PROGRAMME SECURITY INSTRUCTION CONCERNING

GOVSATCOM component of the Union Space Programme

(SHORT TITLE: GOVSATCOM PSI*)*

issued by

European Commission

Version 1.0

Dated

19 October 2022

Participants to the GOVSATCOM component of the EU Space Programme

EU MEMBER STATES

EU COUNCIL

EUROPEAN COMMISSION

EUROPEAN EXTERNAL ACTION SERVICE

EUROPEAN UNION AGENCY FOR THE SPACE PROGRAMME (EUSPA)

EUROPEAN SPACE AGENCY (ESA)

Version history

VERSION	REFERENCE	DATE	COMMENTS
1.0	Approved	19/10/2022	

Table of Contents

Section 1 - Introduction

1.1 Scope and purpose

1. This Programme Security Instruction (PSI) establishes the security procedures to be applied and the common security procedures and processes to be followed for the management of classified contracts awarded under the GOVSATCOM component of the Union Space Programme, and assigns the responsibilities for the protection of classified information generated or exchanged in connection with GOVSATCOM.

2. This PSI provides instructions on: the classification and marking of Classified Foreground Information; protective security procedures, including the handling and transfer of classified information; visit procedures to be followed when classified information is accessed; measures to be taken in the event of a security breach or compromise involving classified information; procedures to be followed for releasing classified information and procedures to be followed when contracting and sub-contracting.

3. The protection of COMSEC Items is covered by Annex H. This document will be provided to Contractors by the Contracting Authority on a need-to-know-basis.

4. Within the scope of the GOVSATCOM component of the Union Space Programme, this PSI repeals and replaces the 'GOVSATCOM Hub Project Security Instruction' (ref GSA-SEC-SREQ-REQ-A07043 Issue/Version: 0.32), in accordance with the terms and conditions of the existing contracts.

Section 2 - Glossary

For the purpose of this PSI, the following terminology is used:

CLASSIFIED BACKGROUND INFORMATION means any classified information which has been generated outside GOVSATCOM and is provided to and used for the purposes of GOVSATCOM.

CLASSIFIED CONTRACT is a framework contract or contract entered into for the supply of movable or immovable assets, execution of works or provision of services by a Contractor, the performance of which requires or involves access to, storage or creation of classified information.

CLASSIFIED FOREGROUND INFORMATION is classified information generated in the implementation of GOVSATCOM and marked with an EU classification marking, as defined in this PSI, and supplemented by any relevant releasability statement.

CLASSIFIED INFORMATION means any information or material designated by a security classification, the unauthorised disclosure or loss of which could cause varying degrees of prejudice to the interests of one or more of the Participants or of the Union as a whole or any other State or international organisation, and which is identified as such by an appropriate security classification marking.

CLASSIFIED SUB-CONTRACT is a sub-contract entered into by a Contractor with a Sub-Contractor for the supply of movable or immovable assets, execution of works or provision of services, the performance of which requires or involves access to, creation, handling or storing of classified information.

COMMISSION SECURITY AUTHORITY is a European Commission authority set up within the Directorate-General Human Resources and Security with responsibilities assigned to it by the Commission Decision on the security rules for protecting EU classified information in the Commission.

COMMUNICATION AND INFORMATION SYSTEM (CIS) is any system enabling the handling of information in electronic form. A CIS shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources.

COMPROMISE of classified information denotes a situation when - due to a security breach or adverse activity (such as espionage, acts of terrorism, sabotage or theft) – 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 unauthorised individuals (e.g. through espionage or to the media), unauthorised modification, destruction in an unauthorised manner, or denial of service.

COMSEC (Communication Security) means the application of security measures to telecommunications in any form in order to deny unauthorised persons to access information of value derived from the possession and study of such telecommunications or to ensure the confidentiality, availability, authenticity, nonrepudiation and integrity of such telecommunications. Such measures include crypto, transmission and emission

(TEMPEST) security, as well as procedural, physical, personnel, document and computer security.

COMSEC ITEM means all material, including keys in all forms, such as documents, devices or equipment, that describe, contain or relate to cryptographic products and is essential to the encryption, decryption or authentication of telecommunications and any other item that performs critical COMSEC functions.

CONSORTIUM, with reference to Part I, Title VIII of Regulation (EU, Euratom) No 2018/1046, means a collaborative grouping of ***Undertakings*** constituted to perform a contract under GOVSATCOM.

CONSORTIUM SECURITY OFFICER (CSO) is a person nominated within the consortium to coordinate and promote actions so that the contractors of that consortium ensure application of the rules on the handling of EU classified information and of the applicable security procedures.

CONTRACTING AUTHORITY is the European Commission or the European Space Agency (ESA) or the European Union Agency for the Space Programme (EUSPA) within the remit of their specific competencies, tasks or delegated responsibilities. Where the European Commission is Contracting Authority, ESA or EUSPA has been entrusted to carry out procurement actions and manage the ensuing contracts. As such, for these contracts, ESA or EUSPA shall be understood as performing all the functions attributed to the Contracting Authority in the text of this PSI.

CONTRACTOR is an economic operator with whom a GOVSATCOM contract has been signed.

COURIER is a government or other Participant entity representative or staff member, or a Contractor's employee who has been appropriately cleared and authorised to hand carry classified material to its destination.

DESIGNATED SECURITY AUTHORITY (DSA) is a state authority responsible to the National Security Authority (NSA) of a Participant which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority in that Participant State.

DOCUMENT means any recorded information regardless of its physical form or characteristics.

ELECTRONIC TRANSMISSION means the sending of the GOVSATCOM information from one place to another by electronic means.

EU CLASSIFIED INFORMATION (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

FACILITY SECURITY CLEARANCE (FSC) means an administrative determination by an NSA, DSA or other competent Security Authority that a facility can afford an adequate level of protection to classified information to a specified security classification level.

GOVSATCOM PARTICIPANTS are the EU Member States, EU bodies and other States and organisations participating in the GOVSATCOM component. In the meaning of this definition, Contractors and Sub-Contractors are not considered Participants.

GOVERNMENT-TO-GOVERNMENT CHANNELS are transfers of classified information via diplomatic pouch or through other channels approved by the Security Authorities involved.

NATIONAL SECURITY AUTHORITY (NSA) is a Government authority with ultimate responsibility for the security of classified information in that country.

NEED-TO-KNOW is the principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to accomplish a designated and approved function relating to GOVSATCOM.

ORIGINATOR of Classified Background Information means a State or an international organisation under whose authority classified information has been created and/or introduced into GOVSATCOM.

ORIGINATOR of GOVSATCOM Classified Foreground Information is the European Commission, no matter who is the Contracting Authority in GOVSATCOM contracts. *(Whilst Contractors or Sub-Contractors can create EU classified information under contracts relating to GOVSATCOM, they are not considered Originators for the purposes of this PSI).*

PERSONNEL SECURITY CLEARANCE or PERSONNEL SECURITY CLEARANCE CERTIFICATE (PSC or PSCC), as applicable, means a statement by a competent authority of a Participant State made following completion of a security investigation conducted by a competent authority of a Participant State and which certifies that an individual is cleared to have access to classified information up to the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above until a specific date.

PSI CUSTODIAN is appointed by the European Commission and is responsible for the control of this PSI, including annexes, and for ensuring the correct issuing and version control.

RELEASE is the passing of GOVSATCOM Information, by any means of communication, to the State or international organisation that is not a Participant to GOVSATCOM.

SECURED AREA is a physically protected area with a visibly defined and protected perimeter through which all entry and exit is controlled by means of a pass or personal recognition system, where unescorted access is contracted only to individuals who are security cleared and are specifically authorised to enter the area on the basis of their need-to-know, and where all other individuals are escorted at all times or are subject to equivalent controls.

SECURITY ASPECTS LETTER (SAL) is a set of special contractual conditions issued by the Contracting Authority, which forms an integral part of any classified contract or classified sub-contract, that identifies the security requirements or those elements of the contract requiring security protection.

SECURITY AUTHORITY is the NSA, DSA or other authority which is responsible for the maintenance of standards for the security of classified information within a State or an organisation.

SECURITY BREACH occurs as result of an act or omission which is contrary to the security provisions set out in this PSI or in any other applicable laws, rules or regulations.

SECURITY CLASSIFICATION GUIDE (SCG) is a document which describes the elements of GOVSATCOM, a project or contract which are classified, specifying the applicable security classification levels. The SCG issued to Contractors may be modified throughout the life of GOVSATCOM or contract, and the classified elements may be re-classified or downgraded**.** The SCG also includes, if applicable, an informative list of Classified Background Information used in the performance of the contract.

SECURITY OFFICER is a person, having the appropriate security expertise, designated by the management to be responsible for the proper implementation of security-related decisions and for the coordination of available security resources and measures within a facility involved in the classified parts of GOVSATCOM, as well as to be the technical advisor to management on security matters related to GOVSATCOM.

SUB-CONTRACTOR means an economic operator, including public entities, that is proposed by a contractor to perform part of the tasks co-financed by a GOVSATCOM contract.

Section 3 – PSI applicability and the security responsibilities of Participants

3.1 Applicability

1. This PSI applies to any Contractor or Sub-Contractor that will access or create classified information under GOVSATCOM. The latest approved version of this PSI and its annexes will be referenced to in the Security Aspects Letter of a contract or sub-contract and, as such, is applicable to Contractors or Sub-Contractors on a contractual basis.

2. The provisions of this PSI do not put any legal obligations either on the Security Authorities of the Participants or on the Security Authorities of non-EU Member States on whose territory Sub-Contractors may be located. The responsibilities of the Security Authorities from non-Participating non-EU Member States regarding the handling of EU classified information by Sub-Contractors on their territory are covered by the relevant security agreement or arrangement in place between the EU and that non-EU Member State.

3. Questions concerning the content and interpretation of this PSI, and any proposed changes, shall be addressed to the European Commission, which will consult the Contracting Authority and the Participants' Security Authorities if required.

4. Nothing in this PSI shall cause prejudice to the national or EU laws and regulations of Participants regarding public access to documents.

5. This PSI has been endorsed by the security authorities of the Participants. It may be reviewed or updated following changes to applicable security regulations or on request of a Programme Participant.

3.2 Responsibilities

3.2.1 Security Authorities

1. In accordance with national rules, the Security Authorities of Contractors or Sub-Contractors under their jurisdiction are responsible for:

    a. Monitoring the implementation of the provisions of this PSI within their establishments, and by Contractors or Sub-Contractors under their jurisdiction;

    b. Conducting the Facility Security Clearance (FSC) process for Contractors or Sub-Contractors that are required to handle and/or store classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above at their facility;

    c. Upon request, and where classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above is involved, responding to FSC Information Sheet (FSCIS) requests from another Security Authority or Contracting Authority;

d. Conducting the Personnel Security Clearance (PSC) process on the personnel handling classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above.

2. The Security Authorities of all Participants are responsible for:

   a. Upon request, and where classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above is involved, responding to PSC Information Sheet (PSCIS) queries submitted by another Security Authority;

   b. Submitting and/or approving Transportation Plans, Courier Certificates, international visit requests (i.e. Request for Visit), etc. in accordance with the provisions of this PSI;

   c. Informing the Originator's competent Security Authority and, where EU Classified information is concerned, the Commission Security Authority, identified in Annex A, about any security breach, which may have led to a loss or compromise of classified information;

   d. Investigating all cases in which it is known, or where there are grounds for suspecting that a compromise of classified information provided or generated pursuant to GOVSATCOM has occurred;

   e. Ensuring, in liaison with the PSI custodian, that their details in Annex A are up to date.

3.2.2 Contracting Authorities

1. The Contracting Authority for GOVSATCOM shall notify the relevant Security Authority of the Contractor or Sub-Contractor of any signed classified contract or sub-contract together with their end-date, the level of classified information to be used, and whether and at what level a capability to store and/or handle EUCI on a CIS is necessary. The Contracting Authority shall also provide a copy of the relevant parts of the classified contract or sub-contract (the Security Aspects Letter) to the Security Authority of the Participant in order to facilitate their security monitoring of the contract or sub-contract.

2. The Contracting Authorities shall distribute the latest issue of this PSI to their Contractors and the NSAs/DSAs involved.

3. The Contracting Authority is responsible for providing to the NSAs/DSAs involved the updated details of their Contractors or of the Sub-Contractors under sub-contracts with their Contractors.

3.2.3 Contractors or Sub-Contractors

1. A Consortium Security Officer (CSO) shall be nominated within the consortium to coordinate and promote actions in ensuring that the rules on the handling of classified information and the applicable security procedures are respected by the Contractors of that

consortium. Within the consortium the CSO shall normally be the first point of contact for the Contracting authority on security matters.

