REQUIREMENTS FOR THE SAFEGUARDING AND TREATMENT OF DEFENSE ARTICLES RECEIVED FROM THE UNITED STATES OF AMERICA UNDER THE UNITED KINGDOM / UNITED STATES OF AMERICA DEFENCE TRADE COOPERATION TREATY (DTCT)

DRAFT PROVISIONS FOR DE&S WEBSITE

REQUIREMENTS FOR THE SAFEGUARDING AND TREATMENT OF DEFENSE ARTICLES RECEIVED FROM THE UNITED STATES OF AMERICA UNDER THE UNITED KINGDOM / UNITED STATES OF AMERICA DEFENCE TRADE COOPERATION TREATY (DTCT)

Introduction

1. The Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America have entered into the Defence Trade Cooperation Treaty (DTCT) which was signed in Washington and London on 21 and 26 June 2007 respectively[1]. The DTCT is intended to facilitate the movement of certain categories of equipment and information between pre-approved US and UK government and industry facilities, and their personnel, (known as the "Approved Community") when destined for certain US or UK government end-uses without the requirement for a licence or other written authorisation under the US International Traffic in Arms Regulations (ITAR). A UK export license is still required for UK exports and transfers to the US. The legally binding obligations of the DTCT are supported by an Implementing Arrangement (IA)[2] signed on the 14th February 2008 that identifies the means by which the Parties will implement the arrangements for the Treaty. A List of exempt technologies, that is those which are excluded from Treaty arrangements, is available at http://www.pmddtc.state.gov/treaties/documents/UK_Exempt.pdf

2. The DTCT requires the Parties to provide an appropriate degree of security protection and access control to Defence Articles received from the other Party and provides a comprehensive framework for exports and transfers of Defence Articles whether protectively marked (classified) or not, to the extent that such exports and transfers are in support of:

> (a). United Kingdom and United States combined military or counter terrorism operations as described in the agreed DTCT Implementing Arrangement;
>
> (b). United Kingdom and United States cooperative security and defence research, development, production and support programmes that are identified pursuant to the DTCT Implementing Arrangement;
>
> (c). Mutually agreed specific security and defence projects where Her Majesty's Government is the end-user that are identified pursuant to the DTCT Implementing Arrangement;
>
> (d). United States Government end-use.

[1] http://www.state.gov/t/pm/rls/othr/misc/92770.htm

[2] http://www.pmddtc.state.gov/treaties/documents/UK_Implementing.pdf

A List of eligible operations, programmes and projects will be maintained and will be available at [***].

Security Classifications

3. The equivalent national security classifications appropriate to Defence Articles under the provisions of the DTCT are:

United Kingdom	United States
UK SECRET	SECRET USML//REL USA and GBR Treaty Community
UK CONFIDENTIAL	CONFIDENTIAL USML//REL USA and GBR Treaty Community
UK RESTRICTED	RESTRICTED USML//REL USA and GBR Treaty Community

Definitions

4. For the purposes of implementing the DTCT the following terms are defined:

"Defence Articles" means articles, services, and related technical data, including software, in tangible or intangible form, listed on the United States Munitions List of the International Traffic in Arms Regulations, as modified or amended;

"Export" means the initial movement of Defence Articles from the United States Community to the United Kingdom Community;

"Her Majesty's Government Personnel" means those persons identified below;

"Her Majesty's Government Facilities" means those facilities identified below;

"Re-export" means the movement of previously Exported Defence Articles by a member of the United Kingdom Community from the Approved Community to a location outside the Territory of the United Kingdom.

"Re-transfer" means the movement of previously Exported Defence Articles by a member of the United Kingdom Community from the Approved Community to a location within the Territory of the United Kingdom.

"Territory of the United Kingdom" means England and Wales, Scotland and Northern Ireland; and any territory for whose international relations the United Kingdom is responsible in respect of which Her Majesty's Government gives notice to the United States Government that such territory shall be included within this definition for the purposes of this Treaty. Her Majesty's Government shall consult with, and give notice through diplomatic channels to, the United States Government regarding the inclusion of any such territories.

"Transfer" means the movement of previously Exported Defence Articles within the Approved Community.

"United Kingdom Community" means the community identified below.

