Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

PROGRAM SECURITY INSTRUCTION FOR

[Option: Insert the purpose of the agreement for which the PSI is being prepared, e.g., COOPERATION IN THE DEVELOPMENT, PRODUCTION AND FOLLOW ON SUPPORT]

OF THE

[Option: Insert the name/type of system or program]

(SHORT TITLE: **[Option: Insert the name of the system or program]** PSI)

Issued by

[Option: Insert the name and address of the Program Management Office]

Effective Date:
[Option: Insert the date on which the PSI is approved by last National Security Authority (NSA)/Designated Security Authority (DSA)]

Disclaimer: This document is provided to students of the IPSR Course as a sample document of a program security instruction for educational purposes only.

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

DISTRIBUTION LIST

PARTICIPANTS	**No. of COPIES**
[Option: List the Participants' governmental offices and prime contractors that are to receive copies of the PSI.]	1

AMENDMENT SHEET
(Guidance: To be filled in as changes to the PSI are approved)

SERIAL	REFERENCE	DATE	SIGNATURE & NAME

PREPARATION GUIDANCE:

a. The PSI is the single-source procedural security document for Program Participants and Participating Contractors in an international program. It should explain how program classified information and controlled unclassified information are to be marked and handled procedurally (e.g., storage, transfers, access) during the course of the program. It must contain all of the security procedures for the program and rationalize any differences in the security procedures of the participating nations, and/or NATO (for NATO programs or when NATO is involved in a "hybrid" program). Therefore, it must be approved by all of the participating nations. Its content is based on Multinational Industrial Security Working Group (MISWG) document #5 and the other MISWG documents (available at www.avanco.com). However, only those MISWG documents that are to be used in the program should be included in the PSI. While the PSI is an important Program document that is used to standardize and facilitate security arrangements for an international program, it is not *just* a security document. When it is used in conjunction with applicable International Traffic in Arms Regulations (ITAR) exemptions, it will significantly facilitate exports of technical data and articles, by having pre-arranged security procedures agreed to by all parties, in advance, in place.

b. To be most effective, the PSI must be completed before involvement in a program by foreign contractors. Therefore, its preparation should begin as soon as there is a decision to include foreign participation in the program. Ideally, it should be prepared concurrent with the negotiation of the program MOU or MOA.

c. The development of the PSI should be the product of a team effort, involving representatives of ALL Participants and those Participating Contractors that have been identified. Contractors often will have the best ideas regarding procedures that will be required. However, the U.S. PM and his/her counterparts in the other countries that are participating in the program ultimately must provide guidance on the security procedures that will be used in the program and endorse it before it goes to the NSAs/DSAs for approval. The international program PM is responsible for the management of the program and the development of the Program Security Instruction document. A security committee or security working group (WG) should be organized to develop the PSI, and to

address security issues during the course of the Program. The Security Committee or WG should report to the Steering Committee (if there is one), or to the international program PM. It should be co-chaired by the international Program Management Office (PMO) Security Manager and the NSA/DSA of the country where the committee or WG meets.

d. If there is a Program Protection Plan (PPP) for the program (see DoD Directive 5200.39), the U.S. participants that are involved in the preparation of the PSI must ensure that the requirements of the PPP are considered and included in the PSI, as applicable. It also should be recognized that the PPP likely will not be releasable to the foreign participants; therefore the U.S. participants will have to explain the rationale for some requirements.

e. One issue that requires special attention in light of U.S. third party transfer restrictions is access to any export controlled information, classified or unclassified, by third country nationals that may be employed by the other Participants. If this situation occurs, and the handling of the situation is not covered by the program agreement, it must be covered by the PSI.)

f. This Generator provides suggested procedures and language only. Each PSI must be tailored to the program, taking into consideration the security requirements for the program agreement, as well as the other participating countries and their national procedures.

FOREWORD

A. BACKGROUND

The **[Option: insert the name of the program]** Memorandum of **[Option: insert either Understanding or Agreement, as applicable]** provided for the **[Option: insert the purpose of the basic MOU or MOA, e.g., co-development]** by the Governments of **[Option: insert the identities of the Participants to the MOU or MOA, e.g., the Ministry of Defense of France, the Ministry of Defense of Germany, and the Department of Defense of the United States]** of the **[Option: insert the name of the system involved, e.g., Short Range Air Defense System].**

B. AUTHORITY

Section **[Option: insert the applicable section of the program MOU or MOA or other source document that established the requirement, e.g., Section XII, paragraph 12.6 of the Short Range Air Defense MOU, dated 12 August 1999]** requires the preparation of this Program Security Instruction (PSI).

(GUIDANCE: The above requirement usually emanates from the program agreement for non-NATO programs/projects. A "NATO Program/Project" is one that is approved by the Council and is managed by a *NATO management agency/office*, using *NATO regulations*. Such programs also may be commonly funded. A PSI and Program Security Classification Guide or a Security Aspects Letter (SAL) and Security Classification Checklist are required by NATO policy for all NATO system programs or projects. Major NATO programs involving several NATO nations and/or their contractors normally will require a PSI. A PSI that is reduced in scope may be used instead of a SAL for other NATO programs, but the decision in this regard rests with the responsible NATO management agency/office.

C. APPROVAL

This PSI is issued by the Program Management Office (PMO) with the approval of the Participants' National Security Authorities/Designated Security Authorities (NSAs/DSAs).

(GUIDANCE: For NATO programs, the management office normally will be a NATO Production and Logistics Organization (NPLO) chartered agency or office, operating under a Council approved Directive. The NATO Office of Security (NOS) normally will serve as the NATO NDA/DSA in such case.)

TABLE OF CONTENTS

(Guidance: The following entries reflect the use of all of the MISWG documents. However, not all of them may be used in a particular program. The person or persons who prepare(s) the PSI must use only those procedures that have been agreed upon by the security authorities of all of the Participants.)

ANNEXES

(GUIDANCE: The procedural documents listed at items A through L, below, represent procedures that might be used in a typical

program. Other procedures may be required depending on the organization and conduct of the program and any special needs identified by the Program Manager, the Participants, or Participating Contractors.

SECTION I

INTRODUCTION AND GLOSSARY

1.1. PURPOSE

The purpose of this Program Security Instruction (PSI) is to establish procedures and assign responsibilities for the implementation of security requirements prescribed by the **[Option: insert either Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA), as applicable] [Option: insert either between or among, as applicable]** the **[Option: insert the identities of the Participants to the MOU or MOA, e.g., the Ministry of Defense of France, the Ministry of Defense of Germany, and the Department of Defense of the United States]** concerning **[insert the purpose of the effort, e.g., Cooperation in the Development, Production and Follow On Support)** of the **(insert the name of the system or product]** (Short Title: **[Option: insert the program name] [Option: insert either MOU or MOA, as applicable]**, dated **[Option: insert the effective date of the MOU or MOA]**. It provides specific security procedures that shall be followed for the Program. Terms used in the PSI are defined in Section 1.4, below.

1.2. AUTHORITY, RESPONSIBILITY, AND APPLICABILITY

1.3.5. . This PSI is issued by the PMO pursuant to **[Option: insert the applicable section of the MOU or MOA or other source document that established the requirement, e.g., Section XII, paragraph 12.6 of the Short Range Air Defense MOU, dated 12 August 1999,]**, and is effective from **[Option: insert the effective date shown on the front page of the PSI]**. This PSI applies to all Participants, including military and civilian personnel and Participating Contractors, involved with the Program. This PSI has been approved by the Participants' National Security Authorities or Designated Security Authorities (NSAs/DSAs), as applicable. Requests for clarification of this PSI should be directed to the PMO, which will coordinate as appropriate with the NSAs/DSAs and provide a response. Recommended changes or revisions to this PSI will be forwarded by the PMO to the NSAs/DSAs for consideration. Changes or revisions will not be made without approval of the NSAs/DSAs. The Steering Committee, established by **[Option: insert the applicable section of the MOU or MOA, e.g., Section IV of the Short Range Air Defense MOU]**, will be notified of clarifications or revisions to this PSI.

1.2.2. The Participants' NSAs/DSAs, the Program Manager and Security Officers of government organizations, and security officers of Participating Contractors that are involved in the Program are listed at Annex A. The NSA or DSA, as applicable, of each Participant listed at Annex A has overall responsibility to ensure national compliance with the security requirements of this Program. The NSA/DSA may delegate authority for industrial security, as appropriate, to a Cognizant Security Office (CSO) to oversee implementation of the PSI by Participating Contractors, after the PSI is approved.

(GUIDANCE: Some countries, such as Germany and the Netherlands, will have two NSAs – one normally at the Ministry of Interior, which has national responsibility for security policy, and the other at the Ministry of Defense (Netherlands) or Ministry of Economics (Germany) to handle industrial security matters. In developing a PSI, the lead ministry should be identified and engaged early to avoid delays. If the program is managed by NATO, the designated program management agency normally will accomplish necessary coordination with the NOS. Industrial security responsibility within the United States will be assigned to the Defense Security Service (DSS), as the U.S. CSO. DSS may in turn delegate certain responsibilities to a Defense Contract Management Agency (DCMA) representative at a contractor facility.)

1.3. SECURITY RESPONSIBILITIES

(GUIDANCE: The program MOU or MOA normally will identify those entities that are responsible for the security requirements that are described in, or are derived from, the MOU/MOA. The responsibilities listed here must be consistent with the MOU/MOA, as well as national regulations, or the NATO security document C-M(55)15(Final), as applicable. The responsibilities listed below are typical, but not necessarily pertinent to all programs. For example, in some cases the steering committee may choose to indorse the PSI before the PSI is forwarded to the NSAs/DSAs for approval. Nevertheless, ultimate authority to approve disclosure and security requirements, and changes thereto, always will rest with the NSA or DSA.)

1.3.1. Program Steering Committee. The Steering Committee is responsible for overseeing and enforcing implementation of security aspects of the Program.

1.3.2 Program Manager. The Program Manager is responsible

for the overall security of the Program, to include the following:

1.3.2.1. Ensuring implementation of the security procedures for the Program, in coordination with the NSAs/DSAs.

1.3.2.2. Reviewing recommended revisions to the PSI and forwarding proposed revisions to the NSAs/DSAs for final approval.

1.3.2.3. Preparing and forwarding the Program Security Classification Guide for approval, as well as revisions thereto.

1.3.2.4.Ensuring that the Participants' Contracting Officers and Participating Contractors' Contract Managers include security requirements in contracts and subcontracts and Invitations to Tender (ITT) or Requests for Proposal (RFP), obligating contractors and sub-contractors to comply with the security requirements of the Program **[Option: insert either MOU or MOA, as applicable]** and this PSI.

1.3.2.5. Appointing a Security Manager at the PMO to enforce the execution of the security requirements and procedures that are described in this PSI

1.3.2.6. Ensuring that prescribed actions are taken in the event of inventory discrepancies, losses or compromises, and security breaches in accordance with **[Option: insert the applicable sections and/or paragraphs of the PSI that deal with this issue, e.g., Section II, paragraph 2.3.4 and section 2.5 of this PSI]**.

1.3.3 PMO Security Manager. The PMO Security Manager is responsible for the following:

1.3.3.1. Enforcing the implementation of this PSI.

1.3.3.2. Day-to-day management of all Program security procedures.

1.3.3.3. Preparation and coordination of recommended updates to this PSI.

1.3.3.4. Maintaining effective liaison with the NSAs/DSAs and the security managers of the Participants and their Participating Contractors.

1.3.3.5. Chairing the **[Option: insert Program Security Committee, Security Working Group, or other group that is organized by the Participants to oversee the security aspects of the Program].**

1.3.4 NSAs/DSAs of the Participants. The NSA or DSA, as applicable, of each Participant is responsible for:

1.3.4.1. Approving this PSI and any changes thereto.

1.3.4.2. Providing security advice on the preparation of and revisions to the Program Security Classification Guide

1.3.4.3. Resolving conflicts that may arise regarding implementation of the procedures described in this PSI.

1.3.5 Participating Contractors. Participating Contractors and their sub-contractors are responsible for:

1.3.5.1. Implementing this PSI at their facilities.

1.3.5.2. Appointing a Security Officer at each facility where Program information is generated, used, or stored, who shall be responsible for the safeguarding at that facility of Program information and material and for executing the security requirements and procedures outlined in this PSI.

1.3.5.3. Ensuring that actions prescribed by this PSI and national regulations are taken in the event of inventory discrepancies, losses or compromises, and security breaches, and that the PMO Security Manager and the Participant's NSAs/DSAs or CSOs, as applicable, are immediately notified of same.

1.4 GLOSSARY OF TERMS

(GUIDANCE: The terms listed below are typical of those that will be used in a PSI. However, the terms to be defined in this section should be only those that are used in the text. Other terms may have to be added and some may have to deleted, depending on program requirements.)

ACCESS

The ability and opportunity to obtain knowledge of Program information.

AUTOMATED INFORMATION SYSTEM (AIS)

An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information, and textual material.

AUTOMATED INFORMATION SYSTEM SECURITY

All security safeguards needed to provide an acceptable level of protection for Automated Information Systems and the data processed on them.

BACKGROUND INFORMATION

Program information not generated in the performance of the Program (i.e., provided from outside the Program by one of the Participants).

CLASSIFICATION AUTHORITY

The authority vested in a government official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

CLASSIFIED CONTRACT

Any Contract that requires or will require access to classified information by a Contractor or his/her employees in the performance of the contract. (A Contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a “Classified Contract” are also applicable to all phases of pre-contract activity, including solicitation (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Contracting Agency program or project which requires access to classified information by a Contractor.

CLASSIFIED INFORMATION

Official information that requires protection in the interests of national security and is so designated by the application of a security classification marking.

(GUIDANCE: For a NATO program, there are four levels of security classification: COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), AND NATO RESTRICTED (NR). If U.S. or UK nuclear information is involved, the term ATOMAL will be added to the classification, i.e., NATO SECRET ATOMAL (NSA). Certain NATO Unclassified information will bear dissemination and access controls, similar to U.S. For Official Use Only information. These restrictions must be honored; the NATO Information Management Policy (NIMP) must be consulted for the applicable procedures.)

CLASSIFIED MEETING

A conference, seminar, symposium, exhibition, convention, or other gathering that is conducted by a Participant or by a cleared Participating Contractor, or in which they participate, with PMO approval and sponsorship, during which classified information is disclosed.

COGNIZANT SECURITY OFFICE (CSO)

The government office or agency designated by a NSA/DSA to implement industrial security requirements of the Program.

(GUIDANCE: Usually only the United States designates a CSO. Most other nations centrally manage the industrial security aspects of international programs in the office of their NSA. The CSO for the United States is the Defense Security Service (DSS).)