2. Contractors or Sub-Contractors are responsible for the implementation of this PSI within their facilities, in particular for ensuring that:

   a. The provisions of the latest version of this PSI are implemented;

   b. Classified information and COMSEC Items generated by the Contractor or Sub-Contractor, or entrusted to them, are appropriately safeguarded;

   c. A Security Officer is appointed who is responsible for supervising and directing security measures in relation to the GOVSATCOM contract. This individual shall be responsible for limiting access to classified information involved in the classified contract or sub-contract to those employees who have been briefed, authorised for access, have a Need-to-Know and (for access to classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above) have been granted a PSC at the appropriate level;

   d. Any Classified Foreground Information generated by the Contractor or Sub-Contractor is classified in accordance with this PSI and the relevant Security Classification Guide (SCG);

   e. The security classifications of Classified Background Information are retained and not changed without the prior written consent of the Originator;

   f. Classified information is only provided to individuals who have a Need-to-Know and an appropriate PSC, if required;

   g. Classified information (at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) is provided only to Contractor or Sub-Contractor facilities that have been granted an FSC. Prior to providing classified information to another Contractor or Sub-Contractor, the FSC status of that Contractor or Sub-Contractor shall be established, in liaison with the relevant NSAs/DSAs;

   h. Classified Information related to GOVSATCOM is not released to entities other than the GOVSATCOM Participants and their Contractors or Sub-Contractors without the appropriate release procedures of this PSI having been followed;

   i. Classified Foreground Information is not used for purposes other than GOVSATCOM, unless the prior written consent of the Originator has been obtained through the Contracting Authority;

   j. The relevant security provisions of this PSI, as referred to in the Security Aspects Letter, or parts thereof, are included as part of any contractual arrangement with Sub-Contractors;

   k. Appropriate action is taken in the event of an incident which has resulted or may result in a compromise or loss of classified information;

   l. Their Security Authority is informed about any such incident as soon as possible;

m. The latest version of this PSI is forwarded to their Sub-Contractors.

Section 4 - Security instructions

4.1 Handling and protection of classified information related to GOVSATCOM contracts

1. EU Classified Information, both Foreground and Background, that is provided to or generated by Contractors or Sub-Contractors in connection with GOVSATCOM shall be handled and protected in accordance with this PSI, which has been based on Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information and the Commission Decision (EU, Euratom) 2019/1963 laying down implementing rules on industrial security with regard to classified procurement contracts.

2. ESA, other International Organisations and non-EU States participating in GOVSATCOM will handle and protect EU Classified Information provided to them in accordance with the respective Security of Information Agreements they have concluded with the EU, and taking into account the supplementary provisions set out in this PSI.

3. Classified Background Information with a national classification marking or a classification marking of international organisation provided to or exchanged among Contractors or Sub-Contractors in connection with GOVSATCOM shall be handled and protected in accordance, respectively, with their applicable national laws and regulations or with the rules and regulations applicable to the international organisation under whose authority the classified information has been generated, in accordance with existing security agreements or arrangements. Annex B provides a table of equivalent security classification markings, for reference.

4. Classified information shall be upgraded, downgraded or declassified only with the consent of the Originator which shall be requested and obtained through the Contracting Authority.

5. For compilations of information (i.e. aggregation) protection measures of a higher classification level may be required. Such stronger protection measures shall be clearly documented in the Security Classification Guide (SCG).

4.2 Marking of Classified Foreground Information

4.2.1 Security classification markings

1. Classified Foreground Information shall be classified in accordance with the Security Classification Guide (SCG) applicable to GOVSATCOM. For contracts which are of limited scope, the relevant parts of the SCG may be extracted from the SCG and specific guidance on classification guidance may be provided in the respective SAL to the sub-contract.

2. Such Classified Foreground Information shall be marked with the appropriate EU classification marking: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET. For documents, the EU classification marking shall be written

a. In full in French and English (French first; not translated into other languages);

b. On one line, with no spaces either side of the forward slash;

c. Centred at the top and bottom of every page of the document;

d. When possible, the SECRET UE/EU SECRET marking shall appear in red.

3. A statement will be added directly underneath the classification marking identifying that the EU Classified Foreground Information is relating to GOVSATCOM. This indicates that this information must not be used for purposes other than those of GOVSATCOM.

   Example:

SECRET UE/EU SECRET

GOVSATCOM

4. For Classified Foreground Information not in the form of documents (e.g. electronic files and physical equipment/material), the EU classification marking shall be applied in such a way as to clearly identify the level of classification.

4.2.2 Declassification and downgrading of markings

1. If Classified Foreground Information needs to maintain its classification only for a defined period, it may be downgraded/declassified at that point by or on behalf of the Originator.

4.2.3 Releasability markings

1. Where the Originator has agreed to release Classified Information to a non-EU State or international organisation, subject to provisions under paragraphs 5.3 and 5.4, a statement on its releasability, shall be added underneath the classification marking as shown in this example:

SECRET UE/EU SECRET

GOVSATCOM
RELEASABLE TO [e.g. NORWAY, ESA, NATO, etc.]

4.2.4 Special category designators

1. In addition to any programme identifier markings or statements on releasability, it is allowed to add the special category designator 'CRYPTO'. This designator identifies that the Classified Information is cryptographic Item.

   Example:

> **SECRET UE/EU SECRET**
>
> GOVSATCOM
> RELEASABLE TO [e.g. NORWAY, ESA, NATO, etc.]
> CRYPTO

4.3 Security Classification Guide (SCG)

1. The SCG provides guidance on the items requiring a security classification as Classified Foreground Information generated in relation to GOVSATCOM. The SCG may also identify items requiring no classification or requiring their identification as relating to a special category (e.g. CRYPTO or CCI).

2. The classification levels assigned in the SCG are those anticipated for each item of listed information or equipment. Changes or questions concerning the interpretation of the SCG shall be addressed to the European Commission, which may consult with the Participants' competent authorities.

4.4 Specific procedures for the protection of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET classified information

4.4.1 Access

1. Access to and handling of classified information at these levels for the purposes of GOVSATCOM shall be limited to individuals having the appropriate level of PSC and a Need-to-Know.

2. When individuals are first granted access to classified information at these levels generated under GOVSATCOM, they must have been briefed by their Security Officer on the security requirements in this PSI. They shall acknowledge their responsibilities for protecting this

information in writing, and a record of this acknowledgement shall be retained by the Security Officer. Individuals required to access classified information at these levels shall be briefed at regular intervals by their Security Officer.

3. Security debriefings shall be given to personnel when they no longer require access to classified information at these levels. The debriefing shall consist of a reminder of the continuing responsibility to protect classified information and the possible penalties for failure to do so. Debriefing certificates may be used to record the debriefings and shall be retained by the Security Officers.

4.4.2 Handling and storage

1. Classified information at these levels shall only be handled and stored in Participants' establishments if they are authorised to handle and store that level of classified information in accordance with the applicable laws, rules or regulations of the Participant, and in the facilities of Contractors or Sub-Contractors that have been granted an appropriate FSC or other appropriate approval to handle and store classified information up to such level.

2. When created or received, documents or material classified at these levels shall be registered for purposes of accountability in dedicated registry or logbooks. For such purposes a classified registry shall be established, which shall be responsible for recording the life cycle of the classified information at these levels at the facility, including its dissemination and destruction. Registering of classified documents or material by electronic means shall be subject to the prior approval of the Security Authority.

3. Classified information at these levels shall only be worked on in a Secured Area approved in accordance with the applicable laws, rules and regulations of the Participant in a manner that prevents unauthorised access to the information, shall not be discussed or worked on in public (e.g. on public transport) and shall not be left unattended or handled in a manner that could result in unauthorised access.

4. Secured Areas that have been designated as 'Technically Secured Areas' by Security Authorities shall be equipped with Intruder Detection Systems (IDS), be locked when not occupied and be guarded when occupied. Any keys shall be controlled, all persons and material entering such areas shall be controlled. Such areas shall be regularly physically and/or technically inspected as required by the competent Security Authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such entry. Technically secured areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment.

5. When not in use, documents or other small items classified at these levels shall be stored in a secured container approved in accordance with the applicable laws, rules or regulations of the Participant. If the material is of such a size or format that it cannot be stored in a secured container, advice shall be sought from the relevant Security Authority as to how it should be protected.

6. The physical reproduction of classified information at these levels shall be limited to the minimum necessary to fulfil a particular action or function. Copies shall be made in a Secured Area using equipment approved in accordance with the applicable laws, rules or regulations of the Participant. The security measures applicable to the original document

shall also apply to any copies made. Copies shall be managed appropriately and securely destroyed when no longer required.

7. Translations of classified information at these levels shall only be undertaken by personnel holding an appropriate level of PSC. If a translation is created, it shall be marked as the original, be afforded the same level of protection as the original and be securely destroyed when no longer required.

8. When no longer required by the holder, classified information at these levels shall be destroyed in such a manner as to ensure that it cannot be reconstructed. The destruction shall be by a method that is in accordance with the applicable laws, rules, or regulations of the Participant. Such destruction shall be carried out by an individual and witnessed by another individual, both holding a PSC of an appropriate level. A destruction certificate shall be created and shall be recorded and filed in the registry/logbook. Destruction certificates are to be retained for 5 years by the establishment or facility where the destruction took place.

4.4.3 Information Assurance

1. Classified information at these levels shall be processed and stored electronically in CIS which have been appropriately accredited for the level of classification to be handled. The accreditation to be applied shall be in accordance with the applicable laws, rules or regulations of the Participant.

2. Classified information at these levels may be stored on removable or portable data storage media or devices. It shall be handled and protected to the same standards as documents containing the same level of classified information, if not encrypted with an approved encryption. Sub-section 4.7.4 provides further information on the procedures and considerations that apply for removable storage media.

3. CIS used within facilities located on the territory of one Participant and handling GOVSATCOM-related classified information will be accredited by the relevant Security Authority or competent Security Accreditation Authority (SAA), as appropriate, in accordance with the applicable laws, rules or regulations of the hosting Participant.

4. For security accreditation of CIS that handles GOVSATCOM-related classified information and whose components are under different jurisdictional domains (e.g. different SAAs), all concerned SAAs shall take part in the security accreditation process. In such case, the system-specific information assurance requirements and the accreditation process will be identified in dedicated security requirements documentation, which will be jointly approved by the SAAs involved.

5. Accredited portable computing devices not using approved encryption shall only be used or stored in an accredited Secured Area.

6. EUCI at this level that is transmitted electronically shall be protected by cryptographic products approved by the Council.

7. Interconnection of Contractor's or Sub-Contractor's CIS handling GOVSATCOM-related classified information to other Contractor's, Sub-Contractor's or Participant's CIS will be

jointly accredited by the respective Security Accreditation Authorities (SAAs). Appropriate security arrangements should be in place to ensure that the SAAs and the different CIS providers of the interconnected CIS are bound by relevant security requirements on the protection of GOVSATCOM-related classified information handled or exchanged via such CIS.

8. Areas in which CIS are installed or operated to display, store, process or transmit GOVSATCOM-related classified information will be established as Secured Areas. CIS areas housing servers, network management systems, network or communications controllers should be established as separate and controlled areas with an appropriate access control system. Access to these CIS areas should be limited to specifically authorised persons.

4.4.4 Tempest

1. Facilities that house CIS handling classified information at these levels shall be assessed by their Security Authority on the threat of compromise by unintentional electromagnetic emanations. TEMPEST security measures shall be commensurate with the risk of exploitation and the level of classification of the information.

4.5 Specific procedures for the protection of RESTREINT UE/EU RESTRICTED classified information

4.5.1 Access

1. Access to classified information at this level shall be limited to individuals who have an established Need-to-Know for the purpose of GOVSATCOM.

2. When individuals are first granted access to classified information of RESTREINT UE/EU RESTRICTED level generated under GOVSATCOM, they must have been briefed by their Security Officer on the security requirements in this PSI. They shall acknowledge their responsibilities for protecting this information in writing, and a record of this acknowledgement shall be retained by the Security Officer.

3. In principle, PSCs are not required for access to Classified Information at this level. Where Participant States require a PSC for contracts or sub-contracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, those national requirements shall not place any additional obligations on other Participant States or exclude tenderers, Contractors or Sub-Contractors from Participants that have no such PSC requirements for access to RESTREINT UE/EU RESTRICTED information from related contracts or sub-contracts.

4.5.2 Handling and storage

1. In principle, FSCs are not required for Contractors or Sub-Contractors handling and storing Classified Information at this level at their facility. Where Participant States require an FSC for contracts or sub-contracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, those national requirements shall not place any additional obligations on other Participant States or require an FSC from a Contractor or Sub-Contractor of another Participant that does not require an FSC at that level according to its applicable laws, rules or regulations.

2. There is no requirement to register classified information at this level in a dedicated classified registry or logbook unless required by a Participant State's applicable laws, rules or regulations.

3. Classified information at this level shall not be discussed or worked on in public (e.g. on public transport).

4. Classified information at this level shall not be left unattended or handled in a manner that could result in unauthorised access. As a general rule, when not in use, such information should be stored in locked desks, cabinets, or similar containers to which access is limited to persons having the required Need-to-Know. Classified information at this level may also be stored in the open in locked rooms, provided access to the room is restricted to persons who have a Need-to-Know.

5. The physical reproduction of classified information at this level shall be limited to the minimum necessary to fulfil a particular action or function. Copies shall be managed appropriately by the facility and securely destroyed when no longer required.

6. Translations of classified information at this level shall be marked as the original, be afforded the same level of protection as the original and be securely destroyed when no longer required.

