DOCUMENT X:

SECURITY PROCEDURES AND INSTRUCTIONS FOR COMSEC INFORMATION AND MATERIAL

CLASSIFICATION LEVEL

RECORD OF CHANGES		
Date	*Issue*	*Changes*
03/10/2011	3.0	Approved version
15/06/2011	2.1	Unclassified version issued by Italy with LoI format
20/07/2009	2.0	Updated version with new shape and title
26/06/2006	1.0	Approved version

INDEX

1. PREFACE AND AIM:

COMSEC information is controlled and managed with rules and procedures which are more restrictive in comparison with those requested for other classified information. This is because COMSEC information, materials and technologies, due to their "strategic" importance, are always targets of the opposing intelligence services and their loss or compromise may damage heavily the national security.

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 industry for one of the following reasons:

- need of electric/electronic transmission of Classified Information between companies and official/government bodies or between different companies;
- research programmes, development, production or test of COMSEC material;
- need of installation of COMSEC material;
- transfer to the company of COMSEC material for specific needs;
- direct acquisition/procurement of COMSEC material by the company for activities related with one of the previous lines.

The Security/COMSEC Officer of the Body/Company that will establish the COMSEC organisation shall arrange and assure the effectiveness of the procedures and rules prescribed for the security of the COMSEC material and information, including (when and if applicable) the management procedure related to the accounting of the same material by the Crypto Custodian.

2. 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 unauthorised access to COMSEC classified area (access control, personal identification systems, alarm and detection systems);

- special security and control measures of the COMSEC materials (including continuous custody, inspections and audits, accounting procedures, secure containers/safes, special COMSEC transportation rules and plans, training of personnel);

- access to COMSEC information/material limited to the cleared and authorised personnel on a strict "need-to-know" principle basis; secure and crypto clearance shall be provided by the relevant national authority;

- special designations for the COMSEC information/material (CRYPTO or CCI - "COMSEC Controlled Item"), to highlight the "sensitiveness" and the consequent need of applying the relative procedures.

When classified crypto material is not used, it should be kept in security containers, armoured closets or strong rooms. Safes (and/or armoured cabinets) should have weight and size such as to prevent their removal or they must be firmly fixed to the bearing structure of the building. 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 material should be kept in separate safes. In any case, this material should not be stored with non-crypto publications or documents.

Cryptographic equipment may be kept in crypto centres in compliance with specific instructions.

Computer and/or cryptographic equipment used for communication protection must be approved or authorised and installed in accordance with established COMSEC technical rules. The installation must be approved by the designated Authority.

Security measures and requirements demanded for the COMSEC information/material management must be contractually binding for the company that should conduct COMSEC activity, and inserted in an appropriate contractual clause.

3. COMSEC MATERIALS/INFORMATION CATEGORY AND RELATIVE DESIGNATIONS:

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 those people in possession of the CRYPTO access authorisation, the following designations are applied:

- CRYPTO. Such a designation is given to cryptographic keys, documents, correspondence, directives, publications and materials which contain particularly sensitive cryptographic information. This category of information/materials must be managed and safeguarded according to specific procedures.

- CCI (Controlled Cryptographic/COMSEC Items). This designation is given 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. The materials designated "CCI" must carry in clear evidence, the stamp "CCI", or the wording "SUBJECT TO COMSEC CONTROL".

- Other COMSEC material and/or information, not designated "CCI" or "CRYPTO", and therefore not immediately or clearly recognisable, must be adequately evaluated on the basis of the "sensitivity" and importance of their content, in order to ascribe, if any, a secrecy classification.

4. 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 assignments 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 COMSEC authority of the Organisation regarding anything dealing with communication security. For the above mentioned tasks and in compliance with the regulations in force, he must:

issue permanent executive norms which, case by case, establish;

- draft a set of rules for personnel in charge of handling classified communications to assist them in the fulfilment of the tasks assigned;

- establish the procedures for the employment and safe custody of COMSEC material;

- issue regulations on the maintenance and repairs of cryptographic apparatus used in the installation;

- define the first immediate actions to be performed to report events which may have brought about violations or compromise of communication security;

- arrange the emergency plans for safeguarding COMSEC material in case of evacuation, fire and emergency of COMSEC material, underlining the task for the personnel employed, the means to be used for destruction and transportation and relating procedures;

- issue permanent regulations designed for the periodical destruction of cryptographic materials;

- submit the personnel involved to regular periodical security briefing to guarantee the constant appropriate use of the cryptographic systems supplied.

b) Crypto Custodian.

He is appointed by the highest Authority in his 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.

Moreover he must:

- have perfect knowledge of the general rules and specific regulations related to the handling of the material he has been entrusted with;

- sign the inventory of the materials received for use, custody and distribution, after having checked the integrity of the seals of parcels and packets;

- carry out a thorough check of all material received (check of quantities, correspondence of serial or registration numbers, integrity of the protective covers for the lists of keys, integrity of the equipment and COMSEC classified publications).

- verify the existence of the minimum security requirements needed for the safe custody of the crypto material for which he is responsible;

- keep numbered updated inventory registers of the publications of crypto material assigned. In these registers he must list all the copies of each edition received, noting where they can be found and their validity;

- keep a numbered updated inventory register of the crypto material assigned.

