EUROPEAN GNSS PSI
version 1.1

PROGRAMME/PROJECT SECURITY INSTRUCTION

FOREWORD (for the European GNSS Programme only)

The attached sample standard format for a Programme/Project Security Instruction (PSI) provides supplementary information for the security section of specific projects/phases within the European GNSS Programmes. The guidance contained in the PSI also supplements the guidance contained in the national security rules of the Participating States and the security rules of the Participating Organisations under which Classified Information and material is protected. It should be used to reconcile differences in policies so that standard procedures will be used for the specific project / phase.

The minimum elements of information to be provided for each section are described, and, in some cases, suggested language is provided. These descriptions and suggested language are for guidance only. Additional requirements may apply depending on the size and complexity of the specific project/phase and on the sensitivity of the information involved.

This standard format is a tool to facilitate the development of a Programme/Project Security Instruction for a specific project/phase. When the terms European GNSS Programmes are used herein, the correct denomination should be inserted as applicable.

PROGRAMME/PROJECT SECURITY INSTRUCTION

CONCERNING

(insert specific project/phase)

(SHORT TITLE: EUROPEAN GNSS PSI *)*

version 1.1 issued by
Galileo Security Board (GSB)

Date
22 January 2008

Participants:

EU MEMBER STATES

EU COUNCIL

EU COMMISSION

ESA

GSA

NORWAY

SWITZERLAND (*)

AMENDMENT SHEET

SERIAL	REFERENCE	DATE	SIGNATURE AND NAME
Issue 1.0	Approved by GSB after silent procedure	5/11/2004	
version 1.1	amendments suggested by GSC	22/01/2008	

1.1 TABLE OF CONTENTS

GLOSSARY

AUTHORISED ACCESS is the ability and opportunity to obtain knowledge of classified information provided the individual to be allowed to access such information is appropriately security cleared and has a need to know.

AUTOMATED INFORMATION SYSTEM (AIS) is an assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information, and textual materiel.

AUTOMATED INFORMATION SYSTEM SECURITY includes all security safeguards needed to provide an acceptable level of protection for Automated Information Systems and the classified data processed.

BACKGROUND INFORMATION means any information, classified or unclassified, necessary or useful to the performance of the European GNSS Programmes of the European GNSS programmes generated before or outside the performance of this European GNSS Programmes.

CLASSIFICATION AUTHORITY is the authority vested in a public entity to make an initial determination that information requires protection against unauthorised disclosure in the interest of national security or the security of the EU or ESA.

CLASSIFIED CONTRACT includes any contract to supply products, execute works or provide services, the performance of which requires or involves access to or generation of classified information by Contractor employees. The requirements prescribed for a "Classified Contract" are also applicable to all phases of pre-contract activity, including solicitation (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Contracting Agency programme or project which requires access to classified information by a Contractor.

CLASSIFIED INFORMATION is information that requires protection against unauthorised disclosure, which could harm in various degrees the essential interests of the Participants. Its classification is indicated by a classification marking. Such information must be protected against any loss of confidentiality, integrity and availability.

CLASSIFIED MEETING is a conference, seminar, symposium, exhibition, convention, or other gathering that is conducted by a public entity or by a cleared Programme Contractor with a public entity's approval and sponsorship, during which Classified Information is disclosed.

COMPROMISE is a situation where - due to a breach of security or adverse activity - the Classified Information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability e.g. through espionage, acts of terrorism, sabotage, theft or unauthorised release to the public. This includes any loss, disclosure to unauthorised individuals, unauthorised modification, destruction in an unauthorised manner, or denial of service.

COMSEC INFORMATION AND MATERIAL is a piece of information or a material (hardware or software) that is important for the security of a communication and/or information system handling classified data and is therefore submitted to specific security rules such as accounting procedures, in accordance with national regulations under the control of national COMSEC/INFOSEC authorities.

CONTRACTING AGENT is ESA, or the European Commission (EC) or the European GNSS Supervisory Authority (GSA) for the activities for which they have a competence.

CONTRACTOR is any entity awarded a Contract by a Contracting Agent.

CO-ORDINATING CONTRACTOR AND CONTRACTING PARTNERS are Contractors holding the appropriate Facility Security Clearance (FSC) issued by the NSA/DSA where they are located in order to be able to handle Classified information generated in the framework of the European GNSS Programmes. They may, if duly authorised by the Contracting Agent, negotiate subcontracts with subcontractors at the first level provided they hold an appropriate FSC. The Co-ordinating Contractor and Contracting Partners are required, under penalty of termination of their contract, to take all measures for safeguarding such Classified information.

COURIER is an appropriately cleared and authorised government employee from participating States or staff member of a participating organisation, or a Contractor employee that is appropriately approved by the NSAs/DSAs to hand-carry Classified material to its destination.

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

DESIGNATED SECURITY AUTHORITY (DSA) is the security authority designated by the National Security Authority (NSA) of a participating State to be responsible for the coordination and implementation of national, ESA and EU industrial security aspects of the European GNSS Programmes. The function of the DSA may be carried out by the NSA.

DOCUMENT includes any recorded information, and is not limited to writing, drawing, or data in the form of letter, note, minute, report, paper, memorandum, signal, message, sketch, stencil, carbon, typewriter ribbon, photograph, film, map, chart, plan, tape recording, and magnetic recording.

FACILITY SECURITY CLEARANCE (FSC) is an administrative determination by the Security Authority of the country where the facility is located that, from a security viewpoint, a facility can afford adequate security protection to information classified CONFIDENTIAL or above and its personnel who require access to classified information have been appropriately security cleared and briefed on the relevant security requirements necessary to access and protect classified information.

FACILITY SECURITY OFFICER is a person designated by management to be responsible for the proper implementation of security related decisions and for co-ordination of available security resources and measures within a facility involved in the classified parts of the European GNSS Programmes, as well as to be the technical advisor to management on security matters related to the European GNSS Programmes.

FOREGROUND INFORMATION is information generated in the performance of the European GNSS Programmes.

GALILEO SECURITY BOARD (GSB) is the body, composed of representatives of European Union (EU) Member States and of the European Commission (EC), set up by the EU Council to deal with all security matters regarding the GALILEO Programme (also known as GALILEO System) and responsible of the establishment and maintenance of this PSI. [to be reviewed in function of governance structure to be agreed in the framework of the European GNSS Implementation Regulation]

GOVERNMENT-TO-GOVERNMENT CHANNELS are transfers of Classified information approved by NSAs/DSAs, either through diplomatic pouch or through other channels approved by the NSAs/DSAs involved.

MATERIAL includes any product, substance, or device in which information is contained, displayed, stored, represented, or embodied. This includes documents as defined above as well as programme equipment.

NATIONAL PROJECT ORGANISATION is the national authority responsible for the coordination of all contractual and sub-contractual activities within the framework of the European GNSS Programmes.

NATIONAL SECURITY AUTHORITY (NSA) is the authority of a participating EU or ESA Member State which is responsible for the maintenance of standards for the security of national, EU or ESA Classified information, at home or abroad.

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 European GNSS Programmes function.

NETWORK is an organisation - geographically disseminated or within a single site - of Information Technology (IT) systems interconnected to exchange data, and comprising the components of the interconnected IT systems and their interface with supporting data or communications network components. Such components may include Automated Information Systems, packet switches, telecommunications controllers, key distribution centres, and technical control devices.

ORIGINAL CLASSIFICATION is an initial determination that information requires protection against unauthorised disclosure in the essential interest of security of the EU or ESA or of national security of participating States.

ORIGINATOR for the purpose of this document means the State or international organisation under whose authority information has been produced.

PARTICIPANTS are those EU and/or ESA Member States and/or international organisations listed on the front page, which are all linked by security agreements or arrangements - whether being bilateral or multilateral -, also covering industrial security and are responsible to co-ordinate the implementation of this PSI.

PARTICIPANTS' CONTRACTORS include any Contractors / Prime Contractors and Subcontractors authorised by the Contracting Agent to take part in the [specific project / phase].

PERSONNEL SECURITY CLEARANCE (PSC) is a determination that an individual is eligible to have access to information classified CONFIDENTIAL and above.

PRIME CONTRACTOR is the contractor who has overall responsibility to the Contracting Agent for completing the work specified in the prime contract. Part of the work may be subcontracted, if duly authorised by the Contracting Agent.

PROGRAMME EQUIPMENT includes any material, end item, subsystem, component, special tooling, or test fixture acquired or provided for use in the European GNSS Programmes of the European GNSS Programmes.

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

PROGRAMME/PROJECT SECURITY INSTRUCTION (PSI) is a compilation of security regulations / procedures, based upon the appropriate security rules and regulations, which are applied to a specific project/programme in order to standardise security procedures. The PSI also constitutes an Annex to a main contract, and may be revised throughout the Programme lifecycle. It is complemented by a Security Classification Guide that is attached to it. For sub-contracts let within the Programme, the PSI constitutes the basis for the SAL

RELEASE TO THE PUBLIC is the passing of information and/or material to the general public, or any member of the general public, by any means of communication.

SECURITY ASPECTS LETTER (SAL) is a set of special contractual conditions, issued by the Contracting Agent, which forms an integral part of a classified contract involving access to or generation of classified information, that identifies the security requirements or those elements of the contract requiring security protection.

SECURITY AUTHORITY is the NSA/DSA or other national authority or a representative of an international organisation competent for security.

SECURITY CLAUSES/CONTRACT SECURITY CLASSIFICATION SPECIFICATION are documents issued by the Contracting Agent or Contractor, as part of any Classified Contract or subcontract, identifying the security requirements or those elements requiring security protection for a Classified Contract.