7. When no longer required by the holder, classified information at this level shall be destroyed in such a manner that ensures it cannot be reconstructed. The destruction shall be by a method that is in accordance with the applicable laws, rules or regulations of the Participant.

4.5.3 Information Assurance

1. Classified information at this level shall be processed and stored in CIS which have been accredited for this level of classification by the appropriate Security Authority.

2. The security accreditation of CIS handling Classified Information at this level and of any interconnection thereof may be delegated to the Security Officer of a Contractor or Sub-Contractor if this is permitted by national laws, rules or regulations. Where that task is delegated, the Contractor or Sub-Contractor shall be responsible for implementing the minimum security requirements described in Annex D of this PSI when handling RESTREINT UE/EU RESTRICTED information on its CIS. However, the relevant Security Authorities or SAAs retain the responsibility for the protection of Classified Information at this level handled by the Contractor or Sub-Contractor and the right to inspect the security measures taken by the Contractor or Sub-Contractor. In addition, the Contractor or Sub-Contractor shall provide to the Contracting Authority and, where required, to its NSA/DSA a statement of compliance certifying that the CIS handling Classified Information at this level have been accredited. The accreditation to be applied shall be in accordance with the applicable laws, rules or regulations of the Participant.

3. Classified information at this level that is transmitted shall be protected by cryptographic products approved by the EU or the relevant Security Authority. For interconnected systems this needs to be approved by the relevant Security Authorities (or SAAs).

4. Portable computing devices not using approved encryption shall only be used or stored in areas with appropriate access control. Data storage media and computing devices containing classified information at this level which are not encrypted with an approved encryption system shall not be carried outside premises unless they can be held under personal custody.

5. Classified information at this level may be stored on removable data storage media or devices. Section 4.7.4 provides further information on the procedures and considerations that apply.

4.6 Access to classified information at meetings

1. Access to classified information at meetings, which include conferences, symposia and seminars, shall be subject to the provisions of this PSI.

4.7 Procedures for the transport and electronic transmission of classified information

1. For the purposes of this document the following terminology is used in the context of exchanging classified information:

   a. **Transport:** for the physical movement of classified information (e.g. by hand carriage, postal service, commercial courier, transport by road, rail, air or sea);

   b. **Electronic transmission:** for the electronic transfer of classified information (e.g. via email).

2. For the purposes of this PSI, electronic transmission does not include the transport of removable storage media and devices. This aspect is addressed in Section 4.7.4.

4.7.1 Transport within a single Participant's territory

1. The transport of Classified Background Information or Classified Foreground Information within the territory of a Participant will be in accordance with the applicable laws, rules or regulations of the Participant.

4.7.2 Procedures for the transport of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET classified information between Participants, Contractors and/or Sub-Contractors

1. As a general principle, the preferred means for the transport or electronic transmission of classified information at these levels under GOVSATCOM is electronic transmission using approved encryption methods or products.

2. The following means may be used for the transport of CONFIDENTIEL UE/EU CONFIDENTIAL classified information:

a. Electronic transmission using approved encryption systems, cryptographic products or methods;

b. Government-to-Government channels;

c. Hand carriage by authorised personnel holding the appropriate level of PSC;

d. Approved transport by road, rail, ship or air by security cleared transport companies or escorting personnel;

e. Carriage by non-security cleared authorised postal services or commercial courier companies, in accordance with national laws and regulations.

3. The following means are permitted for the transport of SECRET UE/EU SECRET classified information:

a. Electronic transmission using approved cryptographic products or methods;

b. Government-to-Government channels;

c. Hand carriage by authorised personnel holding the appropriate level of PSC; or

d. Approved transport by road, rail, ship or air by security cleared transport companies or escorting personnel.

4. Entities will transport Classified Information on the condition that the sender first obtains confirmation from its relevant Security Authority that the receiving site holds a valid FSC at the appropriate level or has been approved otherwise for handling of classified information up to the appropriate classification level, and that the entity is entitled to receive GOVSATCOM-related Classified Information at that level.

International electronic transmission

5. Electronic transmission of classified information at these levels between Participants shall be protected by cryptographic methods or products approved by the EU.

Government-to-Government channels

6. Government-to-Government channels (e.g. diplomatic bag services) to be used for the transport of classified information at these levels shall be in compliance with the regulations of the sending Participant. (Note: this is not to be confused with the hand carriage of classified information, which is covered in the next sub-section.)

Hand carriage

7. Classified information at these levels may be hand carried by an individual holding the appropriate level of PSC.

8. An individual hand-carrying classified information shall be briefed on his/her responsibilities by the Security Officer before the carriage occurs.

9. An individual hand-carrying classified information from one Participant State to another will be issued with a Courier Certificate, a template of which is provided in Annex E, or the national equivalent. Senders can use the template in that Annex, or an equivalent national document approved by their Security Authority. The individual hand-carrying the information shall carry the Courier Certificate during the carriage and be able to present this upon arrival at the receiving facility.

10. During the hand carriage the consignment shall remain in the personal custody of the individual or be appropriately secured as described in this PSI. It shall not be left unattended and shall not be opened en route.

International carriage by approved postal services or commercial courier services

11. SECRET UE/EU SECRET classified information shall not be sent internationally by postal service or commercial courier service.

12. The sending of classified information by approved postal services or commercial courier services is only permitted for consignments up to and including the classification level CONFIDENTIEL UE/EU CONFIDENTIAL, provided such means of exchange are permitted by the applicable laws, rules or regulations of the sending Participant.

13. For consignments up to and including the classification level CONFIDENTIEL UE/EU CONFIDENTIAL, postal services or commercial courier services shall only be used if the following criteria have been met:

    a. The Security Authority of the sender permits the use of postal services or commercial courier services according to its applicable laws, rules or regulations;

    b. The Security Authority of the sender may, according to its applicable laws, rules or regulations, require the postal service or commercial courier service to hold an FSC;

    c. The postal service or commercial courier service to be used is located within the Participant State's territory, has a security programme for handling valuable items, including a signature service, a continuous record of accountability on custody and a tally record or electronic track and trace system;

    d. The postal service or commercial courier service to be used shall ensure that the consignment is delivered to the recipient prior to a specified time and date within a 24-hour period under regular circumstances, or within a clearly defined time frame for consignments over distances that cannot reasonably be covered within a 24 hour period; and

    e. The postal service or commercial courier service shall provide to the sender proof of receipt and delivery of the consignment.

14. When CONFIDENTIEL UE/EU CONFIDENTIAL classified information is sent by postal service or approved commercial courier service, the consignment shall be prepared and packaged as follows:

    a. The consignment shall be sent using double envelopes (the inner envelope being a tamper-evident envelope) or other suitably secure packing material;

b. The classification level shall be clearly visible on the inner envelope/package;

c. The classification shall not be indicated on the outer envelope/package;

d. Both the inner and outer envelope/package shall usually be addressed to the recipient's classified registry or the Security Officer, as indicated on the FSC confirmation, and shall include a return address;

e. A registration receipt form shall be placed inside the inner envelope/packaging for the recipient to complete and return. The registration receipt, which itself shall not be classified, shall quote the reference number, date and copy number of the document, but not the subject;

f. Delivery receipts are required in the outer envelope/packaging. The delivery receipt, which itself shall not be classified, should quote the reference number, date and copy number of the document, but not the subject; and

g. The courier service must first obtain and provide the consignor with proof of delivery of the consignment on the signature and tally record, or the courier must obtain receipts/package numbers.

15. The sender shall liaise with the named recipient before the consignment is sent to agree a suitable date/time for delivery.

16. The sender is solely responsible for the consignment that is sent by postal service or commercial courier service. In the event that the consignment is lost or not delivered on time, the sender shall follow up with the postal service or commercial courier service to ascertain the circumstances of the security incident and inform its NSA/DSA and the Contracting Authority.

Transport by freight – general requirements

17. Classified information at these levels which is of such size or shape that it cannot be transported by one of the methods listed above, or large volumes of classified information, may be transported as freight by a commercial transport company. (Note: this is not to be confused with a commercial courier service as covered in the previous sub-section.)

18. The transport company shall hold an FSC at the appropriate level and/or shall be capable of deploying security cleared couriers or escorts for the transport, if permitted under the sender's applicable laws, rules or regulations.

19. Where classified information at these levels requires overnight storage at the transport company's facilities, an FSC with storage capabilities shall be required. Senders shall check with their Security Authority before selecting a commercial transport company whether an FSC will be required for the transport.

20. The sender shall prepare a Transportation Plan using Annex F (or an equivalent national document approved by its Security Authority). When the sender has completed the Plan, it shall submit it to its Security Authority for consideration. Once reviewed, the sender's Security Authority will submit the Transportation Plan to the Security Authority of the

recipient for its consideration. Transport by freight cannot take place until both the sending and recipient Security Authorities have agreed the Transportation Plan.

21. The degree of protection and measures required for the transport shall be determined by the highest classification level of the contents of the consignment.

22. Containers used for the transport shall not bear any visible indication that they contain classified information. These containers shall be sealed with seals/locks in such a way that any tampering will be evident. Any evidence of tampering shall be considered a security breach and be reported as soon as possible.

23. Journeys will be point-to-point to the extent possible and will be completed with the shortest possible delays and stops. Appropriate security measures shall be in place at all stages during the transport.

24. If possible, routes to be used for road and rail will be limited to the territory of Participant States. If not possible, routes through non-Participant States will be planned in close cooperation with the Security Authorities of the sender and recipient.

Security escorts or security guards

25. Any security escort/guard team shall be composed of an adequate number of personnel to ensure regular tours of duty and rest. Their number shall depend on the highest classification level of the consignment, the method of transport to be used, the estimated time in transit and at designated stops, and the quantity and level of the classified information to be protected.

26. It is the responsibility of the sender and, where applicable, the recipient, to instruct security escorts and security guards on how the consignment shall be protected.

Transport by road

27. The consignment shall be accompanied by at least two individuals with the appropriate level of PSC, who may be the driver, co-driver or another individual escorting the transport. One of these individuals shall be issued with and carry a Courier Certificate (Annex E) or the national equivalent. Before the transport occurs, these individuals shall be briefed on their security responsibilities to protect classified information.

28. Classified information shall be secured in containers by a lock or padlock, or in a closed or locked vehicle. If this is not possible because of the size or nature of the contents, the consignment shall be suitably sealed using a tamper-evident method to protect the classified aspects.

29. Where stops are required during transport, attempts should be made by the sender to arrange for stops to be at suitably cleared government establishments or Contractor’s or Sub-Contractor’s facilities holding an FSC. In the event such arrangements cannot be made, or an emergency situation arises due to accident or breakdown of the vehicle, at least one of the individuals with a PSC accompanying the consignment shall be responsible for monitoring and keeping it under constant control.

30. Where possible, loading and unloading of the consignment will be under the security control of at least one individual holding an appropriate level of PSC.

31. Where appropriate and permissible, the sending and receiving Security Authorities, and any Participant States the transport will pass through, shall advise their customs or other relevant authorities of impending consignments.

Transport by rail

32. The consignment shall be accompanied by at least two individuals with the appropriate level of PSC. One of these individuals shall be issued with and carry a Courier Certificate (Annex E) or the national equivalent. Before the transport occurs, these individuals shall be briefed on their security responsibilities to protect classified information.

33. Passenger accommodation shall be made available for security escorts and/or security guards. During stops, the security escorts and/or guards shall remain with the consignment.

34. Where possible, loading and unloading of the consignment shall be under the security control of at least one individual holding the appropriate level of PSC.

35. Deliveries and collection shall be so timed as to prevent, to the extent possible, a consignment being held in warehouses without an appropriate level of FSC.

Transport by sea

36. The consignment shall be accompanied by at least two individuals with the appropriate level of PSC. One of these individuals shall be issued with and carry a Courier Certificate (Annex E) or the national equivalent. Before the transport occurs, these individuals shall be briefed on their security responsibilities to protect classified information.

37. Preference shall be given to using ships that sail under the flag of a Participant State.

38. The consignment shall be stowed in locked stowage space approved by the Security Authority of the sender. Where practicable, at least one security escort or security guard holding an appropriate PSC shall accompany the consignment.

39. Except in case of emergency, stops at a port of a non-Participant State are not permitted unless the prior approval of the sender’s Security Authority has been obtained. Where possible, loading and unloading of the consignment will be under the security control of at least one individual holding the appropriate level of PSC.

40. Deliveries to the port of embarkation and collection from the port of disembarkation shall be timed to prevent, as far as possible, a consignment being held in port warehouses, unless the warehouse has an appropriate level of FSC.

Transport by air as freight

41. Unless there are clear reasons why this is not possible, the consignment shall be accompanied by at least two individuals with the appropriate level of PSC. If this requirement cannot be met, the sender should consult its Security Authority to seek its approval. One of these individuals shall be issued with and carry a Courier Certificate, as

shown in Annex E, or the national equivalent. Before the transport occurs, these individuals shall be briefed on their responsibilities to protect classified Information.

42. Where possible, the consignment will be delivered straight to the aircraft rather than being stored in warehouses at airports or airfields (unless a warehouse has an approved storage capability for classified items at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above). A sufficient number of security escorts and/or security guards shall be provided to keep the consignment under adequate supervision.

43. Where possible, loading and unloading of the consignment will be under the security control of at least one individual holding the appropriate level of PSC.

