DOCUMENT XI:

SPECIFIC OPERATING INSTRUCTIONS FOR SECURE COMMUNICATIONS

CLASSIFICATION LEVEL

RECORD OF CHANGES		
Date	*Issue*	*Changes*
20/07/2009	2.0	Updated version with new shape and title
15/11/2006	1.0	Approved draft

FRAMEWORK AGREEMENT

(S.O.I.S.C.)

SPECIFIC OPERATING INSTRUCTIONS for SECURE COMMUNICATIONS

PROJECT [NAME]

SECURE COMMUNICATIONS BETWEEN

[COMPANY NAME & LOCATION]

AND

[COMPANY NAME & LOCATION]

AND

[NATIONAL DEFENCE ESTABLISHMENT]

SECURE <DEVICE> <DATA> COMMUNICATIONS

DURING [PROJECT STAGE] STAGE OF

PROJECT [NAME]

[NAME OF COMMUNICATION SYSTEM]

ISSUED BY: [Insert name of NSA/DSA]
Issue: [ ]
Dated: [ ]

RECORD OF CHANGES				
VERSION	AUTHOR	DATE	REASON FOR CHANGE	SUPERSEDED DOCUMENT

TABLE OF CONTENTS

SECTION I - INTRODUCTION

A. PURPOSE

The purpose of this SPECIFIC OPERATING INSTRUCTIONS for SECURE COMMUNICATIONS (SOISC) is to provide instructions for the exchange of classified information between the participating facilities of the under mentioned [companies] and/or national [defence establishments] for use on the [project name] project during the [project stage] stage in accordance with relevant mutually agreed security rules of:

a. [company, full postal address]

b. [national defence establishment, full postal address]

B. SCOPE

1. This SOISC complements respective national security policies pertinent to the control, protection, and transmission of classified information. Additionally, this SOISC identifies the security procedures for the transfer of classified information directly between the participating facilities listed in Paragraph A.

2. Classified information shall be exchanged by [secure voice] [secure data file transfer] [secure facsimile] from authorised terminals. The information will be limited to the following national classification levels: [delete as appropriate] [CONFIDENTIAL] and [SECRET].

3. This SOISC will only be in effect during the period when the participants are in the [project stage] stage, unless otherwise extended by agreement between contractors and their respective governments. This period is known as the Concession Period. *{Dates might be used instead of "project stage", but dates may slip.}*

C. AUTHORITY RESPONSIBILITY AND APPLICABILITY

1. This SOISC has been approved by the following National Security Authorities/Designated Security Authorities (NSA's/DSA's):

FR Délégation générale pour l'Armement Département central de la sécurité de défense et de 1'information (DGA/SDI).
GE Bundesministerium fur Wirtschaft und Arbeit, Referat VIB 3, Villemombler Strasse 76, D-53107 Bonn.
IT Presidenza del Consiglio dei Ministri - Autorità Nazionale per la Sicurezza/CESIS - III Reparto U.C.Si. - Via di Santa Susanna n.15 00187 Roma.
SP Secretario de Estado Director del Centro Nacional de Intelligencia.

SW Defence Materiel Administration - FMV, Security, SE-115 88 Stockholm Sweden.
UK Directorate of Defence Security, Ministry of Defence (MOD) - InfoSy(Tech)COMSEC

2. Requests for clarification, proposed changes or revisions to this SOISC should be directed within the countries to the respective NSA/DSA as listed above, through established government channels. Amendments will not be made without the approval of the NSA's/DSA's concerned in consultations with the appropriate government authorities as appropriate.

3. The NSA's/DSAs have overall responsibility to ensure national compliance with the security requirements of this <programme/project>.

4. The Cognisant Security Agency (CSA), where applicable and/or stated by relevant national rules, is responsible for administering and implementing the security aspects of this SOISC for their respective NSA/DSA's

   {A CSA may be any competent agency or person with security responsibility for the project/programme. There is no requirement for a CSA to be a Government agency, although the nation leading on the project may wish to nominate its Ministry of Defence project management team as its CSA.}

   a) The CSA for France is to be defined on a case by case basis;
   b) The CSA for Germany is : : :;
   c) The CSA for Italy is.;
   d) The CSA for Spain is : : : :
   e) The CSA for Sweden is : : : :
   f) The CSA for the UK is <for a UK project - the project management team> <for the project of another nation - the Security Controller of the company concerned>.

5. The Project Security <Officer/Adviser> is [insert name, full postal address, telephone and facsimile numbers, email address].

6. <The Cryptographic Operating Authority (COA) and point of contact is [insert details as appropriate]>.

