APPENDIX N

PROGRAM/PROJECT SECURITY INSTRUCTION

MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP

MISWG Document Number 5, September 11, 2003

PROGRAM/PROJECT SECURITY INSTRUCTION

INTRODUCTION

The attached sample standard format for a Program/Project Security Instruction (PSI) provides supplementary information to the security section of non-NATO Multinational Cooperative Defense Program/Project Arrangements. The guidance contained in the PSI also supplements the guidance contained in the national security rules of the Participants under which Classified Information and materiel is normally protected. It should be used to reconcile differences in national policies so that standard procedures will be used for the Program/Project. If, in exceptional circumstances, a Program or Project involves the use of both national and NATO procedures, special attention must be given to differences in the procedures, particularly with regard to access control.

The minimum elements of information to be provided for each section are described, and, in some cases, suggested language is provided. These descriptions and suggested language are for guidance only. Additional requirements may apply depending on the size and complexity of the Program/Project, sensitivity of the information involved, any extraordinary security requirements that may be determined by the foregoing factors or differences in the national policies of the Participants, and specific requirements set forth in the applicable Arrangement.

This standard format is not binding on the Participants, but it should be used in the Program/Project Security Instruction whenever possible. When the term "Program/Project" is used herein, the correct word should be selected as it appears in the applicable Arrangement.

PROGRAM SECURITY INSTRUCTION CONCERNING (insert purpose, e.g., COOPERATION IN THE DEVELOPMENT, PRODUCTION AND FOLLOW ON SUPPORT OF) SYSTEM

(SHORT TITLE: PSI)

issued by

JOINT PROGRAM OFFICE
(Address)

Date

DISTRIBUTION LIST

PARTICIPANTS **No OF COPIES_____**
Country:
PM_____

PROSPECTIVE PRIME CONTRACTORS

AMENDMENT SHEET

SERIAL	REFERENCE	DATE	SIGNATURE AND NAME

FOREWORD

A. BACKGROUND

The (insert name of program MOU/MOA) Memorandum of (insert Understanding or Agreement, as applicable) provided for the (insert the purpose of the basic MOU/MOA, e.g., Co-development) by the Governments of (insert the countries of the Participants) of a (insert the name of the system involved, e.g., short range air defense system).

B. AUTHORITY

Section (insert applicable section of the MOU/MOA) requires the preparation of this Program Security Instruction (PSI). This Program Security Instruction is complementary to and not a replacement for the Participants' applicable national security rules and regulations (GUIDANCE: such regulations may be referred to by name and reference if required).

C. APPROVAL

This PSI is issued by the (insert name of program) Joint Program Office (JPO) with the concurrence and approval of the National Security Authorities/Designated Security Authorities (NSAs/DSAs) of (insert names of the Participating countries).

TABLE OF CONTENTS

Page N-

DISTRIBUTION LIST 3

AMENDMENT SHEET 4

FOREWORD 5

TABLE OF CONTENTS 6

INTRODUCTION AND GLOSSARY 8

1.1. PURPOSE 8
1.2 AUTHORITY, RESPONSIBILITY, AND APPLICABILITY 8
1.3. SECURITY RESPONSIBILITIES 8
1.4. GLOSSARY OF TERMS 10

SECTION II 16

SECURITY INSTRUCTIONS 16

2.1. GENERAL PRINCIPLES 16
2.2. ACCESS 16
2.3 INTERNATIONAL TRANSMISSION OF INFORMATION, DATA, OR MATERIEL 16
2.4 MARKING OF PROGRAM INFORMATION 17
2.5 PROCEDURES FOR THE PROTECTION OF CONTROLLED UNCLASSIFIED INFORMATION 18
2.6. PROCEDURES FOR PROTECTION OF RESTRICTED INFORMATION 18
2.7. SECURITY CLASSIFICATION 19
2.8. SECURITY VIOLATIONS 20

RELEASE OF INFORMATION 22

3.1. UNILATERAL RELEASE 22
3.2. RELEASE OF INFORMATION AND MATERIEL TO NON-PARTICIPANTS OR THIRD PARTIES 22
3.3 RELEASE OF PROGRAM INFORMATION AT SYMPOSIA, SEMINARS AND CONFERENCES 22
3.4 PUBLIC RELEASE OF PROGRAM INFORMATION 22
3.5. EXHIBITION AUTHORIZATION 23

INTERNATIONAL VISITS 24

4.1 GENERAL 24
4.2. ALTERNATIVE A: STANDARD PROCEDURES FOR VISITS 24
4.3 ALTERNATIVE B: STREAMLINED VISIT PROCEDURES 26

SUBCONTRACTING 28

5.1 DOMESTIC SUBCONTRACTS 28
5.2 INTERNATIONAL SUBCONTRACTS 28

LISTING OF SECURITY CLEARED FACILITIES 29

6.1. GENERAL 29
6.2. LIST OF SECURITY CLEARED FACILITIES 29
6.3. DISTRIBUTION OF FACILITIES LIST 29
6.4. UPDATED FACILITIES LIST 29
6.5. USE OF THE FIS SHEET AND PSCC SHEET 29

SECURITY PLAN IN EVENT OF TERMINATION OR EXPIRY OF MOU OR NON-SELECTION OF CONTRACTOR 30

7.1. GENERAL *30*
7.2. GOVERNMENT HELD INFORMATION *30*
7.3. CONTRACTOR HELD INFORMATION *30*

SECURITY EDUCATION AND AWARENESS **32**

8.1 GENERAL PRINCIPLES *32*
8.2 SECURITY BRIEFING *32*
8.3 SECURITY AWARENESS *32*
8.4 TRAVEL SECURITY BRIEFING *33*
8.5 SECURITY DEBRIEFING *33*

LIST OF ANNEXES **34**

ANNEX A **35**

LIST OF PROGRAM PARTICIPANTS AND PRIME CONTRACTORS 35

ANNEX B **36**

SECURITY CLASSIFICATION GUIDE 36
TABLE OF CONTENTS 37
GENERAL INFORMATION 38
1.1. PURPOSE *38*
1.2 AUTHORITY *38*
1.3 CLASSIFICATION LEVEL *38*
1.4 GLOSSARY OF TERMS USED IN THIS GUIDE *38*
1.5. CLASSIFICATION RECOMMENDATIONS/GUIDANCE *38*
1.6 DOWNGRADING/DECLASSIFICATION INSTRUCTIONS *39*
1.7 OTHER INSTRUCTIONS *39*
1.8 MARKINGS FOR CLASSIFIED INFORMATION *39*
1.9 REVIEW SCHEDULE *40*

ANNEX C **41**

REQUEST FOR VISIT 41

ANNEX D **45**

PROTECTION OF INFORMATION HANDLED IN IT AND COMMUNICATION SYSTEMS 45
SECTION I - INTRODUCTION 45
SECTION III - NON TECHNICAL SECURITY MEASURES 46
SECTION IV - TECHNICAL SECURITY MEASURES 47
SECTION VI - ACCREDITATION 50
SECTION VII - COMPUTER EQUIPMENT 51
ANNEX A - DEFINITIONS 53

ANNEX K **56**

ABBREVIATIONS AND ACRONYMS 56

SECTION I

INTRODUCTION AND GLOSSARY

1.1. PURPOSE

The purpose of this Program Security Instruction (PSI) is to establish procedures and assign responsibilities for implementation of security requirements prescribed by the (insert Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA), as applicable) the (insert between or among, as applicable) the (insert the names of the Participants) 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: (insert the program name) (insert MOU or MOA, as applicable), dated (insert the effective date). It provides additional specific security procedures to be followed for the Program. It provides instructions for the Participants on the classification of information and equipment; security procedures, including the handling and transfer of classified materiel, and visit procedures for the Program. Terms used in the PSI are defined in Section 1.4.

1.2 AUTHORITY, RESPONSIBILITY, AND APPLICABILITY

1.2.1. This PSI is issued by the JPO pursuant to (insert the applicable section of the MOU/MOA, e.g., Section XII, paragraph 12.6. of the (insert the program name) MOU/MOA), and is effective from the date shown on the front page. This PSI applies to all Participants, as well as military and civilian personnel and approved Contractors involved with the Program. This PSI has been approved by the Participants' National Security Authorities/Designated Security Authorities (NSAs/DSAs), as applicable. Requests for clarification of this PSI should be directed to the JPO, 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 JPO to the NSAs/DSAs, for consideration. Changes will not be made without approval of the NSAs/DSAs. The Steering Committee if established (insert applicable section of the MOU/MOA, e.g., Section IV of the (insert the program name) MOU/MOA) will be notified of clarifications, changes, or revisions.

1.2.2. The Participants' NSAs/DSAs, as well as Program Managers and Security Officers of governments and industrial facilities involved in the Program, are listed at Annex ( ). The NSA or DSA of each Participant has overall responsibility to ensure national compliance with the security requirements of this Program. The NSA/DSA may designate or delegate authority for industrial security, as appropriate, to a Cognizant Security Agency (CSA) to implement the PSI within industry, after the PSI is approved.

1.3. SECURITY RESPONSIBILITIES

1.3.1. **Program Steering Committee**. The Steering Committee has the following security responsibilities:

a. Oversee and assure enforcement of security aspects of the Program.

b. Approve, as appropriate, restrictions on the distribution of Documents and materiel covering technical information as described in (insert the applicable sections of the MOU/MOA, e.g., 9.4.2.1 and 9.6.2. 1) of the (insert MOU/MOA, as applicable).

