COMMISSION DECISION (EU, Euratom) 2019/1963

of 17 October 2019

laying down implementing rules on industrial security with regard to classified procurement contracts

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission ([1]),

Having regard to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information ([2]),

Having regard to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission ([3]),

After consulting the Commission Security Expert Group, in accordance with Article 41(5) of Decision (EU, Euratom) 2015/444,

Whereas:

(1) Articles 41, 42, 47 and 48 of Decision (EU, Euratom) 2015/444 provide that more detailed provisions to supplement and support Chapter 6 of that Decision are to be laid down in implementing rules on industrial security, governing issues such as tendering, conclusion of classified contracts, facility security clearances, personnel security clearances, visits and transmission and carriage of European Union classified information (EUCl).

(2) Decision (EU, Euratom) 2015/444 states that classified contracts are to be implemented in close cooperation with the national security authority, the designated security authority or any other competent authority of the Member States concerned; the Member States have agreed to ensure that any entity under their jurisdiction which may receive or generate classified information originating in the Commission is appropriately security cleared and is capable of providing suitable protection equivalent to that afforded by the security rules of the Council of the European Union for protecting EU classified information bearing a corresponding classification marking, as provided in Agreement between the Member States of the European Union, meeting within Council, regarding the protection of classified information exchanged in the interests of the European Union (2011/C 202/05) ([4]).

(3) The Council, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy have agreed to ensure maximum consistency in the application of security rules regarding their protection of EUCI while taking into account their specific institutional and organisational needs, in accordance with the declarations attached to the minutes of the Council session at which Council Decision 2013/488/EU ([5]) on the security rules for protecting EU classified information was adopted.

(4) The Commission's implementing rules on industrial security with regard to classified contracts should therefore also ensure maximum consistency and take into account the Guidelines on Industrial Security approved by the Council Security Committee on 13 December 2016 and Articles 7 and 22 of Directive 2009/81/EC of the European Parliament and of the Council ([6]).

(5) On 4 May 2016 the Commission adopted a decision ([7]) empowering the Member of the Commission responsible for security matters to adopt, on behalf of the Commission and under its responsibility, the implementing rules provided for in Article 60 of Decision (EU, Euratom) 2015/444,

([1]) OJ L 72, 17.3.2015, p. 41.
([2]) OJ L 72, 17.3.2015, p. 53.
([3]) OJ L 6, 11.1.2017, p. 40.
([4]) OJ C 202, 8.7.2011, p. 13.
([5]) 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).
([6]) 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).
([7]) Commission Decision of 4 May 2016 on an empowerment relating to security (C(2016) 2797 final).

HAS ADOPTED THIS DECISION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Decision sets out implementing rules on industrial security with regard to classified procurement contracts to support the implementation of Decision (EU, Euratom) 2015/444, and in particular Chapter 6 of that Decision.

2. This Decision lays down specific requirements to ensure the protection of EU classified information (EUCI) by economic operators in pre-contract stage, throughout the life cycle of classified contracts concluded by the European Commission, and in subcontracts concluded by Commission contractors.

3. This Decision concerns information classified at the following levels:

(a) RESTREINT UE/EU RESTRICTED;

(b) CONFIDENTIEL UE/EU CONFIDENTIAL;

(c) SECRET UE/EU SECRET.

Article 2

Responsibility within the Commission

1. As part of the responsibilities as described in the Financial Regulation ([8]), each authorising officer of the Commission contracting authority shall ensure that the classified contract refers to the minimum standards on industrial security set out in Chapter 6 of Decision (EU, Euratom) 2015/444 and in these implementing rules, and where appropriate in the contract notice or the invitation to tender, and that these standards are met in the course of implementation.

2. To that end, the authorising officer concerned shall, at all stages, seek the advice of the Commission security authority on issues regarding the security elements of a classified contract, programme or project, and shall inform the local security officer about the contracts concluded. The decision on the classification level of specific subjects shall rest with the contracting authority and shall be taken with due regard to the security classification guide.

3. In respecting the requirements of these implementing rules, the Commission security authority shall cooperate closely with the national security authorities (NSAs) and the designated security authorities (DSAs) of the Member States concerned, in particular as regards facility security clearances (FSCs) and personnel security clearances (PSCs), visit procedures and transportation plans.

CHAPTER 2

HANDLING OF CALLS FOR TENDER FOR CLASSIFIED CONTRACTS

Article 3

Basic principles

1. Classified contracts shall be awarded only to economic operators registered in a Member State, or to economic operators registered in a third country or established by an international organisation where that third country or international organisation has concluded a security of information agreement with the European Union or entered into an administrative arrangement with the Commission ([9]).

2. Before launching an invitation to tender for a classified contract, the contracting authority shall determine the security classification of any information that could be provided to tenderers. The contracting authority shall also determine the maximum security classification of any information generated in the performance of the contract or programme or project, 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 (CIS).

([8]) Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

([9]) The list of agreements concluded by the EU and of administrative arrangements entered into by the European Commission, under which EU classified information may be exchanged with third countries and international organisations, can be found on the Commission website.

3. The contracting authority shall ensure that contract notices for classified contracts provide information about the special security obligations related to classified information. Annex I contains a sample template for the contract notice information.