United Kingdom Approved Community

5. The United Kingdom Approved Community consists of:

(a) Her Majesty's Government Facilities accredited by Her Majesty's Government identified pursuant to the Implementing Arrangement;

(b) Her Majesty's Government Personnel, meeting mutually agreed criteria, including, at a minimum, appropriate United Kingdom security accreditation and a need-to-know, as set out in the Implementing Arrangement;

(c) Specifically identified non-governmental United Kingdom entities and facilities that meet mutually agreed eligibility requirements, are accredited by Her Majesty's Government in accordance with the Implementing Arrangement, and are mutually agreed to by the Parties for inclusion on the Approved Community List and

(d) Employees of those entities and facilities referred to in sub-paragraph (c) who meet criteria set out in the Implementing Arrangement, including, an appropriate United Kingdom security clearance and a need-to-know.

The United States Approved Community consists of:

(a) Departments and agencies of the United States Government, including their personnel with, as appropriate, security accreditation and a need-to-know; and;

(b) Nongovernmental United States entities registered with the United States Government and eligible to export Defense Articles under United States law and regulation, including their employees with, as appropriate, security accreditation and a need-to-know.

Oversight and Assurance of DTCT Obligations

6. The MOD Defence Equipment & Support – Deputy Head Security & Principal Security Adviser Organisation (MOD DE&S DHSY/PSYA) is responsible for ensuring compliance by the non-governmental entities in the UK Approved Community and for this purpose will undertake compliance visits to provide an assurance that Her Majesty's Government obligations under the DTCT are being complied with. The contact details of MOD DE&S DHSY/PSYA are as follows:

Ministry of Defence, DE&S, Security Advice Centre,
Poplar-1 # 2004,
Abbey Wood, Bristol,
England,

BS34 8JH,

Tel: 030679 34378,
mailto:desinfra-securityadvicecentre@mod.uk

7. The following details the minimum criteria that non-governmental United Kingdom entities and facilities will be assessed against, for inclusion on the UK Approved Community referred to in (c) above:

(a). That the entity or facility must be on Her Majesty's Government's "List X" of approved facilities and that it satisfies the required physical security requirement for the protection of the material concerned.

(b). Foreign ownership, control or influence;

(c). Previous convictions or current indictment for violations of United States or United Kingdom export control laws or regulations as considered by the United States Government;

(d). Previous convictions for violations of United States or United Kingdom export control laws or regulations as considered by Her Majesty's Government;

(e) The United States export licensing history of the entity or facility; and

(f). National security risks, including interactions with countries proscribed by United Kingdom or United States laws or regulations

8. Non-governmental United Kingdom entities may apply to the MOD DE&S DHSY/PSYA for inclusion in the United Kingdom Approved Community using the form at **ANNEX A?** if there is a requirement for the entity to receive Defence Articles under the scope of the DTCT from the United States. Any additional supplementary information must also be supplied in support of the application as deemed necessary by DE&S DHSY/PSYA. US government endorsement, obtained by the MOD, is also required. MOD DE&S DHSY/PSYA will inform the non-governmental United Kingdom entities of the results of their application.

9. List X status does **not** automatically mean that a facility is also in the United Kingdom Approved Community. Therefore List X facilities who are to be in receipt of US Defence Articles **must** use the form at **ANNEX A**? to apply to also be included in the UK Approved Community and also provide any supplementary information deemed necessary by DE&S DHSY/PSYA in support of the application.

10. DE&S DHSY/PSYA will require non-governmental United Kingdom entities applying for inclusion in the United Kingdom Approved Community to acknowledge in writing that they will be bound by the relevant security requirements for the protection of Defence Articles, including, the applicable requirements of the Security Policy Framework. Where

the access is only to RESTRITED USML//REL USA and GBR Treaty Community Defence Articles the requirements of **ANNEX B must** be applied.