COMPROMISE

The disclosure of classified information or controlled unclassified information to an unauthorized person.

CONTRACTOR

Any commercial, industrial, educational, or other civilian entity that enters into a legally binding arrangement with a Participant or with a Participating Contractor to provide goods or services.

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Unclassified information to which access or distribution limitations have been applied in accordance with national laws and regulations. Whether the information is provided or generated under the Program MOU/MOA, the information will be marked to identify its "in confidence" nature. It could include information that has been declassified, but remains controlled.

(GUIDANCE: For the U.S., CUI is information that has been determined to be exempt from public disclosure under the Freedom of Information Act and is subject to access and distribution limitations, and includes such information as company proprietary information and certain export controlled information. The information normally is marked "For Official Use Only" or "FOUO". Material containing export-controlled information should bear an export control warning notice. Under a NATO Program, NATO Unclassified (NU) information may fall within this category. NU information is official NATO information that is similar to U.S. "For Official Use Only" information. If NU information is involved, decisions will have to be made on how it will be marked and handled (normally this will be the same as for CUI) and the details will be described in the text of the PSI.)

COURIER

An appropriately cleared and authorized employee of a Participant or a Participating Contractor who is approved pursuant to this PSI to hand carry classified material to its destination.

DERIVATIVE CLASSIFICATION

The process of determining whether information has already been originally classified and, if it has, ensuring that it continues to be identified as classified by marking or similar means when included in newly created material.

DESIGNATED SECURITY AUTHORITY (DSA)

The office that is designated by national authorities to be responsible for international industrial security matters. The DSA, when one is designated, has security oversight responsibility for cooperative programs.

(GUIDANCE: Only the United States currently has a DSA; the NSAs

of most other nations perform all of the functions prescribed in the PSI. The DSA for the United states is the Deputy Under Secretary of Defense for Technology Security Policy and National Disclosure Policy (DUSD/TSP&NDP). The Director, National Disclosure Policy Directorate carries out many of the responsibilities of the DUSD/TSP&NDP. The ODUSD/TSP&NDP will typically delegate certain responsibilities under a PSI, after approving it, but the DUSD/TSP&NDP will always be identified in a MOU, MOA, or PSI as the U.S. DSA.)

DESIGNATED GOVERNMENT REPRESENTATIVE (DGR)

A person designated at a contractor facility by the NSA/DSA, or CSO, as applicable, to ensure that prescribed security requirements are followed for international transfers by a releasing facility and approve and oversee the transfer of classified material on behalf of the releasing government. A DGR at the receiving facility ensures the material is received in proper order and inventoried, and accepts the material on behalf of the receiving government.

(GUIDANCE: The U.S. DGR always will be a DSS representative or another U.S. Government employee, such as a Defense Contract Management Agency (DCMA) representative, appointed by DSS.)

DOCUMENT

Any recorded information including, but not limited to, any letter, note, minute, report, memorandum, signal/message, sketch, stencil, carbon, typewriter ribbon, photograph, film, map, chart, plan, computer chip, tape recording, magnetic recording, and other forms of recorded information.

FACILITY SECURITY CLEARANCE

An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information up to and including a specified classification level.

FOREGROUND INFORMATION

Program information generated in the performance of the Program.

GOVERNMENT-TO-GOVERNMENT CHANNELS

Official government channels (e.g., military courier service, diplomatic courier service, military postal channels, or government approved secure electronic communications).

GOVERNMENT-TO-GOVERNMENT TRANSFER

Transfers through government-to-government channels or through other channels that have been agreed in writing by the sending and receiving governments. (In the latter case, the procedures must provide for accountability and control from the point of origin to the ultimate destination.)

PROGRAM MANAGEMENT OFFICE

The office, headed by the Program Manager (PM), that is established for the management of the Program.

MATERIAL

Any product or substance (including documents and equipment) on or in which information is embodied.

NATIONAL SECURITY AUTHORITY (NSA)

The entity of the government of each Participant country who is responsible for national security policy guidance.

(GUIDANCE: The NSA for the United States is the Secretary of Defense for the purposes of cooperative arms programs.)

NEED-TO-KNOW

For the purpose of this PSI, a determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information in order to accomplish a designated and approved Program function.

NETWORK

An AIS term meaning a structure composed of a communications medium and all components attached to that medium the purpose of which is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

ORIGINAL CLASSIFICATION

An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

PARTICIPANTS

The signatories to the Program MOU/MOA.

PARTICIPATING CONTRACTORS

Contractors or subcontractors authorized to take part in the Program as the result of their being legally bound to comply with the provisions of a contract.

PROGRAM

Program, as used in this PSI, refers to the **[Option: insert the name of the program]** approved by the **[Option: insert the name of the program MOU or MOA, as applicable, and date].**

PROGRAM EQUIPMENT

Any material, equipment, end item, subsystem, component, special tooling or test equipment jointly acquired or provided for use in the Program.

PROGRAM INFORMATION

Any information provided to, generated in, or used in the Program regardless of form or type, including, but not limited to, that of a scientific, technical, business, or financial nature, and also including photographs, reports, manuals, threat data, experimental data, test data, designs, computer software, specifications, processes, techniques, inventions, drawings, technical writings, sound recordings, pictorial representations, and other graphical presentations, whether in magnetic tape, computer memory, or any other form and whether or not subject to copyright, patent, or other legal protection. It includes both Background and Foreground Information.

PUBLIC DISCLOSURE

The passing of information and/or material to the general public, or any member of the general public, by any means of communication.

SECURITY VIOLATION

Any act of commission or omission that is contrary to the provisions of the security requirements of the Program **[Option: insert MOU or MOA, as applicable]** or this PSI, and which could result in the loss or compromise of Program Information.

THIRD PARTY

A government other that the governments of the Participants and any person or other entity whose government is not the government of the Participants. For the purpose of this PSI, contractors that are located or incorporated in the country of a non-Participant, and persons who are citizens or nationals of a country that is a non-Participant, are third parties.

TRANSMISSION

The transmitting (i.e., sending) of information in any form from one place to another. Transmission may occur by radio, microwave, laser, or other non-connective methods, as well as by cable, wire or other connective medium. Transmission also includes the actual transfer of information in material form from a consignor (the sender) to a consignee (the recipient).

SECTION II

SECURITY INSTRUCTIONS

2.1 GENERAL PRINCIPLES

[Option 1: for non-NATO programs involving one or more non-NATO countries use the following language:]

2.1.1 All classified information that is provided, exchanged, held, used, or generated in connection with this Program shall be stored, handled, safeguarded, and transmitted in compliance with the national laws and regulations of the Participants and this PSI. The NSAs/DSAs, in coordination with the Program Manager, shall resolve any conflicts that may arise in the application of specific policies and procedures.

[Option 2: for non-NATO programs involving NATO countries, use the following language. The added phrase serves only as a baseline to assure the application of common security procedures, and does not mean that NATO procedures will be used or that the program is a "NATO Program"]

2.1.1 All classified information that is provided, exchanged, held, used, or generated in connection with this Program shall be stored, handled, safeguarded, and transmitted in compliance with the national laws and regulations of the Participants, provided they result in a degree of protection no less stringent than that provided by the NATO security document C-M(55)15(Final), and this PSI. The NSAs/DSAs, in coordination with the Program Manager, shall resolve any conflicts that may arise in the application of specific policies and procedures.

[Option 3: for NATO Programs, i.e., those that have been approved by the Council and will be managed by a NATO management agency under NATO procedures, use the following language. It means that the NATO security procedures will be used, to the extent there is no conflict with the PSI.]

2.1.1 All classified information that is provided, exchanged, held, used, or generated in connection with this Program shall be stored, handled, safeguarded, and transmitted in compliance with the NATO security document **[cite current number]**, and this PSI. The NSAs/DSAs, in coordination with the Program Manager, shall resolve any conflicts that may arise in the application of specific policies and procedures.

[Option 1: If the only information involved in the program is each Participant's national information, use the following language.]

2.1.2 Access to classified information and material shall be restricted to facilities and persons that have the requisite level of facility or personnel security clearance, and that have a need to know for the purpose of this Program. Access to RESTRICTED information and Controlled Unclassified Information will be in compliance with Sections 2.3 and 2.4, below. In any case, access shall be approved for only that information necessary to satisfy the portion of the Program in which the person or facility is engaged.

[Option 2: If NATO information is involved, use the following language.]

2.1.2 Access to classified information and material shall be restricted to facilities and persons that have the requisite level of facility or personnel security clearance, and that have a need to know for the purpose of this Program. Access to RESTRICTED information and Controlled Unclassified Information will be in compliance with Sections 2.3 and 2.4, below. In any case, access shall be approved for only that information necessary to satisfy the portion of the Program in which the person or facility is engaged. All persons who will have access to NATO information shall be briefed on NATO security procedures and acknowledge their responsibility for protecting the information.

2.1.3 Classified information will be transmitted only through government-to-government channels or other channels that have been agreed in writing by the sending and receiving governments (i.e., "government-to-government transfer"). Upon receipt, it will either retain its original classification markings or be marked with a classification marking that will assure a degree of protection at least equivalent to that required by the originator.

2.2 INTERNATIONAL TRANSFER OF INFORMATION, DATA, OR MATERIAL

2.2.1. A transfer may occur as the result of information being provided by one Participant or Participating Contractor to another Participant or Participating Contractor through material or electronic means. The standard means of transferring classified information and material across international borders is through government-to-government channels, as defined in Section 1.4, or through other channels that have been agreed upon in writing by the NASs/DSAs of the Participants (i.e., a "government-to-government transfer"). The following procedures are approved for this program.

2.2.1.2. Material Through Government Channels. For the Program, the government channels to be used will be in compliance with the national regulations of the dispatching and receiving Participants' governments. Authorized government channels include the diplomatic or military channels of the Participants' governments, specifically military courier, diplomatic pouch, or military postal channels. The NSAs/DSAs or CSO of the Participants or Participating Contractors that are involved in a transfer will

agree in advance on the procedures to be used for a transfer.

2.2.1.3. Hand Carriage of Material. To meet an urgent need to transfer classified documents and program equipment or components among Program Participants and Participating Contractors, arrangements for hand carriage may be approved by the responsible NSAs/DSAs. Hand carriage by Participating Contractor employees may be used on a case-by-case basis when official government-to-government channels are not reasonably available, or transmission through government channels would result in an unacceptable delay that will adversely affect performance on the Program or a Program contract, and it is verified that the information is not available at the intended destination. Classified material being hand carried shall be of such size, weight, and configuration that it can remain in the personal possession of the courier. It shall be sealed, shall not be opened enroute, and shall be delivered direct from the originating point to the destination. The hand carrying of classified material shall be accomplished in accordance with the procedures at Annex B. The oversight of the day-to-day aspects of these procedures shall be supervised by the responsible NSA/DSA or CSO, as applicable. The use of the hand carriage procedure is restricted to the Participating Contractors that are identified in the List of Security Cleared Facilities (see Section V, paragraph 5.2 of this PSI). The modification of the procedures is not permitted without the approval of the Participants' NSAs/DSAs.

(GUIDANCE: Multinational Industrial Security Working Group (MISWG) document # 1 will be used when hand carrying of classified material is to be permitted. However, it must be tailored to fit the needs of the particular program.)

2.2.1.4. Secure Electronic Communications. Secure government-approved communications channels may be used for the transmission of classified information, and such CUI as may be agreed by the Participants. The decision to authorize the use of secure communication channels in the Program shall be approved by the NSAs/DSAs. Upon approval of the concept by the NSAs/DSAs, a written procedure shall be agreed among the communications security authorities of the Participants. The installation and use of communications security equipment shall be in compliance with the national security regulations of the Participants.

(GUIDANCE: If secure voice, fax, or digital communications are to be used, this section must indicate the methods that have been

approved, the approval authorities, who has authority over the use of the method, and who is responsible within the Program. The section must provide for a detailed secure communications plan, which would be included at Annex C to the PSI. If the requirement is being prepared for a NATO Program, the plan must be consistent with the applicable NATO INFOSEC policy. The ODUSD/TSP&NDP or DSS may be consulted for plans that have been approved for other programs. If used, the detailed procedures normally will be at Annex C.)

2.2.1.5. Classified Material as Freight.

2.2.1.5.1. International Transmission. Prior to the international transmission of Program classified material as freight, the consignor and consignee shall jointly prepare a Transportation Plan for the approval of their NSAs/DSAs. The Transportation Plan must provide for secure transport from the point of origin to the ultimate destination. A generic Transportation Plan shall be prepared for the Program; a Notice of Consignment shall be prepared for individual consignments. They will be prepared in compliance with the guidelines at Annex D. The generic Transportation Plan shall be included as Annex D to this PSI.

2.2.1.5.2. Transmission within a Participant's Country. The transmission of classified material as freight within a Participant's country, after the Participant has assumed security control, will be in accordance with national procedures, provided they result in protection consistent with this PSI and the pertinent Transportation Plan.

2.3. MARKING OF PROGRAM INFORMATION

Documents and other material containing information provided to, generated under, or used in the Program shall be marked, in addition to any classification or control marking, with an annotation that identifies it as Program Information. Material containing Foreground Information shall be marked as such to indicate that it was generated under the Program. For Program material that contains Background Information, there shall be an annotation that identifies the fact that the material contains Background Information and the country of origin, in addition to other prescribed markings. Both Foreground and Background Information will be annotated with a statement that identifies any use, distribution or access

limitations. Each participant providing Background Information will ensure that the appropriate markings are applied prior to release to the Program. When the material is of such nature that it cannot be marked, the markings will be applied to a cover or label. The procedures for marking Program information are at Annex E.

(GUIDANCE: Background and Foreground Information and certain other Program Information may require special markings to indicate the nature of controls which are required in accordance with Program requirements, and as the result of restrictions on Background Information. DOD Directive 5230.24 contains dissemination markings that are approved for technical information, and should be used to develop Program markings. Moreover, if certain Participants do not have a RESTRICTED classification or Controlled Unclassified Information, the markings to be used by those countries to identify such information that is provided by other Participants will have to be specified. For the United States, the procedures are contained in DoD 5200.1-R. If NATO information is involved, reference and copy numbers are required on certain documents in compliance with the NATO security document. The Participants need to agree on specific markings and include them in this section, in the Program Security Classification Guide, and/or in an Annex to this PSI - an Annex is preferable.)

2.4. PROCEDURES FOR THE PROTECTION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI)

2.4.1. As required by **[Option: insert applicable section of the Program MOU or MOA that provides instructions for CUI, e.g., Section X of the (program) MOU]**, access to CUI provided to or generated in the Program shall be controlled. The procedures for protecting CUI are described below.