4. The contracting authority shall ensure that information classified RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET is disclosed to tenderers only after they have signed a non-disclosure agreement, obliging tenderers to handle and protect EUCI in accordance with Decision (EU, Euratom) 2015/444 and its implementing rules.

5. All contractors which 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 at the pre-contractual stage, shall hold an FSC at the required level. The following identifies the three scenarios that may arise during the tendering stage 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 stage:

Where the contract notice or the invitation to tender concerns a contract that will involve EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level, but does not require the tenderer to handle such information at the tender stage, a tenderer which does not hold an FSC at the required level shall not be excluded from the bidding process on the grounds that they do not hold an FSC.

(b) access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the contracting authority during the tendering stage:

Access shall be granted to tenderer personnel who hold a PSC at the required level and who have a need-to-know. Before such access is granted, the contracting authority shall verify, through the Commission security authority, with the respective NSA/DSA whether an FSC is also required under national laws and regulations at this stage.

(c) handling or storage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the tenderer during the tendering stage:

Where the contract notice or the invitation to tender requires tenderers to handle or store EUCI on their premises, the tenderer shall hold an FSC at the required level. In such circumstances the contracting authority shall obtain, through the Commission security authority, an assurance from the relevant NSA/DSA that the tenderer has been granted an appropriate FSC. Access shall be granted to tenderer personnel who hold a PSC at the required level and who have a need-to-know.

6. In principle, an FSC shall not be required for access to RESTREINT UE/EU RESTRICTED information, either at the tender stage or for the performance of the contract. Where Member States require an FSC for contracts or subcontracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, as listed in Annex IV, those national requirements shall not place any additional obligations on other Member States or exclude tenderers, contractors or subcontractors from Member States that have no such FSC requirements for access to RESTREINT UE/EU RESTRICTED information from related contracts/subcontracts or a competition for such. These contracts shall be performed in Member States in accordance with their national laws and regulations.

7. Where an FSC is required for the performance of a classified contract, the contracting authority shall submit, through the Commission security authority, a request to the contractor's NSA/DSA using a facility security clearance information sheet (FSCIS). Annex III, Appendix D, contains an example of an FSCIS ([10]). The classified contract shall not be awarded until the contractor's NSA/DSA has confirmed the tenderer's FSC. Response to an FSCIS is provided, to the extent possible, within ten working days of the date of the request.

([10]) Other forms used may differ from the example provided in these implementing rules in their design.

Article 4

Subcontracting in classified contracts

1. The conditions under which a contractor awarded a Commission classified contract may subcontract shall be defined in the invitation to tender and in the contract documentation. Where the classified contract permits subcontracting of some of its parts, such subcontracting shall be subject to prior written consent from the contracting authority. Before giving its consent, the contracting authority shall consult the Commission security authority.

2. Classified contracts shall be subcontracted only to economic operators registered in a Member State, or to economic operators registered in a third country or established by an international organisation where that third country or international organisation has concluded a security of information agreement with the EU or entered into an administrative arrangement with the Commission ([11]).

CHAPTER 3

LETTING COMMISSION CLASSIFIED CONTRACTS

Article 5

Basic principles

1. When letting a classified contract, the contracting authority, together with the Commission security authority, shall ensure that the contractor's obligations regarding the protection of EUCI provided to that contractor or generated in the performance of the contract are an integral part of the contract. Contract-specific security requirements shall take the form of a security aspects letter (SAL). A sample template of a SAL is set out in Annex III.

2. Before signing a classified contract, the contracting authority shall prepare, after consulting the Commission security authority, a security classification guide (SCG) for the tasks to be performed and information generated in the performance of the contract, or at programme or project level, where applicable. The SCG shall be part of the SAL.

3. Programme or project-specific security requirements shall take the form of a programme (or project) security instruction (PSI). The PSI may be drafted using the provisions of the SAL template as set out in Annex III. The PSI shall be developed by the Commission department managing the programme or project, in close cooperation with the Commission security authority, and submitted for advice to the Commission Security Expert Group. Where a contract is part of a programme or project with its own PSI, the SAL of the contract shall have a simplified form and shall include reference to the security provisions set out in the PSI of the programme or project.

4. The contracting authority shall be considered the originator of classified information created and handled for the performance of the contract.

5. The contracting authority, through the Commission security authority, shall notify the NSAs/DSAs of all contractors and subcontractors about the conclusion of classified contracts or subcontracts and any extensions or early terminations of such contracts or subcontracts. A list of country requirements is provided in Annex IV.

6. Contracts involving information classified RESTREINT UE/EU RESTRICTED shall include a contract security clause making the provisions set out in Annex III, Appendix E binding upon the contractor. Those contracts shall include an SAL setting out, as a minimum, the requirements for handling RESTREINT UE/EU RESTRICTED information including information assurance aspects and specific requirements to be fulfilled by the contractor under delegation from the contracting authority for the accreditation of the contractor's CIS handling RESTREINT UE/EU RESTRICTED information.

([11]) The list of agreements concluded by the EU and of administrative arrangements entered into by the European Commission, under which EU classified information may be exchanged with third countries and international organisations, can be found on the Commission website.

