GSA/NP/02/19- EGNOS GEOSTATIONARY SBAS PAYLOAD SERVICE - GEO-4

Annex 3 to the TIP: Security Aspects Letter

Index

1 Introduction

This document is the Security Aspects Letter (SAL) issued by the European GNSS Agency (hereinafter "GSA" or "contracting authority"). It forms integral part of the contract mentioned on the title page and any ensuing specific contract under which EU Classified Information ("EUCI") may be accessed or generated (hereinafter the "Contract").

This document identifies the requirements for the performance of the tasks identified for the Contract involving EUCI. As per the regulation specifying the security rules applicable to the contracting authority (RD1), the contracting authority is obliged to protect such EUCI in accordance with Commission Decision (EU, Euratom) 2015/444 (RD2) and achieves this through the application of this SAL to the Contract. This SAL applies to any legal entity involved through this Contract in contractual or pre-contractual activity.

Where the term "Contractor" is used in this document, the applicable provisions apply to the prime contractor (including all consortium members) and subcontractors as regards the subcontracts which require access to EUCI in order to fulfil the tasks foreseen in the Contract.

The EU GNSS Information Assurance Authority ("IAA") is the Security Authority responsible for assuring compliance to Commission Decision (EU, Euratom) 2015/444 (RD2). Communication channels between the Contractor and the IAA shall be made known to the Contractor by the contracting authority.

Where the SAL refers to national laws, regulations and/or requirements and the Contractor is an international organisation, equivalent rules and requirements of that international organisation apply.

This document includes a Security Classification Guide (SCG – Appendix 1) which describes the classified elements of the Contract and ensuing specific contracts.

The applicable documents mentioned in section 9.1 [European GNSS PSI (AD 1)], in their latest version, shall be considered as applicable to the Contract, providing guidance for the European GNSS Programmes on the interpretation and application of the security rules found in Commission Decision 2015/444 (RD 2) and more specifically in Chapter 6 thereof which deals with Industrial Security.
Definitions laid down in European GNSS PSI (AD 1) shall be applicable to this SAL.

The Contractor's Security Authority (NSAs/DSAs) is responsible for ensuring that the Contractor under their jurisdiction comply with the applicable security provisions for the protection of EUCI.

Where the contract requires the generation, handling or storage of assets or information marked CRYPTO or CCI, the Contractor's Cryptographic Authority is responsible for issuing the crypto account necessary to possess, manage and operate cryptographic material.

Non-compliance with requirements of the SAL may constitute sufficient grounds for termination of the Contract under conditions stipulated in the Contract.

Changes of requirements to the SAL made by the GSA in compliance with new compulsory requirements, notably those imposed by law, PSI or security classification guide of the GNSS

Programme, shall become integral part of the Contract. These additions and changes will be communicated by the GSA to the Contractor and shall become effective upon this communication.

2 General Conditions

- [REQ 2.1] The Contractor shall handle and protect EUCI provided or generated under the Contract in accordance with the EU GNSS PSI (AD 1) and the supplementary provisions as detailed in this SAL. The Contractor shall comply with any additional instructions provided by the Contractor's competent security authority [Requirement truncated to the part applicable to the contract].

- [REQ 2.2] EUCI generated for the performance of the Contract shall be marked as EUCI in accordance with Article 3 of Decision 2015/444 (RD2) corresponding to the level of classification as defined by the SCG in **Appendix 1** to this letter.

- [REQ 2.3] Regarding EUCI created and handled for the performance of the Classified Contract, the rights incumbent on the originator are exercised by the GSA, as the contracting authority.

- [REQ 2.4] Without the written consent of the contracting authority, the Contractor must not make use of any information or material furnished by the contracting authority or produced on behalf of the contracting authority other than for the purpose of the Contract.

3 Access to EUCI

- [REQ 3.1] EUCI released to the Contractor or generated under contractual activity shall not be disclosed to third parties without the prior written consent of the IAA (EUCI originator). The Contractor may request a general approval by the IAA for certain types of activities.

- [REQ 3.2] The Contractor shall only allow access to EUCI to its personnel for the performance of the Contract and only if the personnel:
    - have a justified need-to-know in relation to the performance of the Contract,
    - have been briefed by the Contractor's Security Officer on the applicable security rules for protecting EUCI, on their responsibilities and on the consequences of any compromise or breach of security of such information,
    - have acknowledged in writing their responsibilities with regard to protecting such information
    - as regards EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL level or above, have been granted a personal security clearance within the meaning of Decision 2015/444 (RD2) at the relevant level (PSC);

- [REQ 3.3] [Requirement not applicable to the contract].

