DOCUMENT XII:

USE OF CRYPTOGRAPHIC SYSTEMS FOR CONFIDENTIAL AND ABOVE

CLASSIFICATION LEVEL

RECORD OF CHANGES		
Date	*Issue*	*Changes*
20/07/2009	2.0	Updated version with new shape and title
31/05/2007	1.0	Approved version

1. The Framework Agreement nations agree in principle that secure electronic communications may be used for the exchange of information classified CONFIDENTIAL and above for the following occasions:

    a. Between the participating governments and contractors in a Multinational[1] Cooperative Programme.

    b. Between the contracting government and contractors in a national programme with multinational security aspects, in whichever nation the contractors may be sited.

    c. Between the facilities of one company in different nations. The secure electronic communications may be used to support one or more national or multinational cooperative programmes.

    d. Between the facilities of different companies in different nations. The secure electronic communications may be used to support one or more national or multinational cooperative programmes.

2. Choice of Encryption System. For secure electronic communications between participants in Framework Agreement nations, in compliance with the Annex of EDIR FA, the crypto systems to be used for protection of CONFIDENTIAL and above have to be evaluated and approved by the NSA of at least one FA nation and be acceptable to all the NSAs/DSAs concerned.

    a. In a Multinational Cooperative Programme, each participating nation may offer to the Security Working Group a national encryption system to be used by the programme. Each Programme will choose its encryption system, in accordance with recommendations of its Security Working Group.

    b. In a national programme, the nation will choose the encryption system.

    c. For the occasions described in Paragraphs 1c and 1d, where companies wish to establish secure electronic communications to support one or more national or multinational cooperative programmes they shall apply to their NSA/DSAs and may request to use an encryption system approved by any one of the Framework Agreement nations.

3. Installation and Use. Provided that the National Security Authorities are satisfied that contractor or company facilities comply with agreed standards for security, the national

[1] Multinational also includes Bilateral programmes.

communication security authorities or their designates will authorise the installation and use of approved cryptographic systems, in order to facilitate the secure electronic communications, for each occasion. Other requirements are:

a. For each occasion, a participant in one nation will be nominated to be the principal user. The principal user is responsible for informing a national point of contact of the details of the occasion: this national point of contact shall be the national NCSA, designate or other relevant authority . This national point of contact is responsible for coordinating the authorisations of other nations. Participants in other nations are encouraged to inform their national Authorities on the details of the occasion at the same time.

b. The NCSA, designate or other relevant Authority of each of the participating nations must agree in writing the equipments and procedures to be used on each occasion. Written agreement may be achieved by an exchange of official emails either specifying these details or approving a formal document describing them, such as Specific Operating Instructions for Secure Communications (SOISC). When the national point of contact wishes to classify any of these details, a classified formal document, such as a SOISC, will be required. Whilst this classified document must be distributed to approving Authorities by secure means, unclassified comments and approvals may be returned to the originator of the SOISC by official email.

c. The nation supplying the encryption system will be responsible for supplying encryption keys, in accordance with the Key Management Plan for the encryption system and any special requirements for each occasion, handbooks, operating instructions and security operating procedures for the encryption system.

d. National Distribution Agencies (NDA) will cooperate, both with other NDAs and with other relevant Authorities responsible for the sites participating in the secure communications, in the receipt and distribution of the Cryptographic Items (including encryption keys). Each national NCSA, designate or other relevant authority is responsible for instructing its own NDA of the requirements for each occasion.

4. The installation and use of equipment shall be in accordance with the national security regulations of the Governments. However, such regulations must result in a protection degree at least equivalent to the minimum standards specified in the following references:

a. EDIR-FRAMEWORK AGREEMENT: Minimum Communication Security Standard.

b. TECH-I-01. Subject, Crypto and ComSec Material Management.

c. ISP-202 Guidelines for the installation of sites and systems processing classified information

d. ISP-203 Guidelines on TEMPEST zoning: protection against compromising emanations