7. Where RESTREINT UE/EU RESTRICTED information is provided to tenderers or to potential contractors, the minimum requirements mentioned in paragraph 6 shall be included in tenders or in relevant non-disclosure arrangements concluded at the tender stage.

8. Where this is required by Member States' national laws and regulations, NSAs/DSAs ensure that contractors or subcontractors under their jurisdiction comply with the applicable security provisions for the protection of RESTREINT UE/EU RESTRICTED information and conduct verification visits to contractors' facilities located in their territory. Where the NSA/DSA is not under such an obligation, the contracting authority shall ensure that the contractor implements the required security provisions set out in Annex III.

Article 6

Access to EUCI by personnel of contractors and subcontractors

1. The Commission department, as contracting authority, shall ensure that classified contracts include 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) it has been established that they have a need-to-know;

(b) for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, they have been granted a PSC at the relevant level by the respective NSA/DSA or any other competent security authority;

(c) they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regard to protecting such information.

2. 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 contractor or subcontractor to initiate the security clearance procedure of such a person in accordance with national laws and regulations applicable at the location where access to the EUCI is to be granted.

CHAPTER 4

VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

Article 7

Basic principles

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

2. The visits referred to in paragraph 1 shall be subject to the following requirements:

(a) the visit shall have an official purpose related to a classified contract let by the Commission;

(b) any visitor shall 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 Commission.

Article 8

Requests for visits

1. Visits by contractors to other contractors' facilities, or to Commission premises, that involve access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged in accordance with the following procedure:

(a) the security officer of the facility sending the visitor shall complete all relevant parts of the request for visit (RFV) form and submit the request to the facility's NSA/DSA. A template of the RFV form is set out in Annex III, Appendix C;

(b) the sending facility's NSA/DSA needs to confirm the visitor's PSC before submitting the RFV to the host facility's NSA/DSA (or the Commission security authority if the visit is to Commission premises);

(c) the security officer of the sending facility shall then obtain from its NSA/DSA the reply of the host facility's NSA/DSA (or the Commission security authority) either authorising or denying the RFV;

(d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.

2. Visits by Commission officials to contractor facilities that involve access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged in accordance with the following procedure:

(a) the visitor shall complete all relevant parts of the RFV form and submit it to the Commission security authority;

(b) the Commission security authority shall confirm the PSC of the visitor before submitting the RFV to the host facility's NSA/DSA;

(c) the Commission security authority shall obtain a reply from the host facility's NSA/DSA either authorising or denying the RFV;

(d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.

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

4. The validity of any RFV shall not exceed the validity of the PSC of the visitor.

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

Article 9

Visit procedures

1. Before allowing visitor to have access to EUCI, the security office of the host facility shall comply with all the visit-related security procedures and rules laid down by its NSA/DSA.

2. Visitors shall prove their identity upon arrival at the host facility by presenting a valid ID card or passport. That identification information shall correspond to the information supplied in the RFV.

3. The host facility shall 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 names of the persons visited. Such records shall be retained for a period of at least five years or longer if required by the national rules and regulations of the country where the host facility is located.

Article 10

Visits arranged directly

1. In the context of specific projects, the relevant NSAs/DSAs and the Commission security authority 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. A template of the form to be used for this purpose is set out in Annex III, Appendix C. Such an exceptional procedure shall be set out in the PSI or other specific arrangements. In such cases, the procedures set out in Article 8 and Article 9(1) shall not apply.

2. Visits involving access to information classified RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending and receiving entity without the need to follow the procedures set out in Article 8 and Article 9(1).

CHAPTER 5

TRANSMISSION AND CARRIAGE OF EUCI IN PERFORMANCE OF CLASSIFIED CONTRACTS

Article 11

Basic principles

The contracting authority shall ensure that all decisions related to EUCI transfer and carriage are in accordance with Decision (EU, Euratom) 2015/444 and its implementing rules, and with the terms of the classified contract, including the consent of the originator.

Article 12

Electronic handling

1. Electronic handling and transmission of EUCI shall be carried out in accordance with Chapters 5 and 6 of Decision (EU, Euratom) 2015/444 and its implementing rules.

The communication and information systems owned by a contractor and used to handle EUCI for the performance of the contract ('contractor CIS') shall be subject to accreditation by the responsible security accreditation authority (SAA). Any electronic transmission of EUCI shall be protected by cryptographic products approved in accordance with Article 36(4) of Decision (EU, Euratom) 2015/444. TEMPEST measures shall be implemented in accordance with Article 36(6) of that Decision.

2. 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 this is permitted by national laws and regulations. Where that task is delegated, the contractor shall be responsible for implementing the minimum security requirements described in the SAL when handling RESTREINT UE/EU RESTRICTED information on its CIS. However, the relevant NSAs/DSAs and SAAs 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 shall provide to the contracting authority and, where required by national laws and regulations, the competent national SAA, a statement of compliance certifying that the contractor CIS and related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level ([12]).

Article 13

Transport by commercial couriers

The transport of EUCI by commercial couriers shall abide by the relevant provisions of Commission decisions on implementing rules for handling RESTREINT UE/EU RESTRICTED information and CONFIDENTIEL UE/EU CONFIDENTIAL information.

