APPENDIX EE

COMMUNICATIONS SECURITY PROCEDURES AND INSTRUCTIONS

MULTINATIONAL INDUSTRIAL SECURITY WORKING GROUP

MISWG Document Number 22 **2 December 2012**

COMMUNICATIONS SECURITY PROCEDURESAND INSTRUCTIONS

1. Preface and aim.

Classified information and materials related to the Communication Security (COMSEC) need to be controlled and managed with rules and procedures sometimes more restrictive in comparison with those requested for the other classified information. This because COMSEC information, materials and technologies, due to their "strategic" importance, are always sensible targets and their loss or compromise may damage seriously the security of classified information.
When a body/company needs to handle classified information related to the Communication Security, it should be mandatory to establish a specific COMSEC organisation.
The present paper gives the minimum requirements for the COMSEC information protection, to establish a COMSEC organisation and to exchange COMSEC information among official/ government bodies and/or industrial enterprises.

COMSEC information may be exchanged or provided to companies involved in multinational cooperative programs for one of the following purposes:

- need of electronic transmission of classified information between companies and official/government bodies or between different companies;
- multinational cooperative programs, on the development, production or test of COMSEC material;
- transfer to companies of COMSEC material for specific needs, in the framework of multinational cooperative programs;
- direct procurement of COMSEC material by companies for activities related with one of the previous items.

2. COMSEC materials/information and relevant caveats.

Handling of COMSEC materials and information is therefore subject to specifics regulations and security procedures. To point out such a need and to limit access only to persons adequately cleared and in possession of a specific authorisation, the following caveats apply:

- CRYPTO. Such a caveat applies to documents, correspondence, directives, publications and materials which contain particularly sensitive cryptographic information that, if disclosed to

unauthorised people, may enable to de-cipher classified crypto communications. This category of information/materials must be managed and safeguarded according to specific procedures.

- CCI (Controlled Cryptographic/COMSEC Items) - This caveat applies to those materials, which though not classified are subject to particular handling and control regulations because they are used to handle and/or transmit classified information. This category includes among others: "TEMPEST" materials, some COMSEC devices and cryptographic equipment without keys and/or classified logic inserted.

3. Access to the classified COMSEC information.

Any COMSEC information, whether classified or not, can be given only to personnel belonging to the organisation/company that are directly involved in COMSEC activities and strictly based on the “need to know” principle.

Persons who, in order to carry out their activity, need to have access to classified cryptographic materials/information, must be briefed on the special procedures and rules applicable for COMSEC material. This could be done by a specific authorisation called "Crypto Authorisation", released by the relevant National Security Authority. It, usually, cannot replace the “Personal Security Clearance".

4. General security and control measures.

To reduce risks of COMSEC compromises it will be necessary to establish security and control measures at the premises in which the activities will be carried out. They shall include:

- prevention against not authorised access to COMSEC classified area;
- special security and control measures of the COMSEC materials;
- access to COMSEC information/material limited to the authorised personnel on a strict "Need to Know" principle basis;
- special caveats for the COMSEC information/material.

When classified crypto material is not used, it should be kept in security containers, armoured closets or strong rooms. When storing in safes or strong rooms is impossible, this material should be kept in metal containers with a lock, placed in monitored areas, accessible only to authorised staff.

Crypto keys and ciphering material should be kept in separate safes, whenever possible. In any case, this material should not be stored with non-crypto publications or document.

5. COMSEC information and material management responsibility.

In order to fulfil tasks connected with safeguarding security in communications and controlling each area where COMSEC/cryptographic material is kept and managed, the COMSEC Authority responsible for the Organisation can appoint its own personnel to carry out the duties of "COMSEC Officer", "Crypto Custodian" and "Alternate Crypto Custodian".

a. COMSEC Officer.

He is responsible for the correct application and observance of COMSEC regulations as well as for the efficiency, accuracy and security of cryptographic operations. Moreover, he is the advisor for the highest security authority, responsible of the organisation in the specific area of the communication security.

b. Crypto Custodian.

He is appointed by the highest security responsible of the organisation. He is responsible for the custody, handling, protection and destruction of all cryptographic material. He is also responsible for the reception and distribution of crypto material needed by subordinate organisations.

c. Alternate Custodian of crypto material.

He is appointed by the highest security authority responsible of the organisation. He does not share with the Custodian the responsibility of the cryptographic material when the custodian is present.

d. Crypto operators.

The security and positive results of cryptographic procedures depend to a large extent on the professional level of each single operator. With this aim, any person who uses COMSEC material must follow with diligence, professionalism and accuracy the prescribed procedures for the handling, protection, custody and periodical destruction of the material they have in charge.

Moreover, they must immediately report to their superiors on any intentional or unintentional event and/or circumstance which may have enabled unauthorised persons to acquire classified cryptographic materials/information.

6. COMSEC Violations and Compromises.

Violation.

Any fact or event, that may cause a compromise of classified information transmitted/handled through COMSEC equipment represents a "violation to communications security".

Compromise.

Compromise takes place when an unauthorised person comes into possession of COMSEC/cryptographic information/material.

Any violation or possible compromise shall be reported to the relevant security office that will report the incident to their parent/host Security Authority and investigate on detail about the event, in order to define the suitable actions to be taken to limit the consequence and avoid other future recurrences.

The responsible Security Authority will promptly and fully inform the other Participants' Security Authorities of the known details of the event, will provide updates and a final report of the investigation and of the corrective actions taken .

Reports on the violations and possible compromise shall include at least the following details:

- a description of the circumstances,
- the date or the period of the occurrence,
- the date and place of discovery and location of the occurrence,

- the security classification and caveats of the information involved in the incident,
- specific identification of the information or material, to include originator, subjects, reference, date, copy number, and language,
- a list of the information that has been compromised or material that is unaccounted for,
- responsible person(s) and reasons for loss or compromise or possible loss/compromise,
- assessments of the likelihood of compromise (i.e., "certain," "probable", "possible," or "unlikely") including an explanation,
- a statement on whether the originator has been informed,
- actions taken to secure the material and limit further damage.

The above reporting requirements are in addition to any other reporting requirements of the Participants, required by national regulations.

7. COMSEC material transportation.

Transport of crypto material and classified correspondence marked with the caveat "CRYPTO" has to be made under the control of the National distribution Agency, in accordance to the rules defined by the relevant National Security Authorities, by couriers, adequately authorised, taking care that it must be always granted as follows:

- crypto material be only handled by authorised personnel and never be object of inspections by unauthorised persons (included customs agents);
- clear instructions be issued for the delivery, acceptance and retain of all the crypto material to be sent.

Transportation of crypto material, because of the specific dangers that such operation may represent, has to be made in respect of the following instructions:

- before the transportation of a crypto device, crypto keys must be removed and/or erased (except for cases where it is technically possible without additional risks);
- transportation of crypto equipment must be made separately from the associated crypto keys, operating manuals and maintenance booklets;
- the transfer, when made by plane, should avoid to pass over hostile countries; if made by ship, material must be prepared so that the recovery, in case of accident, is impossible.