2.4.1.1. Protection. The information shall be stored in such a manner that unauthorized persons do not gain access to it (e.g., in a locked desk or cabinet, or a locked room to which access is controlled). It shall destroyed in such a manner that it cannot be easily reconstructed (i.e. paper copies may be shredded or torn several times before being thrown into a bin; computer disks must be erased, shredded, or degaussed before being disposed of or transferred to another office. It shall not be read or otherwise displayed in a public place. It may be transmitted by national postal service or be hand-carried; it may be single

wrapped. It must not be transmitted through non-secure electronic means, unless it is encrypted. Computers used to process the information must be configured so as to prevent unauthorized access, but do not have to be accredited for classified use, unless they also process classified information. Persons who require access do not need a security clearance, but they shall be made aware of the handling procedures and acknowledge their responsibilities for protecting the information.

2.4.1.2. Unauthorized Disclosure. Administrative action shall be taken to fix responsibility for unauthorized disclosure, and appropriate disciplinary action shall be taken against the person or persons who are determined to be responsible. The unauthorized disclosure of CUI shall be reported to each NSA/DSA and the Program Manager.

(GUIDANCE: CUI is protected by law in many countries. Legal action for permitting unauthorized access to the information also is possible if it falls within certain "exempt" categories under the U.S. Freedom of Information Act - - militarily critical technology and company proprietary information are two such categories. Nevertheless, the sensitivity of the information, and thus the measures to be used for its protection, may vary depending on the Participants and the circumstances. Therefore, the language set forth in paragraph 2.4.1.2, above, is representative only. The participants must agree on the specific measures to be adopted. NATO UNCLASSIFIED information that requires protection usually will be handled in the same way as CUI. NATO RESTRICTED is a security classification. However, it will be protected similarly to CUI.)

2.5. SECURITY CLASSIFICATION

The Program Security Classification Guide (SCG) (Annex F) is the basis for the classification, regrading, or declassification of Foreground Information. Questions concerning the content and interpretation of the classification guide, as well as proposed changes to it, will be coordinated by the PMO with the NSA/DSA for each Participant. Pending a final decision on proposed changes to classification levels, the information involved will be protected at either the current assigned level or the proposed level, whichever is higher.

2.6. CONTRACT SECURITY CLAUSES

The Participants' Contracting Officers and the Contract Managers of Participating Contractors shall ensure that all contracts and subcontracts contain provisions requiring strict compliance with the terms of this PSI. In addition, contracts shall contain the Contract Security Clauses at Annex G.

2.7. SECURITY VIOLATIONS

2.7.1. All of the Participants' civilian and military personnel and their Participating Contractors shall be obligated to report the actual or possible loss or compromise of classified information or CUI to their security office. The security office will report the incident to its NSA/DSA, through the CSO, if applicable, in addition to complying with reporting procedures prescribed by national regulations. The Participant's NSA/DSA will notify the PMO, who will notify the Steering Committee and the other NSAs/DSAs. If the incident occurs at the PMO, its Security Manager will report the incident to the NSAs/DSAs of the Participants and to the Steering Committee. The Security Officer of the facility where a violation or compromise may have occurred will investigate all such occurrences and inform its NSA/DSA of the results. Each responsible NSA/DSA will promptly and fully inform the other Participants' NSAs/DSAs and the PMO of the known details of any such occurrences, will provide updates on the investigation, and will provide final results of the investigation and of the corrective actions taken to preclude recurrences. Reports on the loss or compromise or possible compromise shall include, as a minimum, the following information:

a. A description of the circumstances.

b. The date or the period of the occurrence.

c. The date and place of discovery and location of the occurrence.

d. The security classification of the information involved in the incident and any control markings.

e. Specific identification of the information or material, to include originator, subject, reference number, date, copy number, and language.

f. A list of the information that has been compromised or material that is unaccounted for.

g. An assessment of the likelihood of compromise (i.e. "certain," "probable," "possible," or "unlikely") and the reasons for that conclusion.

h. A statement on whether the originator has been informed.

i. Actions taken to secure the material and limit further damage.

j. Responsible person(s) and reasons for loss or compromise or possible loss/compromise.

2.7.2 The above reporting requirements are in addition to any other reporting requirements of the Participants, required by national regulations.

(GUIDANCE: Reports of investigations involving NATO classified information shall be provided to the NATO Office of Security, using the procedures in the NATO security document. Such procedures should be included in the PSI for NATO programs.)

SECTION III

RELEASE OF INFORMATION

3.1. UNILATERAL RELEASE

The release of all classified or unclassified Program Information or material to other than Program Participants and Participating Contractors is prohibited without specific written approval. Requests for release will be handled in accordance with the paragraphs below.

3.2. RELEASE OF INFORMATION AND MATERIAL TO NON-PARTICIPANTS

Program Information, except that which has been approved for public release (see paragraph 3.4 below), shall not be released to any person, organization, company, or other entity that is not a Participant or a Participating Contractor, without the prior written approval of the Participant or Participants that originated or contracted for the information. Foreground Information will not be released without the prior written approval of all of the Participants. Background Information will not be released without the prior written approval of the

originating Participant. Requests for release to other entities will be submitted through the PMO to the **[Option: insert information on the officials that are designated by each Participant to receive and coordinate such requests]**.

COUNTRY	OFFICIAL	TELEPHONE Nr.	e-Mail ADDRESS

(GUIDANCE: Insert other release restrictions as may be specified in the program MOU/MOA or as agreed upon.)

3.3. RELEASE OF PROGRAM INFORMATION AT SYMPOSIA, SEMINARS, EXHIBITS AND CONFERENCES

When persons representing other than the Program Participants or Participating Contractors are present at symposia, seminars, exhibits, conferences, or other gatherings, whether at government establishments, contractor facilities, or other approved venues, speeches and presentations that involve Program Information that are to be presented shall be submitted for approval, through the PMO, to officials that are designated by the Participants to receive, coordinate, and/or approve such matters. Foreground Information will be submitted to all Participants for approval. Background Information will be submitted to the Participant that originated or contracted for the information for approval. The request for review and approval of the speeches and presentations must be submitted at least **[Option: insert the number of days agreed by the Participants]** calendar days before the date for which clearance is required. It will include the name of the requesting individual; the date of presentation; the nationality of representatives from non-participating countries and the countries represented; the title of the symposium, seminar, exhibit or conference; the text of the presentation, and other information which may be required by national regulations. The designated officials are as listed below:

COUNTRY	OFFICIAL	TELEPHONE Nr.	e-mail ADDRESS

3.4. PUBLIC RELEASE OF PROGRAM INFORMATION

3.4.1. Written approval for the public release of all Foreground Information, including publicity material, will be sought through **[Option: insert prescribed channels agreed by the Participants]** to the PMO. Participating Contractors shall ensure that their subcontractors follow the same procedures. The PMO may

reject such proposals without further recourse. However, if the PMO endorses the proposed release, the release authorization shall be made following consultation with the Participant's NSAs/DSAs. All release proposals which the PMO endorses shall be submitted to the appropriate NSA/DSA, or other public release officials of the Participants that are identified by the NSAs/DSAs, who will then grant or deny the release in accordance with national regulations. A minimum of **[Option: insert the number of days agreed by the Participants]** calendar days should be allowed for review of the proposal. The designated public release officials are as listed below.

COUNTRY	OFFICIAL	TELEPHONE Nr.	e-mail ADDRESS

3.4.2. Background Information to be publicly released shall be cleared by the appropriate originating government's public release official in accordance with national regulations. An information copy of the decision will be sent to the PMO.

3.5.3. It shall be incumbent upon the Participants and their public release offices to screen all information submitted to them for public release to ensure that: (1) it is unclassified, (2) it is technically accurate, and (3) release will not be detrimental to the national security or the Program.

3.5 EXHIBITION AUTHORIZATION FOR PARTICIPATING CONTRACTORS

Participating Contractors that disclose or display Program Information and material at exhibitions shall have available at each exhibition a copy of the document that provides authorization for the disclosure or display (see section 3.3, above). Participating Contractors shall ensure that all information on public display (e.g., at air shows, exhibitions, etc.) is displayed in the form in which it was officially authorized for disclosure or display.

SECTION IV
INTERNATIONAL VISITS

4.1 GENERAL

Visits to a facility of another Participant or Participating Contractor by persons representing a Participant or Participating Contractor require advance authorization. In order to avoid the need to submit a visit request for each

visit, maximum use shall be made of the Recurring Visit authorization, as described below. The visit request format and instructions at Annex H shall be used to request visit authorizations. Reference to the **[Option: insert the name of the program]** Program shall be included in all visit requests.

4.2 STANDARD PROCEDURES FOR INTERNATIONAL VISITS

4.2.1. Types of Visits. There are three types of international visits that may be used for the Program:

4.2.1.1. One-time Visit. A One-time Visit authorization is for a single, short-term occasion (normally less than 30 days) for a specified purpose. This type of request should be used only when there is not to be a prolonged stay in another Participant's country and the need for recurring visits cannot be anticipated.

4.2.1.2. Recurring Visit. A Recurring Visit authorization permits intermittent, recurring, short-term visits over a specified period of time, normally for the period of involvement in the Program, subject to annual review and validation. These visits should be used by persons such as engineers and program management personnel who will make frequent, recurring visits to government or contractor facilities in another Participant's country, in order to preclude the need to submit numerous requests for One-time Visits.

4.2.1.3. Extended Visit. An Extended Visit authorization is for a one-time, long-term visit for a specified period of time, subject to annual review and validation. Extended Visit authorizations should be used for persons such a liaison officers and plant representatives who will be stationed at a government or contractor facility in another Participant's country for an extended period of the program.

4.2.2 Lead Times for Requests for Visit Authorization (RVA). All RVAs that are submitted by government or Participating Contractor personnel of one Participant requesting authority to visit a facility or personnel of another Participant shall be submitted through government channels, and will conform to the established visit procedures of the host NSA/DSA. RVAs should be in the possession of the receiving (i.e., host) Participant's NSA/DSA at least **[Option: insert the number of days agreed by the Participants]** working days prior to the starting date of a One-time Visit or Extended Visit, or the date of the first visit for

Recurring Visits. In the case of requests for Recurring Visit authorizations, 72 hours (3 working days) advance notification to the host site security officer is required before each recurring visit, unless agreed otherwise in writing.

4.2.3 RVA Amendments. RVAs that have been approved or that are being processed may be amended only to change, add, or delete names and change dates, except requests for an earlier date may not be accepted. Emergency visit authorizations (see Section 4.4, below) shall not be amended.

(GUIDANCE: THE DETAILED PROCEDURES FOR RECURRING VISITS MAY APPEAR IN THE BODY OF THE PSI OR IN THE ANNEX THAT COVERS INTERNATIONAL VISITS. FOR THIS PROTOTYPE PSI, THE PROCEDURES APPEAR IN BOTH PLACES.)

4.3. STANDARD PROCEDURES FOR RECURRING VISITS

4.3.1. Recurring Visit authorizations shall be used to the maximum extent possible to avoid the need for One-time Visits and Emergency visits. However, only those persons who are actually employed on the Program and have a need to make recurring visits may be included on a request for a recurring visit authorization. The request shall be prepared as described below.

4.3.1.1. Facilities List Preparation. The PMO shall prepare and maintain a consolidated list, known as the "Facilities List," of the facilities of the Participants and Participating Contractors. (The procedures at Section V, paragraph 5.2 of this PSI, may be used to prepare the list of Participating Contractors). The "facilities List' shall be furnished to all of the facilities that are involved in the Program and to the NSAs/DSAs. The lists shall be updated if facilities leave the Program or if new facilities become involved in the Program.

4.3.1.2. Recurring Visits Request Preparation. The Security Officer of each Participant and Participating Contractor facility shall identify and prepare a list employees at their facility who will be involved in the Program and who will need to visit facilities of the other Participants or Participating Contractors on a recurring basis. They will submit the request for a Recurring Visits authorization for the listed employees through their NSA/DSA or CSO, as applicable, to obtain a security clearance verification and security assurance, following the visit request procedures at Annex H.

4.3.4. Review and Update of Visit Lists. The PMO shall initiate a review annually to update the lists of facilities and personnel that are authorized to make recurring visits. Information concerning individuals or facilities derived from One-time or Emergency requests will be added, if they are to be authorized to make recurring visits. Employees and facilities that are no longer involved in the Program shall be deleted.

4.4. PROCEDURES FOR EMERGENCY VISITS

4.4.1. General. To qualify as an emergency visit, the visit must relate to the Program, or a Program contract or announced request for proposal (RFP) or invitation to tender (ITT), and failure to make the visit reasonably could be expected to seriously jeopardize performance on the contract or program, or result in the loss of a contract opportunity. The request should be submitted no less than **[Option: insert number of days agreed by the Participants]** working days prior to the visit. Emergency visits will be approved only as a single, one-time visit. If subsequent visits may be necessary, the requester should submit a follow-up request for a Recurring Visit Authorization. The requester should coordinate the emergency visit in advance with the person to be visited. The requestor also should ensure that the complete name, grade or position, address, and telephone/telefax number and e-mail address of that person and a knowledgeable government point of contact are provided in the RVA, along with the identification of the contract, agreement, or program, and the justification for submission of the emergency visit request.

4.4.2. Procedures. Under extraordinary circumstances, an Emergency visit request may be submitted with less than the required lead-time; however emergency RVAs will not be accepted less than **[Option: insert number of days agreed by the Participants]** working days prior to the start of the proposed visit. Emergency visit requests will be critically reviewed, fully justified, and documented by the Security Officer of the requesting government or contractor facility. When the Security Officer is satisfied that the circumstances warrant an Emergency visit (see paragraph 4.4.1 above), the Security Officer will directly contact the person to be visited at the host government or contractor facility by telephone or telefax, to obtain tentative verbal agreement for the proposed visit. If tentative verbal agreement is provided to proceed with an Emergency visit,

the Security Officer of the government or contractor facility to be visited (host facility) shall then immediately notify, by the most expeditious means (e.g., telefax, e-mail, or voice, followed by written verification), its NSA/DSA that an emergency visit request will be submitted by the requesting government agency or contractor and explain the reason for the emergency. Following receipt of tentative verbal agreement from the host facility, the Security Officer of the requesting facility will send a message, e-mail, or telefax, in the RVA format, as follows:

4.4.2.1. The message, e-mail, or telefax will be sent, by priority precedence, within 24 hours of the verbal agreement for the requested emergency visit. It will be sent through the NSA/DSA of the facility of the requesting country to the NSA/DSA of the facility to be visited and to the Security Officer of the facility to be visited. Either of these officials may deny the visit.