Article 14

Hand carriage

1. The carriage of classified information by hand shall be subject to strict security requirements.

2. RESTREINT UE/EU RESTRICTED information may be hand carried by contractor personnel within the EU, provided the following requirements are met:

(a) the envelope or packaging used is opaque and bears no indication of the classification of its contents;

([12]) The minimum requirements for communication and information systems handling EUCI at RESTREINT UE/EU RESTRICTED level are laid down in Annex III, Appendix E.

(b) the classified information does not leave the possession of the bearer;

(c) the envelope or packaging is not opened *en route*.

3. For information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET, hand carriage by contractor personnel within an EU Member State is arranged in advance between the sending and receiving entities. The dispatching authority or facility informs the receiving authority or facility of the details of the consignment, including reference, classification, expected time of arrival and name of courier. Such hand carriage is permitted, provided the following requirements are met:

(a) the classified information is carried in a double envelope or packaging;

(b) the outer envelope or packaging is secured and bears no indication of the classification of its contents, while the inner envelope bears the level of classification;

(c) EUCI does not leave the possession of the bearer;

(d) the envelope or packaging is not opened *en route*;

(e) the envelope or packaging is carried in a lockable briefcase or similar approved container 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 carries a courier certificate issued by his/her competent security authority authorising the courier to carry the classified consignment as identified.

4. For hand carriage by contractor personnel of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from one EU Member State to another, the following additional rules shall apply:

(a) the courier shall be responsible for the safe custody of the classified material carried until it is handed over to the recipient;

(b) in the event of a security breach, the sender's NSA/DSA may request that the authorities in the country where the breach occurred carry out an investigation, report their findings and take legal or other action as appropriate;

(c) the courier shall have been briefed on all the security obligations to be observed during carriage and shall have signed an appropriate acknowledgement;

(d) the instructions for the courier shall be attached to the courier certificate;

(e) the courier shall have been provided with a description of the consignment and an itinerary;

(f) the documents shall be returned to the issuing NSA/DSA upon completion of the journey(s) or be kept available by the recipient for monitoring purposes;

(g) if customs, immigration authorities or border police ask to examine and inspect the consignment, they shall be permitted to open and observe sufficient parts of the consignment so as to establish that it contains no material other than that which is declared;

(h) customs authorities should be urged to honour the official authority of the shipping documents and of the authorisation documents carried by the courier.

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 courier shall request that the consignment be repacked and shall ask the authorities conducting the inspection to reseal the consignment and confirm in writing that it was opened by them.

5. Hand carriage by contractor personnel of information classified RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET to a third country or an international organisation will be subject to provisions of the security of information agreement or the administrative arrangement concluded between, respectively, the European Union or the Commission and that third country or international organisation.

CHAPTER 6

BUSINESS CONTINUITY PLANNING

Article 15

Contingency plans and recovery measures

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

Article 16

Entry into force

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 17 October 2019.

For the Commission,

On behalf of the President,

Günther OETTINGER

Member of the Commission

ANNEX I

STANDARD INFORMATION IN PROCUREMENT CONTRACT NOTICES

(to be adapted to the contract notices used)

For contracts involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET

Other particular conditions (*if applicable*)

The performance of the contract is subject to particular conditions ● yes ○ no

(*if yes*) Description of particular conditions:

The contract will involve access to, handling and/or storage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, which is subject to the security rules for protecting EU classified information laid down in Decision (EU, Euratom) 2015/444 and to the Decision's implementing rules [1].

Facility security clearance will be required as well as personnel security clearances for contractor personnel handling classified information.

Special security obligations will be part of the contract (security aspects letter, annexed to the contract). Subcontracting will be subject to written prior agreement by the contracting authority and compliance with all the security rules by the subcontractor and its personnel.

For contracts involving information classified RESTREINT UE/EU RESTRICTED

Other particular conditions (*if applicable*)

The performance of the contract is subject to particular conditions ● yes ○ no

(*if yes*) Description of particular conditions:

The contract will involve or entail access to, handling and/or storage of information classified RESTREINT UE/EU RESTRICTED, which is subject to the security rules for protecting EU classified information laid down in Decision (EU, Euratom) 2015/444 and to the Decision's implementing rules [2].

Special security obligations will be part of the contract (security aspects letter, annexed to the contract). Subcontracting will be subject to written prior agreement by the contracting authority and compliance with all the security rules by the subcontractor and its personnel.

---

[1] The contracting authority should insert the references once the implementing rules have been adopted.
[2] The contracting authority should insert the references once the implementing rules have been adopted.

ANNEX II

STANDARD PROCUREMENT CONTRACT CLAUSES

(to be adapted to the contracts used)

ARTICLE XX

SECURITY-RELATED OBLIGATIONS

XX.1 EU classified information

If the implementation of the contract involves using or generating EU classified information, such information must be treated in accordance with the security aspects letter (SAL) and its security classification guide (SCG) as set out in Annex 1, and Decision (EU, Euratom) 2015/444 and its implementing rules [1], until it is declassified.

Any deliverables containing classified information must be submitted in accordance with special procedures agreed with the contracting authority.

Action tasks involving classified information must not be subcontracted without prior explicit written approval from the contracting authority.

EU classified information must not be released to any third party (including subcontractors) without prior explicit written approval from the contracting authority.