11. Non-governmental United Kingdom entities must appoint an employee of suitable grade and standing to act as Security Officer with responsibility for day-to-day management of DTCT security requirements within the Approved Community facility. The Security Officer is responsible as necessary for:

a. liaising within the company, and between the company and the MOD DE&S DHSY/PSYA;

b. processing to, and liaising with, the MOD Defence Vetting Agency applications for Personnel Security Clearances for all company employees requiring access to US Defence Articles;

c. advising company management on the interpretation and implementation of DTCT legislative security controls;

d. being readily available for consultation and giving security advice to the contractor's management and employees;

e. co-ordinating the planning of appropriate security and access controls where DTCT assets are to be handled, stored or produced;

f. arranging for appropriate security education and awareness training, particularly for new, young or inexperienced employees, to ensure that they understand the scale, nature of the threats and protective security controls required for DTCT defence articles;

g. ensuring that any breach of these requirements is immediately reported to the MOD DE&S DHSY/PSYA

Access

12. Access to any United States Defence Articles exported under the Treaty will be granted only to appropriate personnel within an authorised facility in a respective Approved Community who have:

(a) An appropriate security clearance at least at the United Kingdom "Security Check" level; and

(b) A need to know.

13. Security clearance applications for company employees requiring access to USML Defence Articles must be submitted direct to the MOD Defence Business Services – National Security Vetting (DBS-NSV) by the nominated Non-governmental United Kingdom Approved Community entity Security Officer. This will require the Approved Community Security Officer to apply to the DBS-NSV for a CERBERUS sponsor account which will enable the Security Officicer to electronically generate the security clearance

requirement. Annex C provides guidance on how to apply for a CERBERUS sponsor account. The Security Officer, as sponsor, plays a key role in the security clearance process in confirming the requirement for vetting (which is essential under UK law), for confirming the identity of the individual and for checking any other information that may be held on the subject. Following which, the subject of the security clearance to is to complete the security clearance application form and submit it direct to the DBS-NSV.

14. Access to United States USML Defence Articles by persons with the nationality of a country on the United States ITAR 126.1 countries is not permitted without the prior authorisation of the United States Government. MOD DE&S DHSY/PSYA, must be consulted when considering whether to grant an individual, **other** than a serving member of the UK Armed Forces, access to Defence Articles where national security considerations arise, including close ties to countries or entities of concern to either participant. A list of such countries is available at http://www.pmddtc.state.gov/embargoed_countries/index.html

16. Accordingly, United Kingdom Approved Community entities must provide details to MOD DE&S DHSY/PSYA of any nationals from countries included on the list of US embargoed countries and the access required prior to permitting access by such individuals. MOD DE&S DHSY/PSYA will consult with the US authorities and advise the Approved Community entity whether the US have approved the access required.

15. A Baseline Personnel Security Standard (BPSS) is **not** acceptable for access to any United States classified USML Defence Articles.

Protection, Marking and Classification

16. United Kingdom Approved Community recipients of United States classified Defence Articles are required to provide the Defence Articles a degree of protection no less stringent than that provided to United Kingdom assets of equivalent protective marking.

17. Defence Articles at the level of US CONFIDENTIAL USML //REL USA and GBR Treaty Community or US SECRET USML //REL USA and GBR Treaty Community may only be exported to UK non-governmental entities that are in the UK Approved Community and also hold List X status. Such material must be safeguarded in accordance with the protective security measures applicable to UK CONFIDENTIAL or UK SECRET information as required by the Security Policy Framework. UK non-governmental Approved Community entities in receipt of RESTRICTED USML//REL USA and GBR Treaty Community must physically protect the material in accordance with these provisions and the requirements of **Annex B.**

18. All United States Defence Articles Exported or Transferred to entities in the United Kingdom Approved Community will be marked or identified prior to transfer, as follows:

(a) For exports and transfers of Defence Articles classified for purposes other than the Treaty, the standard marking or identification will read [CLASSIFICATION LEVEL] i.e. “CONFIDENTIAL USML/REL USA and GBR Treaty Community”;

(b). For exports and transfers of other Defence Articles i.e. US material which is UNCLASSIFIED, the standard marking or identification will read “RESTRICTED USML/REL USA and GBR Treaty Community”.