1.3.2 **Program Manager, (insert the program name) JPO.** The Program Manager has responsibility for the overall security of the Program, to include the following:

a. Prepare and implement the security procedures for the Program, in coordination with the NSAs/DSAs.

b. Review, approve and recommend revisions to the Security Classification Guide (SCG) with the aim of downgrading the classification whenever possible.

c. Prepare a Security Clause or Contract Security Classification Specification that reflects the requirements of the Program (insert MOU/MOA, as applicable) and this PSI for the release of Classified Contracts and subcontracts as described in Annex J. (See MISWG Document 18 for guidance)

d. Ensure that Program Contracting Officers include security requirements in contracts/subcontracts and Invitations to Tender (ITT) or Requests for Proposal (RFP) consistent with the Program (insert MOU/MOA, as applicable) and this PSI.

e. Appoint a Security Manager at the JPO to enforce the execution of the security requirements and procedures outlined in this PSI.

f. Ensure that necessary actions are taken in the event of inventory discrepancies, Compromises, and security deficiencies or breaches in accordance with Section II, paragraph 2.8 of this PSI.

1.3.3 **Program JPO Security Manager**. The Program JPO Security Manager will have responsibility for the following:

a. Enforcing the implementation of this PSI.

b. Managing all day-to-day Program security procedures.

c. Preparing and staff recommended updates to this PSI.

1.3.4. **NSAs/DSAs of the Participants.** The NSA/DSA of each Participant has the overall security responsibilities described below:

a. Approve any changes or revisions to this PSI.

b. Resolve any conflict that may arise regarding implementation of the procedures described in this PSI.

c. Conduct investigations of reported security violations and recommend corrective actions.

1.3.5. **Program Directors at both government and Contractor facilities**. Program Directors are ultimately responsible for the security of the Program at their facilities, to include the following:

a. Implement this PSI at their facilities.

b. Ensure that a security officer has been appointed at each facility where Program Classified Information is used or stored. This officer is responsible for safeguarding at that facility any information and materiel pertaining to the Program and for executing the security requirements and procedures outlined in this PSI.

c. Ensure that actions prescribed by this PSI and national regulations are taken in the event of inventory discrepancies, Compromises, and security deficiencies or breaches, and that the JPO Security Manager and the Participant's NSAs/DSAs, and the CSAs, as applicable, are immediately notified of same.

1.4. GLOSSARY OF TERMS

ACCESS

The ability and opportunity to obtain knowledge of Classified 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 materiel.

AUTOMATED INFORMATION SYSTEM SECURITY

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

BACKGROUND INFORMATION

Program information not generated in the performance of the Program.

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

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

CLASSIFIED MEETING

A conference, seminar, symposium, exhibition, convention, or other gathering that is conducted by a Participant or by a cleared program Contractor with JPO approval and sponsorship, during which Classified Information is disclosed.

COGNIZANT SECURITY AGENCY (CSA)

The agency designated by the NSA/DSA to oversee implementation of industrial security requirements of the Program.

COMPROMISE

A situation when - due to a breach of security or adverse activity (such as espionage, acts of terrorism, sabotage or theft) - the Classified Information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorized individuals (e.g. through espionage or to the media,) unauthorized modification, destruction in an unauthorized manner, or denial of service..

CONTRACTING OFFICE/AGENCY

A government or contractor activity designated under national laws to have the authority to enter into, administer, or terminate contracts and make related determinations and findings.

CONTRACTOR

Any entity awarded a Contract by a Participant's Contracting Agency.

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Unclassified Information to which Access or distribution limitations may apply in accordance with applicable national laws or regulations. Whether the information is provided or generated under the Program MOU, the information will be marked to identify its "in confidence" nature. It could include information that has been declassified, but remains controlled.

COURIER

An appropriately cleared and authorized employee of the JPO or Contractor approved by the NSAs/DSAs to hand-carry classified materiel 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 materiel.

DESIGNATED SECURITY AUTHORITY (DSA)

The security authority designated by national authorities to be responsible for the coordination and implementation of national industrial security aspects of the Program /Project

DESIGNATED GOVERNMENT REPRESENTATIVE (DGR)

A person designated by the NSA/DSA, or CSA, 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 materiel on behalf of the releasing government at a Contractor facility. A DGR at the receiving facility ensures the materiel is received in proper order and inventoried, and accepts the materiel on behalf of the receiving government.

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, tape recording, or magnetic recording.

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 certain classification level.

FACILITY SECURITY OFFICER

A person designated by management to be responsible for the proper implementation of security related decisions and for co-ordination of available security resources and measures within a facility involved in classified projects, as well as to be the technical advisor to management on security matters.

FOREGROUND INFORMATION

Information generated in the performance of the Program.

GOVERNMENT-TO-GOVERNMENT CHANNELS

The process for transfer of Classified Information approved by the NSA/DSA of the Participants in accordance with National rules and as stated in the respective bilateral Industrial Security MOUs/Arrangements.

JOINT PROGRAM OFFICE (JPO)

The Program Office, headed by the Program Manager (PM), established for the management of the Program.

MATERIEL

Any product or substance on or in which information is embodied.

NATIONAL SECURITY AUTHORITY (NSA)

The entity of the government of each Participant responsible for the security of information of national security importance.

NEED-TO-KNOW

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 organization, geographically disseminated or within a single site, of Information Technology (IT) systems interconnected to exchange data, and comprising the components of the interconnected IT systems and their interface with supporting data or communications network components. Such components may include Automated Information Systems, 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.

PARTICIPANTS' CONTRACTORS

Contractors or Subcontractors authorized to take part in the Program who are legally bound to comply with the provisions of a contract.

PROGRAM

The (insert the name of the program) approved by the (insert name of program MOU/MOA as applicable, and date).

PROGRAM EQUIPMENT

Any materiel, 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.

PUBLIC DISCLOSURE

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

SECURITY CLAUSES/CONTRACT SECURITY CLASSIFICATION SPECIFICATION

A Document issued by the JPO or Contractor, as part of any Classified Contract or subcontract, identifying the security requirements or those elements requiring security protection for a Classified Contract.

SECURITY VIOLATION

Any knowing, willful, or negligent action that could reasonably be expected to result in loss, Compromise or unauthorized disclosure of Classified Information.

SUBCONTRACT

Any contract entered into by a contractor to furnish supplies or services for performance of a prime contract or a subcontract.

SUBCONTRACTOR

A supplier, distributor, vendor or firm that furnishes supplies or services to or for a prime contractor or another subcontractor, who enters into a contract with a prime contractor.

TRANSMISSION

The sending of information from one place to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire or other connective medium. Transmission also includes movement involving the actual transfer of classified materiel from one authorized addressee to another.

THIRD PARTY

Insert definition from MOA/MOU

SECTION II
SECURITY INSTRUCTIONS

2.1. GENERAL PRINCIPLES

2.1.1. All Classified Information exchanged, held, used, or generated in connection with this Program will be stored, handled, safeguarded, and transmitted in accordance with the Participants national security rules and regulations as supplemented by this PSI. Access to Classified Information and materiel will be restricted to facilities and individuals that have the requisite level of facility or personnel security clearance and that have a need to know for the purposes of this Program. Access to and control of Controlled Unclassified Information and RESTRICTED information will be in compliance with paragraphs 2.5 and 2.6, below.

2.1.2. Classified Information will be transmitted only through approved government-to-government channels. Upon receipt, it will either retain its original classification markings or be marked with the recipient Participant's equivalent classification as detailed below:

Security Classification Equivalencies.

Participant	Secret	Confidential	Restricted

2.2. ACCESS

2.2.1 Access to Classified Information and materiel CONFIDENTIAL and above will be granted to individuals holding the sole nationality of a Program Participant without the prior authorization of the originating Participant.

2.2.2 Access to Classified Information and materiel CONFIDENTIAL and above by individuals holding the nationality or dual nationality of a non Program Participant will be subject to prior authorisation of the originating Participant. However, Access to Classified Information and materiel CONFIDENTIAL and above may be granted on a "need-to-know" basis to individuals holding the nationality or dual nationality of (insert name of countries or groups of countries from MOA/MOU) without the prior authorisation of the originating Participant.

2.3 INTERNATIONAL TRANSMISSION OF INFORMATION, DATA, OR MATERIEL

The standard means of transmitting Classified Information and materiel across international borders is through government-to-government channels.

2.3.1. 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 transmission channels of the Participants' governments, specifically military Courier, diplomatic pouch, or military postal channels. However, other channels may be used with the prior approval of the Participants' NSA/DSA.

2.3.2. Hand Carriage. To meet an urgent need to transfer classified Documents and program equipment or components between Program Participants and their Contractors, special arrangements for hand carriage may be approved by the responsible NSAs/DSAs. Hand carriage may be used on a case-by-case basis when 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 materiel being hand carried must be sealed while in transit, may not be opened en route, and requires direct delivery from the secure facility originating point to the secure facility at the destination. The hand carrying of classified materiel will be in compliance with the procedures at Annex (.). Use of the hand carry procedure is restricted to the approved Contractors in the List of Security Cleared Facilities (reference Section VI, paragraph 6.2 of this PSI). The Modification of the procedures is not permitted without the approval of the Participants' NSAs/DSAs.

