

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

- 9.8.4 Ensure that all persons having access to the Classified Information are informed of their responsibilities to protect the Classified Information in accordance with national security laws and regulations, and provisions of this MOU.
- 9.8.5 Carry out periodic security inspections of cleared facilities to ensure that the Classified Information is properly protected.
- 9.8.6 Ensure that access to the Classified Information is limited to those persons who have a need-to-know for purposes of the MOU.
- 9.9 Contractors, prospective Contractors, subcontractors, or prospective subcontractors who are determined by the Participant to be under financial, administrative, policy or management control of a Third Party, may participate in a Contract or subcontract requiring access to Classified Information provided pursuant to this MOU only when enforceable measures are in effect to ensure that a Third Party will not have access to Classified Information. If enforceable measures are not in effect to preclude access by a Third Party, the furnishing Participant will be consulted for written approval prior to permitting such access.
- 9.10 For any facility wherein Classified Information is to be used, the responsible Participant or Contractor will approve the appointment of a person or persons to exercise effectively the responsibilities for safeguarding at such facility the information pertaining to this MOU. These officials will be responsible for limiting access to the Classified Information involved in this MOU to those persons who have been properly approved for access and have a need-to-know.
- 9.11 Each Participant will ensure that access to the Classified Information is limited to those persons who possess requisite security clearances and have a specific need for access to the Classified Information in order to participate in this MOU.
- 9.12 Information provided or generated pursuant to this MOU may be classified as high as TOP SECRET/SPECIAL ACCESS REQUIRED (U.S.) and TOP SECRET/ CODEWORD (UK). The existence and the contents of this MOU are U.S.: FOUO and UK: UK UNCLASSIFIED.

SECTION X

LIABILITY AND CLAIMS

- 10.1 Claims arising under this MOU will be dealt with under the Exchange of Notes between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America Concerning Defence Cooperation Arrangements of May 27, 1993. In respect of paragraph 1.(b)(ii) of the Chapeau, each Participant will consult in respect of claims by third parties for injury or death to persons or damage to property arising from the performance of official duties in connection with this MOU.

SECTION XI

CUSTOMS DUTIES, TAXES, AND SIMILAR CHARGES

- 11.1 Customs duties, import and export taxes, and similar charges will be administered in accordance with each Participant's respective laws and regulations. To the extent existing national laws and regulations permit, the Participants will endeavor to ensure that such readily identifiable duties, taxes and similar charges, as well as quantitative or other restrictions on imports and exports, are not imposed in connection with work carried out under this MOU.
- 11.2 Each Participant will use its best efforts to ensure that customs duties, import and export taxes, and similar charges are administered in a manner favorable to the efficient and economical conduct of the work. If any such duties, taxes, or similar charges are levied, the Participant in whose country they are levied will bear such costs.
- 11.3 If, in order to apply European Community (EC) regulations, it is necessary to levy duties, then these will be met by the EC member end recipient. To this end, parts of the components of the equipment coming from outside the EC will proceed to their final destination accompanied by the relevant customs document enabling settlement of duties to take place. The duties will be levied as a cost over and above that Participant's shared cost of the Project.

SECTION XII

SETTLEMENT OF DISPUTES

- 12.1 Disputes between the Participants arising under or relating to this MOU will be resolved only by consultation between the Participants and will not be referred to a national court, an international tribunal, or to any other person or entity for settlement.

SECTION XIII

AMENDMENT, TERMINATION, ENTRY INTO EFFECT, AND DURATION

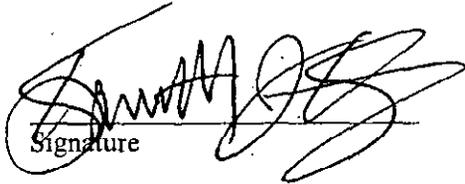
- 13.1 All activities of the Participants under this MOU will be carried out in accordance with their respective national laws.
- 13.2 The responsibilities of the Participants will be subject to the availability of funds for such purposes.
- 13.3 In the event of a conflict between a Section of this MOU, any Annex to this MOU and any IEP Annex under this MOU, the MOU will govern, except with regard to security classifications and information disclosure requirements specified in an IEP Annex.
- 13.4 This MOU may be amended by the mutual written consent of the Participants. However, Annex A (Co-Utilization Arrangement) and SAP IEP Annexes may be amended upon the mutual decision of the U.S. and UK SPWG co-chairs.
- 13.5 This MOU and any SAP IEP Annex may be terminated at any time upon the written consent of the Participants. In the event both Participants consent to terminate this MOU or any SAP IEP Annex, the Participants will consult prior to the date of termination to ensure termination on the most economical and equitable terms. In the event that this MOU is terminated, all annexes and subordinate documents will also terminate no later than the same termination date.
- 13.6 Either Participant may terminate this MOU or any SAP IEP Annex upon 90 days written notification of its intent to terminate to the other Participant. Such notice will be the subject of immediate consultation by the SPWG to decide upon the appropriate course of action to conclude the activities under this MOU or any SAP IEP. In the event of such termination, the following rules apply:
 - 13.6.1 The Participants will continue participation, financial or otherwise, up to the effective date of termination.
 - 13.6.2 All SAP Project Information and rights therein received under the provisions of this MOU prior to the termination will be retained by the Participants, subject to paragraph 13.7.
- 13.7 The respective benefits and responsibilities of the Participants regarding Section VI (Disclosure and Use of Special Access Program (SAP) Project Information), Section VII (Controlled Unclassified Information), Section IX (Security), Section X (Liability and Claims), Section XII (Settlement of Disputes), and this Section XIII (Amendment, Termination, Entry into Effect, and Duration) will continue to apply notwithstanding termination or expiration of this MOU.

