

[ Ken Krieg, Robert Fulton. (Dec. 19, 2005). TOP SECRET US-UK Memo re. Special Access Programs (SAP) for Information Exchange, Kenneth L. Fulton, Sir Robert Fulton KBE KStJ. US Sec. Def., WikiLeaks.  
<https://file.wikileaks.org/file/us-uk-top-secret-sap-mou-2005.pdf> ]

**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 UNITED KINGDOM OF GREAT BRITAIN AND  
NORTHERN IRELAND**

**FOR**

**SPECIAL ACCESS PROGRAM COORDINATION OF  
RESEARCH, DEVELOPMENT, AND ACQUISITION (RD&A)  
INFORMATION EXCHANGE**

(Short Title: U.S. DoD-UK MoD SAPCO MOU)

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

THIS PAGE LEFT INTENTIONALLY BLANK

UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY

2 of 35

TABLE OF CONTENTS

INTRODUCTION..... 4

SECTION I..... 5

    DEFINITIONS..... 5

SECTION II..... 8

    OBJECTIVES AND SCOPE OF WORK..... 8

SECTION III..... 10

    MANAGEMENT (ORGANIZATION AND RESPONSIBILITY)..... 10

SECTION IV..... 13

    FINANCIAL RESPONSIBILITY..... 13

SECTION V..... 14

    CONTRACTUAL ARRANGEMENTS..... 14

SECTION VI..... 15

    DISCLOSURE AND USE OF SPECIAL ACCESS PROGRAM (SAP) PROJECT INFORMATION... 15

SECTION VII..... 17

    CONTROLLED UNCLASSIFIED INFORMATION..... 17

SECTION VIII..... 18

    VISITS TO ESTABLISHMENTS..... 18

SECTION IX..... 19

    SECURITY..... 19

SECTION X..... 22

    LIABILITY AND CLAIMS..... 22

SECTION XI..... 23

    CUSTOMS DUTIES, TAXES, AND SIMILAR CHARGES..... 23

SECTION XII..... 24

    SETTLEMENT OF DISPUTES..... 24

SECTION XIII..... 25

    AMENDMENT, TERMINATION, ENTRY INTO EFFECT, AND DURATION..... 25

ANNEX A..... 27

ANNEX B..... 32

INTRODUCTION

The Secretary of Defense on behalf of the Department of Defense of the United States of America (U.S. DoD) and the Secretary of State for Defence of the United Kingdom of Great Britain and Northern Ireland (UK MOD), hereinafter referred to as the "Participants":

Recognizing 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;

Recognizing the General Security Agreement (GSA) of April 14, 1961 and the Security Implementing Arrangement for Operations of January 27, 2003 between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland;

Having a common interest in defense issues;

Recognizing the benefits to be obtained from standardization, rationalization, and interoperability of military equipments;

Desiring to improve their mutual conventional defense capabilities through the application of emerging technology;

Having a mutual need for Special Access Program (SAP) coordination and information exchange to satisfy common operational requirements and in furtherance of the Bilateral Defense Acquisition Committee Special Programs Working Group decision made on February 9, 2005;

Having independently determined the need for coordination and data sharing between the Participants' SAP Coordination Offices (SAPCOs); and

Desiring to establish a routine channel for sharing SAP Research, Development, and Acquisition (RD&A) information in order to maintain appropriate safeguards, facilitate dissemination of data, and provide a security context for cooperative programs and competitions requiring exchange of such information;

Have reached the following understandings:

SECTION I

DEFINITIONS

The Participants have jointly decided upon the following definitions for terms used in this MOU:

