NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

14 September 2015

DOCUMENT C-M(2002)49-COR12

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION

Corrigendum to C-M(2002)49 dated 17 June 2002

Amendment 12

1. This document is the result of a review of Enclosures "G" to C-M(2002)49 by the Security Committee (SC) and has been approved by Council[1] under the silence period.

2. The amendments concern the overall effort of the SC to update policy and directives on Industrial Security, including the recently approved Directive on Classified Project and Industrial Security (AC/35-D/2003-REV5-COR1 dated 19 May 2015).

3. Accordingly, holders of C-M(2002)49 are requested to insert the attached revised Enclosure "G" and destroy the previous version.

4. This amendment bears serial number 12. Holders of C-M(2002)49 are therefore requested to strike out number 12 on the "Record of Amendments" which can be found on the opposite side of the cover page.

Annex: Enclosure "G"

1 C-M(2015)0063-AS1 refers

Action Officer: Josef Holubik, NOS/POB, Ext: 5043

Original: English

ENCLOSURE “G”

CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

INTRODUCTION

1. This Enclosure deals with security aspects of industrial operations that are unique to the negotiation and letting of contracts involving NATO classified information and their performance by industry, including the release of NATO classified information during pre-contract negotiations and contract performance. This Enclosure sets out the security policy for:

(a) the security requirements for tendering, negotiation and letting of contracts involving NATO classified information;

(b) contracts involving NATO classified information with contractors in non-NATO nations

(c) the industrial security clearances for contracts involving NATO classified information (Facility Security Clearances (FSCs) and Personnel Security Clearances (PSC));

(d) the release of NATO classified information in contracting;

(e) the handling of NATO classified information in Communication and Information Systems (CIS);

(f) International Visit Control Procedures (IVCP); and

(g) the international transmission and transportation of NATO classified material;

2. This Enclosure is supported by the Directive on Classified Project and Industrial Security which sets out the detailed requirements and procedures.

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

3. The prime contract for a NATO programme/project shall be negotiated and awarded by a NATO Programme/Project Agency/Office (NPA/NPO). An FSC shall be required for all Contractors involved in contracts that require the Contractor’s facility to manage, generate or have access to classified information NATO CONFIDENTIAL (NC) and above. For contracts classified NATO RESTRICTED (NR), an FSC is not required.

4. The NPA/NPO or other contracting authority which initiates the contract shall ensure that Contractor’s facilities hold an appropriate FSC for the specific phase of the contract. The contracting authority shall verify that Contractor’s personnel accessing classified information NC or above at the premises of the contracting authority hold the appropriate PSC.

5. After the prime contract has been let, a prime Contractor may negotiate sub-contracts with other Contractors, i.e., Sub-contractors. These Sub-contractors may also negotiate sub-contracts with other Sub-contractors. If these sub-contracts require access to information classified NC and above, the facility and personnel security requirements identified in the "Industrial Security Clearances For NATO Contracts" section of this Enclosure and in the Directive on Classified Project and Industrial Security shall apply. If a potential Sub-contractor is under the jurisdiction[1] of a non-NATO nation *prior* permission to negotiate a sub-contract shall be obtained from the NPA/NPO or other contracting authority respectively. If the NPA/NPO has placed restrictions on the award of contracts to NATO-nations that are not participants in a programme/project, the NPA/NPO shall be requested to consider and give permission prior to contract discussion with contractors from those nations.

6. Upon letting the contract, the NPA/NPO or other contracting authority shall notify the NSA/DSA of the Contractor, and ensure that the Security Aspect Letter (SAL) and/or the Project Security Instruction (PSI), as applicable, is provided to the prime Contractor, with the contract.

SECURITY REQUIREMENTS FOR CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

7. The prime Contractor and Sub-contractors shall be contractually required, under penalty of termination of their contract, to take all measures prescribed by the NSAs/DSAs for protecting all NATO classified information generated by or entrusted to the Contractor, or embodied in articles manufactured by the Contractor.