- [REQ 3.4] The Contractor is responsible for knowing the security certification and/or accreditation status of all consortium members (if any) and sub-contractors involved in the Contract and for reporting any changes to the GSA Security Department.

- [REQ 3.5] [Requirement not applicable to the contract].

- [REQ 3.7] Upon termination of the Contract or when EUCI is no longer required for the performance of the Contract, the Contractor shall return any EUCI they hold to the contracting authority immediately. Where practicable, in accordance with national laws and regulations, and with the prior agreement of and under instruction from the IAA, EUCI may be destroyed in accordance with the PSI by the Contractor instead of being returned. EUCI shall be destroyed in such a way that it cannot be reconstructed in whole or in part.

- [REQ 3.8] Where the Contractor is authorised to retain EUCI after termination or conclusion of the Contract, the EUCI must continue to be protected in accordance with the Commission security rules (RD2) through continual implementation of the requirements in this SAL.

- [REQ 3.9] Electronic handling, processing and transmission of EUCI shall be done in accordance with the provisions laid down in the European GNSS PSI (AD1). These require, inter alia, that Communication and Information Systems (hereinafter 'CIS') owned by the Contractor and used for handling EUCI for the purpose of the Contract (hereinafter 'Contractor CIS') must be subject to accreditation[1]; that any electronic transmission of EUCI shall be protected by approved cryptographic products in accordance with RD2; ; [Requirement truncated to the part applicable to the contract]

- [REQ 3.9.1] EUCI shall only be encrypted using cryptographic products approved in accordance with RD2. Where products are to be used for communication with the GSA, the product shall be agreed with the GSA Security Department.

- [REQ 3.9.2] The security accreditation of Contractor CIS handling EUCI and any interconnection thereof shall be conducted in accordance with the applicable rules set by the Contractor's Security Authorities (NSAs/DSAs/SAAs). In addition, the Contractor shall provide to the contracting authority evidence that the Contractor CIS and respective interconnections have been accredited for handling EUCI.

- [REQ 3.9.3] Where CIS is to be used to handle EUCI, the Contractor shall ensure that Security Operating Procedures (SecOPs) describing how to maintain a secure storage, transport and operating environment for the CIS exist and are available to their personnel for all CIS used to handle EUCI under this Contract. Where there is no explicit SecOPs provided upon acquisition of the CIS, and where no SecOPs exist in documentation provided with the CIS, the Contractor shall create SecOPs specifying the conditions for use of the CIS under the Contract.

- [REQ 3.9.4] All persons involved in contractual activities that are required to access CIS for handling EUCI shall do so in accordance with the Security Operating Procedures (SecOPs) applicable to that CIS; whether provided with the CIS upon acquisition or developed for the CIS by the Contractor.

[1] The party undertaking the accreditation will have to provide a statement of compliance to the contracting authority (via the GSA Security Department) in co-ordination with the relevant national Security Accreditation Authority.

4 Security Incident Management

- [REQ 4.1] All security breaches related to EUCI shall be investigated. Security breaches are to be reported to the IAA as soon as is practicable. The Contractor shall immediately report to his responsible Security Authority (NSA/DSA) and, where permitted by its national laws and regulations, to the GSA Security Department all cases in which it is known or there is reason to suspect that EUCI provided or generated pursuant to the Contract has been lost or disclosed to unauthorised persons.

- [REQ 4.2] The Contractor shall inform the GSA of Business Contingency Plans (BCP) for protecting EUCI handled in the performance of the Classified Contract in emergency situations and shall put in place preventive and recovery measures in the context of BCP to minimise the impact of incidents in relation to the handling and storage of EUCI.

5 Conditions under which the Contractor may subcontract

- [REQ 5.1] Before subcontracting, the Contractor shall obtain permission from the GSA, as foreseen in the Contract, bearing in mind specificities applicable to the Classified Contract.

- [REQ 5.2] Where required by applicable national regulations, when a classified subcontract under this Contract is concluded, the contractor shall notify separately this conclusion in less than one month to the Security Authority (NSA/DSA) of the subcontractor.