BRENT	BRENT is a secure ISDN (Integrated Services Digital Network) telephone, that protects voice and data up to TOP SECRET and all UK caveats.
Classified Information	Information that requires protection in the interests of national security and is so designated by the application of a security classification marking. This information may be in oral, visual, magnetic or documentary form or in the form of equipment or technology.
Compartmented Information	Information held by either Participant requiring enhanced need-to-know access control in the interests of national security and is so designated by the application of a security classification marking. This information may be in oral, visual, magnetic or documentary form or in the form of equipment or technology.
Contract	Any mutually binding legal relationship under national laws that obligates a Contractor to furnish supplies or services, and obligates one or both of the Participants to pay for them.
Contractor	Any entity awarded a Contract by a Participant's contracting agency.
Controlled Unclassified Information	Unclassified information to which access or distribution limitations have been applied in accordance with applicable national laws or regulations. Whether the information is provided or generated under this MOU or an Information Exchange Project (IEP), the information will be marked to identify its "in confidence" nature. It could include information that has been declassified, but remains controlled.
Coordination Officer	The member of the Participant's SAPCO organization responsible for the daily management of the SAPCO and Special Programs Working Group (SPWG) activities.
Designated Security Authority	The security office approved by national authorities to be

**UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY**

(DSA)	responsible for the security aspects of this MOU.
Information Exchange Project (IEP)	A specific program of work or activity undertaken within the framework of acknowledged common mechanisms of information exchange and adopted as an Annex of this MOU.
Project	A research, development, or acquisition activity involving defense technology, equipment or systems. No Project efforts other than IEPs will be implemented under this MOU.
Project Information	Any research, development, or acquisition information provided to, generated in, or used in a Project regardless of form or type, including, but not limited to, that of a scientific, technical, business, or financial nature, and also including photographs, reports, manuals, threat data, experimental data, test data, designs, specifications, processes, techniques, inventions, drawings, technical writings, sound recordings, pictorial representations, and other graphical presentations, whether in magnetic tape, computer memory, software (including source code) or any other form and whether or not subject to copyright, patent, or other legal protection.
Special Access Program Coordination	Activities that create and support a government-to-government channel for sharing SAP Project Information while maintaining appropriate security safeguards.
Special Access Program (SAP)	A defense activity employing enhanced security measures exceeding those normally required for information at the same classification level.
Special Access Program Coordination Office (SAPCO)	A Participant's single focal-point for all SAP activities.
Sensitive Compartmented Information (SCI)	U.S. Classified Information concerning or derived from intelligence sources, methods, or analytical processes and required to be handled within formal access control systems established by the U.S. Director of Central Intelligence.
Special Programs Working Group (SPWG)	A working group established to direct and administer the activities of this MOU.
STRAP	A collective term for a set of nationally (UK) approved principles and procedures for enhanced need-to-know protection of sensitive intelligence (and related operational information) produced by the Principal UK Intelligence Agencies and from elements of the UK MOD. STRAP is accepted by the U.S.

**UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY**

Intelligence and DoD community as the mechanism by which highly sensitive U.S. intelligence material is controlled when in UK Government hands.

STRAP Equivalency Level (SEL)	The adoption of a STRAP security level with associated policies and procedures for the management and control of non-STRAP material.
Secure Telephone Unit (STU)	A U.S. standard for secure analog telephone devices for use as both ordinary telephones and secure instruments over the dial-up public switch telephone network.
Secure Terminal Equipment (STE)	The U.S. evolutionary successor to the STU replacing the analog STU equipment with digital-based STE units.
Technical Project Officer (TPO)	A representative of a government organization who is specifically authorized to exchange Project Information under an IEP.
Third Party	A government other than the government of a Participant and any person or other entity whose government is not the government of a Participant.