SECTION II - GUIDELINES AND REQUIREMENTS

A. DESCRIPTION OF INFORMATION TRANSFERS

1. Secure telephone communications will allow the transfer of information classified up to [insert appropriate security classification] in secure [voice] [data] [facsimile] modes directly between the participating facilities listed in Section I, Paragraph A.

2. Voice Communications. Secure voice communications shall use <device model> secure telephones. There will be a <device model> at each participating facility to allow for secure conversations up to [insert appropriate security classification] level.

3. Data Communications. [insert project name] users will process classified information on a "stand-alone" terminal within their facility Each participating facility may use a local area network of computers to process classified information, but shall have a "stand-alone" terminal for secure data transfers. Data shall be transferred between the local area network and the stand-alone PC on a removable transfer medium. When there is a requirement to send data to other participants, data will be transmitted from the stand-alone PC through an attached <device model> terminal. In all cases, when data is sent from the PC, the transaction shall be recorded.

4. Facsimile Communications. Secure facsimile communications shall use <device model> secure telephones. All facsimile transfers shall be recorded.

5. Software and Equipment Requirements.

    a) In the context of this SOISC, <device models> and combinations of stand-alone PC <or> [facsimile machine] with <device model> will be known as “system equipment”.

    b) The [stand-alone PCs] and [facsimile machines] will be provided by the host facilities.

    c) The <responsible> COA will provide <device model> equipment to each facility detailed in Section I Part A. <device models> will be installed by local technicians in accordance with [delete as appropriate] [the instructions in the <device model> Local Manager Guide, which will be issued by the <responsible> COA] [national physical, personnel and electronic security regulations for cryptographic equipment protecting <appropriate security classification> information]. The <responsible> COA will also issue a copy of the <device model> User Handbook and Security Operating Procedures to each participating facility.

B. SYSTEM RESTRICTIONS

1. System equipment shall not be connected to any local area network.

2. System equipment shall be operated only in areas that have been accredited for work at the relevant security classification.

3. Only information required in the support of the [project name] will be transferred via the secure telephone communications.

4. When importing data into a receiving secure IT system, the removable transfer medium shall not be classified higher than the system.

C. CONFIGURATION CONTROL

1. The CSAs are responsible for configuration management of the communications link.

2. Any proposed changes to the system configuration or to the operating procedures within this SOISC must be submitted by the participating facilities to the CSAs for approval, prior to implementation.

D. SECURITY AUDITS

1. The CSAs will review their respective facilities on a regular basis according to national rules and at least annually to ensure conformance with these instructions and authorised local security regulations.

E. MAINTENANCE

1. Should a <device model> at a site outside the <responsible nation> require maintenance, it shall be returned to the <responsible nation> NDA through the nation's NDA.

F. DESIGNATED RELEASING AUTHORITY (DRA)

1. A Designated Releasing Authority (DRA) and Alternate DRA for each participating facility will be appointed by the [contractor] <or> [defence establishment]: these appointments are subject to the approval of the CSA. These individuals will be

citizens of their respective countries, who are cleared to at least SECRET level by their government, and are responsible to their governments for the following:

a. Reviewing and approving all material and data prior to its actual transmission via the secure telephone communications.

b. Acknowledging receipt of all material and data transmitted via the secure telephone communications.

c. Briefing the system operators to their responsibilities.

d. Ensuring all records required to be executed by the system operators are maintained in a complete and accurate manner.

e. Producing upon request, by the CSA, any records required to be maintained for the secure telephone communications.

f. Reporting to their CSA any security violations, unauthorised disclosures or possible compromises of information transmitted via the secure telephone communications.

2. In the event the DRA is unable to perform his/her duties, the Alternate DRA will assume the responsibilities identified above.

G. SYSTEM OPERATORS

1. At each participating site, [project name] personnel, who are nationals of participating nations, cleared to at least [appropriate security classification] level, will be assigned duties as system operators. System operators are responsible for the following:

a. Ensuring that only authorised personnel use the secure telephone communications for voice.

b. Ensuring that only data authorised by the DRA is transmitted via the secure telephone communications.

c. Providing to the DRA within a timely manner all material received via the secure telephone communications for his/her review.

d. Reporting to the DRA all system irregularities, security violations, unauthorised disclosures or possible compromises as the result of any transmission.

e. Executing all records as required relating to the utilisation of the secure telephone communications.

f. Controlling system equipment as required within this SOISC and as directed by the controlling COMSEC Custodian.

2. System operators are also responsible to the host Facility Security Control Officer for compliance with all respective national and facility security regulations pertinent to the safeguarding, protection, control, and storage of classified material generated and received via the secure telephone communications.

