technical Data With Military or Space Application



November 1990
Office of Director, Defense
Research & Engineering

***** FINAL DRAFT *****

1 OCTOBER 1990

THE U.S.-CANADA JOINT CERTIFICATION PROGRAM

Control of Unclassified Technical Data

With Military or Space Application

NOTE: This draft JCP pamphlet supersedes all previous versions of the pamphlet.

FOREWORD

The United States and Canada share a unique, long-standing military and economic relationship. The two countries are partners in the joint defense of North America and have established a bilateral common structure (NORAD) for mutual defense. Canadian industry is a part of the North American Defense Industrial Base. The United States and Canada consult and cooperate on the development of common industrial security procedures and technology controls. The two governments have entered into numerous bilateral agreements that codify and support this relationship.

In 1985, the United States and Canada signed a Memorandum of Understanding (MOU) that established the U.S.-Canada Joint Certification Program (JCP). As stated in the MOU's "Joint Terms of Reference for the United States-Canada Joint Certification Program," the program was established "to certify contractors of each country for access, on an equally favorable basis, to unclassified technical data disclosing critical technology" controlled in the U.S. by Department of Defense Directive 5230.25 and, in Canada, by the Technical Data Control Regulations. Policy oversight for security and technology transfer matters for the U.S./Canada Joint Certification Program is provided by the U.S./Canada Security and Technology Sharing Subcommittee of the Defense Development/Defense Production Sharing Arrangements Steering Committee (DDPSA).

This pamphlet has been jointly produced by the U.S. Department of Defense and the Canadian Department of Supply and Services to explain how the program has developed and why; how an individual or enterprise located in the U.S. or Canada can become a certified contractor under the JCP; and what specific actions must be taken by persons working with unclassified technical data disclosing critical technology.

North American security demands that we combine our technology resources for mutual benefit. By working upon existing opportunities for defense-economic cooperation, we believe that we can better provide for the security of our respective nations.

This pamphlet supersedes DoD 5230.25-PH, "Control of Unclassified Technical Data with Military or Space Application."

Canadian Signature

U.S. Signature

TABLE OF CONTENTS

FIGURES

I. INTRODUCTION

The establishment of the Joint Certification Program (JCP) benefits U.S. and Canadian defense and high technology industries by facilitating their continued access to unclassified technical data disclosing critical technology in the possession of, or under the control of the U.S. Department of Defense (DoD) or the Canadian Department of National Defence (DND). Certification under the JCP establishes the eligibility of a U.S. or Canadian contractor to receive technical data governed, in the U.S., by DoD Directive 5230.25 and, in Canada, by the Technical Data Control Regulations (TDCR).

U.S. Implementing Regulation

The provisions of Section 1217 of Public Law 98-94 are implemented in Department of Defense Directive 5230.25. This Directive sets forth policies, procedures and responsibilities for the withholding of unclassified technical data from public disclosure. DoD also has issued DoD Directive 5230.24, a companion directive to DoD Directive 5230.25, that establishes the distribution marking system for DoD-controlled technical documents.

Canadian Implementing Regulation

The Government of Canada recognized the need to establish regulations similar to DoD Directive 5230.25, not only for national security reasons, but also to ensure that Canadian contractors would continue to have access to DoD-controlled technical data. The TDCR, which largely parallels DoD Directive 5230.25, has been issued under the authority of the Canadian Defence Production Act. The regulations, for which the Minister of Supply and Services is responsible, came into effect on March 20, 1986.

Joint Certification Office

The U.S./Canada Joint Certification Program is managed by the U.S./Canada Joint Certification Office (JCO). The JCO, a common, jointly staffed office, is located at the Defense Logistics Services Center (DLSC), 74 N. Washington Avenue, Battle Creek, Michigan 49017-3084. The JCO receives and processes certification forms submitted by U.S. and Canadian contractors that wish to obtain access to unclassified technical data disclosing critical technology under the control of DoD or DND.

II. CRITERIA FOR WITHHOLDING OF UNCLASSIFIED TECHNICAL DATA WITH MILITARY OR SPACE APPLICATION

Access to unclassified technical data with military or space application (also referred to as technical data disclosing critical technology) is controlled when such technical data:

a. are in the possession of or under the control of DoD, or administered and controlled by DND;

b. may not be exported lawfully without an approval, authorization or license under U.S. or Canadian export control laws, as applicable; and

c. disclose critical technology (see definition in **Appendix E**).

Unclassified technical data with military or space application (hereafter referred to as "technical data") includes any:

a. blueprints, drawings, plans, instructions, computer software and documentation, or other technical information that can be used, or adapted for use, to:

b. design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce military or space equipment or technology concerning such equipment.

III. COMPANY PROPRIETARY DATA

The U.S./Canada Joint Certification Program and its procedures do not extend to company proprietary technical data. Therefore, it does not govern the private exchange of industry- generated export-controlled technical data. In these cases the contractors must follow the guidelines established in U.S. or Canadian export control regulations, as applicable. U.S. contractors should contact the U.S. Department of State Office of Defense Trade Controls at (703) 875-6644 to obtain additional guidance. Canadian contractors should contact the Department of External Affairs Export Control Division at (613) 996-2387 to obtain more specific guidance.

IV. APPLICATION FOR CERTIFICATION

Because U.S. Public Law 98-94 only granted authority to withhold, not selectively disseminate technical data, a system of certification was established that permitted dissemination for legitimate business purposes while maintaining the ability of the DoD to withhold the data for other purposes. Equivalent withholding and dissemination provisions are reflected in the TDCR.

Completion of DD Form 2345

To become certified, U.S. contractors must submit a completed DD Form 2345 to the JCO. Canadian contractors may submit either a completed DD Form 2345 or DSS-MAS 9379 for certification. However, a DD Form 2345 shall be used when a Canadian contractor intends to request access to DoD-controlled technical data.

Because technical data transferred to a certified contractor are mailed to the location shown on the form, each corporate subsidiary or division that is to receive unclassified technical data should be certified separately.

Contractors applying for certification are required to designate a person by name or position designation to act as the Data Custodian for the facility. This person will be responsible for receiving and disseminating any technical data transferred to the certified contractor under the provisions of the JCP. The individual chosen to fill the position of Data Custodian at a U.S. contractor facility must be a U.S. citizen or a person admitted lawfully for permanent residence into the United States. In the case of a Canadian contractor facility, the Data Custodian must be a Canadian or U.S. citizen or a person admitted lawfully for permanent residence into Canada.

The contractor's business activity is a key element of the certification process since this information will be used by the controlling office as a basis for approving or disapproving specific requests for technical data. Consequently, the business activity statement should be sufficiently detailed to support requests for any data that the contractor expects to need for legitimate business purposes. Proprietary or other sensitive information should not be included in the statement since the information entered on the form will be publicly available.

As a condition of receiving the DoD or DND-controlled technical data, the contractor agrees to use the data only in ways mandated by DoD Directive 5230.25 or the TDCR. The contractor must certify that it needs the technical data to bid or perform on a contract with an agency of the U.S. or Canadian Government or for other legitimate business purposes.

"Other legitimate business purposes" include:

a. Providing or seeking to provide equipment or technology to a foreign government with the prior approval of the U.S. or Canadian Government, as applicable;

b. Bidding or preparing to bid on a sale of surplus property;

c. Selling or producing products for the U.S. or Canadian commercial domestic marketplace, or for the commercial foreign marketplace, providing that any required export license is obtained from the appropriate U.S. or Canadian licensing authority.

d. Engaging in scientific research in a professional capacity for either of the two defense establishments; or

e. Acting as a subcontractor for a concern described in (a) through (d), above.

The contractor must acknowledge its responsibilities under the applicable U.S. or Canadian export control laws. It must agree not to publicly disclose any unclassified technical data it receives under the agreement, unless specifically authorized by the controlling office, and to limit access to the data to individuals employed at its facility meeting the following citizenship requirement:

a. U.S. citizens or intending citizens if the facility is located in the United States; and

b. Canadian or U.S. citizens or permanent residents of Canada if the facility is located in Canada.

As a condition of receiving unclassified technical data, a contractor must certify on the form that to the best of its knowledge and belief the information provided and the certifications made are true, complete, and accurate and are made in good faith. A contractor that knowingly and willfully makes a false statement on the form can be punished by a fine or imprisonment or both under the U.S. Code, Title 18, Section 1001 or Section 21 of the Canadian Defence Production Act, as applicable.

If a contractor violates the provisions of the agreement, the contractor's eligibility for access to unclassified technical data may be revoked. However, a contractor's eligibility for access may be reinstated when the basis for the revocation has been remedied. If a contractor exports the technical data without the benefit of license or other authorization, it may be in violation of export control laws and subject to severe criminal penalties. A contractor violating the provisions of the agreement may be subject to prosecution by the contracting authority.

The certification form is designed for ease of completion. When accepted by the JCO it constitutes an agreement among the certifying company, DoD, and DSS. An example of a fully processed DD Form 2345 is shown at **Figure 1.**

MILITARILY CRITICAL TECHNICAL DATA AGREEMENT

(Please read Privacy Act Statement and Instructions on reverse before completion.)

Form Approved OMB No. 0704-0207 Expires Dec 31, 1989

1. TYPE OF SUBMISSION (X one): [X] INITIAL SUBMISSION [ ] RESUBMISSION [ ] REVISION [ ] 5-YEAR RENEWAL

2. INDIVIDUAL OR ENTERPRISE DATA *(Referred to as a "certified contractor" upon acceptance of certification by the U.S. / Canada - JCO)*

a. NAME: Company X

b. ADDRESS (Street, City, State/Province and Zip/Postal Code): 74 North Washington Ave. Battle Creek, MI 49017-3084

c. NAME OF SUBSIDIARY / DIVISION: Aerospace Division

d. FSCM / FSCNM / CAGE / DSS VENDOR CODE: AAAAA

e. PHONE NO.: (123) 456-7890

3. DATA CUSTODIAN

a. NAME OR POSITION DESIGNATION *(See Instructions)*: John DOE

b. ADDRESS (Street, City, State/Province and Zip/Postal Code): P.O. Box 2345 Battle Creek, MI 49017-2345

c. PHONE NO.: (123) 456-7890

d. TITLE: Facility Security Officer

4. DESCRIPTION OF RELEVANT BUSINESS ACTIVITY

Design and manufacture equipment used on military and commercial aircraft, including:

- electrical controllers/sensors for aircraft control systems and aircraft windshield temperature controls;
- electromechanical rotary/linear actuators, butterfly valve assemblies for various aircraft applications, including aircraft environmental control systems, throttle controls, and bleed air management; and
- pneumatic operated pressure regulators, shut-off valves, flow valves and check valves.

5. AS A CONDITION OF RECEIVING MILITARILY CRITICAL TECHNICAL DATA, THE INDIVIDUAL OR ENTERPRISE CERTIFIES THAT:

a. (1) Citizenship / Residency Status. The individual designated either by name or position designation in Item 3, who will act as custodian of the militarily critical technical data on behalf of the contractor, is: (X one - (a), (b), (c), or (d))

- [X] (a) a U.S. citizen
- [ ] (b) a Canadian citizen
- [ ] or a person admitted lawfully for permanent residence into:
- [ ] (c) the United States
- [ ] (d) Canada

(2) Business Location. Business of individual listed in Item 3 is located in (X (a) or (b))

- [X] (a) the United States
- [ ] (b) Canada

b. The data are needed to bid or perform on a contract with any agency of the U.S. Government or the Canadian Government or for other legitimate business activities in which the contractor is engaged, or plans to engage.

c. It (1) acknowledges all responsibilities under applicable U.S. export control laws and regulations (including the obligation, under certain circumstances, to obtain an export license from the U.S. Government prior to the release of militarily critical technical data within the United States) or applicable Canadian export control laws and regulations, and

(2) agrees not to disseminate militarily critical technical data in a manner that would violate applicable U.S. or Canadian export control laws and regulations.

d. It will not provide access to militarily critical technical data to persons other than its employees, or persons acting on its behalf, unless such access is permitted by U.S. DoDD 5230.25, Canada's TDCR, or by the U.S. or Canadian Government agency that provided the technical data.

e. No person employed by it, or acting on its behalf, who will have access to militarily critical technical data, is debarred, suspended, or otherwise ineligible to perform on U.S. or Canadian Government contracts or has violated U.S. or contravened Canadian export control laws or has had a certification revoked under the provisions of U.S. DoDD 5230.25 or Canada's TDCR.

f. It is not itself debarred, suspended, or otherwise ineligible to perform on U.S. or Canadian Government contracts, and has not violated U.S. or contravened Canadian export control laws, and has not had a certification revoked under the provisions of U.S. DoDD 5230.25 or Canada's TDCR.

6. CONTRACTOR CERTIFICATION

I certify that the information and certifications made by me are true, complete, and accurate to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. *(For U.S. Contractor see U.S. Code, Title 18, Section 1001 and for Canadian Contractor see Section 21 of the Defence Production Act.)*

a. TYPED NAME (Last, First, Middle Initial)	b. TITLE	c. SIGNATURE	d. DATE SIGNED
SMITH Harry T.	VP Sales & Marketing	******SAMPLE******	1 May 90

7. CERTIFICATION ACTION (X one)

- [X] a. CERTIFICATION ACCEPTED: This certification number, along with a statement of intended data use, must be included with each request for militarily critical technical data. NUMBER: 0000000
- [ ] b. RETURNED - Insufficient information:
- [ ] c. REJECTED - Does not meet eligibility requirements of DoDD 5230.25 or of Canada's TDCR.

8. DoD OFFICIAL			9. CANADIAN OFFICIAL		
a. TYPED NAME (Last, First, Middle Initial)			a. TYPED NAME (Last, First, Middle Initial)		
McCLENAHAN, Jospeh M.			CHENIER, Joseph C. L.		
b. TITLE			b. TITLE		
United States Representative			Canadian Representative		
c. SIGNATURE	d. DATE SIGNED		c. SIGNATURE	d. DATE SIGNED	
	1 May 90			1 May 90	

DD Form 2345, APR 86 *Previous editions are obsolete*

Figure 1

DD Form 2345 Review Process

The JCO will review a DD Form 2345 submitted by a U.S. or Canadian contractor within five working days and:

a. accept the certification; or

b. return it because of insufficient information; or

c. refer it to higher authority with a recommendation to reject the certification because the contractor does not meet the criteria for certification.

The chart at **Figure 2** details the procedures followed by the JCO to review DD Forms 2345 submitted by U.S. and Canadian contractors.

CONTRACTOR CERTIFICATION PROCESS

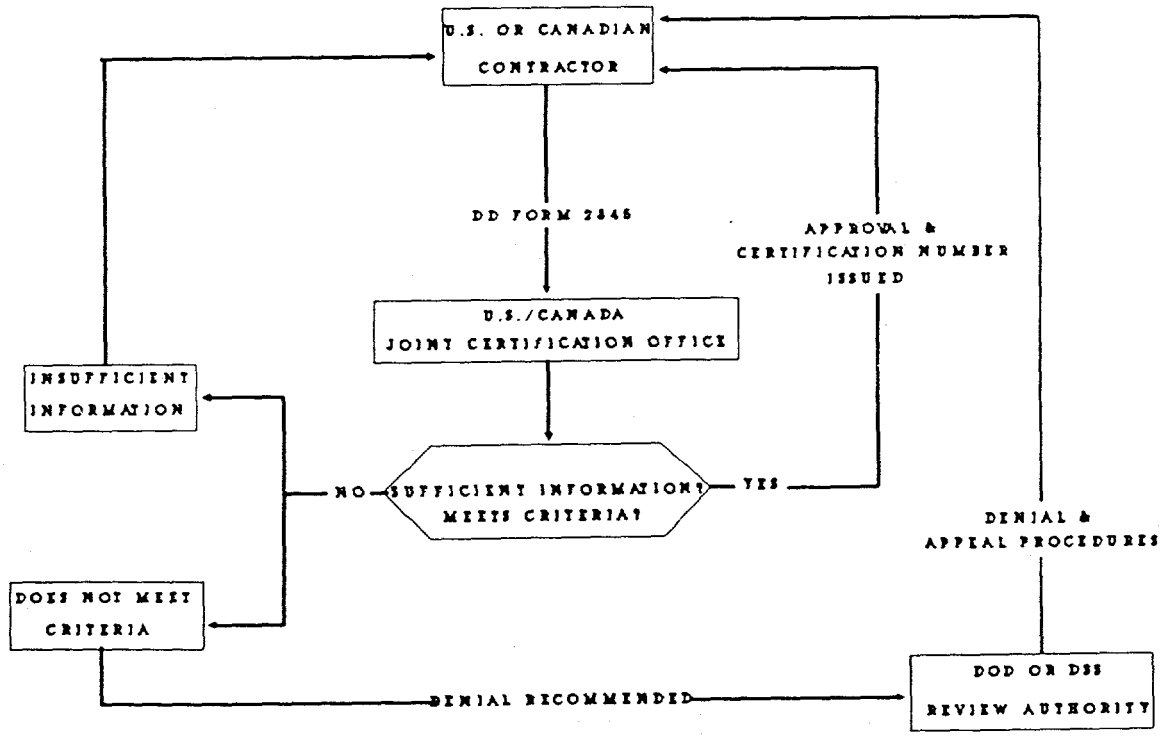


Figure 2

Certification Acceptance

Upon acceptance of the contractor's certification, the JCO will mail the original copy of the form to the Data Custodian. A seven-digit certification number is entered on the form prior to being mailed to the Data Custodian. The certification is valid for a renewable five year period unless the contractor is shown to have violated the terms of the agreement. The certification number refers to the "facility" rather than an "individual employee" and extends to U.S. and Canadian citizens and persons admitted lawfully for permanent residence into the U.S. or Canada (intending citizens) who are employed at the facility.

Once certified, the contractor may:

a. Request unclassified technical data controlled by the DoD or DND;

b. Respond to defense-related contracts whose specifications involve unclassified technical data releasable only to certified contractors;

c. Attend restricted gatherings where unclassified technical data are presented (i.e., symposia, program briefings, meetings designed to publicize advance requirements of the contracting agency, pre-solicitation, pre-bid, pre-proposal and pre-award conferences).

d. Arrange unclassified visits directly with other certified U.S. or Canadian defense contractors or U.S. and Canadian military facilities. The type of directly arranged visit (DAV) authorized as a result of JCP certification is discussed in **Appendix B.**

Rejection of DD Form 2345

If a certification is rejected, the contractor will be notified by registered mail and provided a copy of the rejection, stating the reasons for the rejection, explaining appeal rights, and advising the firm that it may appeal within thirty days.