2.3.3. Secure Communications. Secure government communications channels may be used for transmission of Classified Information, and such CUI as may be agreed by the Participants. The decision to authorize such use for the Program requires the approval of the NSAs/DSAs, and a written agreement among the communications security authorities of the Participants. The installation and use of communications security equipment will be in compliance with the national security regulations of the Participants. 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 (.) to the PSI.

2.3.4. Transmission of Classified Materiel as Freight.

a. International Transmission. Prior to the international transmission of Program classified materiel as freight, the NSAs/DSAs of the consignor and of the consignee must agree upon a Transportation Plan for its movement. The Transportation Plan will be prepared in compliance with the guidelines at Annex ( ).

b. Transmission within a Participant's Country. The transmission of classified materiel as freight within a Participant's country will be in accordance with national procedures.

2.4 MARKING OF PROGRAM INFORMATION

Documents and other materiel containing information provided to or generated under the program will be marked by the originating Participants with a legend reflecting the country of origin and in addition to any classification marking, with an annotation that identifies it as (insert program name) program information. Materiel containing Foreground Information also will be marked to indicate that it was generated under the (insert program name) Program. For program materiel that contains Background Information, there will be an annotation that identifies the fact that the materiel 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 materiel is of such nature that it cannot be marked, the markings will be applied to a cover or label.

(NOTE: Background and Foreground Information and certain other Program Information may require special markings to indicate the nature of controls that are required in accordance with Program requirements, and as the result of restrictions on Background Information. If one or more Participants does not have national rules to protect national or foreign CUI or RESTRICTED information, the markings to be used by those countries to identify such information for control must be specified here, in the Classification Guide, or in an Annex to this PSI.)

2.5 PROCEDURES FOR THE PROTECTION OF CONTROLLED UNCLASSIFIED INFORMATION

2.5.1. NOTE: If required by (insert applicable section of the Program MOU/MOA, e.g., Section X of the Program MOU), Access to Controlled Unclassified Information (CUI) provided to or generated pursuant to the Program will be controlled. The procedures for the protection of CUI are outlined below. If one or more parties do not have national laws and regulations to require safeguarding of CUI, include instead: "The procedures for the protection of CUI will be implemented on a contractual basis as outlined below:"

2.5.2. Protection. CUI must be locked in a desk, file cabinet, office or protected by such means to preclude unauthorized Access when not in use. The information must be destroyed in a manner that it can not 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). Transmission may be through normal mail channels or by hand carrying without formal Courier orders. CUI may not be displayed in a public place, such as an airport or train station. It must not be transmitted through non-secure electronic mail on public networks, unless it is encrypted. Computers used to process the information must prevent unauthorized Access, but do not have to be accredited for classified use, unless they also process Classified Information.

2.5.3. Unauthorized Disclosure. Administrative action will be taken to fix responsibility for unauthorized disclosure, and appropriate disciplinary action will be taken against the responsible party. The unauthorized disclosure will be reported to each Participant's Program Office security office.

2.6. PROCEDURES FOR PROTECTION OF RESTRICTED INFORMATION

GUIDANCE: This section will be included or not as appropriate based on the MOU.

Documents or other media that contain RESTRICTED information, but that otherwise would be unclassified, will be protected as below.

2.6.1 Access.

a. Where required by national regulations, Contractor facilities that require Access to RESTRICTED information must be security cleared.

b. The information will be provided only to facilities or persons whose Access is necessary in connection with their involvement in the Program.

c. All persons who are to be given Access to the information must be informed of and acknowledge their responsibilities for protecting the information. Personnel security clearances are not necessary unless required under national regulations.

2.6.2 Protection.

The information will not be left unattended or handled in a manner that could result in unauthorized Access. It must be stored in locked desks, cabinets, or similar containers to which Access is restricted. It also may be stored in the open in locked rooms, provided Access to the room is restricted to persons who are authorized to have Access to the information by the local Security Manager. When the information is not secured in a container, it will be turned face down or be protected by a cover sheet that is marked to identify the fact that it covers RESTRICTED information. During hand carriage by government or Contractor personnel the information must remain in the personal custody of the Courier or be secured as described herein. It may not be left unattended in hotel rooms or vehicles. It may not be read in public.

2.6.3 Transmission. (Suggested terms only. Details of protection may vary based on national laws)

a. Documents or other media containing RESTRICTED information may be transmitted within the Participants' countries by a national mail system or by non-cleared commercial delivery services. Double envelopes or wrappings are not required. The envelope or wrapping will be opaque and will not reveal that the package contains RESTRICTED information. (The Participants must agree whether receipts are required and insert that information here.)

b. The international transmission of Documents or other media containing RESTRICTED information may be through international postal channels or commercial delivery services approved by the NSAs/DSAs. (The Participants must agree whether receipts are required and insert that information here.)

c. RESTRICTED information may be transmitted or Accessed electronically via a public network like the Internet, using government or commercial encryption devices mutually accepted by the relevant national authorities. However, telephone conversations, video conferencing or facsimile transmissions containing RESTRICTED information may be in clear text, if an approved encryption system is not available. (Approval of encryption devices will vary based on national law.)

2.6.4. Destruction. Documents or other media containing RESTRICTED (program name) information will be destroyed by any method approved for the destruction of Classified Information. There is no requirement for a record of destruction.

2.6.5. Reproduction. The reproduction of RESTRICTED information will be limited to that which is necessary in support of a (program name) contract.

2.6.6. Use in Automated Information Systems (AIS). RESTRICTED information will be processed and stored in AIS in accordance with approved national regulations.

2.7. SECURITY CLASSIFICATION

a. The Program Security Classification Guide (SCG) (Annex ( ) and changes thereto are the basis for classification, regrading, or declassification of Foreground Information or materiel concerning the Program. Questions concerning the content and interpretation as well as proposed changes to the classification guide will be coordinated, as appropriate, by (insert the name of the JPO), with the Program Steering Committee and 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.

b. Information generated under the Program will be classified and marked in accordance with the Program SCG. If the appropriate classification is unclear, the matter will be referred to (insert the name of the JPO). Until the matter is resolved, the classification level assigned should be the highest anticipated. Security classification must be determined by considering all applicable information and references.

2.8. SECURITY VIOLATIONS

2.8.1 All Participants' civilian and military personnel and their approved Contractors must 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 their NSA/DSA, through the CSA, as applicable, in addition to reporting procedures prescribed by national regulations. The Participants NSA/DSA will notify the JPO. If the incident occurs at the JPO, the security officer will report the incident to the (insert name of Program Manager) and to the NSAs/DSAs of the Participants. The security officer of the facility where a violation or Compromise may have occurred will investigate all such occurrences and inform their NSA/DSA of the results. Each Participant's NSA/DSA will promptly and fully inform the other Participants' NSAs/DSAs 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 must include the following details:

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 and markings of the information involved in the incident.

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

f. An assessment of the likelihood of Compromise (i.e. "certain", "probable", "possible", or "unlikely")

g. A statement of whether the originator has been informed.

h. Actions taken to secure the materiel and limit further damage.

i. A list of the information that has been Compromised or materiel that is unaccounted for.

j. Reasons for loss/Compromise or possible loss/Compromise.

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

2.8.3. Reports of investigations involving CONFIDENTIAL information and above must be provided to the NSA/DSA and JPO within 90 days.

SECTION III

RELEASE OF INFORMATION

3.1. UNILATERAL RELEASE

The unilateral release of classified or unclassified program information or materiel to other than program Participants and their 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 MATERIEL TO NON-PARTICIPANTS OR THIRD PARTIES

3.2.1 No program information (except that which has been approved for public release in accordance with paragraph 3.4 below) may be released to non-Participants or their Contractors, 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. Access on a need-to-know basis will be given in any case to nationals of (insert list of countries from program MOA/MOU if any) without prior consent of the Program Participants.

3.2.2 Requests for release to non-Participants or their Contractors will be submitted through the JPO to the (insert the official that is designated by each Participant to receive and coordinate such requests).

3.3 RELEASE OF PROGRAM INFORMATION AT SYMPOSIA, SEMINARS AND CONFERENCES

Speeches and presentations involving program information to be presented at symposia, seminars, and conferences, whether at government establishments, Contractor facilities, or other properly approved venues, when persons representing other than the Program Participants or their Contractors are present, must be submitted through the JPO to (insert the officials that are designated by the Participants to receive and coordinate such requests) for prior approval. 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 (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, date of presentation, nationality of non-participating representatives and the countries represented, title of the symposium or seminar, and other information which may be required by national regulations. (NOTE: The designated officials should be listed at an Annex

3.4 PUBLIC RELEASE OF PROGRAM INFORMATION

3.4.1 Written approval for public release of all Foreground Information, including publicity materiel and materiel for open release at symposia, conferences or exhibitions will be sought

through (insert prescribed channels agreed by the Participants) to the JPO. Contractors must ensure that Subcontractors follow the same procedures. The JPO may reject such proposals without further recourse. Release authorization will be made following consultation with the NSAs/DSAs. All proposals that the JPO endorses are to be submitted to the appropriate NSA/DSA or other NSA/DSA specified authorities of the Participants (NOTE: The designated officials should be listed at Annex ( ).)who will then grant or deny release in accordance with national regulations. A minimum of (insert number) calendar weeks should be allowed for review of the proposal.

3.4.2 Background Information to be publicly released will be cleared by the appropriate originating government's release authority in accordance with national regulations. An information copy of the clearance will be sent to the JPO.