SECURITY VIOLATION is any knowing, wilful, or negligent action that could reasonably be expected to result in loss, compromise or unauthorized disclosure of Classified Information.

SUBCONTRACT is any contract entered into by a contractor duly authorised by the contracting agent to furnish supplies or services for performance of a prime contract or a subcontract.

SUBCONTRACTOR is a supplier, distributor, vendor or firm, duly authorised by the contracting agent, that furnishes supplies or services to or for a prime contractor or another subcontractor, who enters into a contract with a prime contractor.

TRANSMISSION is the sending of information from one place to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire or other connective media. Transmission also includes movement involving the transfer of classified material from one authorised addressee to another.

THIRD PARTY is any country or international organisation which is not a Participant.

SECTION I

INTRODUCTION

1.1 **BACKGROUND** [to be reviewed in function of the status of the European GNSS programmes]

The European Global Navigation Satellite System (GNSS) consists in two programmes : the EGNOS Programme and the GALILEO Programme.

The GALILEO Programme is the European independent implementation of a GNSS aiming at satisfying all users requirements, composed of three segments:
- the Space Segment (S/S),
- the Regional Augmentation System,
- and the Local Augmentation System, including the User Segment (U/S).

and providing five types of services
- an Open Service (OS),
- a Commercial Service (CS),
- a Safety of Life Service (SoL),
- a governmental Public Regulated Service (PRS),
- and a Search and Rescue service (SAR) contributing to the COSPAS-SARSAT system.

The different segments of GALILEO may provide highly accurate position, velocity, and time information to an unlimited number of properly equipped users anywhere on the ground, at sea, in the air and out in space.
The accuracy provided by GALILEO determines it as a system with strategic potential. As such it must be protected. Therefore the access to documents, hardware and technology that define the details of the system design must be limited.
Although GALILEO will be developed and operated extensively by the civil community, it will contain some key military technologies particularly in satellite design, cryptography, micro-circuitry that would be advantageous to potential hostile forces. Satellite navigation is a force multiplier capable of significantly improving the accuracy of weapons, reducing their numbers required, providing more efficiency to the logistic support and to the key military areas of command, control, communication and intelligence. These issues should be remembered in the formulation of the security requirements and whenever information on the system is released.
It is intended that GALILEO will be used for high integrity operations. As such the detailed design of the system and its operating functions must be protected to ensure that the economic investment is safeguarded.

The EGNOS (European Geostationary Navigation Overlay Service) Programme uses and enhances through three satellites places in geostationary orbit, the information provided by signals from the American GPS and Russian GLONASS satellite constellations. Accurate to within one to two meters, it provides all satellite radionavigation users with a top-quality navigation and positioning service which is better than any available to date in Europe using GPS alone and is close to what GALILEO will be providing in the future, in particular in terms of providing an integrity message.

This manual provides guidance on the protection of the following types of information:

- Information concerning technical advances and breakthroughs in space applications,
- Technical information that could provide adversaries with significant assistance in the use of the system or the design and development of a similar system.

The release of commercial data and information must also be considered as significant investment that will be made by European Industry in the Programmes.

The European Commission has requested the National Security Authorities of those Member States in which the companies involved in the GALILEO Programmes are / may be located to co-ordinate the implementation of the Galileo PSIs.

This PSI is based on

- the European GNSS Implementing Regulation, and in particular its article 10b [1],
- the Security Regulations of the Council of the EU [2],
- the European Commission's provisions on security [3],
- the Agreement between ESA and the EU on the security and exchange of classified information [4],
- the Administrative Arrangement between ESA and the GSA on the security and exchange of classified information [5],
- the ESA Security Regulations [6] and the Agreement between ESA Member States and ESA,
- for the protection and the exchange of classified information [7].

1.2 PURPOSE

This PSI provides instructions on the safeguarding of Classified information and material that is provided or generated on behalf of the [specific project / phase]. Further, this document informs the Contractors of their obligations to prevent espionage, compromise, or unauthorised disclosure of Classified information. It provides instructions for the Participants on the classification of

---

1 Regulation to be adopted by the Council and the European Parliament - the draft art 10b of which reads (still under examination in Council instances) : "1. Member States make applicable to their nationals and to the companies active on their territory and dealing with EU classified information regarding programmes, the Commission security regulations stipulated in the annex of Commission Decision n° 2001/844//CE, CECA, Euratom of 29 November 2001, in particular section 27.
2. The measures referred to in paragraph 1 are taken before 31 December 2008. Member States immediately inform the Commission of these measures.
3. Third countries participating at the deployment phase of the Galileo programme should, beforehand, have concluded an agreement, either with the European Union, or with the European Space Agency, envisaging that, for the course of this phase, their nationals and the companies active in these states are subject to regulations equivalent to those ensuing from the Commission security regulations and from the European Union Council security regulation appearing in the annex of Council Decision of 19 March 2001."

2 Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations, JO L101, 11.4.2001, p. 1, as last amended by Council Decision 2007/438/EC of 18 June 2007.

3 Commission Decision 2001/844/EC, ECSC, Euratom of 20 November 2001 amending its internal Rules of Procedure (notified under document C(2001) 3031), JO L317, 3.12.2001, p. 1, as last amended by Commission Decision 2006/548/ EC, Euratom of 2 August 2006.

4 Insert reference when signed - probably around March 2008.

5 Administrative arrangement to be concluded between ESA and any relevant EU or EC agency (here the GSA) confirming that any exchange of classified information would take place in accordance with the basic principles and minimum standards set out in the ESA-EU agreement and their respective security rules and regulations. (as suggested by the GSC to ESA and acknowledged by ESA in the framework of the negotiations of the EU-ESA agreement referred to above). Insert reference when adopted.

6 ESA Council Resolution on Part I of the Security Regulations adopted on 11 December 2002 at the 161st Council meeting.

7 Agreement between the States Parties to the Convention for the establishment of a European Space Agency and the European Space Agency for the protection and exchange of classified information approved by ESA Council on 13 June 2002.

information and material, security procedures, including the handling and transfer of Classified material, and visit procedures for the [specific project / phase].

1.3 AUTHORITY, APPLICABILITY AND RESPONSIBILITY FOR THIS PSI

1.3.1 Authority

The GSB is responsible for the approval of this PSI and its further modifications. [to be reviewed in function of governance decisions to be taken]

The Security Authority or other relevant authority of each Participant are responsible for developing and updating of this PSI, and of the Security Classification Guide that is attached to it. Requests for clarification of this PSI should be addressed to them as listed in Annexes A1, A2 and A3.

The NPOs report to the Contracting Agent.

The Contracting Agent will co-ordinate the NPOs and report to the GSB.

1.3.2 Applicability

This PSI applies to any governmental organisation, intergovernmental organisation and any company or national entity involved through a contract by contractual or pre-contractual activity in the European GNSS Programmes.

If Classified information is transmitted to a possible sub-contractor or if a Classified contract is granted, the hosting NSA/DSA will be responsible for the control of security measures for the protection of Classified information pursuant to its national laws and regulations provided there are not less stringent than the provisions set out in this document.

The NSA/DSA will fulfil regular security inspections of the cleared facilities to ensure that information is correctly protected. They will check that access to Classified information is limited to appropriately cleared individuals on a need to know basis.

1.3.3 Security Responsibilities

1.3.3.1 Participants' Authorities

The Participants' authorities are those governmental or international organisations / bodies responsible for security of Classified information for the European GNSS Programmes and the coordination and implementation of industrial security aspects of the European GNSS Programmes which are listed in Annex A1 and A2.

1.3.3.2 Participants' Contractors

Contractors are the companies and agencies of Participants acting as Contracting Partners in the [specific project / phase] which are listed in Annex A4.

SECTION II

SECURITY INSTRUCTIONS FOR CLASSIFIED INFORMATION

2.1 GENERAL PRINCIPLES

a) All Classified Information held, used, or generated in connection with the European GNSS Programmes will be stored, handled and safeguarded in compliance with the Participants' rules governing the handling and exchange of Classified information and the provisions set out in this PSI.

b) Access to and handling of information classified CONFIDENTIAL or SECRET will be restricted to entities and individuals that have the requisite level of facility or personnel security clearance and that have a need-to-know for the purposes of the [specific project / phase]. Access to information marked RESTRICTED requires a need to know. FSC and PSC are only required when stated in national laws and regulations.

c) Exchange and transmission of classified information between the Participants will be in compliance with existing applicable bilateral and/or multilateral security agreements / arrangements where applicable.

d) Information classified CONFIDENTIAL or SECRET will be transmitted only through government-to-government channels. Upon receipt, it will either retain its original classification markings or be marked with a classification marking that will assure a degree of protection at least equivalent to that required by this PSI. The classification level cannot be modified without the prior written consent of the originator.

e) Electronic transmission of information classified RESTRICTED is not permitted unless a cryptographic system approved by the Security Authorities of the Participants is used.

f) Electronic transmission of information classified CONFIDENTIAL or above is not permitted unless a cryptographic system approved by the GSB.

g) The minimum requirements to protect GALILEO COMSEC items are set out in the applicable document COMSEC SECURITY INSTRUCTIONS, version 2.0 and subsequent updates.

h) In situations where provision in national legislation and regulations differ from the provisions in this PSI, the provisions in national legislation and regulations should be applied provided they are not less stringent than the provisions set out in this document. In such cases the Security Authorities of the other Participants shall be informed. The differing provisions shall be circulated to all Participants via the GSB.