44. Direct flights will be used whenever possible.

45. Intermediate routine stops of short duration may be permitted, provided the consignment remains in the aircraft. If the cargo compartment is to be opened at a stop, every effort shall be made to ensure that a security escort or security guard accompanying the consignment is present.

46. In the event that the aircraft is delayed at an intermediate stop for a significant period of time or is forced to make an unscheduled or emergency landing, the individual holding the Courier Certificate will take all reasonable measures possible for the protection of the consignment. That individual shall inform his/her Security Authority of the delay as soon as possible. If necessary, that individual will seek the assistance of his/her Diplomatic mission in the country concerned.

47. At its final destination, every effort will be made for the aircraft to be met on landing and the consignment to be placed under the security control of at least one individual holding an appropriate level of PSC.

4.7.3 Procedures for the transport of RESTREINT UE/EU RESTRICTED classified information

1. As a general principle, the preferred means for the exchange of classified information at this level under GOVSATCOM is by electronic transmission. Such transmission shall be protected by approved cryptographic methods or products.

2. When electronic transmission is not possible, the following physical means are permitted for the exchange of classified information at this level without additional requirements, unless required by the sender’s Security Authority:

    a. Hand carriage;

    b. Transport by postal services or commercial courier services;

    c. Government-to-Government channels;

    d. By freight.

3. The transport shall be in accordance with the sender's applicable laws, rules or regulations. The envelope or wrapping shall not reveal the classification level of the information contained.

4.7.4 Procedures for transporting of classified information using removable storage media

1. The use of removable storage media to transfer classified information under GOVSATCOM is generally encouraged over sending physical documents, for both cost and practical reasons, but using removable storage media also carries additional risks that must be mitigated by the sender. The compromise of removable storage media containing a number of classified documents will usually be more damaging than the compromise of a consignment of physical documents, given the volume of information which can be stored on such media.

2. When considering using removable storage media, only the necessary classified documents to perform a particular task/activity should be stored on the media. It is not permitted to store classified documents that are not relevant or no longer associated with a task/activity. Mixing unclassified information with classified information is strongly discouraged. Sender should bear in mind that large amounts of classified information stored on such devices may warrant a higher classification level.

3. Personal USB sticks and those given freely at conferences, seminars, etc. must not be used for storing or transferring classified information.

4. Removable storage media containing classified information are required to be labelled with the appropriate classification marking. Measures shall be taken to prevent unauthorised access to such storage media and to maintain the Need-to-Know principle.

5. If CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET classified information is stored on removable storage media, it must be logged and registered as stipulated by this PSI.

6. The use of removable storage media in a facility must be strictly controlled and accounted for.

7. Only CIS that has been appropriately accredited and/or approved shall be used to transfer classified information from the removable storage media.

8. When transporting classified information on removable storage media particular care should be taken to ensure that the media does not contain viruses or malware prior to the transfer of the data onto the media.

9. All CIS used for processing EUCI shall use appropriate system configuration to preserve integrity, functionality and to enforce access control. For example, AutoRun and AutoPlay (or similar functions) shall be disabled on all CIS to prevent unauthorised applications or malware from running automatically from removable media. In the event that an application attempts to run automatically from removable media, the user must cancel it and take steps to ensure that it does not run again.

10. Unless the removable storage media is encrypted with an EU approved cryptographic product for that level of classification, it must be prepared, packaged and transported in exactly the same manner as classified information in physical form. If suitably encrypted, the removable storage media shall be handled in accordance with security operating procedures pertinent to the encryption system used.

11. Removable storage media that is used to transport classified information shall be accompanied by a dispatch note, detailing the removable storage media containing classified information, as well as all files contained on it, to allow the recipient to make the necessary verifications and to confirm receipt.

12. As a general rule, documents on the removable storage media that are either no longer required or have been transferred onto an appropriate CIS are to be securely removed or deleted using approved products or methods. Unless stored in an appropriate security cabinet or facility, CDs/DVDs without rewriting capability should be destroyed when no longer needed. Any destruction/deletion shall be by use of a method that is in accordance with the applicable laws, rules or regulations of the Participant holding the removable storage media.

Section 5 – Sharing and release of classified information

5.1 Sharing by GOVSATCOM Contractors

1. There will be no restrictions for the Contractors of a given GOVSATCOM contract to share the GOVSATCOM Classified Foreground Information between themselves as well as with the Commission, with the Contracting Authority and with the Participants of that GOVSATCOM contract.

5.2 Sharing with Sub-Contractors

1. Classified Foreground Information related to GOVSATCOM contract may be shared on a Need-to-Know basis with Sub-Contractors of that GOVSATCOM contract only. Routine sharing of such information with Sub-Contractors will be implemented, on a Need-to-Know basis, by the Contractors under the general supervision of the Contracting Authority.

5.3 Sharing with, and release to, ESA

1. There will be no restrictions on sharing the GOVSATCOM Classified Foreground Information with ESA for Contractors (and their Sub-Contractors) that have been awarded a contract under GOVSATCOM by ESA, or where ESA manages the contract on behalf of the Commission.

2. In all other cases the GOVSATCOM Classified Foreground Information may be transferred to ESA only by following the release procedure described in sub-section 5.4.

5.4 Release to non-Participants

1. The release of Classified Foreground Information, related to GOVSATCOM contract, to entities other than the Participants to that GOVSATCOM contract and their Contractors or Sub-Contractors is not permitted without the specific written approval of the Commission, as Originator. This decision has to be taken after consultation with Member States whose national Classified Background Information has been used for generating Classified Foreground Information.

2. Requests for release of Classified Foreground Information will be submitted through the Contracting Authority to the competent European Commission officer representing the Originator (as identified in Annex A) for approval. Any such requests by Contractors or Sub-Contractors shall be made through the contractual chain.

3. If Classified Background Information is being considered for release, the prior written approval of the Originator is required before such information is released.

5.5 Release of classified information at conferences or other venues

1. At conferences or other venues with representatives from non-Participants attending or for any release of Programme Information to the public, as a rule, only unclassified information should be considered for discussion or presentation. Any such release shall be subject the prior written consent of the Commission, which shall be requested and obtained through the relevant Contracting Authority or, where Background Information is concerned, the Originator.

Section 6 - International visits among Participants, Contractors and Sub-Contractors

1. Each Participant and their Contractors or their Sub-Contractors will permit visits involving access to classified information to their establishments, or to Contractor or Sub-Contractor facilities located on their territory or under their jurisdiction, by Government representatives of another Participating State, staff of Participants, and by Contractor or Sub-Contractor employees. Such visits are subject to the provisions of this Section.

6.1 Procedures for international visits at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET

1. The arrangements described hereafter apply to representatives of the Participants and to the personnel of Contractors or Sub-Contractors who need to undertake visits to another GOVSATCOM Participant or to facilities of GOVSATCOM Contractors or Sub-Contractors, and where such visits require or may require access to contract information classified at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET.

2. Each Participant and Contractor or Sub-Contractor will permit visits involving access to GOVSATCOM classified information on a case-by-case basis to its facilities, by representatives of other GOVSATCOM Participants or by personnel of Contractors or Sub-Contractors, provided that the visitor holds the appropriate PSC (for CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET) and has a Need-to-Know.

3. Such visits will be arranged directly between the security officials of the visitor and the establishment/facility to be visited without involving the NSAs/DSAs concerned, however, by respecting additional national requirements for notification of such visits to their NSAs/DSAs[1]

4. Visitors shall comply with all security regulations and other relevant regulations of the host establishment to be visited. Any classified information disclosed or made available to visitors shall be treated as if supplied via official channels to the entity sponsoring the visit.

5. Prior to arrival at the facility to be visited, a Request for Visit, as shown in Annex G, or the national equivalent, including confirmation of the visitor’s PSC, shall be provided at least 24 hours before arrival directly by the Security Officer of the sending facility/establishment to the Security Officer of the facility to be visited.

6. Both the sending and receiving facilities are to confirm that there is a need for the visit, and both must hold an FSC.

    (a) Responsibilities of the sending Security Officer:

[1] NSAs/DSAs will retain the right to request facilities under their jurisdiction to be visited or conducting such international visits to inform their NSA/DSA about any such visits.

- The sending Security Officer must ensure with the parent NSA/DSA that the receiving facility is in possession of an appropriate FSC or is otherwise approved for handling of classified information up to the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET;
- Confirm that the visitor holds a valid PSC.

(b) Responsibilities of the receiving Security Officer:

- The receiving Security Officer must ensure with the parent NSA/DSA that the sending facility is in possession of an appropriate FSC or is otherwise approved for handling of classified information up to the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET;
- The receiving Security Officer must ensure that records are kept of all visitors, including the name/first name, the organisation they represent, confirmation of the appropriate and valid level of clearance, the date(s) of the visit(s) and the name(s) of the person(s) visited.

Such records are to be retained for a period of no less than 3 years.

(c) Responsibilities of the Visitor:

- To confirm identity, the visitor must be in possession of a valid ID card or passport for presentation to the Security Officer or other authorised official at the receiving facility/establishment.

6.2 Procedures for international visits at the level of RESTREINT UE/EU RESTRICTED

1. Visits relating to classified information at the level of RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending facility and the receiving facility without formal requirements.

Section 7 – Contracting and sub-contracting (security aspects)

1. An FSC is granted by an NSA/DSA to indicate, in accordance with its applicable laws, rules or regulations, that a Contractor or Sub-Contractor under its jurisdiction is capable of protecting classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET at that facility. FSCs are confirmed by the Security Authority responding to a Facility Security Clearance Information Sheet (FSCIS) request submitted by another Security Authority. Participant States may, in accordance with their applicable laws, rules or regulations, issue FSC certificates for their Contractors or Sub-Contractors.

2. In case where the Contractor or Sub-Contractor is a Government or a Government controlled entity, the responsible NSA of that entity shall confirm to the Contracting Authority that the entity is capable in handling EU classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, as appropriate and in accordance with national laws and regulations.

3. NSAs/DSAs will notify the appropriate authorities of the Participants if an FSC that it has issued to one of its Contractors or Sub-Contractors has been suspended or withdrawn.

7.1 Tendering stage and awarding of classified contracts under GOVSATCOM

1. Before launching an invitation to tender for a classified contract, the Contracting Authority shall determine the security classification of any information that could be provided to tenderers.

2. All Contractors or their Sub-Contractors which are required to handle or store information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either during the performance of the classified contract itself or at the pre-contractual stage, must hold a Facility Security Clearance (hereinafter 'FSC') at the required level, where appropriate. The following identifies the three scenarios that may arise during the tendering stage for a classified contract or sub-contract involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level:

   a) No access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level during the tendering stage

   Where the contract notice or the invitation to tender concerns a contract that will involve EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level, but does not require the tenderer to handle such information at the tendering stage, a tenderer which does not hold an FSC at the required level shall not be excluded from the bidding process on the grounds that they do not hold an FSC.

   b) Access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the Contracting Authority during the tendering stage

   Access shall be granted to tenderer personnel who hold a Personnel Security Clearance (hereinafter 'PSC') at the required level and who have a need-to know.

Where EUCI is provided to a tenderer at the tendering stage, a non-disclosure agreement shall be signed, obliging the tenderer to handle and protect EUCI provided to it in accordance with this PSI, which has been based on Commission Decision (EU, Euratom) 2015/444.

c) **Handling or storage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the tenderer during the tendering stage**.

Where the contract notice or the invitation to tender requires tenderers to handle or store EUCI on their premises, the tenderer shall hold an FSC at the required level or shall be granted other appropriate approval to handle and store classified information at these levels. In such circumstances, the Contracting Authority will obtain an assurance from the relevant NSA/DSA that the tenderer has been granted an appropriate FSC or other approval. Access will be granted to the tenderer personnel who hold a PSC at the required level and who have a need-to-know.

Where EUCI is provided to a tenderer at the tendering stage, a non-disclosure agreement shall be signed, obliging the tenderer to handle and protect EUCI provided to it in accordance with this PSI, which has been based on Commission Decision (EU, Euratom) 2015/444.

3. An FSC is not required for access to classified information at RESTREINT UE/EU RESTRICTED level, either at the tendering stage or for the performance of the classified contract. However, some EU Member States require an FSC for contracts or sub-contracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, as listed in Annex C. Such national requirements shall not place additional obligations on other Member States or exclude tenderers, Contractors or Sub-Contractors from Member States that have no such FSC requirements for access to RESTREINT UE/EU RESTRICTED information for related contracts or sub-contracts or a competition for such. These contracts or sub-contracts shall be performed in Member States according to their national laws and regulations.

4. Where an FSC is required for the performance of a classified contract, the Contracting Authority will submit, through its Security Authority, a request to the Contractor's or Sub-Contractor's NSA/DSA using a Facility Security Clearance Information Sheet (hereinafter 'FSCIS'). The classified contract or sub-contract will not be signed until the tenderer's NSA/DSA has confirmed the tenderer's or potential sub-contractor's FSC or has otherwise approved its capability to handle and store classified information up to required level.

7.2 Sub-contracting to Sub-Contractors located in an EU Member State

1. Sub-contracting to entities other than already permitted under the contract shall be subject to prior written consent by the Contracting Authority.