3.4.3 It is incumbent upon government organizations 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 national security.

3.5. EXHIBITION AUTHORIZATION

Contractors that display program information and materiel at exhibitions must have available at each exhibition a copy of the Document that provides authorization for the display. Contractors must ensure that all information on public display (e.g., at Air Shows, International Exhibitions, etc.) is displayed in the form in which it was officially authorized for release.

SECTION IV

INTERNATIONAL VISITS

4.1 GENERAL

4.1.1 Visits by the Participants' government and Contractor personnel to facilities of another Participant for Program purposes require advance authorization. In order to avoid the need to submit a visit request for each visit, maximum use will be made of the recurring visit authorization, as described below. Reference to the (insert program name) Program will be included in all visit requests.

4.1.2 Types of visits. There are three types of international visits that will be used for the Program:

a. One-Time Visit. A one-time visit is for a single, short-term occasion (normally less than 30 days) for a specified purpose.

b. Recurring Visit. Recurring visits permit 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.

c. Extended Visit/Attachment. A one-time, long-term visit for a specified period of time, subject to annual review and validation.

4.1.3 Facilities List Preparation. The JPO will prepare and maintain a consolidated list, known as the "Facilities List", of the participating government and Contractor facilities. (See Section VI, paragraph 6.2 of this PSI). Only those facilities listed on the "Facilities List" will be authorized to submit Requests for Visit Authorization (RVA) or receive visitors in connection with the Program. The list must be updated if new facilities become involved in the Program.

(NOTE: Based on prior agreements among participants, and with the approval of the NSA/DSA of the parties, variants of instructions for visits may be needed. Two possible alternatives are presented as Alternatives A: Standard Procedures, and B: Streamlined Procedures.)

4.2. ALTERNATIVE A: STANDARD PROCEDURES FOR VISITS

4.2.1 REQUESTS FOR VISIT AUTHORIZATION (RVA) FOR VISITS RELATED TO INFORMATION CLASSIFIED CONFIDENTIAL AND ABOVE.

A. SUBMISSION OF RVAs. All RVAs by personnel of one Participant to a facility of another Participant will be submitted through government channels, and will conform to the established visit procedures of the host NSA/DSA. RVAs will contain the information described in Annex C. RVAs should be in the possession of the receiving (i.e., host) Participant's NSA/DSA at least (insert the number of days) working days prior to the starting date of a one-time visit or extended visit, or the date of the first recurring visit. Those facilities submitting RVAs should remember that lead time is also required to process the request through the requesting NSA/DSA. In the

case of recurring visit authorizations, the host site security officer must be notified 72 hours (3 working days) in advance of each recurring visit, unless the host site security officer agrees otherwise.

B. 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. Amendments that request earlier dates than originally specified will not be accepted. Emergency visit authorizations will not be amended.

C. RECURRING VISIT REQUESTS. The security officers of each Participant's government and Contractor facilities will identify and list employees who are involved in the Program, and submit requests for recurring visits for those employees through their NSA/DSA or CSA, as applicable.

D. REVIEW AND UPDATE OF VISIT LISTS. The JPO will 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 will be deleted.

E. EMERGENCY VISITS

1. General. Occasionally, the minimum time allowed for a visit approval is not available. Such visits may be arranged as emergency visits. To qualify as an emergency visit, the visit must relate to the Program, or a Program related contract or announced request for proposal, and failure to make the visit reasonably could be expected seriously to jeopardize performance on the contract or program, or result in the loss of a contract opportunity. Emergency visits will be approved only as a single, one-time visit. If subsequent visits are necessary, the requester should submit a follow-up request for a recurring visit authorization.

2. Procedures. Emergency visit requests will be critically reviewed, fully justified, and Documented by the security officer of the requesting government agency or Contractor facility. When the security officer is satisfied that the circumstances warrant an emergency visit, the security officer will directly contact the security officer at the host facility by telephone or fax, to obtain tentative verbal agreement for the proposed visit. If tentative verbal agreement is provided, the security officer of the host facility will immediately notify, by the most expeditious means (e.g., fax, email, 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.

3. The security officer of the requesting facility will send a message or fax, in the visit request format, through the NSA/DSA of the requesting country, to the NSA/DSA of the host facility; and to the security officer of the host facility. Any of these officials may deny the visit. The sending security officer should ensure that the complete name, grade or position, address, and telephone number of the person who gave tentative authorization is included in the visit request, along with the identification of the contract, agreement, or program and the justification for submission of the emergency visit request.

4. Upon receipt of the request, each NSA/DSA involved will 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 two (2) working days prior to the start of the emergency visit, the security office of the facility that initiated the request will contact the security office of the host facility to determine the status of the emergency visit request.

5. If the NSA/DSA of the country of the host facility approves or denies the request, it will immediately notify the security officer of the facility to be visited and the NSA/DSA of the requesting country of the decision. The host security officer will then notify the requesting security officer that the visit is approved or denied.

4.2.2 REQUESTS FOR VISIT RELATING TO INFORMATION CLASSIFIED BELOW CONFIDENTIAL

A. VISITS ONLY RELATED TO INFORMATION CLASSIFIED RESTRICTED. Depending on the laws and regulations of the Participants, visits related to information classified as RESTRICTED may be included under standard visit request procedures or be processed using procedures only for visits related to Unclassified Information.

B. VISITS ONLY RELATED TO UNCLASSIFIED INFORMATION. These visits may be arranged directly between the sending and receiving facility. It is the responsibility of the host facility to ensure that all requirements for export or other release controls and facility security are met.

4.3 ALTERNATIVE B: STREAMLINED VISIT PROCEDURES

4.3.1 VISITS RELATING TO INFORMATION CLASSIFIED CONFIDENTIAL AND ABOVE

A. Prior to arrival at a government department or establishment or at an industrial facility (all together hereinafter called Facility), confirmation of the visitor's PSC must be provided directly to the receiving Facility in the form of Annex C by the security officer of the sending Facility.

B. The visitor must present an ID card or passport to confirm their identity to the security authorities at the receiving Facility.

C. It is the responsibility of the security officer of :

1. The sending Facility to ensure with their NSA/DSA that the Facility to be visited is in possession of an appropriate FSC,

2. Both the sending and receiving Facilities to agree that there is a need for the visit.

D. The receiving security officer must ensure that records are kept of all visitors, including their name, the organization they represent, date of expiry of the PSC, the date(s) of the visit(s), and the name(s) of the person(s) visited.

4.3.2 VISITS RELATING TO INFORMATION CLASSIFIED RESTRICTED OR UNCLASSIFIED

Such visits also may be arranged directly between the sending and receiving Facility.

SECTION V

SUBCONTRACTING

5.1 DOMESTIC SUBCONTRACTS

a. Before entering into negotiations for a subcontract or order involving the release of Program Classified Information CONFIDENTIAL or above to a company in his/her own country, the security officer of the company letting the contract will ask his/her NSA/DSA or CSA, as applicable, for an FSC verification for the potential Subcontractor. The FSC Information Sheet at Annex ( ) will be used. [**GUIDANCE:If required under national regulations an FSC should also be obtained for the release of RESTRICTED Information].**

b. The request for an FSC verification must include details of the highest level of Classified Information to be released, the nature and volume of the information and an explanation of the need for the potential Subcontractor to receive the information.

c. If an FSC verification is issued by the NSA/DSA and the classified subcontract is let, two copies of the subcontract (security related aspects only) will be forwarded to the NSA/DSA or CSA to enable the security performance of the Subcontractor to be monitored.

5.2 INTERNATIONAL SUBCONTRACTS

a. Prior to letting a subcontract with a company in another Participating nation, or outside any of the Participating nations, the security officer of the company that wishes to let the subcontract will first obtain the approval of the JPO. The above requirements also will be required for such international subcontracts.

b. On receipt of the request for an FSC verification for precontract discussions, the NSA/DSA of the country in which the potential Subcontractor is located will complete the reply section of the request for FSC form. Precontract discussions may take place after receipt of the reply.

c. If an international contract is let, two copies of the subcontract (security related aspects only) will be passed from the placing company to its NSA/DSA. The NSA/DSA will then pass the security aspects to the NSA/DSA of the Subcontractor who will make the necessary arrangements for the protection of all Classified Information released to the Subcontractor under the subcontract.

SECTION VI

LISTING OF SECURITY CLEARED FACILITIES

6.1. GENERAL

This section outlines the procedures for the development and maintenance of the list of Government organizations and Contractor and Subcontractor facilities that are involved in the Program and to which Classified Information/materiel can be distributed. (Annex ( )). It also covers the use of the Facility Security Clearance Information (FIS) Sheet (Annex ( )) and the Personnel Security Clearance Confirmation Sheet (PSCC) Sheet (Annex ( )).

6.2. LIST OF SECURITY CLEARED FACILITIES

The JPO will prepare a list of the government and Contractor facilities participating in the Program. The level of Facility Security Clearance and storage capability of each Contractor facility will be verified by each Participants NSA/DSA, or CSA, as applicable, prior to the facility being placed on the list. The list will include the information described in the FIS sheet at Annex ( ).

6.3. DISTRIBUTION OF FACILITIES LIST

The JPO, after validating that it is correct, will distribute the Facilities List to each Participant's NSA/DSA and the CSAs, if applicable.