19. Where Defence Articles are returned to the United States, any Defence Articles classified as RESTRICTED USML//REL USA and GBR Treaty Community purely for the purposes of the Treaty will revert to an unclassified state and any markings associated with this classification will be removed. Defence Articles with other classifications must continue to be protected in accordance with the United Kingdom national security regulations for the classification of the Defence Article concerned and

(a). Tangible Defence Articles (including hardware, equipment, and software) will be individually labelled or, where such labelling is impracticable, will be accompanied by documentation (such as contracts, invoices, shipping bills, or bills of lading) clearly associating the Defence Articles with the appropriate markings as detailed above;

(b) Technical data (including data packages, technical papers, manuals, presentations, specifications, guides and reports), regardless of media or means of transmission (physical, oral or electronic) will be individually labelled or, where such labelling is impracticable, will be accompanied by documentation (such as contracts, invoices, shipping bills, or bills of lading) or a verbal notification clearly associating the Defence Articles with the appropriate markings as detailed above; and

(c) Other intangible Defence Articles, including defence services, will be accompanied by documentation (such as contracts, invoices, shipping bills, or bills of lading) clearly associating the Defence Articles with the appropriate markings as detailed above.

20. Accordingly, on receipt of Defence Articles exported to entities in the United Kingdom Approved Community, the recipient is to ensure that;

(a) The appropriate standard markings detailed above have been applied. In the event that irregularities are found, Her Majesty's Government will require the recipient to correct the marking and to notify the irregularity and action taken to the DE&S DHSY/PSYA. DE&S DHSY/PSYA will report such notifications to the United States Government in order that corrective action can be taken with the United States exporter.

(b) Defence Articles that are located within the United Kingdom, having been previously exported under a license or other export authorization, will be marked, identified, transmitted, stored, and handled in accordance with the Treaty, by the holding United Kingdom Community entity;

(c) They comply with additional record keeping and handling requirements for Defence Articles, including:

(i) Recording dates of receipt and details of the United States exporter;

(ii) Recording the location, incorporation, Transfer, Re-export, Re-transfer or destruction of the Defence Articles, to enable a full audit trail to be established regarding the handling of the Defence Articles;

(iii) Applying and maintaining appropriate markings or other identification and ensuring that these requirements are passed to any future recipient of the Defence Articles within the Approved Community;

(iv) Establishing and carrying out a self-audit regime to monitor the effectiveness of the application of relevant controls on the Defence Articles; and

(vi) Maintaining such records for a minimum of 5 years and providing such records on request to Her Majesty's Government, which may be provided to the United States Government.

(e) There are access controls appropriate to the level of classification of the Defence Articles and their status under the DTCT, including password protection for electronically held Defence Articles, and that such Defence Articles be contained on information systems that have been accredited in accordance with Her Majesty's Government standards and guidelines appropriate to the classification of the Defence Articles;

(f) Any material violations of the procedures established pursuant to the terms of the DTCT must be reported immediately, and all other violations must be reported as soon as reasonably practicable, to Her Majesty's Government, which will notify the United States Government as appropriate Accordingly any violations must be reported to the relevant Approved Community Departmental Security Officer or, in respect of the non-governmental Approved Community entities to MOD DE&S DHSY/PSYA; and

(g). Defence Articles are not to be Re-transferred or Re-exported without the prior authorization of both the United States Government and Her Majesty's Government, and be in compliance with the process for seeking such authorizations. Members of the United Kingdom Community may seek such authorizations from the United States Department of State,

Directorate of Defence Trade Controls, directly or through the original United States exporter.

Transmission

21. The transmission or transportation of United States classified Defence Articles within the UK must be by methods approved for the classification of the material concerned as detailed in the SPF. The international transportation of classified Defence Articles in the form of equipment to organisations in the United States Approved Community must be only undertaken under a transportation plan approved by the relevant DSO or, in respect of the non-governmental Approved Community entities, MOD DE&S DHSY/PSYA The electronic transmission of United States classified Defence Articles in clear text is not permitted.. Encryption devices approved by the UK or US governments for the transmission of classified information must be used for such transmissions.

Transfers

22. Non-governmental entities in the Approved Community in receipt of Defence Articles exported to it under the DTCT and wishing to transfer such Defence Articles to a UK non-governmental entity not already in the United Kingdom Approved Community **must** sponsor the proposed recipient for Approved Community and, if applicable, List X status. Such transfer cannot occur until DE&S DHSY/PSYA has advised that Approved Community and/or List X status has been granted.