13.8 This MOU, which consists of 13 Sections and two Annexes, will enter into effect upon signature by both Participants and will remain in effect for ten (10) years. It may be extended by the mutual written consent of the Participants.

The foregoing represents the understandings reached between the Secretary of Defense on behalf of the Department of Defense of the United States of America and the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland on the matters referred to herein,

Signed in duplicate, in the English language.

FOR THE SECRETARY OF DEFENSE
ON BEHALF OF THE DEPARTMENT OF
DEFENSE OF THE UNITED STATES OF
AMERICA


Signature

KENNETH J. KRIEG

Name

USD (AT&L)

Title

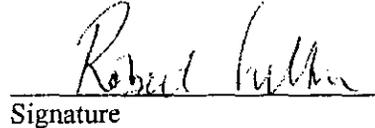
DECEMBER 19, 2005

Date

WASHINGTON, D.C.

Location

FOR THE SECRETARY OF STATE FOR
DEFENCE ON BEHALF OF THE
MINISTRY OF DEFENCE OF THE
UNITED KINGDOM OF GREAT
BRITAIN AND NORTHERN IRELAND


Signature

LT. GEN. SIR ROBERT FULTON KBE, RM

Name

DCDS (EC)

Title

DECEMBER 19, 2005

Date

WASHINGTON, D.C.

Location

ANNEX A

**SPECIAL ACCESS PROGRAM CO-ORDINATION OFFICE CO-UTILIZATION
ARRANGEMENTS BETWEEN THE DEPARTMENT OF DEFENSE OF THE
UNITED STATES OF AMERICA AND THE MINISTRY OF DEFENCE OF THE
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND**

References:

- (a) The Exchange of Notes between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America Concerning Defence Cooperation Arrangements of May 27, 1993
- (b) *United States – United Kingdom General Security Agreement (GSA)*, April 14, 1961
- (c) Security Implementing Arrangement for Operations between the Ministry of Defence of the United Kingdom and the Department of Defense of the United States, January 27, 2003
- (d) DCID 1/19 (Security Policy for Sensitive Compartmented Information and Security Policy Manual)
- (e) DCID 6/4 (Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI))
- (f) DCID 1/21 (Physical Security Standards for Sensitive Compartmented Information Facilities)
- (g) DCID 6/3 (Protecting Sensitive Compartmented Information within Information Systems – Manual)
- (h) DOD Overprint to the National Industrial Security Program Operating Manual Supplement, January 3, 1998
- (i) DOD 5101.21-M-1 (SCI Administrative Security Manual)
- (j) CNO (N89) Instruction “Fleet Special Access Programs Security Desk Operating Guide” OPNAV/N89-0017-00
- (k) UK JSP440 (The Defence Manual of Security Issue 3.3)
- (l) DCID 3/29 (Controlled Access Program Oversight Committee)
- (m) UK JSP440 Supplement 2 (STRAP Management)
- (n) “Memorandum of Understanding (MOU) Between the Secretary of Defense on Behalf of the Department of Defense of The United States of America and the Secretary of State for Defence of the Ministry of Defence of the United Kingdom of Great Britain and Northern Ireland for Special Access Program Coordination of Research, Development, and Acquisition (RD&A) Information Exchange”

A. DEFINITIONS

1. **Co-Utilization:** Use of the same facility / resource to handle various types of Compartmented Information (CI).
2. **National Co-Utilization Facility (NCF):** A facility implemented using the appropriate national standards and procedures by each Participant to provide a degree

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

of protection at least equivalent to that of the Compartmented Information furnishing Participant.

3. **Compartmented Information Clearance (CIC):** The Participant clearance level necessary to gain access to Compartmented Information furnished by the other Participant. For U.S. personnel, the clearance level will be SCI/SAP whilst for UK personnel it will be Developed Vetting (DV) with the addition of STRAP indoctrination for SAPCO personnel. By reciprocal agreement each Participant will accept the other Participant's assessment of an individual's qualifications for meeting clearance requirements without additional reviewer adjudication.
4. **SAPCO Integrity Manager (SIM).** The individual at the Participants' respective SAPCOs appointed by SCO as his empowered designate to manage security for Compartmented Information shared under reference (m) on a day-to-day basis.