6.4. UPDATED FACILITIES LIST

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

6.5. USE OF THE FIS SHEET AND PSCC SHEET

The FIS Sheet (Annex ( )), and the PSCC Sheet (Annex ( )) will be used when there is a need to request and verify facility security clearances and personnel security clearances for facilities and personnel that are to be added to the Facilities List or the list of personnel who are to make recurring visits, or who may otherwise become involved in the Program.

SECTION VII

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

7.1. GENERAL

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

a. Any of the Participants terminate the MOU.

b. The MOU expires.

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

d. A Contractor receives and 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.

The responsible Contracting Officer will ensure that the terms of this section are included as an obligatory requirement of each contract let by the JPO or by a Participant.

7.2. GOVERNMENT HELD INFORMATION

In the event of termination or expiration of the MOU, the Participants' respective rights and responsibilities with regard to Background Information and Foreground Information will be determined in accordance with the provisions of (cite the applicable section of the Program MOU/MOA, e.g., Section XVIII of the (insert 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, must safeguard it in accordance with national rules and regulations and this PSI. The Participant will protect that information at the same level or higher as described in the Program Security Classification Guide, if classified, and will not use that information for other purposes without the prior written consent of the Participant that provided the Background Information.

7.3. CONTRACTOR HELD INFORMATION

7.3.1 All Classified Information or CUI received in the performance of, or in anticipation of a Program contract must be returned to the Contracting Office on completion or termination of, the contract unless the information has been declassified or removed from control, destroyed, or authorized for retention by the Contracting Office.

7.3.2 Contractors must return or destroy program classified or Controlled Unclassified Information not approved for retention in accordance with the following schedule:

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

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

c. 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.

d. If the Classified Information was not received under a specific contract, such as information obtained at Classified Meetings or from a secondary distribution center: within 1 year after receipt.

7.3.3 Termination of Facility Security Clearance. In the event that a Facility Security Clearance is to be terminated, the Contractor must return all Classified Information and CUI in its possession to the Contracting Office or dispose of such information in accordance with instructions from the Contracting Office.

SECTION VIII

SECURITY EDUCATION AND AWARENESS

8.1 GENERAL PRINCIPLES

8.1.1 Government and Contractor employees who will have Access to program Classified Information and CUI and materiel will be briefed on, or otherwise informed of, and acknowledge their understanding of their responsibilities for protection of such information and materiel. This may be accomplished by a briefing, the use of written materiel or by electronic means.

8.1.2 Participants engaged in classified work in connection with the program will develop a security education and awareness program to ensure that personnel are thoroughly familiar with their individual security responsibilities regarding classified program information and materiel. Security education and awareness programs will be tailored to satisfy the specific security aspects of the program by using national security procedures and regulations as a baseline.

8.1.3 Program participants shall remind all personnel who require Access to Classified Information and materiel of their continuing responsibilities for safeguarding classified program information, to include:

a. The pertinent national laws and regulations which apply to the protection of Classified Information, the requirements of the program MOU/MOA or this PSI and the penalties or other consequences for their violations.

b. Indoctrination on the hostile intelligence threat, collection techniques and methods and defensive measures employed to counter the threat.

c. The need to report promptly all security violations, unauthorized disclosures, or possible Compromise of classified program information and materiel to the FSO.

d. Those security requirements, which specifically pertain to the employee's work assignment and the contents of this PSI.

8.2 SECURITY BRIEFING

Prior to permitting personnel to have Access to classified program information and materiel and periodically during the course of the program, persons will be briefed on the applicable elements in the security briefing outline (which could be included as an APPENDIX () to this PSI). Personnel may be asked to sign a certificate acknowledging that they have received and understand the briefing and that they will comply with all the regulations as they have been explained. Refusal to sign the certification will result in denial of Access to classified program information.

8.3 SECURITY AWARENESS

The security awareness of personnel performing classified work under the program may be addressed by the applicable NSA/DSA during any security inspections. Security awareness also

should be made a matter of interest during self-inspections conducted by the participant's security staff.

8.4 TRAVEL SECURITY BRIEFING

When persons travel to countries where a special security risk may exist, security briefings may be required prior to travel. These briefings will include a discussion of the intelligence threat, tactics used by collectors, and protective measures and precautions the traveler can employ to minimize his/her susceptibility to exploitation. The traveler also will be reminded to report all suspicious contacts to the proper security authorities promptly upon completion of the travel. Travel security briefings should be included in the original security briefing and should be given again as a reminder prior to travel.

8.5 SECURITY DEBRIEFING

Security debriefings may be given to personnel when they no longer require Access to classified program information and materiel and will consist of a reminder of the continuing responsibility to protect classified program information and the penalties for failure to do so. Debriefing certificates may be used to record the debriefings.

LIST OF ANNEXES

A.	LIST OF PROGRAM PARTICIPANTS AND PRIME CONTRACTORS	A-1
B.	SECURITY CLASSIFICATION GUIDE	B-1
C.	VISIT REQUESTS	C-1
D.	PROTECTION OF INFORMATION HANDLED IN IT AND COMMUNICATION SYSTEMS	D-1
E.	HAND CARRIAGE PROCEDURES *(See MISWG 1)*	E-1
F.	TRANSPORTATION PLAN *(See MISWG 10)*	F-1
G.	LIST OF SECURITY CLEARED FACILITIES	G-1
H.	FACILITY SECURITY CLEARANCE INFORMATION SHEET *See MISWG 12)*	H-1
I.	PERSONNEL SECURITY CLEARANCE CONFIRMATION SHEET *(See MISWG 19)*	1-1
J.	CONTRACTOR SECURITY REQUIREMENTS *(See MISWG 18)*	J-1
K.	ACRONYMS AND ABBREVIATIONS	K-1

ANNEX A

LIST OF PROGRAM PARTICIPANTS AND PRIME CONTRACTORS

A-1 NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY

Participants' NSA & DSA

Participants' CSA

A-2 JOINT PROGRAM OFFICE (JPO)

JPO, (insert program name)
(ATTN: PM (insert program name))

ANNEX B

SECURITY CLASSIFICATION GUIDE

OF

PROGRAM SECURITY INSTRUCTION

FOR

(insert program name) PROGRAM

issued by
JOINT PROGRAM OFFICE (Insert program name)
(DATE)

TABLE OF CONTENTS

SECTION **PAGE**

1. GENERAL INFORMATION

- 1.1. PURPOSE
- 1.2. AUTHORITY
- 1.3. CLASSIFICATION LEVEL
- 1.4. APPLICATION
- 1.5. GLOSSARY OF TERMS
- 1.6. CLASSIFICATION RECOMMENDATIONS/GUIDANCE
- 1.7. DOWNGRADING/DECLASSIFICATION INSTRUCTIONS
- 1.8. OTHER INSTRUCTIONS
- 1.9. MARKING INSTRUCTIONS
- 1.10. REVIEW SCHEDULE

2. OVERALL EFFORT

- 2.1. IDENTIFICATION
- 2.2. END ITEM

3. TECHNOLOGY AND CAPABILITIES

4. SPECIFICATIONS

- 4.1. PRODUCTION CHARACTERISTICS

5. MODELLING AND SIMULATION

- 5 1. MODELLING AND SIMULATION

6. ADMINISTRATIVE DATA

- 6 1. FUNDING
- 6.2. QUANTITIES
- 6.3. KEY SCHEDULE DATES

SECTION 1

GENERAL INFORMATION

1.1. PURPOSE

1.1.1 To provide instructions and guidance for classification of information and materiel pertaining to all versions of the (insert program name) system.

1.1.2 Information classified pursuant to this Security Classification Guide (SCG) will be safeguarded in accordance with the applicable national laws, regulations, policies and procedures of the Participants of the (insert program name) and its Program Security Instruction (PSI).

1.2 AUTHORITY

This guide is issued under the authority of the (insert title and date of the applicable MOU/MOA). This guide constitutes authority and may be cited as the basis for classification, regarding, or declassification of information and materiel generated under the (insert program name) Program.

1.3 CLASSIFICATION LEVEL

The highest classification of information covered by this Security Classification Guide is (insert classification level).

1.4 GLOSSARY OF TERMS USED IN THIS GUIDE

1.4.1 ASSEMBLY. A group of two or more physically connected parts.

1.4.2 COMPONENTS. A group consisting of one or more connected assemblies, subassemblies, and/or parts which is capable of operating independently but may be externally controlled or derive -its power from another source, e.g., ballistic computer, engine, transmission.

1.4.3 EXPOSURE. That which can be seen.

1.5. CLASSIFICATION RECOMMENDATIONS/GUIDANCE

1.5.1. Requests for classification determinations referred to the JPO will be decided jointly by the NSAs/DSAs of the Participants.

1.5.2. If the security classification imposed by this guide imposes requirements that are impractical, or if current conditions change or progress attained in the state-of-the-art of this effort, or any other contributory factors indicate a need for changes in this guide, complete, documented, and justified recommendations should be made to the JPO. Pending final decision, the items of information involved will be considered and protected at the higher of the current classification or the recommended level. All users of the guide are encouraged to assist in improving the adequacy of this guide.

1.6 DOWNGRADING/DECLASSIFICATION INSTRUCTIONS

1.6.1 Program Background Information will be downgraded or declassified only by the originating Participant.

1.6.2 Program Foreground Information will be downgraded or declassified only after receiving written approval from the JPO, with concurrence from the NSA/DSA of the Participants.