Re-transfers and Re-exports

23. All Re-transfers or Re-exports of Defence Articles will require authorization by Her Majesty's Government. In reviewing a request for authorization, the UK MOD will require supporting evidence that includes United States Government approval of the proposed Re-transfer or Re-export. The existence of UK MOD authorization and US Government approval is also a consideration in reviewing export licence applications that may be required under the export control process of Her Majesty's Government.

24. Her Majesty's Government procedures relating to the Re-transfer or Re-export of Defence Articles originally exported or treated as if they were exported under the Treaty require that:

(a) As part of the UK export control procedures, confirmation that US Government approval has been obtained; and

(b) It is made a condition of relevant open licences that US Government approval must have been obtained.

25. Her Majesty's Government will require a United Kingdom Community member seeking to Re-transfer or Re-export to first approach the United States Department of State, Directorate of Defence Trade Controls, directly or through the original exporter, to obtain United States Government approval.

26. For Re-transfers, in view of paragraph 23 above, the approval to Re-transfer Defence Articles received under the DTCT to United Kingdom non Approved Community

entities shall only be considered by Her Majesty's Government in exceptional circumstances. In such cases the F680 procedure must be followed and supported with detailed evidence identifying the full circumstances when seeking permission for the Re-transfer of Defence Articles.

27. For Re-exports of Defence Articles received under the Treaty which are classified RESTRICTED USML//REL USA and GBR Treaty Community or above the F680 procedure must be followed as well as any procedures that may be required under the export control process of Her Majesty's Government. Her Majesty's Government's audit procedures will check that relevant open licence conditions have been met, including checks to ensure F680 clearance has been obtained as required.

28. In the event of authorization from Her Majesty's Government, the proposed Re-transfer or Re-export may take place. The Defence Articles thereafter will be considered to fall outside of the Scope of the Treaty and will be governed by the applicable terms of any licence or authorization granted by the United States Government and, as appropriate, Her Majesty's Government, in place of the terms of the Treaty.

29. In the event that an entity seeking Her Majesty's Government approval for Re-transfer or Re-export is unable to demonstrate to the UK MOD that it has obtained prior United States Government approval, the UK MOD will not give authorization for the proposed release of classified material, and therefore, will not give authorization for the proposed Re-transfer or Re-export.

30. Re-transfer or Re-export of Defence Articles without the approval of the UK MOD will be considered by the DTCT Parties to be a breach of the procedures established pursuant to the terms of the Treaty.

31. Where Defence Articles are Re-transferred or Re-exported, markings and classifications arising solely from the DTCT will be withdrawn.

32. Further to paragraph (X), the following exceptions to the Re-transfer and Re-export authorization provisions of the DTCT apply:

(a) Re-exports of Defence Articles from non-governmental entities of the United Kingdom Approved Community to United Kingdom Armed Forces deployed outside the Territory of the United Kingdom conducting operations, including training, as mutually determined and listed pursuant to Sections 2(1) and 2(3) of the Implementing Arrangement, via United Kingdom Armed Forces transmission channels, or other transmission channels approved by the DTCT Parties; and

(b) Re-exports of Defence Articles from non-governmental entities of the United Kingdom Approved Community to Approved Community members operating in direct support of United Kingdom Armed Forces deployed outside the Territory of the United Kingdom conducting operations, including training, as mutually determined and listed pursuant to Sections 2(1) and 2(3) of the Implementing Arrangement, via United Kingdom Armed Forces transmission channels, or other

transmission channels approved by the by the DTCT Parties.

Compliance

33. United Kingdom Approved Community members must maintain records with respect to all Defence Articles Exported, Transferred, Re-transferred, or Re-exported for a period of at least 5 years, including records regarding intangible items or technical data.