Revision of DD Form 2345

Certified contractors should submit a revised DD Form 2345 whenever information previously furnished becomes outdated - if, for example, ownership, purpose of business, or the name of the company changes, or a new Data Custodian is designated by the certified contractor. Approval of a revision submittal starts a new five-year eligibility period for the certified contractor.

Renewal Notice

U.S. and Canadian contractors become certified on the date the JCO approves their certification. These contractors will be added to the Certified Contractor Access List (CCAL) and provided a renewal notice 120 days before their certification expires.

V. REQUESTS FOR UNCLASSIFIED TECHNICAL DATA

Requests For DoD-Controlled Technical Data

Certified contractors obtain DoD-controlled technical data by:

a. Requesting technical data in support of a DoD contract directly from the DoD contracting authority or through the U.S. prime contractor (U.S. prime contractors are referred to Appendix C for guidelines regarding the transfer of DoD- controlled technical data to a certified Canadian sub-contractor);

b. Requesting technical data needed to respond to Requests for Proposal (RFP) directly from the Program Manager;

c. Requesting technical data desired for other legitimate business purposes through a library or other technical data repository.

A copy of the JCO-approved DD Form 2345 should accompany all requests for DoD-controlled technical data. DD Form 2345 also should accompany any requests for Direct Arranged Visits (DAV), or attendance at a conference or symposia when unclassified technical data is being presented. The chart at **Figure 3** shows the review procedures that are in place to process requests for DoD-controlled technical data.

Requesting DoD-Controlled Technical Data From DTIC

Certified U.S. contractors that are registered with the Defense Technical Information Center (DTIC) should request DoD- controlled technical data directly from DTIC at the following address:

Defense Technical Information Center
Attn: DTIC-FDRB, Cameron Station
Alexandria, VA 22304-6145

Certified Canadian contractors should request DoD-controlled technical data, the distribution of which is administered by the DTIC, through the Directorate Scientific Information Service (DSIS) at the address shown on page 10.

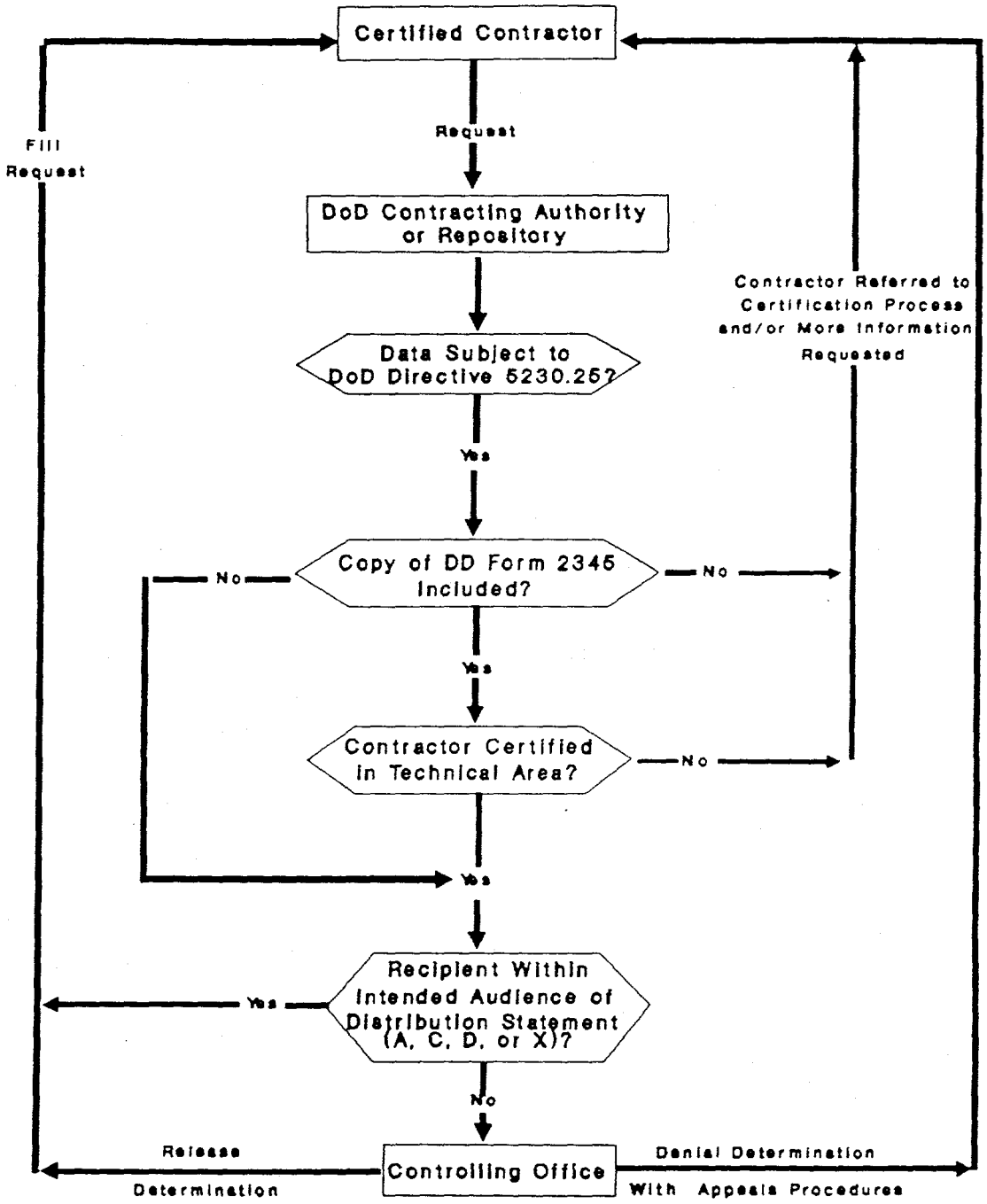

Certified Contractor
Request
DoD Contracting Authority or Repository
Data Subject to DoD Directive 5230.25?
Yes
Copy of DD Form 2345 Included?
No
No
Yes
Contractor Certified in Technical Area?
No
Yes
Recipient Within Intended Audience of Distribution Statement (A, C, D, or X)?
Yes
No
Controlling Office
Release Determination
Denial Determination With Appeals Procedures
Fill Request
Contractor Referred to Certification Process and/or More Information Requested

Figure 3

Requests For DND-Controlled Technical Data

Certified contractors obtain DND-controlled technical data by submitting a request to the International Programmes Division at the following address:

Directorate-General of International Programs
Attention: DDSS
National Defence Headquarters
MGen George Pearkes Bldg.
Ottawa, CANADA K1A 0K2

A copy of the JCO-approved DD Form 2345 should accompany all requests for DND-controlled technical data. **Figure 4** shows the review procedures that are in place to process requests for DND- controlled technical data.

Requesting DND-Controlled Technical Data From DSIS

Certified Canadian contractors that are registered with the Directorate Scientific Information Services (DSIS) should request DND-controllled technical data, the distribution of which is administered by DSIS, directly from the DSIS at the following address:

Customer Services Centre
Directorate Scientific Information Services (DSIS),
National Defence Headquarters
MGen Pearkes Bldg.
Ottawa, CANADA K1A 0K2

Certified U.S. contractors should request DSIS-administered unclassified technical data through the Defense Technical Information Center (DTIC) at the address shown on page 8.

Responding to DSS Requests for Proposals and Requests for Quotes

Certified contractors should request unclassified Requests for Proposals (RFP) and Requests for Quotes (RFQ) that involve unclassified technical data directly from the DSS procurement office.

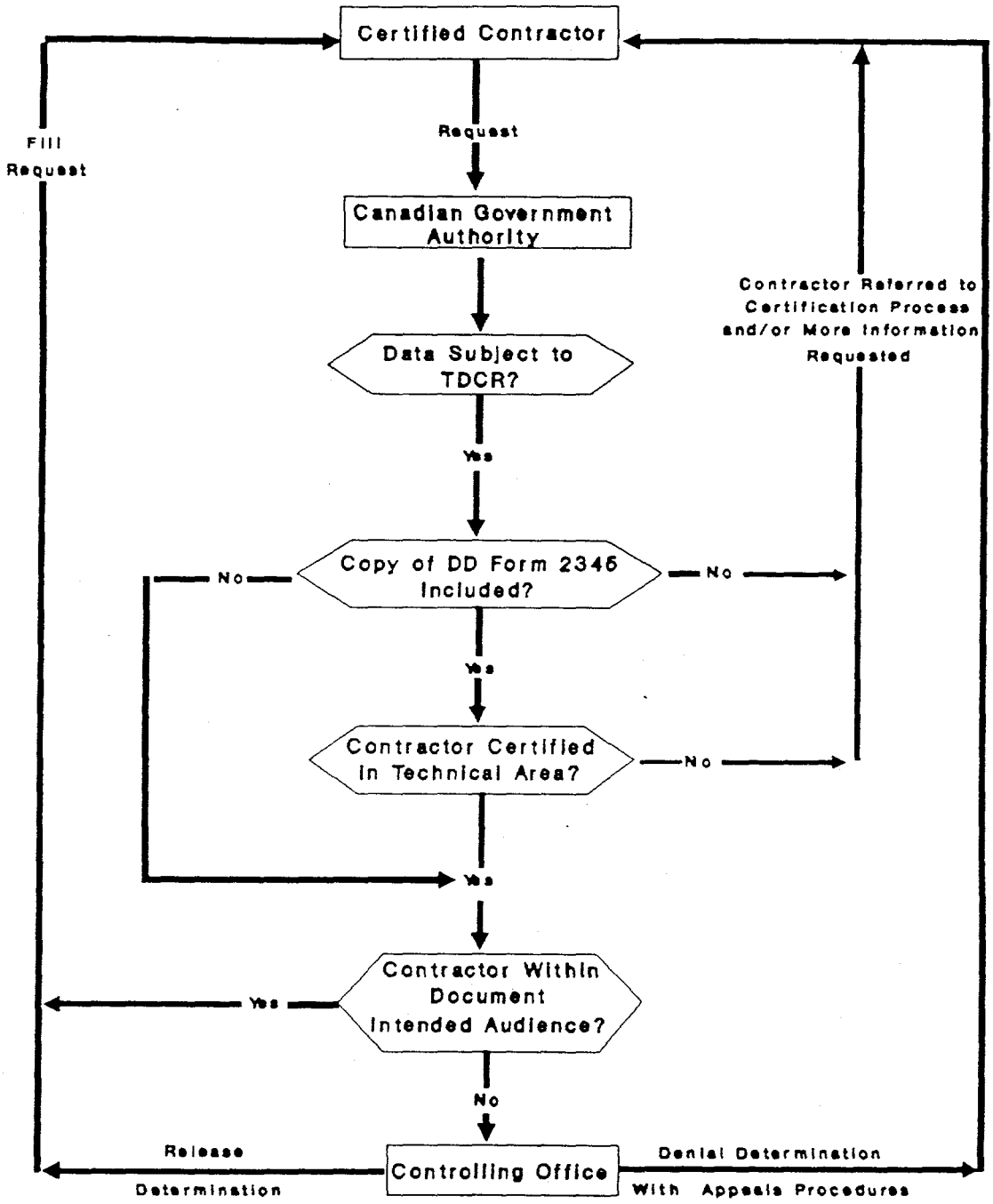

Certified Contractor
Request
Canadian Government Authority
Data Subject to TDCR?
Yes
Copy of DD Form 2345 Included?
No
No
Yes
Contractor Certified in Technical Area?
No
Yes
Contractor Within Document Intended Audience?
Yes
No
Controlling Office
Release Determination
Denial Determination With Appeals Procedures
Fill Request
Contractor Referred to Certification Process and/or More Information Requested

Figure 4

Denial of a Request for Technical Data

When a U.S. or Canadian Government agency denies access to unclassified technical data, the certified contractor will be provided an explanation of applicable procedures to request a reconsideration of the denial, and, subject to security considerations, the reasons for denial.

VI. ACCESS BY FOREIGN PARENT OR FOREIGN SUBSIDIARY

Participation in the JCP is restricted to individuals and enterprises that are located in the U.S. or Canada. Where a parent-subsidiary relationship exists between two companies, and the parent or subsidiary is located in a country other than the U.S. or Canada, such parent or subsidiary and its employees are not authorized access to any DoD or DND-controlled technical data which a certified U.S. or Canadian contractor has obtained under the provisions of the JCP without prior written government approval. This approval may be provided in the form of an export license obtained from the appropriate export control authority or dissemination authorization granted by the controlling office.

VII. DOCUMENT MARKINGS

Document markings will be applied to all documents released under the provisions of the JCP. These markings include those described below. An example of a DoD marking for a Distribution X document containing export-controlled technical data is shown at **Figure 5.**

Export Control Warning Notice

DoD documentation released pursuant to a JCO-approved certification will have a specific **EXPORT CONTROL WARNING NOTICE** and a **DISTRIBUTION STATEMENT** affixed to the front of the document. The Export Control Warning Notice is intended to remind recipients that the documentation was obtained under their Militarily Critical Technical Data Agreement (DD Form 2345) and may not be exported without an export license or other authorization, as applicable, unless permitted under the International Traffic in Arms Regulations (ITAR) exemptions outlined in **Appendix D.**

Documents that have an Export Warning Statement may be released outside the DoD only to companies and individuals who have made certifications in accordance with DoD Directive 5230.25, using DD Form 2345. Export controls are separate and distinct from Distribution Statements (**see Appendix A**).

DND documentation released pursuant to a JCO-approved certification will have a **DOCUMENT CONTROL WARNING NOTICE** affixed to the front of the document. The Document Control Warning Notice is intended to remind recipients that the documentation may not be further disseminated without the written authority of the DND. **Figure 6** shows the marking affixed to DND documentation.

EXAMPLE OF AN EXPORT CONTROL WARNING NOTICE AND A DISTRIBUTION STATEMENT

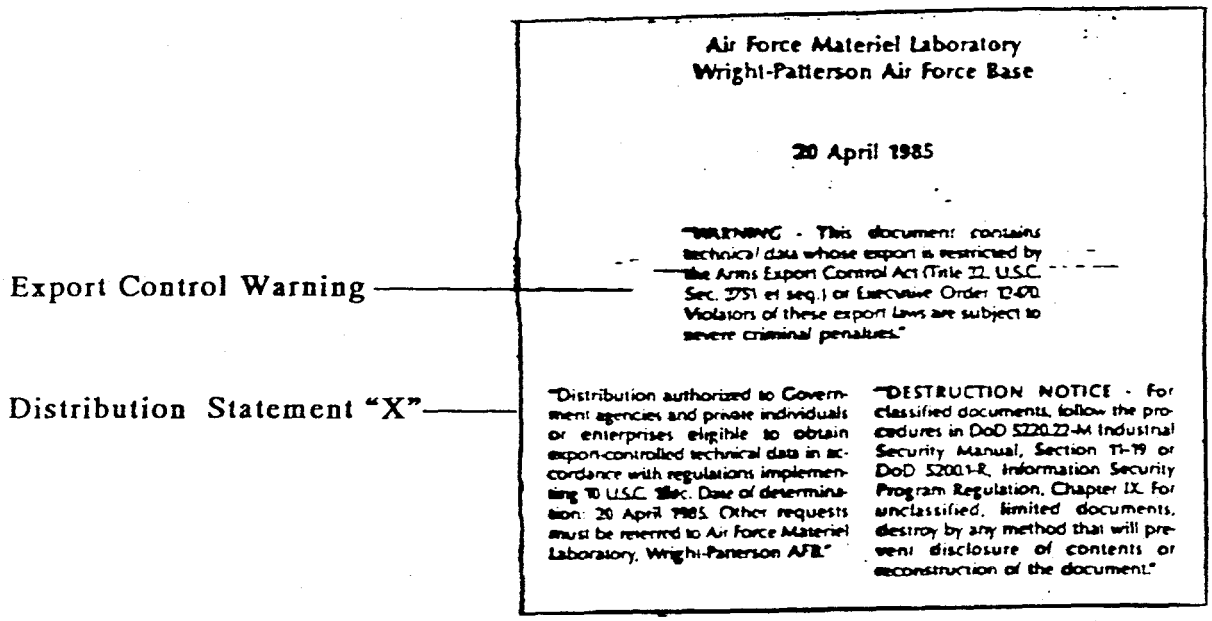


Figure 5

DND DOCUMENT CONTROL WARNING NOTICE

This document is furnished with the express understanding that:

a. it is for the use of the recipient only in the performance of the requirement for which it was requested, and shall not be disseminated further without the written authority of the Department of National Defence, Canada;

b. it shall be given adequate protection to prevent disclosure to unauthorized persons; and

c. improper or unauthorized disclosure of this information may result in one or both of the following:

- loss of certification in both the United States and Canada; and

- prosecution under section 21 of the Defence Production Act.

Figure 6

Destruction Notice

Documents containing unclassified technical data will also bear a notice to the effect that destruction of the document is authorized provided that the method selected will prevent disclosure of the content or reconstruction of the document.

Distribution Statements

Distribution statements are used by controlling offices to authorize secondary distribution to specific audiences. Controlling offices reserve the right to make determinations on all requests from outside the intended audience. The distribution statements are discussed in greater detail at Appendix A.

Contractor Imposed Distribution Statements

In addition to the above markings, contractors may apply markings to control the dissemination of technical data to which the U.S. and Canadian governments have limited rights.