- draft periodically an inventory of the material he effectively has in charge;

- distribute the material to the technically subordinate Organisations according to the regulations in force, making the person officially appointed to use and keep in custody the crypto material sign the receipts or concession inventories;

- have perfect knowledge of the emergency plans for the destruction, evacuation or protection of materials in case of natural disasters, fire or other emergencies;

- report immediately to the COMSEC Officer any possible compromise, loss or unauthorised destruction of the crypto material he has in charge;

- carry out, as and when ordered, the periodical and emergency destruction.

For periods of absence of less than 60 days, the Crypto Custodian is substituted in his job by the Alternate Crypto Custodian. If the Crypto Custodian is absent for a continuous period of more than 60 days, a new Crypto Custodian must be appointed.

c) Alternate Crypto Custodian of crypto material

He is appointed by the authority responsible for the parent Organisation. He does not share with the Crypto Custodian the responsibility of the cryptographic material when the latter is present.
When the Crypto Custodian has to leave for a period of less than 60 days, the Alternate Crypto Custodian takes over all the responsibilities and tasks. When the Crypto Custodian returns, he must:

- inform him of all the variations in the materials assigned, which took place in his absence;

- show him all the documents and/or cryptographic material he may have received.

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.

5. 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 and need to have access to classified cryptographic materials/information, must possess a specific authorisation. The above mentioned authorisation indicated as "Crypto Authorisation" is limited to citizens of member countries; it cannot replace the "Security Clearance". Responsibility must be formalised by the interested person’s signature on the crypto authorisation certificate.

In the case in which, for whatever reason, a person is no longer employed in the activity which required crypto, he loses this authorisation and must be properly indoctrinated, signing a declaration which verifies his responsibility to not divulge any information he was in possession of. Whenever the person is removed from his responsibility or activity for discipline or security reasons, a detailed report which contains the causes that have determined this action must be sent to the relevant COMSEC Authority.

The persons who have the need to handle classified cryptographic information must receive adequate instructions (briefing). These instructions must include information on the respective responsibilities and individual tasks for the treatment and safeguard of such information which at the various classification levels are requested in order to carry out the expected work.

Personnel who no longer have the need for "Crypto Authorisation" must receive a debriefing concerning the obligation not to divulge information which he had access to and must sign a liberating declaration.

Being the crypto authorization, released by the National relevant Authorities, strictly related to national information, in case of activities related to international programmes and staffed with different nationalities, a problem could arise for the authority that should issue the relevant crypto authorization. If this is the case, it would be better that such authorization, related to COMMON SHARED COMSEC INFORMATION ONLY, be issued, case by case, by the staff parent NSA or by the COMSEC OFFICE or the relevant international organisations if any.

6. COMSEC SECURITY VIOLATIONS AND COMPROMISES:

Violation.

Any unusual fact or event, that may cause a compromise, represents a "violation to communications security". The violation can be:

- "material" , when due to the non-observance of security regulations of safeguarding COMSEC material;

- "cryptographic", when due to the non-observance of regulations, pertaining to procedures, management and use of COMSEC material and/or malfunctioning of the cryptographic equipment

Compromise.

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

- "material", when an unauthorised person comes into possession of cryptographic material as a result of loss, capture, theft, recovery after an accident, unauthorised access, or any other material cause;

- "cryptographic", when an unauthorised person succeeds through cryptographic analysis to get information pertaining:

    - the cryptographic techniques used;

    - the "plain text" - or part of it - contained in the ciphered message.

Personnel, staff members and approved Contractors shall report the actual or possible loss or compromise of classified information to their security office. The security office will report the incident to their parent/host Security Authority in addition to reporting procedures prescribed by national security regulations.

7. COMSEC MATERIAL TRANSPORTATION:

Transport of crypto material and classified correspondence marked "CRYPTO" has to be made by cleared couriers, authorised and designated by the Security Organisation, 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;

Couriers employed for transferring crypto material are to:

- be in possession of an adequate security clearance and officially authorised;

- when the journey for the transport is presumed to take more than six hours the courier must be accompanied (if a motor-vehicle is employed, the driver, with an adequate clearance, can be also considered a second courier);

- not to be employed for other duties, unless they are of secondary importance;

- have precise instructions, so that in case of unexpected events (capture, sequestration or other events that could cause a possible compromise of the crypto material), the material itself must be adequately destroyed with any means, to make it useless;

- couriers themselves have to notify, when possible and using the faster mean, the emergency destruction of the material to the sender and/or the receiving Organisation;

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

The Crypto Custodian is the only one authorised to open, check and subscribe the receipt of packages containing crypto material. Signed transfer reports are to be given back within 48 hours from the reception of the package.

The control of every envelope or package by the Crypto Custodian must include:

- before the opening, the check to exclude any sign of tampering or violation;

- careful check of the contents based on the included transfer report;

- check of the pages of each crypto publication.

If discovered an evident tampering or discrepancy, an immediate report of possible compromise will have to be sent to the competent Authority.