Council of the
European Union

Brussels, 16 December 2016
(OR. en)

15643/16

CSC 378

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	**Guidelines on Industrial Security**

Delegations will find attached the "Guidelines on Industrial Security" as approved by the Council Security Committee on 13 December 2016.

GUIDELINES ON INDUSTRIAL SECURITY

I. INTRODUCTION

1. These guidelines, agreed by the Council Security Committee in accordance with paragraph 2 of Annex V to the Council security rules[1] (hereinafter 'CSR'), are designed to support implementation of the CSR, and in particular Article 11 and Annex V thereto.

2. These guidelines also take into account Articles 7 and 22 of the Defence and Security Directive[2].

3. These guidelines lay down specific requirements to ensure the protection of EU classified information (hereinafter 'EUCI') by industrial or other entities in pre-contract negotiations and throughout the life-cycle of classified contracts let by the General Secretariat of the Council (GSC) and in subcontracts let by GSC prime contractors.

4. The GSC will apply these security guidelines when entrusting by contract tasks involving or entailing access to or the handling or storage of EUCI by industrial or other entities.

5. When entrusting by contract tasks involving or entailing access to or the handling or storage of EUCI by a contractor or subcontractor, Member States should use these security guidelines as a benchmark.

6. EU agencies and bodies established under Title V, Chapter 2 of the TEU, Europol and Eurojust should use these security guidelines as a reference for implementing security rules in their own structures.

[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).

[2] Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security (OJ L 216, 20.8.2009, p. 76).

II. RESPONSIBILITY WITHIN THE GSC

7. Each GSC Authorising Officer, as part of his or her responsibilities as described in the Financial Regulation[3], will ensure that the minimum standards on industrial security set out in Article 11 of and Annex V to the CSR and in these guidelines are referred to in the contract, and where appropriate in the invitation to tender, and complied with when letting classified contracts.

8. To that effect, the Authorising Officer concerned must seek the advice of the GSC Security Office on issues regarding the classified nature of the contract and the elements of the procedure at all stages.

9. In respect of the requirements of these guidelines, the GSC must cooperate closely with the NSA/DSA or any other relevant competent authority of the Member States concerned, in particular concerning Facility Security Clearances (hereinafter 'FSCs') and Personnel Security Clearances (hereinafter 'PSCs'), visit procedures and transportation plans.

III. PRE-CONTRACTUAL STAGE AND NEGOTIATION OF GSC CLASSIFIED CONTRACTS

Classified contracts

10. A classified contract is a contract to be entered into by the GSC with a contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access or potential access to or the creation of EUCI.

[3] Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 298, 26.10.2012, p. 1).

11. No classified contract 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 entered into an administrative arrangement with the GSC. Should the security of information agreement or administrative arrangement not cover industrial security aspects, a review of the agreement/arrangement is necessary before an entity registered in that non-EU Member State may be awarded a classified contract.

12. Prior to launching an invitation to tender or letting a classified contract, the Authorising Officer, in liaison with the GSC Security Office, must determine the security classification of any information that may be provided to bidders. The Authorising Officer, in liaison with the GSC, will also determine the maximum security classification of any information generated in the performance of the contract, or at least the anticipated volume and type of information to be produced or handled, and the need for a classified Communication and Information System (hereinafter 'CIS'). For that purpose the contracting authority must prepare, in accordance with the 'Policy on creating EUCI'[4], a Security Classification Guide (hereinafter 'SCG') to be used for the performance of the contract.

13. All contractors who are required to handle or store information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either during the performance of the classified contract itself or during the pre-contractual stage, must hold a Facility Security Clearance (hereinafter 'FSC') at the required level. The following identifies the three scenarios that may arise during the tendering phase for a classified contract involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level:

a) No access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level during the tendering phase

When the contract notice, invitation to tender or call for proposals concerns a contract that will involve EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET

[4] 10872/11.

UE/EU SECRET level, but does not require the bidder to handle such information at the tender stage, a bidder not holding an FSC at the required level must not be excluded from the bidding process.

b) Access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level at the premises of the contracting authority during the tendering phase

Access will be granted to contractor personnel who are in possession of a Personnel Security Clearance (hereinafter 'PSC') at the required level and who have a need-to know. The contracting authority will verify with the respective NSA/DSA whether an FSC is also required under national laws and regulations at this stage, before such access is granted.

Where EUCI is provided to a bidder at the tender stage, a non-disclosure agreement must be signed, obliging the bidder to handle and protect EUCI provided to him in accordance with the CSR.

c) Handling or storage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level at the premises of the bidder during the tendering phase

When the contract notice, invitation to tender or call for proposals requires bidders to handle or store EUCI at their premises, the bidder holds an FSC at the required level. In such circumstances the contracting authority will obtain an assurance from the relevant NSA/DSA that the bidder has been granted an appropriate FSC. Access will be granted to contractor personnel who are in possession of a PSC at the required level and who have a need-to-know.

Where EUCI is provided to a bidder at the tender stage, a non-disclosure agreement must be signed, obliging the bidder to handle and protect EUCI provided to him in accordance with the CSR.

An FSC is not required for access to classified information at RESTREINT UE/EU RESTRICTED level, either at the tender stage or for the performance of the contract. However, some EU Member States require an FSC for contracts and subcontracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, as listed in Annex III to these guidelines. Such national requirements shall not put additional obligations on other Member States nor exclude bidders or contractors/subcontractors from Member States not having such FSC requirements for access to RESTREINT UE/EU RESTRICTED information for related contracts/subcontracts or a competition for such, while these contracts shall be performed in Member States according to their national laws and regulations.