1.7 OTHER INSTRUCTIONS

1.7.1 The classification levels assigned in this classification guide are the highest level of classification anticipated for each item of information or equipment. A higher classification may be assigned to compilations of information if the compilation provides an added factor that warrants higher classification than that of its component parts. Classification on this basis will be fully supported by a written explanation that will be provided with the materiel so classified.

1.7.2 Reports, publications, drawings, schematics, photographs, mock-ups, training aids, test data, hardware, etc., will be assigned a security classification commensurate with the information classified by this guide and other applicable security classification guides. External and internal views that may yield classified parameters, characteristics, and/or performance will be classified in accordance with classification of those items revealed.

1.7.3 The originating Participant will classify program Background Information. Program Foreground Information, warranting a derivative classification, will be based on a joint decision by both Participants' NSA/DSA, and the JPO.

1.8 MARKINGS FOR CLASSIFIED INFORMATION

1.8.1 All classified Documents will be stamped or marked according to instructions contained in this paragraph. A sample of the front cover markings for a Program Document is at Appendix 1.

1.8.2 Markings

a. Overall Document markings. Each Document will be conspicuously marked or stamped at the top and bottom of the front cover, the first page and the back side of the last page, and the back side of the back cover with the security classification (e.g., RESTRICTED). The following notation will be added directly under the classification marking: “(insert program name) Use Only”.

b. “Classified by”, “Downgrade to”, or “Declassify on” Markings. These markings, together with the agreed dates for the action, will be annotated on the front lower left cover of Documents and will be in compliance with instructions set forth in section (cite the applicable section) of this Security Classification Guide (SCG).

c. Originator and Date Markings. Classified Documents also will be marked on the front, lower right cover, immediately above the marking described above, to show the name and address of the originator responsible for its preparation, and the date of preparation.

d. Page Markings. The overall classification of each page will be reflected at the top and bottom of each page with the following annotation directly underneath the classification marking: "(insert program name) Use Only". The classification marking will reflect the highest level of Classified Information on that page. The level of classification of information in the paragraphs or portion of information on each page will be adequately identified in accordance with the paragraph and portion marking requirement outlined in paragraph e. below.

e. Paragraph/Portion Marking. Paragraph or portion markings on CONFIDENTIAL and SECRET classified Program Documents will be as follows: (U) for UNCLASSIFIED; (R) for RESTRICTED; (C) for CONFIDENTIAL; (S) for SECRET information. Documents that contain only UNCLASSIFIED and RESTRICTED information do not require paragraph markings. If a Document contains Background Information, the paragraph or portion containing such information will be marked to identify the originator (e.g., US-S).

f. Titles of Documents. Portion markings as outlined in paragraph e., above, will be used to annotate the classification of a title. Unclassified titles will be selected for classified Documents whenever possible.

g. Control Markings. One of the following control markings will be annotated on the lower left front page of all Documents to ensure that the information contained therein is used only for purposes outlined in the Program MOU:

> (insert program name) FOREGROUND INFORMATION
> Access Restricted to Program Participants or nationals of non-participants according to para. 3.2 of the Program PSI for Program Use. Release Outside Program Requires Prior Written Consent Of All Participants
>
> OR
>
> (insert program name) BACKGROUND INFORMATION
> Access Restricted to Program Participants for Program Use. Release Outside Program Requires Originator's Prior Written Consent

1.9 REVIEW SCHEDULE

This Security Classification Guide will be reviewed annually on (insert the day of the month, e.g., third day) of (indicate the month), and prior to entering into a new phase of the Program.

ANNEX C

REQUEST FOR VISIT

(To be used with Alternative A: Standard Procedures
Detailed instructions are found in MISWG document 7)

<table>
<tr><td colspan="3">REQUEST FOR VISIT</td></tr>
<tr><td>[ ] One-time
[ ] Recurring
[ ] Emergency
[ ] Amendment</td><td>[ ] Unclassified/RESTRICTED information or access to areas without access to information classified CONFIDENTIAL or above

[ ] CONFIDENTIAL or above involved.</td><td>Annexes:
[ ] Yes

[ ] No</td></tr>
<tr><td colspan="3">1. ADMINISTRATIVE DATA</td></tr>
<tr><td colspan="2">REQUESTOR:

TO:</td><td>DATE:

VISIT ID:</td></tr>
<tr><td colspan="3">2. REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY</td></tr>
<tr><td colspan="2">NAME</td><td></td></tr>
<tr><td colspan="2">POSTAL ADDRESS</td><td>E-MAIL ADDRESS (when known)</td></tr>
<tr><td colspan="2">TELEX/FAX NR.</td><td>TELEPHONE</td></tr>
<tr><td colspan="3">3. GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED</td></tr>
<tr><td colspan="2">NAME</td><td></td></tr>
<tr><td colspan="2">ADDRESS</td><td>E-MAIL ADDRESS (when known)</td></tr>
<tr><td colspan="2">TELEX/FAX NR.</td><td>TELEPHONE</td></tr>
<tr><td colspan="2">POINT OF CONTACT</td><td></td></tr>
<tr><td colspan="3">4. DATES OF VISIT: / / TO / / (/ / TO / /)</td></tr>
<tr><td colspan="3">5 TYPE OF VISIT: (SELECT ONE FROM EACH COLUMN)</td></tr>
<tr><td>[ ] GOVERNMENT INTITIATIVE</td><td colspan="2">[ ] INITIATED BY REQUESTING AGENCY OR FACILITY</td></tr>
<tr><td>[ ] COMMERCIAL INITIATIVE</td><td colspan="2">[ ] BY INVITIATION OF THE FACILITY TO BE VISITED</td></tr>
</table>

6. SUBJECT TO BE DISCUSSED/JUSTIFICATION:		
7. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED		
8. IS THE VISIT PERTINENT TO:		SPECIFY
Specific equipment or weapon system	[ ]	
Foreign military sales or export license	[ ]	
A Program or Agreement	[ ]	
A defense acquisition process	[ ]	
Other	[ ]	
9. PARTICULARS OF VISITORS		
NAME		
DATE OF BIRTH; / /		PLACE OF BIRTH
SECURITY CLEARANCE:		ID/PP NR:
POSITION		NATIONALITY
COMPANY/AGENCY		
NAME		
DATE OF BIRTH; / /		PLACE OF BIRTH
SECURITY CLEARANCE:		ID/PP NR:
POSITION		NATIONALITY
COMPANY/AGENCY		
10. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY		
NAME:		TELEPHONE/FAX NRS. E-MAIL-ADDRESS (when known):
SIGNATURE:		
11. CERTIFICATON OF SECURITY CLEARANCE (only if information or areas classified CONFIDENTIAL or above will be involved unless required by bilateral agreements)		

NAME:
ADDRESS: STAMP
SIGNATURE:
12. REQUESTING NATIONAL SECURITY AUTHORITY:
NAME:
ADDRESS: STAMP
SIGNATURE:
13. REMARKS:

ANNEX C

(To be used with Alternative B: Streamlined Procedures)

[INSERT NAME OF PROGRAME]

REQUEST FOR VISIT

** To be completed in the English language*

[ ] One-time
[ ] Recurring
[ ] More than 21 days

REQUESTING ESTABLISHMENT/COMPANY/AGENCY:

Name:

Address:

Security Officer:

Telephone/Fax/E-mail: **Point of contact:**

ESTABLISHMENT/COMPANY/AGENCY TO BE VISITED

Name:

Address:

Security Officer:

Telephone/Fax/E-mail: **Point of contact:**

DATE OF VISIT:

From: to:

SUBJECT TO BE DISCUSSED:

Project/Contract/Program:

Anticipated Level of Discussions □ C □ S

VISITOR DETAILS

Name: **Passport Nº:**

Date of Birth: **Nationality:**

Security Clearance level: **Expiry Date:** **Rank/Grade:**

Company/Agency: **Position:**

Continue on additional sheets for extra visitors.

Signature: _____Date: _____

ANNEX D

PROTECTION OF INFORMATION HANDLED IN IT AND COMMUNICATION SYSTEMS

Systems handling CONFIDENTIAL information and above require security measures to protect confidentiality, integrity and availability of the information they contain. The security measures needed to meet requirements as laid down in this Document will be determined by the designated Security Accreditation Authority (SAA) and will be commensurate with the assessed risk and consistent with the policy stated in this Document.

Section I - INTRODUCTION

SECURITY MEASURES

1. The main purpose of the security measures stated in this Document is to provide requirements for protection against unauthorised disclosure of information (the loss of confidentiality). Loss of integrity and availability of information is in this context regarded as important only as far as this, in turn, would lead to loss of confidentiality.

SYSTEM-SPECIFIC SECURITY REQUIREMENT STATEMENT (SSRS)

2. For all SYSTEMS handling Classified Information, a SYSTEM-Specific Security Requirement Statement (SSRS) shall be required to be produced by the System Operational Authority (SOA) in co-operation with input and assistance as required from the project staff and INFOSEC Authority, and approved by the SAA.

3. The SSRS shall form the binding agreement between the System operational authority and the SAA against which the SYSTEM is to be accredited.

4. All SYSTEMS handling Classified Information shall be accredited.

Section II - SECURITY RESPONSIBILITIES

SECURITY ACCREDITATION AUTHORITY (SAA)

5. The SAA shall be either:
   - a National Security Authority (NSA),
   - a Designated Security Authority (DSA). This authority is designated by the Member States
     depending on the SYSTEM to be accredited.