[1] The contracting authority should insert the references once the implementing rules have been adopted.

ANNEX III

[Annex IV (to the Framework Contract)]

SECURITY ASPECTS LETTER (SAL)

[Model]

Appendix A

SECURITY REQUIREMENTS

The contracting authority must include the following security requirements in the security aspects letter (SAL). Some clauses may not be applicable to the contract. These are shown in square brackets.

The list of clauses is not exhaustive. Further clauses may be added depending on the nature of the classified contract.

GENERAL CONDITIONS

[*N.B.: 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. Failure to meet these requirements may constitute sufficient grounds to terminate the contract.

2. Contractors are subject to all obligations set out in Decision (EU, Euratom) 2015/444 and its implementing rules ([1]).

3. Classified information generated when performing the contract must be marked as EU classified information (EUCI) at security classification level, as determined in the security classification guide (SCG) in Appendix B to this letter. Deviation from the security classification level stipulated by the SCG is permissible only with the written authorisation of the contracting authority.

4. The rights pertaining to the originator of any EUCI created and handled for the performance of the classified contract are exercised by the Commission, as the contracting authority.

5. 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 that authority for any purpose other than that of the contract.

6. The contractor must investigate all security breaches related to EUCI and report them to the contracting authority as soon as is practicable. The contractor or subcontractor must immediately report to its responsible national security authority (NSA) or to the designated security authority (DSA), and, where national laws and regulations so permit, to the Commission security authority, 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.

7. After the end of the contract, the contractor or subcontractor must return any EUCI it holds to the contracting authority as soon as possible. Where practicable, the contractor or subcontractor may destroy EUCI instead of returning it. This must be done in accordance with the national laws and regulations of the country where the contractor is based, with the prior agreement of the Commission security authority, and under the latter's instruction. EUCI must be destroyed in such a way that it cannot be reconstructed, either wholly or in part.

8. 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 Decision (EU, Euratom) 2015/444 (hereinafter 'CD 2015/444'), and with its implementing rules ([2]).

9. Any electronic handling, processing and transmission of EUCI must abide by the provisions laid down in Chapters 5 and 6 of CD 2015/444. These include, inter alia, the requirement that communication and information systems owned by the contractor and used to handle EUCI for the purpose of the contract (hereinafter 'contractor CIS') must be subject to accreditation ([3]); that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 36(4) of CD 2015/444, and that TEMPEST measures must be implemented in accordance with Article 36(6) of CD 2015/444.

([1]) The contracting authority should insert the references once the implementing rules have been adopted.
([2]) The contracting authority should insert the references once the implementing rules have been adopted.
([3]) The party undertaking the accreditation will have to provide the contracting authority with a statement of compliance, through the Commission security authority, and in coordination with the relevant national security accreditation authority (SAA).

10. The contractor or subcontractor shall have business contingency plans (BCP) to protect any EUCI handled in the performance of the classified contract in emergency situations and shall put in place preventive and recovery measures to minimise the impact of incidents associated with the handling and storage of EUCI. The contractor or subcontractor must inform the contracting authority of its BCP.

CONTRACTS REQUIRING ACCESS TO INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

11. A personnel security clearance (PSC) is not required for compliance with the contract. However, information or material classified RESTREINT UE/EU RESTRICTED must be accessible only to contractor personnel who require such information to perform 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 who have acknowledged in writing the consequences of a failure to protect EUCI.

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

13. 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 written consent from the contracting authority.

14. 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*.

15. The contractor or subcontractor may transmit documents classified RESTREINT UE/EU RESTRICTED to the Commission using commercial courier companies, postal services, hand carriage or electronic means. To this end, the contractor or subcontractor must follow the programme (or project) security instruction (PSI) issued by the Commission and/or the Commission implementing rules on industrial security with regard to classified procurement contracts ([4]).

16. When no longer required, documents classified RESTREINT UE/EU RESTRICTED must be destroyed in such a way that they cannot be reconstructed, either wholly or in part.

17. 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 national laws and regulations so permit. Where accreditation is thus delegated, the NSAs/DSAs/SAAs retain responsibility for protecting any RESTREINT UE/EU RESTRICTED information that is handled by the contractor and the right to inspect the security measures taken by the contractor. In addition, the contractor shall provide the contracting authority and, where required by national laws and regulations, the competent national SAA with a statement of compliance certifying that the contractor CIS and the related 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)

18. Minimum requirements for CIS handling information classified RESTREINT UE/EU RESTRICTED are laid down in Appendix E to this SAL.

CONDITIONS UNDER WHICH THE CONTRACTOR MAY SUBCONTRACT

19. The contractor must obtain permission from the Commission department concerned, as the contracting authority, before subcontracting any part of a classified contract.

([4]) The contracting authority should insert the references once the implementing rules have been adopted.

20. No subcontract may be awarded to a company registered in a non-EU Member State or to an entity belonging to an international organisation, if that non-EU Member State or international organisation has not concluded a security of information agreement with the EU or an administrative arrangement with the Commission.