2. Before a Contractor enters into negotiations for a sub-contract involving classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET to a Sub-Contractor based in another EU Member State, the Security Officer of the

Contractor proposing the sub-contract shall first obtain confirmation from its NSA/DSA that the potential Sub-Contractor has a valid FSC, if required. FSCs will be queried and confirmed as described at the start of this Section.

3. During the performance of the sub-contract, no classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be provided to the facility of the Sub-Contractor before an FSC confirmation has been obtained from the relevant NSA/DSA.

4. The Contracting Authority shall notify, through its Security Authority, the NSA/DSA of a Sub-Contractor when a classified sub-contract is awarded, and shall provide a copy of the sub-contract-specific security provisions.

7.3 Sub-contracting to Sub-Contractors located in a non-EU State or established by an international organisation associated to GOVSATCOM

1. Any sub-contracting to an entity which is located in a non-EU State or established by an international organisation constitutes a release of EUCI to that non-EU State or international organisation.

2. Where the classified contract permits sub-contracting, such sub-contracting to entities located in a non-EU State or established by an international organisation shall be subject to prior written consent from the Contracting Authority.

3. Before a Contractor enters into negotiations for a sub-contract involving classified information at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET to a Sub-Contractor based in a non-EU State or established by an international organisation, the Security Officer of the Contractor proposing the sub-contract shall first obtain confirmation from its NSA/DSA that the potential Sub-Contractor has a valid FSC, if required. FSCs will be queried and confirmed as described at the start of this Section.

4. Prior to authorising the signature of a sub-contract with a Sub-Contractor located in a non-EU State or established by an international organisation, the Contracting Authority shall verify whether a Security of Information Agreement is in place with that non-EU State or international organisation and, if applicable, ensure, following the consultation with the Member States whose national Classified Background Information has been used for generating Classified Foreground Information, that the award of such sub-contract does not contravene the security and defence interests of the Union and its Member States.

5. Sub-contracts signed with a Sub-Contractor located in a non-EU State or established by an international organisation will include a security clause requiring the Sub-Contractor to protect EUCI in accordance with the security of information agreement in place between the EU and that non-EU State or international organisation.

6. The Contracting Authority shall notify, through the Commission Security Authority, the Security Authority of a Sub-Contractor when a classified sub-contract is awarded, and shall provide a copy of the sub-contract-specific security provisions.

7.4 Security plan in the event of non-selection of a tenderer, or termination or expiry of a classified contract

1. This sub-section describes the procedures which the Participants and Contractors or Sub-Contractors shall follow in the event of the following:

   a. A Contracting Authority or Contractor terminates, respectively, a classified contract or a sub-contract;

   b. A classified contract or sub-contract expires;

   c. A potential Contractor receives or generates classified information in the pre-contractual stage but is not selected; or

   d. A Contractor receives and generates classified information during an early phase of GOVSATCOM but is not selected for funding or work on a future phase of GOVSATCOM.

7.4.1 Participant-held information

1. In the event of termination or expiry of a classified contract, the Participants' respective rights and responsibilities with regard to Classified Background and Classified Foreground Information relating to GOVSATCOM shall be determined by the Contracting Authority, respecting the decision of the Originator.

2. A Participant that retains classified information shall continue to safeguard it in accordance with this PSI and its applicable laws, rules or regulations, and shall not use that information for other purposes without the prior written consent of the Originator requested and obtained through the Contracting Authority.

7.4.2 Contractor-held information

1. A Contractor or Sub-Contractor that is authorised by the Commission, through the Contracting Authority, (or the Originator for Classified Background Information) to retain classified information shall safeguard it in accordance with this PSI and the applicable laws, rules, or regulations.

2. Without the prior written consent of the Commission requested and obtained through the Contracting Authority (or the Originator for Classified Background Information), a Contractor or Sub-Contractor shall not use classified information for any other purpose than for which it was provided.

3. All classified information released within the context of a classified contract, sub-contract or tender, will be retained, returned or destroyed according to the following provisions:

   a. A tenderer for a contract or a sub-contract receives or generates information during the tendering stage, and is not selected:

      i. All invitations to submit a tender shall contain a clause requiring a tenderer who does not eventually submit a tender to return all classified documents which were provided to enable the tenderer to submit a tender for a contract to the Contracting Authority or a tender for a sub-contract to the Contractor by the date set for opening of tenders.

ii. An unsuccessful tenderer shall be required to return all classified documents after a stipulated period of time (normally within 15 working days after notification that a tender or negotiation proposal was not accepted).

b. When a Contractor or Sub-Contractor has held a classified contract or sub-contract but the classified contract or sub-contract is terminated, expires or if the Contractor or Sub-Contractor is not selected for further funding or work on the next phase of GOVSATCOM, the Contractor or Sub-Contractor:

i. Shall return all classified information unless approval for retention or destruction has been given, as provided for in paragraphs ii. and iii. below.

ii. If the Commission (or Originator) approves that a Contractor or Sub-Contractor can retain the classified information, the Contractor or Sub-Contractor shall continue to protect the information in accordance with the applicable laws, rules or regulations and this PSI.

iii. If the Commission Security Authority (or Originator) approves that a Contractor or Sub-Contractor can destroy the classified information, the Contractor or Sub-Contractor shall ensure that the destruction is undertaken in accordance with the relevant security rules and regulations.

4. In the event that an FSC is withdrawn, the Contractor or Sub-Contractor shall return all classified information to, respectively, their Contracting Authority or Contractor, or dispose of such information in accordance with instructions from their Security Authority.

7.5 Procedures related to breaches, compromises or loss of classified information

1. The personnel shall report suspected or actual security breaches, compromises and losses of classified information to their Security Officer or Local Security Officer as soon as possible, and no later than 24 hours after their discovery.

2. Where applicable, the Security Officer concerned will initiate damage limitation or mitigation measures promptly.

3. The Security Officer of the facility concerned shall investigate the circumstances of the security incident and report it to its Security Authority in accordance with the following:

a. if it is suspected that classified information has been compromised, lost, or a security breach that represents a significant risk of future compromise has occurred, this shall be reported to the competent Security Authority as soon as possible, and no later than 48 hours after the discovery;

b. if classified information is known to have been compromised, this shall be reported immediately in order for the Security Authority to mitigate the potential damage that may be caused.

4. Once informed of a security incident, the Security Authority concerned shall take the appropriate action in accordance with its applicable laws, rules or regulations.

5. For suspected or actual compromise, or loss of classified information, or serious security breaches that may represent a significant risk of future compromise, the Security Authority shall submit a report to the Commission Security Authority and the relevant NSA/DSAs, as identified in Annex A, including the following details as a minimum:

   a. A description of the circumstances of the security incident;

   b. The date or period when the security incident occurred;

   c. The location of the security incident;

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

   e. A list of the classified information that has been or may have been compromised or that is unaccounted for;

   f. Specific identification of the classified information, to include Originator, subject, reference, date, copy number, and language;

   g. Actions taken to locate and recover the classified information;

   h. The responsible person(s) and reasons for compromise or possible compromise;

   i. Assessments of the likelihood of compromise (i.e. "certain”, "probable", "possible”, or "unlikely"), including an explanation;

   j. A statement on whether the Originator has been informed of the security incident; and

   k. Actions taken to secure the classified information and limit further damage.

6. Such reports should be classified, at least, at RESTRICTED level.

7. The Security Officer where the security incident occurred shall provide all necessary assistance to its Security Authority in preparing the report.

8. Any additional measures related to the reporting of security breaches, compromise or loss of COMSEC Items are addressed in the GOVSATCOM COMSEC Instructions (Annex H).

ANNEX A - SECURITY AUTHORITIES PARTICIPATING IN GOVSATCOM

1. Austria

NSA

Bundeskanzleramt / Büro der Informationssicherheitskommission,
Federal Chancellery / Federal Office for Information Security
Ballhausplatz 2
1010 Wien
Österreich

Telephone: +43 1 53115/202594
Fax: +43 1 53109/202749
Email: isk@bka.gv.at

DSA

Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology

Telephone: +43 1 711 62-65 7426
Email: claudia.sterkl@bmk.gv.at

2. Belgium

NSA

National Security Authority
FPS Foreign Affairs, Foreign Trade and Development Cooperation
Rue des Petits Carmes 15
B-1000 BRUXELLES
Belgium

Telephone: +32 2 501 45 42
Fax: +32 2 501 45 96
Email: nvo-ans@diplobel.fed.be

DSA

Ministry of Defense
General Intelligence and Security Service
Industrial Security Office
Queen Elisabeth Barracks
Rue d’Evère 1
B-1140 BRUXELLES
Belgium

Telephone: +32 2 501 46 03
Email: bureau.industrie@qet.be

3. Bulgaria

NSA

Държавна комисия по сигурността на информацията (ДКСИ)
ул. “Козлодуй” No. 4
1202 София
България

State Commission on Information Security (SCIS)
4, Kozloduy Str.
BG-1202 Sofia
Bulgaria

Telephone: +3592 9333 600
Fax: +3592 9873 750
Email: dksi@dksi.bg

4. Cyprus

NSA

National Security Authority
172-174, Strovolos Avenue
2048 Strovolos, Nicosia
Cyprus

Telephone: +357 22 80 77 64
Email: cynsa@mod.gov.cy

5. Croatia

NSA/DSA

Telephone: +385 1 4681 222
Fax: +385 1 4686 049
Email: ivcp@uvns.hr

Point of Contact for standard Requests for Visits (RfV)

Telephone: +385 1 4681 255
Fax: +385 1 4579 914
Email: ivcp@uvns.hr

6. Czech Republic

NSA

Národní bezpečnostní úřad
(National Security Authority)

Na Popelce 2/16
CZ-150 06 Praha 56
Czech Republic

Telephone: +420 257 28 33 35
Fax: +420 257 28 31 10

7. Denmark

NSA

Politiets Efterretningstjeneste (the Danish Security Intelligence Service)
Klausdalsbrovej 1
DK – 2860 Søborg
Denmark

Telephone: + 45 33 14 88 88
Fax: + 45 45 15 01 90
Email: pet@pet.dk

DSA

Forsvarets Efterretningstjeneste (the Danish Defence Intelligence Service)
Kastellet 30
DK – 2100 Copenhagen Ø
Denmark

Telephone: + 45 33 32 55 66
Fax: + 45 33 93 13 20
Email: milsik@fe-ddis.dk

8. Estonia

NSA

Estonian National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn, Estonia

Telephone: + 372 6939211
Email: nsa@fis.gov.ee

9. Finland

NSA

National Security Authority (NSA)
Ministry for Foreign Affairs
Kanavakatu 3 B, Helsinki
PO Box 453

FI-00023 Government
Finland

Telephone: +358 9 160 55890
Fax: +358 9 16 05 5140
Email: nsa@formin.fi

DSAs

COMSEC and NDA Issues

NCSA-FI
Finnish Transport and Communications Agency Traficom
PO Box 320
FI-00059 TRAFICOM
Finland

Email: ncsa@traficom.fi

10. France

NSA

Secrétariat général de la défense et de la sécurité nationale (SGDSN)
Direction protection et sécurité de l'Etat
Sous-direction de la protection du secret
51 Boulevard de Latour-Maubourg
75700 Paris
France

Telephone: +33 1 71 75 81 93
Email: ANSFrance@sgdsn.gouv.fr

11. Germany

NSA

Federal Ministry of the Interior
Referat ÖSII5
Alt-Moabit 140
10557 Berlin
Germany

Telephone: +49 30 18 681 11593
Fax: +49 30 18 681 51593
Email: OESII5@bmi.bund.de

DSA

For industrial security policy matters, FSCs, Transportation Plans (except for COMSEC/ CRYPTO):

Federal Ministry for Economic Affairs and Climate Action
Industrial Security Division – ZC4
Villemombler Str. 76
D- 53123 Bonn
Germany

Telephone: +49 228 99615 ext.no. 4065 or ext. no. 3986
Fax: +49 228 99615 2676
Email: zc4-international@bmwk.bund.de (office email address)

For standard visit requests from/ to German contractors:

Federal Ministry for Economic Affairs and Climate Action
Industrial Security Division – ZC3
Villemombler Str. 76
D- 53123 Bonn
Germany

Telephone: +49 228 99615 2484/2041
Fax: +49 228 99615 2603
Email: zc3-International@bmwk.bund.de (office email address)

12. Greece

NSA

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020
Holargos — Athens
Greece

Telephone: +30-210 657 20 09 (ώρες γραφείου), +30-210 657 20 10 (ώρες γραφείου)
Fax: +30-210 642 64 32, +30-210 652 76 12

13. Hungary

NSA

Nemzeti Biztonsági Felügyelet
H-1399 Budapest
Pf. 710/50

Telephone: +36 1 391 1862

Fax: +36 1 391 1889
Email: nbf@nbf.hu

14. Ireland

NSA/DSA

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45
Ireland

Telephone: + 353 1 408 2724
Email: nsa@dfa.ie

15. Italy

NSA/DSA

Presidenza Del Consiglio Dei Ministri
Dipartimento Informazioni Per La Sicurezza
Ufficio Centrale Per La Segretezza
Via Galilei 32
00185 ROMA
Italy

Telephone: + 39 06 467688 604
+ 39 06 467688 874
+39 06 467688 369
+39 06 467688 618

Email: nsa.spazio@alfa.gov.it
3rintaff@alfa.gov.it

Point of Contact for standard Requests for Visits (RfV)

Presidenza Del Consiglio Dei Ministri
Dipartimento Informazioni Per La Sicurezza
Ufficio Centrale Per La Segretezza
Via Galilei 32
00185 ROMA
Italy

Email: k090@alfa.gov.it

16. Latvia

NSA

Constitution Protection Bureau of the Republic of Latvia
National Security Authority
Miera iela 85 A
LV-1013 Rīga
Latvia

Telephone: +371 702 54 73
Fax: +371 702 54 54
Email: ndi@sab.gov.lv

17. Lithuania

NSA

National Security Authority of the Republic of Lithuania
Pilaitės pr. 19
LT-06264 Vilnius
Lithuania

Telephone: +370 706 66128
Email: nsa@vsd.lt

18. Luxembourg

Autorité nationale de Sécurité

207, route d'Esch
L-1471 LUXEMBOURG

Telephone: +352 2 478 2210
Fax: +352 2 478 2243
Email: ans@me.etat.lu

Point of Contact for standard Requests for Visits (RfV)

Autorité nationale de Sécurité

Telephone: +352 2 478 2210
Fax: +352 2 478 2243
Email: ans@me.etat.lu

Note: Luxembourg does not have a DSA.