H. CONTROL OF THE <DEVICE MODEL>

2. [delete if not appropriate] [Each participating site requires the appointment of a <device model> Local Manager.] The <device model> are registered cryptographic items in the <responsible nation> and are controlled cryptographic items in the other nations. They will be issued to the designated system operators at each contractor facility by the controlling COMSEC Custodian within the COMSEC Material Control System. All personnel responsible for the control, accountability, and operation of the terminals will be briefed by the respective COMSEC Custodian as to his/her responsibilities.

3. <device model> use <specific key material> which is replaced <time plan> under the arrangements of the <responsible nation> COA. <device model> cryptographic keys will be marked <appropriate security classification> but approved for use at <appropriate security classification>, supplied by <responsible nation agency> and distributed by the <responsible nation> National Distribution Agency (NDA) to the relevant National Distribution Agencies for distribution within nations. Encryption keys will be maintained in:

a) [nation A] by: [participating site], COMSEC Account Number [number]; [participating site], COMSEC Account Number [number].

b) [nation B] by: [participating site], COMSEC Account Number [number]; [participating site], COMSEC Account Number [number].

SECTION III - PROCEDURES

A. SECURE VOICE

1. The following procedures shall be implemented when utilising a <device model> for a classified voice communication:

   a. The terminal must be located in an area conducive to acoustic security. The area should be constructed in a manner that would preclude non-cleared personnel gaining access to the information being discussed.

   b. Secure calls should be prearranged to ensure system operators are available at both ends.

   c. The system operator initiating the call, and the system operator receiving the call, will execute the "Secure Voice Record" (see Attachment 1). This shall include call duration (date/starting and ending times), names, citizenship and clearance level of all participants and the unclassified subject matter of discussion.

   d. It is the responsibility of each system operator to verify the identities and clearance levels of the participants at their respective sites.

   e. Every participant in a conversation has the responsibility of ensuring that the appropriate foreign disclosure authorisations for the information being discussed have been received from their respective governments.

   f. Although prior approval to conduct a classified conversation is not required from the DRA, any classified notes made during a call should be passed to the DRA. It is the responsibility of the participant originating such material to classify (or otherwise mark), protect and control it in accordance with the host facility's security regulations and procedures.

   g. The DRA will review the Secure Voice Record on a weekly basis to ensure the records are being properly maintained.

      {By mutual agreement of the NSA's/DSAs, the Secure Voice Record may be not included.}

B. SECURE DATA FILE TRANSFER

1. All data to be transmitted over the secure telephone communications must be approved by the DRA prior to transmission. Interactive processing between the system equipment PC workstations is not permitted.

2. The requesting sender of the data file is responsible for:

    a. Ensuring that the removable transfer medium, to which the relevant data file will be copied, is pre-formatted to ensure erasure of all other information that may have previously resided on that medium. Only files for transmission may reside on the medium.

    b. Ensuring that the appropriate classification level indicators are contained within the file and on the outside of the medium.

    c. Initiating a "Secure Data File Transfer Request" form (Attachment 2), including the number of files to transfer and their names, classifications and descriptions.

3. The requesting sender will then obtain the approval of the facility DRA. After DRA approval has been received, the transfer medium, along with the request, will be provided to the system operator for transmission.

4. Upon receipt of the Secure Data File Transfer Request and the transfer medium, the sending system operator will:

    a. Ensure the Secure Data File Transfer Request is complete so far.

    b. Initiate a secure session with the distant system operator, pass the details from the Secure Data File Transfer request, including the number of files to transfer and their names, classifications and descriptions, and transmit the file(s).

5. After transmission, the sending system operator shall:

    a. Confirm with the Receiving Facility System Operator that all data files listed on the Secure Data File Transfer Request were received.

    b. Complete the remainder of the Secure Data File Transfer Request.

    c. Retain the Secure Data File Transfer Request.

    d. Release the transfer medium back to the requesting sender in accordance with the host facility's security regulations and procedures.

6. Upon initiation of a secure data file transfer session, the receiving system operator shall begin completion of a Secure Data File Transfer Receipt (Attachment 3), in accordance with the details passed by the sending system operator.

7. Upon completion of the transfer session, the receiving system operator shall

    a. Complete the Secure Data File Transfer Receipt.

b. Ensure that the transfer medium is marked with the highest classification level shown on the Secure Data File Transfer Receipt.

c. Provide the transfer medium to the DRA for his/her acceptance.

d. Retain the Secure Data File Transfer Receipt and distribute the transfer medium to the Intended Addressee in accordance with the host facility's security regulations and procedures.

8. As an alternative to passing the information about the transfer verbally to the receiving system operator, the sending system operator may create a computer text file, in which to list the relevant information from the Secure Data File Transfer Request, and transmit this at the beginning of the data transfer.