14. Where an FSC is required for the performance of a classified contract, the contracting authority will submit a request to the contractor's NSA/DSA using a Facility Security Clearance Information Sheet (hereinafter 'FSCIS'); for guidance, an example of an FSCIS[5] is provided in Annex II, Appendix D. The classified contract will not be awarded until the contractor's NSA/DSA has confirmed the bidder's FSC. Response to an FSCIS should be provided within ten working days of the date of the request.

Subcontracting in classified contracts

15. The conditions under which a contractor awarded a GSC prime contract may subcontract should be defined in the invitation to tender and in the prime contract documentation. If subcontracting is permitted, then a contractor must obtain written consent from the GSC before subcontracting any parts of a classified contract. No classified 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 entered into an administrative arrangement with the GSC.

[5] Other forms used may differ from the example provided in these guidelines in their design. However, they must not differ in their content.

IV. LETTING GSC CLASSIFIED CONTRACTS

16. Upon letting the prime contract, the GSC Security Office will ensure that the obligations of the contractor regarding the protection of EUCI provided to the contractor or generated in the performance of the contract are an integral part of the contract. Contract-specific security requirements may take the form of a Security Aspects Letter (hereinafter 'SAL') (an example of a SAL is provided in Annex II to these guidelines) or of Programme/Project Security Instructions (hereinafter 'PSI').

17. To ensure appropriate security oversight of the contractor, the GSC Security Office will notify and provide a copy of the contract-specific security provisions to the contractor's or subcontractor's NSA/DSA. NSAs/DSAs or any other competent security authority requiring notification about the security provisions of classified contracts at RESTREINT UE/EU RESTRICTED level only are listed in Annex III to these guidelines.

18. Contracts involving classified information at RESTREINT UE/EU RESTRICTED level will include a contract security clause making the provisions specified in Annex II, Appendix E to these guidelines binding upon the contractor. For such purpose contracts involving RESTREINT UE/EU RESTRICTED information will include a SAL detailing, as a minimum, the requirements for handling RESTREINT UE/EU RESTRICTED information including information assurance aspects and specific provisions to be satisfied by a contractor under delegation from the contracting authority for the accreditation of the contractor's CIS handling RESTREINT UE/EU RESTRICTED information.

19. When RESTREINT UE/EU RESTRICTED information is provided to bidders or potential contractors such minimum requirements will also be included in tenders or relevant non-disclosure arrangements concluded at the tender stage.

20. Where required by Member States' national laws and regulations, NSAs/DSAs will be responsible for ensuring that contractors or subcontractors under their jurisdiction comply with the applicable security provisions for the protection of RESTREINT UE/EU

RESTRICTED information and should conduct verification visits on contractors' facilities located in their territory. If an NSA/DSA does not have such an obligation, it is the responsibility of the contracting authority to ensure that the required security provisions detailed in Annex II are implemented by the contractor.

Access to EUCI by contractor and subcontractor personnel

21. The GSC, as contracting authority, will make sure that the classified contract includes provisions indicating that personnel of a contractor or subcontractor who, for the performance of the classified contract or subcontract, require access to EUCI may be granted such access only if:

a) their need-to-know has been determined;
b) they have been granted a PSC at the relevant level for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET by the respective NSA/DSA or any other competent security authority; and
c) they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regard to protecting such information.

22. If a contractor or subcontractor wishes to employ a national of a non-EU country in a position that requires access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, it is the responsibility of the NSA/DSA or any other competent security authority under whose jurisdiction the contractor or subcontractor falls to begin the security clearance procedure in accordance with national laws and regulations.

V. VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

23. Where the GSC, contractors or subcontractors require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract, visits will be arranged in liaison with the NSAs/DSAs or any other competent security authority concerned.

24. Those visits are subject to the following conditions:
    a) the visit must have an official purpose related to a classified contract let by the GSC;
    b) all visitors must hold a PSC at the required level and have a need-to-know in order to access EUCI provided or generated in the performance of a classified contract let by the GSC.

Requests for Visits

25. Visits by contractors to other contractors' facilities, or to GSC premises, that involve access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level are authorised by the following procedure:

    a) the Security Officer of the visitor(s) must complete all the relevant parts of the Request for Visit (RFV) form (an example of the form is provided in Annex II, Appendix C) and submit that request to its NSA/DSA;
    b) the visitor's NSA/DSA will confirm the PSC of the visitor(s) before submitting the RFV to the host facility's NSA/DSA (or the GSC Security Office if the visit is to GSC premises);
    c) the host facility's NSA/DSA (or the GSC Security Office) will reply to the request either authorising or denying the RFV;
    d) an RFV can be considered as approved unless objections are raised five working days prior to the date of the visit.

26. Visits by GSC officials to contractor facilities that involve access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level are authorised by the following process:

a) the visitor(s) must complete all the relevant parts of the RFV form (an example of the form is provided in Annex II, Appendix C), and submit that request to the GSC Security Office;
b) the GSC Security Office will confirm the PSC of the visitor(s) before submitting the RFV to the host facility's NSA/DSA;
c) the host facility's NSA/DSA will reply to the request either authorising or denying the RFV;
d) an RFV can be considered as approved unless objections are raised five working days prior to the date of the visit.

27. An RFV may cover either a single visit or recurring visits. In the case of recurring visits, the RFV can only be valid for up to one year from the start date requested.

28. The validity of any RFV must not exceed the validity of the PSC of the visitor(s).

29. As a general rule an RFV should be submitted to the host facility's competent security authority at least 15 working days prior to the date of the visit.

Visit procedures

30. Before permitting the visitor(s) to have access to EUCI, the host facility must have received authorisation from its NSA/DSA or other competent security authority.

31. Visitors must prove their identity upon arrival at the host facility by presenting a valid ID card or passport as indicated in the RFV.