19. Malta

NSA

National Security Authority
Ministry for Home Affairs, Security, Reforms and Equality
P.O. Box 146
Valletta
Malta

Telephone: +356 25695300

DSA

Malta Competition and Consumer Affairs Authority (MCCAA)
Mizzi House
National Road
Blata I-Bajda HRM 9010
Malta

Telephone: +356 23952000
Email: certification@mccaa.org.mt

Point of Contact for standard Requests for Visits (RfV)

National Security Authority

Telephone: +356 25695300
Email: maltansa.info@gov.mt

Malta Competition and Consumer Affairs Authority (MCCAA)

Telephone: +356 23952000
Email: certification@mccaa.org.mt

20. Netherlands

NSA (civil contracts)

Ministry of Internal Affairs and Kingdom Relations
General Intelligence and Security Service of the Netherlands
PO box 20010
2500 EA The Hague
Netherlands

Telephone: +31 70 320 44 00
Fax: +31 70 320 07 33
Email: nsa-nl-industry@minbzk.nl

DSA (military contracts)

Ministry of Defence
Netherlands Defence Intelligence and Security Service
Office of Industrial Security
PO box 20701
2500 ES The Hague
Netherlands

Telephone: +31 70 441 94 63
Email: indussec@mindef.nl

Point of Contact for standard Requests for Visits (RfV)

Telephone: +31 70 441 94 41
Email: mivd.requestforvisit@mindef.nl (military personnel)
mivd.requestforvisit.business@mindef.nl (civil personnel)

21. Poland

NSA

Agencja Bezpieczeństwa Wewnętrznego – ABW
Departament Ochrony Informacji Niejawnych
ul. Rakowiecka 2 A
00-993 Warszawa
Polska

Email: nsa@abw.gov.pl

Służba Kontrwywiadu Wojskowego
Zarząd V
ul. Oczki 1
02-007 Warszawa
Polska

Email: zarzad5@skw.gov.pl

22. Portugal

NSA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Portugal

Telephone: +351 210 403 600
Email: geral@gns.gov.pt

23. Romania

<u>NSA</u>

Romanian ANS – ORNISS
Strada Mureș nr. 4
RO-012275 București
Romania

Telephone: +40 21 224 58 30
Fax: +40 21 224 07 14

24. Slovakia

<u>NSA</u>

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
851 06 Bratislava
Slovenská republika

Telephone: +421 2 68 69 11 11
Fax: +421 2 68 69 17 00
Email: podatelna@nbu.gov.sk

25. Slovenia

<u>NSA</u>

Urad Vlade RS za varovanje tajnih podatkov
Šmartinska cesta 152
SI-1000 Ljubljana
Slovenia

Telephone: +386 1 478 75 70
Email: gp.uvtp@gov.si

26. Spain

<u>NSA</u>

Autoridad Delegada para la Seguridad de la Información Clasificada
Oficina Nacional de Seguridad
C/ Argentona 20
28023 Madrid
Spain

Telephone: +34 91 283 2583; +34 91 283 2752
Fax: +34 91 372 58 08
Email: programas@ons.cni.es

Point of Contact for standard Requests for Visits (RfV) and Transportation Plans

Telephone: +34 91 372 50 97
Fax: +34 91 372 58 08
Email: sp-ivtco@ons.cni.es

27. Sweden

NSA

Utrikesdepartementet (Ministry for Foreign Affairs)
UD SÄK/NSA
SE-103 39 STOCKHOLM
Sweden

Telephone: +46 8 405 10 00
Fax: +46 8 723 11 76
Email: ud-nsa@gov.se

DSA

Försvarets Materielverk (Swedish Defence Materiel Administration)
FMV Säkerhetsskyddsavdelning
SE-115 88 Stockholm
Sweden

Telephone: +46 8 782 40 00
Fax: +46 8 782 69 00
Email: security@fmv.se

30. ESA

ESA Security Authority

ESA Security Office
Telephone: +39 0694 180 881
Fax: +39 0694 180 882

Head of the ESA Security Office – Mr. Massimo Mercati
Telephone: +39 344 274 6564
Email: Massimo.Mercati@esa.int

Points of Contact for standard Requests for Visits (RfV)

ESA Personnel Security Administration – Ms. Virginia Sulis
Telephone: +39 0694 180 885
Email: virginia.sulis@ext.esa.int

Point of Contact for direct Requests for Visits (RfV) in the scope of GOVSATCOM to the ESA NAV Directorate Secure Facility at ESTEC

ESA GOVSATCOM Security Officer: Mr. Sergio Agut Sanz
Telephone: +31 628 287 085
Email: Sergio.Agut.Sanz@esa.int

Point of Contact for direct Requests for Visits (RfV) to the ESA Test Centre in ESTEC

ESTEC Test Centre Security Officer: Mr. Frans Starkenburg
Telephone: +31 71 565 5607
Email: Frans.van.starkenburg@esa.int

31. European Commission

European Commission Security Authority

European Commission Security Directorate
DG HR Security Directorate (HR.DS)
Rue de la Loi 200
B-1049
Brussels
Belgium

Telephone: +32 2 2958716 (Industrial Security Advice)

Point of Contact for standard Requests for Visits (RfV)

Phone: +32 2 2991551
Email: EC-SECURITY-CLEARANCE@ec.europa.eu
Please send a copy to the LSO:
Christophe MORAND – Head of DEFIS task force on the security of information
Tel: +32 2 2993495
Email: DEFIS-LSO@ec.europa.eu

For matters related to the release of EU GOVSATCOM information:

Christophe MORAND – Head of DEFIS task force on the security of information
Tel: +32 2 2993495
Email: Christophe.Morand@ec.europa.eu or DEFIS-SECURITY-TASK-FORCE@ec.europa.eu

For matters related to the PSI document content:

Email: DEFIS-SECURITY-TASK-FORCE@ec.europa.eu

32. European Union Agency for the Space Programme (EUSPA)

Security Authority

Janovskeho 438/2
170 00 Prague 7

Czech Republic

Email: security.authority@euspa.europa.eu

EUSPA HQ Local Security Officer

Janovskeho 438/2
170 00 Prague 7 – Czech Republic

Phone: +420 234 766 940
Email: lso@euspa.europa.eu

33. General Secretariat of the Council

Security Authority

Secretary General
General Secretariat of the Council of the European Union
Rue de la Loi, 175
B-1048 Brussels
Belgium

Telephone: +32 2 281 8517

34. European External Action Service (EEAS)

Security Authority

Security and Real Estate Directorate - RM.SECRE
Rond Point Schuman 9A
B-1046 Brussels
Belgium

Telephone: +32 2 584 5108

Point of Contact for standard Requests for Visits (RfV)

RM SECRE.2

Telephone: +32 2 584 4305
Email: EEAS-SECURITY-CLEARANCE@eeas.europa.eu

For matters related to Space Programme issues:

Email: SPACE@eeas.europa.eu

ANNEX B - TABLE OF EQUIVALENT SECURITY CLASSIFICATION MARKINGS[2]

Participant	Secret	Confidential	Restricted
EU	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Austria	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
Belgium	SECRET (Loi du 11 Dec 1998) or GEHEIM (Wet van 11 Dec 1998)	CONFIDENTIEL (Loi du 11 Dec 1998) or VERTROUWELIJK (Wet van 11 Dec 1998)	*(Note 1, see below)*
Bulgaria	СЕКРЕТНО	ПОВЕРИТЕЛНО	ЗА СЛУЖЕБНО ПОЛЗВАНЕ
Croatia	TAJNO	POVJERLJIVO	OGRANIČENO
Cyprus	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΜ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Czech Republic	TAJNÉ	DŮVĚRNÉ	VYHRAZENÉ
Denmark	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Estonia	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland	SALAINEN or HEMLIG	LUOTTAMUKSELLINEN or KONFIDENTIELL	KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG
France	SECRET SECRET DÉFENSE *(Note 2, see below)*	CONFIDENTIEL DÉFENSE *(Notes 2 and 3, see below)*	*(Note 4, see below)*
Germany *(Note 5, see below)*	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Greece	ΑΠΌΡΡΗΤΟ ABR:(ΑΠ)	ΕΜΠΙΣΤΕΥΤΙΚΌ ABR:(ΕΠ)	ΠΕΡΙΟΡΙΣΜΈΝΗΣ ΧΡΉΣΗΣ ABR:(ΠΧ)
Hungary	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTÉSŰ!

[2] This table is provided for reference to help compare classification markings of Classified Foreground Information (EUCI) with those of Classified Background Information. Please note that the main principles for handling and protecting Classified Foreground Information (EUCI) and Classified Background Information are set out in section 4.1 of this PSI.

Ireland	SECRET	CONFIDENTIAL	RESTRICTED
Italy	SEGRETO	RISERVATISSIMO	RISERVATO
Latvia	SLEPENI	KONFIDENCIĀLI	DIENESTA VAJADZĪBĀM
Lithuania	SLAPTAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
Luxembourg	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
Malta	SIGRIET SECRET *(Note 6, see below)*	KUNFIDENZJALI CONFIDENTIAL *(Note 6, see below)*	RISTRETT RESTRICTED *(Note 6, see below)*
Netherlands	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Poland	TAJNE	POUFNE	ZASTRZEŻONE
Portugal	SECRETO *(Note 7, see below)*	CONFIDENCIAL	RESERVADO *(Note 7, see below)*
Romania	STRICT SECRET	SECRET	SECRET DE SERVICIU
Slovakia	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenia	TAJNO	ZAUPNO	INTERNO
Spain	RESERVADO *(Note 7, see below)*	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIG
ESA	ESA SECRET	ESA CONFIDENTIAL	ESA RESTRICTED

Note 1. Belgium: ‘Diffusion Restreinte/Beperkte Verspreiding’ is not a security classification in Belgium. Belgium handles and protects RESTREINT UE/EU RESTRICTED information and classified information bearing the national classification markings of RESTRICTED level in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

Note 2. France: Information generated by France before 1 July 2021 and classified SECRET DÉFENSE and CONFIDENTIEL DÉFENSE continues to be handled and protected at the equivalent level of SECRET UE/EU SECRET and CONFIDENTIEL UE/EU CONFIDENTIAL respectively.

Note 3. France: France handles and protects CONFIDENTIEL UE/EU CONFIDENTIAL information in accordance with the French security measures for protecting SECRET information.

Note 4. France: France does not use the classification ‘RESTREINT’ in its national system. France handles and protects RESTREINT UE/EU RESTRICTED information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union. France will handle classified information bearing the national classification markings of RESTRICTED level in accordance with its national rules and regulations in force for ‘DIFFUSION RESTREINTE’. The other Participants will handle and protect information marked ‘DIFFUSION RESTREINTE’ according to their national laws and regulations in force for the level RESTRICTED or equivalent, and according to the standards defined in the present document.

Note 5. Germany: VS = Verschlusssache.

Note 6. Malta: The Maltese and English markings for Malta can be used interchangeably.

Note 7. Portugal and Spain: Attention is drawn to the fact that the markings RESERVADO and SECRETO used by Portugal and Spain refer to different classifications. Creators of documents with RESERVADO or SECRETO markings are advised to put below these classification markings an annotation indicating the country of origin – either “(ORIGINATOR: PORTUGAL)” or “(ORIGINATOR: SPAIN)”.