VIII. CERTIFICATION VIOLATIONS

Violation of the certification agreement can result in one or all of the following:

a. Loss of certification in both the U.S. and Canada. Once certification is lost, the contracting facility becomes ineligible to receive controlled technical data from both the U.S. and Canada;

b. Liability to sanction (fine or imprisonment) under Part 127 of the ITAR for certified U.S. contractors;

c. Liability to sanction (fine or imprisonment) under Section 21 of Canada's Defense Production Act for certified Canadian contractors;

IX. INQUIRIES

Individuals or enterprises wishing to obtain more information regarding the U.S./Canada Joint Certification Program should contact the Joint Certification Office at 1-800-352-3572 (USA only), or (616) 961-7431 (Canadian Representative), or (616) 961-4358 (U.S. Representative) or direct the inquiry to the following address:

U.S./Canada Joint Certification Office
Defense Logistics Services Center
Federal Center
74 N. Washington
Battle Creek, Michigan 49017-3084

APPENDIX A

DOD DISTRIBUTION STATEMENTS

DoD Distribution Statements authorize secondary document dissemination organizations, such as libraries and data repositories, to release documentation containing DoD-controlled technical data to other eligible recipients. All requests from outside the audience described in the statement are to be referred to the DoD controlling office for a release decision. DoD controlling offices make release determinations considering all applicable laws and regulations.

All contractors certified by the U.S.-Canada Joint Certification Office (JCO) are authorized access to DoD- controlled documents bearing Distribution Statements "A" or "X" as follows:

DISTRIBUTION STATEMENT "A"

"Approved for public release; distribution unlimited."

DISTRIBUTION STATEMENT "X"

"Distribution authorized to U.S Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with regulations implementing 10 U.S.C. 140c (date of determination). Other requests must be referred to (insert controlling DoD office)."

Certified contractors who are supporting U.S. Government agencies are eligible to receive unclassified documents bearing Distribution Statement "C":

DISTRIBUTION STATEMENT "C"

"Distribution authorized to U.S. Government agencies and their contractors (reason for restriction) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)."

If there is a contract with DoD, the certified contractors are eligible to receive unclassified documents bearing Distribution Statement "D":

DISTRIBUTION STATEMENT "D"

"Distribution authorized to the Department of Defense and DoD contractors only (reason for restriction) (date of determination). Other requests shall be referred to (insert controlling DoD office)."

However, if the reason for restriction in Distribution Statement "C" or "D" specifies that the document contains "foreign government" or "company proprietary" information, written consent must be obtained from the owners of the information before release.

Distribution to anyone outside the U.S. Government of unclassified technical documents bearing the following Distribution Statements requires the permission of the DoD controlling office:

DISTRIBUTION STATEMENT "B"

"Distribution authorized to U.S. Government agencies only (reason for restriction) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)."

DISTRIBUTION STATEMENT "E"

"Distribution authorized to the DoD Components only (reason for restriction) (date of determination). other requests shall be referred to (insert controlling DoD office)."

DISTRIBUTION STATEMENT "F"

"Further dissemination only as directed by (insert controlling DoD office) (date of determination) or higher DoD authority."

The Table at Figure 7 shows the intended audience for Distribution Statements A, C, D, and X. The guidelines provided in the Table allow secondary distribution organizations to serve the broadest audience possible without the need to consult controlling offices for instructions.

INTENDED AUDIENCE	DOCUMENTATION DISTRIBUTION STATEMENTS
Certified contractors	A,X
Certified contractors doing business with the U.S. Government	A,C,X
Certified contractors doing business with the Department of Defense	A,C,D,X

Figure 7

APPENDIX B

DIRECTLY ARRANGED VISITS (DAV)

DoD Criteria for DAV

A DAV to a DoD contractor or military facility is permitted when the following two conditions are satisfied:

1. First condition:

a. There is a valid license covering the export of the data; or

b. The export or release is permitted under the exemptions in Part 125.4 or 126.5 of the ITAR (see Appendix D); or

c. The export or release qualifies for a General License under the Export Administration Regulations (EAR); and

2. Second condition:

a. The distribution statement applied to the data pursuant to DoD Directive 5230.24 permits release; or

b. The controlling office authorizes release.

DAV to DoD Contractor Facilities

Canadian contractors that are registered with the JCO are authorized to make unclassified visit arrangements directly with the DoD contractor concerned.

When release of the data is not authorized under the above DoD criteria for a DAV, it is the responsibility of the U.S. contractor to notify the proposed Canadian visitor that the requested visit does not meet the requirement for a DAV and that an official request through the Canadian Embassy is required.

DAV to DoD Military Facilities

Canadian Government officials and certified Canadian contractors wishing to initiate an unclassified visit to a U.S. military facility should make arrangements directly with the security office at the concerned facility. DAV to DoD military facilities may be conducted for the purpose of:

a. collecting or discussing unclassified solicitations; or

b. in furtherance of procurement activities related to unclassified solicitations (e.g. pre-solicitation conferences).

By regulation, the host agency head or facility commander retains final approval authority for any visit and may deny it at any time for security or operational purposes.

Meetings, Conferences and Symposia

Certified Canadian contractors and Canadian government officials will normally be admitted to meetings, conferences and symposia where technical data governed by DoD Directive 5230.25 will be presented. However, if such an event contains information that does not fall under the ITAR exemption for Canada, the sponsor should obtain approval from the appropriate DoD authority to release the information in question to Canadian participants, or, if release approval is denied, exclude Canadians from participation.

DAV to Canadian Contractor Facilities

U.S. and Canadian contractors that are registered with the JCO are authorized to make unclassified visit arrangements directly with the Canadian contractor concerned when release of the data is governed by the Technical Data Control Regulations.

DAV to DND Military Facilities

A DAV to a DND military facility is permitted when the visit involves UNCLASSIFIED technical data that are subject to the provisions of the Technical Data Control Regulations and the visit is conducted for the purpose of:

a. collecting or discussing unclassified solicitations; or

b. in furtherance of a procurement activity related to unclassified solicitations (e.g. pre-solicitation conferences).

When these criteria are met, no requirement exists for certified U.S. and Canadian contractors to submit formal Visit Clearance Requests through either the U.S. Defense Investigative Service Cognizant Office (DISCO) or the Industrial and Corporate Security Branch of Supply and Services Canada.

U.S. Government officials and certified U.S. contractors wishing to initiate a JCP-related unclassified visit to a DND facility should make arrangements directly with the DND officials they wish to visit. Before the visit may proceed, the DND official to be visited must agree to the visit and confirm that it complies with any local access requirements applicable to the DND facility being visited.

APPENDIX C

GUIDELINES FOR CONTRACTOR EXPORT OF UNCLASSIFIED TECHNICAL DATA

U.S. Prime Contractor to Canadian Subcontractor

Canadian contractors who are subcontractors to a U.S. prime contractor on a DoD contract may request unclassified technical data directly from the U.S. prime contractor. If the information is not releasable to the Canadian subcontractor in accordance with U.S. export control laws and regulations and/or DoD document distribution statements, the U.S. prime should inform the Canadian subcontractor that it should request the technical data directly from the DoD contracting authority. If it so desires, the DoD contracting authority, in accordance with the ITAR, may direct the U.S. prime to release the technical data to the Canadian subcontractor.

U.S. prime contractors may retransmit DoD unclassified technical data to Canadian subcontractors to use for government purposes provided:

a. The exporter has determined that the Canadian recipient is qualified under the Distribution Statements found in DoD Directive 5230.24 (see Appendix A).

b. The Canadian recipient has been certified by the Joint Certification Office in Battle Creek.

c. The exporter has determined that the technical data involved does not contain detailed design or manufacturing data, to include unique hardware or software processing technology, unless there is an existing Technical Assistance or Manufacturing License Agreement covering the specific data. Unclassified technical data may not be exported by Canadian companies to a non-U.S. destination without prior U.S. Government approval.

d. The exporter files a Shipper's Export Declaration (Department of Commerce Form 7525-V) with the District Director of Customs at the port of exit. The exporter must certify that the export is exempt from the licensing requirements by writing "22 CFR _" (with the applicable section of ITAR) on the shipper's export declaration. A copy of each declaration must be mailed immediately by the exporter to the Office of Defense Trade Controls, Department of State. An export declaration is not required if the shipment is pursuant to a U.S. Government sponsored program. When the technical data are subject to a case-by-case review before release, the exporter also should provide a brief summary of the data transferred to include its intended end-use and end-user to the Office of the Director, Defense Technology Security Administration ATTN: Munitions Control Directorate, Department of Defense. This will allow the Munitions Control Directorate to record the transaction in FORDTIS (Foreign Disclosure Technical Information System) database.

If for any reason, a U.S. prime contractor is not sure whether certain unclassified technical data may be exported to Canada without a license, it should obtain an advisory opinion from the Office of Defense Trade Controls, Department of State.

Canadian Prime Contractor to U.S. Subcontractor

U.S. contractors who are subcontractors to a Canadian prime contractor on a DND contract may request unclassified technical data directly from the DSS contracting authority or they may obtain it through the Canadian prime contractor.

Canadian prime contractors may transfer DND-controlled unclassified technical data to U.S. subcontractors to support a DND contract provided the following conditions are satisfied:

a. The technical data are governed by the TDCR;

b. The U.S. recipient has been certified by the Joint Certification Office;

c. The intended use of the technical data falls within the scope of the business activity as stated on the subcontractor's certification; and

d. Written consent is obtained from the DND controlling office prior to releasing technical data that contain third party information, such as foreign government, company proprietary, or limited rights information.

A Canadian prime contractor may request assistance from the DND controlling office in making a release determination.

APPENDIX D

LICENSING EXEMPTIONS

Canadian Exemption Under U.S. Export Control Law

In general, unclassified munitions list equipment and technical data may be exported to Canada without a license or other authorization for end-use in Canada or return to the United States with the exception of the articles and technical data listed below (Part 126.5 of the International Traffic in Arms Regulations (ITAR), Department of State).

a. Fully automatic firearms in Category 1(a) of the U.S. Munitions List which are not for end-use by the Federal Government, or a Provincial or Municipal Government of Canada;

b. Nuclear weapons strategic delivery systems and all components, parts, accessories or attachments specifically designed for such systems and associated equipment;

c. Nuclear weapon design and test equipment listed in Munitions List Category XVI;

d. Naval nuclear propulsion equipment listed in Munitions List Category VI(e);

e. Aircraft listed in Munitions List Category VIII(a);

f. Submersible and oceanographic vessels and related articles in Munitions List Category XX(a) through (d);

g. Technical data that can be used for manufacturing purposes except in furtherance of a technical assistance agreement (TAA) or manufacturing license authorized pursuant to part 124.3 of the ITAR.

A license (or, in some cases, another license) is not required if the export or release of unclassified technical data falls under one of the following general exemptions (Part 125.4 of the ITAR).

a. Technical data to be disclosed pursuant to an official written request or directive from the U.S. Department of Defense.

b. Technical data in furtherance of a manufacturing license or technical assistance agreement approved by the Department of State provided that data does not exceed the scope and limitations of the relevant agreement.

c. Technical data in furtherance of a contract between the exporter and an agency of the U.S. Government, if the contract provides for the export of the relevant technical data, and such data does not disclose the details of design, development, production, or manufacture of any defense article.

d. Copies of technical data previously authorized for export to the same recipient. Revised copies of such technical data are also exempt if they pertain to the identical defense article, and if the revisions are solely editorial and do not add to the content of technology previously exported or authorized for export to the same recipient.

e. Technical data in the form of basic operations, maintenance, and training information relating to a defense article lawfully exported or authorized for export to the same recipient. This exemption applies only to exports by the original exporter.

f. Technical data related to firearms not in excess of caliber .50 and ammunition for such weapons, except detail, design, development, production or manufacturing information.

g. Technical data being returned to the original source of import.

h. Technical data directly related to classified information which has been previously exported or authorized for export to the same recipient, and which does not disclose the details of the design, development, production, or manufacture of any defense article.

i. Technical data sent by a U.S. corporation to a U.S. government agency. (This exemption is subject to limitations in Section 125.1 (b) of the ITAR).

j. Technical data for which the exporter, pursuant to an arrangement with the Department of Defense or NASA which requires such export, has been granted an exemption in writing from licensing provisions by the Office of Defense Trade Controls. Such an exemption will normally be granted only if the arrangement directly implements an international agreement to which the United States is a party and if multiple exports are contemplated.

k. Technical data approved for public release (i.e., unlimited distribution) by the cognizant U.S. Government department agency.

l. Unclassified technical data disclosed during a plant visit approved by the Office of Defense Trade Controls or a U.S. Government agency provided the documents do not contain technical data in excess of that approved for oral and visual disclosure.

Export to Canada of classified equipment and data, and manufacturing license, technical assistance, and distribution agreements must be approved by the Office of Defense Trade Controls, Department of State.

U.S. Exemption Under Canadian Export Control Law

Under Canadian law, export of DND-controlled technical data that are subject to the TDCR to certified U.S. contractors does not require an export permit or license from the Export Control Division at the Department of External Affairs.

APPENDIX E

DEFINITIONS

Certified Contractor. A private individual or enterprise who is located in the United States or Canada and who has been approved for access to export-controlled technical data in the possession of, or under the control of DoD or DND. Access to DoD-controlled technical data is granted under the authority of DoD Directive 5230.25, and access to DND-controlled technical data is granted under the authority of Canada's Technical Data Control Regulations (TDCR).

Controlling Office. The DoD or DND activity that sponsors the work that generates the technical data or the office that receives the technical data on behalf of a Government agency and has the responsibility for distributing the data to eligible recipients.

Critical Technology. Technologies that consist of:

a. arrays of design and manufacturing know-how (including technical data);

b. keystone manufacturing, inspection, and test equipment;

c. keystone materials; and

d. goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States or Canada (also referred to as militarily critical technology).

Export Administration Regulations (EAR). The EAR, which is administered by the Bureau of Export Administration, U.S. Department of Commerce, implements the Export Administration Act of 1979. The EAR controls export of dual use items (materials with both civilian and military uses) specified on the Control List and technical data as defined in the regulations.

International Traffic in Arms Regulations (ITAR). The ITAR, which is administered by the Office of Defense Trade Controls, U.S. Department of State, implements the U.S. Arms Export Control Act. The ITAR controls export of defense articles specified on the U.S. Munitions List and technical data directly related to them.

Technical Data with Military or Space Application/ Technical Data. Any blueprints, drawings, plans, instructions, computer software and documentation, or other technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

APPENDIX F

ABBREVIATIONS

DD	Department of Defense
DGIP	Directorate General International Programmes
DLSC	Defense Logistics Services Center
DND	Department of National Defence
DOD	Department of Defense
DSIS	Directorate Scientific Information Services
DSS	Department of Supply and Services
DTIC	Defense Technical Information Center
EAR	Export Administration Regulations
ITAR	International Traffic in Arms Regulations
JCO	Joint Certification Office
JCP	Joint Certification Program
MAS	Ministere Approvisionnements et Services
MOU	Memorandum of Understanding
RFP	Request for Proposal
STI	Scientific and Technical Information
US	United States

APPENDIX G

REFERENCES

1. DoD Directive 2040.2, International Transfers of Technology, Goods, Services, and Munitions.

2. DoD Directive 5230.24, Distribution Statements on Technical Documents.

3. DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure.

4. International Traffic in Arms Regulations (ITAR), 22 C.F.R. 120-130.

5. Technical Data Control Regulations (TDCR), SOR/86-345, 20 March 1986.

6. United States-Canada Certification Program, Department of Supply and Services Supply Policy Manual Directive 3158.

7. Memorandum of Understanding (MOU) between the United States and Canada Concerning Strategic Technology Exchange, 13 December 1985.

8. Joint Terms of Reference for the United States-Canada Joint Certification Program, 13 May 1986 (appended to the MOU).

9. Title 10, U.S.C., section 130, as added by PL 98-94 "DoD Authorization Act of 1984," section 1217, September 24, 1983.

U.S./Canada Joint Certification Program

One result of a Memorandum of Understanding (MOU) signed after the 1985 Quebec Summit Declaration Regarding International Security was the establishment of the U.S./Canada Joint Certification Program. The establishment of the Joint Certification Program benefits U.S. and Canadian defense and high technology industries by facilitating their continued access to unclassified militarily critical technical data under the control of the U.S. Department of Defense or the Canadian Department of National Defence which is needed to perform on a government contract or support a legitimate business activity as defined in DoD Directive 5230.25, and in Canada's Technical Data Control Regulations (TDCR). As stated in the MOU's "Joint Terms of Reference for the United States-Canada Joint Certification Program", the Joint Certification Program was established "to certify contractors of each country for access, on an equally favorable basis, to unclassified technical data disclosing critical technology governed in the U.S. by DoD Directive 5230.25 and, in Canada, by the Technical Data Control Regulations (TDCR)."

The U.S./Canada Joint Certification Program is handled by the Joint Certification Office (JCO), Defense Logistics Service Center, Federal Center, 74 N. Washington Avenue, Battle Creek, Michigan 49017-3084. The JCO receives and processes certification forms submitted by contractors of each country who wish to obtain access to unclassified militarily critical technical data from the Military Departments of the two countries.

1. Authorized Canadian access to DoD-Controlled Militarily Critical Technical Data.

The information dissemination and control procedures set forth in DoDD 5230.24 and DoDD 5230.25 for DoD-held data are in place to support contractors doing business with the Department of Defense or for other legitimate business activities in which the contractors are engaged, or plan to become engaged. To the extent that Canadian contractors require access to technical data for this purpose, they should be treated no differently from U.S. contractors, subject to the constraints described below.

The technical data that are directly releasable to certified Canadian entities, without the need for a license, must fall within the exemption for Canada under Part 126 of the ITAR. Canadian contractors would have access to unclassified documents available to contractors through libraries and technical data repositories. Technical data that have a Distribution Statement "A" may be obtained by the general public. Canadian contractors and individuals certified by the JCO would also have access to technical data that have a Distribution Statement "X". Canadian contractors who are supporting U.S. Government agencies would have access to unclassified documents with Distribution Statement "C". If their contract was with DoD, they also would be eligible for unclassified documents with Distribution Statement "D". However, if the Distribution Statement "C" or "D" specifies that the document contains "foreign government information" or "proprietary information", written consent must be obtained from the owners before release. Documentation with any other kind of Distribution Statement other than those listed above (e.g., "B", "E", "F") must have the written permission of the controlling office for release. A chart showing the "intended audience" (See Definitions) of Distribution Statements found in DoD Directive 5230.24 is attached.