4.4.2.2. The subject of the message will be: EMERGENCY VISIT – **[Option: insert the name of the program].** The message must contain all of the information included in the RVA format at Annex H. The name and telephone and telefax numbers of the person(s) contacted, pursuant to paragraph 4.4.2 above, will be placed in the Remarks section of the RVA.

4.4.2.3. Upon receipt of the request, each NSA/DSA involved shall confirm that the information provided meets the requirements set forth in this section and that the requesting facility is authorized access to the requested information, and provide an immediate response, by the most expeditious means. In the event a positive response is not received at least **[Option: insert the number of days agreed by the NSAs/DSAs]** working days prior to the start of the Emergency visit, the Security Officer of the facility that initiated the request shall contact the Security Officer of the facility to be visited to determine the status of the Emergency visit request.

4.4.2.4. When the NSA/DSA of the country of the host facility approves or denies the request, it shall immediately notify the Security Officer of the facility to be visited and the NSA/DSA of the requesting country of the decision. The host facility Security Officer will then notify the requesting facility Security Officer that the visit is approved or denied.

(GUIDANCE: MISWG document # 7 contains the international visit request format and instructions. The visit request format and

those instructions that are not covered above must be included at Annex H. The U.S. as well NATO and many other countries have adopted the MISWG procedures; therefore, they must be followed. It is reiterated that the Recurring Visits authorization should be used to the extent possible to avoid the need for One-time and Emergency visits.)

SECTION V

LIST OF SECURITY CLEARED FACILITIES

5.1. GENERAL

This section outlines the procedures for the development and maintenance of the list of contractor and subcontractor facilities that are involved in the Program and to which classified information or material can be distributed (Annex I). It also covers the use of the Facility Security Clearance Information (FIS) Sheet (Annex J) and the Personnel Security Clearance Information Sheet (PSCI) Sheet (Annex K).

(GUIDANCE: The format and instructions for Annexes I, J, and K are in MISWG documents #11, #12, and # 19, respectively. These procedures also apply to NATO programs. The procedures, tailored for this program, should be included here; the formats should be at annexes.)

5.2. PREPARATION OF THE LIST OF SECURITY CLEARED FACILITIES

The PMO shall prepare a list of the contractor facilities that are participating in the Program (i.e., the Participating Contractors). The level of Facility Security Clearance and storage capability of each contractor facility will be verified by each Participant's NSA/DSA, or CSO, as applicable, prior to the facility being placed on the list. The list shall include the full name and address of each facility; the address and telephone and telefax numbers and e-mail addresses of the facility Security Officers; the level of facility security clearance and storage capability; and the identity of contracts held by the facility and the level of security classification for each contract. The list shall be included at Annex I.

(GUIDANCE: Some Participating Contractors may be comprised of multiple facilities. It is important to verify the specific facilities that are to be involved in the program and ensure that

their addresses are accurate.)

5.3. DISTRIBUTION OF FACILITIES LIST The PMO, after verifying that it is correct, will distribute the Facilities List to each Participant, Participating Contractor, and NSA/DSA or CSO, as applicable.

5.4. UPDATING THE FACILITIES LIST

The responsible NSAs/DSAs shall notify the PMO immediately of any changes regarding the security status of facilities on the list. The PMO also will be notified of any additions or deletions to the Facilities List. The PMO shall disseminate amendments to the Facilities List, as required, and will issue an updated Facilities List at least annually.

(GUIDANCE: The format and procedures for the initial Facilities List, and for amendments thereto, are described in MISWG document # 11. That format and the instructions, modified as necessary to accommodate the particular program, should be used by the PMO to develop the actual Facilities List, which will be at Annex I.)

5.5 USE OF THE FIS SHEET AND PSCI SHEET

The Facility Security Clearance Information (FIS) Sheet (Annex J) and the Personnel Security Clearance Information (PSCI) Sheet (Annex K) formats shall be used to request and verify facility security clearances for facilities that are to be added to the Facilities List and the personnel security clearances for the personnel who are to make recurring visits, or who may otherwise become involved in the Program.

(GUIDANCE: The FIS sheet and the PSCI sheet will be used on a case-by-case basis as needed to request and validate individual facility and personnel clearances. Therefore, the MISWG documents, sanitized to delete reference to the MISWG, will be included at Annexes J and K as guidance. The procedure may be modified, if agreed by the Participants' NSAs/DSAs, for the particular program.)

SECTION VI

SECURITY EDUCATION AND AWARENESS

The PMO shall prepare a security education and awareness

program. Government and contractor employees who will have access to Program classified and Controlled Unclassified Information shall be briefed on, or otherwise be informed of, and acknowledge their understanding of their responsibilities for protecting the information. This may be accomplished by a briefing, the use of written material, or by electronic means. The material to be presented shall include the pertinent aspects of applicable laws and regulations; the perceived threat; procedures for handling the information during use, transmission, visits, travel, and meetings; how to handle possible losses or compromises and security violations; procedures for safeguarding classified material in the event of a man-made or natural emergency situation; special security requirements that are unique to the Program; and penalties that may be imposed for violating the security requirements of national regulation, the Program MOU/MOA, or this PSI.

(GUIDANCE: The purpose of the security education and awareness program is to ensure that all government and contractor employees in the Program are aware of the standardized procedures that apply to the Program, as well as any known threats against the Program. MISWG document # 9 should be used an outline. If NATO classified information is involved, persons involved in the program also must be briefed on or otherwise informed of and acknowledge their understanding of NATO security procedures. It is recommended that a standard briefing be prepared for the program and included as an annex to this PSI; it can be supplemented by each Participant to meet local requirements.)

SECTION VII

SECURITY PLAN IN EVENT OF TERMINATION OR EXPIRATION OF MOU OR NON-SELECTION OF CONTRACTOR

[Option: The text set forth below may or may not appear in the PSI. Text similar to that set forth below is appropriate if specific details to implement the requirements of the Program MOU or MOA are necessary, and the Participants determine that the details are to be placed in the PSI. The specific provisions set forth below are based on NATO security policy. Provisions similar to those set forth below for a non-NATO program should appear in the program MOU or MOA; they in turn should appear in program contracts, based on national requirements, or they may

appear in a SAL (for NATO contracts) or DD Form 254 (for U.S. contracts). If the details are to be included in the PSI, they must be consistent with the governing authority (e.g., the Program MOU or MOA).]

7.1. GENERAL

The purpose of this section is to describe procedures by which the Participants and Participating Contractors will dispose of Background and Foreground Information in any of the following events:

a. The Program agreement expires or is terminated,

b. Any of the Participants withdraw from the program,

c. A potential Participating Contractor receives or generates information through the ITT/RFP process, and is not selected,

d. A Participating Contractor receives and/or generates information and/or hardware during an early phase of the Program and is not selected for work on a further phase of the Program, or

e. A Participating Contractor's facility security clearance is terminated.

The responsible Participant's Contracting Officer or Participating Contractor's Contract Manager shall ensure that the terms of this section are included as an obligatory requirement of each Program contract and sub-contract.

7.2. GOVERNMENT HELD INFORMATION

[Option: the following text will be used for a non-NATO program.]

In the event of termination or expiration of the Program **[Option: insert MOU or MOA, as applicable]**, the Participants' respective rights and responsibilities with regard to Background Information and Foreground Information will be determined in accordance with the provisions of **[Option: cite the applicable section of the program MOU or MOA, e.g., Section XVIII of the (program name) MOU]**. A Participant that is authorized to retain

Background Information developed by the another Participant, or Program Foreground Information developed with the use of another Participant's Background Information, shall safeguard it in accordance with this PSI and any bilateral security of information agreement that may exist between the Participants. Moreover, such Participant shall not use that information for other purposes without the prior written consent of the Participant that provided it.

[Option: the following text will be used for a NATO program. The words, "any security of information agreement that may exist between the Participants" is replaced with "the NATO security document C-M(55)15(Final)".]

In the event of termination or expiration of the Program **[Option: insert MOU or MOA, as applicable]**, the Participants' respective rights and responsibilities with regard to Background Information and Foreground Information will be determined in accordance with the provisions of **[Option: cite the applicable section of the program MOU or MOA, e.g., Section XVIII of the (program name) MOU]**. A Participant that is authorized to retain Background Information developed by the another Participant, or Program Foreground Information developed with the use of another Participant's Background Information, shall safeguard it in accordance with this PSI and the NATO security document, C-M(55)15(Final). Moreover, such Participant shall not use that information for other purposes without the prior written consent of the Participant that provided it.

7.3. CONTRACTOR HELD INFORMATION

7.3.1. All classified or Controlled Unclassified Information that is received in the performance of, or in anticipation of, a Program contract shall be returned to the Contracting Office on completion or termination of involvement in the pre-contract activity or in the contract, unless the information has been declassified or removed from control, or authorized in writing by the Contracting Office for destruction or for retention.

7.3.2. Contractors shall return or destroy Program classified information or Controlled Unclassified Information not approved for retention in accordance with the following schedule:

7.3.2.1. If a bid, proposal, or quote is not submitted or is withdrawn, within 180 days after opening date of bids, proposals, or quotes.

7.3.2.2. If a bid, proposal, or quote is not accepted, within 180 days after notification that the bid, proposal, or quote has not been accepted.

7.3.2.3. If a successful bidder, within 2 years after final delivery of goods and services, or after completion or termination of the classified contract, whichever comes first.

7.3.3. Termination of Facility Security Clearance. In the event that a Facility Security Clearance is to be terminated, the contractor shall return all classified and Controlled Unclassified Information in its possession to the Contracting Office or dispose of such Information in accordance with instructions from the Contracting Office, the NSA/DSA, or the CSO, as applicable.

ANNEX A

LIST OF PROGRAM PARTICIPANTS

A1 NATIONAL SECURITY AUTHORITIES (NSAs) AND DESIGNATED SECURITY AUTHORITIES (DSAs)

Participants' NSA or DSA, as applicable:	United States DSA ODUSD/TSP&NDP ATTN: Director, National Disclosure Policy Directorate 2200 Defense Pentagon Washington, DC 20301-2200 Tel: 703-602-xxxx Fax: 703-602-xxxx **[Option: insert other NSAs/DSAs, as applicable]**
Participants' CSO, if applicable	United States CSO HQ Defense Security Service 1320 Braddock Place Alexandria, VA 22314-1651 Tel: 703-325-9510 Fax: 703-325-1329 **[Option: insert other CSOs, as applicable]**

A-2 PROGRAM MANAGEMENT OFFICE

Program Manager	**(insert PMO name, ATTN: PM)** **(insert address)** **(insert Telephone and Fax #)** **(Insert email address)**

PMO Security Manager **(insert PMO name, ATTN: Security Mgr)**
(insert address)
(insert Telephone and Fax #)
(insert email address)

ANNEX B

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

1. HAND CARRIAGE OF CLASSIFIED DOCUMENTS

1.1. The standard method of transmitting classified documents across international borders is through government-to-government channels. These are methods that have been determined by individual governments as being secure, and they involve constant physical control by government employees (e.g., military or diplomatic courier, military postal service, government communications channels).

1.2. To meet an urgent need to transmit classified documents between **[Option: insert the name of the programme/project or contract]** Participants and Participating Contractors that are listed in Appendix A, these Hand Carriage arrangements have been approved by the responsible National Security Authorities (NSAs)/Designated Security Authorities (DSAs). They may be used on a case-by-case basis when government-to-government channels are not reasonably available, or transmission through government-to-government channels would result in an unacceptable delay that will adversely affect performance on the programme/project or contract, and it is verified that the information is not available at the intended destination.

1.3. Administration of the day-to-day aspects of these procedures shall be handled in each country by the NSA/DSA or Cognizant Security Office, as applicable, listed in Enclosure A. Use of these procedures is restricted to the approved contractors also listed in Enclosure A. Modification of these procedures is not permitted without the approval of the participating NSAs/DSAs. Any requests for modification of this arrangement must be submitted in writing to the responsible NSA/DSA who shall coordinate the proposal with the other NSAs/DSAs.

1.4. The word "document" means any letter, note, minute, report, memorandum, sketch, photograph, film, map, chart, plan, stencil, carbon, typewriter ribbon, chip, tape recording, magnetic recording, punched card/tape, and other forms of

recorded information. (The documents must be of such size, weight, and configuration that they can be hand-carried).

1.5. The table of equivalent security classifications is at Enclosure B. Classified documents shall be marked accordingly.

1.6. The arrangements in this section apply to the hand carriage by an appointed courier of classified documents only and under circumstances when the courier can maintain personal possession of them at all times. The highest classification shall not exceed SECRET and the documents must have been authorized by the owning government for release in conjunction with the **[Option: insert the name of the programme, project, or contract]. [Option: The NSAs/DSAs may impose a lower maximum classification level on the documents to be hand carried under this arrangement. If the level of classification is to be lower, this sentence will change to reflect the level**.

1.7. The courier shall be a permanent employee of the dispatching or receiving company. **[Option: Government employees also may be used. If the NSAs/DSAs agree, other courier services may be used provided they are under contract to a Participant and they are properly cleared. If this option is used, the sentence will be changed to reflect the decision on couriers.]**

1.7.1. The courier shall be granted a personnel security clearance to at least the level of the classified documents(s) that is/are to be hand carried.

1.7.2. Before commencement of each journey, the courier shall read and sign the “Courier Declaration” at Enclosure C indicating that he/she has read and understands these "ARRANGEMENTS" and the "NOTES FOR THE COURIER," which is at Annex 2 to the "Courier Certificate" (Enclosure D).

1.7.3. The courier shall be provided with a "Courier Certificate" written in English and, as necessary, in the national language of one or more of the participating countries. The "Courier Certificate" will be stamped and signed by the NSA/DSA, Cognizant Security Office or Designated Government Representative, as applicable, and by the company Security Officer of the dispatching company. "Courier Certificates" shall be numbered to assure accountability by the issuing NSA/DSA, Cognizant Security Office or Designated Government Representative; will bear the date of the beginning of the

journey; will be valid for one journey only (the journey may include more than one stop); and must be returned to the issuing NSA/DSA, Cognizant Security Office or Designated Government Representative through the dispatching company's Security Officer as soon as possible after the end of the journey.