2.2 SECURITY CLASSIFICATION

Security classifications of the information related to the European GNSS Programmes are as indicated in the table of equivalent security classifications listed in Annex B1.

The fact that any information related to the European GNSS Programmes is not marked with a security classification grading does not mean that it can be released to

the public. Any release of information requires a written authorisation and will be done according to the provisions of section 3.

2.3 SECURITY GRADING

a) Information generated under the European GNSS Programmes will be classified and marked in accordance with the relevant Security Classification Guide. If needed, a double marking detailed in the Classification Guide may be applied. Questions concerning the content and interpretation as well as proposed changes to the Classification Guide will be co-ordinated between the Security Authority or other competent authority of each Participant (s. Annex A1 – A3) and the Contracting Agent. Pending a final decision on proposed changes to classification levels, the information involved will be protected at either the current assigned level or the proposed level, whichever is higher.
The GSB will review the Security Classification Guide at least annually. [to be reviewed in function of governance decisions to be taken]

b) Classified information will be downgraded or declassified only after receiving written approval from the originator..

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

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

e) Classified information, warranting a derivative classification, will be based on a decision by the Participants' authorities.

f) Information generated by the Contractor which requires classification shall be marked using one of the EU security classifications marking.

2.4 MARKINGS FOR European GNSS Programmes CLASSIFIED INFORMATION

Each document will be conspicuously marked or stamped at the top and bottom of the front cover and all pages and the back side of the last page and back side of the back cover with the security classification (e.g. "RESTREINT UE").

Documents and other material containing information provided to (i.e background information) or generated under (i.e foreground information) the European GNSS Programmes will be marked by the originator with a legend reflecting the country of originator, EU or ESA, as appropriate, and in addition to any classification marking, with an annotation that identifies it as European GNSS Programmes information.

Material containing Foreground Information also will be marked to indicate that it was generated under the European GNSS Programmes.

For European GNSS Programmes material that contains Background Information, there will be an annotation that identifies the fact that the material contains Background Information and the country of origin, EU or ESA, as appropriate, in addition to other prescribed markings.

Both Foreground and Background Information will be annotated with a statement that identifies any use, distribution or access limitations. Each Participant providing Background Information will ensure that the appropriate markings are applied prior to release to the European GNSS Programmes.

When the material is of such nature that it cannot be marked, the markings will be applied to a cover or label.

2.5 PROTECTION OF INFORMATION CLASSIFIED CONFIDENTIAL OR SECRET [8]

2.5.1 General principle

Preparation, distribution, transmission, storage and destruction of information classified CONFIDENTIAL or SECRET will be in accordance with national and Community rules and regulations, bilateral or multilateral agreements as applicable.

2.5.2 Access

a) Access to information classified CONFIDENTIAL or SECRET will be restricted to individuals that have both, a need-to-know for the purposes of the [specific project / phase] and the requisite level of Personnel Security Clearance.

b) All persons who are to be given access to Classified information must be informed of and acknowledge their responsibilities for protecting the information.

2.5.3 Transmission

2.5.3.1 Standard Means of International Transmission
The standard means of transmitting Classified information and material across international borders is through government-to-government channels. The government channels to be used for the transfer of the Classified information will be in compliance with the national regulations of the dispatching and receiving Participant. Authorised government channels include the diplomatic or military transmission channels of the Participants' governments, specifically military courier, diplomatic pouch or military postal channels.

2.5.3.2 Transmission to Subcontractor
If Classified information is transmitted to a possible subcontractor or if a classified contract is granted, the Security Authority of the hosting Participant (s. Annex A1)

[8] Chapter renumbered as Chapter 2.6 in GalileoSat PSI v 4.0.

will be responsible for the control of security measures for the protection of Classified information pursuant to its national laws and regulations.
The Security Authority of the hosting Participant (s. Annex A1) will fulfil regular security inspections of the cleared facilities to ensure that information is correctly protected. They will check that access to Classified information is limited to appropriately cleared individuals on a need to know basis.
For any facility where Classified information is to be handled, the Security Authority of the hosting Participant (s. Annex A1) will, in accordance with national laws and regulations, appoint a security officer of sufficient rank responsible for the protection of Classified information and for the restriction of access to such information to those individuals who have a need to know and are appropriately cleared.
Any company which has been identified by the Security Authority of the hosting Participant (s. Annex A1) as being under the financial or administrative control of individuals or entities belonging to a third state will be authorised to participate to a contract requiring access to Classified information of the European GNSS Programmes, only if efficient measures are actually in force to prevent any access to information by individuals or entities of this third State.
The Contractors are obliged, under penalty of termination of their contract, to take all measures prescribed by their parent Security Authority (s. Annex A1) for safeguarding all Classified information entrusted to, generated, or manufactured by the contractor in the framework of the European GNSS Programmes. Furthermore, Contractors on this European GNSS Programmes are equally obliged to follow the provisions of this PSI.

2.5.3.3 Case of urgency

To meet an urgent need to transfer Classified documents and Programme equipment or components between Participants and their Contractors, the responsible Security Authority may approve special arrangements for hand carriage, or delivery by a national mail system or by cleared commercial delivery services. Hand carriage may be used on a case-by-case basis when government channels are not reasonably available, or transmission through government channels would result in an unacceptable delay that will adversely affect performance on the European GNSS Programmes, and it is verified that the information is not available at the intended destination. Classified material being hand carried must be sealed while in transit, may not be opened en route, and requires direct delivery from the secure facility originating point to the secure facility at the destination. The hand carrying of Classified material will be in compliance with the procedures at Annex C. The responsible Security Authority will handle administration of the day-to-day aspects of these procedures. Use of the hand carry procedures is restricted to the approved Contractors in the list of security cleared facilities. Modification of the procedures is not permitted without the approval of the Participants' authorities (s. Annex A1 and A2).

2.5.3.4 International Transmission via Commercial Courriers

In cases of urgency, i.e. only when the standard means for transmission as well as the hand carriage described in the previous paragraphs cannot meet the needs of industry and provided the dispatching and receiving Security Authorities have in principal agreed on this procedure, information classified up to CONFIDENTIAL may be transmitted via commercial courier companies, provided that the following criteria are met:

a) The courier company is located within the territory of the Participating States and has established a protective security Programme for handling valuable items with a

signature service, including a record of continuous accountability on custody through either a signature and tally record or an electronic tracking / tracing system.

b) The courier company must obtain and provide to the Consignor proof of delivery on the signature and tally record, or the courier must obtain receipts package numbers.

c) The courier company must offer that the consignment will be delivered to the Consignee prior to a specific time and date within a 24-hour-period under regular circumstances.

A list of commercial couriers fulfilling these criteria is attached as Annex C2

2.5.3.5 Freight

Items classified CONFIDENTIAL and/or SECRET that cannot be transmitted by one of the methods listed above or where large volumes of Classified equipment are to be conveyed, they may be transported as freight by commercial carriers in line with the following criteria for handling international shipment, as appropriate:

a) hold an appropriate FSC issued by the responsible Security Authority if deemed necessary and according to national security regulations;
b) be authorised by laws or regulations of Participant where the carrier is located to provide international transportation services;
c) be obligated to comply with safety, security and emergency procedures which must be observed.

The transmission of Classified material as freight within a Participant's country will be in accordance with approved national procedures provided they result in a degree of protection commensurate with this PSI.

The consignor and the consignee are responsible for jointly organising the transport and for its notification to their respective Security Authority who should jointly approve the transportation plan prior to the shipment. The Transportation Plan will include at least the information shown in the example located in Annex D of this PSI.

The following principles shall be enforced when examining proposed security arrangements for the international transportation of consignments of Classified equipment:

a) security shall be assured at all stages during the transportation and under all circumstances, from the point of origin to the ultimate destination;
b) the degree of protection accorded to a consignment shall be determined by the highest classification level of equipment contained within it;
c) a FSC shall be obtained, where appropriate, for entities providing transportation. In such cases, personnel handling the consignment shall be cleared according to an appropriate level;
d) journeys shall be point-to-point to the extent possible, and shall be completed as quickly as circumstances permit, and
e) care shall be exercised to arrange routes only through Participants. Routes through non participating states should only be undertaken when authorised by the Security Authorities of the consignor and the consignee.

Arrangements for consignments of Classified equipment shall be agreed between the Security Authorities concerned. However, such arrangements shall ensure that there is no risk of unauthorised access to Classified equipment.

2.5.3.5.1 Transportation by road

The following standards shall be applied when consignments of Classified equipment are transmitted by road transportation:

a) if required by national rules and regulations, the carrier, the driver and/or co-driver must be security cleared up to the level of the classification of the consignment.
b) the equipment will be secured in vehicles or containers by a lock or padlock, closed van or cars that may be sealed;
c) containers must bear no visible indication of their contents;
d) consignments will be transported point-to-point;
e) where appropriate the Security Authorities will advise their customs or other relevant national authorities of impending consignments and should be urged to give maximum priority to the shipment.

If the Classified consignment cannot be secured as described above, the consignment should be encased or sheathed so as to protect the classified aspects and prevent unauthorised persons from gaining access.

2.5.3.5.2 Transportation by rail

Transportation by rail may be used for consignments of Classified equipment on the basis of the following condition: passenger accommodations shall be made available for security guard personnel and during stops the security guard shall remain with the consignment.