2. Authorized U.S. Access to DND-Controlled Militarily Critical Technical Data

The information dissemination and control procedures set forth in the TDCR are in place to support certified contractors doing business with Canada's Department of National Defence or for other legitimate business activities in which the contractors are engaged, or plan to become engaged. To the extent that U.S. contractors require access to technical data for this purpose, they should be treated no differently from Canadian contractors.

3. Impact of the U.S./Canada Joint Certification Program on U.S. and Canadian Contractors.

U.S. and Canadian contractors who wish to receive militarily critical technical data from either the Department of Defense or the Department of National Defence must become certified by the Joint Certification Office.

Certified U.S. and Canadian contractors who are not doing business with the U.S. Government are eligible to receive DoD Distribution Statement "A" and Distribution Statement "X" technical data only. Certified U.S. and Canadian contractors may purchase unclassified/uncontrolled technical data (Distribution Statement "A") from the National Technical Information Service (NTIS) and technical data with a Distribution Statement "X" from one of DoD's technical data repositories.

THE U.S.-CANADA JOINT CERTIFICATION PROGRAM DIRECTLY ARRANGED VISITS (DAV)

I. Introduction:

In 1985, the United States and Canada signed a Memorandum of Understanding (MOU) that established the U.S.-Canada Joint Certification Program. As stated in the MOU's "Joint Terms of Reference for the United States-Canada Joint Certification Program," the program was established "to certify contractors of each country for access, on an equally favorable basis, to unclassified technical data disclosing critical technology." This information is controlled in the U.S. by DoD Directive 5230.25 and, in Canada, by the Technical Data Control Regulations (TDCR). Under each Nations' laws, the U.S. Department of Defense and Canada's Department of National Defence may withhold such technical data from public disclosure.

To ensure that the goals of the 1985 MOU are realized, the United States and Canada have agreed that the certification process can be used to facilitate visits that involve access to unclassified technical data. The procedures discussed in this paper have been developed to permit directly arranged visits (DAV) by Canadian Government officials and certified Canadian contractors to DoD contractor facilities. Canadian authorities have developed similar procedures that permit DAVs by U.S. officials and contractors to Canadian contractor facilities.

II. Conditions for a Directly Arranged Visit (DAV):

A directly arranged visit (DAV) is permitted when the following two conditions are satisfied:

1. First condition:

a. There is a valid license covering the export of the data; or

b. The export or release is permitted under the Canadian exemption in Part 126.5 of the International Traffic in Arms Regulations (ITAR) (see Section V.1., Canadian Exemptions, below); or

c. The export or release is covered by the general exemptions in Part 125.4 of the ITAR (see Section V.2., General Exemptions, below); or

d. The export or release qualifies for a General License under the Export Administration Regulations (EAR); and

2. Second condition:

a. The distribution statement applied to the data pursuant to DoD Directive 5230.24 permits release (see Section VI., Technical Data Markings, below); or

b. The originator or U.S. Government controlling office authorizes release.

III. U.S. Contractor Responsibilities:

a. In the case of unclassified visits to DoD contractor facilities, it is the responsibility of the U.S. contractor to notify potential Canadian visitors if a proposed visit meets the conditions for a DAV or if an official visit request must be submitted through government channels.

b. When a U.S. contractor sponsors any meetings, conferences and symposia, at which controlled unclassified technical data will be presented or discussed, and Canadian participation is anticipated or requested, it is the responsibility of the U.S. contractor to ensure that the information provided at the meeting is releasable to Canadian Government officials and certified Canadian contractors. The conditions listed in paragraph II., above, apply.

c. Certified U.S. contractors wishing to initiate an unclassified visit to a certified Canadian contractor or Canadian military installation should make arrangements with the contractor security office or the DND personnel they wish to visit. DAVs to military installations may be conducted only for the purpose of:

(1) collecting or discussing unclassified solicitations; or

(2) in furtherance of procurement activity related to unclassified solicitations (e.g., pre-solicitation conferences).

By Canadian regulation, the installation commander retains final approval authority for any visit and may deny it for security or operational reasons.

IV. Procedures for Processing Requests for Visits and Documentation

Upon receipt of a request for a visit which will involve the release of unclassified technical data to Canadian officials or certified Canadian contractors, the recipient U.S. contractor security office will:

a. if the requestor is a government official, verify identity and status prior to release of information; if the requestor is a contractor, verify that the purpose falls within the scope of the business activity stated in the requestor's certification, DD Form 2345, which must accompany all requests;

b. determine whether the information is releasable under the Canadian exemption in Part 126.5 of the ITAR or the general exemptions in Part 125.4 of the ITAR, or under a General License;

c. if the data bears a distribution statement, determine whether release is authorized or whether release must be approved by the originator or U.S. Government controlling office (e.g., the requestor is outside the intended audience).

d. if release requires approval of a license or other written approval, action should be initiated to obtain approval and the requestor should be notified of such action.

V. Licensing Exemptions

1. Canadian Exemptions (Part 126.5 of the ITAR).

In general, unclassified articles and technical data may be exported to Canada without a license or other authorization, for end-use in Canada or return to the United States, with the exception of the articles and technical data listed in subparagraphs a. through g., below. If the data to be released during the proposed visit is included in subparagraphs a. through g., a valid export license or approved visit request is necessary, unless release is permitted under a general exemption described in paragraph 2. below.

a. Fully automatic firearms in Category 1(a) of the U.S. Munitions List which are not for end-use by the Federal Government, or a Provincial or Municipal Government of Canada;

b. Nuclear weapons strategic delivery systems and all components, parts, accessories or attachments specifically designed for such systems and associated equipment;

c. Nuclear weapon design and test equipment listed in Munitions List Category XVI;

d. Naval nuclear propulsion equipment listed in Munitions List Category VI(e);

e. Aircraft listed in Munitions List Category VIII(a);

f. Submersible and oceanographic vessels and related articles in Munitions List Category XX(a) through (d);

g. Technical data that can be used for manufacturing purposes except in furtherance of a technical assistance agreement (TAA) or manufacturing license authorized pursuant to part 124.3 of the ITAR.

2. General Exemptions (Part 125.4 of the ITAR).

A license (or, in some cases, an additional license) is not required if the export or release of unclassified technical data falls under one of the following general exemptions.

a. Technical data to be disclosed pursuant to an official written request or directive from the U.S. Department of Defense.

b. Technical data in furtherance of a manufacturing license or technical assistance agreement approved by the Department of State provided that data does not exceed the scope and limitations of the relevant agreement.

c. Technical data in furtherance of a contract between the exporter and an agency of the U.S. Government, if the contract provides for the export of the relevant technical data, and such data does not disclose the details of design, development, production, or manufacture of any defense article.

d. Copies of technical data previously authorized for export to the same recipient. Revised copies of such technical data are also exempt if they pertain to the identical defense article, and if the revisions are solely editorial and do not add to the content of technology previously exported or authorized for export to the same recipient.

e. Technical data in the form of basic operations, maintenance, and training information relating to a defense article lawfully exported or authorized for export to the same recipient. This exemption applies only to exports by the original exporter.

f. Technical data related to firearms not in excess of caliber .50 and ammunition for such weapons, except detail, design, development, production or manufacturing information.

g. Technical data being returned to the original source of import.

h. Technical data directly related to classified information which has been previously exported or authorized for export to the same recipient, and which does not disclose the details of the design, development, production, or manufacture of any defense article.

i. Technical data sent by a U.S. corporation to a U.S. government agency. (This exemption is subject to limitations in Section 125.1 (b) of the ITAR).

j. Technical data for which the exporter, pursuant to an arrangement with the Department of Defense or NASA which requires such export, has been granted an exemption in writing from licensing provisions by the Office of Defense Trade Controls. Such an exemption will normally be granted only if the arrangement directly implements an international agreement to which the United States is a party and if multiple exports are contemplated.

k. Technical data approved for public release (i.e., unlimited distribution) by the cognizant U.S. Government department agency.

VI. Technical Data Markings

On unclassified DoD-controlled technical data look for two important markings, the **Export Warning Statement** and the **Distribution Statement**. The Export Warning Statement tells you that the data may be withheld from public disclosure under authority granted by Congress. The Distribution Statement identifies the users for whom the data is intended.

Unclassified technical data that has an Export Warning Statement may be released outside the Government only to companies and individuals who have executed certifications (DD Form 2345) in accordance with DoD Directive 5230.25 and Canada's TDCR. All non-Government recipients of technical data must describe their access requirements through certification by the U.S.-Canada Joint Certification Office, located in Battle Creek, Michigan, prior to obtaining information that is controlled by a Distribution Statement.

Distribution Statements authorize secondary document dissemination organizations (e.g., libraries and data repositories) to release the documentation to eligible recipients identified by the Distribution Statement. All requests from outside the intended audience are to be referred to the U.S. Government controlling office for action. Controlling offices make release determinations in accordance with applicable laws and regulations.

All contractors certified by the U.S.-Canada Joint Certification Office (JCO) are authorized access to technical data that have the following Distribution Statements "A" and "X":

Distribution Statement "A"

"Approved for public release; distribution unlimited."

Distribution Statement "X"

"Distribution authorized to U.S Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with regulations implementing 10 U.S.C. 140c (date of determination). Other requests must be referred to (insert controlling DoD office)."

Certified contractors who are supporting U.S. Government agencies also would have access to unclassified documents with Distribution Statement "C":

"Distribution authorized to U.S. Government agencies and their contractors (reason for restriction) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)."

If there is a contract with DoD, they also are eligible to receive unclassified documents with Distribution Statement "D":

"Distribution authorized to the Department of Defense and DoD contractors only (reason for restriction) (date of determination). Other requests shall be referred to (insert controlling DoD office)."

However, if the reason for restriction in Distribution Statement "C" or "D" specifies that the document contains "foreign government" or "company proprietary" information, written consent must be obtained from the owners before release.

Access by anyone outside the U.S. Government to documentation with the following Distribution Statements requires the permission of the controlling office:

Distribution Statement "B"

"Distribution authorized to U.S. Government agencies only (reason for restriction) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)."

Distribution Statement "E"

"Distribution authorized to the DoD Components only (reason for restriction) (date of determination). other requests shall be referred to (insert controlling DoD office)."

Distribution Statement "F"

"Further dissemination only as directed by (insert controlling DoD office) (date of dissemination) or higher DoD authority."

VII. Conclusion

Further explanation of the U.S.-Canada Joint Certification Program, which provides the foundation for DAVs, can be found in the soon to be published pamphlet on the U.S.-Canada Joint Certification Program. Contractors who have questions about whether specific DoD-controlled technical data is releasable through a DAV should contact the U.S. Government controlling office or originator cited on the document. Any questions about the U.S.-Canada Joint Certification Program should be directed to:

U.S.-Canada Joint Certification Office
Defense Logistics Services Center
Federal Center
74 N. Washington
Battle Creek, Michigan 49017-3084
Tel. (616) 961-4358 or (800) 352-3572

UNITED STATES-CANADA TECHNOLOGY SECURITY UNDER THE JOINT CERTIFICATION PROGRAM

PREPARED FOR CONSIDERATION BY THE U.S./CANADA TECHNOLOGY SECURITY SUBCOMMITTEE WORKING GROUP
JANUARY 18, 1990

PREPARED BY CYNTHIA STRINGHAM
ORION ENTERPRISES, INCORPORATED

UNITED STATES-CANADA TECHNOLOGY SECURITY UNDER THE JOINT CERTIFICATION PROGRAM

PREPARED FOR THE DEPARTMENT OF THE ARMY
BY ORION ENTERPRISES, INC.

BRIEFING

U.S./CANADA TECHNOLOGY SECURITY

UNDER THE

JOINT CERTIFICATION PROGRAM

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

AUTHORITY FOR THE JOINT CERTIFICATION PROGRAM (JCP)

- MEMORANDUM OF UNDERSTANDING CONCERNING STRATEGIC TECHNOLOGY EXCHANGE
  - SIGNED AFTER THE 1985 QUEBEC SUMMIT DECLARATION REGARDING INTERNATIONAL SECURITY

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

PURPOSE OF THE JCP

- "...TO CERTIFY CONTRACTORS OF EACH COUNTRY FOR ACCESS, ON AN EQUALLY RECIPROCAL BASIS, TO UNCLASSIFIED TECHNICAL DATA CONTROLLED BY DOD DIRECTIVE 5230.25 AND, IN CANADA, BY THE TECHNICAL DATA CONTROL REGULATIONS (TDCR)..." WHEN THAT DATA IS NEEDED TO DO BUSINESS WITH THE U.S. OR CANADIAN GOVERNMENT, OR FOR OTHER LEGITIMATE BUSINESS PURPOSES AS DEFINED IN DOD DIRECTIVE 5230.25 AND THE TDCR

(Source: "Joint Terms of Reference for the United States-Canada Joint Certification Program.")

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

SCOPE OF THE JCP

- THE JCP DIRECTLY AFFECTS BOTH NATIONS' SECURITY, CONTRACTING AND PROGRAM MANAGEMENT OFFICIALS AND HOW THEY TREAT U.S. AND CANADIAN CONTRACTORS IN THEIR EFFORT TO OBTAIN MILITARILY CRITICAL UNCLASSIFIED TECHNICAL INFORMATION GOVERNED BY DOD DIRECTIVE 5230.25 OR THE TDCR

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

AUTHORIZED CANADIAN ACCESS TO DOD-HELD TECHNICAL DATA (SEE DODD 5230.24)

- TECHNICAL DATA DIRECTLY RELEASABLE TO CERTIFIED CANADIAN ENTITIES WITHOUT A LICENSE MUST FALL WITHIN THE EXEMPTION FOR CANADA UNDER PART 126 OF THE ITAR
- TECHNICAL DATA WITH DISTRIBUTION STATEMENTS "A" AND "X" ARE AVAILABLE TO CERTIFIED CONTRACTORS
- TECHNICAL DATA WITH DISTRIBUTION STATEMENT "C" MAY BE OBTAINED BY CONTRACTORS SUPPORTING U.S. GOVERNMENT AGENCIES
- TECHNICAL DATA WITH DISTRIBUTION STATEMENT "D" MAY BE OBTAINED BY CONTRACTORS SUPPORTING DOD
- TECHNICAL DATA WITH DISTRIBUTION STATEMENTS "B", "E","F" (OR "C" OR "D" WHEN THE DATA CONTAINS "FOREIGN GOVT INFO" OR "PROPRIETARY INFO") MUST HAVE WRITTEN PERMISSION FOR RELEASE

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

IMPACT OF THE JCP ON U.S. AND CANADIAN CONTRACTORS

- U.S. AND CANADIAN CONTRACTORS WHO WISH TO RECEIVE UNCLASSIFIED MILITARILY CRITICAL TECHNICAL DATA CONTROLLED EITHER BY THE DOD OR THE CANADIAN GOVERNMENT MUST BECOME CERTIFIED BY THE JOINT CERTIFICATION OFFICE (JCO)

- SINCE THE PROGRAM'S INCEPTION IN 1986 13,418 U.S. CONTRACTORS AND 557 CANADIAN CONTRACTORS HAVE BECOME CERTIFIED BY THE JCO

- CERTIFIED U.S. AND CANADIAN CONTRACTORS ARE ELIGIBLE TO RECIEVE TECHNICAL DATA WITH DISTRIBUTION STATEMENT "X", WHICH THEY MAY PURCHASE FROM ONE OF DOD'S TECHNICAL DATA REPOSITORIES OR PUBLICLY AVAILABLE TECHNICAL DATA WHICH CAN BE PURCHASED FROM NTIS

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

REMINDER

- THE CANADIAN EXEMPTION OF PART 126 OF THE ITAR DOES NOT APPLY TO:
  - THOSE ITEMS LISTED IN PART 126.5(b) OF THE ITAR
  - TECHNICAL DATA THAT CAN BE USED FOR MANUFACTURING PURPOSES EXCEPT IN FURTHERANCE OF A TECHNICAL ASSISTANCE AGREEMENT (TAA) OR MANUFACTURING LICENSE AUTHORIZED PURSUANT TO PART 124.3 OF THE ITAR

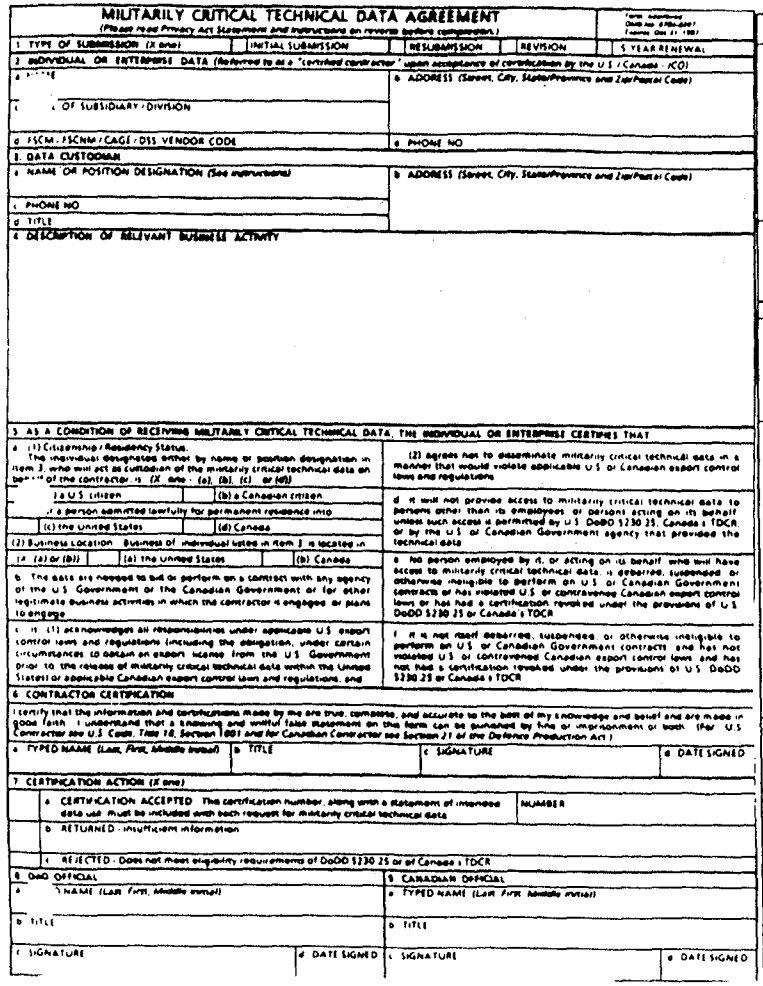
U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

IMPACT OF THE JCP ON U.S. AND CANADIAN GOVERNMENT AGENCIES

- U.S. AND CANADIAN GOVERNMENT AGENCIES THAT ARE "CONTROLLING OFFICES" FOR UNCLASSIFIED MILITARILY CRITICAL TECHNICAL DATA GOVERNED BY DODD 5230.25 OR THE TDCR MUST ENSURE THAT U.S. AND CANADIAN CONTRACTORS RECEIVING ACCESS TO SUCH TECHNICAL DATA ARE CERTIFIED BY THE JCO
- U.S. CONTROLLING OFFICES DETERMINE THE INTENDED AUDIENCE(S) FOR THE TECHNICAL DATA AND APPLY DISTRIBUTION STATEMENTS
    - LIBRARIES AND TECHNICAL DATA REPOSITORIES PROVIDE DOCUMENTS IN ACCORDANCE WITH THE DISTRIBUTION STATEMENTS
- CERTIFIED U.S. AND CANADIAN CONTRACTORS ARE GIVEN EQUAL STATUS WITHIN THE PROVISIONS OF THE ITAR AND DODD 5230.24

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

CERTIFICATION



MILITARILY CRITICAL TECHNICAL DATA AGREEMENT

(Please read Privacy Act Statement and instructions on reverse before completing.)