- [REQ 5.3] Where the Contractor has let a classified subcontract, the security provisions of the Contract shall apply *mutatis mutandis* to the subcontractor(s) and their personnel. In such case, it is the responsibility of the Contractor to ensure that all subcontractors apply these principles to their own subcontracting arrangements.

    - [REQ 5.3.1] A SAL and a SCG shall be part of each classified subcontract, describing the specific elements which are classified and specifying the applicable security classification levels.

    - [REQ 5.3.2] Where the provisions of both the SAL and SCG applied to this Contract are also applicable to a subcontract, the resulting subcontract SAL and SCG shall not be less stringent than the SAL and SCG applicable to this Contract, unless duly justified by the Contractor and agreed by the GSA Security Department.

6 Marking of EUCI

- [REQ 6.1] The Contractor shall mark EUCI in accordance with Article 3 of Decision 2015/444 (RD2) corresponding to the level of classification as defined by the Contract SCG.

- [REQ 6.2] The Contractor must maintain the security classification markings of EUCI generated by or provided during the performance of a Contract and must not declassify information without the written consent of the IAA.

7 Security Organisation

- [REQ 7.1] Where not already established by the Contractor through virtue of an FSC, the Contractor shall establish and maintain an appropriate security organisation responsible for monitoring and implementing the content of this SAL.

    - [REQ 7.1.1] The Contractor shall declare to the GSA the interface to its security organisation via nominated point(s) of contact, in each case specifying the name, post, address, telephone number and email address of the point(s) of contact.

    - [REQ 7.1.2] The Contractor shall ensure that at least one of their points of contact be the Local Security Officer who is able to act as a liaison and co-operation contact for the GSA Local Security Officer regarding security matters pertaining to the Contract.

- [REQ 7.2] In case of any change to the security organisation which is relevant to the Contract and is established by the Contractor throughout the term of applicability of the Contract, the Contractor shall immediately update the information and inform the GSA Local Security Officer in writing about all relevant details of the changes within 30 (thirty) days of their occurrence.

8 Visits and access to GSA classified premises

- [REQ 8.1] Where access to GSA premises is required for contractual activities, contractors and their personnel shall comply with the GSA's internal security rules and regulations and shall follow any instructions given by the GSA's Local Security Officer. They will be briefed accordingly by the GSA Local Security Officer. They shall grant their full co-operation to prevent and report any (security) incident they detect.

9 Applicable and reference documents

9.1 Applicable documents

AD 1 The European GNSS PSI, latest version;

9.2 Reference documents

RD 1 Regulation (EU) No 912/2010 of the European Parliament and of the Council, setting up the European GNSS Agency, as amended by Regulation (EU) No 512/2014;

RD 2 Commission Decision No 2015/444 of 13 March 2015 on the security rules on the protection of EUCI;

RD 3 *[Document not applicable to the contract]*

RD 4 Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite

navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council.

RD 5 EU GNSS Programme Security Classification Guide, latest version (RESTREINT UE/EU RESTRICTED)

Appendix 1 – Security Classification Guide - Part I – General principles

1. Information generated by the Contractor that requires classification shall be
    a. considered as EUCI for which the originator is the European Commission GNSS IAA; and
    b. classified and protectively marked in accordance with the Security Classification Guide (SCG) issued with the Contract using only classification, annotation and caveat markings detailed in the European GNSS PSI (AD 1).

2. *[Principle not applicable to the contract]*

3. If the Contractor intends to use a marking which differs from the marking specified or implied in the SCG, the Contractor shall provide written justification of the intended marking for consideration and receive approval by the GSA Security Department.

4. While waiting for the reply of the GSA, the information shall either not be produced in recorded form, or be classified as per the specification assigned in the SCG and all parties shall handle it accordingly until the GSA has decided on the final classification level to be assigned and communicated it in writing to the Contractor. The SCG shall then be updated by the GSA to reflect the new classification scenario and re-issued to the Contractor.

5. In instances where the Contractor encounters a classified asset with an EU classification marking that differs from the Programme marking scheme defined in the European GNSS PSI (AD 1), the information and assets shall be handled as per the European GNSS PSI (AD 1); if possible, the marking shall be changed accordingly[2].

[2] Such instances may arise where revisions of AD1and RD5 result in unsupported markings assigned to existing information and assets, or where the legacy marking for information or assets needs to be revised/updated. In all instances where ambiguity exists, the EU GNSS PSI (AD 1) provides clarification on handling legacy markings.