32. The facility hosting the visit must ensure that records are kept of all visitors, including their names, the organisation they represent, the date of expiry of the PSC, the date of the visit and the name(s) of the person(s) visited. Without prejudice to European data-protection rules, such records are to be retained for a period of no less than three years or in accordance with national rules and regulations, as appropriate.

Visits arranged directly

33. In the context of specific projects, the relevant NSAs/DSAs and the GSC may agree on a procedure whereby visits for a specific classified contract can be arranged directly between the visitor's Security Officer and the Security Officer of the facility to be visited (an example of the form is provided in Annex II, Appendix C). Such an exceptional procedure will be set out in the PSI or other specific arrangements. In such cases, the procedures in paragraphs 25 to 30 do not apply.

34. Visits involving access or potential access to EUCI at RESTREINT UE/EU RESTRICTED level will be arranged directly between the sending and receiving entity without the need to follow the procedure described in paragraphs 25 to 30.

VI. TRANSMISSION AND CARRIAGE OF EUCI

35. The contracting authority must ensure that all transfer and carriage decisions are in accordance with the CSR and with the terms of the classified contract, including the consent of the originator.

Electronic handling

36. Electronic handling and transmission of EUCI must be done in accordance with the provisions laid down in Article 10 of and Annexes IV and V to the CSR. These include, *inter alia*, that Communication and Information Systems owned by a contractor and used for handling EUCI for the performance of the contract (hereinafter 'contractor CIS') will be subject to accreditation by the responsible Security Accreditation Authority, that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 10(6) of the CSR, and that TEMPEST measures must be implemented in accordance with Article 10(5) of the CSR.

37. 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 task is delegated, it is the responsibility of the contractor to implement the minimum security requirements described in the SAL when handling RESTREINT UE/EU RESTRICTED information on its CIS. However, the relevant 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 contractors. 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[6].

[6] Minimum requirements for CIS handling EUCI at R-UE/EU-R level are laid down in Annex II, Appendix E.

Carriage by commercial couriers

38. Carriage of EUCI by commercial couriers, where necessary for the performance of the contract, must be in accordance with the 'Guidelines on the carriage of EUCI by commercial couriers'[7].

Hand carriage of EUCI

39. Hand carriage of EUCI at RESTREINT UE/EU RESTRICTED level by contractor personnel is permitted provided that contractors comply with the following instructions:

a) the envelope/package used must be opaque and bear no indication of the classification of its contents;
b) EUCI must not leave the possession of the bearer; and
c) the envelope/package must not be opened *en route* and the EUCI must not be read in public places.

40. Hand carriage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level by contractor personnel will be arranged between the sending and receiving entities and must comply with the following minimum standards:

a) the EUCI must be carried in a double envelope/package;
b) the outer envelope/package must be secured and bear no indication of the classification of its contents, while the inner envelope must bear the level of classification;
c) EUCI must not leave the possession of the bearer;

[7] 5385/13.

d) the envelope/package must not be opened *en route* and the EUCI must not be read in public places;

e) a lockable briefcase or similar approved container must be of such size and weight that it can be retained at all times in the personal possession of the bearer and not be consigned to a baggage hold;

f) the courier must carry a courier certificate issued by his/her competent security authority authorising the courier to carry the classified consignment as identified.

41. Additional precautions must be taken when CONFIDENTIEL UE/EU CONFIDENTIAL information is carried internationally by contractor personnel:

a) the courier must be responsible for the safe custody of the classified material carried until such time as it has been handed over to the consignee. In the event of a breach of security, the consignor's NSA/DSA may request that the authorities in the country in which the breach occurred carry out an investigation, report their findings and take legal or other action as appropriate;

b) the courier must be briefed on all the security obligations to be observed during carriage and must sign a relevant acknowledgement;

c) the instructions for the courier must be attached to the courier certificate;

d) the courier must also be provided with a description of the consignment and an itinerary;

e) the documents must be returned to the issuing NSA/DSA upon completion of the journey(s) or be kept available at the company for monitoring purposes;
if customs, immigration authorities or border police ask to examine and inspect the consignment, they must be permitted to open and observe sufficient parts of the consignment so as to determine that it does not contain material other than that which is declared;

f) customs authorities may be advised by the appropriate national authorities of the impending consignment and should be urged to honour the official authority of the shipping documents and of the authorisation documents carried by the courier;

g) if a consignment is opened by customs, this should be done out of sight of unauthorised persons and in the presence of the courier where possible. The consignment must be repacked and the authorities conducting the inspection should be asked to reseal the consignment and confirm in writing that it was opened by them.

42. The dispatching authority/facility must inform the receiving authority/facility of the details (e.g. reference, classification, expected time of arrival, name of courier) prior to the hand carriage taking place.

VII. BUSINESS CONTINUITY PLANNING

43. The GSC, as contracting authority, will ensure that the classified contract obliges the contractor to set out contingency plans for protecting EUCI handled in connection with the performance of the classified contract in emergency situations, as well as to put in place preventive and recovery measures in the context of business continuity planning (hereinafter 'BCP') to minimise the impact of incidents in relation to the handling and storage of EUCI. The contractor must inform the GSC of its BCP.

ANNEX I

ARTICLE ON SECURITY IN THE FRAMEWORK CONTRACT
for contracts involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level

21.2 The contractor or subcontractor, and their personnel, must be security cleared to the appropriate level where:

a) the contract or subcontract involves or entails access to, or handling and/or storage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, for which a Facility Security Clearance is required;

b) for the performance of a classified contract, contractor or subcontractor personnel require access to information classified CONFIDENTIEL UE/EU CONFIDENTIEL or SECRET UE/EU SECRET, for which a Personnel Security Clearance is required;

c) for the performance of a contract, contractor or subcontractor personnel are employed in circumstances where they may have access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, for which a Personnel Security Clearance is required;

d) for the performance of the contract, contractor or subcontractor personnel have access to secured areas or are involved in the technical operation or maintenance of communications and information systems containing information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, for which a Personnel Security Clearance is required.