B. PURPOSE

1. Cognizant of references (a) through (c) within which the Participants assure to provide an equivalent degree of protection to all levels of Classified Information furnished by the other Participant, this Annex supplements existing national security and disclosure controls to define the additional security policies and procedures both Participants will apply within their SAPCO to maintain security and integrity of all types of Compartmented Information handled under reference (n).
2. This Annex, in conjunction with References (b) and (c), collectively accommodates the requirements of References (d) through (k). Further, it can serve as the basis for including additional and other relevant security requirements which may be required to facilitate protection of Compartmented Information to intelligence activities as addressed in Reference (l) and Reference (m).

C. APPLICABILITY

1. The policies and procedures in this Annex apply to all personnel granted access to and those working full-time and temporarily within either Participants' SAPCO.

D. SCOPE

1. The areas of security management responsibility will entail information security to include access, control and handling transmission and reproduction, physical security, technical security, personnel security, operations security, emanations security, and automated information system (AIS) security to include system accreditation and administration security.
2. This Annex is additional to, and does not replace or take precedence over, the Participants' existing security regulations and bilateral security agreement / arrangements (References (a) through (c)) to provide for the equivalent degree of protection to Classified Information furnished by the other Participant as described in this MOU.

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

E. RESPONSIBILITIES:

1. The Designated Security Authority:

- a. Is responsible for the accreditation of the integrity and overall physical security of the SAPCO through the application of the Participant's national security standards addressing physical access control methods, audio countermeasures, TSCM, TEMPEST, and AIS security for Compartmented Information.
- b. Is responsible for approving the Participant's Compartmented Information document control procedures to include receipt, storage, dissemination, couriating, inventory and destruction of all accountable material and AIS media in the proper separate control system within the SAPCO.
- c. Is responsible for approving the personnel security, Compartmented Information segregation, Compartmented Information management and personnel access procedures to the SAPCO.
- d. Will review and approve Coordination Officer investigations and reports of all security incidents and violations.
- e. Is responsible for approving an Emergency Action Plan (EAP) for the SAPCO.
- f. Will periodically inspect the SAPCO to ensure compliance with appropriate Participant's security standards and procedures.
- g. Will provide Compartmented Information security awareness information and other guidance and assistance to the Coordination Officer.

2. The SAPCO Coordination Officer:

- a. May designate an individual who is knowledgeable of security requirements to serve as the SAPCO Integrity Manager (SIM). If a SIM is designated, the Coordination Officer retains overall responsibility, but may delegate day-to-day responsibility for security management to the SIM.
- b. Will be responsible for the receipt, storage, control, access, dissemination, destruction, maintenance of accountability records and periodic inventory of all Compartmented Information materials held within the Participant's SAPCO.
- c. Will obtain applicable national Accreditation or certification for electronic processing systems processing Classified Information.
- d. Will coordinate, develop and implement local security policy and guidance specifying procedures that are consistent with maintaining adequate segregation and protection of differing control systems for the various types of Compartmented Information stored within the Participant's SAPCO.
- e. Will develop an Emergency Action Plan (EAP) for the SAPCO.
- f. Will provide on-site security oversight of Compartmented Information and material contained within the SAPCO.
- g. Will ensure all personnel are knowledgeable of national regulations to ensure appropriate control of all levels of Classified Information and material.
- h. Will provide visitor control and clearance/access verification/certification of all personnel entering the SAPCO.

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

- i. Will within 48 hours investigate and report all security incidents/violations, investigate all alarm violations, and evaluate guard responses involving the SAPCO to include notification to the other Participant's Coordination Officer where the occurrence affects their Compartmented Information.
- j. Will obtain applicable Compartmented Information TEMPEST and AIS systems accreditation/certification from the appropriate national Authority for equipment processing Compartmented Information material.
- k. Is responsible for all types of Compartmented Information-related security education and training of Participant's CIC personnel.
- l. Will establish additional personnel security and access controls for persons entering the Participant's SAPCO.