2.5.3.5.3 Transportation by sea

The following standards shall be applied when consignments of classified equipment are sent by sea:

a) a cleared guard or escort shall accompany the consignment;
b) equipment shall be stowed in locked stowage space approved by the Security Authority of the consignor. The consignment must be under security control;
c) stops at maritime countries presenting special security risks shall be assessed by the Security Authorities of the consignor/consignee. Unless the ship is in emergencies, it shall not enter the territorial waters of any of these countries without the authorisation of the Security Authorities concerned;
d) stops at any non Participating States' port shall not be permitted unless prior approval of the consignor's Security Authority has been obtained;
e) in all cases, loading and unloading shall be under security control;
f) deliveries to the port of embarkation and collection from the port of disembarkation must be so timed to prevent, as far as possible, a consignment being held in port warehouses.

2.5.3.5.4 Transportation by air

An air carrier may be used provided the following standards shall be applied:

a) airlines of Participants shall normally be used. However in exceptional circumstances such as the extreme size of the consignment, airlines of non Participating States may be used in consultation with the Security Authority of the consignor;
b) the consignment shall be delivered straight to the aircraft rather than being stored in warehouses, etc.. at airports, airfields. A sufficient number of security guards must be provided to keep the consignment under adequate supervision;
c) every effort shall be made for the aircraft to be met on landing and the consignment to be removed at its final destination.
d) intermediate routine stops of short duration may be permitted, provided the consignment shall remain in the aircraft;
e) in the event the aircraft is delayed at an intermediate stop or has to make an emergency landing, the security guard shall take all measures considered necessary for the protection of the consignment;
f) direct flights shall be used whenever possible and, except in an emergency, stops at airfields in non Participating States shall not be permitted unless the final destination is in the same non Participating State.

2.5.3.5.5 Security Guards and Escorts

Individuals fulfilling the duties of security guards may be armed or unarmed depending on national practices and arrangements made between the Security Authorities of the Member States affected by the transportation. They must be nationals of Participant States and be security cleared at the appropriate level

The security guard/escort shall be composed of an adequate number of personnel to ensure regular tours of duty and rest. Their number shall depend on the classification level of the equipment, the method of transportation to be used, the estimated time in transit and the quantity of equipment will also be considered.

It is the responsibility of the consignor and, where applicable, the consignee to instruct security guards in their duties. Security guards may, if appropriate, also be given a copy of "Notes for the Courier" and be required to sign a receipt for it.

2.5.4 Use of Automated Information Systems (AIS)

a) During transmission the confidentiality of Classified information at SECRET or equivalent level shall be protected by cryptographic methods or products approved, after a successful evaluation[9], by the GSB upon recommendation of GSB WG1. [to be reviewed in function of governance decisions to be taken]

[9] Evaluation
In the case of cryptographic products to be used to protect the confidentiality of Galileo related classified information, evaluation and approval by an EU Council approved "appropriately qualified authority" in an PSI Member State needs to be supplemented by additional safeguards:
a. As a general rule, products designed and produced in one or more PSI Member States of the GalileoSat Programme shall be used;
b. In all cases, the product shall be subject to an additional evaluation by an appropriately qualified authority (AQUA) in another Member State not involved in its design or manufacture.

During transmission of information classified at CONFIDENTIAL or RESTRICTED or equivalent level it shall be protected by cryptographic methods or products approved either by the GSB [to be reviewed in function of governance decisions to be taken] or approved by a Member State's NSA/DSA.

The GSB [to be reviewed in function of governance decisions to be taken] shall be notified of any deployment of equipments to be used for the transmission of Classified information related to the European GNSS Programmes.

b) Information classified CONFIDENTIAL or SECRET will be processed and stored in AIS appropriately accredited for classified information.

2.6 PROTECTION OF RESTRICTED INFORMATION [10]

2.6.1 General Principle

Documents or other media that contain RESTRICTED information, will be protected as below in order to ensure the common minimum standards of protection by all Participants.

2.6.2 Access/Handling

a. Only where required by national regulations, Contractor facilities that require handling of RESTRICTED information must be security cleared.

b. The information will be provided only to facilities or persons who need to know the information in connection with their involvement in the European GNSS Programmes.

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

2.6.3 Protection

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

2.6.4 Transmission

[10] Chapter renumbered as Chapter 2.5 in GalileoSat PSI v 4.0.

a. Documents or other media containing RESTRICTED information as well as material classified RESTRICTED may be transmitted within the Participants' countries by a national mail system or by non-cleared commercial delivery services.

b. Double envelopes or wrappings are required. The envelope or wrapping will be opaque and will not reveal that the package contains RESTRICTED information.

c. The international transmission of Documents or other media containing RESTRICTED information as well as material classified RESTRICTED should be through international postal channels or commercial delivery services approved by the Security Authorities.

d. RESTRICTED informationshould be transmitted or accessed electronically via a public network like the Internet, using an encryption system nationally approved and mutually accepted by the Participants. [11]

2.6.5 Destruction

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

2.6.6 Reproduction

The reproduction of RESTRICTED information will be limited to that which is necessary in support of a contract related to the European GNSS Programmes.

2.6.7 Use in Local Automated Information Systems (AIS)

RESTRICTED information will be processed and stored in accredited / approved AIS in accordance with national regulations, bilateral or multilateral agreements as applicable.

2.7 SECURITY VIOLATIONS

a) All Participants' personnel and Contractors shall report the actual or possible loss or compromise of Classified information to their security office. The security office will report the incident to their parent/host Security Authority in addition to reporting procedures prescribed by national, EU or ESA security regulations. Similarly the security officer of the facility where a violation or compromise may have occurred will investigate all such occurrences and inform their parent/host Security Authority of the results. The responsible Security Authority will promptly and fully inform the other Participants' Security Authorities and GSA of the known details of any such occurrences, will provide updates on and a final report of the investigation and of the corrective actions taken to preclude recurrences.

[11] Either this generic formulation or the more specific formulation referring to Chiasmus as in the GalileoSat PSI v 4.0 : "using the encryption system Chiasmus for windows as approved by the GSB." To be decided upon.

b) Reports on the compromise or possible compromise shall include the following details:
   - a description of the circumstances,
   - the date or the period of the occurrence,
   - the date and place of discovery and location of the occurrence,
   - the security classification and markings of the information involved in the incident,
   - specific identification of the information or material, to include originator, subjects, reference, date, copy number, and language,
   - a list of the information that has been compromised or material that is unaccounted for,
   - responsible person(s) and reasons for loss or compromise or possible loss/compromise,
   - assessments of the likelihood of compromise (i.e., "certain," "probable", "possible," or "unlikely") including an explanation,
   - a statement on whether the originator has been informed,
   - actions taken to secure the material and limit further damage.

c) The above reporting requirements are in addition to any other reporting requirements of the Participants, required by national, EU or ESA security regulations.

d) Reports of investigations involving CONFIDENTIAL information and above must be provided to the Security Authorities involved within 90 days.

SECTION III

RELEASE OF INFORMATION

3.1 UNILATERAL RELEASE OF CLASSIFIED INFORMATION AND MATERIAL

The unilateral release of Classified European GNSS Programmes information and material to other than European GNSS Programmes Participants and their Contractors is prohibited without specific written approval of the country or international organisation originating the information. Requests for release will be handled in accordance with the paragraphs below.

3.2 RELEASE OF CLASSIFIED INFORMATION AND MATERIAL TO THIRD PARTIES

Release of Classified information and material related to the European GNSS Programmes to third parties will be restricted to those individuals who have demonstrated a need to know for purposes of performance of the European GNSS Programmes and hold an appropriate PSC.

a) European GNSS Programmes information (except that which has been approved for public release in accordance with paragraph 3.4 below) may only be released to Third Parties or their Contractors, with the prior written approval of
   - the Participant originating the Background Information
   - all Participants in regard with Foreground information.

b) Requests for release will be submitted through the Contracting Agent or the NPOs to the Participants' authorities.

3.3 RELEASE OF CLASSIFIED European GNSS Programmes INFORMATION AND MATERIAL AT SYMPOSIA, SEMINARS AND CONFERENCES

Release of Classified information and material at symposia, seminars, conferences and workshops, regarding the European GNSS Programmes must be approved in advance by the Participants' Security Authorities in co-ordination with the Contracting Agent and the GSB [to be reviewed in function of governance decisions to be taken]. The Contractor will submit through the Contracting Agent or the NPOs the particulars of the classified meeting in advance with sufficient time to allow the relevant Security Authorities to ascertain the extent of the Classified information access and disclosures, and determine the organisation and composition of the proposed audience. Detailed requests for permission to release Classified information shall be submitted to the competent Security Authority a minimum of 45 days before the proposed date of release. Requests will include the name of the requesting individual, date of presentation, third parties represented, title of the symposium or seminar, and other information which may be required by national regulations.

3.4 PUBLIC RELEASE OF European GNSS Programmes INFORMATION

Only unclassified information may be considered for release to the public, provided that written approval for public release of all Foreground and Background Information, including papers, advertising, brochures, displays, web pages, and other publicity material, will be sought in writing through the competent NPO. Contractors must ensure that subcontractors follow the same procedures. The NPO may reject such proposals without further recourse. The Participant's NPO will grant or deny release in accordance with national rules and regulations. A minimum of 45 days shall be allowed for review of the proposal.

It is incumbent upon the Participants to screen all information submitted to them for public release to ensure that:

- it is unclassified,
- it is technically accurate, and
- release will not harm the essential interests of the Participants or of the Programmes.

3.5 EXHIBITION AUTHORISATION

Contractors that display European GNSS Programmes information and material at exhibitions (e.g., at Air Shows, International Exhibitions, etc.) must have a copy of the document that provides authorisation for the display available at each exhibition. Contractors must ensure that all information is displayed in the form in which it was officially authorised for release.