21.3 The contractor or his personnel and, where applicable their subcontractors, must comply with Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information[8]; with the security requirements provided for in the Security Aspects Letter (hereinafter 'SAL'); and with any additional instructions from the Council's Security Office. Should the contractor fail to comply with any of those rules, requirements or instructions, the GSC may, without prejudice to any indemnity due by the contractor to the GSC, terminate the specific contract with immediate effect to the contractor. In those circumstances, no costs or compensation relating to such termination will be due by the GSC to the contractor.

[8] OJ L 274, 15.10.2013, p. 1.

ARTICLE ON SECURITY IN THE FRAMEWORK CONTRACT
for contracts involving EUCI at RESTREINT UE /EU RESTRICTED level only

[21.2] The contractor must handle and protect information classified RESTREINT UE/EU RESTRICTED in accordance with the requirements stated in the SAL.

[21.3] The GSC or competent national security authorities, where required by national laws and regulations, must be entitled to conduct verification visits on the contractor's facilities to ensure compliance with these requirements.

[Annex 4 (to the Framework Contract)]

SECURITY ASPECTS LETTER (SAL)

[Model]

APPENDIX A

SECURITY REQUIREMENTS

The contracting authority must include the following security requirements in the SAL. Some clauses may not be applicable to the contract and are indicated by brackets.

The clauses listed are not an exhaustive list, and additional clauses may be added depending on the nature of the classified contract.

GENERAL CONDITIONS [*note: applicable to all classified contracts*]

1. This Security Aspects Letter (SAL) is an integral part of the classified contract [or subcontract] and describes contract-specific security requirements. Non-compliance with 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 B 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 the GSC, 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, where permitted by its national laws and regulations, to the GSC Security Office 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.

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 instruction from the GSC 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[9].

8. Electronic handling, processing and transmission of EUCI must be done in accordance with the provisions laid down in Article 10 of and Annexes IV and V to the Council security rules (hereinafter 'CSR'). These include, *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[10]; 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] 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).

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

9. The contractor or subcontractor will inform the GSC 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.

CONTRACTS REQUIRING ACCESS TO INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

10. A Personnel Security Clearance (PSC) is not required. However, RESTREINT UE/EU RESTRICTED information or material must only be accessible to contractor 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 security of such information, and have acknowledged in writing the consequences of a failure to protect EUCI.

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

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

13. Information or material classified RESTREINT UE/EU RESTRICTED must be stored in locked office furniture when not in use. When in transit documents must be carried inside an opaque envelope. The documents must not leave the possession of the bearer and they must not be opened *en route* or read in public places.

14. The contractor or subcontractor may transmit documents classified RESTREINT UE/EU RESTRICTED to the GSC using commercial courier companies, postal services, hand carriage or electronic means. To this end, the contractor or subcontractor must follow the Programme Security Instructions (PSI) issued by the GSC.

15. When no longer required, documents classified RESTREINT UE/EU RESTRICTED must be destroyed in such a way that it cannot be reconstructed in whole or in part.

16. 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.

HANDLING OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

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

CONDITIONS UNDER WHICH THE CONTRACTOR MAY SUBCONTRACT

18. The contractor must obtain permission from the GSC, as contracting authority, before subcontracting any parts of a classified contract.

19. No subcontract may be awarded to companies registered in a non-EU Member State which has not concluded a security of information agreement with the EU or an administrative arrangement with the GSC.

20. Where the contractor has let a subcontract, the security provisions of the contract will 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.

21. The contractor may not release any EUCI to a subcontractor without the prior written approval of 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

If the standard RFV procedure is to be applied for visits involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level, then the contracting authority must include paragraphs 22, 23 and 24 and delete paragraph 25. If visits involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level are arranged directly between the sending and receiving establishments, then the contracting authority must delete paragraphs 23 and 24 and only include paragraph 25.

22. Visits involving access or potential access to EUCI at RESTREINT UE/EU RESTRICTED level will be arranged directly between the sending and receiving establishments without the need to follow the procedure described in paragraphs 23 to 25 hereafter.

[23. Visits involving access or potential access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level must be subject to the following procedure:

a) the Security Officer of the visitor(s) must complete all the relevant parts of the RFV form (Appendix C) and submit that request to its NSA/DSA;
b) the NSA/DSA of the visitor(s) will confirm the PSC of the visitor(s) before submitting the RFV to the host facility's NSA/DSA (or the GSC Security Office if the visit is to GSC premises);
c) the host facility's NSA/DSA (or the GSC Security Office) will reply either authorising or denying the RFV;
d) an RFV can be deemed approved unless objections are raised five working days prior to the date of the visit.]

[24. Before permitting the visitor(s) to have access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level, the host facility must have received authorisation from its NSA/DSA.]

[25. Visits involving access or potential access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level will be arranged directly between the sending and receiving establishments (an example of the form that may be used for this purpose is provided in Appendix C).]

26. Visitors must prove their identity upon arrival at the host facility by presenting a valid ID card or passport.

27. The facility hosting the visit must ensure that records are kept of all visitors, including their names, the organisation they represent, the date of expiry of the PSC (if applicable), the date of the visit and the name(s) of the person(s) visited. Without prejudice to European data-protection rules, such records are to be retained for a period of no less than three years or in accordance with national rules and regulations, as appropriate.

ASSESSMENT VISITS

28. The GSC Security Office may, in cooperation with the relevant NSA/DSA, conduct visits at contractors' or subcontractors' facilities to verify proper implementation of the security requirements for handling EUCI.

SECURITY CLASSIFICATION GUIDE

29. A list of all the items in the contract which are classified or to be classified in the course of the performance of the contract and the rules for so doing are contained in the Security Classification Guide (hereinafter 'SCG'). The SCG is an integral part of this contract and can be found in Appendix B to this Annex.