(a) Contracts for major programme/projects involving NATO classified information shall contain a PSI as an annex; a "Project Security Classification Guide" shall be a part of the PSI. All other contracts involving NATO classified information shall include, as a minimum, a SAL, which may be a PSI that is reduced in scope. In the latter case, the Programme/Project Security Classification Guide may be referred to as a "Security Classification Checklist".

The PSI supplements the NATO security policies and requirements, establishes specific security procedures associated with the NATO programme/project concerned and assigns responsibilities for the implementation of security measures concerning classified information.

(b) For contracts involving only NR information specific regulations have been established in the Directive on Classified Project and Industrial Security, in particular in its Appendix 4 "Contract Security Clause for Tenders and Contracts involving NATO RESTRICTED Information".

8. The classification for programme/project elements of information associated with possible sub-contracts shall be based on the Programme/Project Security Classification Guide.

1 Power to exercise authority over a subject matter or a territory/geographic area

CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION *WITH CONTRACTORS* IN NON-NATO NATIONS

9. The letting of contracts involving NATO classified information with Contractors in non-NATO nations constitutes release of information and has to be in accordance with Enclosure “E” to C-M(2002)49, the Directive on Security of Information and the Directive on Classified Project and Industrial Security. The release shall always be with the consent of the relevant originator(s).

10. Contracts involving NATO classified information with Contractors in non-NATO nations require the existence of a bilateral Security Agreement/Arrangement between NATO or a contracting/sponsoring NATO nation and the non-NATO nation where the Contractor is under the jurisdiction of a NSA/DSA or other competent authority with the authority to commit the Contractor to provide the required protection. If the contract is governed by a bilateral Security Agreement/Arrangement between a contracting/sponsoring NATO nation and a non-NATO nation, the NATO nation shall provide a written security assurance to NATO confirming that the NATO classified information provided is governed under the scope of that Security Agreement/Arrangement. A copy of the assurance shall be provided to the NOS and the relevant NPO/NPA.

11. The undertaking of placing a contract to a Contractor of a non-NATO nation shall follow the procedures as established in the Directive on Classified Project and Industrial Security.

12. For non-NATO nations, an appropriate security authority(s) shall be identified that fulfils the equivalent functions of the NSA/DSA in a NATO nation.

INDUSTRIAL SECURITY CLEARANCES FOR NATO CONTRACTS

General

13. The policy described in subsequent paragraphs for facilities and individuals apply to contracts and sub-contracts.

Facility Security Clearances (FSC)

14. The NSA/DSA of each NATO nation is responsible for ensuring that any facility under its jurisdiction which will require access to information classified NC and above has adopted the protective security measures necessary to qualify for an FSC. In granting an FSC, the NSA/DSA shall ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted.

15. The assessment to be made prior to issuing an FSC shall be in accordance with the requirements and criteria set out in the supporting Directive on Classified Project and Industrial Security in addition to any applicable national laws and regulations.

16. A bidder, not holding an appropriate FSC as required by the potential contract/subcontract shall not be automatically excluded from the competition. The contracting authority should make all efforts in restricting the classification level of the information required to be provided to bidders to the lowest possible level still permitting an informed and qualified response to the invitation to tender. However, the tender document shall advise on the requirement for an appropriate FSC prior to the award of the contract/subcontract.

17. Scenarios identifying FSC requirements are provided in the supporting Directive on Classified Project and Industrial Security.

18. An FSC or PSC is not required for contracts or access to information classified NR. A nation which, under its National security laws and regulations, requires an FSC for a contract or sub-contract classified NR shall not discriminate against a Contractor from a nation not requiring an FSC , but shall ensure that the contractor has been informed of its responsibilities in respect to the protection of the information, and obtains an acknowledgement of those responsibilities.

Personnel Security Clearances for Facility Employees

19. The facility’s employees who require access to NATO classified information NC and above shall hold an appropriate PSC. The issuing of PSCs shall be in accordance with Enclosure “C” to C-M(2002)49, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

20. Applications for the security clearance for employees of Contractor facilities shall be made to the NSA/DSA which is responsible for the facility. In submitting the request for verification or initiation of a PSC, the facility shall include the level of NATO classified information to which the employee will have access.

