ANNEX 4.07(1) SECURITY ASPECTS LETTER (SAL) SAMPLE FOR CONFIDENTIAL OR SECRET

Security Aspects Letter (SAL)

CONTRACT.: xxx/xx.

This contract may require or involve your company accessing European Union participating Member States (EU pMS)' national classified information or creating European Union classified information or material (EUCI) up to the level of **SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL (delete accordingly).** It is a condition of this contract that this information or material is appropriately protected. The level of protection required varies in accordance with the level of classification. To assist you in providing the appropriate degree of protection to classified information or material, this letter and its appendices identify the security requirements (Appendix I) and those elements of the contract requiring security protection (Appendix II).

Non-compliance with these requirements and the related security classification guide (SCG) may constitute sufficient grounds for the contract to be terminated.

The SCG, which can be found in Appendix II to this letter determines the security classification of any information provided or granted to you, as well as the security classification of any information to be created by your company for the performance of the contract. The SCG is part of the SAL but is laid-out as a separate document since it may vary throughout the life of the contract.

You are requested to bring this letter to the attention of your Facility Security Officer appointed for the performance of this contract, that they are fully understood and they can and will be respected so to safeguard the information and material concerned.

If you have any difficulty in interpreting the meaning of the above aspects or in complying with the security requirements laid down in this letter, please contact EDA immediately.

A copy of this letter will be sent to the National Security Authority (NSA)/ Designated Security Authority (DSA) of the country where your company is registered.

APPENDIX I
SECURITY REQUIREMENTS

GENERAL CONDITIONS

1. This Security Aspects letter is an integral part of the classified contract [or subcontract] and describes contract-specific requirements. Non-compliance with the basic principles and minimum standards of security laid down in the Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU) and these requirements may constitute sufficient grounds for termination of the contract.

2. Classified information generated for the performance of the contract must be marked as EU classified information (EUCI) as determined in the Security Classification Guide (SCG) in Appendix II to this letter.

3. Regarding EUCI created and handled for the performance of the classified contract, the rights incumbent on the originator are exercised by EDA, as the contracting authority.

4. Without the written consent of the contracting authority, the contractor or subcontractor 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.

5. All security breaches related to EUCI must be investigated. Security breaches are to be reported to the contracting authority as soon as is practicable. The contractor or subcontractor must immediately report to his responsible NSA/DSA and to the EDA Security Office, all case 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.

6. Upon termination of the contract, the contractor or subcontractor must return any EUCI held by him to the contracting authority as soon as possible. Where practicable, in accordance with national laws and regulations, and with the prior agreement of and under instructions from the EDA Security Office, EUCI may be destroyed by the contractor or subcontractor instead of being returned. EUCI must be destroyed in such a way that it cannot be reconstructed in whole or in part.

7. Where the contractor or subcontractor is authorised to retain EUCI after termination or conclusion of the contract, the EUCI must continue to be protected in accordance with the Council Security Rules[1].

8. Electronic handling, processing and transmission of EUCI must be done in accordance with the provisions laid down in Article 10 and Annexes IV and V to the Council security rules (hereinafter "CSR"). This includes inter alia, that communication and information systems (hereinafter "CIS") must be subject to accreditation; that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 10(6) CSR; and that TEMPEST measures must be implemented in accordance with Article 10(5) CSR.

9. The contractor or subcontractor will inform EDA of Business Contingency Plans (BCP) for protecting EUCI handled in the performance of the classified contract in emergency situations and will 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.

10. Safeguarding of EUCI will require physical security measures in accordance with the provisions laid down in Article 8 and Annex II of the Council security rules (CSR).

[1] Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p.1)

11. Management of classified information must be in accordance with the provisions laid down in Article 9 and Annex III of the Council security rules (CSR). This includes inter alia the following particular requirements

(a) To indicate clearly EDA, as the originator of the information to be created during the performance of this contract and guarantee originator rights, classified information originated by the contractor will, in addition to the EU security classification marking mentioned in the Security Classification Guide, bear the originator identifier "EDA" alongside or below every occurrence of the security classification marking.

(b) In addition to the security classification markings provided for in the Security Classification Guide, classified information might include explicit releasability statements, and further access or distribution limitations may be added to the reselability statement as deemed necessary by the originator.