[Option: If permitted by national security regulations, the NSA/DSA or Cognizant Security Office may deliver to the company's Security Officer a limited number of pre-signed and pre-numbered "Courier Certificates" according to the foreseeable needs of the company for a reasonable period of time. The company Security Officer may personally authorize their use for the hand carriage of CONFIDENTIAL documents. The certificates should be pre-printed to show the name and address of the participating companies to which they are provided and the name of the programme, project, or contract for which they may be used. They will be annotated to indicate that they are valid for a single trip between the participating countries and return, and for specifically approved CONFIDENTIAL documents. If it becomes necessary to issue a "Courier Certificate" for documents classified SECRET, the NSA/DSA of the dispatching Government will be provided with the details of the requirement and will authorize the company Security Officer, the Cognizant Security Office, or the Designated Government Representative, as applicable, to issue the certificate or authorize the company Security Officer to issue the certificate, on a case by case basis, according to national regulations. If an arrangement as described herein is approved, the requirements stated herein will be included.]

1.7.4. A copy of the "NOTES FOR THE COURIER" shall be attached to the Courier Certificate. The courier is to be made aware that the non-fulfillment of the obligation to safeguard the classified information contained in the consignment entrusted to the courier and/or any other negligent action by the courier that gives rise to a security breach will constitute not only a breach of contractual obligation, but also is a matter of possible penal responsibility. In the event of a breach by the courier, the dispatching NSA/DSA that authorized the hand carriage may request the NSA/DSA in the country where the breach occurred to initiate an investigation and return the findings to the requesting NSA/DSA who may take legal action as appropriate.

1.8. The company Security Officer shall make sure that the

courier and escorts or guards (if any) that accompany the consignment have their personal expatriation and travel documentation (e.g., passport, currency, and medical documents), which are complete, valid, and current. Moreover, the NSA/DSA, Cognizant Security Office or Designated Government Representative, as applicable, shall ensure that there is a valid export license or other appropriate government authorization, if a license is required.

1.9. The "Courier Certificate" shall be as shown at Enclosure D. **[Option: the Participants may agree on other requirements to be included in the "Courier Certificate"]**

1.10. Before each used "Courier Certificate" is returned to the issuing NSA/DSA, Cognizant Security Office or Designated Government Representative, the courier shall sign the NOTE at the bottom of the "Appendix to the Courier Certificate" certifying that no situation occurred that might have compromised the security of the consignment during the journey. The declaration shall be witnessed by the company Security Officer.

1.11. The dispatching company Security Officer shall inventory the documents and 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 shall be wrapped, sealed, and placed in a container approved by the courier's national security authorities, by or in the presence of the company Security Officer, and the Cognizant Security Office or Designated Government Representative, as applicable, in accordance with national procedures.

1.11.1. The address of the Security Officer of the receiving and dispatching company or the Designated Government Representative shall be shown on the inner and outer envelope or wrapping. (Note: When there is a Cognizant Security Office or Designated Government Representative located at a cleared contractor facility, the address of the Cognizant Security Office or Designated Government Representative will be shown on the outer envelope or wrapping.)

1.11.2. The dispatching company Security Officer shall instruct the courier in all of his/her duties and ensure that

he/she understands them and completes the Declaration described in paragraph 7.2, above.

1.11.3. The dispatching company Security Officer, or the Cognizant Security Office or Designated Government Representative, shall obtain a receipt from the courier for the sealed package.

1.11.4. The courier shall be responsible for the safe custody of the classified documents until such time that they have been handed over to the receiving company Security Officer, or the Cognizant Security Office or Designated Government Representative, and a receipt has been provided as evidence of delivery.

1.11.5. The receiving company Security Officer, or the Cognizant Security Office or Designated Government Representative, shall sign both copies of the receipt in the package. One copy shall be returned to the courier. On his/her return, the courier shall pass the completed receipt to the dispatching company Security Officer, or the Cognizant Security Office or Designated Government Representative. The second copy of the receipt shall be forwarded by the receiving company Security Officer or the Cognizant Security Office or Designated Government Representative, as applicable, to the NSA/DSA who is responsible for ensuring that the classified documents are properly protected while they are under that Government's cognizance.

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

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

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

1.12.3 Name and position/title of the individual that signed the receipt.

1.12.4 Stamp, official seal, or other designation of the recipient's organization.

1.12.5 Signature of the recipient.

1.13. The dispatching company Security Officer shall notify the receiving company Security Officer, or the Cognizant Security Office or 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 the Cognizant Security Office or Designated Government Representative, shall consult the dispatching Security Officer to determine the circumstances of the late arrival. The dispatching company Security Officer shall notify his/her Cognizant Security Office or Designated Government Representative, unless officially notified of a change to the courier's itinerary.

1.14. Throughout the journey, the classified documents shall remain in the personal possession of the courier. In particular, they must not be left unattended at any time during the journey, either in the means of 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. In addition, envelopes/packages containing the classified documents shall not be opened en route, unless required by the Customs Service or other public officials as described under paragraph 1.15., below.

1.15. he courier shall comply with official requests to open classified consignments by the Customs or other public officials. When inspection is unavoidable, care shall 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.

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

1.17. Under no circumstances shall the classified

consignment be handed over to Customs or other public officials for their custody.

1.18. When carrying classified documents, the courier shall not travel:

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

1.18.2. On carriers of or by air routes over countries that may present a threat, as mutually agreed to by the NSAs/DSAs. Further advice on this matter may be requested from the NSA/DSA, Cognizant Security Office or Designated Government Representative, if necessary.

1.19. In cases where documents classified RESTRICTED (see Enclosure B) are being carried, national security regulations will apply.

2. HAND CARRIAGE OF CLASSIFIED EQUIPMENT AND/OR COMPONENTS

2.1. The procedures described in Section 1. of this document shall be complied with, supplemented by the following requirements that govern the urgent hand carriage by couriers of equipment and/or components classified SECRET or below relative to programmes, projects, or contracts. The consignment shall be of such size, weight, and configuration that it can be retained at all times in the personal possession of the courier.

2.1.1. The "Courier Certificate" shall be used only to verify the bona fides of the courier and to avoid direct inspections of the hand-carried items or, if an inspection is unavoidable, to have it done under secure conditions. It shall 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.

2.1.2. The dispatching company Security Officer, in collaboration with the company export officer, shall:

2.1.2.1. Obtain approval for the urgent transfer of the classified consignment from the national programme or project director or contracting officer and responsible NSA/DSA, Cognizant Security Office or Designated Government

Representative, as required by national regulations;

2.1.2.2. Visually verify, in the presence of the Cognizant Security Office or Designated Government Representative, the contents of the consignment against a receipt and/or shipping documentation;

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

2.1.2.4. 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;

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

2.1.2.6. Arrange, in coordination with the Cognizant Security Office, NSA/DSA, or CS, as applicable, 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.

2.1.3. The dispatching company's Security Officer shall also provide to the courier all the instructions necessary to fulfill 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 shall contain appropriate addresses and telephone numbers of company and government officials in the countries to be transited and entered, who may be contacted for assistance. They may be the addresses and telephone numbers of:

- Diplomatic or consular authorities or Defense Attaches of the courier’s country;

- Police or other governmental authorities of the

countries where the courier stop or transit;

- Security Officer of the receiving company;
- NSAs/DSAs and Cognizant Security Offices of the other countries.

2.1.4. In the event of difficulties, the courier shall reveal 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 content of 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 shall the courier relinquish possession of the consignment until it is delivered in accordance with the security instructions.

2.1.5. The Security Officer of the receiving company shall inform the company's Cognizant Security Office or NSA/DSA of the anticipated arrival of the classified consignment, and assist as necessary with entry, customs, security, and/or other administrative requirements.

Enclosures

A - List of Responsible Government and Company Participants
B - Table of Equivalent Security Classifications
C - Courier Declaration
D - Courier Certificate and Annexes

ENCLOSURE A

LIST OF RESPONSIBLE GOVERNMENT AND COMPANY PERSONNEL TO CONTACT FOR ASSISTANCE

[Option: List the name, address, telephone and telefax numbers and e-mail address of points of contact at government and company offices that might provide assistance. These include the NSAs/DSAs or CSOs, the points of contact for companies that might provide assistance, and diplomatic and military personnel. For companies that may be contacted for assistance, in addition to the foregoing, indicate the level of facility security clearance and level of safeguarding capability.

ENCLOSURE B

TABLE OF EQUIVALENT SECURITY CLASSIFICATIONS

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
BELGIUM (French)	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTE
(Flemish)	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERKTE VERSPREI-DING
CANADA	TOP SECRET	SECRET	CONFIDENTIAL	NO EQUIVALENT
DENMARK	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTE-BRUG
FRANCE	(1)	SECRET DEFENCE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
GERMANY	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	VS-NUR FUR DENIENSTGE-BRAUCH
GREECE	ΑΚΡΩΕ ΑΠΟΡΡΗΤΟΝ	ΑΠΟΡΡΗΤΟΝ	ΕΜΠΙΣΤΕΥΤΙΚΟΝ	ΠΕΡΙΩΡΙΣ-ΜΕΝΗΣ ΧΡΗΣΕΩΣ
ITALY	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	
LUXEMBOURG	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTE
NETHERLANDS	Stg ZEER GEHEIM	Stg GEHEIM	Stg CONFIDENTIEEL	NO EQUIVALENT
NORWAY	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
PORTUGAL	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
SPAIN	SECRETO	RESERVADO	CONFIDENCIAL	
TURKEY	COK GIZLI	GIZLI	OZEL	HIZMETE OZEL
UNITED KINGDOM	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
UNITED STATES	TOP SECRET	SECRET	CONFIDENTIAL	NO EQUIVALENT

(1) ONLY FOR GOVERNMENT PRIORITIES

ENCLOSURE C

Disclaimer: This document is provided to students of the IPSR Course as a sample document of a program security instruction for educational purposes only.

[Insert office name heading and address of NSA/DSA]

C O U R I E R D E C L A R A T I O N

[Option: insert identifying information on the courier as follows

(Name, Forename)
(Name of Company)
(Position in Company)]

The Security Officer of the **{Option: insert the name of company/organization that is to dispatch the courier]** provided to me the "Notes" concerning the handling and custody of classified documents/equipment to be carried by me. I have read, I understand, and I shall comply with their contents.

I shall always retain enroute the classified documents/equipment that have been entrusted to my custody and shall not open the package unless required by the Customs, Police, or Immigration Authorities.

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

(Place and date) **(Typed name and signature of courier)**

Witnessed by: (Typed name and signature of company Security Officer, and date)

ENCLOSURE D

(Insert office heading name and address of NSA/DSA)

COURIER CERTIFICATE NO._____
FOR THE INTERNATIONAL HAND CARRIAGE
OF CLASSIFIED DOCUMENTS, EQUIPMENT, AND/OR COMPONENTS
[Option: insert program name]

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

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

- The material comprising this consignment is classified in the interests of national security of: **(insert the country or countries having that are involved. At least the country of origin of the shipment and that of the destination should be indicated. The country/ies to be crossed also may be indicated, if they are Participants.)**

- It is requested that the consignment not be inspected by other than properly authorized officials or those to whom special permission is granted by the governments cited above.

- 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 by the officials who request the inspection, after re-closing, to show evidence of the opening. This should be accomplished by sealing and signing the package and by annotating the shipping documents (if any) that the consignment has been opened.

- Customs, Police, and/or Immigration officials of countries to be transmitted, entered, or exited are requested to give assistance, if necessary, to assure the successful and secure delivery of the consignment.

(Insert the name, title, organization, and telephone number of the issuing authority, and signature.)

Annex (2)
1. Itinerary
2. Notes to Courier

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

(Office heading name and address of NSA/DSA)

ANNEX 1 TO COURIER CERTIFICATE NO._____

ITINERARY

From: **(insert originating country)**

To: **(insert destination country**)

Through: **(list intervening countries)**

Authorized stops: **(list locations with addresses and points of contact)**

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

(Name and Signature of Company Security Officer) **(Name and Signature of NSA/DSA or CSO or designated representative)**

_____ _____

(Company's stamp) **(Designated Security Authority's stamp, if applicable)**

TRIP COMPLETION CERTIFICATION

(N O T E: 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: (insert date of return)

Disclaimer: This document is provided to students of the IPSR Course as a sample document of a program security instruction for educational purposes only.

[Insert office heading name and address of NSA/DSA]

ANNEX 2 TO COURIER CERTIFICATE No._____

NOTES FOR THE COURIER

You have been appointed to carry/escort a classified consignment. Your "COURIER CERTIFICATE" has been provided. Before starting the journey, you will be briefed on the security regulations governing the hand carriage of the classified consignments and on your security obligations during the specific journey (behavior, itinerary, schedule, etc). You will also be requested to sign a declaration that you have read and understand and will comply with prescribed security obligations.

The following general points are brought to your attention:

1. You will be held liable and responsible for the consignment described in the Courier Certificate.

2. Throughout the journey, the classified consignment must stay in your personal possession, unless you are accompanying a classified consignment under an NSA/DSA-approved transportation plan, when the consignment may be stored.

3. The consignment will not be opened enroute except in the circumstances described in paragraph 10, below.

4. The classified consignment is not to be discussed or disclosed in any public place.

5. The classified consignment is not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance may be utilized. You are to be instructed on this matter and be provided locations by your company Security Officer.

6. While hand carrying or accompanying a classified consignment, you are forbidden to deviate from the travel schedule provided.

7. In cases of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal possession except under circumstances described in paragraph 2, above. To this end, your instructions include details on how to contact the security authorities of the countries you will transit as listed in paragraph 12, below. If you have not received these details, ask for them from your company Security Officer.

8. You and the company Security Officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency, and medical documents, etc.) are complete, valid, and current.

9. If unforeseen circumstances make it necessary to transfer the consignment to other than the designated representatives of the company or government you are to visit, you will give it only to authorized employees of one of the points of contact listed in paragraph 12.

10. There is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing. Therefore, should such officials inquire into the contents of the consignment, show them your "Courier Certificate" and this Note and insist on showing the contents only to the actual senior Customs, Police and/or Immigration Official; this action should normally suffice to pass the consignment through unopened. However, if the senior Customs, Police, and/or Immigration Official demands to see the actual contents of the consignment you may open it in his presence, but this should be done in an area out of sight of the general public.

a. You should take precautions to show officials only as much of the contents as will satisfy them that the consignment does not contain any other item except that which has been declared, and ask the official to repack or assist in repacking it immediately upon completion of the examination.

b. You should request the senior Customs, Police, and/or Immigration Official to provide evidence of the opening and inspection of the consignment by sealing and signing it when it is closed, and confirming in the shipping documents (if any)

that the consignment has been opened by them.

c. If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving company Security Officer and the dispatching company Security Officer as soon as possible, and they should be requested to inform the NSAs/DSAs of their governments.

11. Upon your return, you must produce a bona fide receipt for the consignment, signed by the Security Officer of the company or agency receiving the consignment or by a NSA/DSA, CSO or CSO designee of the receiving government.