34. United Kingdom Approved Community non-governmental members must, within five days of the event, provide written notification to MOD DE&S DH Sy/PSyA of a material change within, or to the company, including a change in the senior officers; the establishment, acquisition or divestment of a subsidiary or foreign affiliate; a merger; a take-over; or a change of location. United Kingdom Approved Community non-governmental members must provide MOD DE&S DHSY/PSYA with written notification at least 60 days, or as soon as reasonably practicable, in advance of any intended sale or transfer to a foreign person or entity of ownership or control of the United Kingdom Approved Community non-governmental member;

35. Any material violations of the procedures established pursuant to the terms of the DTCT must be reported immediately, and all other violations must be reported as soon as reasonably practicable, to MOD DE&S DHSY/PSYA who will notify the United States Government as appropriate;

36. United Kingdom Approved Community non-governmental members members must inform their employees and personnel who may be handling Defence Articles of the above requirements.

37. In the case of removal from the United Kingdom Approved Community, the non-governmental entity will continue to abide by the undertakings it assumed as part of the United Kingdom Approved Community until such time as other appropriate United States Government licenses or arrangements are in place.

Compliance Inspections

38. No objection will be made by the United Kingdom Approved Community non-governmental entity to any reasonable request by MOD DE&S DHSY/PSYA to undertake an investigation, review records, or inspect any premises where Defence Articles are stored, handled or processed.

ANNEX A

APPLICATION FOR A NON-GOVERNMENTAL UNITED KINGDOM ENTITY TO JOIN THE DTCT APPROVED COMMUNITY

NAME & ADDRESS OF FACILITY TO BE CONSIDERED	NAME & ADDRESS OF HEAD OFFICE (IF DIFFERENT)
Post Code:	Post Code:

Tel N^{o}
Fax N^{o}

Tel N^{o}
Fax N^{o}
VAT Reg N^{o}
Company Reg N^{os}

DETAILS OF INDIVIDUAL ACTING AS OR NOMINATED TO BE FACILITY SECURITY CONTROLLER	DETAILS OF INDIVIDUAL ACTING AS OR NOMINATED TO BE COMPANY BOARD LEVEL CONTACT
Name:	Name:
DoB:	DoB:
Place of Birth:	Place of Birth:
Country of Birth:	Country of Birth:
Nationality/ties:	Nationality/ties:
Work Address:	Work Address:
Post Code:	Post Code:
Fax N^{o}	Fax N^{o}
e-Mail	e-Mail

In accordance with the Data Protection Act 1998, the Ministry of Defence will collect, use, protect and retain the information on this form in connection with all matters relating to our personnel administration and policies.

IF YOUR COMPANY HAS BEEN INCORPORATED, PLEASE GIVE DETAILS OF ALL ASSOCIATED COMPANIES, SUBSIDIARIES, PARENT OR HOLDING COMPANIES, INCLUDING FULL NAME AND ADDRESS AND COUNTRY IN WHICH THE COMPANY/IES ARE REGISTERED

Post Code:	Post Code:

Post Code:	Post Code:

Post Code:	Post Code:

DATE OF FORMATION OF THE COMPANY, OR THE INCORPORATION AND A BRIEF HISTORY.

DIRECTORS INFORMATION

PLEASE PROVIDE DETAILS OF CHAIRMAN, DEPUTY CHAIRMAN, ALL DIRECTORS (INDICATING SPECIFICALLY THOSE WHO HOLD EXECUTIVE APPOINTMENTS) AND COMPANY SECRETARY. SIMILAR INFORMATION SHOULD BE PROVIDED FOR INDIVIDUALS HOLDING MORE THAN ONE FIFTH OF PAID UP SHARES, PREFERENCE SHARES, OR LOAN CAPITAL.

	Chairman	**Deputy Chairman**	**Director**	**Director**
Surname Now				
Surname at Birth if different				
All other surnames used				
Full Forenames				
Place of Birth				
County/State				
Country				
Date of Birth				
Current Nationality				
Previous Nationalities				
Dual National Y/N				
State Dual Nationality				
If Naturalised, Number and Date of Certificate				
Full Permanent Address Post Code:				
Since (Date)				
Position in Company				
Signature*****				