F. PROCEDURES:

1. In accordance with existing international agreements (references (a) and (c)), each Participant will afford an equivalent degree of protection to the other Participant's Compartmented Information through the application of the necessary national policies and procedures.
2. In addition:
 - a) All persons entering the NCF must hold the appropriate CIC or be escorted at all times by a person with such a clearance.
 - b) Non-CIC visitors will be permitted access to perform official duties only after all Compartmented Information material has been properly secured to prevent access.
 - c) The approval of the furnishing Participant's SCO will be required before access to Compartmented Information is granted to individuals with a clearance level less than CIC.
 - d) No individuals who have CIC clearances based on a waiver, exception, or deviation will be allowed access to Compartmented Information without the specific agreement of the furnishing Participant's SCO.
 - e) There will be a system to validate the currency of known information on SAPCO staff and those having access within the SAPCO to Compartmented Information.
 - f) All types of Compartmented Information records and logs will be kept within designated areas totally separated from other types of Compartmented Information records, except those pertaining to joint Compartmented Information material.
 - g) Participant's DSA personnel will have access at any time to their respective SAPCO upon coordination with the SCO or SIM to perform various Compartmented Information security-related tasks. Additionally, DSA personnel will be CIC.
 - h) SAPCO personnel with access to the other Participant's Compartmented Information will validate not less than every six months that there has been no change to the information originally provided to the relevant authorities as the basis for approving their security clearance.

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

- i) Pursuant to established rules, any items of security concern or suitability for a Participant's SAPCO-related personnel including DSA will be immediately reported to the appropriate national authority for review and evaluation.
- j) All electronic processing equipment brought into the SAPCO NCF must be approved by the DSA. All equipment processing Compartmented Information must be accredited through the appropriate national authorities.

G. IMPLEMENTATION:

- I. This Annex will be reviewed annually by the SPWG and may be modified at any time upon mutual consent of the SPWG representatives.

ANNEX B

MODEL INFORMATION EXCHANGE PROJECT ANNEX

"MODEL" U.S. DoD – UK MOD
SPECIAL ACCESS PROGRAM (SAP) INFORMATION EXCHANGE PROJECT (IEP)
ANNEX

CONCERNING

(Provide Title)

In accordance with the Special Access Program (SAP) Coordination of Research, Development, and Acquisition (RD&A) Information Exchange Memorandum of Understanding between the Secretary of Defense on behalf of the Department of Defense of the United States of America and the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland (U.S. DoD – UK MOD SAPCO MOU), signed on _____, _____, in _____, the following SAP IEP Annex is established. All of the provisions of the U.S. DoD-UK MOD SAPCO MOU are incorporated by reference.

1. DESCRIPTION: (Note: Provide a description of the scope.)

a. The scope of this SAP IEP Annex comprises exchange of SAP Project Information in the following technology areas:

(1) (Note: Provide a specific description of the SAP IEP Annex's scope by listing pertinent technology areas where RD&A Information is to be exchanged.)

(2) (Note: Specifically identify any proposed exchange of technology base computer software within the tasks established in the scope, if envisioned.)

b. Exchanges of SAP Project Information under this SAP IEP Annex will be on an equitable basis.

2. COORDINATION OFFICERS, SAPCO SECURITY OFFICERS, DSA POINT OF CONTACT, TECHNICAL PROJECT OFFICERS, LIAISON OFFICERS, AND ESTABLISHMENTS:

a. For the U.S. DoD:

- (1) SAPCO Officer (or his/her designee)
- (2) SAPCO Security Officer (or his/her designee)
- (3) DSA Point of Contact
- (4) Technical Project Officer
- (5) Establishments

(a) _____

- b. For the UK MOD:
- (1) SAPCO Officer (or his/her designee)
 - (2) SAPCO Security Officer (or his/her designee)
 - (3) DSA Point of Contact
 - (4) Technical Project Officer
 - (5) Establishments.
 - (a) _____

3. SPECIAL DISCLOSURE AND USE OF INFORMATION PROVISIONS
(Optional):

Note: Most SAP IEP Annexes will not require the addition of any special provisions in this area. However, if the Participants desire to establish such provisions, descriptive text should be inserted here. For example,

"Use of SAP Project Information may be authorized for use in designated defense programs of the Participants."

Wider use may be specified, but this will require establishment of special disclosure and use rights provisions for Foreground and Background Information.

4. ESTABLISHMENT, DURATION, AND TERMINATION OF THIS SAP IEP ANNEX:

a. This SAP IEP Annex, an Annex under the SAPCO MOU, will enter into effect upon signature by the SAPCO MOU SPWG representatives and will remain in effect for [specify] years unless terminated in accordance with Section XIII of the SAPCO MOU. It may be extended by the written mutual determination of the SPWG representatives.

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

FOR THE SECRETARY OF DEFENSE
ON BEHALF OF THE DEPARTMENT OF
DEFENSE OF THE UNITED STATES OF
AMERICA

FOR THE SECRETARY OF STATE FOR
DEFENCE ON BEHALF OF THE
MINISTRY OF DEFENCE OF THE
UNITED KINGDOM OF GREAT
BRITAIN AND NORTHERN IRELAND

Signature

Signature

Name

Name

Title

Title

Date

Date

Location

Location

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

THIS PAGE LEFT INTENTIONALLY BLANK

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

35 of 35