12. Along the route you may contact the following officials to request assistance: **[Option: provide the names, organization, address, telephone and telefax numbers and e-mail address of government and contractor officials with whom arrangements have been made for providing assistance.]**

.....

.....

.....

.....

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

ANNEX C

PROCEDURES FOR THE USE OF SECURE VOICE, FACIMILE, AND DATA COMMUNICATIONS FOR THE (insert the name of the programme or project)

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

ANNEX D

(insert the name of the programme or project)

TRANSPORTATION PLAN No.(insert number)
FOR THE MOVEMENT OF CLASSIFIED MATERIAL
AS FREIGHT

A. INTRODUCTION

This plan delineates procedures for the commercial transfer of classified **[Option: insert name of the Programme/Project or contract]** material as freight between **[Option: insert participating countries].**

[Guidance: If this plan is to be a generic plan that provides the general terms of reference for recurring shipments, with the individual consignments described in detail in separate documentation, that fact should be so stated here. Also see section B, below, and Annex 1, "Notice of Classified Consignment", which is to be used for the shipment of each consignment.]

B. DESCRIPTION OF CONSIGNMENT

[Option: Provide a general description of the material to be transmitted. If necessary, a detailed, descriptive listing of items to be transmitted under this plan, including military nomenclature, may be appended to this plan as an annex when the plan is used for a single shipment, or included in a Notice of Classified Consignment (see annex) for recurring shipments.

C. IDENTIFICATION OF PARTICIPATING GOVERNMENT AND COMPANY REPRESENTATIVES

[Option: This section will identify, by name, title and organization, the company security officials and/or the authorized Designated Government Representatives of each Participant who will arrange the transfer of, sign receipts for, and assume security responsibility for the classified freight. Mailing addresses, telephone numbers, telefax numbers, telex addresses and e-mail addresses are to be listed for each country's representatives. This information also may be included as an attachment or in the "Notice of Classified Consignment" when

there are to be recurring shipments.]

D. DELIVERY POINTS, TRANSFER POINTS, AND/OR PROCESSING POINTS

[Option: Provide the information described below; for recurring shipments the specific details may appear in the "Notice of Classified Consignment":

1. Identity of the points of origin and ultimate destination and any locations other than the destination where the transfer of custody will occur, (e.g. ports, railheads, airports etc.) and describe how secure transfer between carriers is to be arranged.

2. Describe the security arrangements that are required while the material is located at the points described above.

3. Specify any additional security arrangements that may be required due to the unique nature of the transmission or of a delivery, transfer, or processing point (e.g., an airport freight terminal or port receiving station)].

E. IDENTIFICATION OF COMMERCIAL ENTITIES TO BE INVOLVED IN EACH MOVEMENT

[Option: if they are known in advance (i.e., for a single shipment), identify fully all commercial entities, such as commercial carriers, freight forwarders, and transportation agents that might be involved, to include names, addresses, telephone and telefax numbers, e-mail addresses, the level of facility security clearance and storage capability of each, and the functions that they will perform. If the information will vary for recurring shipments, the details will be placed in the "Notice of Classified Consignment".]

F. ROUTING OF CONSIGNMENT

[Option: If this plan is for a single shipment, specify in this section the routes to be used under the plan. The description must cover all routes from point of origin to the ultimate destination in the recipient country. This shall include each segment of the route from the point of origin to the ultimate destination including all border crossings and actions required at border crossings. Routes should be detailed for each Participant in a logical sequence from point-to-point.

If overnight stops are required, security arrangements for each stopping point must be specified. Contingency stop-over locations must also be identified as necessary. If there are going to be recurring shipments, use the "Notice of Consignment" Annex to describe the details, instead of this section.]

G. PORT SECURITY AND CUSTOMS OFFICIALS

[Option: In this section, describe procedures, as applicable, for notifying the Customs and port security officials of each consignment. The facility must verify that the courier has been provided the necessary documentation and is aware of the rules necessary to comply with Customs and security requirements. Prior coordination with Customs and port security agencies (including carrier security officials, if applicable) may be required to facilitate Programme/Project transfers. Include in this section or in an Annex the procedures for handling Customs searches and points of contact who will assist Customs in processing consignments from and into each participating country, along with the names and telephone numbers of Customs and security officials with whom any arrangements have been made.

H. COURIERS

[Option: This section will describe the procedures for the use of couriers. When couriers are to be used, they must each be identified by name and title, Participant organization, and passport number, and/or other secondary identification. Couriers must be cleared at the appropriate level and be briefed on their security responsibilities. Briefings should be tailored to the mode of transmission (e.g. commercial air, ships, truck, rail etc.). Each courier will be issued a "Courier Certificate" and will be provided a list of possible secure storage locations and points of contact and emergency phone numbers. The Courier Certificate and security responsibility briefings from MISWG Document No. 1, "Arrangements for the International Hand Carriage of Classified Documents, Equipment and/or Components", should be used and included as an enclosure to this plan. For recurring shipments, the identity of couriers will appear in the "Notice of Classified Consignment".]

I. RECIPIENT RESPONSIBILITIES

[Option: Describe the responsibilities of each recipient

to inventory the material and to examine all documentation upon receipt of the consignment including:

1. The recipient organization must notify its NSA/DSA and the dispatching organization of any deviation in prescribed routes or methods.

2. The recipient organization must notify its NSA/DSA and the releasing organization of any discrepancies in the documentation or shortages in the consignment.

3. Clearly state the requirement for recipients to promptly advise the NSA/DSA of the dispatching organization and/or Designated Government Representative of any known or suspected compromise of classified material or any other exigencies that may place the movement in jeopardy.]

J. PROCEDURAL DETAILS

[Option: This section shall contain the all of the following items, unless they are to appear in a "Notice of Classified Consignment for recurring shipments:

1. Identification of dispatch assembly points where the consignment will be validated against the export authorization.

2. Packaging requirements that conform to the national security rules of the Participants. The requirements for dispatch documents, inventories, seals, receipts, storage, and security containers should be explained. Any unique requirement of the Participants should also be stated.

3. Documentation required for the dispatch points.

4. Courier authorization documentation and travel arrangements.

5. Procedures for verifying, sealing, loading, and locking the consignments. Describe procedures at the loading points, to include tally records, surveillance responsibilities, and witnessing of the counting and loading arrangements.

6. Procedures for accessibility by the courier to the consignment enroute (e.g., overnight stops, diversions, etc.).

7. Procedures for unloading at the destination, to include identification of recipients and procedures for change of custody, and receipt arrangements. If there are to be shipments to various locations and/or the arrangements are to be different for each shipment, this section may be very brief and the "Notice of Classified Consignment" would be used for the details.

8. Emergency communication procedures. List appropriate telephone numbers and points of contact for notification in the event of emergency. For recurring shipments, this information will be placed in the "Notice of Classified Consignment".

9. Procedures for identifying each consignment (e.g., date, time, flight number, etc.) and for providing details of each consignment. For recurring shipments, the "Notice of Classified Consignment," should be used instead of providing details in this paragraph. The notification should be transmitted no less than 6 working days before the transmission of the classified consignment.

K. RETURN OF CLASSIFIED MATERIAL

[Option: This section will identify requirements for the return of classified or sensitive material to the manufacturer or dispatching country (e.g. for warranty, repair, test, and evaluation etc.). The information must be specific with regard to methods, routes, carriers, etc., and therefore, may be placed in an annex to the plan. When there are to be recurring shipments, the details for each shipment will be in a "Notice of Classified Consignment".]

(GUIDANCE: Samples of the forms listed below should be included, as appropriate, as enclosures to the plan, so they are easily recognized by persons who are participating in the transfer.

(1) Packing list
(2) Classified material receipts
(3) Bills of lading
(4) Export declaration
(5) Waybills
(6) Other nationally required forms that will used.)

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

NOTICE OF CLASSIFIED CONSIGNMENT ANNEX
TO
APPROVED TRANSPORTATION PLAN No.(insert Plan number)
FOR
(insert the name of the programme or project)

ACKNOWLEDGE BEFORE: (insert date and time by which the consignee must acknowledge acceptance)

1. Responsible Security Officers: **(insert identifying information on the consignor/consignee Security Officers: include the name, telephone number, e-mail address, and postal address of the Security Officer(s) who are to be responsible for the consignment at both locations).**

2. Designated Government Representatives: **(insert identifying information on the Designated Government Representatives: include the name, telephone number, e-mail address and postal address of the releasing and receiving authorized designated government representatives, as applicable).**

3. Description of Consignment: **(provide the following information for each shipment)**

3.1. Contract, Proposal or Tender Number: **(provide the contract, request for proposal or invitation to tender number under which the consignment is being delivered)**

3.2. Export Authorization: **(list the license or other applicable export authorization citation, e.g., a licensing exemption)**

3.3. Consignment Description: **(describe the items to be shipped and their classification)**

3.4. Package Description: **(provide the following details to describe the consignment)**

Type of package: (wood, cardboard, metal, etc.)
Number of packages:
Number of enclosed classified items in each package:
Package dimensions/weight: (include length,

width, height, and weight)

3.5. Indicate whether package contains any hazardous material.

4. Routing of Consignment: **(provide the following information for each shipment)**

4.1. Date/time of Departure:

4.2. Date/Estimated Time of Arrival:

4.3. Routes: (describe the routes to be used between the point of origin of the shipment, the point of export from the country of origin, the point of import into the recipient country and the ultimate destination point (identify specific transfer points; use codes that appear in transportation plan, if applicable)

4.4. Method of Transport: (for each portion of the shipment, include names, telephone numbers, e-mail addresses, and postal addresses of all carriers, and the flight, rail, or ship number as applicable)

4.5. Freight Forwarders/Transportation Agents: (include the name, telephone number, e-mail address, and postal address of the companies to be used, if they are if not specified in the transportation plan. **(Note: The releasing Security Officer must re-verify the clearance and safeguarding capability of these entities before releasing each consignment)**

4.6. Customs or Port Security Contacts: (list names, e-mail addresses, and telephone numbers if they are not listed in the approved transportation plan)

5. Name(s) and Identification of Courier/Escort: **(if couriers are to be used, provide their full names, passport numbers and secondary identification, courier orders number and issuing authority, and the name and telephone number and e-mail address of an official that Customs or security authorities may contact, if further identification is necessary)**

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

ANNEX E

[insert the name of the programme or project]

MARKING PROGRAM INFORMATION

[Option: This annex is to describe how the Participants and Participating Contractors will mark Background, Foreground, and other Program Information.]

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

ANNEX F

[insert the name of the programme or project]

SECURITY CLASSIFICATION GUIDE

[Option: this annex is to describe how elements of Program Information that require security protection in the interest of national security of the Participants are to be classified, declassified, and downgraded or re-graded.]

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

ANNEX G

CONTRACT SECURITY CLAUSES

(insert the name of the programme or project)

(The following contract security clauses should be placed in all Program prime contracts and subcontracts. The clauses may not apply, in some respects, to contracts involving RESTRICTED information. For such contracts, the contracting authority will consult with their National Security Authority (NSA) or Designated Security Authority (DSA) to determine which clauses are appropriate. Certain clauses may have to be inserted or deleted to accommodate the laws and regulations of all participating nations. "Contracting Authority," is the government entity that awards the contract

1. CLASSIFIED information provided or generated pursuant to this contract shall be protected as follows:

a. The recipient shall not disclose the classified information to a third party government, person, or firm, or representative thereof, without the prior written consent of the releasing government. Such consent shall be sought through the recipient's National Security Authority/Designated Security Authority (NSA/DSA). The responsible NSAs/DSAs for this contract are: **[Option: insert names, postal addresses, e-mail addresses and telephone numbers of the responsible NSAs/DSAs].**

b. The recipient shall provide the CLASSIFIED information a degree of protection no less stringent than that provided by the releasing government in accordance with National Security regulations and as prescribed by its NSA/DSA;

c. The recipient shall not use the classified information for any purpose other than for which it was provided or generated, without the prior written consent of the releasing government. **(Option: insert the channels that must be followed to obtain such consent.)**

2. CLASSIFIED information provided or generated pursuant to this contract shall be transferred internationally only through government channels or as specified in writing by the Governments concerned.

3. CLASSIFIED information shall only be disclosed to individuals who have an official need-to-know for the performance of the contract and who have a Government granted Personnel Security Clearance at least equal to the classification of the information involved.

4. CLASSIFIED information provided pursuant to this contract shall be marked by the recipient with its government's equivalent security classification.

5. CLASSIFIED information generated pursuant to this contract shall be assigned a security classification in accordance with the security classification specifications provided with this contract, as attached at ANNEX ____). **(Note: the security classification specifications shall be provided in the form of a security classification checklist (for NATO programs), security classification guide or the Programme Security Instruction, as agreed by the Participants).**

6. All cases in which it is known, or there is reason to suspect, that CLASSIFIED information provided or generated pursuant to this contract has been lost or disclosed to unauthorized persons, shall be reported promptly and fully. The content of the report shall be in accordance with national regulations, unless specified otherwise in the relevant contract or agreement between the responsible governments.

7. **[Option: insert the procedures that are agreed upon by the Participants on the disposition of classified information that is no longer required for participation in the program, i.e., whether it shall be destroyed or returned to the originator and the procedures to be followed. Refer to section 7 of the draft PSI.]**

8. CLASSIFIED information provided or generated pursuant to this contract shall not be further provided to another potential contractor or subcontractor unless:

a. A written assurance is obtained from the recipient's NSA/DSA to the effect that the potential contractor or subcontractor has been approved for access to classified information at the requisite classification level by its NSA/DSA; and

b. Written consent is obtained from the contracting authority for the prime contract if the potential subcontractor is located in a third country.

9. All classified information and material provided or generated under this contract shall continue to be protected in the event of withdrawal by the recipient party or upon termination of the contract, in accordance with national regulations, provided such regulations are consistent with the terms of any security agreement or relevant program agreement between the governments of the Participants.

10. The recipient shall insert terms that substantially conform to the language of these clauses, including this clause, in all subcontracts under this contract that involve access to CLASSIFIED information provided or generated under this contract.

ANNEX H

INTERNATIONAL VISIT PROCEDURES
FOR THE
[Insert the name of the programme or project]

These procedures shall be used for visits by both the Participants' and Participating Contractors' personnel who are involved in the [**Option: insert the name of the program]** Program. The following subjects are covered in this Annex.