6. The SAA shall be responsible for ensuring the compliance of SYSTEMS with security policy. One of its tasks shall be to grant the approval of a SYSTEM to handle Classified Information to a defined level of classification in its operational environment.

SYSTEM OPERATIONAL AUTHORITY (SOA)

7. An SOA shall be responsible for the implementation and operation of controls and special security features for each SYSTEM. This responsibility shall extend throughout the life cycle of the SYSTEM from the project concept stage to final disposal.

8. The SOA shall be responsible for all security measures designed as part of the SYSTEM. This responsibility includes the preparation of the SSRS and the Security Operating Procedures (SecOPs).

9. The SOA may delegate a part of its responsibilities where appropriate to, for instance the INFOSEC security officer and the INFOSEC site security officer. The various INFOSEC functions may be performed by a single person.

INFOSEC AUTHORITY (IA)

10. The SOA can appoint an INFOSEC Authority (IA) to assist in daily business. The IA will act as direct representative of the SAA. As a minimum the IA will be responsible for following INFOSEC office activities:
    - providing technical advice and assistance to the SAA
    - assisting in the development of the SSRS
    - reviewing the SSRS to ensure consistency with the present Council Security Regulations and the INFOSEC policies and architecture Documents
    - participating in the accreditation panels/boards as required and providing INFOSEC recommendation on accreditation to the SAA
    - providing support to the INFOSEC training and education activities
    - providing technical advice in investigation of INFOSEC related incidents
    - establish technical policy guidance to ensure that only authorised software is used.

USERS

11. All users shall be responsible for ensuring that their actions do not adversely affect the security of the SYSTEM that they are using. Furthermore users are required to report unusual incidents or prospective vulnerabilities to the IT SOA.

INFOSEC TRAINING

12. INFOSEC education and training shall be available at various levels, and for various personnel, as appropriate.

Section III - NON TECHNICAL SECURITY MEASURES

PERSONNEL SECURITY

13. Users of the SYSTEM shall be cleared and have a need-to-know, as appropriate for the classification and content of the information handled within their particular SYSTEM. Access to certain equipment (e.g. cryptographic) or information specific to security of SYSTEMS will call for special clearance issued by the relevant NSA/DSA.

14. The SAA shall designate all sensitive positions and specify the level of clearance and supervision required by all personnel occupying them.

15. In general, as far as possible, SYSTEMS shall be specified and designed in a way that facilitates the allocation of duties and responsibilities to personnel. The intent is to prevent one person having complete knowledge or control of the system security keys points. The aim should be that collusion between two or more individuals would be necessary for alteration or intentional degradation of the system or network to take place. This can be achieved applying procedural measures. For SYSTEMS intended for processing SECRET and higher information or systems processing SPECIAL CATEGORY information, it will be mandatory to have such procedures in place.

PHYSICAL SECURITY

16. IT and Remote Terminal/Workstation Areas in which Classified Information is handled by IT means, or where potential Access to such information is possible, shall be established in a secure area approved by the appropriate security authority.

CONTROL OF ACCESS TO A SYSTEM

17. All information and materiel which allow access control to a SYSTEM shall be protected under arrangements commensurate with the highest classification and the category designation of the information to which it may give access.

Section IV - TECHNICAL SECURITY MEASURES

SECURITY OF INFORMATION

18. It shall be incumbent upon the originator of the information to identify and classify all information-bearing Documents, whether they are in the form of hard-copy output or computer storage media. Each page of hard-copy output shall be marked, at the top and bottom, with the classification. Output, whether it is the form of hard-copy or computer storage media shall have the same classification as the highest classification of the information used for its production. The way in which a SYSTEM is operated may also impact on the classification of outputs of that system.

19. It shall be incumbent upon an organisation and its information holders to consider the problems of aggregation of individual elements of information, and the inferences that can be gained from the related elements, and determine whether or not a higher classification is appropriate to the totality of the information.

20. The fact that the information may be a brevity code, transmission code or in any form of binary representation does not provide any security protection and should not, therefore, influence the classification of the information.

21. When information is transferred from one SYSTEM to another the information shall be protected during transfer and in the receiving SYSTEM in the manner commensurate with the original classification and category of the information.

22. All computer storage media shall be handled in a manner commensurate with the highest classification of the stored information or the classification identified on the media label, and at all times shall be appropriately protected.

23. Re-usable computer storage media used for recording Classified Information shall retain the highest classification for which they have ever been used until that information has been properly downgraded or declassified and the media reclassified accordingly, or the media declassified or destroyed by an approved national procedure.

CONTROL AND ACCOUNTABILITY OF INFORMATION

24. The SYSTEM shall have an automated and / or manual mechanism to enable investigation of system and user activity. This mechanism will provide logging information with the possibility to indicate user or system identification, date and time of activity and executed activity. Depending on the level of classification of the SYSTEM, following activities will be logged:
    - ALL CLASSIFICATION LEVELS: access to the SYSTEM and activities to alter user rights,
      including unsuccessful attempts
    - CONFIDENTIAL and above : access to Classified Information (files)
    - SECRET and above : alterations to content of Classified Information (files).

25. Access and manipulation related data shall be retained for 18 months as a minimum. After that time they will be destroyed in accordance with national rules for the classification of the system.

26. Classified outputs held within the secure area may be handled as one classified item and need not be registered, provided the materiel is identified, marked with its classification and controlled in an appropriate manner.

27. Where output is generated from a SYSTEM handling Classified Information, and transmitted to a remote terminal/workstation area from an IT area, procedures, agreed by the SAA shall be established for controlling the remote output. For SECRET and above, such procedures shall include specific instructions for accountability of the information.

HANDLING AND CONTROL OF REMOVABLE COMPUTER STORAGE MEDIA

28. All classified removable computer storage media shall be handled as classified materiel. Appropriate identification and classification markings need to be adapted to the specific physical appearances of the media, to enable it to be clearly recognised.

29. Users shall take the responsibility for ensuring that Classified Information is stored on media with the appropriate classification marking and protection. Procedures shall be established to ensure that, for all levels of information, the storage of information on computer storage media is being carried out in accordance with the security regulations.

DECLASSIFICATION AND DESTRUCTION OF COMPUTER STORAGE MEDIA

30. Computer storage media used for recording Classified Information may be downgraded or declassified if approved by appropriate security authority and/or national procedures are applied.

31. Computer storage media, which has held TOP SECRET or special category information, shall not be declassified and reused.

32. If computer storage media cannot be declassified or is not reusable, it shall be destroyed by a procedure approved by the SAA.

COMMUNICATIONS SECURITY

33. When Classified Information is transmitted electromagnetically, special measures shall be implemented to protect the confidentiality of such transmissions. The appropriate security authority shall determine the requirements for protecting transmissions from detection, interception or exploitation. The information being transmitted in a communication system shall be protected based upon the requirements for confidentiality.

34. Classified Information shall not be transmitted in clear text. Only cryptographic systems approved by the NSA/DSA concerned shall be used for the encryption of Classified Information, irrespective of the method of transmission.

35. However, under exceptional circumstances, information classified RESTRICTED, CONFIDENTIAL and SECRET may be transmitted in clear text provided each occasion is explicitly authorised by the relevant NSA/DSA.

INSTALLATION AND EMISSION SECURITY

36. All equipment shall be installed in accordance with current national security policy.

37. Security measures shall be implemented to protect against the Compromise of Classified Information through unintentional electromagnetic emissions. The measures shall be commensurate with the risk of exploitation and the sensitivity of the information.

Section V - SECURITY DURING HANDLING

SECURITY OPERATING PROCEDURES

38. Security Operating Procedures (SecOPs) define the principles to be adopted on security matters, the operating procedures to be followed, and personnel responsibilities. The SecOPs shall be prepared under the responsibility of the System Operational Authority.

SOFTWARE PROTECTION/CONFIGURATION MANAGEMENT

39. The software versions in use should be verified at regular intervals to ensure their integrity and correct functioning.

40. New or modified versions of software should not be used for the handling of Classified Information until authorised by the System Operational Authority.

CHECKING FOR THE PRESENCE OF MALICIOUS SOFTWARE/COMPUTER VIRUSES

41. Checking for the presence of malicious software/computer viruses shall be periodically carried out in accordance with the requirements of the SAA.

42. All computer storage media should be checked for the presence of any malicious software or computer viruses, before being introduced to any SYSTEM.

MAINTENANCE

43. Contracts and procedures for scheduled and on-call maintenance of SYSTEMS for which a SSRS has been produced shall specify requirements and arrangements for maintenance personnel and their associated equipment entering an IT area.

44. The requirements shall be clearly stated in the SSRS and the procedures shall be clearly stated in the SecOPs. Contractor maintenance requiring remote access diagnostic procedures shall be permitted only in exceptional circumstances, under stringent security control, and only with the approval of the SAA

SECURITY ADMINISTRATION

45. The security settings of SYSTEMS shall only be changed with approval of the SOA. For SYSTEMS intended for processing SECRET or higher information or for systems processing SPECIAL CATEGORY information, it will be mandatory to have written approval of the SOA prior to making such changes.

46. Alterations to security settings of SYSTEMS shall be reviewed by the SOA using log file information.

Section VI - ACCREDITATION

INTRODUCTION

47. All SYSTEMS handling information classified CONFIDENTIAL and above shall be accredited prior to processing such information. Accreditation is the authorisation and approval granted to a SYSTEM to process Classified Information in its specified operational environment. Such accreditation should be made after all appropriate security procedures have been implemented and a sufficient level of protection of the system resources has been achieved.