APPENDIX B

SECURITY CLASSIFICATION GUIDE

[specific text to be adjusted depending on the object of the contract]

APPENDIX C

REQUEST FOR VISIT

(MODEL)

DETAILED INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT

(The application must be submitted in English only)

HEADING	Check boxes for visit type, information type, and indicate how many sites are to be visited and the number of visitors.
4. ADMINISTRATIVE DATA	To be completed by requesting NSA/DSA).
5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY	Give full name and postal address. Include city, state and post code as applicable.
6. ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED	Give full name and postal address. Include city, state, post code, telex or fax number (if applicable), telephone number and e-mail. Give the name and telephone/fax numbers and e-mail of your main point of contact or the person with whom you have made the appointment for the visit. Remarks: 1) Giving the correct post code (zip code) is important because a company may have various different facilities. 2) When applying manually, Annex 1 can be used when two or more facilities have to be visited in connection with the same subject. When an Annex is used, item 3 should state: "SEE ANNEX 1, NUMBER OF FAC.:.." (state number of facilities).

7. DATES OF VISIT	Give the actual date or period (date-to-date) of the visit in the format 'day - month - year'. Where applicable, give an alternate date or period in brackets.
8. TYPE OF INITIATIVE	Specify whether the visit has been initiated by the requesting organisation or facility or by invitation of the facility to be visited.
9. THE VISIT RELATES TO:	Specify the full name of the project, contract or call for tender using commonly used abbreviations only.
10. SUBJECT TO BE DISCUSSED/ **JUSTIFICATION**	Give a brief description of the reason(s) for the visit. Do not use unexplained abbreviations. Remarks: In the case of recurring visits this item should state 'Recurring visits' as the first words in the data element (e.g. Recurring visits to discuss_____)
11. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED	State SECRET UE/EU SECRET (S-UE/EU-S) or CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C) as appropriate.
12. PARTICULARS OF VISITOR	Remark: when more than two visitors are involved in the visit, Annex 2 should be used.
13. THE SECURITY OFFICER OF THE REQUESTING ENTITY	This item requires the name, telephone number, fax number and e-mail of the requesting facility's Security Officer.

14. CERTIFICATION OF SECURITY CLEARANCE	This field is to be completed by the certifying authority. Notes for the certifying authority: a. Give name, address, telephone number, fax number and e-mail (can be pre-printed). b. This item should be signed and stamped (if applicable).
15. REQUESTING SECURITY AUTHORITY	This field is to be completed by the NSA/DSA. Note for the NSA/DSA: a. Give name, address, telephone number, fax number and e-mail (can be pre-printed). b. This item should be signed and stamped (if applicable).

All fields must be completed and the form submitted via Government-to-Government channels[11]

REQUEST FOR VISIT

(MODEL)

TO: _____

1. TYPE OF VISIT REQUEST	**2. TYPE OF INFORMATION**	**3. SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____
4. ADMINISTRATIVE DATA:		

[11] If it has been agreed that visits involving access or potential access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level can be arranged directly, the completed form can be submitted directly to the Security Officer of the establishment to be visited.

Requester: To:	NSA/DSA RFV Reference No_____ Date *(dd/mm/yyyy)*: _____/_____/_____

5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED *(Annex 1 to be completed)*

7. DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. TYPE OF INITIATIVE:

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. THE VISIT RELATES TO CONTRACT:

10. SUBJECT TO BE DISCUSSED/REASONS/PURPOSE (Include details of host entity and any other relevant information. Abbreviations should be avoided):

11. ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:
12. PARTICULARS OF VISITOR(S) ***(Annex 2 to be completed)***
13. THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY: NAME: TELEPHONE NO: E-MAIL ADDRESS: SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:

NAME:

ADDRESS:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. REMARKS *(Mandatory justification required in the case of an emergency visit)*:

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

2.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
3. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
4. NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

PARTICULARS OF VISITOR(S)

1.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:
3. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:

4.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

(Continue as required)

APPENDIX D

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

(MODEL)

1. INTRODUCTION

1.1 Attached is a sample Facility Security Clearance Information Sheet (hereinafter 'FSCIS') for the rapid exchange of information between the National Security Authority or Designated Security Authority (hereinafter 'NSA/DSA'), other competent national security authorities and the GSC (as contracting authority) with regard to the Facility Security Clearance (hereinafter 'FSC') of a facility involved in classified tenders, contracts or subcontracts.

1.2 The FSCIS is valid only if stamped by the relevant NSA/DSA or other competent authority.

1.3 The FSCIS is divided into a request and reply section and can be used for the purposes identified above or for any other purposes for which the FSC status of a particular facility is required. The reason for the enquiry must be identified by the requesting NSA/DSA in field 7 of the request section.

1.4 The details contained in the FSCIS are not normally classified; accordingly, when an FSCIS is to be sent between the respective NSAs/DSAs/GSC this should preferably be done by electronic means.

1.5 NSAs/DSAs should make every effort to respond to an FSCIS request within ten working days.

1.6 Should any classified information be transferred or a contract awarded in relation to this assurance, the issuing NSA/DSA must be informed.