C. SECURE FACSIMILE

1. All material required to be transmitted via secure facsimile must be approved by the DRA prior to transmission.

2. Material for a secure facsimile transmission must be accompanied by a "Secure Facsimile Cover Sheet" (see Attachment 4).

3. The requesting sender will complete the facsimile cover sheet and obtain the approval of the facility DRA. After DRA approval has been received, the material, along with the Secure Facsimile Cover Sheet, will be provided to the system operator for transmission.

4. Upon receipt of the material and Secure Facsimile Cover Sheet, the sending system operator will:

   a. Ensure that the cover sheet is complete.

   b. Assign a sequential transmission number.

   c. Annotate on the cover his/her name and initials.

   d. Establish a voice connection with the receiving system operator.

   e. If the connection is made, annotate the date and time of transmission on the cover.

   f. Initiate a secure facsimile session and transmit the material.

5. After transmission, the sending system operator will confirm that all material was received. The sending system operator will retain a copy of the facsimile cover sheet on file and release the material back to the requesting sender in accordance with the host facility's security regulations and procedures.

6. Upon receipt of the facsimile transmission, the receiving system operator will:

   a. Annotate on the Secure Facsimile Cover Sheet his/her name and initials.

   b. Provide the material to the DRA for his/her acceptance.

   c. After the DRA's acceptance, retain a copy of the Secure Facsimile Cover Sheet on file and distribute the material to the addressee in accordance with the host facility's security regulations and procedures.

D. MISCELLANEOUS

1. In the event a secure transmission is not completed during a session and the session, for whatever reason, cannot be re-established, the session will be considered to be complete. Any "partial" receipt of material/data will be provided to the DRA for approval and processed in accordance with the host facility's security regulations and procedures.

2. All transmission/receipt records will be maintained during the Concession Period and disposed of at the conclusion of the Concession Period by each contractor security staff only in accordance with the instructions of [insert relevant authority].

ATTACHMENT 1 - SECURE VOICE RECORD

SECURE VOICE RECORD

Facility location _____

DATE	TIME STARTING TIME ENDING	NAMES OF PARTICIPANTS CITIZENSHIP/CLEARANCE	SUBJECT OF DISCUSSION (Description must be UNCLASSIFIED)

ATTACHMENT 2 - SECURE DATA FILE TRANSFER REQUEST

Name/Position/Title of
Requesting Sender _____

Name/Position/Title of
Intended Addressee: _____

Number of Files To Transfer: _____

FILE NAME(S)	CLASSIFICATION	DESCRIPTION (INCLUDING No. OF BYTES)

Name & Signature of Approving
Designated Releasing Authority: _____ Date: _____
(Releasing Facility)

Transmitting Facility: _____

Transmission Number: _____

Date of transmission: _____Start Time: _____Stop Time: _____

Status of Transmission: _____ (successful/partial)

Receiving Facility System Operator Name: _____

Transmitting Facility System Operator Name: _____ Initials: _____

ATTACHMENT 3 - SECURE DATA FILE TRANSFER RECEIPT

Name of Approving
Designated Releasing Authority: _____ Date: _____
(Sending Facility)

Transmitting Facility: _____

System Operator Name: _____ Transmission Number: _____

Receiving Facility: _____

System Operator Name & Initials: _____

Number of Files Received: _____ Date of transmission: _____

Start Time: _____

Stop Time: _____

Name/Position/Title of
Sender: _____

Name/Position/Title of
Intended Addressee: _____

FILE NAME(S)	CLASSIFICATION	DESCRIPTION (INCLUDING No. OF BYTES)

Name & Signature of Approving
Designated Releasing Authority:
(Receiving Facility) _____Date _____

ATTACHMENT 4 – secure FACSIMILE COVER SHEET

_____
(Classification Level of Cover Sheet if required)
COVERING _____
(Classification Level of Transmitted Document)

FACSIMILE COVER SHEET

Name/Position/Title of
Requesting Sender _____

Name/Position/Title of
Intended Addressee: _____

Subject/Description of Document: _____

Comments: _____

Name and Signature of Approving
Designated Releasing Authority: _____ Date: _____
(Releasing Facility)

Transmitting Facility: _____ Transmission Number: _____

Number of pages (including this page): _____ Date & Time of Transmission: _____

System Operator Name & Initials: _____
(Transmitting Facility)

System Operator Name & Initials: _____
(Receiving Facility)

Status of Transmission: _____ (successful/partial)

Name & Signature of Approving
Designated Releasing Authority: _____ Date:_____
(Receiving Facility)

COVERING _____
(Classification Level of Transmitted Document)

_____
(Classification Level of Cover sheet if required)