ANNEX C – FACILITY AND PERSONNEL SECURITY CLEARANCE FOR CONTRACTORS AND SUB-CONTRACTORS INVOLVING RESTREINT UE/EU RESTRICTED INFORMATION[3]

Member State	FSC		PSC	
	YES	NO	YES	NO
Belgium		X		X
Bulgaria		X		X
Czechia		X		X
Denmark	X		X	
Germany		X		X
Estonia	X			X
Ireland		X		X
Greece		X		X
Spain		X		X
France		X		X
Croatia		X		X
Italy		X		X
Cyprus		X		X
Latvia		X		X
Lithuania	X			X
Luxembourg	X		X	
Hungary		X		X
Malta		X		X
Netherlands	X (only for defence-related contracts and sub-contracts)			X
Austria		X		X
Poland		X		X
Portugal		X		X
Romania		X		X
Slovenia	X			X
Slovakia	X			X
Finland		X		X
Sweden		X		X

[3] These national requirements for FSC/PSC must not place any additional obligations on other Member States or beneficiaries, contractors and sub-contractors under their jurisdiction.

ANNEX D – MINIMUM REQUIREMENTS FOR PROTECTION OF EUCI IN ELECTRONIC FORM AT RESTREINT UE/EU RESTRICTED LEVEL HANDLED IN THE CONTRACTOR'S (SUB-CONTRACTOR'S) CIS[4]

General

1. The Contractor (Sub-Contractor) must be responsible for ensuring that the protection of RESTREINT UE/EU RESTRICTED classified information is in compliance with the minimum security requirements as stated within this security clause and any other additional requirements advised by the Contracting Authority or, if applicable, with the National Security Authority (NSA) or Designated Security Authority (DSA).

2. It is the responsibility of the Contractor (Sub-Contractor) to implement the security requirements identified in this document.

3. For the purpose of this document a Communication and Information System (CIS) covers all equipment used to handle, store and transmit EUCI, including workstations, printers, copiers, fax, servers, network management system, network controllers and communications controllers, laptops, notebooks, tablet PCs, smart phones and removable storage devices such as USB-sticks, CDs, SD-cards, etc.

4. Special equipment, such as cryptographic products, must be protected in accordance with its dedicated Security Operating Procedures (SecOPs).

5. Contractors (Sub-Contractors) must establish a structure responsible for the security management of the CIS handling information classified RESTREINT UE/EU RESTRICTED and appoint a responsible Security Officer of the facility.

[4] This Annex is applied where security accreditation of CIS handling classified information at RESTREINT UE/EU RESTRICTED level and any interconnection thereof are delegated to the Security Officer of a Contractor or Sub-Contractor, if permitted by national laws, rules, or regulations (see Article 4.5.3.2).

6. The use of privately-owned equipment of Contractor's (Sub-Contractor’s) personnel (hardware and software) for processing RESTREINT UE/EU RESTRICTED classified information is not permitted.

7. Contractor's (Sub-Contractor's) CIS handling information classified RESTREINT UE/EU RESTRICTED must be accredited by the Participant's Security Accreditation Authority (SAA) or, where permitted by national laws and regulations, by the respective Contractor (Sub-Contractor) on the basis of agreed minimum standards via delegation from the SAA to the Security Officer of the Contractor (Sub-Contractor).

8. Only information classified RESTREINT UE/EU RESTRICTED encrypted using approved cryptographic products may be handled, stored or transmitted (wired or wireless) as any other unclassified information under the contract (sub-contract). These cryptographic products must be approved by the EU or a Member State.

9. External facilities involved in the maintenance/repair work must be obliged, on a contractual basis, to comply with the applicable provisions for handling of information classified RESTREINT UE/EU RESTRICTED as set out in this document.

10. At the request of the Contracting Authority or relevant NSA/DSA/SAA, the Contractor (Sub-Contractor) must provide evidence of compliance with the contract (sub-contract) Security Clause. If also requested, the Contractors (Sub-Contractors) will permit an audit and inspection of the Contractor's (Sub-Contractor's) processes and facilities by representatives of the Contracting Authority, the NSA/DSA/SAA, or the relevant EU Security Authority, in order to ensure compliance with these requirements.

Physical security

11. Areas in which CIS are used to display, store, process or transmit RESTREINT UE/EU RESTRICTED information, or areas housing servers, network management system, network controllers and communications controllers for such CIS should be established as separate and controlled areas with an appropriate access control system. Access to these separate and controlled areas should be limited to only specifically authorised persons. Without prejudice to paragraph 8 equipment as described in paragraph 3 has to be stored in such separate and controlled areas.

12. Security mechanisms and/or procedures must be implemented to regulate the introduction or connection of removable computer storage media (for example, USB, mass storage devices, CD-RWs) to components on the CIS.

Access to CIS

13. Access to Contractor's (Sub-Contractor's) CIS handling EUCI is based on a strict need to know principle and authorisation of personnel.

14. All CIS must have up to date lists of authorised users and an authentication of all users at the start of each processing session.

15. Passwords, which are part of most identification and authentication security measures, must be a minimum of 9 characters long and must include numeric and "special" characters (if permitted by the system) as well as alphabetic characters. Passwords must be changed at least every 180 days. Passwords must be changed as soon as possible if they have or are suspected of having been compromised or disclosed to an unauthorised person.

16. All CIS must have internal access controls to prevent unauthorised users from accessing or modifying information classified RESTREINT UE/EU RESTRICTED and from modifying system and security controls. Users are to be automatically logged off the CIS if their terminals have been inactive for some predetermined period of time, or the CIS must activate a password protected screen saver after 15 minutes of inactivity.

17. Each user of the CIS is allocated a unique user account and ID. User accounts must be automatically locked after at most 5 successive incorrect login attempts.

18. All users of the CIS must be made aware of their responsibilities and the procedures to be followed to protect information classified RESTREINT UE/EU RESTRICTED on the CIS. The responsibilities and procedures to be followed must be documented and acknowledged by users in writing.

19. SecOPs must be available for the Users and Administrators and must include the descriptions of security roles and the associated list of tasks, instructions and plans.

Accounting, audit and incident response

20. Any access to the CIS must be logged.

21. The following events must be recorded:

    a) all log on attempts, whether successful or failed;
    b) log off (including time out where applicable);
    c) creation, deletion or alteration of access rights and privileges; and
    d) creation, deletion or alteration of passwords.

22. For all of the events listed above at least the following information must be communicated:

    a) type of event;
    b) user ID;
    c) date and time; and
    d) device ID.

23. The accounting records should support the capability to be examined by a Security Officer for potential security incidents and that they can be used to support any legal investigations in the event of a security incident. All security records should be regularly checked to identify potential security incidents. The accounting records must be protected from unauthorised deletion or modification.

24. The Contractor (Sub-Contractor) must have an established response strategy to deal with security incidents. Users and Administrators must be instructed on how to react to incidents, how to report incidents and what to do in case of emergencies.

25. The compromise or suspected compromise of information classified RESTREINT UE/EU RESTRICTED must be reported to the Contracting Authority. The report must contain a description of the information involved and a description of the circumstances of the (suspected) compromise. All users of the CIS must be made aware of how to report any actual or suspected security incident to the Security Officer.

Networking & interconnection

26. When a Contractor (Sub-Contractor) CIS that handles information classified RESTREINT UE/EU RESTRICTED is interconnected to a CIS that is not accredited, this leads to a significant increase in threat to both the security of the CIS and the RESTREINT UE/EU RESTRICTED classified information handled by that CIS. This includes the internet, other public or private CIS, such as other CIS owned by the Contractor (Sub-contractor). In this case, the Contractor (Sub-Contractor) must perform a risk assessment to identify the additional security requirements that need to be implemented as part of the security accreditation process. The Contractor (Sub-Contractor) will provide to the Contracting Authority, and where nationally required, the competent SAA, a statement of compliance certifying that the Contractor (Sub-Contractor) CIS and the respective interconnection have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED.

27. Remote access from other systems to LAN services (e.g., remote access to email and remote SYSTEM support) are prohibited unless special security measures are implemented and agreed by the Contracting Authority, and where nationally required, approved by the competent SAA.

Configuration management

28. A detailed hardware and software configuration, as reflected in the accreditation/approval documentation (including system and network diagrams) must be available and regularly maintained.

29. Configuration checks must be carried out by the Security Officer of the Contractor (Sub-Contractor) on hardware and software to ensure that the unauthorised hardware and software have not been introduced.

30. Changes to the Contractor (Sub-Contactor) CIS configuration must be assessed for their security implications and must be approved by the Security Officer, and where nationally required, the SAA.

31. The system must be scanned for the presence of security vulnerabilities at least quarterly. Software must be implemented allowing detection of malware. Such software must be kept up to date. If possible, the software should have a national or recognised international approval, otherwise it should be a widely accepted industry standard.

32. The Contractor (Sub-Contractor) must develop a Business Continuity Plan. Back-up procedures are established addressing the following:

a) frequency of back-ups;
b) storage requirements on-site (fireproof containers) or off-site;
c) control of authorised access to back-up copies.

Sanitisation and destruction

33. For CIS or data storage media that has at any time held RESTREINT UE/EU RESTRICTED classified information, the following sanitisation must be performed to the entire system or storage media prior to its disposal:

a) Flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must be overwritten at least three times and then verified to ensure that the original content cannot be recovered, or be deleted using approved deletion software;
b) Magnetic media (e.g. hard disks) must be overwritten or degaussed;
c) Optical media (e.g. CDs and DVDs) must be shredded or disintegrated; and
d) For any other storage media, the Contracting Authority or, if appropriate, the NSA/DSA/SAA should be consulted on the security requirements to be met.

34. Information classified RESTREINT UE/EU RESTRICTED must be sanitised on any data storage media before it is given to an entity not authorised to access RESTREINT UE/EU RESTRICTED (e.g. for maintenance work).

ANNEX E - PROCEDURE FOR HAND CARRIAGE OF CLASSIFIED INFORMATION[5]

C.1. When hand carriage of material classified at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level is permitted, the following procedures will apply:

a. The Courier will carry a Courier Certificate recognised by all Participants, authorising him to carry the package as identified (see the Courier Certificate example below) stamped and signed by the Security Authority and the consignor's officer;

b. A copy of the "Notes for the Courier" (shown below) will be attached to the certificate; and

c. The Courier Certificate will be returned to the issuing Security Authority through the consignor's Security Officer immediately after completion of the journey.

C.2. The consignor's Security Officer is responsible for instructing the bearer in all of his duties and of the provisions of the "Notes for the Courier".

C.3. The courier will be responsible for the safe custody of the classified material until such time that it has been handed over to the consignee's Security Officer. In the event of a security breach, the consignor's Security Authority may request the authorities in the country in which the breach occurred to carry out an investigation, report their findings, and take legal action, as appropriate.

[5] This annex contains standard forms used by the Member States. The term ‘company’ in this annex should be understood as also meaning ‘entity’.

(LETTERHEAD)

COURIER CERTIFICATE

EU GOVSATCOM COMPONENT (optional)

COURIER CERTIFICATE NO. …………………… (*)

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

This is to certify that the bearer:

Mr./Ms. **(name/title)**

Born on**: (day/month/year)** in **(country)**

A national of **(country)**

Holder of passport/identity card no.: **(number)**

Issued by: **(issuing authority)**

On: **(day/month/year)**

Employed with: **(company or organisation)**

Is authorised to carry on the journey detailed below the following consignment:

(Number and particulars of the consignment in detail, i.e. No. of packages, weight and dimensions of each package and other identification data as in shipping documents)

………………………………………………………………………………………..

………………………………………………………………………………………..

(*) May also be used by security guards.

- The material comprising this consignment is classified in the interests of the security of:

(Indicate the countries having interest. At least the country of origin of the shipment and that of the destination should be indicated. The country (or countries) to be transited also may be indicated).

- It is requested that the consignment will not be inspected by other than properly authorised persons of those having special permission.

- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not belong to the service, and in the presence of the courier.

- It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

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

(LETTERHEAD)

Annex to the "Courier Certificate" No…………
for the international hand carriage of
classified material

NOTES FOR THE COURIER(*)

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

2. The following general points are brought to your attention:

   (a) You will be held liable and responsible for the consignment described in the Courier Certificate;
   (b) Throughout the journey, the classified consignment must stay under your personal control;
   (c) The consignment will not be opened en route except in the circumstances described in sub-paragraph (j) below;
   (d) The classified consignment is not to be discussed or disclosed in any public place;
   (e) The classified consignment is not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance and storage facilities may be utilised. You are to be instructed on this matter by your company Security Officer;
   (f) While hand-carrying a classified consignment, you are forbidden to deviate from the travel schedule provided, unless unforeseen circumstances require a change of schedule;
   (g) In cases of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal control; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as listed in sub-paragraph (l) below. If you have not received these details, ask for them from your company Security Officer;
   (h) You and the company Security Officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc.) are complete, valid and current;

(*) May also be used by security guards.

(i) If unforeseen circumstances make it necessary to transfer the consignment to an individual other than the designated representatives of the company or government you are to visit, you will give it only to authorised employees of one of the points of contact listed in sub-paragraph (l);

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

You should take precautions to show officials the minimum content necessary to them that the consignment does not contain any other item and ask the official to repack or assist in re-packing it immediately upon completion of the examination.

You should request the senior Customs, Police and/or Immigration Official to provide evidence of the opening and inspection of the packages by signing and sealing them when closed and confirming in the shipping documents (if any) that the consignment has been opened.