Procedures and Instructions for the

use of the Facility Security Clearance Information Sheet (FSCIS)

These detailed instructions are for the NSA/DSA or GSC contracting authority that completes the FSCIS. The request should preferably be typed in capital letters

HEADER	The requester inserts full NSA/DSA and country name.
1. REQUEST TYPE	The requesting contracting authority selects the appropriate checkbox for the type of FSCIS request. Include the level of security clearance requested. The following abbreviations should be used: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = Communication and information systems for processing classified information
2. SUBJECT DETAILS	Fields 1 to 6 are self-evident. In field 4 the standard two-letter country code should be used. Field 5 is optional.
3. REASON FOR REQUEST	Give the specific reason for the request, provide project indicators, number of contract or invitation to tender. Please specify the need for storage capability, CIS classification level, etc. Any deadline/expiry/award dates which may have a bearing on the completion of an FSC should be included.
4. REQUESTING NSA/DSA	State the name of the actual requester (on behalf of the NSA/DSA) and the date of the request in number format (dd/mm/yyyy).
5. REPLY SECTION	Fields 1-5: select appropriate fields. Field 2: if an FSC is in progress, it is recommended to give the requester an

	indication of the required processing time (if known). Field 6: a) Although validation differs by country or even by facility, it is recommended that the expiry date of the FSC be given. b) In cases where the expiry date of the FSC assurance is indefinite, this field may be crossed out. c) The requester is responsible for applying for a renewal of the FSC.
6. REMARKS	May be used for additional information with regard to the FSC, the facility or the foregoing items.
7. ISSUING NSA/DSA	State the name of the providing authority (on behalf of the NSA/DSA) and the date of the reply in number format (dd/mm/yyyy).

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

(MODEL)

All fields must be completed and the form communicated via Government-to-Government or Government-to-international organisation channels

REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE

TO: _____

(NSA/DSA Country name)

Please complete the reply boxes, where applicable:

[ ] Provide an FSC assurance at the level of: [ ] S-UE/EU-S [ ] C-UE/EU-C

for the facility listed below

[ ] Including safeguarding of classified material/information

[ ] Including Communication and Information Systems (CIS) for processing classified information

[ ] Initiate the process of obtaining an FSC up to and including the level of .....… with …….level of safeguarding and ……level of CIS, if the facility does not currently hold these levels of capabilities.

Confirm accuracy of the details of the facility listed below and provide corrections/additions as required.

1. Full facility name: Corrections/Additions:

…….. ……..…….

2. Full facility address:

…….. …….

3. Postal address(if different from 2)

…….. …….

4. Zip/post code/city/country

……... …….…….

5. Name of the Security Officer

…….....

...…….……..….

6. Telephone/Fax/E-mail of the Security Officer

…….. …….…….

7. This request is made for the following reason(s): (provide details of the pre-contractual stage, contract, subcontract, programme/project, etc.)

…….....……

Requesting NSA/DSA/EU contracting authority: Name: …… Date:(dd/mm/yyyy) ……

REPLY (within ten working days)

This is to certify that:

1. [ ] the abovementioned facility holds an FSC up to and including the level of [ ] S-UE/EU-S

[ ] C-UE/EU-C.

2. The abovementioned facility has the capability to safeguard classified information/material:

[ ] yes, level: ……. [ ] no.

3. the abovementioned facility has accredited/authorised CIS:

[ ] yes, level: ……. [ ] no.

4. [ ] in relation to the abovementioned request, the FSC process has been initiated. You will be informed

when the FSC has been established or refused.

5. [ ] the abovementioned facility does not hold an FSC.

6. This FSC assurance expires on: ……. (*dd/mm/yyyy*), or as advised otherwise by the NSA/DSA. In the case of earlier invalidation or any changes to the information listed above, you will be informed.

7. Remarks:

.....……..……
…

Issuing NSA/DSA Name: …… *Date:(dd/mm/yyyy)……*

APPENDIX E

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

General

1. The contractor must be responsible for ensuring that the protection of RESTREINT UE/EU RESTRICTED 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 RESTREINT UE/EU RESTRICTED 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 RESTREINT UE/EU RESTRICTED classified information is not permitted.

7. Accreditation of the contractor's CIS handling information classified RESTREINT UE/EU RESTRICTED 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 RESTREINT UE/EU RESTRICTED 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 RESTREINT UE/EU RESTRICTED 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 RESTREINT UE/EU RESTRICTED 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. Without prejudice to paragraph 8 equipment as described in paragraph 3 has to be stored in such separate and controlled areas.

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 and authorisation of personnel.

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 RESTREINT UE/EU RESTRICTED 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 RESTREINT UE/EU RESTRICTED 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 RESTREINT UE/EU RESTRICTED 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 RESTREINT UE/EU RESTRICTED 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 RESTREINT UE/EU RESTRICTED.

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 and where nationally required, approved by the competent SAA.

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 Security Officer and where nationally required, the SAA.

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 recognised 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 RESTREINT UE/EU RESTRICTED must be sanitised on any data storage media before it is given to an entity not authorised to access RESTREINT UE/EU RESTRICTED (e.g. for maintenance work).

ANNEX III

Facility and Personnel Security Clearance for contractors involving RESTREINT UE/EU RESTRICTED information and NSAs/DSAs requiring notification of the security provisions of classified contracts at RESTREINT UE/EU RESTRICTED level[12]

Member State	FSC		Notification of contract/subcontract involving R-UE/EU-R information to NSA/DSA		PSC	
	YES	NO	YES	NO	YES	NO
Belgium		X		X		X
Bulgaria		X		X		X
Czech Republic		X		X		X
Denmark	X		X		X	
Germany		X		X		X
Estonia	X		X			X
Ireland						
Greece	X			X	X	
Spain		X	X			X
France		X		X		X

[12] These national requirements for FSC/PSC and notifications for contracts involving RESTREINT UE/EU RESTRICTED classified information must not place additional obligations on other Member States or contractors under their jurisdiction.

