ANNEX 6

SECURITY ASPECTS LETTER

European GNSS Supervisory Authority. Rue de la Loi, 56 B-1049 Brussels, Belgium. Office: L56 07/81
Telephone: (32-2) 295.84.26, Fax: (32-2) 292.08.72. Email: olivier.crop@gsa.europa.eu (Head of Security)
Website: http://www.gsa.europa.euWebsite: http://www.gsa.europa.eu

European GNSS Supervisory Authority

Security Department

GSA 3SC 08-01-03-03
Version 2, 07/02/2008

European GNSS Supervisory Authority

SECURITY ASPECTS LETTER

Concerning the Contract

GSA/OP/01/09

—o§o—

The PROPHET Contract

Participants:

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

European GNSS Supervisory Authority. Rue de la Loi, 56 B-1049 Brussels, Belgium. Office: L56 07/81
Telephone: (32-2) 295.84.26, Fax: (32-2) 292.08.72. Email: olivier.crop@gsa.europa.eu (Head of Security)
Website: http://www.gsa.europa.euWebsite: http://www.gsa.europa.eu

Table of Contents

1 Introduction

This document is a Security Aspects Letter (SAL) issued by the GSA as part of contract GSA/OP/01/09, The PROPHET Contract. It defines the security contractual conditions issued by the GSA. 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 security cleared companies and sites involved in the contract is at Annex A. For a list of security authorities and National Project Offices refer to the European GNSS PSI.

This document includes a Security Classification Guide (SCG), distributed separately, 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 2001/444, 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 GSA of the revised security procedures.

[The following paragraph will be deleted for SALs created for signature but should remain for draft SALs to indicate that this information will be completed once the list of participants is known.]

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 security cleared companies;

The GSA 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 GSA or to the contractor's NSA/DSA.

2 Background

Council Regulation 1321/2004 article 20, states "The Authority shall apply the security principles contained in Commission Decision 2001/844". Article 2.1.j.(i) further states that the GSA will approve the security annexes of industrial contracts. 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.

3 Security Instructions for Classified Information

3.1 General Principles

- [REQ 1] The performance of this contract shall involve classified information up to the level of SECRET, and it shall be classified at SECRET UE level.

- [REQ 2] Contractor's personnel as well as subcontractors' personnel involved in work under this Contract shall be nationals of an EU Member State unless otherwise agreed in advance with the GSA, and shall hold a valid PSC for handling EU or national classified information at the level of SECRET

- [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.

- [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 GSA. If this failure is of such a nature as to result in the withdrawal of the contractor's Facility Security Clearance (FSC) to handle classified documents as necessary for the execution of the Contract, the GSA shall have the right to terminate the Contract with immediate effect in accordance with the relevant provisions of the General Terms and Conditions for Contracts awarded by the GSA, without prejudice to criminal and civil proceedings against the contractor.

- [REQ 7] If the responsible NSA/DSA has identified such a failure to comply with the relevant security Regulations by any subcontractor resulting in the withdrawal of the subcontractor's FSC, the GSA shall be entitled to require the contractor to terminate the sub-contract with immediate effect, without prejudice to the GSA's right to terminate the contract with immediate effect and/or to initiate criminal and/or civil proceedings against the subcontractor.

- [REQ 8] For work performed on the GSA's premises, the contractor and its personnel shall comply with the security requirements as described in Annex B: Access to the GSA's 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) 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 and of the GSA.

- [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 GSA.

- [REQ 18] The NSA/DSA of the participant in which the contractor is registered shall be informed by the contractor and by the GSA Security Department separately of the award of a classified contract.

- [REQ 19] When a classified contract or a classified subcontract is terminated, the contractor and the GSA 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 20] Throughout the life of the classified contract, compliance with all its security provisions shall be monitored by the GSA, 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} . Any change to or withdrawal of an FSC shall immediately be communicated to the GSA Security Department.

- [REQ 21] 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.

3.2 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 GSA. 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 the GSA and shall be done according to the provisions of this section.

3.3 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

3.4 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.

4 Reference documents

RD 1 Council Regulation (EC) No 1321/2004 of 12 July 2004 on the establishment of structures for the management of the European satellite radio-navigation programmes

RD 2 Council Regulation (EC) No 1942/2006 of 12 December 2006 amending Regulation (EC) No 1321/2004 on the establishment of structures for the management of the European satellite radio-navigation programmes

RD 3 The European GNSS PSI issued by Galileo Security Board (GSB) v1.519 Dec 2008.

RD 4 Galileo COMSEC Security Instructions draft 2.4, 12 April 2007 (RESTRICTED)

RD 5 Galileo Stand alone Security Classification guide v2.0 (RESTRICTED)

5 Annex A: List of security cleared companies

[To be completed once known]

6 Annex B: Access to the GSA's premises

1. Contractors or subcontractors and their personnel shall comply with the GSA's internal security and safety rules and Regulations and shall follow any instructions given by the GSA's Security Department.

2. Any failure to comply with the GSA's security or safety instructions may result in access to the premises being denied or the personnel being expelled from the GSA premises.

3. Unless otherwise agreed with the GSA, contractor or subcontractor personnel performing work on the GSA's premises, except attendance at meetings with the GSA 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 GSA 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 GSA's 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 GSA's 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 GSA.

7. The contractor shall notify the GSA's 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 GSA's premises.

8. The GSA 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 GSA shall be addressed to "European GNSS Supervisory Authority (GSA), Security Department, Rue de la Loi 56, 1049 Bruxelles, e-mail: olivier.crop@gsa.europa.eu, fax-mail: fax-security@gsa.europa.eu, fax phone number: 00 32 2 292 08 72".