48. The SAA will base accreditation upon information provided in the SSRS, Security Operating Procedures (SecOPs) and any other relevant Documentation. Sub-systems and remote terminals/workstations shall be accredited as part of all SYSTEMS to which they are connected. Where a SYSTEM supports other organisations, the relevant Security Authorities shall mutually agree on the accreditation.

49. The accreditation process may be carried out in accordance with an accreditation strategy appropriate to the particular SYSTEM and defined by the SAA.

EVALUATION AND CERTIFICATION

50. The hardware, firmware and software security features of such SYSTEM shall be evaluated and certified as being capable of safeguarding information at the intended level of classification.

51. The requirements for evaluation and certification shall be included in system planning, and clearly stated in the SSRS.

52. The evaluation and certification process shall be carried out in accordance with commonly accepted guidelines and by technically qualified and appropriately cleared personnel acting on behalf of the SAA.

53. The teams may be provided from a nominated Member State's evaluation or certification authority or its nominated representatives, for example a competent and cleared Contractor.

54. The degree of evaluation and certification processes involved may be lessened (for example, only involving integration aspects) where SYSTEMS are based on existing nationally evaluated and certified computer security products.

ROUTINE CHECKING OF SECURITY FEATURES FOR CONTINUED ACCREDITATION

55. The System operational authority shall establish routine control procedures, which shall ensure that all security features of the SYSTEM are still valid.

56. The types of change that would give rise to re-accreditation, or the types of change that require the prior approval of the SAA, shall be clearly identified and stated in the SSRS. After any modification, repair or failure, which could have affected the security features of the SYSTEM, the System Operational Authority shall ensure that a check is made to ensure the correct operation of the security features. Continued accreditation of the SYSTEM shall normally depend on the satisfactory completion of the checks.

57. All SYSTEMS where security features have been implemented shall be inspected or reviewed on a periodic basis by the SAA. In respect of SYSTEMS handling TOP SECRET or special category information the inspections shall be carried out not less than once annually.

Section VII - COMPUTER EQUIPMENT

SECURITY OF MICROCOMPUTERS/PERSONAL COMPUTERS

58. Microcomputers/Personal Computers (PCs) with fixed disks (or other non-volatile storage media), operating either in stand-alone mode or as networked configurations, and portable computing devices (for example, portable PCs and electronic "notebooks") with fixed hard disks, shall be considered as information storage media in the same sense as floppy diskettes or other removable computer storage media.

59. This equipment shall be afforded the level of protection, in terms of access, handling, storage and transportation, commensurate with the highest classification level of information ever stored or processed (until downgraded or declassified in accordance with approved procedures).

USE OF PRIVATELY-OWNED IT EQUIPMENT FOR OFFICIAL WORK

60. The use of privately-owned removable computer storage media, software and IT hardware (for example, PCs and portable computing devices) with storage capability shall be prohibited for handling Classified Information.

61. Privately owned hardware, software and media shall not be brought into any area where Classified Information is handled without the permission of the Head of the Security Office or of a Member State's Department.

USE OF CONTRACTOR-OWNED OR NATIONALLY-SUPPLIED IT EQUIPMENT FOR OFFICIAL WORK

62. The use of Contractor-owned IT equipment and software in organisations in support of official work may be permitted by the Head of the Security Office or of a Member State's Department. The use of nationally-provided IT equipment and software may also be permitted. In this case, the IT equipment shall be brought under the control of the appropriate inventory. In either case, if the IT equipment is to be used for handling Classified Information, then the appropriate SAA shall be consulted in order that the elements of INFOSEC that are applicable to the use of that equipment are properly considered and implemented.

PLANNING THE LIFECYCLE

63. Hardware or software should be procured after approval by the SAA.
In deciding whether equipment, particularly computer storage media, should be leased rather than purchased, it should be borne in mind that such equipment, once used for handling Classified Information, cannot be released outside an appropriately secure environment without first being declassified to the approval of the SAA and that such approval may not always be possible.

ANNEX A - DEFINITIONS

CERTIFICATION shall mean: The issue of a formal statement, supported by an independent review of the conduct and results of an evaluation, of the extent to which a SYSTEM meets the security requirement, or a computer security product meets pre-defined security claims.

COMMUNICATION CONTROLS incorporate boundary protection devices such as firewalls, intrusion detection systems, sandboxes, honey pots etc. intended to prevent unauthorised intrusion into the IT system.

COMPUTER SECURITY PRODUCT shall mean: A generic computer security item which is intended for incorporation into an IT system for use in enhancing, or providing for, confidentiality, integrity or availability of information handled.

EVALUATION shall mean: The detailed examination, by an appropriate authority, of the security aspects, technical and non-technical, of a SYSTEM or of a cryptographic or a computer security product.

Notes: (1) The evaluation investigates the presence of required security functionality and the absence of compromising side-effects from such functionality and assesses the incorruptibility of such functionality; and

(2) The evaluation determines the extent to which the security requirements of a SYSTEM, or the security claims of a computer security product, are satisfied and establishes the assurance level of the SYSTEM or of the cryptographic, or the computer security product's trusted function.

INFORMATION SECURITY (INFOSEC) shall mean: The application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity and availability of the systems themselves. INFOSEC measures include those of computer, transmission, emission and cryptographic security, and the detection, Documentation and countering of threats to information and to the SYSTEMS.

IT AREA shall mean: An area that contains one or more computers, their local peripheral and storage units, control units and dedicated network and communications equipment.

Note: This does not include a separate area in which remote peripheral devices or terminals/workstations are located even though those devices are connected to equipment in the IT area.

IT NETWORK shall mean: Organisation, geographically disseminated, of IT systems interconnected to exchange data, and comprising the components of the interconnected IT systems and their interface with the supporting data or communications networks.

Notes: (1) An IT network can use services of one or several communications networks interconnected to exchange data; several IT networks can use the services of a common communications network.

(2) An IT network is called “local” if it links several computers together in the same site.

IT NETWORK SECURITY FEATURES include the IT system security features of individual IT systems comprising the network together with those additional components and features associated with the network as such (for example, network communications, security identification and labelling mechanisms and procedures, access controls, programs and audit trails) needed to provide an acceptable level of protection for Classified Information.

IT SYSTEM shall mean: Assembly of equipment, methods and procedures, and if necessary, personnel, organised to accomplish information processing functions.
Notes: (1) This is taken to mean an assembly of facilities, configured for handling information within the system;

(2) Such systems may be in support of consultation, command, control, communications, scientific or administrative applications including word processing;

(3) The boundaries of a system will generally be determined as being the elements under the control of a single System Operational Authority; and

(4) An IT system may contain subsystems some of which are themselves IT systems.

IT SYSTEM SECURITY FEATURES comprise all hardware/firmware/software functions, characteristics, and features; operating procedures, accountability procedures, and access controls, the IT area, remote terminal/workstation area, and the management constraints, physical structure and devices, personnel and communications controls needed to provide an acceptable level of protection for Classified Information to be handled in an IT system.

REMOTE TERMINAL / WORKSTATION AREA shall mean: An area containing some computer equipment, its local peripheral devices or terminals/workstations and any associated communications equipment, separate from an IT area.

SPECIAL CATEGORY: Additional markings such as CRYPTO or any other special handling designator, shall apply where there is a need for limited distribution and special handling in addition to that designated by the security classification.

SSRS shall mean: SYSTEM-Specific Security Requirement Statement. It will contain as a minimum:

a) A statement of the objective of accreditation for the system; in particular, what classification level(s) of information are to be handled and what system or network security mode(s) of operation is being proposed;

b) Production of a risk management review to identify the threats and vulnerabilities and measures to counter them;

c) The Security Operating Procedures (SecOPs) with a detailed description of the proposed operations (e.g., modes, services, to be provided) and including a description of the SYSTEM security features which shall form the basis of accreditation;

d) The plan for the implementation and maintenance of the security features;

e) The plan for initial and follow-on system security or network security test, evaluation and certification; and

f) Certification, where required, together with other elements of accreditation.

TEMPEST countermeasures: security measures intended to protect equipment and communication infrastructures against the Compromise of Classified Information through unintentional electromagnetic emissions.

ANNEX K

ABBREVIATIONS AND ACRONYMS

AIS	Automated Information System
CSA	Cognizant Security Agency
CUI	Controlled Unclassified Information
DGR	Designated Government Representative
DSA	Designated Security Authority
FIS	Facility Security clearance Information Sheet
FSC	Facility Security Clearance
FSO	Facility Security Officer
IA	INFOSEC Authority
INFOSEC	Information Security
IT	Information Technology
ITT	Invitation to Tender
JPO	Joint Project/Program Office
MOU/A	Memorandum of Understanding/Agreement
NATO	North Atlantic Treaty Organization
NSA	National Security Authority
PC	Personal Computer/Microcomputer
PSC	Personnel Security Clearance
PSCC	Personnel Security Clearance Confirmation Sheet
PSI	Program/Project Security Instruction
RFP	Request for Proposal
RVA	Request for Visit Authorization

SAA	Security Accreditation Authority
SCG	Security Classification Guide
SecOPs	Security Operating Procedures
SOA	System Operational Authority
SSRS	System-Specific Security Requirement Statement