SECTION II

OBJECTIVES AND SCOPE OF WORK

- 2.1 The objectives and scope of work of this MOU are to:
- 2.1.1 Establish a conduit for sharing SAP Project Information while maintaining appropriate safeguards. This conduit will allow dissemination of SAP Project Information to in-country, defense activities and provide a security structure for cooperative programs and competitions requiring SAP Project Information protection.
  - 2.1.2 Implement equivalent, nationally accredited, central SAP Coordination Offices (SAPCO) to be the single in-country focal point for administration and execution of this MOU. The UK and U.S. SAPCOs will be operated in accordance with Annex A (Co-Utilization Arrangement).
  - 2.1.3 Establish a framework for U.S. DoD-UK MOD SAPCO coordination and monitoring of SAP-related exchange of Project Information, personnel, transfers or loans of SAP material and/or equipment, and research, development, acquisition, or support of SAP material and/or equipment conducted through existing or future program or project-specific Memoranda of Understanding (MOUs), Information Exchange Projects (IEPs), Project Arrangements (PAs), or other written arrangements.
  - 2.1.4 Conduct U.S. DoD-to-UK MOD SAPCO coordination of bilateral cooperation in SAP areas of interest, including coordinated oversight of all bilateral SAPs through equivalent security oversight requirements and standards to the maximum extent possible, taking into account differences in the Participants' legal and regulatory standards regarding SAP Projects.
  - 2.1.5 Establish and implement a common access database for bilateral SAP Projects whereby both Participants can determine the program access status for a specific individual.
  - 2.1.6 Establish and implement common secure communication protocols for transmission of SAP Project Information, including, but not limited to, secure telephone (i.e., STU/STE, BRENT) and secure fax communication links, between authorized entities of the Participants.
- 2.2 SAP Project Information exchange activities under this MOU will be managed under separate Information Exchange Projects (IEP). Each IEP will specify the scope of the information that may be exchanged. Once approved, each IEP will form an integral part of this MOU. An IEP will generally conform to the format in Annex B and will:



- 2.2.1 Specify the scope of the exchange.
  - 2.2.2 Identify national Technical Project Officers and Establishments.
  - 2.2.3 When necessary, specify an applicable special disclosure and use provisions.
  - 2.2.4 Identify the highest level of classification of information that may be exchanged under the IEP.
  - 2.2.5 Establish a termination date for the IEP which will precede the termination date of this MOU.
- 2.3 Information exchanged specifically for the purpose of harmonizing the Participants requirements for formulating, developing, and negotiating IEPs is permitted under this MOU. In addition to markings as specified in sections 7.3 and 9.2, such Information will be marked "For UK / U.S. SAPCO MOU Requirements Harmonization Only" and may not be used for any other purpose.
- 2.4 This MOU is limited to information exchange. Collaborative projects that may arise from information exchange under this MOU that involve the commitment of resources are outside the scope of this MOU and will be established through separate arrangements.

SECTION III

MANAGEMENT (ORGANIZATION AND RESPONSIBILITY)

- 3.1 This MOU will be directed and administered by a Special Programs Working Group (SPWG) co-chaired by:
  - 3.1.1 U.S.: Director, Special Programs, Office of the Under Secretary of Defense (Acquisition, Technology & Logistics) (or his/her successor in the event of reorganization).
  - 3.1.2 UK: Science and Technology Director, UK MOD (or his/her successor in the event of reorganization).
- 3.2 The SPWG will report to U.S.-UK Bilateral Defense Acquisition Committee (BDAC) (or its equivalent in the event of reorganization) for the duration of this MOU.
- 3.3 The SPWG will have overall authority for SAP Project Information proposed for exchange. The SPWG, or their designees, will have primary responsibility for implementation, management, and direction of the exchange activity in accordance with the provisions of this MOU.
- 3.4 Each SPWG co-chair will appoint a Coordination Officer to manage day-to-day MOU activities. The SPWG representatives, Coordination Officers, and supporting U.S. DoD and UK MOD personnel will meet twice per year, with additional meetings held at the request of either representative. Each meeting of the SPWG will be chaired by the representative of the Participant hosting the meeting.
- 3.5 Decisions of the SPWG will be made unanimously by the co-chairs or their designated representatives. In the event that the SPWG is unable to reach a timely decision on an issue, each SPWG co-chair will refer the issue to their higher authority for resolution. In the meantime, the approved MOU activities will continue to be implemented without interruption under the direction of the Coordination Officers while the issue is being resolved by higher authority.
- 3.6 The SPWG will be responsible for:
  - 3.6.1 Exercising executive-level oversight of the SAP Project Information exchange.
  - 3.6.2 Discussing policies, plans, and requirements pertaining to future SAP activities being considered for bilateral collaboration.

**UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY**

- 3.6.3 Identifying potential areas for bilateral SAP collaboration.
- 3.6.4 Approving proposed SAP IEPs.
- 3.6.5 Overseeing the implementation of approved SAP IEPs and the SAP elements of duly authorized program or project-specific MOUs, PAs, or other written arrangements.
- 3.6.6 Reviewing and forwarding to the Participants for approval recommended amendments to this MOU in accordance with Section XIII (Amendment, Termination, Entry into Effect, and Duration) of this MOU.
- 3.6.7 Approving amendments to each IEP consistent with Section XIII (Amendment, Termination, Entry into Effect, and Duration) of this MOU.
- 3.6.8 Reviewing the twice-annual status reports submitted by the Coordination Officers.
- 3.7 Coordination Officers for the DoD and MOD, located in Washington, D.C. and in London, respectively, will oversee execution of this MOU.
- 3.8 The Coordination Officers are responsible for management of the unique national aspects of Section II (Objectives and Scope of Work) of this MOU.
- 3.9 In addition to the responsibilities detailed in the Co-Utilization Arrangement (Annex A), the Coordination Officers will also be responsible for:
  - 3.9.1 Managing the security and technical aspects of the SAP Project activities.
  - 3.9.2 Proposing the establishment of SAP IEPs.
  - 3.9.3 Monitoring the implementation of approved SAP IEPs.
  - 3.9.4 Monitoring the implementation of duly authorized SAP-related exchange of personnel, transfers or loans of SAP materiel and/or equipment, and research, development, acquisition, or support of SAP materiel and/or equipment conducted through existing or future program or project-specific MOUs, PAs, or other written arrangements.
  - 3.9.5 Referring issues that cannot be resolved by the Coordination Officers to the SPWG.
  - 3.9.6 Developing and recommending amendments to this MOU and its Annexes to the SPWG.
  - 3.9.7 Providing twice-annual status reports on each SAP IEP to the SPWG, and

**UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY**

other such reports as directed by the SPWG.

- 3.9.8 Appointing U.S. DoD and UK MOD SAPCO security officers.
- 3.9.9 Ensuring that the appropriate security management measures are in place and the coordination of any necessary security investigations.

SECTION IV

FINANCIAL RESPONSIBILITY

- 4.1 Each Participant will bear the full cost it incurs in conducting all activities under this MOU. No funds will be transferred between the Participants. A Participant will promptly notify the other Participant if available funds are not adequate to fulfill its responsibilities under this MOU. If a Participant notifies the other Participant that it is terminating or reducing its appropriated funding for any SAP Project Information exchange effort covered by a specific SAP IEP, the Participants will immediately consult with a view toward termination or continuation of the information exchange on a changed or reduced basis. In the event that an understanding to continue on a modified basis cannot be reached by the MOU Participants, the MOU Participant having reduced or modified its funding will be deemed to have withdrawn from this MOU and the provisions of Section XIII (Amendment, Termination, Entry into Effect and Duration) will apply.
- 4.2 The costs of any services or equipment provided by either Participant at the request of the other Participant that are not specifically addressed under the provisions of this MOU or IEPs will be borne by the Participant receiving such services through separate arrangements.

SECTION V

CONTRACTUAL ARRANGEMENTS

- 5.1 This MOU provides no legal authority for one Participant to place Contracts on the other Participant's behalf.

SECTION VI

DISCLOSURE AND USE OF SPECIAL ACCESS PROGRAM (SAP)  
PROJECT INFORMATION

- 6.1 SAP Project Information may not be released to Contractors without the prior written consent of the furnishing Participant unless specifically authorized in an IEP.
- 6.2 Any SAP Project Information provided by one Participant will be used by the other Participant only for information and evaluation purposes by their military personnel and civilian employees (excluding contractor support personnel), unless otherwise consented to in writing by the providing Participant. The receiving Participant will not disclose SAP Project Information provided under this MOU to any Third Party, other persons, or entities without the prior written consent of the providing Participant.
- 6.3 The receiving Participant will take all lawful steps available to ensure that any persons or entities to whom it discloses SAP Project Information provided under this MOU comply with the provisions of this MOU and any relevant IEP concerning the use, control, and protection of that specific SAP Project Information. The receiving Participant will ensure that any Third Parties, other persons, or entities (other than the military and civilian employees mentioned in paragraph 6.2) to whom it discloses SAP Project Information provided under this MOU are placed under a legally binding obligation to comply with the provisions of this MOU concerning use, control, and protection of SAP Project Information.
- 6.4 The Participants may determine in a specific SAP IEP Annex that SAP Project Information provided may be used for a purpose other than for information and evaluation purposes by their military personnel and civilian employees. The SAP IEP Annex will contain specific provisions for such use, which may include definition of Background and Foreground Information, as appropriate. Use for any other purpose will require the prior written consent of the providing Participant.
- 6.5 Under this MOU, SAP Project Information will remain the property of the originating Participant. No transfer of ownership of SAP Project Information will take place.
- 6.6 SAP Project Information will be provided only when it can be done without incurring liability to holders of proprietary rights, and where disclosure is in accordance with national disclosure policies and regulations of the furnishing Participant.