SECTION IV

INTERNATIONAL VISITS

4.1 GENERAL

a) Each Participant will permit visits involving access to Classified information to their national (governmental) facilities or the facilities of the Contracting Agents or of the Contractors by representatives of another Participant, by Contractor employees or staff of international organisations listed in Annex A2.2 (Non-Participants).

b) These visits are subject to the following conditions:
- the visit has an official purpose related to the European GNSS Programmes,
- the facility to be visited has the appropriate Facility Security Clearance,
- the visitor has an appropriate security clearance and a need to know.

c) Visits must be requested by:
- the Security Officer for Contractor employees,
- the Security Officer or other representative of the NSA/DSA for representatives of a Participant State,
- the Security Officer or other representative of the organisation competent for security for staff of an international organisation.

d) All visiting personnel will comply with security regulations of the host Participant. Any Classified information disclosed or made available to visitors will be treated as if supplied to the Participant sponsoring the visiting personnel and will be protected accordingly.

e) To confirm his/her identity, the visitor must be in possession of an ID card or passport for presentation to the Security Officer of the receiving facility.

4.2 PROCEDURES FOR INTERNATIONAL VISITS

4.2.1. Visits arranged directly

a) The arrangements described in the following paragraphs apply to Contractors and representatives of Participants who need to undertake visits to the facilities of the Contracting Agent, Contractors or their subcontractors involved in the European GNSS Programmes listed in Annex A, and need access to classified information at CONFIDENTIAL or SECRET level.

b) Prior to arrival at a facility involved in the European GNSS Programmes, confirmation of the visitor's Personnel Security Clearance must be provided directly by the Security Officer of the sending facility to the receiving facility,
- for contractor personnel by using the RfV form in Annex E1
- and for representatives of Participants by using the RfV in Annex E2.

c) It is the responsibility of the Security Officer of:
- the sending facility to ensure with their Security Authority that the company facility to be visited is in possession of an appropriate Facility Security Clearance,
- both the sending and the receiving facilities to agree that there is a need for the visit.

d) The receiving facility Security Officer must ensure that records are kept of all visitors, including their names, the organisation they represent, the date of expiry of the Personal Security Clearance, the date of the visit and the name(s) of the person(s) visited. Such records are to be retained for a period no less than two years.

e) The Security Authority of the host Participant has the right to require prior notification from their facilities to be visited for visits of more than 21 days duration. This Security Authority may then grant approval, but should a problem arise it will consult with the Security Authority of the visitor.

4.2.2. Visits arranged through Security Authorities requiring a standard International Request for Visit (RfV)

a) The arrangements described in the following paragraphs apply to visits of
- staff members of non participating international organisations to the facilities of Contractors or their subcontractors involved in the European GNSS Programmes located in one or more of the Participants,
- Contractors to the Contracting Agents

involving access to classified information at CONFIDENTIAL or SECRET level.

Visits of representatives of Participants to these facilities will be handled as in 4.2.1.

b) A standard International Request for Visit (RfV, Annex E2) should be sent at least 21 days prior to the visit to the parent Security Authority of the staff member or Contractor who requires access to Classified information. When the facility is located in a Participant other than the parent State of the visitor, the Security Authority will send the RfV to the Security Authority of the facility to be visited.

4.2.3. Visits relating to information classified RESTRICTED

Visits relating to information classified RESTRICTED will be arranged directly between the sending facility and the receiving facility.

4.3 LIST OF FACILITIES

Each Participant will prepare and maintain a consolidated list, known as the " List of facilities", of the participating government or international organisation, Contracting Agent and contractor facilities (see Section IV). Only those facilities listed on the "Facilities List" will be authorised to submit RfVs or receive visitors in connection with the [specific project / phase] Contract.

SECTION V

SUBCONTRACTING

5.1 NATIONAL SUBCONTRACTS

a) Before entering into negotiations for a subcontract or order involving the release of European GNSS Programmes Information classified CONFIDENTIAL or above to a company in his/her own country, the Security Officer of the company letting the contract will ask his parent Security Authority for an FSC verification for the potential Subcontractor. The FSC Information Sheet (FIS) at Annex F will be used.

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

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

5.2 INTERNATIONAL SUBCONTRACTS

a) Prior to letting a subcontract with a company in another Participating State, or outside any of the Participating States, the Security Officer of the company that wishes to let the subcontract will first obtain the approval of the Contracting Agent. The above requirements also will be required for such international subcontracts.

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

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

5.3 RESPONSIBILITY

For any facility where Classified information is to be handled, the Security Authority of the facility will, in accordance with national laws and regulations and with ESA and EC security regulations where applicable, appoint a Security Officer of sufficient rank responsible for the

protection of Classified information and for the restriction of access to such information to those individuals who have a need to know and are appropriately cleared.
The Security Authority of the hosting Participant (s. Annex A1) will fulfil regular security inspections of the cleared facilities to ensure that information is correctly protected. They will check that access to Classified information is limited to appropriately cleared individuals on a need to know basis.

Any company which has been identified by the Security Authority as being under the financial or administrative control of individuals or entities belonging to a third State will be authorised to participate to a contract requiring access to Classified information of the European GNSS Programmes only after approval of the GSB and if efficient measures are actually in force to prevent any access to information by individuals or entities of this third State.

The Contractors are obliged, under penalty of termination of their contract, to take all measures prescribed by their parent Security Authority for safeguarding all Classified information entrusted to, generated, or manufactured by the Contractor in the framework of the European GNSS Programmes. Furthermore, Contractors on this European GNSS Programmes are equally obliged to follow the provisions of this PSI.

5.4 TRANSMISSION TO SUBCONTRACTOR

Before any transmission of Classified information to a subcontractor, the Security Authority of the recipient Participant (s. Annex A1) will on request make sure that the facility of the subcontractor is security cleared or grant a FSC, where appropriate.

SECTION VI

LISTING OF SECURITY CLEARED FACILITIES

6.1 INTRODUCTION

This section outlines the procedures for the development and maintenance of the list of Government organisations and Contractor and Subcontractor facilities that are involved in the European GNSS Programmes and to which information or material classified CONFIDENTIAL or above can be distributed.

6.2 LIST OF SECURITY CLEARED FACILITIES

Each Participant will prepare a list of the government and contractor facilities participating in the European GNSS Programmes (Facility List). The level of FSC and storage capability of each Contractor facility will be verified by each Participant's Security Authority prior to the facility being placed on the list.

6.3 DISTRIBUTION OF FACILITY LIST

After validation, this Facility List will be included in Annex A4 of this PSI and distributed to each Participant's Security Authority.

6.4 UPDATED FACILITY LIST

The Security Authority of a Participant will notify the Security Authority of the other Participants immediately of any changes regarding security status of facilities on the list. The Contracting Agent will also be notified of any approved additions or deletions to the Facilities list. The Contracting Agent will disseminate amendments to the Facilities List, as required, and will issue an updated Facilities List on a regular basis.

6.5 USE OF THE FIS

An Example of the FSC Information Sheet (FIS) is at Annex F. The FIS is used when there is a need to request or to verify Facility Security Clearances.

SECTION VII

SECURITY PLAN IN EVENT OF TERMINATION

7.1 PURPOSE

The purpose of this section is to describe procedures by which the Participants and Contractors will dispose of Background and Foreground information relating to the European GNSS Programmes Contract in any of the following events:

a) A Participant terminates the Contract.
b) The Contract expires.
c) A potential Contractor receives or generates information through a proposal process or an ITT procedure, and is not selected.
d) A Contractor receives and generates information and/or hardware during an early phase of the European GNSS Programmes and is not selected for work on a further phase of the European GNSS Programmes.

The responsible Contracting Agent will ensure that the terms of this section are included as an obligatory requirement of each contract let.

7.2 GOVERNMENT HELD INFORMATION

In the event of termination or expiry of a European GNSS Programmes Contract, the Participants' respective rights and responsibilities with regard to Background and Foreground information relating to the European GNSS Programmes will be determined by the Contracting Agent.

A Participant that is authorised to retain Classified information must safeguard it in accordance with this PSI and national security regulations or ESA or EC Security Regulations, as applicable. The Participant will protect Classified information as described in the Security Classification Guide, and will not use that information for other purposes without prior written consent of the originating Participant.

7.3 CONTRACTOR HELD INFORMATION

a) All Classified information related to the European GNSS Programmes Contract shall remain the property of the Participants.

b) Classified information released within the context of a European GNSS Programmes Contract, whether the recipient participates in the bidding or not and whether the bidder was successful or not, must be returned/destroyed according the following provisions:
   - In the case where the recipient/contractor is not successful: All invitations to bid in respect of Classified contracts will contain a clause requiring a potential contractor who does not submit a bid to return all documents which were provided to enable him to submit a bid to the Contracting Agent by the date set for the opening of bids. Similarly, an unsuccessful bidder will be required to return all documents after a stipulated period of time (normally within 15 days after notification that a bid or negotiation proposal was not accepted).
   - When the bidder was successful and the contract terminated, he must:
     -- return all Classified information to the Security Authority, or to the Contractor that let the sub-contract, unless – only in the case of

information classified RESTRICTED – it has been destroyed, or its retention has been duly authorised with the approval of the Security Authority, or the Contractor, as applicable;

-- ensure that destruction is regulated and recorded following the relevant security rules and regulations.

c) In the event that a FSC is withdrawn, the Contractor must return all Classified information to the Contracting Agent or dispose of such information in accordance with instructions from the Security Authority concerned.