SECTION I

STANDARD PROCEDURES FOR ONE TIME AND RECURRING VISITS

1. Types of Visits. There are three types of international visits; they are defined below:

a. One-time Visit. A single visit (normally less than 30 days) for a specified purpose. A one time visit may also be for a longer period of time (i.e., an Extended Visit), normally for up to one year, as described below.

b. Extended Visit. A single visit for an extended period of time, normally for the duration of a programme, project or contract, subject to annual review and validation. An Extended Visit is normally used for the assignment of liaison officers and exchange personnel.

b. Recurring Visit. Visits over a specified period of time not covered by the above, normally for up to one year or for the duration of a government approved programme, project, or contract, including a government approved license, that require participating personnel to make intermittent (recurring) visits to government agencies or industrial facilities of the other country or countries that are involved in the programme, project, or contract. Visits covering a period of more than one year will be subject to annual review, unless otherwise arranged by the participating countries' NSA/DSA.

2. Use of the standard Request for Visit Authorization (RVA) Format.

a. The standard RVA format (Enclosure 1 to this Annex) should be used.

b. This RVA format has been designed for automated as well as manual use. It is therefore essential that the "Detailed Instructions for Completion of the RFV" be used to fill in each data element. To fulfill this requirement it is advised that Enclosure 1, as a whole, be provided to potential visitors through the security officer of their agency or facility. Furthermore, it is advisable to translate the General and Detailed Instructions for the use and completion of the RVA (Enclosure 1) into the language of the user.

3. Lead-time.

a. The following table gives the number of working days prior to the beginning date of the One-time Visit or Extended Visit, or the date of the first Recurring Visit, that the request should be in the possession of the *receiving* NSA/DSA. **[Option: select the countries that are Participants in the Program.]**

Belgium	BE	14
Canada	CA	20
Czech Rep	CZ	..
Denmark	DA	07
France	FR	25
Germany	GE	20
Greece	GR	20
Hungary	HU	..
Italy	IT	20 (working days)
Luxembourg	LU	14
Netherlands	NL	10
Norway	NO	20
Poland	PL	..
Portugal	PO	15
Spain	SP	20
Turkey	TU	25
United Kingdom	UK	15
United States of America	US	21

b. The lead-times stated above should not be confused with the "Submitting Terms" discussed in the "General Instructions," paragraph 1.4. of Enclosure 1. That table in that paragraph gives the requesting visitor, agency, or facility an indication of the number of working days prior to the visit(s) that the request should be in the possession of the *requesting* NSA/DSA.

In the case of recurring visits that have already been approved by the NSA/DSAs under the Recurring Visit Authorization, advance notification to the host site is required before each actual visit.

4. Amendments.

a. Amendments to approved or pending One-time, Extended, and Recurring Visits are authorized, provided that the amendments are limited to:

(1) Dates of visit, provided the amended date is a later date, or
(2) Addition or deletion of names.

b. The deletion of names will be reported immediately to the requesting NSA/DSA, who will notify the receiving NSA/DSA. Other amendments will be accepted by the receiving NSA/DSA up to the number of working days prior to the approved or pending visit as follows:

BE:	09	GR:	10	PL:	..
CA:	10	HU:	..	PO:	07
CZ:	..	IT:	07	SP:	08
DA:	05	LU:	09	TU:	10
FR:	05	NL:	05	UK:	05
GE:	10	NO:	10	US:	05

There is no format for this action; however, such amendments shall refer to the original requests, by visit request number, that have already been approved by the NSAs/DSAs.

SECTION II

EMERGENCY VISIT PROCEDURES

1. Background. Unforeseen situations may occur that do not permit the use of standard visit request procedures. Such unforeseen situations may necessitate an Emergency Visit. However, a request for an Emergency Visit should be used only in exceptional circumstances. If visits are properly planned at the beginning of bilateral and multinational government programmes or government approved contracts, and authorizations

for Recurring Visits are obtained, the Recurring Visit authorization should satisfy the majority of requirements for visits related to the programmes and contracts. To qualify as an "Emergency Visit" the following criteria must be met:

a. The proposed visit is related to an official government request for proposal or request for tender offer (e.g. submission of or amendment to a bid or proposal; attendance at pre-contract negotiations or bidder's conference), or

b. The visit is to be made in response to the invitation of a Participant government official or Participating Contractor official and is in connection with an official government project, programme, or contract, and

c. A programme, project, or contract opportunity will be placed in jeopardy if the visit request is not approved.

2. Procedures

a. Emergency Visit requests will be critically reviewed, fully justified and documented by the Security Officer of the requesting government agency or industrial facility. When the Security Officer is satisfied that the circumstances warrant an Emergency Visit, the Security Officer will contact a knowledgeable person at the government agency or industrial facility to be visited, directly by telephone, e-mail, or facsimile, to obtain tentative verbal agreement for the proposed visit. This normally should be accomplished no later than *three* working days in advance. If tentative, verbal agreement is provided to proceed with a visit request, the government agency or industrial facility to be visited (host facility) shall then immediately notify its NSA/DSA that an emergency visit request will be submitted by the government agency or industrial facility that wants to make the visit (requesting facility) and explain the reason for the emergency.

b. Following receipt of tentative verbal agreement from the host facility, the Security officer of the requesting facility will then send a message in the Request for Visit format (as in Annex 1 of this document) as follows:

(1) The message must be sent by priority precedence within 24 hours of the verbal agreement for the requested emergency visit to the NSA/DSA of the country to be visited,

through the NSA/DSA of the originating country and the Security Officer of the facility to be visited. Any of those officials may deny the visit.

(2) The subject of the message will be: "EMERGENCY VISIT - (name of programme, project, or contract or request for proposal or tender offer)". The message must contain all of the information included in the RFV format. The name, telephone, and facsimile numbers of the person contacted pursuant to paragraph 2.a., above, will be placed in the *Remarks* section of the RFV.

(3) If the NSA/DSA of the host country approves the request, it will subsequently notify the Security Officer of the facility to be visited and the NSA/DSA of the requesting country of the approval. The host facility Security Officer will then notify the requesting facility Security Officer that the visit is approved or denied.

c. Emergency visit procedures shall not be used in lieu of standard visit request procedures. Therefore, each MISWG country will establish guidelines to ensure compliance with these procedures. When it becomes apparent that the procedures are being abused by personnel of another country, the NSA/DSA of that country will be notified and should take corrective action.

Enclosure 1 to Annex H

STANDARD REQUEST FOR VISIT AUTHORIZATION FORMAT

The Participants and Participating Contractors shall use the attached instructions for the use and completion of a Request for Visit Authorization (RVA) when a visit authorization is required. The format standardizes the elements required for a RVA and places them in a logical order. The RVA format will be used for manual as well as automated processing.

It is advisable to use this enclosure as a "hand-out" to the visitor. The general principle of this RVA is that only one format will be used when a visit request is necessary.

When a visit involves access to information subject to government approval, or when access to controlled areas is necessary, the visit request will be submitted by the visitor through their organization's security officer, the certifying/requesting NSA/DSA, and receiving NSA/DSA to the agency or facility to be visited.

The following appendices are contained in this Enclosure:

Appendix A: Instructions for the use and completion of a Request for Visit.

Appendix B: Sample RVA format and annexes thereto.

Appendix C: Number of characters for each data element of the RVA format.

Appendix A to Enclosure 1

INSTRUCTIONS FOR THE USE AND COMPLETION OF A REQUEST FOR VISIT AUTHORIZATION

1. GENERAL INSTRUCTIONS

1.1. The Request for Visit Authorization (RVA) is an important document and must be completed without misstatement or omission. Failure to provide all requested information will delay the processing of the request.

1.2. The RVA should be used for a One-time, Extended, and/or Recurring Visit.

1.3. This RVA should be typed or hand-written in block letters. Automated processing of the RVA is encouraged, provided that the original form and content are maintained.

1.4. Submitting Terms and Country Codes

The RFV should be in the possession of the *requesting* NSA/DSA the specified number of working days prior to the visit as follows: **[Option: select the countries that will be Participants. The number of days required will be agreed upon during the preparation of the PSI.]**

Country Visited	*Country code*	*Working days **
Belgium	BE	..
Canada	CA	..
Czech Rep.	CZ	..
Denmark	DA	..
France	FR	..
Germany	GE	..
Greece	GR	..
Hungary	HU	..
Italy	IT	..
Luxembourg	LU	..
Netherlands	NL	..
Norway	NO	..
Poland	PL	..
Portugal	PO	..
Spain	SP	..
Turkey	TU	..

United Kingdom	UK	..
United States of America	US	..

1.5 The completed RVA shall be sent by the Participants' and Participating Contractors' potential visitors to their national agency at the address specified below. That agency will process the request. **(Insert the office of each Participant that will verify clearances, provide security assurances, and process RVAs for visits to the countries of the other Participants. The name of a point of contact, postal address, telephone number, telex address, telefax number, and e-mail address will be provided.]**

INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT AUTHORIZATION (RVA)

These instructions provide guidance for completion of the RVA for One-time and Extended Visits. The request is to be prepared by the agency or facility security officer in the case of Recurring Visits in the framework of government approved programmes or projects. Since this RVA format is designed for manual as well as for automated use, a corresponding distinction is made in the completion of some items. When this distinction is applicable, reference is made in the text of the item under "Remark(s)".

HEADING: The Heading is "Request for Visit Authorization". Under the heading, mark the appropriate box in left (type of visit) and right (annexes) columns.

1. **ADMINISTRATIVE DATA**: Do not fill in (to be completed by the Embassy of the requesting Participant).

2. **REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY:** Provide the full name and postal address; include city, state, and postal zone (zip code), as applicable.

3. **GOVERNMENT AGENCY OR INDUSTRY FACILITY TO BE VISITED:** Provide the full name and precise address; include the street address, city, state, and postal zone and the telex address and the telefax and telephone number. Include the name and telephone number of the host person or other point of contact who has knowledge of any arrangements that were made for the visit.

(GUIDANCE:

(a) Providing the correct postal zone (zip-code) and precise street address is very important, because there can be different facilities of the same company.

(b) In case of an automated application, only 1 agency or facility can be stated.

(c) In case of a manual application, an annex can be used when two or more agencies or facilities are to be visited in the framework of the same subject. When an annex is used, item 3 should include the statement: "SEE ANNEX 1 FOR (insert number of agencies/facilities) ADDITIONAL FACILITIES". The format is at Annex to the RVA.)

4. **DATES OF VISIT:** Provide the actual date or period of the visit (date-to-date). Provide the actual date or period as day-month-year." If applicable, request an alternate date or period in brackets.

5. **TYPE OF VISIT:** Mark one item of each column as indicated. Government Initiative will be specified only if the visit is in support of an authorized government initiative (e.g., Foreign Military Sales (FMS - i.e., government sale), government-to-government agreement), which must be fully described in item 8.

6. **SUBJECT TO BE DISCUSSED/JUSTIFICATION:** Give a brief description of the subject(s) that are to be discussed during the visit. Explain all abbreviations.

(GUIDANCE:

(a) In the case of a recurring visit, this item should state "Recurring Visits" as the first words in the data element (e.g., Recurring Visits to discuss....)

(b) This item should be prepared in the language of the receiving country, unless agreed otherwise.)

7. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE DISCUSSED:** Indicate SECRET, CONFIDENTIAL, RESTRICTED or UNCLASSIFIED, as applicable. Indicate whether such information is to be disclosed by the visitors or it is expected that the host facility will disclose the information, and indicate the government that originated the information.

8. **IS THE VISIT PERTINENT TO**: Mark the appropriate line, Yes (Y)

or No (N); and if the "Yes" is marked, specify the full name of the government project/programme, i.e., FMS case, or Request for Proposal or Invitation to Tender. Explain all abbreviations.

9. **PARTICULARS OF VISITOR**

NAME: Include the family name, followed by the first forename in full, and middle initial(s)
DOB: Date of birth (day-month-year)
POB: Place of birth (city-state-country)
SC: Actual security clearance status; e.g., TS, S, C. Indicate NATO clearance (e.g., NS) *only* if the visit is related to NATO business
ID-PP: Enter the number of the person's identification card or passport, as required by host government.
NATIONALITY: Enter nationality and/or citizenship in 2-letter-code in accordance with the General Instructions paragraph 1.4.
POSITION: Provide the position the visitor holds in the organization (e.g., director, product manager, etc.)
COMPANY/AGENCY: Provide the name of the government agency or industry facility that the visitor represents (if different from item 2).

(GUIDANCE: When more than two visitors are involved in the visit, an annex may used. The format at Annex 2 should be used. In such case, item no. 9 should state, "SEE ANNEX 2 FOR (state the number of visitors) ADDITIONAL VISITORS".)

10. **SECURITY OFFICER OF THE REQUESTING AGENCY:** Provide the name and telephone number of the requesting agency/facility security officer.

11. **CERTIFICATION OF SECURITY CLEARANCE:** *Do not fill in* (to be completed by requesting government's clearance certifying authority).

(GUIDANCE FOR THE CLEARANCE CERTIFYING AUTHORITY:

(a) Provide the certifying authority's name, address, and telephone number (can be preprinted).

(b) This item should be signed and eventually stamped, if required pursuant to national policy.

(c) If the certifying authority corresponds with the

requesting National Security Authority, enter: "See item 12."

(d) If provided by national policy, items 11 and 12 may be filled in by the appropriate official of the Embassy of the requesting country.)

12. **REQUESTING NATIONAL SECURITY AUTHORITY:** (To be filled in by the applicable NSA.)

(GUIDANCE FOR THE REQUESTING NSA:

(a) Provide name, address, and telephone number (can be preprinted).

(b) This item should be signed and stamped, if required pursuant to national policy.)

13. **REMARKS:**

a. This item can be used for administrative requirements (e.g., proposed itinerary, request for hotel, and/or transportation).

b. This space is also available to the receiving NSA for processing comments; e.g., "no security objections," etc.

c. In case of an Emergency Visit, the name, telephone and telefax numbers, and e-mail address of the knowledgeable person with whom the visit was arranged should be stated.

d. In case a special security briefing is required, the type of briefing and the date that the briefing was given should be stated.