***A SIGNATURE CONFIRMS AGREEMENT TO BACKGROUND CHECKS BEING MADE ON THE BOARD MEMBERS WITH OTHER GOVERNMENT AGENCIES**

PLEASE CONTINUE OVERLEAF AND ON CONTINUATION SHEETS AS NECESSARY

DIRECTORS CONTINUATION SHEET

	Chairman	Deputy Chairman	Director	Director
Surname Now				
Surname at Birth if different				
All other surnames used				
Full Forenames				
Place of Birth				
County/State				
Country				
Date of Birth				
Current Nationality				
Previous Nationalities				
Dual National Y/N				
State Dual Nationality				
If Naturalised, Number and Date of Certificate				
Full Permanent Address Post Code:				
Since (Date)				
Position in Company				
Signature*				

***A SIGNATURE CONFIRMS AGREEMENT TO BACKGROUND CHECKS BEING MADE ON THE BOARD MEMBERS WITH APPROPRIATE OTHER GOVERNMENT AGENCIES.**

PLEASE CONTINUE OVERLEAF AND ON CONTINUATION SHEETS AS NECESSARY

INFORMATION ON VIOLATIONS OF UNITED STATES EXPORT CONTROL LAWS OR REGULATIONS AS CONSIDERED BY THE UNITED STATES GOVERNMENT

In accordance with the criteria set out in the Cabinet Office Security Policy Framework and to inform the assessment of the suitability of the above named facility to become a member of the Defence Trade Co-operation Treaty Approved Community. Previous convictions or current indictments for violations of United Kingdom or United States export control laws or regulations as considered by the Unites States Government are to be listed below.

Law/Regulation	Date of Indictment	Details of Violation	Date of Conviction	Penalty

If necessary please continue on a separate sheet.

INFORMATION ON VIOLATIONS OF UNITED KINGDOM EXPORT CONTROL LAWS OR REGULATIONS AS CONSIDERED BY HER MAJESTY'S GOVERNMENT

In accordance with the criteria set out in the Cabinet Office Security Policy Framework and to inform the assessment of the suitability of the above named facility to become a member of the Defence Trade Co-operation Treaty Approved Community. Previous convictions or current indictments for violations of United Kingdom or United States export control laws or regulations as considered by Her Majesty's Government are to be listed below.

Law/Regulation	Date of Indictment	Details of Violation	Date of Conviction	Penalty

If necessary please continue on a separate sheet.

Do you have a current contract with the US Government or a US Company? If yes please give details below, including details of the Contracting Authority.

Do you have facilities cleared to List X standards, if yes, list them below

PLEASE PROVIDE FULL REASONS FOR APPLYING TO JOIN THE APPROVED COMMUNITY INCLUDING THE DETAILS OF AN UK OR US DEFENCE CONTRACT/S CURRENTLY BEING UNDERTAKEN BY THE COMPANY.

DECLARATION

I confirm that the information provided on this form is, to the best of my knowledge, complete and accurate.

I confirm that, as a duly authorised officer of the company, I agree on behalf of the company to background checks being completed on the company and the identified Directors.

By signing and submitting this application to join the Approved Community, I confirm that the Company is aware of the terms and conditions attached to Approved Community status and fully accept them.

PRINT NAME …… **SIGNATURE ……..**

POSITION IN COMPANY ……

DATE ……..

The Ministry of Defence is committed to ensuring that all your personal data including that of a sensitive nature is used with your consent, respect for your privacy and only for the limited, clearly stated purposes within the form/or as stated below. This also accords with our legal obligations under the Data Protection Act 1998.

The information of a sensitive nature contained in this form will be used by the Ministry of Defence, Defence Equipment & Support – Deputy Head Security & Principal Security Adviser Organisation (MOD DE&S DHSY/PSYA) to consider the suitability of the company to be included in the "Approved Community" as a non-governmental United Kingdom entity under the provisions of the United Kingdom/United States Defence Trade Cooperation Treaty (DTCT).

The information contained within this form may be required to be passed to the United States government authorities involved in the DTCT Approved Community approval process.

By signing this form you are confirming that you understand the above and that you agree that the personal data of a sensitive nature contained in this form can be used as stated.

ANNEX B

Security Requirements for the Protection of Restricted USML Defence Articles United Kingdom Members of the DTCT Non-Governmental Approved Community

1. Defence Articles transferred to non-governmental UK Approved Community will be marked “RESTRICTED USML//REL USA and GBR Treaty Community”.