Croatia		**X**	**X**			**X**
Italy		**X**	**X**			**X**
Cyprus		**X**	**X**			**X**
Latvia		**X**		**X**		**X**
Lithuania	**X**		**X**			**X**
Luxembourg	**X**				**X**	
Hungary		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Netherlands	**X** (for defence-related contracts only)		**X** (for defence-related contracts only)			**X**
Austria						
Poland		**X**		**X**		**X**
Portugal		**X**		**X**		**X**
Romania		**X**		**X**		**X**
Slovenia	**X**		**X**			**X**
Slovakia	**X**		**X**			**X**
Finland		**X**		**X**		**X**

Sweden	**X** (for defence-related contracts only)		**X** (for defence-related contracts only)		**X** (for defence-related contracts only)	
United Kingdom		**X**		**X**		**X**

ANNEX IV

LIST OF NSA/DSA DEPARTMENTS RESPONSIBLE FOR HANDLING INDUSTRIAL SECURITY-RELATED PROCEDURES

BELGIUM

National Security Authority

FPS Foreign Affairs

Rue des Petits Carmes 15

1000 Brussels

Tel.: +32 25014542 (Secretariat)

Fax: +32 25014596

E-mail: nvo-ans@diplobel.fed.be

BULGARIA

1. State Commission on Information Security - National Security Authority

Cherkovna Str. 90

1505 Sofia

Bulgaria

Tel.: +3592 9333 600

Fax: +3592 9873 750

E-mail: dksi@government.bg

2. Military Information Service of the Ministry of Defence (Security Service)

3 Dyakon Ignatiy Str. the Secu

1092 Sofia

Bulgaria

Tel.: +3592 8551 042; +3592 9220 922; +3592 9227 526

E-mail: presscntr@md.government.bg

3. State Agency Intelligence (Security Service)

12 Haidushka Polyana Str.

1612 Sofia

Bulgaria

Tel.: +3592 9813 221

E-mail: headoffice@nrs.bg

4. State Agency for Technical Operations (Security Service)

29 Shesti Septemvri Str.

1000 Sofia

Bulgaria

Tel.: +3592 9877 121, +3592 9824 110

Conduct the vetting procedures for issuing FSC and PSC to legal entities and individuals that apply for concluding a classified contract or who fulfil a classified contract for the needs of these authorities.

5. State Agency 'National Security' (Security Service)

45 Cherni Vrah Blvd

1407 Sofia

Bulgaria

Tel.: +3592 8147 109; +3592 8147 108

Fax: +3592 9632 188; +3592 8147 441

E-mail: dans@dans.bg

Conducts the vetting procedures for issuing FSC and PSC to all other legal entities and individuals in the country that apply for concluding a classified contract or who fulfil a classified contract.

CZECH REPUBLIC

National Security Authority
Industrial Security Department
Ms Lenka Ivincova, Head of INDUSEC unit
Tel.: +420 257 283 388
E-mail: l.ivincova@nbu.cz
PO BOX 49
150 06 Praha 56
Czech Republic

DENMARK

1. Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel.: +45 33148888
Fax: +45 33430190

2. Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel.: +45 33325566
Fax: +45 33931320

GERMANY

1. For industrial security policy matters, FSCs, Transportation Plans (except for crypto /CCI):

Federal Ministry of Economic Affairs and Energy

Industrial Security Division - ZB3

Villemombler Str. 76

53123 Bonn

Germany

E-mail: dsagermany-zb3@bmwi.bund.de (office e-mail address)

Tel.: +49 228 99615 4028

Fax: +49 228 99615 2676

2. For standard visit requests from/to German companies:

Federal Ministry of Economic Affairs and Energy

Industrial Security Division – ZB2

Villemombler Str. 76

53123 Bonn

Germany

Tel.: +49 228 99615 2401

Fax: +49 228 99615 2603

E-mail: zb2-international@bmwi.bund.de (office e-mail address)

3. Transportation Plans for crypto material:

Federal Office for Information Security (BSI)

National Distribution Agency/NDA-EU DEU

Mainzer Str. 84

53179 Bonn

Tel.: +49 (0)228 99 9582 6052

Fax: +49 (0)228 99 10 9582 6052

E-mail: NDAEU@bsi.bund.de

ESTONIA

National Security Authority Department

Estonian Information Board

Rahumäe tee 4B

11316 Tallinn

Tel.: +372 693 9211

Fax: +372 6935001

E-mail: nsa@teabeamet.ee

IRELAND

Ray Walker

National Security Authority

Department of Foreign Affairs and Trade

76-78 Harcourt Street

Dublin 2

Ireland

Official direct line: +353 1 4082123

Mobile phone: +353 87 829 1918

E-mail address: Raymond.Walker@dfa.ie

GREECE

POC Lieutenant Commander (Ltcdr) Spyridon Mexias, Hellenic Navy

Hellenic National Defence General Staff

F' Branch

Security & Counter-Intelligence Directorate

Industrial Security Office

Mesogeion Avenue 227-231

15561 Holargos, Athens Hellas

Tel.: +30 2106572022

Fax: +30 2106527612

E-mail: daa.industrial@hndgs.mil.gr

SPAIN

Autoridad Nacional de Seguridad

Oficina Nacional de Seguridad

Calle Argentona 2028023 Madrid

Tel.: +34 913725000

Fax: +34 913725808

E-mail: nsa-sp@areatec.com

asip@areatec.com

FRANCE

1. Secrétariat général de la défense et de la sécurité nationale

Sous-direction Protection du secret (SGDSN/PSD)

51 boulevard de la Tour-Maubourg

75700 Paris 07 SP

France

Tel.: +33 171758177

Fax: +33 171758200

2. DSA: Direction Générale de l'Armement

Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)

60 boulevard du général Martial Valin

CS 21623

75509 Paris CEDEX 15

France

Tel.: +33 9 8867 0418

E-mail: dga.fax-ssdi.fct@intradef.gouv.fr

CROATIA

Office of the National Security Council

Croatian NSA

Jurjevska 34

10000 Zagreb

Croatia

Tel.: +385 14681222

Fax: +385 14686049

www.uvns.hr

ITALY

Presidenza del Consiglio dei Ministri

D.I.S. - U.C.Se.