PARTICULAR REQUIREMENTS FOR INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

12. A Personnel Security Clearance (PSC) is not required. However, classified information at RESTREINT UE/EU RESTRICTED level shall only be accessible to contractor/subcontractor personnel requiring such information for the performance of the contract (need-to-know principle), who have been briefed by the contractor's Security Officer on their responsibilities and on the consequences of any compromise or breach of such information, and have acknowledged in writing the consequences of failing to protect EUCI.

13. The contractor must have appointed a Security Officer (FSO), who will be responsible for enforcing its security obligations regarding this contract. The following data shall be provided to the contracting authority before the signature of the contract to EDA, and every time thereafter when any change occurs: FSO's name, phone, fax and email.

14. Except where the contracting authority has given its written consent, the contractor or sub-contractor shall not grant access to RESTREINT UE/EU RESTRICTED information or material to any entity or person other than those of its personnel who have a need-to-know.

15. The contractor or sub-contractor must maintain the security classification markings of classified information generated by or provided during the performance of a contract and must not downgrade or declassify information without the written consent of the contracting authority.

16. Information or material classified RESTREINT UE/EU RESTRICTED must be stored in locked office furniture inside Administrative Areas, when not in use. When in transit, documents must be carried inside an opaque envelope bearing only the addressee's name. The document must not leave the possession of the bearer and it must not be opened en route or read in public spaces.

17. The contractor or subcontractor may transmit documents classified RESTREINT UE/EU RESTRICTED to EDA using commercial courier companies, postal services, hand carriage or electronic means.

18. When no longer required, classified RESTREINT UE/EU RESTRICTED documents shall be destroyed by methods preventing its reconstruction in whole or in part.

19. The security accreditation of contractor CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the Security Officer of a contractor if permitted by national laws and regulations. Where that delegation is exercised, the NSAs/DSAs/SAAs must retain responsibility for the protection of RESTREINT UE/EU RESTRICTED information handled by the contractor and the right to inspect the security measures taken by the contractor. In addition, the contractor will provide to the contracting authority and, where nationally required, the competent national SAA a statement of compliance certifying that the contractor CIS and respective

interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.

20. Minimum requirements for CIS handling EUCI at RESTREINT UE/EU RESTRICTED level are laid down in Appendix III to this SAL.

PARTICULAR REQUIREMENTS FOR INFORMATION CLASSIFIED CONFIDENTIEL UE/EU CONFIDENTIEL OR SECRET UE/EU SECRET

21. A Facility Security Clearance (FSC) at the relevant classification level, confirmed to the Contracting Authority by the NSA/DSA of the EU pMS where the contractor/subcontractor is registered is a mandatory requirement for the handling or granting access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL OR SECRET UE/EU SECRET. Additionally, contractor or subcontractor personnel who, for the performance of this classified contract require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL OR SECRET UE/EU SECRET shall be granted a Personnel Security Clearance (PSC) by the respective NSA/DSA or any other competent security authority in accordance with national laws and regulations and the minimum standards laid down in Article 7 and Annex I of the CSR.

22. For obtaining the confirmation of a FSC, the following information shall have been provided by the potential contractors to the contracting authority when making the offer for the classified contract's call for tender, and every time thereafter when there is a change to it: 1- Full facility name, 2- full facility physical address, 3- mailing address (if different from 2), 4- Zip code / city / country, 5- Facility Security officer' name, phone, fax and email :

Any communication relating to security clearances (FSC/PSC/RfV) should be sent to the following address:

European Defence Agency
Security Office
Rue de Drapiers 17-23
B - 1050 Brussels

e-mail: security@eda.europa.eu

CONDITIONS UNDER WHICH THE CONTRACTOR MAY SUBCONTRACT

23. The contractor must obtain written permission from EDA, as contracting authority, before subcontracting any parts of a classified contract.

24. No subcontract may be awarded to industrial or other entities registered in a non-EU Member State which has not concluded a security of information Agreement with the EU or Security Administrative Arrangement with EDA.

25. Where the Contractor has let a subcontract, the security provisions of this annex will apply *mutatis mutandis* to the subcontractor(s) and its/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.

26. The contractor may not grant access to subcontractors' personnel or to transmit any classified information or material to a subcontractor without the prior written consent from the contracting authority. If transmission of EUCI to subcontractors will be frequent or routine, then the contracting authority may issue an approval to cover a specified length of time (e.g. 12 months) or the duration of the subcontract.

VISITS

27. Should EDA, contractor(s) or subcontractors require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above or unescorted access to secured areas, in each other premises, visits shall be arranged in connection with the NSA/DSA concerned, following standard international visit procedures: a visit request will be submitted by the visitor through his/her Facility Security Officer, certifying/requesting NSA/DSA and receiving NSA/DSA to the agency, organization or facility to be visited. For related visits to the same level of classified meetings organized by EDA, a Request

for Visit (RfV) form[2] shall be sent filled out with the required data to EDA Security Unit (security@eda.europa.eu), at least five (5) working days prior to the visit.

28. Visits relating to information classified RESTREINT UE/EU RESTRICTED will be arranged directly between the sending and receiving establishments, without the need to follow the above described procedure.

ASSESSMENT VISITS

29. EDA Security Office may, in coordination with the relevant NSA/DSA, conduct visits at concerned contractors' or subcontractors' facilities to verify proper implementation of the security requirements for handling EUCI.

SECURITY CLASSIFICATION GUIDE

30. A list of the items in this contract which are classified or to be classified in the course of performance and the rules for so doing are contained in the Security Classification Guide (SCG). The SGC is an integral part of this contract and can be found in Appendix II to this annex.

31. Changes may occur, during the life-time of the contract, regarding the classification of information to be created by or provided to Contractors. In such case, any subsequent change to the SCG (up to the overall level of classification of the contract) will be officially notified by EDA to the contractor(s) and to the Member State(s) NSA(s)/DSA(s) to keep them informed over the abovementioned changes.

[2] An EDA RfV in electronic form could be provided by EDA Security, upon FSO's contractors requests to security@eda.europa.eu.

APPENDIX II
SECURITY CLASSIFICATION GUIDE

TABLE OF CONTENT

Introduction

As stated in the Council Security Rules 2013/488/EU (CSR), prior to launching the call for tender and letting this classified contract, the EDA, as the contracting authority, has determined the security classification of any information that has been provided to bidders or contractors, as well as the security classification of any information that has to be created by the contractor. For that purpose, the EDA has prepared this Security Classification Guide (SCG) to be used for the performance of the contract.

The overall level of classification of this contract may not be lower than the highest classification of any of its elements. At this respect, the overall classification is SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL (delete accordingly).

This SCG may be expanded throughout the life of this contract and the elements of information may be re-classified or downgraded.

The SCG has two parts: the General Instructions and the Elements Table

General Instructions

With regard to European Union Classified Information (EUCI) created or handled by the contractor or subcontractor, the rights incumbent on the originator shall be exercised by the EDA, as the contracting authority (see point 23, Annex V of CSR). In this respect, EUCI created during the performance of this contract should bear the originator identifier as explained further below in these general instructions (markings).

EDA, as originator, retains control of every EUCI which created under the performance of this contract. This means that its prior written consent must be sought before EUCI is:

(a) downgraded or declassified;

(b) used for purposes other than those established by the originator;

(c) disclosed to any third State or international organisation;

(d) disclosed to another contractor or prospective contractor.

EUCI in electronic form may only be created on CIS accredited by the competent Security Accreditation Authority. The classified information itself as well as the filename and storage device (if external, such as CD-ROMs or USB sticks) must bear the relevant security classification marking.

Hardcopies or electronic versions of documents (e.g. studies, reports, analysis, specifications and descriptions, technical requirements, performances or any other documentation) as well as data storage media (e.g. floppy disks, compact disks, CD ROMS, DVD, MP3, memory sticks, microchips, etc.) containing information generated in connection with the Contract shall be assigned an EU security classification as prescribed in this appendix. This includes copies, reproductions, extracts or any other derivatives of documents or data storage media containing such EUCI.

Unless otherwise specified hereafter each document or data storage media shall bear the overall security classification level at maximum SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL (delete accordingly).

In case documents or parts thereof contain information not requiring a security classification or requiring a security classification at a lower level, the different elements shall be identified in a separate check list, stating their respective level of classification. In such a case, each document or data storage media shall bear the highest level of classification of the information contained therein.

A higher classification may be assigned to compilations of documents, which individually require a security classification at a lower level, provided the compilation provides an added factor that warrants a higher classification than that applied to its

component parts. However, such classification of compilations shall not exceed the highest classification level provided for under this Contract.

Any uncertainties concerning security classifications to be applied or any proposals for changes or amendments shall be addressed to the Agency's Contracting Unit, the Project Officer and electronically to security@eda.europa.eu.