21. Where the contractor has let a subcontract, the security provisions of the contract shall apply *mutatis mutandis* to the subcontractor(s) and its (their) personnel. In such a case, it is the contractor's responsibility to ensure that all subcontractors apply these principles to their own subcontracting arrangements. To ensure appropriate security oversight, the contractor's and subcontractor's NSAs/DSAs shall be notified of the letting of all related classified subcontracts at the levels of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET. Where appropriate, the contractor's and subcontractor's NSAs/DSAs shall be provided with a copy of the subcontract-specific security provisions. NSAs/DSAs requiring notification about the security provisions of classified contracts at RESTREINT UE/EU RESTRICTED level are listed in the annex to the Commission's implementing rules on industrial security with regard to classified procurement contracts ([1]).

22. The contractor may not release any EUCI to a subcontractor without the prior written approval of the contracting authority. If EUCI to subcontractors is to be sent frequently or as a matter of routine, then the contracting authority may give its approval for a specified length of time (e.g. 12 months) or for the duration of the subcontract.

VISITS

If the standard RFV procedure is to be applied to visits involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, then the contracting authority must include paragraphs 23, 24 and 25 and delete paragraph 26. If visits involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET are arranged directly between the sending and receiving establishments, then the contracting authority must delete paragraphs 24 and 25 and include paragraph 26 only.

23. Visits involving access or potential access to information classified RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending and receiving establishments without the need to follow the procedure described in paragraphs 24 to 26 below.

[24. Visits involving access or potential access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be subject to the following procedure:

(a) the security officer of the facility sending the visitor shall complete all relevant parts of the RFV form (Appendix C) and submit the request to the facility's NSA/DSA;

(b) the sending facility's NSA/DSAneeds to confirm the visitor's PSC before submitting the RFV to the host facility's NSA/DSA (or to the Commission security authority if the visit is to Commission premises);

(c) the security officer of the sending facility shall then obtain from its NSA/DSA the reply of the host facility's NSA/DSA (or the Commission security authority) either authorising or denying the RFV;

(d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.]

[25. Before giving the visitor(s) access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, the host facility must have received authorisation from its NSA/DSA.]

[26. Visits involving access or potential access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall 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).]

([1]) The contracting authority should insert the references once the implementing rules have been adopted.

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

28. The facility hosting the visit must ensure that records are kept of all visitors. These must include 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 five years or in accordance with national rules and regulations, as appropriate.

ASSESSMENT VISITS

29. The Commission security authority may, in cooperation with the relevant NSA/DSA, conduct visits to contractors' or subcontractors' facilities to check that the security requirements for handling EUCI are being complied with.

SECURITY CLASSIFICATION GUIDE

30. A list of all the elements in the contract which are classified or to be classified in the course of the performance of the contract, the rules for so doing and the specification of the applicable security classification levels are contained in the security classification guide (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 subject 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 email. Give the name and telephone/fax numbers and email 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 email 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 email (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 email (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 [2]

[2] 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.

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:**

Requester:	NSA/DSA RFV Reference No_____
To:	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:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

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

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

<Placeholder for reference to applicable personal data legislation and link to mandatory information to the data subject, e.g. how Article 13 of the General Data Protection Regulation ([3]) is implemented.>

([3]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

ANNEX 1 to RFV FORM

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:

(Continue as required)

<Placeholder for reference to applicable personal data legislation and link to mandatory information to the data subject, e.g. how Article 13 of the General Data Protection Regulation ([1]) is implemented.>

([1]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

ANNEX 2 to RFV FORM

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:

(Continue as required)

<Placeholder for reference to applicable personal data legislation and link to mandatory information to the data subject, e.g. how Article 13 of the General Data Protection Regulation ([1]) is implemented.>

([1]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Appendix D

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

(MODEL)

1. **Introduction**

1.1. Attached is a sample Facility Security Clearance Information Sheet (FSCIS) for the rapid exchange of information between the National Security Authority (NSA) or Designated Security Authority (DSA), other competent national security authorities and the Commission (as contracting authority) with regard to the Facility Security Clearance (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/Commission 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 the Commission 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 check-box 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) In compliance with respective national rules and regulations, the requester or either the contractor or subcontractor 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, directly or upon a corresponding request of a contractor or subcontractor, 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/Email of the Security Officer	
.....	.....

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

.....

Requesting NSA/DSA/Commission 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)* .....

<Placeholder for reference to applicable personal data legislation and link to mandatory information to the data subject, e.g. how Article 13 of the General Data Protection Regulation ([2]) is implemented.>

([2]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

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 information complies with the minimum security requirements as laid down in this security clause and with any other additional requirements advised by the contracting authority or, if applicable, by the national security authority (NSA) or designated security authority (DSA).

2. It is the contractor's responsibility 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 machines, servers, network management systems, network controllers and communications controllers, laptops, notebooks, tablet PCs, smart phones and removable storage devices such as USB-sticks, CDs, SD-cards, etc.

4. Special equipment, such as 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 security officer responsible for the facility concerned.

6. The use of IT solutions (hardware, software or services) privately owned by contractor staff for storing or processing RESTREINT UE/EU RESTRICTED information is not permitted.

7. Accreditation of the contractor's CIS handling information classified RESTREINT UE/EU RESTRICTED must be approved by the security accreditation authority (SAA) of the Member State concerned or delegated to the contractor's security officer as permitted by national laws and regulations.

8. Only information classified RESTREINT UE/EU RESTRICTED that is encrypted using approved cryptographic products may be handled, stored or transmitted (by wired or wireless means) as any other unclassified information under the contract. Such cryptographic products must be approved by the EU or a Member State.

9. External facilities involved in maintenance/repair work must be contractually obliged 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 an audit and inspection of the contractor's processes and facilities are also requested, to ensure compliance with these requirements, contractors shall permit representatives of the contracting authority, the NSA/DSA/SAA, or the relevant EU security authority to conduct such an audit and inspection.

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 systems, 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 restricted to individuals with specific authorisation. Without prejudice to paragraph 8, equipment as described in paragraph 3 must 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 (such as USBs, mass storage devices or CD-RWs) to components on the CIS.

Access to CIS

13. Access to a contractor's CIS handling EUCI is allowed on a basis of strict need-to-know and authorisation of personnel.

14. All CIS must have up-to-date lists of authorised users. All users must be authenticated at the start of each processing session.

15. Passwords, which are part of most identification and authentication security measures, must be at least nine 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. They must be changed as soon as possible if they have been compromised or disclosed to an unauthorised person, or if such compromise or disclosure is suspected.

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 the 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 must be automatically locked once at least five successive incorrect login attempts have been made.

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. SecOPs must be available for the users and administrators and must include descriptions of security roles and associated list of tasks, instructions and plans.

Accounting, audit and incident response

20. Any access to the CIS must be logged.

21. The following events must be recorded:

    (a) all attempts to log on, whether successful or failed;

    (b) logging off (including being timed out, where applicable);

    (c) creation, deletion or alteration of access rights and privileges;

    (d) creation, deletion or alteration of passwords.

22. For all of the events listed above the following information must be communicated as a minimum:

    (a) type of event;

    (b) user ID;

    (c) date and time;

    (d) device ID.

23. The accounting records should provide help to a security officer to examine the potential security incidents. They can also 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 must have an established response strategy to deal with security incidents. Users and administrators must be instructed on how to respond to incidents, how to report them and what to do in the event of emergency.

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 compromise or 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 and interconnection

26. When a contractor CIS that handles information classified RESTREINT UE/EU RESTRICTED is interconnected to a CIS that is not accredited, this significantly increases the threat to both the security of the CIS and the RESTREINT UE/EU RESTRICTED information that is handled by that CIS. This includes the internet and other public or private CIS, such as other CIS owned by the contractor or subcontractor. 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 shall provide to the contracting authority, and where required by national laws and regulations, the competent SAA, a statement of compliance certifying that the contractor CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.

27. Remote access from other systems to LAN services (e.g. remote access to email and remote SYSTEM support) is prohibited unless special security measures are implemented and agreed by the contracting authority, and where required by national laws and regulations, 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) must be available and regularly maintained.

29. The contractor's security officer must conduct configuration checks on hardware and software to ensure that no unauthorised hardware or software has been introduced.

30. Changes to the contractor CIS configuration must be assessed for their security implications and must be approved by the security officer, and where required by national laws and regulations, the SAA.

31. The system must be scanned for any security vulnerabilities at least once a quarter. Software to detect malware must be installed and kept up-to-date. If possible, such 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 must be established to address 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 have at any time held RESTREINT UE/EU RESTRICTED information the following sanitisation must be performed to the entire system or to storage media before its disposal:

(a) flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must be overwritten at least three times and then verified to ensure that the original content cannot be recovered, or be deleted 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;

(d) for any other storage media, the contracting authority or, if appropriate, the NSA/DSA/SAA should be consulted on the security requirements to be met.

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

ANNEX IV

Facility and personnel security clearance for contractors involving RESTREINT UE/EU RESTRICTED information and NSAs/DSAs requiring notification of classified contracts at RESTREINT UE/EU RESTRICTED level [1]

Member State	FSC		Notification of contract or 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
Czechia		X		X		X
Denmark	X		X		X	
Germany		X		X		X
Estonia	X		X			X
Ireland		X		X		X
Greece	X			X	X	
Spain		X	X			X
France		X		X		X
Croatia		X	X			X
Italy		X	X			X
Cyprus		X	X			X
Latvia		X		X		X

[1] These national requirements for FSC/PSC and notifications for contracts involving RESTREINT UE/EU RESTRICTED information must not place any additional obligations on other Member States or contractors under their jurisdiction.
N.B.: Notifications of contracts involving CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information are obligatory.

Member State	FSC		Notification of contract or subcontract involving R-UE/EU-R information to NSA/DSA		PSC	
	YES	NO	YES	NO	YES	NO
Lithuania	X		X			X
Luxembourg	X		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		X		X		X
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 V

LIST OF NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY DEPARTMENTS RESPONSIBLE FOR HANDLING PROCEDURES ASSOCIATED WITH INDUSTRIAL SECURITY

BELGIUM

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels
Tel. +32 25014542 (Secretariat)
Fax +32 25014596
Email: nvo-ans@diplobel.fed.be

BULGARIA

1. State Commission on Information Security — National Security Authority
   4 Kozloduy Street
   1202 Sofia
   Tel. +359 29835775
   Fax +359 29873750
   Email: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)
   3 Dyakon Ignatiy Street
   1092 Sofia
   Tel. +359 29227002
   Fax +359 29885211
   Email: office@iksbg.org

3. State Intelligence Agency (security service)
   12 Hajdushka Polyana Street
   1612 Sofia
   Tel. +359 29813221
   Fax +359 29862706
   Email: office@dar.bg

4. State Agency for Technical Operations (security service)
   29 Shesti Septemvri Street
   1000 Sofia
   Tel. +359 29824971
   Fax +359 29461339
   Email: dato@dato.bg

   (The competent authorities listed above conduct the vetting procedures for issuing FSCs to legal entities applying to conclude a classified contract, and PSCs to individuals implementing a classified contract for the needs of these authorities.)