Form Approved (OMB No. 0704-0207) Expires Dec 31 1987

1. TYPE OF SUBMISSION (X one) — INITIAL SUBMISSION | RESUBMISSION | REVISION | 5 YEAR RENEWAL

2. INDIVIDUAL OR ENTERPRISE DATA (Referred to as a "certified contractor" upon acceptance of certification by the U.S./Canada JCO)

a. NAME
b. ADDRESS (Street, City, State/Province and Zip/Postal Code)
c. OF SUBSIDIARY/DIVISION
d. FSCM/FSCNM/CAGE/DSS VENDOR CODE
e. PHONE NO

3. DATA CUSTODIAN

a. NAME OR POSITION DESIGNATION (See instructions)
b. ADDRESS (Street, City, State/Province and Zip/Postal Code)
c. PHONE NO
d. TITLE

4. DESCRIPTION OF RELEVANT BUSINESS ACTIVITY

5. AS A CONDITION OF RECEIVING MILITARILY CRITICAL TECHNICAL DATA, THE INDIVIDUAL OR ENTERPRISE CERTIFIES THAT

a. (1) Citizenship/Residency Status. The individual designated either by name or position designation in item 3 who will act as custodian of the militarily critical technical data on behalf of the contractor is (X one - (a), (b), (c) or (d)):
(a) a U.S. citizen | (b) a Canadian citizen | (c) a person admitted lawfully for permanent residence into the United States | (d) Canada

(2) Business Location. Business of individual listed in item 3 is located in (X (a) or (b)): (a) the United States | (b) Canada

b. The data are needed to bid or perform on a contract with any agency of the U.S. Government or the Canadian Government or for other legitimate business activities in which the contractor is engaged or plans to engage.

c. It is (1) acknowledges all responsibilities under applicable U.S. export control laws and regulations (including the obligation, under certain circumstances to obtain an export license from the U.S. Government prior to the release of militarily critical technical data within the United States) or applicable Canadian export control laws and regulations; and

(2) agrees not to disseminate militarily critical technical data in a manner that would violate applicable U.S. or Canadian export control laws and regulations.

d. It will not provide access to militarily critical technical data to persons other than its employees or persons acting on its behalf unless such access is permitted by U.S. DoDD 5230.25, Canada's TDCR, or by the U.S. or Canadian Government agency that provided the technical data.

e. No person employed by it, or acting on its behalf, who will have access to militarily critical technical data, is debarred, suspended, or otherwise ineligible to perform on U.S. or Canadian Government contracts or has violated U.S. or contravened Canadian export control laws or has had a certification revoked under the provisions of U.S. DoDD 5230.25 or Canada's TDCR.

f. It is not itself debarred, suspended, or otherwise ineligible to perform on U.S. or Canadian Government contracts and has not violated U.S. or contravened Canadian export control laws and has not had a certification revoked under the provisions of U.S. DoDD 5230.25 or Canada's TDCR.

6. CONTRACTOR CERTIFICATION

I certify that the information and certifications made by me are true, complete, and accurate to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (For U.S. Contractor see U.S. Code, Title 18, Section 1001 and for Canadian Contractor see Section 21 of the Defence Production Act.)

a. TYPED NAME (Last, First, Middle Initial) | b. TITLE | c. SIGNATURE | d. DATE SIGNED

7. CERTIFICATION ACTION (X one)

a. CERTIFICATION ACCEPTED. The certification number, along with a statement of intended data use, must be included with each request for militarily critical technical data. NUMBER
b. RETURNED - Insufficient information
c. REJECTED - Does not meet eligibility requirements of DoDD 5230.25 or of Canada's TDCR

8. DoD OFFICIAL

a. NAME (Last, First, Middle Initial)
b. TITLE
c. SIGNATURE | d. DATE SIGNED

9. CANADIAN OFFICIAL

a. TYPED NAME (Last, First, Middle Initial)
b. TITLE
c. SIGNATURE | d. DATE SIGNED

INSTRUCTIONS FOR COMPLETION OF DD FORM 2345

Privacy Act Statement

AUTHORITY: For U.S. individuals and enterprises: 10 USC, Section 140c, as added by PL 98-94, Section 1217, September 24, 1983, and implemented by DoDD 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984 (32 CFR Part 250).
For Canadian individuals and enterprises: Defence Production Act.

PRINCIPAL PURPOSE: To identify individuals and enterprises eligible to receive militarily critical technical data.

ROUTINE USE: To support decisions regarding dissemination or withholding of militarily critical technical data. Information provided on this form describing your business may be published from time to time for the benefit of other "certified contractors."

DISCLOSURE: Voluntary; however, failure to provide the information may result in a denial of access to militarily critical technical data.

Mail the original, completed copy of this form and any attachments to:

United States/Canada Joint Certification Office
Defense Logistics Services Center
Federal Center
Battle Creek, Michigan USA 49017-3084

SPECIFIC INSTRUCTIONS

1. Mark only one box. Mark "RESUBMISSION" only if your previous submission was returned or rejected. Mark "REVISION" (of a previously accepted submission) to show revised information, such as addresses or business description. Mark "5-YEAR RENEWAL" in response to a renewal notice from U.S./Canada JCO. When either the "REVISION" or "5-YEAR RENEWAL" box is marked, enter your current Certification Number in item 7.a.

2. a. For an individual, show full name (Last, First, Middle Initial). For an enterprise, show full name of corporate parent, or institution.

b. Enter the mailing address of the individual or enterprise making the certification. If a P.O. Box is used for mailing purposes, include street address as well.

Each corporate subsidiary or division that is to receive militarily critical technical data must be certified separately. If not applicable, so state.

d. For U.S. individual or enterprise, enter the Federal Supply Code for Manufacturers (FSCM) or Non-Manufacturers (FSCNM) or Commercial and Government Entity (CAGE) code assigned to the individual or enterprise making the certification. For a Canadian individual or enterprise, enter the Department of Supply and Services Vendor Code assigned to the individual or enterprise making the certification. If none, so state. If a subsidiary or division is certified, enter the organization's code.

e. Show telephone number of the certifying official identified in item 6, include the area code.

3. Show the name, address, phone number (including area code), and title of the individual who will receive militarily critical technical data and be responsible for its further dissemination. A position designation may be used only when conditions described in items 5.a. (1) and (2) are prerequisites for handling that position.

4. Describe the business activity of the entity identified in item 2 in sufficient detail for the U.S. or Canadian Government agency contracting the data to determine whether the militarily critical technical data which you may request from time to time are reasonably related to your stated business activity. For example, state that you design and construct high-pressure, high-volume hydraulic pumps for use in connection with aircraft control surfaces, do not state simply "hydraulic pumps." Provide concise statements within the space provided.

5. If certifications 5.a. and 5.f. cannot be made, provide (on a separate sheet) a description of any extenuating circumstances that may give sufficient reason to accept your certification.

6. If item 2 identifies an individual, that individual must sign. If item 2 identifies an institution or a corporate entity, a person who can legally obligate the enterprise to a contract must sign.

7. Explanation of Certification Action.

a. ACCEPTED. The U.S./Canada - JCO has assigned the individual or enterprise identified in item 2.a., a Certification Number which will identify the individual or enterprise as a "certified contractor" as defined in U.S. DoDD 5230.25 or in Canada's TDCR. The acceptance is valid for a period of five years from the acceptance date unless sooner revoked under the provisions of U.S. DoDD 5230.25 or Canada's TDCR. If at any time a certified contractor is unable to adhere to the conditions under which a certification was accepted, the contractor's certification is considered to be void, and the contractor will either submit a revised certification or surrender all militarily critical technical data obtained under this agreement to the data controlling offices specified on the documents.

b. RETURNED. Your submission did not contain all information required to process your certification. Please review any comments provided with the returned submission and resubmit in accordance with the applicable instructions.

c. REJECTED. Reasons for rejection include, for example, determination, a business activity that does not fall within the scope of U.S. DoDD 5230.25 or Canada's TDCR, or failure to make all of the required certifications.

ABBREVIATIONS

"DoD": Department of Defense
"DD": Department of Defense Directive
"Canada JCO": United States-Canada Joint Certification Office
"DSS": Department of Supply and Services
"TDCR": Technical Data Control Regulations
"Militarily Critical Technical Data": means unclassified technical data as governed by U.S. DoDD 5230.25 or Canada's TDCR

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

CERTIFIED CONTRACTORS MAY:

- REQUEST UNCLASSIFIED MILITARILY CRITICAL TECHNICAL DATA FROM LIBRARIES AND TECHNICAL DATA REPOSITORIES FOR DOD TECHNICAL DATA, AND FROM THE DIRECTORATE OF INTERNATIONAL PROGRAMS AT NATIONAL DEFENCE HEADQUARTERS FOR DND TECHNICAL DATA
- RESPOND TO DEFENSE-RELATED CONTRACTS WHOSE SPECIFICATIONS INVOLVE MILITARILY CRITICAL TECHNICAL DATA
- ATTEND RESTRICTED GATHERINGS WHERE UNCLASSIFIED TECHNICAL DATA GOVERNED BY DODD 5230.25 OR THE TDCR ARE PRESENTED
- ARRANGE UNCLASSIFIED VISITS DIRECTLY WITH OTHER CERTIFIED U.S. OR CANADIAN DEFENSE CONTRACTORS

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

REQUESTS FOR DOD-CONTROLLED TECHNICAL DATA

- U.S. AND CANADIAN CONTRACTORS SUBMIT REQUESTS FOR TECHNICAL DATA RELATED TO AN RFP DIRECTLY TO THE PROGRAM MANAGER

- U.S. AND CANADIAN CONTRACTOR REQUESTS FOR TECHNICAL DATA NOT RELATED TO AN RFP ARE SUBMITTED TO A LIBRARY OR TECHNICAL DATA REPOSITORY

- IF THE CONTRACTOR DOES NOT FALL INTO THE "INTENDED AUDIENCE" AS DEFINED BY THE DISTRIBUTION STATEMENT ON THE DOCUMENT, THE REQUEST WILL BE REFERRED TO THE APPROPRIATE CONTROLLING OFFICE FOR RELEASE AUTHORITY

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

REQUESTS FOR DND-HELD TECHNICAL DATA

- U.S. AND CANADIAN CONTRACTORS SUBMIT REQUESTS TO THE DIRECTORATE OF INTERNATIONAL PROGRAMS AT THE NATIONAL DEFENCE HEADQUARTERS IN OTTAWA

- U.S. AND CANADIAN CONTRACTORS SUBMIT REQUESTS FOR TECHNICAL DATA RELATED TO AN RFP DIRECTLY TO THE PROGRAM MANAGER

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

DENIAL OF A REQUEST

- SUBJECT TO SECURITY CONSIDERATIONS, THE GOVERNMENT AGENCY (U.S. OR CANADIAN) CONTROLLING THE TECHNICAL DATA PROVIDES CONTRACTOR WITH REASONS FOR DENIAL

- UPON REQUEST, THE GOVERNMENT AGENCY DENYING THE REQUEST WILL PROVIDE SPECIFIC REASONS FOR DENIAL TO THE CONTRACTOR'S GOVERNMENT

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

ADMITTANCE TO RESTRICTED GATHERINGS IN THE U.S. AND CANADA WHERE MILITARILY CRITICAL TECHNICAL DATA IS PRESENTED IS LIMITED TO-

- MILITARY PERSONNEL AND CIVILIAN EMPLOYEES OF THE U.S. AND CANADIAN GOVERNMENTS AND;

- REPRESENTATIVES OF U.S. AND CANADIAN CONTRACTORS CERTIFIED UNDER THE U.S./CANADA JOINT CERTIFICATION PROGRAM

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

BID/SOLICITATION CLAUSES

- BID OPPORTUNITIES SHOULD STIPULATE A REQUIREMENT FOR CERTIFICATION WHERE IT IS DETERMINED THAT THE RFP OR RFQ CONTAINS TECHNICAL DATA GOVERNED BY DODD 5230.25 OR THE TDCR

- BID PACKAGES, SUCH AS RFPS OR RFQS, SHOULD BE OBTAINED FROM THE PROGRAM MANAGER WITH RESPECT TO DOD BIDS AND FROM THE PROGRAM PROCUREMENT MANAGER AT CANADA'S DEPARTMENT OF SUPPLY AND SERVICES WITH RESPECT TO CANADIAN BIDS

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

UNCLASSIFIED VISITS TO CONTRACTOR INSTALLATIONS

- JANUARY 1989 DOD DECISION EXEMPTS CERTIFIED CANADIAN CONTRACTORS FROM THE NEED FOR DOD APPROVAL IN ORDER TO CONDUCT UNCLASSIFIED VISITS TO DOD CONTRACTOR INSTALLATIONS TO OBTAIN TECHNICAL DATA GOVERNED BY DODD 5230.25 OR THE TDCR

- CANADA'S INDUSTRIAL SECURITY PROCEDURES ALLOW DIRECT CONTRACTOR-TO-CONTRACTOR UNCLASSIFIED VISIT ARRANGEMENTS TO OBTAIN TECHNICAL DATA GOVERNED BY THE TDCR OR DODD 5230.25

- CONTRACTORS FROM BOTH NATIONS ARE STILL REQUIRED TO COMPLY WITH THE APPLICABLE LICENSING REQUIREMENTS OF THE COUNTRY FROM WHICH THE TECHNICAL DATA ORIGINATES

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

CONTRACTOR EXPORT OF MILITARILY CRITICAL TECHNICAL DATA

- CANADIAN CONTRACTORS WHO ARE SUBCONTRACTORS TO A U.S. PRIME ON A DOD CONTRACT MAY REQUEST UNCLASSIFIED MILITARILY CRITICAL TECHNICAL DATA DIRECTLY FROM THE DOD OR THEY MAY OBTAIN IT THROUGH THE U.S. PRIME CONTRACTOR

U.S./CANADA TECHNOLOGY SECURITY

JOINT CERTIFICATION PROGRAM

U.S. PRIME CONTRACTORS MAY RETRANSMIT DOD UNCLASSIFIED MILITARILY CRITICAL TECHNICAL DATA TO CANADIAN SUBCONTRACTORS TO USE PROVIDED:

- CANADIAN RECIPIENT IS ELIGIBLE UNDER THE DISTRIBUTION STATEMENTS FOUND ON THE DOCUMENTS
- THE TECHNICAL DATA DOES NOT CONTAIN DETAILED DESIGN OR MANUFACTURING DATA, TO INCLUDE UNIQUE HARDWARE OR SOFTWARE PROCESSING TECHNOLOGY UNLESS THERE IS AN EXISTING TECHNICAL ASSISTANCE AGREEMENT OR MANUFACTURING LICENSE
- THE EXPORTER FILES A SHIPPERS EXPORT DECLARATION (DOC FORM 7527-V) WITH THE DISTRICT DIRECTOR OF CUSTOMS AT THE PORT OF EXIT
- WHEN RELEASE AUTHORITY IS REQUIRED, THE EXPORTER PROVIDES A SUMMARY OF THE DATA TRANSFERRED, END USE AND END USER TO DTSA

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

EXPORTER'S RESPONSIBILITIES (CONT)

- CONTRACTORS WHO ARE UNSURE WHETHER CERTAIN UNCLASSIFIED MILITARILY CRITICAL TECHNICAL DATA MAY BE EXPORTED TO CANADA WITHOUT A LICENSE SHOULD REQUEST AN ADVISORY OPINION FROM THE OFFICE OF MUNITIONS CONTROL, DEPARTMENT OF STATE

- INDUSTRY-GENERATED, EXPORT CONTROLLED TECHNICAL DATA ARE NOT GOVERNED BY THE JCP AND ITS PROCEDURES BUT BY APPLICABLE EXPORT REGULATIONS

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

MARKINGS

- ALL DOCUMENTS RELEASED UNDER THE PROVISIONS OF THE JCP WILL BE MARKED TO ALERT RECIPIENTS OF THE NEED FOR SPECIAL HANDLING:

  "THE CONTROL OF INFORMATION CONTAINED IN THIS DOCUMENT IS GOVERNED, IN THE UNITED STATES, BY DOD DIRECTIVE 5230.25 AND, IN CANADA, BY THE TDCR"

- DOCUMENTATION RELEASED UNDER THE PROVISIONS OF THE JCP WILL ALSO HAVE, AFFIXED TO THE FRONT OF THE DOCUMENT, *AN EXPORT CONTROL WARNING NOTICE AND A DISTRIBUTION STATEMENT*

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

VIOLATIONS

- ANY VIOLATION OF THE CERTIFICATION AGREEMENT MAY RESULT IN THE FOLLOWING:
  - LOSS OF CERTIFICATION IN THE U.S. AND CANADA
  - LIABILITY TO SANCTION UNDER THE ITAR
  - LIABILITY TO SANCTION UNDER CANADA'S DEFENCE PRODUCTION ACT