Via di Santa Susanna 15

00187 Roma

Tel.: +39 0661174266

Fax: +39 064885273

CYPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ

ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ

Εθνική Αρχή Ασφάλειας (ΕΑΑ)

Υπουργείο Άμυνας

Λεωφόρος Εμμανουήλ Ροΐδη 4

1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22807569; +357 22807643; +357 22807764

Τηλεομοιότυπο: +357 22302351

Ministry of Defence

Minister’s Military Staff

National Security Authority (NSA)

Industrial Security Department

Emanuel Roidi Street 4

1432 Nicosia

Tel.: +357 22807569; +357 22807669; +357 22807764

Fax: +357 22302351

E-mail: cynsa@mod.gov.cy

LATVIA

National Security Authority

Constitution Protection Bureau of the Republic of Latvia

P.O. Box 286

Riga LV-1001

Tel.: +371 67025418 or +371 67 025 463

Fax: +371 67025454

E-mail: ndi@sab.gov.lv or ndi@zd.gov.lv

LITHUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija

(The Commission for Secrets Protection Coordination of the Republic of Lithuania

National Security Authority)

Gedimino 40/1

LT-01110 Vilnius

Tel.: +370 706 66 703, +370 706 66 701

Fax: +370 706 66 700

E-mail: nsa@vsd.lt

LUXEMBOURG

Autorité Nationale de Sécurité

POC: Mr Carlo Mreches

207, route d'Esch

L-1471 Luxembourg

Tel.: +352 24782210

E-mail: ans@me.etat.lu

HUNGARY

National Security Authority of Hungary

POC: Ms Erika Némethné Stadler

Szilágyi Erzsébet fasor 11/B

H-1024 Budapest

Tel.: +36 17952303

Fax: +36-1-795-0345

E-mail: nbf@nbf.hu

postal address: P.O. Box 314, H-1903 Budapest

MALTA

Francis Farrugia

Director

Designated Security Authority for Industrial Security

Standards & Metrology Institute

Malta Competition and Consumer Affairs Authority

Mizzi House,

National Road,

Blata I-Bajda HMR9010

Tel.:+356 2395 2000

Fax: +356 2124 2406

E-mail: francis.p.farrugia@mccaa.org.mt

NETHERLANDS

1. Ministry of the Interior and Kingdom Relations

PO Box 20010

2500 EA The Hague

Tel.: +31 703204400

Fax: +31 703200733

E-mail: nsa-nl-industry@minbzk.nl

2. Ministry of Defence

Industrial Security Department

PO Box 20701

2500 ES The Hague

Tel.: +31 704419407

Fax: +31 703459189

E-mail: indussec@mindef.nl

AUSTRIA

1. Federal Chancellery of Austria,

Department I/12, Office for Information Security

Ballhausplatz 2

1014 Vienna

Austria

Tel.: +43 1 53115 202594

E-mail: isk@bka.gv.at

2. DSA in the military sphere:

BMLVS/Abwehramt

Postfach 2000

1030 Vienna

Austria

E-mail: abwa@bmlvs.gv.at

POLAND

Internal Security Agency

Department for the Protection of Classified Information

Rakowiecka 2A

00-993 Warsaw

Tel: +48 22 58 57 944

Fax: +48 22 58 57 443

E-mail: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança

Serviço de Segurança Industrial

Rua da Junqueira nº 69

1300-342 Lisbon

Tel.: +351 21 303 17 10

Fax: +351 21 303 17 11

E-mail: sind@gns.gov.pt; franco@gns.gov.pt

ROMANIA

Oficiul Registrului Național al Informațiilor Secrete de Stat

(Romanian NSA – ORNISS

National Registry Office for Classified Information)

PoC Prof. dr. Marius Petrescu

Secretary of State

Director General

Tel./Fax: +40 21 224 58 30

E-mail: relatii.publice@orniss.ro

Mr Ion Mihai

Head of Industrial Security and Access Control to Classified Information Department

Tel.: +40 21 20 75 133

Fax: +40 21 224 58 33

E-mail: relatii.publice@orniss.ro; ion.mihai@orniss.ro

Ms Monica Nidelea

Director of Industrial Security Agency

Tel.: +40 21 20 75 132

Fax: +40 21 224 58 33

E-mail: relatii.publice@orniss.ro; monica.nidelea@orniss.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov

Tel.: +386 1 478 1390 Fax: +386 1 4781399

E-mail: gp.uvtp@gov.si

SLOVAKIA

Národný bezpečnostný úrad

(National Security Authority)

Security Clearance Department

Budatinska 30

850 07 Bratislava 57

Tel.: +421 2 6869 2627 (secretariat), +421 2 6869 2629

Fax: +421 2 6869 1706

E-mail: podatelna@nbusr.sk

FINLAND

National Security Authority

Ministry for Foreign Affairs

P.O. Box 453

FI-00023 Government

E-mail: NSA@formin.fi

E-mail: DSA@defmin.fi

SWEDEN

1. National Security Authority

Utrikesdepartementet (Ministry for Foreign Affairs)

UD SÄK

SE-103 39 Stockholm

Tel.: +46 84051000

Fax: +46 87231176

E-mail: ud-nsa@gov.se

2. DSA

Försvarets Materielverk (Swedish Defence Materiel Administration)

FMV Säkerhetsskydd

SE-115 88 Stockholm

Tel.: +46 8 782 40 00

Fax: +46 8 782 69 00

E-mail: registrator@fmv.se

UNITED KINGDOM

UK National Security Authority

Room 335, 3rd Floor

70 Whitehall

London

SW1A 2AS

Tel. 1: +44 2072765497

Tel. 2: +44 2072765645

Fax: +44 2072765651

E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk