Attachment

SECURITY OF INFORMATION BETWEEN SUBSCRIBING MEMBER STATES (SMS) -

COMMON MINIMUM STANDARDS ON INDUSTRIAL SECURITY

1. This Attachment deals with security aspects of industrial activities that are unique to negotiating and awarding contracts entrusting tasks involving, entailing and/or containing EU classified information and to their performance by industrial or other entities, including the release of, or access to, EU classified information during the public procurement procedure (bidding period and pre-contract negotiations) done under the Code of Conduct on Defence Procurement.

DEFINITIONS

2. For the purposes of these common minimum standards, the following definitions shall apply:

   (a) "Classified contract": any contract to supply products, execute works or provide services, the performance of which requires or involves access to or generation of EU classified information;

   (b) "Classified sub-contract": a contract entered into by a contractor with another contractor (i.e. the sub-contractor) for the supply of goods, execution of works or provision of services, the performance of which requires or involves access to or generation of EU classified information;

   (c) "Contractor": an individual or legal entity possessing the legal capability to undertake contracts;

   (d) "Designated Security Authority (DSA)": an authority responsible to the National Security Authority (NSA) of an EU Member State which is responsible for communicating to industrial or other entities the national policy in all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA;

   (e) "Facility Security Clearance (FSC)": an administrative determination by a NSA/DSA that, from the security viewpoint, a facility can afford adequate security protection to EU classified information of a specified security classification level and its personnel who require access to EU classified information have been appropriately security cleared and briefed on the relevant security requirements necessary to access and protect EU classified information;

   (f) "Industrial or other entity": an entity involved in supplying goods, executing works or providing services; this may involve industrial, commercial, service, scientific, research, educational or development entities;

   (g) "Industrial security": the application of protective measures and procedures to prevent, detect and recover from the loss or compromise of EU classified information handled by a contractor or sub-contractor in pre-contract negotiations and contracts;

   (h) "National Security Authority (NSA)": the Government Authority of an EU Member State with ultimate responsibility for the protection of EU classified information;

(i) "Overall level of the security classification of a contract": determination of the security classification of the whole contract, based on the classification of information and/or material that is to be, or may be, generated, released or accessed under any element of the overall contract. The overall level of security classification of a contract may not be lower than the highest classification of any of its elements, but may be higher because of the aggregation effect;

(j) "Security Aspects Letter (SAL)": a set of special contractual conditions, typically issued by the contracting authority, which forms an integral part of a classified contract involving access to or generation of EU classified information, that identifies the security requirements or those elements of the contract requiring security protection;

(k) "Security Classification Guide (SCG)": a document which describes the elements of a programme or contract which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme or contract and the elements of information may be re-classified or downgraded. The SCG must be part of the SAL.

(l) “sMS”: a subscribing Member State to the Code of Conduct on Defence Procurement of the EU Member States participating in the European Defence Agency.

(m) “Contracting sMS”: a sMS contracting authority which is negotiating and awarding a contract under the Code of Conduct on Defence Procurement.

(n) “Host sMS”: a sMS where a contractor or sub-contractor participating in a classified contract of a contracting sMS is located or registered in accordance with the national rules and regulations.

(o) “EU classified information”: any information and material, an unauthorised disclosure of which could cause varying degrees of prejudice to the EU interests, or to one or more of its Member States, whether such information originates within the EU or is received from Member States, third states or international organisations[1].

ORGANISATION

3. A Contracting sMS may entrust by contract tasks involving, entailing and/or containing EU classified information to industrial or other entities located or registered in a sMS.

4. The Contracting sMS shall ensure that all requirements deriving from these minimum standards are complied with when awarding classified contracts.

5. Each sMS shall ensure that its NSA has appropriate structures to apply these minimum standards on industrial security. These may include one or more DSA.

6. The ultimate responsibility for protecting EU classified information within industrial or other entities rests with their management.

7. Whenever a contract or a sub-contract falling within the scope of these minimum standards is awarded, the Contracting sMS’ NSA/DSA will promptly notify the NSA/DSA of the Host sMS in which the contractor or sub-contractor is located or registered.

CLASSIFIED CONTRACTS

[1] As defined in Article 2 of Part I of the Annex to Decision 2001/264/EC of 19/03/01 « Security regulations of th eCouncil of the EU ».

8. The security classification of classified contracts must take account of the following principles:

   (a) the Contracting sMS determines, as appropriate, the aspects of the contract which require protection and the consequent security classification; in doing so, it must take into account the original security classification assigned by the originator to information generated before awarding the contract;

   (b) the overall level of classification of the contract may not be lower than the highest classification of any of its elements;

   (c) EU classified information generated under contractual activities is classified in accordance with the SCG;

   (d) when appropriate, the Contracting sMS is responsible for changing the overall level of classification of the contract, or security classification of any of its elements, in consultation with the originator, and for informing all interested parties;

   (e) classified information released to the contractor or subcontractor or generated under contractual activity must not be used for purposes other than those defined by the classified contract and must not be disclosed to third parties without the prior written consent of the originator.