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

PROBLEMS

- U.S. IMPLEMENTING AUTHORITY FOR THE JCP (DODD 5230.25) NEEDS TO BE REWRITTEN TO INCLUDE THE JCP (THE JCP IS IMPLEMENTED IN CANADA BY THE TECHNICAL DATA CONTROL REGULATIONS (TDCR))

- CANADIAN VISITS TO U.S. CONTRACTOR INSTALLATIONS HAMPERED BY LACK OF WRITTEN INSTRUCTION ON THE PROCESS AND LACK OF KNOWLEDGE OF THE EXPANDED USE OF JCP TO COVER RELATED VISITS

- U.S. VISITS TO CANADIAN CONTRACTOR INSTALLATIONS HAMPERED BY LACK OF KNOWLEDGE OF THE CANADIAN PROCEDURES RELATING TO LICENSING REQUIREMENTS FOR CANADIAN TECHNICAL DATA AND CANADIAN VISIT PROCEDURES

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

RECOMMENDATIONS

- REVISE DOD DIRECTIVE 5230.25 TO FACILITATE PROPER FUNCTIONING OF THE JCP (IN PROCESS)
- DISSEMINATE INFORMATION ARTICLE ON THE JCP THROUGH:
  - SERVICE MESSAGES
  - DIS NEWSLETTER
  - OMC NEWLETTER
  - VARIOUS DEFENSE TRADE PUBLICATIONS
- PUBLISH INFORMATION ARTICLE ON CANADIAN PROCEDURES FOR U.S. CONTRACTORS

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

RECOMMENDED EXPANSION OF THE JCP

- DOD RECOMMENDS EXPANSION OF THE JCP FURTHER TO EXEMPT CERTIFIED CONTRACTORS FROM THE NEED TO OBTAIN GOVERNMENT APPROVAL IN ORDER TO CONDUCT UNCLASSIFIED VISITS TO DOD OR DND MILITARY INSTALLATIONS IN RESPONSE TO AN UNCLASSIFIED SOLICITATION CONTAINING TECHNICAL DATA CONTROLLED BY DODD 5230.25 OR THE TDCR

- THE U.S. MILITARY SERVICES HAVE CONCURRED IN AN AFFIRMATIVE RESPONSE TO THIS PROPOSAL PROVIDED THERE IS RECIPROCITY

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

RECIPROCITY

- DND HAS AGREED IN PRINCIPLE TO, AND IS DEVELOPING PROCEDURES FOR CONTRACTOR-TO-MILITARY INSTALLATION VISITS TO OBTAIN UNCLASSIFIED TECHNICAL DATA SIMILAR TO THOSE PROCEDURES PROPOSED BY THE DOD

U.S./CANADA TECHNOLOGY SECURITY
JOINT CERTIFICATION PROGRAM

GOALS AND OBJECTIVES

- FACILITATE THE FUNCTIONING OF THE JCP AS IT WAS ENVISIONED IN THE 1986 MOU

- PROMOTE AND ENHANCE U.S./CANADA STRATEGIC TECHNOLOGY SHARING IN KEEPING WITH THE SPIRIT OF THE REAGAN/MULRONEY FREE TRADE AGREEMENT

9-X38-1032U-1

ATTACHMENT 10

Visits Involving Access to Unclassified Technical Data by Canadian Government Officials and Certified Canadian Contractors

OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D. C. 20301-2000

POLICY

17 July 1990

In reply refer to:
I-90/10763

MEMORANDUM FOR DIRECTOR, DEFENSE INVESTIGATIVE SERVICE
DIRECTOR, NAVY INTERNATIONAL PROGRAMS OFFICE, USN
DIRECTOR, COUNTERINTELLIGENCE AND SECURITY COUNTERMEASURES, ODCSINT (DAMI-CI), USA
CHIEF, INTERNATIONAL AFFAIRS DIVISION, CVAI, USAF
CHIEF, FOREIGN LIAISON DIVISION, DI-4, DIA

SUBJECT: Visits Involving Access to Unclassified Technical Data by Canadian Government Officials and Certified Canadian Contractors

REFERENCES: (a) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
(b) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984
(c) DoD Directive 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987

The United States and Canada share a unique, long-standing military and economic relationship. The two countries are partners in the joint defense of North America and have established a bilateral command structure (NORAD) for mutual air defense. Canadian industry is a part of the North American Defense Mobilization Base. The United States and Canada consult and cooperate on the development of common industrial security procedures and technology controls; approximately 70% of Canadian industry is owned by U.S. interests. The two governments have entered into numerous bilateral agreements that codify and support this relationship.

In 1985, the United States and Canada signed a Memorandum of Understanding (MOU) that established the United States-Canada Joint Certification Program. As stated in the MOU's "Joint Terms of Reference for the United States-Canada Joint Certification Program," the program was established "to certify contractors of each country for access, on an equally favorable basis, to unclassified technical data disclosing critical technology." This information is controlled in the United States by DoD Directive 5230.25 and, in Canada, by the Technical Data Control Regulations (TDCR). Under each Nation's laws, the U.S. Department of Defense and Canada's Department of National Defence may withhold such technical data from public disclosure.

To ensure that the goals of the 1985 memorandum are realized, the United States-Canada Security Subcommittee has agreed that the certification process can be used to facilitate visits that involve access to unclassified technical data. The attached procedures have been developed in coordination with the Military Departments to permit directly arranged visits (DAV) by Canadian Government officials and certified Canadian contractors to DoD contractors or military installations. Canadian authorities have developed similar procedures that permit DAVs by U.S. officials and contractors to Canadian contractors and military installations.

You are requested to initiate action necessary to implement the attached procedures. A copy of your implementing instructions should be provided to this office, Attention: Director for International Security Programs by 31 August 1990.

Maynard C. Anderson
Assistant Deputy Under Secretary of Defense
(Counterintelligence and Security)

Attachment
As stated

cc:
Director, DTSA

Subject: Directly Arranged Visits (DAV) by Canadian Government Officials and Certified Canadian Contractors

I. Applicability:

A directly arranged visit (DAV) is permitted when the following two conditions are satisfied:

1. First condition:

a. There is a valid license covering the export of the data; or

b. The export or release is permitted under the Canadian exemption in Part 126.5 of the International Traffic in Arms Regulations (ITAR) (see Tab A, paragraph 1); or

c. The export or release is covered by the general exemptions in Part 125.4 of the ITAR (see Tab A, paragraph 2); or

d. The export or release qualifies for a General License under the Export Administration Regulations (EAR); and

2. Second condition:

a. The distribution statement applied to the data pursuant to DoD Directive 5230.24 permits release (see Tab B); or

b. The controlling office authorizes release.

II. Responsibilities:

a. In the case of unclassified visits to DoD contractor facilities, it is the responsibility of the U.S. contractor to notify potential Canadian visitors if a proposed visit meets the conditions for a DAV or if an official visit request must be submitted through government channels.

b. Canadian Government officials and certified Canadian contractors wishing to initiate an unclassified visit to a U.S. military installation should make arrangements with the installation security office. These direct unclassified visits to military installations may be conducted for the purpose of:

(1) collecting or discussing unclassified solicitations; or

(2) in furtherance of procurement activity related to unclassified solicitations (e.g., pre-solicitation conferences).

By regulation, the installation commander retains final approval authority for any visit and may deny it for security or operational reasons.

c. It is the responsibility of the sponsors of meetings, conferences and symposia, at which controlled unclassified technical data will be presented or discussed, to ensure that the information provided at the meeting is releasable to Canadian Government officials and certified Canadian contractors. The conditions listed in paragraph 1. above, apply. DoD Instruction 5230.27 provides further guidance regarding the presentation of DoD-related scientific and technical papers at meetings, conferences and symposia.

III. Procedures for Processing Requests for Visits and Documentation

Upon receipt of a request for a visit which will involve the release of unclassified technical data to Canadian officials or certified Canadian contractors, the recipient DoD Component or contractor security office, or the controlling office, as applicable, will:

a. if the requestor is a government official, verify identity and status; if the requestor is a contractor, verify that the purpose falls within the scope of the business activity stated in the requestor's certification, DD Form 2345, which must accompany all requests;

b. determine whether the information is releasable under the Canadian exemption in Part 126.5 of the ITAR or the general exemptions in Part 125.4 of the ITAR, or under a General License;

c. if the data bears a distribution statement, determine whether release is authorized or whether release must be approved by the controlling office (e.g., the requestor is outside the intended audience) (see Tab B). It is the responsibility of the controlling office to obtain any written consent required (e.g. for foreign government or proprietary information);

d. if the data cannot be released, the requestor will be provided a written explanation of the reasons for denial and the procedures to be followed for an appeal. If release requires approval of a license or other written approval, action should be initiated to obtain approval and the requestor should be notified of such action.

TAB A. Licensing Exemptions

TAB B. Technical Data Markings

Licensing Exemptions

1. Canadian Exemptions (Part 126.5 of the ITAR).

In general, unclassified articles and technical data may be exported to Canada without a license or other authorization, for end-use in Canada or return to the United States, with the exception of the articles and technical data listed in subparagraphs a. through g., below. If the data to be released during the proposed visit is included in subparagraphs a. through g., a valid export license or approved visit request is necessary, unless release is permitted under a general exemption described in paragraph 2. below.

a. Fully automatic firearms in Category 1(a) of the U.S. Munitions List which are not for end-use by the Federal Government, or a Provincial or Municipal Government of Canada;

b. Nuclear weapons strategic delivery systems and all components, parts, accessories or attachments specifically designed for such systems and associated equipment;

c. Nuclear weapon design and test equipment listed in Munitions List Category XVI;

d. Naval nuclear propulsion equipment listed in Munitions List Category VI(e);

e. Aircraft listed in Munitions List Category VIII(a);

f. Submersible and oceanographic vessels and related articles in Munitions List Category XX(a) through (d);

g. Technical data that can be used for manufacturing purposes except in furtherance of a technical assistance agreement (TAA) or manufacturing license authorized pursuant to part 124.3 of the ITAR.

2. General Exemptions (Part 125.4 of the ITAR).

A license (or, in some cases, an additional license) is not required if the export or release of unclassified technical data falls under one of the following general exemptions.

a. Technical data to be disclosed pursuant to an official written request or directive from the U.S. Department of Defense.

b. Technical data in furtherance of a manufacturing license or technical assistance agreement approved by the Department of State provided that data does not exceed the scope and limitations of the relevant agreement.

c. Technical data in furtherance of a contract between the exporter and an agency of the U.S. Government, if the contract provides for the export of the relevant technical data, and such data does not disclose the details of design, development, production, or manufacture of any defense article.

d. Copies of technical data previously authorized for export to the same recipient. Revised copies of such technical data are also exempt if they pertain to the identical defense article, and if the revisions are solely editorial and do not add to the content of technology previously exported or authorized for export to the same recipient.

e. Technical data in the form of basic operations, maintenance, and training information relating to a defense article lawfully exported or authorized for export to the same recipient. This exemption applies only to exports by the original exporter.

f. Technical data related to firearms not in excess of caliber .50 and ammunition for such weapons, except detail, design, development, production or manufacturing information.

g. Technical data being returned to the original source of import.

h. Technical data directly related to classified information which has been previously exported or authorized for export to the same recipient, and which does not disclose the details of the design, development, production, or manufacture of any defense article.

i. Technical data sent by a U.S. corporation to a U.S. government agency. (This exemption is subject to limitations in Section 125.1 (b) of the ITAR).

j. Technical data for which the exporter, pursuant to an arrangement with the Department of Defense or NASA which requires such export, has been granted an exemption in writing from licensing provisions by the Office of Defense Trade Controls. Such an exemption will normally be granted only if the arrangement directly implements an international agreement to which the United States is a party and if multiple exports are contemplated.

k. Technical data approved for public release (i.e., unlimited distribution) by the cognizant U.S. Government department agency.

Technical Data Markings

On unclassified DoD-controlled technical data look for two important markings, the **Export Warning Statement** and the **Distribution Statement.** The Export Warning Statement tells you that the data may be withheld from public disclosure under authority granted by Congress. The Distribution Statement identifies the users for whom the data is intended.

Technical data that has an Export Warning Statement may be released outside the Government only to companies and individuals who have executed certifications (DD Form 2345) in accordance with DoD Directive 5230.25. All non-Government recipients of technical data must describe their access requirements through certification prior to obtaining information that is controlled by a Distribution Statement.

Distribution Statements authorize secondary document dissemination organizations (e.g., libraries and data repositories) to release the documentation to eligible recipients identified by the Distribution Statement. All requests from outside the intended audience are to be referred to the controlling office for action. Controlling offices make release determinations in accordance with applicable laws and regulations.

Contractors certified by the U.S.-Canada Joint Certification Office (JCO) are authorized access to technical data that have a Distribution Statement "A" or "X". Certified contractors who are supporting U.S. Government agencies also would have access to unclassified documents with Distribution Statement "C". If there is a contract with DoD, they also are eligible to receive unclassified documents with Distribution Statement "D". However, if the Distribution Statement "C" or "D" specifies that the document contains "foreign government" or "company proprietary" information, written consent must be obtained from the owners before release. Access to documentation with Distribution Statements "B", "E", or "F" requires the permission of the controlling office for release.

ATTACHMENT 11

DoDD 5230.20--International Visits and Personnel Exchanges

Department of Defense
DIRECTIVE

March, 1990
5230.20

USD(P)

SUBJECT: International Visits and Personnel Exchanges

References: (a) DoD Instruction 5230.20, "Policy and Procedures for the Control of Foreign Representatives," June 25, 1984 (canceled)
(b) Title 22, CFR, Sections 120-130, "International Traffic in Arms Regulations (ITAR)," Department of State, November 1989
(c) Title 15, CFR 768 et seq, "Export Administration Regulations (EAR)," Department of Commerce, December 1990
(d) through (t), see Enclosure 1

A. **PURPOSE**: This Directive:

1. Cancels reference (a) and provides policy and procedures governing visits by and the assignment of foreign nationals to DoD Components.

2. Establishes the International Visits Program and Defense Personnel Exchange Program.

B. **APPLICABILITY**

1. This Directive applies to:

a. The Office of the Secretary of Defense (OSD) and activities supported by OSD, the Military Departments, The Joint Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "**DoD Components**").

b. All arrangements whereby foreign persons visit or are assigned to DoD Components or to facilities over which DoD Components have security responsibility.

2. This Directive does not apply to:

a. Visits that are conducted at defense contractor facilities which involve access only to unclassified information that is not subject to export licensing under the Department of State's International Traffic in Arms Regulations (ITAR) (reference (b)) or the Department of Commerce's Export Administration Regulations (EAR) (reference (c)).

b. Visits to DoD Components or DoD contractor facilities by foreign national employees of a U.S. contractor. Such visits will be processed in compliance with the ITAR (reference (b), DoD 5220.22-M (reference (d), and Enclosure 3, section B.4.

c. Programs involving the training of foreign nationals that are subject to Chapter 10 of DoD 5105.38-M (reference (e)) and the Joint Security Assistance Training (JSAT) Regulation (reference (f)).

C. **DEFINITIONS**: The terms used in this Directive are defined at Enclosure 2. Only these terms will be used in connection with foreign visits and personnel exchanges.

D. **POLICY**: It is DoD Policy that:

1. **Contacts With Foreign Representatives**. All contacts by foreign representatives with DoD Components shall be conducted under the International Visits Program or the Defense Professionals Exchange Program and only in compliance with this Directive.

2. **International Visits Program**. Visits by foreign nationals and assignments of liaison officials to DoD Components shall be arranged as a *one-time* visit, *recurring* visit or *extended* visit as described in Enclosure 3 of this Directive.

a. **Licensing Requirements**. DoD visit authorizations shall not be used to circumvent export licensing requirements (see Enclosure 3, section B.9.).

b. **Sponsorship**. Visits by foreign nationals to DoD Components that will involve access to classified information or controlled unclassified information shall be sponsored by the visitor's government. Requests for visits within the United States shall be submitted through the requesting government's Embassy in Washington.

3. **Defense Personnel Exchange Program** (DPEP). Assignments of foreign nationals to DoD Component organizations to perform functions for the host organization shall be arranged only under a Defense Personnel Exchange Program (DPEP) agreement in compliance with DoD Directive 5530.3 (reference (g)) and Enclosure 4 of this Directive.

4. **Release of Information**.

a. Access by foreign nationals to classified information shall be in compliance with DoD Directive 5230.11 (reference (h)) and DoD 5200.1-R (reference (i)).

b. Access to controlled unclassified information shall be in compliance with DoD Directives 5230.25 and 5400.7 (references (j), and (k)).

c. Exceptions to the National Disclosure Policy (NDP-1) (reference (l)) will not be granted to accommodate assignment of a foreign exchange professional under the DPEP.

5. **DDL**. A Delegation of Disclosure Authority Letter (DDL), containing the information in the example at Enclosure 5 shall be prepared and provided to the contact officer for each foreign national assigned to a DoD Component as a liaison officer or under a Defense Personnel Exchange agreement.

6. **Contact Officers**. Contact officers shall be designated to control the activities of foreign visitors and exchange personnel. The contact officer must be familiar with DoD Directive 5230.11 (reference (h), applicable guidelines governing the release of classified and controlled unclassified information, and the specific disclosure guidelines established in the DDL.

7. **Identification for Foreign Nationals**. All foreign visitors, including attaches, liaison personnel, and exchange personnel, that are authorized unescorted access to DoD facilities shall be issued badges or passes that clearly identify them as foreign nationals. Decisions on issuance of badges and passes shall be made after consideration of the factors at Enclosure 3.

E. **RESPONSIBILITIES**

1. The **Heads of DoD Components** shall:

a. ***Designate***, in writing, an official to manage the International Visits Program and the Defense Personnel Exchange Program for their Component.

b. ***Promulgate written instructions***, consistent with DoD Directives 5230.11, 5230.25, and 5400.7 and DoD 5200.1-R (references (h), (j), (k) and (i)) and this Directive to govern visits and assignments of foreign nationals and their access to classified and controlled unclassified information.

c. ***Record decisions on foreign visits*** involving access to classified and controlled unclassified information in the Foreign Visits System (FVS) in compliance with DoD Instruction 5230.18 (reference (m)).