21. If a facility wishes to employ a citizen of a non-NATO nation in a position that requires access to NATO classified information, it is the responsibility of the NSA/DSA of the nation which has jurisdiction over the hiring facility, to carry out the security clearance procedure prescribed herein, and determine that the individual can be granted access in accordance with the requirements of Enclosure “C”, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

22. The release of NATO classified information in contracting can constitute either release to non-NATO Nations and International Organisations or release to non-Programme/Project participants from NATO Nations. The release shall be with the consent of the relevant NPA/NPO and/or originator, as applicable, and in accordance with other relevant enclosures to the NATO Security Policy, the Directive on Security of Information as well as the Directive on Classified Project and Industrial Security.

THE HANDLING OF CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

23. Only appropriately security accredited CIS shall be used for the storing, processing or transmitting (called hereafter “handling") of NATO classified information. Enclosure “F” to C-M(2002)49, the “Primary Directive on CIS Security” (AC/35-D/2004), the “INFOSEC Management Directive for CIS” (AC/35-D/2005) and all relevant Technical and Implementation Directives on CIS Security (AC/322 documents) provide further policy and directions for the conformant implementation of CIS handling NATO classified information.

24. The security accreditation of CIS handling NR information may be delegated to Contractors according to national security laws and regulations. Where this delegation is exercised, the relevant NSAs/DSAs/SAAs shall retain the responsibility for the protection of NR information handled by the Contractor and the right to inspect the security measures taken by the Contractors. In addition, the Contractor shall provide the Contracting Authority and, where appropriate, the security authority as established in the Directive on Classified Projects and Industrial Security with a statement of compliance certifying that the CIS handling NR information has been accredited in compliance with the policy on Security within NATO and its supporting directives on CIS Security.

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCP)

25. IVCP apply to international visits by representatives of NATO Nations, NATO Civil and Military Bodies, Contractors and Sub-Contractors involving NATO classified information. They also apply to representatives of a Non NATO Nation including Contractors/Sub-Contractors of such Nation if the Nation has adopted the IVCP.

26. Visits involving access to NATO information classified NC and above or unescorted access to security areas shall be approved by the NSA/DSA. Visits involving access to NU[2] or NR information may be arranged directly between the sending and receiving facility without formal requirements.

27. Detailed arrangements for the conduct of International Visits are laid down in the Directive on Classified Project and Industrial Security.

PERSONNEL ON LOAN WITHIN A NATO PROJECT/ PROGRAMME

28. When an individual who has been cleared for access to NATO classified information is to be loaned from one facility to another in the same NATO programme/project, but in a different NATO nation, the individual’s parent facility shall request its NSA/DSA to provide a NATO Personnel Security Clearance Certificate for the individual to the NSA/DSA of the facility to which he is to be loaned. The individual on loan shall be assigned using the international visit request procedures set out in the Directive on Classified Project and Industrial Security, and in accordance with National security laws and regulations.

2 NU is not a NATO security classification

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL

Security Principles Applicable to all Forms of Transportation

29. The following principles shall be enforced when examining proposed security arrangements for the international transportation of consignments of classified material:

(a) security shall be 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 shall be determined by the highest classification level of material contained within it;

(c) an FSC shall be obtained, where required, for companies providing transportation. In such cases, personnel handling the consignment shall be issued an PSC in compliance with the provisions of this Enclosure;

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

(e) care shall be exercised to arrange routes only through NATO nations. Routes through non-NATO nations should only be undertaken when authorised by the NSA/DSA having jurisdiction over the consignor and in accordance with the supporting Directive on Security of Information.

30. Arrangements for consignments of classified material shall be stipulated for each programme/project. However, such arrangements shall ensure that there is no likelihood of unauthorized access to classified material.

31. The security standards for the international transportation of NATO classified material can be found in the supporting Directive on Security of Information. However, the detailed requirements for the hand carriage of NATO classified material, carriage of classified material by commercial courier companies, security guards and escorts, and the transportation of explosives, propellants or other dangerous substances are set out in the supporting Directive on Classified Project and Industrial Security.