ANNEX A

PARTICIPANTS' AUTHORITIES, INTERNATIONAL ORGANISATIONS (PARTICIPANTS AND NON-PARTICIPANTS), PARTICIPANTS' PROJECT ORGANISATIONS, LIST OF European GNSS Programmes CONTRACTORS

A1 SECURITY AUTHORITIES OF THE PARTICIPATING NATIONS

Austria

NSA

Bundeskanzleramt/Büro der Informationssicherheitskommission,
Federal Chancellery/Office of the Information Security Commission
Ballhausplatz 2,
1014 Wien
Österreich

Ing. Gerald TROST, BSc
Telephone: +43 1 53115/2749
Fax: +43 1 2697861
E-Mail: gerald.trost@bka.gv.at

DSA

Bundesministerium für Verkehr, Innovation und Technologie/
Federal Ministry of Transport, Innovation and Technology
Sektion I/Abteilung CS3 - Recht und Koordination/
Division I/Department CS 3 – Legal Services and Coordination
Radetzkystraße 2
1030 Wien
Österreich

Mag. Michael LUCZENSKY
Bundesministerium für Verkehr, Innovation und Technologie
Federal Ministry for Transport, Innovation and Technology
Sektion I/ Präs. 3 - Recht und Koordination
Division I/ Präs. 3 - Legal Services and Coordination
Tel. +43 1 711 62 65 7408
Fax: +43 1 711 62 65 7499
GSM: +43 664 8188928
E-Mail: michael.luczensky@bmvit.gv.at

Point of Contact for standard Requests for Visits (RfV)

Mag. Michael LUCZENSKY
Bundesministerium für Verkehr, Innovation und Technologie
Federal Ministry for Transport, Innovation and Technology
Sektion I/ Präs. 3 - Recht und Koordination
Division I/ Präs. 3 - Legal Services and Coordination
Tel. +43 1 711 62 65 7408
Fax: +43 1 711 62 65 7499
GSM: +43 664 8188928
E-Mail: michael.luczensky@bmvit.gv.at

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 - Point of Contact for standard Requests for Visits (RfV)

Ministry of DEFENCE
General Intelligence and Security Service (SGRS)
Security Division-Military and Industrial Security
Quartier Reine Elisabeth-Bloc 14S
Rue d'Evere, 1
B-1140 BRUSSELS
BELGIUM

Bulgaria

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Cyprus

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Czech Republic

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Denmark

NSA

Politiets Efterretningstjeneste (the Danish Security Intelligence Service)
Klausdalsbrovej 1
DK – 2860 Søborg
Telephone: + 45 33 14 88 88
Fax: + 45 33 43 01 90
E-mail: rpchg@politi.dk

DSA

Forsvarets Efterretningstjeneste (the Danish Defence Intelligence Service)
Kastellet 30
DK – 2100 Copenhagen Ø
Telephone: + 45 33 32 55 66
Fax: + 45 33 93 13 20
E-mail: milsik@fe-ddis.dk

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Estonia

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Finland

NSA

Ulkoasiainministeriö
Turtvallisuusyksikkö / HAL-07
Laivastokatu 22
PL 176
FI-00161 Helsinki
Finland

Telephone:	+358-9-16 05 55 10 (Erkki Väätäinen)
	+358-9-16 05 64 87 (Timo Repo)
Fax:	+358-9-16 05 55 16
email:	Erkki.Vaatainen@formin.fi
	Timo.Repo@formin.fi

DSAs

1. Industrial Security issues, general matters

Puolustusministeriö/DSA
Eteläinen Makasiinikatu 8
PL 31
FI-00131 Helsinki
Finland

Telephone :	+358-9-160 88 307 (Juha Pekkola)
	+358-9-160 88 311 (Matti Kesäläinen, Galileo POC)
Fax :	+358-9-160 88 278
Email :	juha.pekkola@defmin.fi
	matti.kesalainen@defmin.fi

2. FSCs (both defence and civilian related) and PSCs (only defence related) :

Pääesikunta
Tutkintaosasto/DSA
Fabianinkatu 2
PL 919
FI-00131 Helsinki
Finland

Telephone :	+358-9-181 0111 (Juha Putkonen)
Fax :	+358-9-181 22 069
E-mail :	juha.putkonen@mil.fi

3. Personal Security Clearances (civilian cases)

Please contact Finnish NSA

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

France

NSA for Policy and National Regulations

Secrétariat Général de la Défense Nationale
51 Boulevard de Latour-Maubourg
75700 Paris
France

Telephone: +33 1 71 75 81 91
TELEX: SEGEDEFNAT 20 00 19
Fax: +33 1 71 75 82 00

DSAs for Implementation

Délégation Générale pour l'Armement
Département Central de la Sécurité de Défense et de l'information
(DGA/ SDI)
7 rue des Mathurins
92221 Bagneux Cedex
France

Mr. François David
Chief Industrial & industrial Security Dpt
Telephone: +33 1 46 19 69 49
Mr. Guido Venditti
Assistant
Telephone: +33 1 46 19 70 00
TELEX: 27 00 03 DEFNAT PARIS
Telegraphic Address: DELEGARM CABSECUR
Fax: +33 1 46 19 69 51

Centre National d'Etudes Spatiales (CNES)
Fonctionnaire de Sécurité de Défense
CNES/DG/FD

2 Place Maurice Quentin
75039 Paris Cedex 01
France

Tel: +33 1 44 76 75 19
Fax: +33 1 44 76 78 39

Point of Contact for standard Requests for Visits (RfV)

from France to abroad
Mr. Christophe Thireau (assistant)
Tel: +33 1 46 19 69 76
Fax: +33 1 46 19 69 51

from abroad to France
Mr. Matthieu Nicolo (assistant)
Tel: +33 1 46 19 69 89
Fax: +33 1 46 19 69 90

Germany

NSA

Federal Ministry of the Interior
Referat IS 4
Alt-Moabit 101 D
11014 Berlin
Germany

Telephone: +49 1888 681 1969
Fax: +49 1888 681 51969

DSA

Federal Ministry of Economics and Technology
Division of Industrial Security: Security control, International affairs
Villemombler Str. 76
53123 Bonn
Germany

Telephone: +49 228 615 25 23
Fax: +49 228 615 26 76

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Greece

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Hungary

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Ireland

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Italy

NSA/DSA

ANS/UCSi
PRESIDENZA DEL CONSIGLIO DEI MINISTRI
AUTORITA' NAZIONALE PER LA SICUREZZA
UFFICIO CENTRALE PER LA SICUREZZA
Via di S.Susanna, 15
00187 ROMA

Telephone: +39 06 61 29 75 29
Fax: +39 06 48 852 73 or 00 39 06 61 29 70 04
E-mail: pdc1@palazzochigi.it
mg3439@mclink.it

Point of Contact for standard Requests for Visits (RfV)

Mr. Mariani Carlo
ANS/UCSi
PRESIDENZA DEL CONSIGLIO DEI MINISTRI
AUTORITA' NAZIONALE PER LA SICUREZZA
Industrial Security Division
Via di S.Susanna, 15
00187 ROMA

Telephone: +39 06 61 17 43 28
Fax: +39 06 48 85 273

Latvia

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Lithuania

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Luxembourg

NSA/DSA

Boîte postale 2379
1023 Luxemburg

Telephone: +352 478 2210
Fax: +352 478 2243
E-Mail: carlo.mreches@me.etat.lu

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Malta

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Netherlands

NSA/DSA

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

Point of Contact for standard Requests for Visits (RfV)

Netherlands Industrial Visit Control Office, NIVCO

Telephone: +31 70 320 0331
Fax: +31 70 327 9430

Norway

NSA

Norwegian National Security Security Authority
P.O. Box 14
N-1306 Bærum postterminal
NORWAY

Telephone: +47 67 86 40 00
Fax: +47 67 86 40 09

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Poland

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Portugal

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Romania

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Slovakia

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Slovenia

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Spain

NSA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,500
E-28023 Madrid
Telephone: +34 91 372 50 27
Fax: +34 91 372 58 08
E-mail: nsa-sp@areatec.com

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Sweden

NSA/DSA

Security Secretariat
Ministry for Foreign Affairs
SE-103 39 STOCKHOLM
Sweden

Telephone: +46 8 405 10 00
Fax: +46 8 723 11 76

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Switzerland

NSA

Telephone:
TELEX:
Fax:
E-Mail:

DSA

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

United Kingdom

NSA/DSA (also for Requests for Visits (RfV)

British National Space Centre
Kingsgate House
66-74 Victoria Street
London
SW1E 6SW
United Kingdom

Mr John R Davey
Telephone: +44 20 7215 5862
Fax: +44 20 7215 0804
E-mail: john.davey@bnsc.gsi.gov.uk

A2 INTERNATIONAL ORGANISATIONS

A2.1 SECURITY AUTHORITIES OF PARTICIPATING INTERNATIONAL ORGANISATIONS

ESA

Security Authority

Telephone:
TELEX:
Fax:
E-Mail:

(possibly) local Security Officer

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:

Fax:
E-Mail:

European Commission

Security Authority

Telephone:
TELEX:
Fax:
E-Mail:

GSA local Security Officer

Telephone:
TELEX:
Fax:
E-Mail:

Point of Contact for standard Requests for Visits (RfV)

Telephone:
TELEX:
Fax:
E-Mail:

Council of the European Union, Office of the Secretary General / High Representative, General Secretariat of the Council