2. The **Secretaries of the Military Departments**, or their designee, additionally shall:

a. ***Approve or deny requests for visits*** by foreign representatives to their Departments and their contractors.

b. ***Negotiate all agreements*** with foreign counterpart Military Departments involving the assignment of exchange military personnel to their Component, in compliance with existing laws and regulations, DoD Directive 5530.3 (reference (g)) and this Directive.

c. ***Process visit requests*** from foreign governments through the Foreign Visits System in compliance with DoD Instruction 5230.18 (reference (m)).

d. ***Conduct periodic on-site visits*** to the military organizations and facilities under their cognizance to monitor implementation of this Directive.

2. The **Director, Defense Intelligence Agency**, or a designee, shall:

a. ***Process requests for visits*** by foreign nationals to the OSD, The Joint Staff and the Defense Agencies, and their contractors, except those visits approved by the National Security Agency/Central Security Service and the immediate offices of the Secretary and Deputy Secretary of Defense.

b. ***Administer***, in coordination with the Deputy Under Secretary of Defense (Security Policy), ***the assignment of exchange personnel*** to OSD, The Joint Staff and DoD agencies.

c. ***Promulgate a Department of Defense Foreign Attache Manual*** to provide standard instructions and formats governing visit requests, document requests, liaison officer certifications and exchange personnel. The manual shall be coordinated with the Military Departments and the Office of the Deputy Under Secretary of Defense (Security Policy) prior to publication.

3. The **Deputy Under Secretary of Defense (Security Policy)** shall:

a. ***Provide policy guidance and exercise oversight*** within the Department of Defense for the International Visits Program and the Defense Personnel Exchange Program.

b. ***Manage automation support*** to the International Visits Program and the Defense Personnel Exchange Program through the Foreign Disclosure and Technical Information System (FORDTIS) under DoD Instruction 5230.18 (reference (m)).

c. ***Authorize the negotiation*** of Defense Personnel Exchange agreements that involve the assignment of foreign personnel to OSD, The Joint Staff and the Defense Agencies, except as specified in subsection E.5., and E.8., below.

d. ***Promulgate additional guidance*** as necessary to ensure effective implementation of this Directive.

4. The **Comptroller of the Department of Defense** shall establish policies and procedures concerning the financial aspects of the Defense Personnel Exchange Program.

5. The **Under Secretary of Defense (Acquisition)** shall promulgate procedures consistent with DoD Directive 5530.3 (reference (g)) and this Directive governing the

negotiation and conclusion of agreements for exchange of scientific and technical personnel.

6. The **General Council** will ***review and assure the legality of agreements*** involving visits and assignments of foreign persons to DoD Components.

7. The **Assistant Secretary of Defense (Force Management and Personnel)** will ***review agreements*** with foreign governments that establish Defense Professionals Exchange positions to ensure compliance with DoD manpower and personnel policies.

8. The **Assistant Secretary of Defense (Command, Control, Communications and Intelligence)** shall ***promulgate procedures consistent with DoD Directive 5530.3*** (reference (g)) and this Directive governing the negotiation of agreements that involve the assignment of foreign exchange personnel in ***DoD intelligence*** and intelligence-related positions.

9. The **Chairman, Joint Chiefs of Staff** shall ***promulgate procedures consistent with DoD Directive 5530.3*** (reference (g) and this Directive governing visits by foreign nationals and assignments of foreign exchange personnel to the ***Unified and Specified Commands***.

10. The **Secretary of the Air Force** shall ***provide resources*** for the operation, maintenance and administration of the ***Foreign Visits System (FVS)*** and comply with DoD 7110.1-M (reference (n) regarding requests for funds to carry out this responsibility.

F. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing documents to the Deputy Under Secretary of Defense for Security Policy within 120 days.

SIGNATURE

Enclosures - 5
1. References
2. Definitions
3. International Visits
4. Exchange Personnel
5. Delegation of Disclosure Authority Letter

(d) DoD 5220.22-M, "Industrial Security Manual For Safeguarding Classified Information," January 1991
(e) DoD 5105.38-M, "Security Assistance Management Manual," October 1, 1988 authorized by DoD Directive 5105.38, August 10, 1978.
(f) "Joint Security Assistance Training (JSAT) Regulation," AR 12-15, SECNAVINST 4950.4, AFR 50-29, February 28, 1990
(g) DoD Directive 5530.3 "International Agreements," June 11, 1987
(h) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," **(under revision)**
(i) DoD 5200.1-R, "Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, June 7, 1982
(j) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," **(under revision)**
(k) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988
(l) National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (short title: National Disclosure Policy (NDP-1)) (U), October 1988[1]
(m) DoD Instruction 5230.18, "The DoD Foreign Disclosure and Technical Information System (FORDTIS)," November 6, 1984 **(under revision)**
(n) DoD 7110.1-M, "Department of Defense Budget Guidance Manual," July 1988
(o) Executive Order 12356, "National Security Information," April 16, 1983
(p) DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs," April 21, 1982
(q) DoD Instruction C-5220.29, "Implementation of the North Atlantic Treaty Organization Industrial Security Procedures (U)," December 15, 1982
(r) DoD Directive 5200.12, "Conduct of Classified Meetings," May 16, 1988
(s) DoD 5230.25-Ph, "Control of Unclassified Technical Data With Military or Space Application," **(To Be Published)**
(t) U.S.C., Title 22, Section 2751 et seq, "Arms Export Control Act of 1976," as amended.

---

[1] Provided to designated disclosure authorities on a need-to-know basis from the Office of the Deputy Under Secretary of Defense for Security Policy.

DEFINITIONS

1. **Attache**: A diplomatic official or military officer attached to an embassy or legation, especially in a technical capacity.

2. **Certification**: Formal recognition by a DoD Component of a working relationship with a representative of a foreign government (i.e., a Liaison Officer) for specified purposes and on a recurring basis.

3. **Classified Military Information** is information originated by or for the Department of Defense or its departments or agencies or under their jurisdiction or control and which requires protection in the interests of national security. It is designated TOP SECRET, SECRET and CONFIDENTIAL, as described in Executive Order 12356 (reference (o)). Classified military information may be in oral, visual or material form. DoD Directive 5230.11 (reference (h)) further defines the eight categories into which classified military information has been subdivided.

4. **Contact Officer**: A DoD official designated in writing to oversee and control all contacts, requests for information, consultations, and other activities of foreign representatives who are assigned to or are visiting a DoD Component or subordinate organization. In the case of personnel exchange programs, the host supervisor may be the contact officer.

5. **Controlled Unclassified Information**: Unclassified information to which access or distribution limitations have been applied in accordance with national laws and regulations of the originating country. For the purpose of this Directive, it generally is U.S. information that is exempt from public disclosure pursuant to DoD Directives 5230.25 and 5400.7 (references (j) and (k)) or which is subject to export controls.

6. **Delegation of Disclosure Authority Letter (DDL)**: A letter issued by the appropriate designated disclosure authority describing classification levels, categories, scope, and limitations concerning information that may be disclosed to specific foreign governments or foreign nationals.

7. **Executive Agent**: The office designated to negotiate and sign agreements establishing exchange programs; and as final approval authority for all exchange programs that take place within that DoD Component.

8. **Exchange Personnel (formerly "Integrated Personnel")** : Military or civilian officials of a foreign defense establishment who are assigned to a DoD Component following the terms of an exchange agreement and who perform duties, prescribed by a position description, for the DoD Component.

9. **Foreign National**: For this Directive, a person who is not a citizen of the United States.

10. **Foreign Representative**: Either a foreign person or a representative of a foreign interest as defined in item 16., below.

11. **International Organization**: An entity established by recognized governments pursuant to an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.

12. **Liaison Officer**: A foreign government official, either a military or civilian employee, who is certified by his or her government to act as a representative of that government to a DoD Component in connection with bilateral or multinational programs.

13. **Meeting**: For this Directive, a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified or controlled unclassified information is disseminated.

14. **Representatives of a Foreign Interest**: A citizen or national of the United States, or an intending citizen to the United States, who is acting as a representative of a foreign government, organization or firm.

15. **Security Assurance**: The written confirmation, requested by and exchanged between governments, of the security clearance level or eligibility for clearance, or their national contractors and citizens. For the purposes of this Directive, it also includes a statement by a responsible official of a foreign government or international organization that the original recipient of U.S. classified military information possesses the requisite security clearance and is approved by his or her government for access to information of the security classification involved on behalf of the government or organization and that the recipient government will comply with security requirements specified by the U.S.

16. **Training**. Training as it applies to this Directive includes formal or informal instruction of foreign students in the United States or overseas by:

a. officers or employees of the United States, contract technicians, or contractors (including instruction at civilian institutions); **or**

b. correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice to foreign military units and forces.

17. **Visit Authorization**: There are three types of visit authorizations:

a. An **One-time Visit Authorization** permits contact by a foreign representative with a DoD Component or DoD contractor facility for a single short-term occasion for a specified purpose.

b. A **Recurring Visit Authorization** permits intermittent visits over a specified period of time in connection with a government approved license, contract or agreement or other program when the technical data to be released has been defined and approved for release in advance by the U.S. Government.

c. An **Extended Visit Authorization** permits a single visit for an extended period of time. Extended visit authorizations are to be used when a foreign national is required to be in the United States, normally beyond 30 days, in connection with one of the following situations:

(1) A foreign government contract or joint program (e.g., joint venture, representative to a joint or multinational program, etc.);

(2) Participation in an exchange program under the DPEP;

(3) Training;

(4) Certification as a liaison officer to a DoD Component(s).

INTERNATIONAL VISITS PROGRAM

A. GENERAL

1. **Control of Visitors**. Visits by foreign nationals to DoD Components shall be controlled to ensure that the visitors receive access to only that classified and controlled unclassified information that is authorized by a disclosure official designated pursuant to DoD Directive 5230.11 (reference (h)) for disclosure to their government.

2. **International Visits Program**. The International Visits Program is established to ensure that classified and controlled unclassified information to be disclosed to foreign visitors has been properly authorized for disclosure to their governments, that the requesting foreign government provides a security assurance on the visitors, and to facilitate administrative arrangements for the visit.

3. **Security Assurance**. Classified information and controlled unclassified information shall not be disclosed to a foreign national unless the appropriate designated disclosure authority has received a security assurance from the foreign national's government. Classified documentary information may not be transferred to a foreign national unless the security assurance specifically states that the individual may assume custody on behalf of the government. A receipt must be obtained for the information, regardless of its classification level.

4. **Foreign Visits System (FVS)**. Requests for visits submitted by foreign governments shall be submitted and processed using the FVS. Requests for visits by governments that do not participate in FVS, and visits to locations where FVS is not available, shall be submitted directly to the applicable Military Department or DIA, which shall enter and process the request in the FVS.

B. PROCEDURES

1. **Recurring Visit Authorizations** shall be established to support intermittent, recurring visits associated with approved programs, such as agreements, contracts or licenses. Authorizations will be valid for the duration of the program, subject to annual review and revalidation.

2. **Extended Visit Authorizations** shall be used for the assignment of certified liaison officers and exchange personnel.

3. **Hosted Visit**. Visits by foreign nationals at the invitation of DoD officials do not normally require the submission of a complete visit request by the visitors since designated disclosure officials should have authorized disclosures of information prior to the invitation being extended. Nevertheless, certain security requirements must be satisfied. To facilitate arrangements for these visits, DoD officials who extend such invitations shall notify their designated visitor control office of the invitation so that the necessary security assurances can be obtained and expedited arrangements can be made for the visits.

4. **Visits by Foreign National Employees of U.S. Defense Contractors** to DoD Components or to other contractor facilities on official business do not require the submission of a visit request through foreign government channels. Access to export controlled technical data by foreign national employees of U.S. contractors are authorized pursuant to an export license or by other written U.S. Government authorization that is obtained by the employing contractor. When these employees visit another contractor facility or a DoD Component, the employing facility should provide a copy of the export license or other written authorization to the designated disclosure authority or security office, as applicable, at the facility to be visited.

5. **Visits by Representatives of the North Atlantic Treaty Organization (NATO)**

a. **NATO Classified Information**. One-time or recurring visits by representatives of NATO commands or agencies or the NATO international staff, which involve access to NATO classified information, will be processed under paragraph 40, Section III, of Attachment 1 to USSAN Instruction 1-69 (enclosure 2 to DoD Directive 5100.55 (reference (p)). Recurring visits related to NATO Production and Logistics Organization (NPLO) or NATO Industrial Advisory Group (NIAG) activities will be processed under Section VI of USSAN Instruction 1-70 (enclosure to DoD Instruction C-5220.29 (reference (q)).

b. **Non-NATO Classified Information**. Visits by representatives of a NATO command, agency or the NATO international staff, including US citizens assigned to NATO positions, which involve access to US classified information, will be processed in compliance with the requirements of this Directive.

6. **Visits for Foreign Participation in U.S. Procurement - Related Meetings**. Potential foreign attendance must be assumed when planning for meetings that may lead to contract opportunities for nations with which the U.S. has reciprocal procurement agreements. Security requirements for classified meetings shall be in compliance with DoD Directive 5200.12 (reference (r)) and DoD 5200.1-R (reference (i)). The following procedures also apply:

a. **Disclosure Decision.** DoD Components will determine the extent to which classified information may be involved throughout the life cycle of a program before the announcement of a procurement action. Decisions on disclosures of classified information shall be in compliance with DoD Directive 5230.11 (reference (h)). The extent of foreign attendance at meetings related to the announced procurement action will be contingent upon the disclosure decision. If attendance by foreign nationals is permitted, any classified information to be disclosed must be at a level that is authorized for release to all foreign nationals that are present.

b. **Denials.** The head of the DoD Component conducting the meeting, or a senior designee, will approve any denials of a specific appeal by a foreign government for attendance by its representatives at such meetings.

7. **Canadian Visits**. Visits by Canadian government officials or certified Canadian contractors to DoD Components or contractors, that involve the disclosure of controlled unclassified information, will follow the procedures outlined in DoD 5230.25-Ph (reference (s)).

8. **DoD Components supported by DIA** shall:

a. **Obtain a disclosure authorization** from the originating department or agency for the release of any classified or controlled unclassified information that is not under the Component's disclosure jurisdiction. This shall be accomplished prior to notifying DIA of the acceptance of a visit by foreign nationals that will involve access to such information.

b. **Notify DIA, ATTN: DI-4A**, when they extend invitations to foreign nationals to visit their organization.

9. **DoD-authorized visits to contractor facilities**. DoD-authorized visits of foreign nationals to contractor facilities constitute an exemption to the licensing requirements of the ITAR (reference (b)). DoD authorized visits may not be used to circumvent the licensing requirements of the ITAR by contractors. Therefore, DoD Components shall:

a. **Approve the Request** for a visit if it is in support of an actual or planned U.S. Government program; or

b. If the proposed visit is **not in support of a U.S. Government program**, notify the requestor and applicable contractor that arrangements for the visit may be made between the requestor and the contractor, provided the contractor has or obtains an export license for any technical data that may be disclosed; or,

c. **Deny the Request** for the visit if it is determined that the information associated with the proposed visit cannot be authorized for disclosure, and notify the requestor and the applicable contractor of the decision.

10. **Liaison Officers**.

a. **General.**

(1) DoD liaison officer certification does not bestow diplomatic or other special privileges, even though certified liaison officers who also have attache status may have diplomatic accreditation by the Department of State.

(2) Liaison officers' activities shall be limited to the representational responsibilities of their government described in the certification. They may not perform functions for the DoD Component(s) to which they are certified.

(3) DoD certification shall not be used to assign foreign nationals to U.S. defense contractor facilities. U.S. defense contractors must obtain an export license for such assignments and comply with the provisions of Chapter 10 of DoD 5220.22-M (reference (d)).

b. **Certification Procedures**. The following requirements shall be satisfied for DoD certification of foreign government liaison officers:

(1) Notification to the Department of Defense by the foreign government concerned that the specified official is an officially sponsored representative of that government.

(2) A statement of legal status of the liaison officer (including any privileges and immunities to which the liaison officer is entitled) and parent government responsibilities.

(3) A statement that the official concerned is authorized by the sponsoring government to conduct business with the Department of Defense for purposes that must be specified, citing related agreements, contracts or other arrangements.

(4) An assurance by the foreign government that the official holds a specified level of security clearance.

(5) A statement concerning whether the liaison officer may assume custody of documentary information on behalf of the government.

(6) An assurance that the liaison officer's government will be responsible for any US classified or controlled unclassified information provided to the liaison officer.

11. **Access to DoD Facilities**. Foreign national visitors of allied and friendly countries, including attaches and liaison officers, may be authorized unescorted access to DoD facilities when all of the following conditions are met:

a. The foreign government concerned extends reciprocal privileges to U.S. in-country Defense personnel.

b. Security measures are in place to control access to information and sensitive areas within the facility.

c. Access is required for official purposes on a frequent basis (i.e., more than once per week).

d. A badge or pass is issued which identifies the bearer as a foreign national and which is valid for a specific facility during normal duty hours.

e. The badge or pass is displayed on the outer clothing so that it is clearly visible.

f. Issuance of the badge or pass must be authorized in writing by a senior official designated for this purpose based on written justification describing how items a. through c., above, will be met.

DEFENSE PERSONNEL EXCHANGE PROGRAM (DPEP)

A. GENERAL

1. **Voluntary Services**. The United States Government may not accept voluntary services from any source or employ personal services exceeding that authorized by law, except for emergencies involving the safety of human life or the protection of property, unless the service is gratuitous. The essential element of "gratuitous service" is that the person rendering the service must agree in writing, in advance, that he or she waives any and all claims against the Government on account of the services.

2. **Use of U.S. Resources for Training**. United States Government resources may not be used to provide training to foreign persons except as provided by the Arms Export Control Act (reference (t)) as implemented by Chapter 10 of DoD 5105.38-M (reference (e)).

3. **Security Clearances**. United States Government policy also prohibits the granting of security clearances to foreign nationals and therefore discourages the hiring of foreign nationals. However, classified information may be shared with other governments and their representatives in support of lawful and authorized government programs.