9. The NSAs/DSAs of the Host sMS are responsible for ensuring that contractors and sub-contractors awarded classified contracts which involve information classified CONFIDENTIEL UE or SECRET UE take all appropriate measures for safeguarding such EU classified information released to or generated by them in the performance of the classified contract in accordance with national laws and regulations. Non-compliance with the security requirements may result in termination of the contract.

10. All industrial or other entities participating in classified contracts which involve access to information classified CONFIDENTIEL UE or SECRET UE must hold a national FSC. The FSC is granted by the NSA/DSA of a Host sMS to confirm that a facility can afford and guarantee adequate security protection to EU classified information to the appropriate classification level.

11. The NSA/DSA of a Host sMS is responsible for granting, in accordance with its national regulations, a Personnel Security Clearance (PSC) to all persons employed in industrial or other entities located or registered in that sMS whose duties require access to EU information classified CONFIDENTIEL UE or SECRET UE subject to a classified contract.

12. Classified contracts must include the SAL as defined in point 2(j). The SAL must contain the SCG.

13. Before initiating the negotiation of a classified contract the Contracting sMS will contact the NSA/DSA of the Host sMS in which the industrial or other entities concerned are located or registered in order to obtain confirmation that they hold a valid FSC appropriate to the level of security classification of the contract.

14. The contracting authority must not place a classified contract with a preferred bidder before having received the valid FSC certificate.

15. Unless required by national laws and regulations of the sMS where the contractor is located, an FSC is not required for contracts involving information classified RESTREINT UE.

16. In the case of bids in respect of classified contracts, invitations must contain a provision requiring that a bidder which fails to submit a bid or which is not selected be required to return all documents within a specified period of time.

17. It may be necessary for a contractor to negotiate classified sub-contracts with sub-contractors at various levels. The SAL must state that the contractor is responsible for ensuring that all subcontracting activities are undertaken in accordance with the common minimum standards contained in this Attachment. However, the contractor must not transmit EU classified information or material to a subcontractor without the prior written consent of the Contracting sMS.

18. The conditions under which the contractor may sub-contract must be defined in the tender and in the contract. No classified sub-contract may be awarded to entities located or registered in a non-sMS without the express written authorisation of the Contracting sMS.

19. Throughout the life of the contract, compliance with all its security provisions will be monitored by the relevant NSA/DSA of the Host sMS in coordination with the Contracting sMS. Notification of security incidents shall be reported, in accordance with the provisions laid down in Part II, Section X of the Council Security Regulations. Change or withdrawal of an FSC shall immediately be communicated to the Contracting sMS and to any other NSA/DSA to which it has been notified.

20. When a classified contract or a classified sub-contract is terminated, the Contracting sMS' NSA/DSA will promptly notify the NSA/DSA of the Host sMS in which the contractor or sub-contractor is located or registered.

21. The SAL must state that the common minimum standards contained in this Attachment shall continue to be complied with, and the confidentiality of classified information shall be maintained by the contractors and sub-contractors, after termination or conclusion of the classified contract or sub-contract.

22. Specific provisions for the disposal of classified information at the end of the contract will be laid down in the SAL or in other relevant provisions identifying security requirements.

VISITS

23. Visits by personnel of the Contracting sMS to industrial or other entities in the Host sMS performing EU classified contracts must be arranged with the relevant NSA/DSA of the Host sMS. Visits by employees of industrial or other entities within the framework of EU classified contract must be arranged between the NSAs/DSAs concerned. However, the NSAs/DSAs involved in a EU classified contract may agree on a procedure whereby the visits by employees of industrial or other entities can be arranged directly.

TRANSMISSION AND TRANSPORTATION OF EU CLASSIFIED INFORMATION

24. With regard to the transmission of EU classified information, the provisions of Part II, Section VII, Chapter II, and where relevant of Section XI, of the Council Security Regulations shall apply. In order to supplement such provisions, any existing procedures in force among sMS will apply.

25. The international transportation of EU classified material relating to classified contracts are to be carried out in accordance with sMS' national procedures. The following principles will be applied when examining security arrangements for international transportation:

    (a) security is assured at all stages during the transportation and under all circumstances, from the point of origin to the ultimate destination;

    (b) the degree of protection accorded to a consignment is determined by the highest classification level of material contained within it;

(c) an FSC is obtained, where appropriate, for companies providing transportation. In such cases, personnel handling (including, where appropriate, escorting) the classified consignment, shall be appropriately cleared in compliance with the common minimum standards contained in this Attachment;

(d) journeys are point to point to the extent possible, and are completed as quickly as circumstances permit;

(e) whenever possible, routes should be only through EU Member States. Routes through non-EU Member States should only be undertaken when authorised by the NSA/DSA of the States of both the consignor and the consignee;

(f) prior to any movement of EU classified material, a Transportation Plan is made up by the consignor and approved by the NSAs/DSAs concerned.