Security Authority

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

Telephone: +32 2 281 8517
TELEX:
Fax:
E-Mail:

A2.2 SECURITY CLEARED STAFF MEMBERS OF NON-PARTICIPANTS

[if any]

A2.3 SECURITY CLEARED FACILITIES OF THE PARTICIPATING INTERNATIONAL ORGANISATIONS

Country	Name	Address	Security Officer (Name, Tel, Fax, Email)	Project Leader (Name, Tel, Fax, Email)
The Netherlands	ESA Galileo Project Office	ESTEC Keplerlaan 1 PO Box 299 NL-2200 AG Noordwijk ZH	Nathalie GAY Tel: +31 71 565 3904 Fax: +31 71 565 4369 nathalie.gay@esa.int	Javier BENEDICTO RUIZ Tel: +31 71 565 3738 Fax: +31 71 565 4369 javier.benedicto@esa.int
Belgium	GSA			

A3 NATIONAL PROJECT ORGANISATIONS

Austria

National Project Office

Österreichische Forschungsförderungsgesellschaft/Austrian Research Promotion Agency
Bereich Luft- und Raumfahrt/Aeronautics and Space Agency
Sensengasse 1
1090 Vienna
Österreich

Dipl.-Ing. Dr. Stephan MAYER
Telephone: +43 057755/3305
Fax: +43 057755/9330
E-Mail: stephan.mayer@ffg.at

Belgium

Bulgaria

Cyprus

Czech Republic

Denmark

Estonia

Finland

National Project Office

Mr Esa Panula-Ontto
Tekes, the National Technology Agency
P.O. BOX 69, FI-00101 Helsinki Finland
Tel. +358 10 521 5853
Fax. +358 10 521 5901
e-mail. Esa.Panula-Ontto@tekes.fi

France

National Project Office

Délégation Générale pour l'Armement
Direction des systèmes de forces et des stratégies, industrielle, technologique et de coopération

2 rue des Mathurins92221 Bagneux Cedex
FRANCE

Project leader : ICA (Col.) Benoit Laurensou
Office Symbol : DGA/ D4S/SASF
Telephone : +33 1 46 19 72 93
Fax :
E-mail : benoit.laurensou@dga.defense.gouv.fr

Security Officer : Mr Louis Allanic
Office Symbol : DGA/D4S/BSD
Telephone : +33 1 46 19 71 62
Fax : +33 1 46 19 71 61

National Expert

Délégation Générale pour l'Armement
Direction de l'expertise technique
Laboratoire de Recherche Balistiques et Aérodynamiques

27207 VERNON CEDEX
FRANCE

Project leader : Mr. André Lanciano
Office Symbol : DGA/ DET/LRBA/SDA
Telephone : +33 2 27 24 42 58
Fax : +33 2 27 24 44 58
e-mail : andre.lanciano@dga.defense.gouv.fr

Security Officer : Mr Fabrice Saunier
Office Symbol : DGA/LRBA/OS
Telephone : +33 2 27 24 41 72
Fax : +33 2 27 24 44 94

CELAR : Centre d'électronique de l'armement
Boite postale 7
35998 Rennes Armees
Project Leader : Mr Pascal Chantrenne
Telephone: +33 2 99 42 90 11

CNES : Centre National d'études spatiales
BP 2518
18, Avenue Edouard Belin
31055 Toulouse Cedex
Project Leader : Mr Alain Brissaud
Telephone: +33 5 61 27 31 31

Germany

National Project Office

Deutsches Zentrum für Luft- und Raumfahrt (DLR)
Königswinterer Str. 522-524
53227 Bonn

Dr. Ulrich Theis
Telephone: +49 228 447 231
Fax: +49 228 447 703
E-mail: ulrich.theis@dlr.de

National Expert

BSI (Bundesamt für Sicherheit in der Informationstechnik)
Project Leader : Mr. Frank Christophori

VS-Registry
Mainzer Str. 84
53179 Bonn-Mehlem (Germany)
Telephone: +49 228 9582812

Greece

Hungary

Ireland

Italy

Latvia

Lithuania

Luxembourg

National Project Office

Dr. Marc Serres
ESA Programmes

Ministry for Culture, Higher Education and Research
Research and Innovation
20 Montée de la Pétrusse
L-2912 Luxembourg

Tel.: +352 478-6643
Fax: +352 460927
e-mail: Marc.Serres@mcesr.etat.lu

Malta

The Netherlands

National Project Office

Nederlands Instituut voor Vliegtuigontwikkeling en Ruimtevaart (NIVR)
Kluyverweg 1
2600 AA Delft

Project Leader
W. van der Meulen
Telephone: +31 (0)15 – 27 89 485
Fax: +31 (0)15 – 26 23 096
E-mail: W.vanderMeulen@NIVR.nl

Norway

National Project Office

Norwegian Spacecentre
Drammensveien 165
Po. Box 113 Skøyen
N-0212 Oslo

Lars Giske
Telephone:
Fax:
E-mail: lars.giske@spacecenter.no

Poland

Portugal

Romania

Slovakia

Slovenia

Spain

Sweden

National Project Office

Swedish National Space Board
Box 4006
SE-17104 SOLNA
Telephone: +46 8 627 6480
Fax: +46 8 627 5014

Switzerland

The United Kingdom

National Project Office

British National Space Centre
Kingsgate House
66-74 Victoria Street
London
SW1E 6SW
United Kingdom

Mr John R Davey
Telephone: +44 20 7215 5862
Fax: +44 20 7215 0804
E-mail: john.davey@bnsc.gsi.gov.uk

National Expert

BNSC (British National Space Center)
Project Leader : Mr. Antony John Anderson

Mr. John Owen
DSTL
Air Systems, Navigation Department,
Room 1037, A2 Building
DSTL Farnborough
Hants. GU14 0LX (UK)
Telephone: +44 1252455546

A4 LIST OF COMPANIES AND SITES INVOLVED IN [SPECIFIC PROJECT / PHASE] SECURITY ACTIVITIES

[to be included, possibly copied from GalileoSat PSI]

Country	**Company Name**	**Address**	**Security Officer (Name, Tel, Fax, E-Mail)**	**Project Leader (Name, Tel, Fax, E-Mail)**

ANNEX B

TABLE OF EQUIVALENT SECURITY CLASSIFICATIONS

Participant	Secret	Confidential	Restricted
Austria	GEHEIM	VERTRAULICH	EINGESCHRÄNKT
Belgium	SECRET GEHEIM	CONFIDENTIEL VERTROUWELIJK	DIFFUSION RESTREINTE BEPERKTE VERSPREIDING
Bulgaria			
Cyprus	ABR:(• •)	ABR:(• •)	• • • • • • ABR:(• •)
Czech Republic	TAJNÉ	D•V•RNÉ	VYHRAZENÉ
Denmark	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Estonia	SALAJANE	KONFIDENTSIAALNE	PIIRATUD
Finland	SALAINEN	LUOTTAMUKSELLINEN	KÄYTTÖ RAJOITETTU
France	SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	(Nota, see below)
Germany [12]	GEHEIM	VS - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Greece	ABR:(• •)	ABR:(• •)	• • • • • • ABR:(• •)
Hungary	TITKOS!	BIZALMAS!	KORLÁTOZOTT TERJESZTÉS• !
Ireland	SECRET	CONFIDENTIAL	RESTRICTED
Italy	SEGRETO	RISERVATISSIMO	RISERVATO
Latvia	SLEPENI	KONFIDENCI• LI	DIENESTA VAJADZ•B• M
Lithuania	SLAPYAI	KONFIDENCIALIAI	RIBOTO NAUDOJIMO
Luxembourg	SECRET LUX	CONFIDENTIEL LUX	RESTREINT LUX
Malta	SIGRIET	KUNFIDENZJALI	RISTRETT

[12] Germany : VS = Verschlusssache.

Netherlands [13]	GEHEIM or STG. GEHEIM	CONFIDENTIEEL or STG. CONFIDENTIEEL	VERTROUWELIJK or DEPARTEMENTAALVERTROUWELIJK
Norway	HEMMELIG	KONFIDENSIELT	BEGRENSET
Poland	TAJNE	POUFNE	ZASTRZE• ONE
Portugal	SECRETO	CONFIDENCIAL	RESERVADO
Romania	STRICT SECRET	SECRET	SECRET DE SERVICIU
Slovakia	TAJNÉ	DÔVERNÉ	VYHRADENÉ
Slovenia	TAJNO	ZAUPNO	INTERNO
Spain	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden [14]	HEMLIG or HEMLIG/SECRET or HEMLIG	HEMLIG or HEMLIG/CONFIDENTIAL	HEMLIG or HEMLIG/RESTRICTED
Switzerland	SECRET	CONFIDENTIEL	CONFIDENTIEL
United Kingdom	SECRET	CONFIDENTIAL	RESTRICTED
EU/EC	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
ESA	ESA SECRET	ESA CONFIDENTIAL	ESA RESTRICTED

NOTA : France handles and protects classified information bearing the marking “RESTRICTED” or equivalent according to its national laws and regulations in force for the protective level “DIFFUSION RESTREINTE” or the standards defined in the present document whichever is higher. The other Participants handle and protect information marked “DIFFUSION RESTREINTE” according to their national laws and regulations in force for the level “RESTRICTED” or equivalent or according to the standards defined in the present document whichever is higher.

13 Should be checked. The classification equivalence in GalileoSat PSI v4.0 does not match those in Council Security regulations.

14 Should be checked. The classification equivalence in GalileoSat PSI v4.0 does not match those in Council Security regulations.