4. **Advantages to DoD**. Despite the above restrictions, advantages can accrue to DoD from the assignment of foreign personnel to selected defense positions that permit DoD Components to take advantage of specified expertise of the foreign person and foster better understanding on the part of the participants of the organization and management of defense programs and operations. The DPEP is designed to permit the assignment of foreign defense personnel to DoD Components for these purposes based on a government-to-government agreement that provides for reciprocity.

5. **Scope**. The DPEP covers all initiatives that involve the assignment of foreign personnel to positions with DoD Components other than for training. Assignment of foreign personnel under the DPEP will not be used for training (see subsection B.2.c., of this Directive) or in lieu of, or in combination with liaison officer certification. DPEP agreements normally will cover:

a. Personnel exchanges involving assignments of military personnel to operational positions under the jurisdiction of the Military Departments;

b. Senior professional personnel to administrative and planning positions within OSD;

c. Scientists and engineers to technical positions within the DoD Components; and

d. Intelligence analysts controlled by DIA.

B. POLICY

1. **Status of Personnel**. Personnel assigned to DPEP positions shall be career military or civilian employees of the participating Defense establishments.

2. **Purpose**. DPEP agreements may be negotiated to foster better understanding on the part of the participants and their governments of the organization and management of defense programs and operations while taking advantage of specified expertise of the participating exchange personnel. The criteria in subsection D.1, below shall be considered prior to making commitments concerning the negotiation of a DPEP agreement.

3. **Reciprocity**. DPEP agreements shall provide for the reciprocal assignment of DoD personnel to substantially equivalent positions within the Defense establishment of the other participating government.

4. **Limitations**. The DPEP may not be used as a mechanism for exchanging technical data or other controlled information between the governments or for training of foreign nationals. Information exchanges will be governed by an appropriate agreement (e.g., cooperative research and development or data exchange agreement); training of foreign nationals shall be in compliance with DoD 5105.38-M (reference (e)).

5. **Executive Agents**. DoD officials who are responsible for authorizing the negotiation of personnel exchange agreements may appoint an executive agent to negotiate and administer a program for a specific country or countries.

C. RESTRICTIONS AND SECURITY REQUIREMENTS

1. **Restrictions on Exchange Personnel**.

a. **Dual Status.** Foreign exchange personnel may not act in the dual capacity as a DPEP participant and as a representative of their government while assigned to DoD Components. They also may not act as an official DoD representative with other Departments or governments or with contractors.

b. **Official Conduit.** Foreign exchange personnel may not serve as a conduit between DoD and their government for requests and transmission of classified and controlled unclassified information.

c. **Exercise of Command.** Foreign exchange personnel may not be assigned to a position that requires the exercise of command or supervision over personnel of the host DoD Component.

2. Security Requirements.

a. **Access Limitations.** Foreign exchange personnel shall not have access to restricted areas or to the following types of information:

(1) RESTRICTED DATA and FORMERLY RESTRICTED DATA;

(2) Information Security (INFOSEC) information;

(3) Classified or controlled unclassified information provided by another government, department or agency (including DoD Departments and Agencies);

(4) Compartmented information;

(5) Information bearing a special handling notice which restricts access;

(6) Any classified information that has not been authorized previously for release by the responsible designated disclosure authority to the exchange professional's government;

(7) Information that is exempt from public disclosure pursuant to DoD Directive 5230.25 and 5400.7 (references (j) and (k)).

The above limitations may be waived by the head of the host DoD Component if it has an existing agreement with the exchange professional's government that authorizes release of the specific information or with the prior written consent of the originator. However, exceptions to policy shall not be approved to accommodate the assignment of exchange personnel.

b. **Security Responsibilities.** Exchange personnel may not be given security responsibilities (e.g., escort responsibility, document custodian, security checks, etc.).

c. **Delegation of Disclosure Authority Letter (DDL).** Disclosure guidance, in the form of a DDL, will be established for each exchange position. The DDL will be prepared by the foreign exchange professional's host supervisor, in collaboration with Component disclosure officials. The DUSD(SP) for OSD, The Joint Staff and Defense Agency positions, and the designated disclosure authority for the Military Departments will approve the DDL.

The DDL must contain the information in Enclosure 5.

d. **Custody of Information.** Foreign exchange personnel shall not have custody of classified or controlled unclassified information. They may have access to the information during normal duty hours at the place of assignment when access is necessary to perform the functions set forth in the position description for the billet, provided the information has been properly authorized for disclosure.

D. PROCEDURES

1. **DPEP Criteria**. DoD Components shall consider the following criteria prior to establishing a DPEP position and discuss them in their requests for authority to negotiate an exchange agreement:

a. Likely political or military advantage to be gained;

b. Ability to adequately utilize a foreign exchange person in the organization considering the policy and access limitations and security requirements described in Sections B. and C., above;

c. Financial costs;

d. Other military arrangements with the country and the results of those arrangements;

e. Reciprocity, particularly the ability of the DoD Component to assign a person within the defense establishment of the other country.

2. **Authorized Billets**. Foreign exchange personnel normally will serve in authorized personnel billets. Exceptions to this policy may be authorized by the head of the concerned DoD Component if the assignment will result in significant military or political benefits to DoD.

3. **Position Description**. A position description, similar to that at Figure 1, will be prepared for each exchange billet.

4. **Content of DPEP Agreement**. DPEP agreements shall cover the following issues:

a. Type of exchange positions to be established.

b. Length of tour.

c. Financial responsibilities (e.g., travel, salary, etc.) and use of facilities.

d. Entitlements (e.g., commissary privileges, medical care, etc.).

e. Liabilities and claims.

f. Status of assigned personnel, to include privileges and exemptions.

g. Security.

h. Disciplinary matters.

i. Administrative matters and oversight responsibilities (e.g., leave, dress, reviews and performance reports).

5. **Administrative and Operational Control**. Foreign exchange personnel shall remain under the administrative control (e.g., pay, ratings, disciplinary actions) of their parent governments. They shall be under the operational control of the host DoD Component to which they are assigned. They may participate in the functions of the host DoD Component consistent with security considerations and the limitations described in subsection C.1., above.

6. **Supervisor Responsibilities**. The DoD official designated to supervise a foreign exchange person shall be responsible for:

a. Assuring that the person understands the duties to be performed in the position to which he or she is assigned;

b. Insuring that the person is provided access only to that classified and controlled unclassified information necessary to fulfill the duties of the position description as described in the DDL, or as otherwise authorized in writing by the originator;

c. Ensuring that co-workers are informed of the limitations on access to information by the exchange person and their responsibilities in dealing with the individual; and

d. Informing the person of his or her obligations, rights and responsibilities.

7. **Identification**.

a. **Dress.** Foreign exchange personnel shall wear their military uniform, if applicable, or wear in clear view a DoD building or installation pass or badge that identifies them as foreign nationals.

b. **Status.** Any other identification, such as business cards, issued to foreign exchange personnel by the host DoD Component shall clearly identify the person's status as a foreign exchange person.

8. **Certification of Conditions and Responsibilities.**

a. Foreign exchange personnel must sign a certification similar to that at Figure 2 prior to being assigned to the host DoD Component.

b. Foreign exchange personnel assigned to positions that might provide access to technical data also must sign a certification governing the rights of the individual and DoD with regard to inventions and rights in property.

POSITION DESCRIPTION FORMAT

1. Title of Position:

2. Position Location:

3. Qualification/Skills Required for Position:

4. Description of Specific Duties:

5. General Categories of Information to Which Access Will be Required:

6. Host Supervisor:

   Name:

   Title/Grade:

   Address:

7. Clearance Level Required for Access:

Figure 1

CERTIFICATION OF CONDITIONS AND RESPONSIBILITIES

I understand and acknowledge that I have been accepted for assignment to (name and location of organization to which assigned) as agreed between the (name of country's defense establishment) and the United States Department of Defense. I further understand, acknowledge, and certify that I will comply with the following conditions and responsibilities:

a. The purpose of the assignment is to gain knowledge of the organization, management and operation of the host defense establishment. There will be no access to technical data or other information except that which is required to perform the duties of the position to which I am assigned.

b. I will perform only functions as described in the Position Description for my work assignment, and will not act in any other capacity for my government.

c. Access to information will be limited to that information determined by my designated host supervisor to be necessary to fulfill the functions described in the Position Description for my work assignment.

d. All information to which I may have access during this assignment will be treated as information provided to my government in confidence and will not be further released or disclosed by me to any other person, firm, organization or government without the prior written authorization of the host government.

e. I have been briefed on, understand, and will comply with all applicable security regulations of the host government.

_____
(Signature)

_____
(Typed Name)

_____
(Grade/Title)

_____
(Date)

Figure 2

DELEGATION OF DISCLOSURE AUTHORITY LETTER (DDL) FOREIGN VISITORS AND EXCHANGE PERSONNEL

The following DDL format should be used by DoD Components. While all elements identified should be provided in the general order shown, information should be presented in the clearest and easiest-to-use manner.

TITLE: **DATE:**

1. **CLASSIFICATION:** Identify highest classification of information to be disclosed.

2. **DISCLOSURE METHODS:** E.g., oral, visual, or documentary. If documentary access is permitted, control procedures must be described in paragraph 7., below.

3. **CATEGORIES PERMITTED:** Specify NDP categories to be disclosed.

4. **SCOPE:** Specify who is authorized to release material or information, and to whom disclosure is authorized.

5. **AUTHORIZED FOR RELEASE/DISCLOSURE:** Describe material, information, and documents to which access can be permitted. If access is permitted to information described in Enclosure 4, subsection C.2.a., the specific agreement or other written authorization on which access is based must be cited.

6. **NOT AUTHORIZED FOR RELEASE/DISCLOSURE:** Describe material, information and documents, or portions thereof, to which access is not permitted.

7. **PROCEDURES:** Specify review and release procedures for information that is not covered by the DDL, and describe controls and special security procedures (e.g., badges, briefings) established to limit access to information and controlled areas.

8. **REDELEGATION:** Specify the extent of redelegation of authority (if any) permitted to subordinate activities.

OVERVIEW OF VARIOUS ASPECTS OF FOREIGN VISITS AND DISCLOSURE

ASPECT	D5230.20	D5230.20NOTES	D5230.XX	D5230.XXNOTES	ARMY	ARMY NOTES	NAVY	NAVY NOTES	AF	AF NOTES	CON
REFERENCE		FOR. REPS		EXCHANGES	AR 380-10		OP 5510.48		AR 200-9		
REFERENCE:CLASSIFIED MAT.	NDP-1				AR 380-10	COVERS BOTH	OP 5510.48	COVERS BOTH	Y	NEED TO VERIFY	
REFERENCE:UDTI	2040.20				AR 70-1		N	NEEDED	Y	NEED TO VERIFY	
REFERENCE:UDTI	5530.24				AR 380-66						
REFERENCE:UDTI	5530.25										
GENERAL REQUIREMENTS											
DDAL LIMITS NOT REVEALED	I	DDL DEF IN APP.	I	DDL DEF IN APP.	I		Y		N		
UDTI COVERED IN DISCL	I		I		Y		N		I		
DOD SPONS/EXEMPT ITAR	Y		NA		N		Y		N		
CONTACT OFFICER REQ'D	N		N		N		Y	GOOD IDEA	N		
REPT UNUSUAL PERSISTENCE	N		N		N		Y	GOOD IDEA	N		
PEP ON 1:1	N		N	QUID PRO QUO			I		N	SEE NOTES	
POLICY RESP	Y		I		DCSINT		OP-13		CVAII		CLE
NO DOD SPONS IF UNRELATED	N	NEEDED	NA		I		Y		I		
TYPES OF VISITS	Y		N		I		N	NOT SPECIFIED	Y		
ONE-TIME	Y		N	NEEDED	I		N	NOT SPECIFIED	Y		
RECURRING	Y		N	NA	I		N	NOT SPECIFIED	N		NE
EXTENDED	Y		Y		I		N	NOT SPECIFIED	Y		
APPL. BY PROG. TYPE	I		NA		I		I		I		
DEA	I		NA		I		I		I		
IEP	I		NA		I		I		I		
IACP/MOUS	I		NA		I		I		I		
SPECIAL EXCLUSIONS	N		N		N		Y		N		
FACILITIES/ACTIVITIES	N		N	NA	N		Y	SHIPBLDG, NUC	N		
COM/CRYPTO	N		N	?	N		Y		N		
SEC. PHONE/FAX	N		N	?	N		Y		N		
COUNTRIES/GROUPS	N	PROBABLY NEEDED	N	PROBABLY NEEDED	Y	NEEDS EXP.	I	NEEDED	Y	NEEDS EXP.	NEEDS
ACCREDITED PERSONNEL	N	NEEDED	N		N		N		N	SEE NOTES	BASIC
APPROVAL	N		N		Y		Y		I		
INTEGRATION PROHIBITED	N		N	NEEDED	Y		Y		I	NEED TO VERIFY	
FOREIGN LIAISON OFFICERS	Y		NA		Y		Y		Y		
APPROVAL	Y		NA		Y		Y		Y		
PERSONNEL EXCHANGE PROGRAM											
PROCEDURES	NA		Y		Y		Y		Y		
APPROVAL/CRITERIA	NA		Y		Y		OP 13		Y		
APPROVED POSITION DESC.	NA		Y		Y		Y		Y		
TOUR REPT	NA		N	PROBABLY NEEDED	N	PROBABLY NEEDED	Y		Y		
CONTACT OFFICER	NA		N	NEEDED	N	NEEDED	Y		N		
IND. DISCL. GUIDANCE	NA		N	NEEDED	I	NEEDED	Y	GOOD IDEA	N	NEEDED	
PEP ON 1:1 BASIS	NA		Y	SEE NOTES	N	SEE NOTES	I	"TWO-WAY EXCH"	N		OU
RESTRICTIONS	Y	NEEDS CLAR.	Y	NOT REPRESENT.	Y		Y	NOT REPRESENT.	N	NEEDED	M

VISITS AND DISCLOSURE

D5230.XX	D5230.XXNOTES	ARMY	ARMY NOTES	NAVY	NAVY NOTES	AF	AF NOTES	COMMENTS
	EXCHANGES	AR 380-10		OP 5510.48		AR 200-9		
		AR 380-10 AR 70-1 AR 380-66	COVERS BOTH	OP 5510.48 N	COVERS BOTH NEEDED	Y Y	NEED TO VERIFY NEED TO VERIFY	
I	DDL DEF IN APP.	I		Y		N		
I		Y		N		I		
NA		N		Y		N		
N		N		Y	GOOD IDEA	N		GOOD IDEA
N	QUID PRO QUO	N		Y	GOOD IDEA	N		GOOD IDEA
I		DCSINT		OP-13		CVAII	SEE NOTES	CLEAR IN ALL SVC REGS
NA		I		Y		I		NEEDED
N		I		N	NOT SPECIFIED	Y		
N	NEEDED	I		N	NOT SPECIFIED	Y		
N	NA	I		N	NOT SPECIFIED	N		NEEDS CLARIFICATION
Y		I		N	NOT SPECIFIED	Y		
NA		I		I		I		SEE NOTES
NA		I		I		I		
NA		I		I		I		
N		I		I		I		
N	NA	N		Y	SHIPBLDG, NUC	N		SHIPBUILDING
N	?	N		Y		N		
N	?	N		Y		N		
N	PROBABLY NEEDED	Y	NEEDS EXP.	I	NEEDED	Y	NEEDS EXP.	NEEDS TO INCL. N-S CONCERNS
N		N		N		N	SEE NOTES	BASIC RIGHTS OF AO NOT CLEAR
N		Y		Y		I		
N	NEEDED	Y		Y		I	NEED TO VERIFY	
NA		Y		Y		Y		
NA		Y		Y		Y		
Y		Y		Y		Y		
Y		Y		OP 13		Y		
Y		Y		Y		Y		
N	PROBABLY NEEDED	N	PROBABLY NEEDED	Y		Y		
N	NEEDED	N	NEEDED	Y		N		
N	NEEDED	I	NEEDED	Y	GOOD IDEA	N	NEEDED	
Y	SEE NOTES	N	SEE NOTES	I	"TWO-WAY EXCH"	N		QUID-PRO-QUO POLICY?
Y	NOT REPRESENT.	Y		Y	NOT REPRESENT.	N	NEEDED	MAY NOT REPRESENT

ASPECT	D5230.20	D5230.20NOTES	D5230.XX	D5230.XXNOTES	ARMY	ARMY NOTES	NAVY	NAVY NOTES	AF	AF NOTES
SEEP PROGRAMS										
PROCEDURES	N		N		I		Y		Y	NEED TO VERIFY
APPROVAL	N		N		I		OP98F		*	NEED TO VERIFY
APPROVED POSITION DESC.	N		N		I		Y		*	NEED TO VERIFY
REPORT REQ'D	N		N		I		Y		*	NEED TO VERIFY
CONTACT OFFICER	N		N		I		Y		*	NEED TO VERIFY
IND. DISCL. GUIDANCE	N		N		I		Y		*	NEED TO VERIFY
1:1 EXCHANGE	N		N		I		I	SEE NOTES	*	NEED TO VERIFY
RESTRICTIONS	Y	NEEDS CLAR.	Y	NOT REPRESENT.	I		Y	NOT REPRESENT.	*	NEEDED
VISITS TO CONTRACTORS										
PROCEDURES	N		N		Y		Y		Y	
APPROVAL	N		N		Y		Y		Y	
DEL PROC. SPEC'D	N	NEEDS TO BE EXPL.	N		Y		Y		Y	

D5230.XX	D5230.XXNOTES	ARMY	ARMY NOTES	NAVY	NAVY NOTES	AF	AF NOTES	COMMENTS
	N	I		Y		Y	NEED TO VERIFY	
	N	I		OP98F		*	NEED TO VERIFY	
	N	I		Y		*	NEED TO VERIFY	
	N	I		Y		*	NEED TO VERIFY	
	N	I		Y		*	NEED TO VERIFY	
	N	I		Y		*	NEED TO VERIFY	
	N	I		I	SEE NOTES	*	NEED TO VERIFY	
AR.	Y	I		Y	NOT REPRESENT.	*	NEEDED	MAY NOT REPRESENT
	N	Y		Y		Y		
	N	Y		Y		Y		
EXPL'.	N	Y		Y		Y		