If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving company Security Officer and the dispatching company Security Officer, who should be requested to inform the DSAs of their respective governments;

(k) Upon your return, you must produce a bona fide receipt for the consignment signed by the Security Officer of the company or agency receiving the consignment or by a DSA of the receiving government;

(l) Along the route you may contact the following officials to request assistance:

………………………………………………………………………………………

………………………………………………………………………………………

From:
(Originating country)

To:
(Country of destination)

Through:
(List intervening countries)

Authorised stops:
(List locations)

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

Signature of company's Security Officer	Signature of the Security Authority
(Name)	(Name)
Company's stamp	Official stamp or NSA/DSA's seal

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

I declare in good faith that, during the journey covered by the "Courier Certificate", I am not aware of any occurrence or action, by myself or by others, that could have resulted in the compromise of the consignment, except the events listed below *(if needed)*:
…….
…….

Courier's signature:

Witnessed by:
(Company Security Officer's signature)

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

MULTI-TRAVEL COURIER CERTIFICATE N° ……….

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

This is to certify that the bearer Mr/Ms (name and title) …………………… born on (day, month, year) ………… in (country) ………..……, a national of (country) ……………., holder of passport or identity card n° …………… issued by (issuing authority) : ………… on (day, month, year) :…………, employed by (company or organization) : ……..……………..., is authorized to carry classified documents, equipment and/or components between the following countries: …………………………………………..……………….………………
The bearer above is authorized to use this certificate as many times as necessary, for classified shipments between the countries here above until (date): ………….

The shipment description should be attached to each consignment.

The attention of customs authorities, police and immigration services is drawn to the following points:

- The material forming each consignment is classified in the interest of national security of the countries here above.
- It is requested that the consignment will not be inspected by other than properly authorized persons or those having special permission.
- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not have a Need-to-Know and in the presence of the courier.
- It is requested that the package, if opened for inspection, be marked after reclosing to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.
- Customs, Police and/or Immigration officials of countries to be transited, entered or exited are requested to give assistance if necessary to assure successful and secure delivery of the consignment.

Signature of Security Officer Signature of the Security Authority

NOTES FOR THE COURIER

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

The following general points are brought to your attention:

1. You will be held liable and responsible for the consignments described in the "descriptions of shipments".
2. Throughout the journey, the classified consignments must stay in your personal possession, unless you are accompanying a classified consignment under NSA/DSA approved Transportation Plan.
3. The consignments will not be opened en route except in the circumstances described in paragraph 10 below.
4. The classified consignments are not to be discussed or disclosed in any public place.
5. The classified consignments are not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance may be utilized. You are to be instructed on this matter by your company Security Officer.
6. While hand-carrying or accompanying a classified consignment, you are forbidden to deviate from the schedule provided.
7. In case of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal possession except under circumstances described in paragraph 2 above; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as stated in paragraph 11 below. If you have not received these details, ask for them from your company Security Officer.
8. You and the company Security Officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc.) are complete, valid and current.
9. If unforeseen circumstances make it necessary to transfer a consignment to other than the designated representative of the company or government you are to visit, you will give it only to authorised employees of one of the points of contact listed in the description of shipment.
10. There is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing; therefore, should such officials enquire into the contents of the consignment, show them your "Courier Certificate" the description of shipment and this note and insist on showing them to the senior Customs, Police, and/or Immigration Official. This action should normally suffice to allow the consignment to pass through unopened. However, if the senior Customs, Police, and/or

Immigration Official demands to see the actual contents of the consignment you may open it in his presence, but this should be done in area out of sight of the general public.

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

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

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

11. Along the route you may contact the officials whose details will be provided to you before each journey and request assistance from them.
12. Upon return from each journey, you must produce a bona fide receipt for the consignment signed by the Security Officer of the company or agency receiving the consignment or by a NSA/DSA of the receiving government.

ANNEX to multi-travel certificate

Multi-Travel Courier Certificate No:......................

Description of shipment no.: ……..

Transport from (date): …………… to (date): ……………
Bearer (name): ……………………………………………

Itinerary: from (originating country) ……………… to (destination country) ……………… through (crossed countries) ……………………………… authorized stops (list of locations): …………………………………………

References of receipt or inventory list: ……………………………………
Description of the shipment (number of package, dimensions and, if needed, weight of each package)

Officials you may contact to request assistance

Signature of company’s Security Officer

N O T E : **To be signed on completion of each shipment:**

I declare in good faith that, during the journey covered by this "shipment description", I am not aware of any occurrence or action, by myself or by others, that could have resulted in the compromise of the consignment, except the events listed below *(if needed)*:
……….
……….

Place and date of declaration: ……………

Courier's signature:…………………………..

Witnessed by (name and signature of company Security Officer): ………………………….

ANNEX F - TRANSPORTATION PLAN

(LETTERHEAD)

TRANSPORTATION PLAN -
FOR THE MOVEMENT OF CLASSIFIED CONSIGNMENTS

(INSERT THE TITLE OF THE GOVSATCOM CONTRACT)

1. INTRODUCTION

This transportation plan lists the procedures for the movement of classified ***(insert the title of the contract under GOVSATCOM)*** consignments between ***(insert Participants, Contractors or Sub-Contractors in the GOVSATCOM contract)***.

2. DESCRIPTION OF CLASSIFIED CONSIGNMENT

Provide a general description of the consignment to be moved. If necessary, a detailed, descriptive listing of items to be moved under this plan, including nomenclature, may be appended to this plan as an annex. Include in this section a brief description as to where and under what circumstances transfers of custody will occur.

3. IDENTIFICATION OF AUTHORISED PARTICIPATING GOVERNMENT REPRESENTATIVES

This Section should identify by name, title and organisation, the authorised representatives of each contract Participant who will authorise receipt for and assume security responsibilities for the classified consignment. Mailing addresses, telephone numbers, telefax numbers and/or telex address, network addresses should be listed for each Participant’s representatives.

4. DELIVERY POINTS

(a) Identify the delivery points for each Participant (e.g. ports, railheads, airports, etc.) and how transfer is to be effected.

(b) Describe the security arrangements that are required while the consignment is located at the delivery points.

(c) Specify any additional security arrangements, which may be required due to the unique nature of the movement or of a delivery point (e.g. an airport freight terminal or port receiving station).

5. IDENTIFICATION OF CARRIERS

Identify the commercial carriers, freight forwarders and transport agents, where appropriate, that might be involved, including the level of their security clearance and storage capability.

6. STORAGE/PROCESSING FACILITIES AND TRANSFER POINTS

(a) List, by participant, the storage or processing facilities and transfer points that will be used.

(b) Describe specific security arrangements necessary to ensure the protection of the classified consignment while it is located at the storage/processing facility or transfer point.

7. ROUTES

Specify in this section the routes for movements of the classified consignments under the plan. This should include each segment of the route from the initial dispatch point to the ultimate destination including all border crossings, in particular travel through non-Participant States. Routes should be detailed for each Participant in the logical sequence of the shipment from point to point. If overnight stops are required, security arrangements for each stopping point should be specified. Contingency stop over locations should also be identified as necessary.

8. PORT SECURITY AND CUSTOMS OFFICIALS

In this Section, identify arrangements for dealing with customs and port security officials of each Participant. The facility must verify that the courier has been provided with the necessary documentation and is aware of the rules necessary to comply with customs and security requirements. Prior co-ordination with customs and port security agencies may be required so that the Project/GOVSATCOM movements will be recognised. Procedures for handling custom searches and points of contact for verification of movements at the initial dispatch points should also be included here.

9. COURIERS

When couriers are to be used, provisions for the international hand carriage of classified material specified in Section 4.7 and Annex E will apply.

10. RECIPIENT RESPONSIBILITIES

Describe the responsibilities of each recipient to carry out an inventory of movement and to examine all documentation upon receipt of the movement and:

(a) Notify the dispatcher of any deviation in routes or methods prescribed by this plan.

(b) Notify the dispatcher of any discrepancies in the documentation or shortages in the shipment.

(c) Clearly state the requirement for recipients to promptly advise the Security Authority of the dispatcher of any known or suspected compromise of classified consignment or of any other exigencies that may place the movement in jeopardy.

11. DETAILS OF CLASSIFIED MOVEMENTS

This section should contain the following items:

(a) Identification of dispatch assembly points.

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

(c) Documentation required for the dispatch points.

(d) Courier authorisation documentation and travel arrangements.

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

(f) Procedures for accessibility by courier to the shipment en route.

(g) Procedures for unloading at destination, to include identification or recipients and procedures for change of custody, and receipt arrangements.

(h) Emergency communications procedures. List appropriate telephone numbers and points of contact for notification in the event of emergency.

(i) Procedures for identifying each consignment and for providing details of each consignment; the notification should be transmitted no less than six working days prior to the movement of the classified consignment.

12. RETURN OF CLASSIFIED MATERIAL

This section should identify requirements for return of classified material to the manufacturer or sending Participant (e.g. warranty, repair, test and evaluation, etc.).

NOTE: Samples of these forms should be included, as appropriate, as enclosures to the plan, as necessary:

(1) Packing list

(2) Classified material receipts

(3) Bills of loading

(4) Export declaration

(5) Waybills

(6) Other Participant-required forms.

ANNEX G - REQUEST FOR VISIT[6]

Note: The completed form shall be submitted directly to the Security Officer of the establishment to be visited. Fields of the form related to NSAs/DSAs should be left empty.

REQUEST FOR VISIT **TO:** ______________________________________ ***(Country/international organisation name)***

1. TYPE OF VISIT REQUEST	**2. TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS**	**3. SUMMARY**

☐ One-time
☐ Recurring
☐ Emergency
☐ Amendment
    ☐ Dates
    ☐ Visitors
    ☐ Agency/Facility
 	
For an amendment, insert the NSA/DSA original RFV Reference No.______________
	☐ C-UE/EU-C
	
	☐ S-UE/EU-S
		No. of sites: _______
		
		No. of visitors: _____

4. ADMINISTRATIVE DATA:	
Requestor: To:	NSA/DSA RFV Reference No.________________ Date *(dd/mm/yyyy)*: _____/_____/_____

5. REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:
☐ Government   ☐ Industry   ☐ EC   ☐ ESA   ☐ Other If other, specify: ______________________ NAME: POSTAL ADDRESS: E-MAIL ADDRESS: FAX NO: TELEPHONE NO:

6. GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED - *(Annex 1 to be completed)*

[6] This annex contains standard forms used by the Member States. The terms 'contract' and 'company' in this annex should be understood as also meaning 'contract' and 'entity', respectively.

7. DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____	
8. TYPE OF INITIATIVE *(Select one from each column)*:	
☐ Government initiative ☐ Commercial initiative	☐ Initiated by requesting agency or facility ☐ By invitation of the facility to be visited
9. SUBJECT TO BE DISCUSSED/JUSTIFICATION/PURPOSE *(To include details of host Government/Project Authority and solicitation/contract number if known and any other relevant information. Abbreviations should be avoided)*:	
10. ANTICIPATED HIGHEST LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:	
	☐ C-UE/EU-C ☐ S-UE/EU-S If other, specify: _______________________
11. PARTICULARS OF VISITOR(S) - *(Annex 2 to this form to be completed)*	
12. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY: NAME: TELEPHONE NO: E-MAIL ADDRESS: SIGNATURE:	

13. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO: STAMP

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

14. REQUESTING NATIONAL SECURITY AUTHORITY / DESIGNATED SECURITY AUTHORITY:

NAME:

ADDRESS:

TELEPHONE NO: STAMP

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. REMARKS *(Mandatory justification required in case of an emergency visit)*:

ANNEX 1 to RFV FORM

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. ☐ Government ☐ Industry ☐ EC ☐ ESA ☐ Other If other, specify: ______________________ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. ☐ Government ☐ Industry ☐ EC ☐ ESA ☐ Other If other, specify: ______________________ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:

3. ☐ Government ☐ Industry ☐ EC ☐ ESA ☐ Other If other, specify: ______________________ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
4. ☐ Government ☐ Industry ☐ EC ☐ ESA ☐ Other If other, specify: ______________________ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:

5. ☐ Government ☐ Industry ☐ EC ☐ ESA ☐ Other If other, specify: ______________________ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: ***(Continue as required)***

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)
1 ☐ Government ☐ Industry ☐ EC Employee ☐ ESA Employee ☐ Other (Specify: ____________________________) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:
2 ☐ Government ☐ Industry ☐ EC Employee ☐ ESA Employee ☐ Other (Specify: ____________________________) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:

3 ☐ Government ☐ Industry ☐ EC Employee ☐ ESA Employee
☐ Other (Specify: ______________________________)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

4 ☐ Government ☐ Industry ☐ EC Employee ☐ ESA Employee
☐ Other (Specify: ______________________________)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

5 ☐ Government ☐ Industry ☐ EC Employee ☐ ESA Employee
☐ Other (Specify: ______________________________)

SURNAME:
FORENAMES *(as per passport)*:
RANK *(if applicable)*:
DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____
PLACE OF BIRTH:
NATIONALITY:
SECURITY CLEARANCE LEVEL:
PP/ID NUMBER:
POSITION:
COMPANY/AGENCY:

(Continue as required)

ANNEX H – COMSEC INSTRUCTIONS FOR COMSEC ITEMS WITH AN EU SECURITY CLASSIFICATION EXCHANGED UNDER GOVSATCOM