ANNEX C

Annex C1:

PROCEDURE FOR HAND CARRIAGE OF CLASSIFIED INFORMATION

C1.1. When hand carriage of classified material 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 NSA/DSA 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 NSA/DSA through the consignor's security officer immediately after completion of the journey.

C1.2. 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".

C1.3. The courier will be responsible for the safe custody of the classified material until such time that it has been handed over the consignee's security officer. In the event of a breach of security, the consignor's NSA/DSA 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.

(LETTERHEAD)

COURIER CERTIFICATE

PROGRAMME TITLE (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(ies) 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 transmitted, 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 lift unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance 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;
   (g) In cases of emergency, you much 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;
   (i) If unforeseen circumstances make it necessary to transfer the consignment to other than the designated representatives of the company or government you are to visit, you will give it only to authorised employees of one of the points of contact listed in sub-paragraph (I);
   (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 actual senior Customs, Police and/or Immigration Official; this action should normally suffice to pass the consignment through unopened. However, if the senior Customs, Police and/or Immigration Official demands to see the actual contents of the consignments you may open it in his presence, but this should be done in an area out of sight of the general public.

(*) May also be used by security guards.

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 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 DSA's 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
(Name)
Company's stamp
Official stamp
Or NSA/DSA's seal

Signature of the
Designated Security Authority
(Name)

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.

Courier's Signature:

Witnessed by:
(Company Security Officer's signature)

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

ANNEX C2:COMMERCIAL COURRIERS FOR INTERNATIONAL TRANSMISSION OF INFORMATION CLASSIFIED UP TO CONFIDENTIAL

[to be included, possibly copied from GalileoSat PSI]

ANNEX D :

TRANSPORTATION PLAN

(LETTERHEAD)

TRANSPORTATION PLAN -
FOR THE MOVEMENT OF CLASSIFIED CONSIGNMENTS

(INSERT NAME OF European GNSS Programmes)

1. INTRODUCTION

This transportation plan lists the procedures for the movement of classified **(insert European GNSS Programmes /Contract name)** consignments between **(insert European GNSS Programmes Participants)**.

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 military 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 European GNSS Programmes participant who will 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 country'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 transportation agents, where appropriate, that might be involved to include the level of 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 point of movement to the ultimate destination including all border crossing. 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/Programme 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 materials specified in Section V, will apply.

10. RECIPIENT RESPONSIBILITIES

Describe the responsibilities of each recipient to inventory the 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 NSA/DSA of the dispatcher of any known or suspected compromise of classified consignment or any other exigencies which 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 national security rules of the European GNSS Programmes participants. The requirements for dispatch documents seals, receipts, storage and security containers should be explained. Any unique requirement of the European GNSS Programmes 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 (Appendix 1); 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 or sensitive material to the manufacturer or sending country (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 lading

(4) Export declaration

(5) Waybills

(6) Other nationally-required forms

ANNEX E :

REQUEST FOR VISIT FORMS (RFV)

ANNEX E .1,
REQUEST FOR VISIT FORM (for representatives of the Participants)

One-time
Recurring

REQUEST FOR VISIT

Annex(es)
[ ] Yes: ……
[ ] No

ADMINISTRATIVE DATA

1. REQUESTOR:
   DATE:…./…./….
   TO: VISIT ID:

REQUESTING GOVERNMENT AGENCY OR INDUSTRIAL FACILITY

2. NAME:
   POSTAL ADDRESS:

   TELEFAX/FAX No.: TELEPHONE No.:
   POINT OF CONTACT:

GOVERNMENT AGENCY OR INDUSTRIAL FACILITY TO BE VISITED

3. NAME:
   ADDRESS:

   TELEFAX/FAX No.: TELEPHONE No.:
   POINT OF CONTACT:

4. DATES OF VISIT: …./…./…. TO …./…./…. (…./…./…. TO …./…./….)

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

( ) GOVERNMENT INITIATIVE ( ) INITIATED BY REQUESTING AGENCY OR FACILITY
( ) COMMERCIAL INTIATIVE ( ) BY INVITATION OF THE FACILITY TO BE VISITED

6. SUBJECT TO BE DISCUSSED/JUSTIFICATION

7. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED:

8. IS THE VISIT PERTINENT TO: (Y) SPECIFY
   A SPECIFIC EQUIPMENT OR WEAPON SYSTEM ( )
   FOREIGN MILITARY SALES OF EXPORT LICENCE ( )
   A PROGRAMME OF AGREEMENT ( )
   A DEFENCE ACQUISITION PROCESS ( )

OTHER	( )

REQUEST FOR VISIT (continuation)

9.	PARTICULARS FOR VISITORS
NAME: DATE OF BIRTH: …./…./…. SECURITY CLEARANCE: ID/PP NUMBER: NATIONALITY: POSITION: COMPANY/AGENCY:	PLACE OF BIRTH:
NAME: DATE OF BIRTH: …./…./…. SECURITY CLEARANCE: ID/PP NUMBER: NATIONALITY: POSITION: COMPANY/AGENCY:	PLACE OF BIRTH:
10. AGENCY	THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT OR INDUSTRIAL FACILITY
NAME: SIGNATURE:	TELEPHONE NO.:
11.	CERTIFICATION OF SECURITY CLEARANCE
NAME: ADDRESS: TELEPHONE: SIGNATURE:	STAMP (optional)
12.	REQUESTING NATIONAL SECURITY AUTHORITY
NAME: ADDRESS: TELEPHONE: SIGNATURE:	STAMP (optional)
13.	REMARKS

ANNEX E .2,
REQUEST FOR VISIT FORM (for Contractor personnel)

☐ One-time
☐ Recurring
☐ More than 21 days

REQUESTING ESTABLISHMENT/COMPANY/AGENCY Name		
Address		
Security Officer/Security Office		
Telephone	Fax	E-mail
Point of contact/POC Office		
Telephone	Fax	E-mail
☐ **GOVERNMENT AGENCY TO BE VISITED**		☐ **INDUSTRIAL FACILITY TO BE VISITED**
Name		
Address		
Security Officer		
Telephone	Fax	E-mail
Point of contact		
Telephone	Fax	E-mail
DATE OF VISIT **From**		To
SUBJECT TO BE DISCUSSED Project/Contract/Programme		
ANTICIPATED LEVEL TO BE DISCUSSED		
☐ **CONFIDENTIAL**		☐ **SECRET**
VISITOR DETAILS		
Name, First Name		Passport No.
Date of Birth		Nationality
Security Clearance		Expiry Date
Rank/Grade		Position
Company/Agency		
		Continue on additional sheets for extra visitors
SIGNATURE		DATE

ANNEX TO REQUEST FOR VISIT

Visit ID Date

VISITOR DETAILS	
Name, First Name	Passport No.
Date of Birth	Nationality
Security Clearance	Expiry Date
Rank/Grade	Position
Company/Agency	
Name, First Name	Passport No.
Date of Birth	Nationality
Security Clearance	Expiry Date
Rank/Grade	Position
Company/Agency	
Name, First Name	Passport No.
Date of Birth	Nationality
Security Clearance	Expiry Date
Rank/Grade	Position
Company/Agency	
Name, First Name	Passport No.
Date of Birth	Nationality
Security Clearance	Expiry Date
Rank/Grade	Position
Company/Agency	
Name, First Name	Passport No.
Date of Birth	Nationality
Security Clearance	Expiry Date
Rank/Grade	Position
Company/Agency	

ANNEX F:

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FIS)

FACILITY SECURITY CLEARANCE INFORMATION SHEET(FIS)

REQUEST

Please [ ] provide a FSC assurance of the facility listed below.
[ ] start initiating a FSC up to and including the level of... if the facility does not hold acurrent FSC.
[ ] confirm the FSC up to and including the level of ... as provided on .....(ddmmyy).
[x] provide the correct and complete information, if applicable.

	corrections/completions:
1. Full facility name:	
_____	_____
2. Full facility address:	
_____	_____
3. Mailing address (if different from 2):	
_____	_____
4. Zip code/city/country:	
_____	_____
5. Name of the security officer:	
_____	_____

6. This request is made for the following reason(s):
(indicate particulars of the precontractual stage, contract, sub-contract, programme/project)
_____
_____
_____
_____

REQUESTING NSA/DSA: Name:.....Date:.....

REPLY

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

[ ] holds a FSC up to and including the level of [ ] S [ ] NS [ ] C [ ] NC
[ ] does not hold a FSC.
[ ] does not hold a FSC but, on your above mentioned request, the FSC is in progress. You will be informed when the FSC has been established. Expected date: .../...(mm/yy). (if known).

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

3. This FSC certification expires on:.....(ddmmyy).
You will be informed in case of an earlier invalidation or significant change to any information listed above.

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

5. REMARKS:
.....
.....
.....

PROVIDING NSA/DSA:Name:..... Date:.....

ANNEX G :

PERSONNEL SECURITY CLEARANCE CERTIFICATE

Format for Security Clearance Assurance

ASSURANCE OF SECURITY CLEARANCE

This is to certify that:

Name/surname/title:

Place and date of birth (country):

National of (country/countries):

Holder of passport/identity card (number):

Employed with (company, authority, organisation):

Is the holder of a security clearance issued by the NSA/DSA of:

In conformity with national laws and regulations and may have access to classified information up to and including:

CONFIDENTIAL ☐

SECRET ☐

The current security clearance expires on: (date)

Issuing:
Company/Authority (address or stamp)
Security official (full name, rank)

(Date) (Signature)

1.2