

ANNEX V:
SECURITY ASPECTS LETTER
CALL FOR TENDERS NO ENTR/30/PP/2010/FC

This Framework Service Contract (FSC) is established to provide expert support to the Directorate (Consumer Goods and EU Satellite navigation programmes) of the European Commission's Directorate General Enterprise & Industry (hereafter referred as the DG) for a manifold of technical tasks which have to be carried out in this DG in the frame of the Galileo and EGNOS programmes. Some of these tasks are intended to be externalized in order to overcome and mitigate existing resource limitations in the technical support teams for the European GNSS project management. The precise scope, timing and volume of the services to be procured cannot be specified in advance for the entire contract period of 48 months, hence the format of a FSC is chosen.

Participants:

[To be filled later on (at contract signature)]

Table of Contents

1 Introduction	3
2 Background	3
3 Security Instructions for Classified Information	3
3.1 <i>General Principles</i>	3
3.2 <i>Release of contract information</i>	5
3.3 <i>Security plan in event of termination</i>	6
3.4 <i>International Visits</i>	6
4 Reference documents	6
5 Annex A: List of security cleared companies	7
6 Annex B: Access to the EUROPEAN COMMISSION premises	8

I. INTRODUCTION

This document is a Security Aspects Letter (SAL) issued by the European Commission (EC) as part of contract the service contract for the provision of mission and service implementation.

It defines the security contractual conditions issued by the EC. These conditions form an integral part of the contract under which classified information shall be accessed or generated. This document identifies those elements of the contract which involve classified information which requires protection and identifies the essential security requirements. This SAL applies to any legal entity involved through this contract by contractual or pre-contractual activity. A list of companies and sites handling EU RESTRICTED information of the contract are in Annex A. For a list of security authorities and National Project Offices refer to the European GNSS PSI (ANNEX D).

This document includes a Security Classification Guide (SCG), contained in ANNEX C. which describes the classified elements of the Contract and specifies the applicable security classification levels. This document is created from {RD 5, Standalone Galileo Security Classification Guide} containing only those parts relevant to the contract. The SCG may be amended throughout the life of the Contract and the elements it contains may be reclassified or downgraded.

This document is intended to provide an overview of the essential security requirements that the contractor must implement. These security provisions based on the European GNSS PSI provide additional security requirements matching a specific contract. RD 3 should be considered as provided guidance for the EU GNSS programme on the interpretation and application of the security policies found in {RD 1: Commission Decision 2001/844} and especially those to be found in the amendment to {RD 1: Commission Decision 2001/844}, {RD 2: Commission Decision 2006/548} which deals with the Common Minimum Standards on Industrial Security.

In situations where provisions in national legislation and regulations differ from the provisions in this SAL, the provisions in national legislation and regulations may be applied provided that they are not less stringent than the provisions set out in this SAL. In all such cases the contractor shall inform the EC of the revised security procedures.

This current version is only a draft to be used by the tenderers and shall be completed after the selection of the contractor and subcontractors with a clarification of the Participants list and the following information:

Annex A: List of companies handling EU RESTRICTED documents;

The EC is responsible for the approval of this SAL and any future modifications.

Comments or questions on the interpretation of this SAL should be directed to the EC or to the contractor's NSA/DSA.

II. BACKGROUND

The Commission's Common Minimum Standards on Industrial Security {RD 2: Commission Decision 2006/548} state that all classified contracts must include a SAL and a SCG.

III. SECURITY INSTRUCTIONS FOR CLASSIFIED INFORMATION

III.1. General Principles

- [REQ 1] The performance of this contract shall involve classified information up to the level of RESTRICTED, and it shall be classified at RESTREINT UE level.
- [REQ 2] Contractor's personnel as well as subcontractors' personnel involved in work under this Contract shall be nationals of a Participant State in the EU GNSS Programmes (EU Member States plus Norway and Switzerland) unless otherwise agreed in advance with the EC. Access by non-participants nationals shall be done in accordance with European GNSS PSI requirements.
- [REQ 3] The documents referenced in {section 4} shall be applicable to the contractor and subcontractors.
- [REQ 4] Information generated by the contractor which requires classification shall be marked using the EU security classification markings and, if needed, a double marking detailed in the {European GNSS PSI} in accordance with the {SCG at Annex C}.
- [REQ 5] The contractor shall handle and protect classified information or material provided to them or generated by the contractor pursuant to this Contract in accordance with its classification as described in {RD 3, The European GNSS PSI} or, provided they are no less stringent, in accordance with national regulations.
- [REQ 6] If the contractor's responsible NSA/DSA identifies a failure by the contractor to observe the security provisions described and Regulations referred to under this SAL, it shall inform the EC.
- [REQ 7] If the responsible NSA/DSA has identified such a failure to comply with the relevant security Regulations by any subcontractor the procedure for Security Violations reported in the European GNSS PSI section 2.7 should be followed.
- [REQ 8] For work performed on the EC premises, the contractor and its personnel shall comply with the security requirements as described in {Annex B: Access to the EC premises}.
- [REQ 9] The contractor shall not transmit any classified information or material to a subcontractor without the prior written consent of the originator.
- [REQ 10] The ultimate responsibility for protecting classified information within industrial or other entities rests with the management of those entities.
- [REQ 11] It may be necessary for the contractor to negotiate classified subcontracts with subcontractors at various levels. The contractor is responsible for ensuring that all subcontracting activities are undertaken in accordance with the common minimum standards contained in this SAL. The procedures for subcontracting in {RD 3, The European GNSS PSI} will be applied to all potential subcontracts.
- [REQ 12] A Security Classification Guide (SCG) contained in ANNEX C shall also be a part of each classified subcontract, describing the specific elements which are classified and specifying the applicable security classification levels. The SCG will be distributed separately from the SAL.
- [REQ 13] Classified information released to the contractor or subcontractor or generated under contractual activity shall not be used for purposes other than those defined by the classified contract and shall not be disclosed to third parties without the prior written consent of the originator, in accordance with the European GNSS PSI section III.