- 6.7 All SAP Project Information subject to proprietary interests will be identified, marked, and handled in accordance with Section VII (Controlled Unclassified Information) and IX (Security).



SECTION VII

CONTROLLED UNCLASSIFIED INFORMATION

- 7.1 Except as otherwise provided in this MOU, or as authorized in writing by the originating Participant, Controlled Unclassified Information provided or generated pursuant to this MOU or IEPs will be controlled as follows:
- 7.1.1 Such information will be used only for the purposes authorized for use of SAP Project Information as specified in Section VI (Disclosure and Use of Special Access Program (SAP) Project Information).
  - 7.1.2 Access to such information will be limited to personnel whose access is necessary for the permitted use.
  - 7.1.3 Each Participant will take all lawful steps, which may include national classification, available to it to keep SAP Project Information free from further disclosure (including requests under any legislative provisions), except as provided in paragraph 7.1.2, unless the originating Participant consents to such disclosure. In the event of unauthorized disclosure, or if it becomes probable that the information may have to be further disclosed under any legislative provision, immediate notification will be given to the originating Participant.
- 7.2 *Controlled Unclassified Information provided or generated pursuant to this MOU will be handled in a manner that ensures control as provided for in paragraph 7.1.*
- 7.3 To assist in providing the appropriate controls, the originating Participant will ensure that Controlled Unclassified Information is appropriately marked. Unless otherwise specified in a Project Security Instruction for a specific IEP, such information will bear the appropriate Controlled Unclassified Information legend, denote the country of origin, the provisions of release, and the fact that the information relates to this MOU.
- 7.4 Prior to authorizing the release of Controlled Unclassified Information to Contractors, the Participants will ensure the Contractors are legally bound to control such information in accordance with this MOU.

SECTION VIII

VISITS TO ESTABLISHMENTS

- 8.1 Each Participant will permit visits to its government establishments, agencies and laboratories, and Contractor industrial facilities by employees of the other Participant or by employees of the other Participant's Contractor(s), provided that the visit is authorized by both Participants and the employees have any necessary and appropriate security clearances and a need-to-know.
- 8.2 All visiting personnel will be required to comply with security regulations of the hosting Participant. Any information disclosed or made available to visitors will be treated as if supplied to the Participant sponsoring the visiting personnel, and will be subject to the provisions of this MOU and the appropriate IEP.
- 8.3 Requests for visits by personnel of one Participant to a facility of the other Participant will be coordinated through official channels, and will conform to the established visit procedures of the host country. Requests for visits will provide an unclassified rationale. SAP-related visits will be coordinated through U.S. and UK SAPCOs.
- 8.4 Lists of personnel of each Participant required to visit, on a continuing basis, facilities of the other Participant will be submitted through official channels in accordance with recurring international visit procedures.