Classification

The classification level of EUCI to be created under this contract (elements) shall be determined in accordance with this SCG (see the part Elements Table).

The EUCI to be created during the performance of this contract shall be classified at one of the following levels:

SECRET UE/EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States;

CONFIDENTIEL UE/EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States;

RESTREINT UE/EU RESTRICTED: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

Markings

As stated in the CSR, EUCI shall bear a security classification marking in accordance with the rules given in the paragraph above, and it may bear additional markings to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability. EUCI created during the performance of this contract must bear the originator identifier as explained in the following paragraph.

EDA, as originator, must be clearly identifiable. His originator identifier may be placed alongside or below every occurrence of the security classification marking. Two examples of this are:

RESTREINT UE/EU RESTRICTED – EDA

RESTREINT UE/EU RESTRICTED

EDA

EUCI may bear security caveats in addition to security classification markings .

Elements Table (The data below is just a sample. This elements table shall be completed by the Contracting Authority, the latest before the signature of the contract)

Security classification assigned to information provided, or classification guide for EUCI to be created:

Element	Classification	Declassification/ Downgrading	Remark
EDA Study "xxx", 08.CAP.27	R-UE/EU-R	Declassified after the end of operation XYZ	Available to the selected contractor for assessment during contract performance
A list and description of technology challenges derived from military xxx capabilities requirements, from trends in xxx, vulnerability and defence, enabling technologies identification.	C-UE/EU-C		Expected study result.

APPENDIX III

Minimum requirements for protection of EUCI in electronic form at the level RESTREINT UE/EU RESTRICTED handled in contractor's CIS

General

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

2. It is the responsibility of the contractor to implement the security requirements identified in this document.

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

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

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

6. The use of privately-owned equipment of contractor’s personnel (hardware and software) or processing R-UE/EU-R classified information is not permitted.

7. Accreditation of the contractor’s CIS handling information classified R-UE/EU-R must be approved by the Member State's Security Accreditation Authority (SAA) or delegated to the Security Officer of the contractor as permitted by national laws and regulations.

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

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

10. At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor must provide evidence of compliance with the Contract Security Clause. If also requested, contractors will permit an audit and inspection of the contractor's processes and facilities by representatives of the contracting authority, the NSA/DSA/SAA, or the relevant EU security authority in order to ensure compliance with these requirements.

Physical Security

11. Areas in which CIS are used to display, store, process or transmit R-UE/EU-R information or areas housing servers, network management system, network controllers and communications controllers for such CIS should be established as separate and controlled areas with an appropriate access control system. Access to these separate and controlled areas should be limited to only specifically authorised persons.
Exclusively as described in paragraph 3 have to be stored in this separate and controlled area.

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

Access to CIS

13. Access to contractor's CIS handling EUCI is based on a strict need to know principle.

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

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

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

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

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

19. Security Operating Procedures are available for the Users and Administrators and include security roles descriptions and associated list of tasks, instructions and plans.

Accounting, Audit and Incident Response

20. Any access to the CIS are logged.

21. The following events must be recorded:

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

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

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

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

24. The contractor has established a response strategy to deal with security incidents. Users and Administrators are instructed how to react to incidents, how to report incidents and what to do in case of emergencies.

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

Networking & Interconnection

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

27. Remote access from others systems to LAN services (e.g., remote access to e-mail and remote SYSTEM support) are prohibited unless special security measures are implemented and agreed by the Contracting Authority.

Configuration Management

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

29. Configuration checks are carried out by the Security Officer of the Contractor on hardware and software to ensure that unauthorised hardware and software has not been introduced.

30. Changes to the contractor CIS configuration are assessed for their security implications and must be approved by the SAA/Security Officer.

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

32. The contractor must develop a Business Continuity Plan. Back-up procedures are established addressing the following:

(a) Frequency of back-ups;
(b) Storage requirements on-site (fireproof containers) or off-site;
(c) Control of authorised access to back-up copies.

Sanitisation and Destruction

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

(a) Random data in flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must overwrite at least three times then verify storage content matches the random data or using approved deletion software;
(b) Magnetic media (e.g. hard disks) must be overwritten or degaussed;
(c) Optical media (e.g. CDs and DVDs) must be shredded or disintegrated; and
(d) Concerning other storage media the contracting authority, or if appropriate the NSA/DSA/SAA, should be consulted for the security requirements that need to be met.

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