- [REQ 14] All industrial or other entities participating in classified contracts which involve access to information classified CONFIDENTIEL UE or above shall hold a FSC. The FSC is granted by the NSA/DSA of the participating State in which it is located to confirm that a facility can afford and guarantee adequate security protection of classified information to the appropriate classification level. Questions regarding FSCs should be addressed to the participant's NSA/DSA, details of which can be found in the European GNSS PSI.

- [REQ 15] If changes to the security requirements emerge during the performance of the contract and if such changes significantly deviate from the initial arrangements, the contract shall be amended accordingly or terminated, as appropriate.

- [REQ 16] Where changes of security requirements result in additional security measures to be taken or investments to be made by the contractor, a contract amendment shall be negotiated on a fair and reasonable basis.

- [REQ 17] In case the contractor cannot comply with increased security requirements, the contract shall be terminated. However, any contract termination resulting from changes of the security requirements shall not be by default the responsibility of the contractor, and the contractor may be entitled to compensation by the EC.

The NSA/DSA of the participant in which the contractor is registered shall be informed by the contractor and by the EC GNSS Security Officer

- [REQ 18] When a classified contract or a classified subcontract is terminated, the contractor and the EC Security Department shall notify separately this termination in less than one month to the NSA/DSA of the participants in which the contractor and subcontractors are registered.

- [REQ 19] Throughout the life of the classified contract, compliance with all its security provisions shall be monitored by the EC, in conjunction with the relevant NSA/DSA. Any security incidents shall be reported, in accordance with the provisions laid down in {the European GNSS PSI}.

- [REQ 20] The contractor shall - under penalty of termination of the contract - comply with any security requirements prescribed by the Contracting Authority as detailed in this Security Aspects Letter.

III.2. Release of contract information

The unilateral release of classified information or material used by or issued from the Contract to other than SAL participants' authorities and contractors is prohibited without the specific written approval of the originator of the information and the EC. Requests for release shall be handled in accordance with the procedures outlined in {RD 3, The EU GNSS PSI}.

The fact that any information related to the Contract is not marked with a security classification does not mean that it can be released to the public. Any release of information requires the written authorisation of the originator and shall be done according to the provisions of the European GNSS PSI section III.

III.3. Security plan in event of termination

In the event of the contract being terminated by either party, the procedures described in {RD 3, The EU GNSS PSI} for the disposal of classified information shall be implemented

III.4. International Visits

Procedures for international visits contained in {RD 3, The EU GNSS PSI} shall be applied to all visits necessary in the performance of this contract.

IV. REFERENCE DOCUMENTS

- RD 1 Commission Decision 2001/844/EC of 29 November 2001
- RD 2 Commission Decision 2006/548/EC of 2 August 2006 amending Commission Decision 2001/844/EC of 29 November 2001
- RD 3 The European GNSS PSI issued by Galileo Security Board (GSB) v2.0, 21.05.2010
- RD 4 Galileo COMSEC Security Instructions issue 3, 28 June 2007 (RESTRICTED)
- RD 5 Galileo Stand alone Security Classification guide v2.0 (RESTRICTED)

V. ANNEX A: LIST OF COMPANIES OR SITES INVOLVED IN THE HANDLING OF RESTREINT UE INFORMATION OF THE CONTRACT

[To be completed once known]

Company	Site	Mail address

VI. ANNEX B: ACCESS TO THE EC PREMISES

1. Contractors or subcontractors and their personnel shall comply with the EC internal security and safety rules and Regulations and shall follow any instructions given by the EC Security Department.
2. Any failure to comply with the EC security or safety instructions may result in access to the premises being denied or the personnel being expelled from the EC premises.
3. Unless otherwise agreed with the EC, contractor or subcontractor personnel performing work on the EC premises, except attendance at meetings with the EC representatives, shall hold the nationality of an EU Member State and shall hold a security clearance at CONFIDENTIAL level issued by the contractor's or subcontractor's responsible national security authority.
4. The EC may temporarily authorise, on a case-by-case basis, contractor or subcontractor personnel to perform work on its premises for whom initial security checks have revealed no adverse information and the security clearance procedure has been initiated or is still in progress.
5. In case the required security clearance for the contractor's or subcontractor's personnel performing work on the EC premises is withdrawn or not obtained within a reasonable period of time after award of the Contract, this shall be considered as a failure to comply with the EC security requirements.
6. Any information or material provided to the contractor's or subcontractor's personnel shall be treated as if supplied officially by the EC.
7. The contractor shall notify the EC Security Department at least 5 working days in advance of any visit with the names, dates of birth and nationalities together with a certification of the individual's security clearance and where appropriate the details of vehicles, for all contractor or subcontractor personnel temporary performing work on the EC premises.
8. The EC shall be entitled to refuse access to its premises to any contractor or subcontractor personnel without giving justification, as deemed necessary for security reasons.
9. Any security-related notices or communication to the EC shall be addressed to Mr. Louis CHARLES, Security Officer for EGNOS and Galileo, EC, Directorate General Enterprise and Industry, Rue de Mot 28, 1049 Brussels, e-mail: louis.charles@ec.europa.eu

VII. ANNEX C: SECURITY CLASSIFICATION GUIDE (SCG)

1. The study to be provided under the service Contract N° ENTR/30/PP/2010/FC will be classified as RESTREINT UE.

VIII. ANNEX D: PROGRAMME/PROJECT SECURITY INSTRUCTION (PSI)