SECTION IX

SECURITY

- 9.1 All Classified Information provided or generated pursuant to this MOU will be afforded an equivalent level of protection by the Participants in accordance with the UK/U.S. General Security Agreement dated April 14, 1961, as amended and including the Security Implementing Arrangement dated January 27, 2003, thereto.
- 9.2 Classified Information will be transferred only through official government-to-government channels or through channels approved by the Designated Security Authorities (DSAs) of the Participants. Such Classified Information will bear the level of classification, denote the country of origin, the provisions of release, and the fact that the information relates to this MOU and the specific IEP.
- 9.3 Each Participant will take all lawful steps available to it to ensure that Classified Information provided pursuant to this MOU is protected from further disclosure, except as permitted by paragraph 9.10, unless the other Participant consents in writing to such disclosure. Accordingly, each Participant will ensure that:
- 9.3.1 The recipient will not release the Classified Information to any government, national, organization, or other entity of a Third Party without the prior written consent of the originating Participant.
- 9.3.2 The recipient will not use the Classified Information for other than the purposes provided for in this MOU.
- 9.3.3 The recipient will comply with any distribution and access restrictions on information that is provided under this MOU.
- 9.4 The Participants will investigate all cases in which it is known or where there are grounds for suspecting that Classified Information provided pursuant to this MOU has been lost or disclosed to unauthorized persons. Each Participant also will promptly and fully inform the other Participant of the details of any such occurrences, and of the final results of the investigation and of the corrective action taken to preclude recurrences.
- 9.5 Information furnished under this MOU will, through existing agreements and arrangements (see 9.1), be provided the equivalent level of protection by the recipient through the application of the appropriate national security policies and procedures. Where information is not subject to enhanced need-to-know restrictions it will be protected to a level equivalent to the furnishing nation's

**UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY**

classification as specified in the GSA. In the case of SAP information exchanged under this MOU, the following conditions will be adhered to:

- 9.5.1 For UK SAP information under U.S. control, the recipient will apply SCI / SAP classification security policies and procedures.
- 9.5.2 For U.S. SAP information held under UK control the recipient will apply security policies and procedures associated with a STRAP Equivalency Level (SEL) of Level 1. The SEL-1 classification will be prefixed by the appropriate UK classification to align with the U.S. classification of the furnished information.
- 9.6 In the exceptional instances where both Participants deem existing national standards for protection of Classified / Compartmented Information require augmentation, a Project Security Instruction (PSI) will be written by the Technical Project Officers (TPOs) for the specific IEP. This PSI will describe the supplementary methods by which Project Information exchanged through the IEP will be marked, used, transmitted, and safeguarded. Individual PSIs will be reviewed and forwarded by the Coordination Officers to the SPWG for endorsement. PSIs will be approved by the appropriate DSA prior to the transfer of any Classified Information or Controlled Unclassified Information and will be applicable to all government and Contractor personnel participating in the specific IEP.
- 9.7 For each IEP a Security Classification Guide (SCG) will be established. The SCG describes how information exchanged within each IEP will be classified. SCGs will be subject to regular review and revision with the aim of downgrading the classification as appropriate.
- 9.8 The DSA of a Participant that awards a classified Contract will assume responsibility for administering within its territory security measures for the protection of the Classified Information, in accordance with its laws and regulations. Prior to the release to a Contractor, prospective Contractor, subcontractor, or prospective subcontractor of any Classified Information received under this MOU and appropriate IEP, the Participant will:
  - 9.8.1 Determine that such Contractor, prospective Contractor, subcontractor, or prospective subcontractor and their facility have the capability to protect the Classified Information adequately.
  - 9.8.2 Grant program access to the facility(ies), if appropriate.
  - 9.8.3 Grant program access for all personnel whose duties require access to Classified Information, if appropriate.

**UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY**

**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.

**UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY**

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

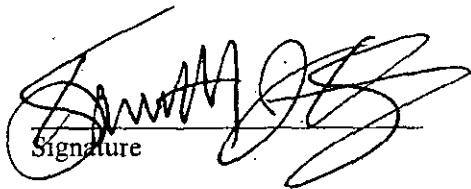
- 13.1 All activities of the Participants under this MOU will be carried out in accordance with their respective national laws.
- 13.2 The responsibilities of the Participants will be subject to the availability of funds for such purposes.
- 13.3 In the event of a conflict between a Section of this MOU, 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

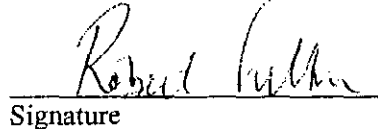
DECEMBER 19, 2005

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, *couriering, 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.

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**

**THIS PAGE LEFT INTENTIONALLY BLANK**

**UK UNCLASSIFIED - U.S. FOR OFFICIAL USE ONLY**

35 of 35