5. State Agency National Security (security service)
   45 Cherni Vrah Blvd.
   1407 Sofia
   Tel. +359 28147109
   Fax +359 29632188, +359 28147441
   Email: dans@dans.bg

   (The above security service conducts the vetting procedures for issuing FSCs and PSCs to all other legal entities and individuals in the country applying to conclude a classified contract or implementing a classified contract.)

CZECHIA

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56
Tel. +420 257283129
Email: sbr@nbu.cz

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 matters concerning industrial security policy, FSCs, transportation plans (except for crypto/CCI):
Federal Ministry of Economic Affairs and Energy
Industrial Security Division — ZB3
Villemombler Str. 76
53123 Bonn
Tel. +49 228996154028
Fax +49 228996152676
Email: dsagermany-zb3@bmwi.bund.de (office email address)

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
Tel. +49 228996152401
Fax +49 228996152603
Email: zb2-international@bmwi.bund.de (office email 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 2289995826052
Fax +49 228991095826052
Email: NDAEU@bsi.bund.de

ESTONIA

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn
Tel. +372 6939211
Fax +372 6935001
Email: nsa@fis.gov.ee

IRELAND

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45
Tel. +353 14082724
Email: nsa@dfa.ie

GREECE

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Athens
Tel. +30 2106572022, +30 2106572178
Fax +30 2106527612
Email: daa.industrial@hndgs.mil.gr

SPAIN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid
Tel. +34 913725000
Fax +34 913725808
Email: nsa-sp@areatec.com
For matters concerning personnel security clearances: asip@areatec.com
For Transportation plans and international visits: sp-ivtco@areatec.com

FRANCE

National Security Authority (NSA) (for policy and for implementation in fields other than the defence industry)
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
Tel. +33 171758193
Fax +33 171758200
Email: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (for implementation in the defence industry)
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
Tel. +33 988670421
Email: for forms and outgoing RFVs: dga-ssdi.ai.fct@intradef.gouv.fr
for incoming RFVs: dga-ssdi.visit.fct@intradef.gouv.fr

CROATIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Tel. +385 14681222
Fax +385 14686049
Email: NSACroatia@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
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία
Τηλέφωνα: +357 22807569, +357 22807764
Τηλεομοιότυπο: +357 22302351
Email: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia
Tel. +357 22807569, +357 22807764
Fax +357 22302351
Email: 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, +371 67025463
Fax +371 67025454
Email: ndi@sab.gov.lt, 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 70666703, +370 70666701
Fax +370 70666700
Email: nsa@vsd.lt

LUXEMBOURG

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg
Tel. +352 24782210
Email: ans@me.etat.lu

HUNGARY

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 13911862
Fax +36 13911889
Email: nbf@nbf.hu

MALTA

Director of Standardisation
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 23952000
Fax +356 21242406
Email: certification@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
Email: 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
Email: indussec@mindef.nl

AUSTRIA

1. Federal Chancellery of Austria
Department I/12, Office for Information Security
Ballhausplatz 2
1014 Vienna
Tel. +43 153115202594
Email: isk@bka.gv.at

2. DSA in the military sphere:
BMLVS/Abwehramt
Postfach 2000
1030 Vienna
Email: abwa@bmlvs.gv.at

POLAND

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warsaw
Tel. +48 225857944
Fax +48 225857443
Email: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira nº 69
1300-342 Lisbon
Tel. +351 213031710
Fax +351 213031711
Email: sind@gns.gov.pt, franco@gns.gov.pt

ROMANIA

Oficiul Registrului Național al Informațiilor Secrete de Stat — ORNISS
Romanian NSA — ORNISS — National Registry Office for Classified Information
4th Mures Street
012275 Bucharest
Tel. +40 212075115
Fax +40 212245830
Email: relatii.publice@orniss.ro, nsa.romania@nsa.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Fax +386 14781399
Email: gp.uvtp@gov.si

SLOVAKIA

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava
Tel. +421 268691111
Fax +421 268691700
Email: podatelna@nbu.gov.sk

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Email: NSA@formin.fi

SWEDEN

1. National Security Authority
   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK/NSA
   SE-103 39 Stockholm
   Tel. +46 84051000
   Fax +46 87231176
   Email: ud-nsa@gov.se

2. DSA
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Tel. +46 87824000
   Fax +46 87826900
   Email: security@fmv.se

UNITED KINGDOM

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel. +44 2072765497, +44 2072765645
Email: UK-NSA@cabinet-office.x.gsi.gov.uk