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

Appendix B to Enclosure 1

REQUEST FOR VISIT AUTHORIZATION

[ ] One time
[ ] Recurring
[ ] Emergency

Annex(es)
[ ] Yes:
[ ] No:

ADMINISTRATIVE DATA

1. **REQUESTOR:** **DATE: / /**

TO: **VISIT REQUEST ID Nr.:____**

2. **REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY:**
NAME:

POSTAL ADDRESS:

TELEX/FAX Nr.: **TELEPHONE Nr:.** **e-mail ADDRESS:**

3. **GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED**
NAME:

POSTAL ADDRESS:

TELEX/FAX NR.: **TELEPNONE NR.:** **e-mail ADDRESS:**

POINT OF CONTACT:

4. **DATES OF VISIT: / / TO / / [Alternate: / / TO / /]**

5. **TYPE OF VISIT: (SELECT ONE FROM EACH COLUMN)**

( ) GOVERNMENT INITIATIVE **( ) INITIATED BY REQUESTING AGENCY/FACILITY**

( ) COMMERCIAL INITIATIVE **( ) BY INVITATION OF FACILITY TO BE VISITED**

6. **SUBJECT TO BE DISCUSSED/JUSTIFICATION:**

7. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED:**

8. **IS THE VISIT PERTINENT TO: (Mark "yes" or "No")**

A SPECIFIC EQUIPMENT OR WEAPON SYSTEM	**(Y)**	**(N)**
FOREIGN MILITARY SALES OR EXPORT LICENSE	**(Y)**	**(N)**
A PROGRAMME OR AGREEMENT	**(Y)**	**(N)**
THE DEFENSE ACQUISITION PROCESS	**(Y)**	**(N)**

OTHER (Describe the other program)

9. **PARTICULARS OF VISITORS**

NAME:
DATE OF BIRTH: / /
PLACE OF BIRTH:
SECURITY CLEARANCE:
ID/PP NUMBER:
NATIONALITY:
POSITION:
COMPANY/AGENCY:

NAME:
DATE OF BIRTH: / /
PLACE OF BIRTH:
SECURITY CLEARANCE:
ID/PP NUMBER:
NATIONALITY:
POSITION:
COMPANY/AGENCY:

10. **SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY/INDUSTRY FACILITY:**

NAME:
TELEPHONE NR.:
TELEFAX NR.:
e-mail ADDRESS:

SIGNATURE:

11. **CERTIFICATION OF SECURITY CLEARANCE**

NAME:
ADDRESS:
TELEPHONE NR.:
TELEFAX NR.:
e-mail ADDRESS:

SIGNATURE:

12. **REQUESTING NATIONAL SECURITY AUTHORITY**

Disclaimer: This document is provided to students of the IPSR Course as a sample document of a program security instruction for educational purposes only.

NAME:
ADDRESS:

TELEPHONE:

SIGNATURE:

13. **REMARKS:**

Annex 1 to RVA

GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED
(Continued)

Reference: RVA Nr._____, item 3.

1. **NAME:**
   ADDRESS:

   TELEX/TELEFAX NR.:
   POINT OF CONTACT: **TELEPHONE NR.:**
   e-mail ADDRESS:

2. **NAME:**
   ADDRESS:

   TELEX/TELEFAX NR.:

   POINT OF CONTACT: **TELEPHONE NR.:**
   e-mail ADDRESS:

3. **NAME:**
   ADDRESS:

   TELEX/TELEFAX NR.:

   POINT OF CONTACT: **TELEPHONE NR.:**
   e-mail ADDRESS:

4. **NAME:**
   ADDRESS:

   TELEX/TELEFAX NR.:

   POINT OF CONTACT: **TELEPHONE NR.:**
   e-Mail ADDRESS:

5. **NAME:**
   ADDRESS:

   TELEX/TELEFAX NR.:

   POINT OF CONTACT: **TELEPHONE NR.:**
   e-Mail ADDRESS:

6. **NAME:**
   ADDRESS:

   TELEX/TELEFAX NR.:

   POINT OF CONTACT: **TELEPHONE NR.:**
   e-Mail ADDRESS:

(CONTINUE AS REQUIRED)

Annex 2 to RVA

PARTICULARS OF VISITORS
(Continued)

Reference: RVA Nr._____, item 9.

1. **NAME:**
   DATE OF BIRTH: / /
   PLACE OF BIRTH:
   SECURITY CLEARANCE:
   ID/PP NUMBER:
   NATIONALITY:
   POSITION:
   COMPANY/AGENCY:

2. **NAME:**
   DATE OF BIRTH: / /
   PLACE OF BIRTH:
   SECURITY CLEARANCE:
   ID/PP NUMBER:
   NATIONALITY:
   POSITION:
   COMPANY/AGENCY:

3. **NAME:**
   DATE OF BIRTH: / /
   PLACE OF BIRTH:
   SECURITY CLEARANCE:
   ID/PP NUMBER:
   NATIONALITY:
   POSITION:
   COMPANY/AGENCY:

4. **NAME:**
   DATE OF BIRTH: / /
   PLACE OF BIRTH:
   SECURITY CLEARANCE:
   ID/PP NUMBER:
   NATIONALITY:
   POSITION:
   COMPANY/AGENCY:

5. **NAME:**
   DATE OF BIRTH: / /
   PLACE OF BIRTH:
   SECURITY CLEARANCE:
   ID/PP NUMBER:
   NATIONALITY:
   POSITION:
   COMPANY/AGENCY

Avanco International, Inc.
www.avanco.com
International.Programs@avanco.com

ANNEX I
(insert the name of the programme or project)

CONTROL OF SECURITY-CLEARED FACILITIES

(GUIDANCE:

a. The purpose of this Annex is to provide the Programme Management Office (PMO) Security Office with the procedures for the development and maintenance of the list of Contractors and Sub-Contractors to which classified information and/or material will be distributed.

b. The PMO Security Office will prepare a list (Basic List) of Contractors and Sub-Contractors that have been awarded or are to be awarded contracts within the programme or project (see item c, below). The level of facility security clearance and storage capability of each company will be verified before preparing the list.

c. The List, prepared in the format of Appendix 1, will be based on the information given, respectively, by Prime contractor(s), during the tendering phase and by Prime contractor(s) and sub-contractor(s) during the contract phase.

d. The PMO Security Office will send copies of the "Basic List" to the participating National Security Authorities/Designated Security Authorities (NSAs/DSAs) who, in conjunction with the National Programme/Project Office, as applicable, will check the details of the entries regarding facilities within their security responsibility and return the checked and corrected list to the PMO Security Office.

e. The PMO Security Office will prepare a "Final Consolidated List" and send copies of it to the NSAs/DSAs of the Participants, and to National Project Offices.

f. The PMO Security Office will be notified of any changes to the Final Consolidated List by the participating NSAs/DSAs or National Programme/Project Offices, as applicable (Appendix 2). The PMO Security Office will then prepare an Amendment to the Final Consolidated List and forward copies to the participating NSAs/DSAs and National Programme/Project Offices.

Appendix 1 to Annex I

LIST OF SECURITY CLEARED FACILITIES

(insert the name of the programme or project)

From: PMO Security Officer
To : **(insert addresses of Participants' NSAs/DSAs)**

The following list identifies prime contractors and sub-contractors employed on the **(insert the name of the programme.)**

(GUIDANCE: The serial number is assigned by the PMO for reference purposes. The identification of the facility Security Officer must contain the telephone and telefax numbers and e-mail address.)

Serial Nr.	Full Address of the Facility	Full Address of Security Officer	Class. Level of the Contract	Identity of Contract

The above details are confirmed.

(Signature of PMO Security Officer (Signature of NSA/DSA)

Typed Name Typed Name

Appendix 2 To Annex I

From: Participating NSA/DSA
To : PMO Security Officer
(address)

The following amendment Nr. **(insert the serial number of the request or amendment submitted by the originating NSA/DSA)** should be made to the list of contractors/sub-contractors in **(insert the name of the country that is represented)** employed on **(insert name of the Programme) Programme)**.

(GUIDANCE: The information should be submitted using the basic format that is used for Appendix 1 to Annex I.)

The above details are confirmed

(Signature of NSA/DSA)

Typed Name

ANNEX J

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FIS)
(insert the name of the programme or project)

(GUIDANCE:

The FIS format is to be used for the quick exchange of information between NSAs/DSAs with regard to the verification of a Facility Security Clearance of a facility that is involved or that is to be involved in classified Invitations to Tender, Requests for Proposals, pre-bidders conferences and/or contracts or sub-contracts.

The FIS is divided into a request and a reply section and can be used for different purposes as indicated in the heading of the request section. The preferable way for the exchange of the FIS will be by fax or e-mail, and, in the case of classified information, through approved secure channels.)

PROCEDURES FOR USE OF THE FIS

a. The FIS preferably should be typed or hand-written in capital letters.

b. The following classification abbreviations should be used:

S = Secret
NS = NATO Secret
C = Confidential
NC = NATO Confidential

c. The REQUEST section should be completed as follows:

(1) Select one or more items, depending on the action being requested. The last item (correct and complete information) is a standard selection which requests that any erroneous or incomplete information be corrected.

(2) Items 1 through 5 are self-evident. In item number 4 the standard 2-letter country code should be used. The completion of item number 5 is optional.

(3) Reason for Request (Item 6). Give the specific reason for the request and provide project indicators, the number of the contract, letter of intent, invitation, etc. Any deadline/expiration/award dates that may have a bearing on the completion of a FSC should be included. Provide the name of the actual requestor (if on behalf of the NSA/DSA) and the date of the request.

d. REPLY Section

(1) Item 1: Select appropriate fields. In case a FSC investigation is in progress, it is essential to give the requestor an indication of the required processing time (if known).

Item 2: Select the appropriate fields.

Item 3: Although the validation procedure differs for each country, or even for each facility, the mentioning of the expiration date of the given FSC is mandatory. For obvious reasons, the requesting NSA/DSA should be informed immediately about an earlier invalidation of the provided FSC. It is understandable that, with regard to other changes (e.g. the name of the security officer), this statement is not always attainable. However, if changes come to the knowledge of the providing NSA/DSA, it is assumed that the requesting NSA/DSA will be informed accordingly. The requestor is responsible for the application for a renewal of the FSC.

Item 4: This is a standard clause.

Item 5: The “Remarks” item may be used for additional information with regard to the FSC, the facility, or any of the foregoing items.

(2) Provide the name of the providing authority (the NSA/DSA or other official on behalf of the NSA/DSA) and the date.

e. ADP, COMSEC, AND OTHER SENSITIVE REQUIREMENTS

The security information related to these subjects is generally classified and does not lend itself to the purpose of the FIS. In general, a simple “yes” or “no” answer to the question whether or not the facility holds an ADP and/or a

COMSEC capability is insufficient. When such information is nevertheless required, it is advised to contact the providing NSA/DSA separately on specific items such as compatibility, security policy, key material, etc.

Enclosure-Annex J Format

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FIS)
(insert the name of the programme or project)

TO: (insert name and address of responsible NSA/DSA or CSO)

SUBJECT: REQUEST FOR FACILITY SECURITY CLEARANCE (FSC) ASSURANCE

REQUEST

Please:

[ ] provide a FSC assurance for the facility listed below.

[ ] initiate a FSC up to and including the level of **(insert level of FSC required)** if the facility does not hold a current FSC.

[ ] confirm the FSC up to and including the level of **(insert level of FSC)** as provided on **(insert the date that initial FSC was provided in day, month, year (ddmmyy)).**

[x] provide the correct and complete information, as applicable.

1. Full Facility Name:

2. Full Facility Street Address:

3. Postal Address (if different from item 2)

4. City/Zip Code/Country:

5. Name of the Requesting Security Officer: **(insert name, telephone and telefax numbers, and e-mail address)**

6. This request is made for the following reason(s):
(describe the need for the clearance verification; for example: specified work during the pre-contractual stage or during a specified contract or sub-contract related to the programme or project)

Requesting NSA/DSA: **(insert the name, telephone/telefax numbers and email address)**

Date:

REPLY

1. This is to inform you that the above mentioned facility:

[ ] holds a FSC up to and including the level of: [ ]S [ ]NS [ ]C [ ]NC.

[ ] does not hold a FSC.

[ ] does not hold a FSC, but, pursuant to your above request, the FSC is in progress. You will be informed when the FSC is established. Expected completion date:../..(mmyy).

2. Safeguarding of classified documents: [ ] yes, level:....[ ] no.

Safeguarding of classified material: [ ] yes level:.... [ ] no.

3. This FSC certification expires on: .....(ddmmyy). In the case of an earlier invalidation or in the case of any change to the information listed above, you will be so informed.

4. Should any contract be let or classified information be transferred in relation to this certification, please inform us on all relevant data, including the security classification of the contract.

5. Remarks:

Providing NSA/DSA: **(insert the name, telephone and telefax numbers and e-mail address)**

Date:

ANNEX K

PERSONAL SECURITY CLEARANCE INFORMATION SHEET

(GUIDANCE:

a. When a NSA/DSA requires confirmation of an individual's Personal Security Clearance from another NSA/DSA, in connection with the granting or maintenance of a Facility Security Clearance or for other official purposes, the Personnel Security Clearance Information Sheet will be used to obtain the confirmation.

b. In order to standardize the format for such confirmations, the PSC Information Sheet (PSCIS) provided below has been developed.

c. The information provided in the PSCIS does not constitute an official PSC Certificate and is provided for information purposes only. The recipient NSA/DSA may use such information in accordance with its national rules and regulations. Moreover, this procedure is not intended for use in those circumstances where a formal visit clearance is required; the pertinent information is to be included in the Request for Visit Authorization.)

FORMAT

PERSONAL SECURITY CLEARANCE INFORMATION SHEET
(insert the name of the programme or project)

TO: **(insert the name and address of the NSA/DSA to whom the request is directed.)**

REQUEST

Please confirm the PSC of the person listed below:

1. Full Name:

2. Date/Place of Birth:

3. Nationality:

4. Employed by:

5. This request is made for the following reason(s):
(describe the particulars of the Invitation to Tender, Request for Proposal, pre-bidders conference, contract or sub-contract, or programme for which the clearance is necessary).

Requesting NSA/DSA: **(insert the name, telephone and telefax numbers and e-mail address)**

Date:

REPLY

1. This is to inform you that the above mentioned person, **(insert the persons name as shown on the request)**:

( ) holds a PSC up to and including the level of: ( )S ( )NS ( )C ( )NC

( ) does not hold a PSC.

2. This PSC certification expires:

Yes ( ) Certification of Expiry Date:
No ( ) Not Applicable
3. Remarks:

Providing NSA/DSA: **(insert the name, telephone and telefax numbers and e-mail address)**

Date:

Date and Times Transmitted to the Requesting NSA/DSA:

APPENDIX L
ABBREVIATIONS AND ACRONYMS

AIS	Automated Information System
CSO	Cognizant Security Office
CUI	Controlled Unclassified Information
DGR	Designated Government Representative
DPM	Deputy Program Manager
DSA	Designated Security Authority
FOUO	For Official Use Only
FSC	Facility Security Clearance
ITT	Invitation to Tender
JPO	Joint Program Office
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NSA	National Security Authority
PD	Project Definition
PM	Program Manager
PMSO	Program Managers Support Office
PSI	Program Security Instruction
PSO	Program Security Officer
RFP	Request for Proposal
RVA	Request for Visit Authorization
SAL	Security Aspects Letter

SCG Security Classification Guide