Official Secrets Acts

2. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to make sure that all individuals employed on any work involving access to RESTRICTED USML//REL USA and GBR Treaty Community Defence Articles have notice that these statutory provisions apply to them and shall continue so to apply after the need for such access.

Protection of RESTRICTED USML Information

3. RESTRICTED USML//REL USA and GBR Treaty Community Defence Articles shall be protected in a manner to promote discretion in order to avoid unauthorised access. The Contractor shall take every effort to prevent the loss or compromise of the information or deliberate or opportunist attack.

4. Disclosure of RESTRICTED USML//REL USA and GBR Treaty Community Defence Articles shall be strictly in accordance with the "need to know" principle. Except with the written consent of the UK and, if applicable, the US Governments the Contractor shall not disclose the Defence Articles to any person other than a person directly employed by the Contractor.

5. When not in use RESTRICTED USML//REL USA and GBR Treaty Community Defence Articles shall be stored under lock and key.

Access

6. Access to RESTRICTED USML//REL USA and GBR Treaty Community Defence Articles shall be confined to those individuals who have been granted an appropriate security clearance (at least a Security Check) by the MOD Defence Business Services – National Security Vetting (DBS-NSV) , have a “need-to-know”, and whose access is essential for the purpose of his or her duties.

7. The Contractor shall ensure that all individuals having access to RESTRICTED USML//REL USA and GBR Treaty Community information meet legal requirements in respect of immigration and the right to work in the UK and have undergone basic recruitment checks. Accordingly, prior to submission of security clearance applications to the (DBS-NSV) contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) (excluding the Criminal record check with) Further details and the full requirements of the BPSS can be found at the Cabinet Office website at :

http://www.cabinetoffice.gov.uk/sites/default/files/resources/baseline-personnel-security-standard.pdf

Transmission of RESTRICTED USML//REL USA and GBR Treaty Community **Information**

8. RESTRICTED USML//REL USA and GBR Treaty Community Defence Articles shall be transmitted, both within and outside company premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post in a single envelope. The words RESTRICTED USML//REL USA and GBR Treaty Community Defence Articles must **NOT** appear on the envelope. The envelope should bear a company stamp that clearly indicates the full address of the office from which it was sent. Approved Commercial Couriers may be used.

9. Advice on the transmission of RESTRICTED USML//REL USA and GBR Treaty Community Defence Articles abroad or any other general advice including the transmission of RESTRICTED USML//REL USA and GBR Treaty Community Defence Articles hardware shall be sought from MOD DE&S DHSY/PSYA.

Use of Communications and IT Systems

10. The following describes the minimum Accreditation security requirements for processing and accessing RESTRICTED USML//REL USA and GBR Treaty Community information on stand alone or facility Local Area Network IT systems.

a. Access Physical access to all hardware elements of the IT system is to be strictly controlled.

b. Identification and Authentication (ID&A). All systems shall have the following functionality:

(1) Up-to-date lists of authorised users.

(2) Positive identification of all users at the start of each processing session.

c. Passwords. Passwords are part of most ID&A, Security Measures. Passwords shall be minimum of 6 characters long (9 is preferred) and shall include numeric and “special” characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control. All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission. RESTRICTED USML//REL USA and GBR Treaty Community information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using encryption devices accepted by the UK Government Advice on encryption requirements for the transmission of RESTRICTED USML//REL USA and GBR Treaty Community information shall be sought from MOD DE&S DHSY/PSYA.

f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

(1) The following events shall always be recorded:

(a) All log on attempts whether successful or failed.

(b) Log off (including time out where applicable).

(c) The creation, deletion or alteration of access rights and privileges.

(d) The creation, deletion or alteration of passwords.

(2) For each of the events listed above, the following information is to be recorded:

(a) Type of event,

(b) User ID,

(c) Date & Time

(d) Device ID

The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know.

If the operating system is unable to provide this then the equipment shall be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

g. Integrity & Availability. The following supporting measures shall be implemented:

(1) Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)

(2) Defined Business Contingency Plan

(3) Data backup with local storage

(4) Anti Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software).

h. Logon Banners Wherever possible, a "Logon Banner" shall be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring.

(1) A suggested format for the text depending on national legal requirements could be:

(a) "Unauthorised access to this computer system may constitute a criminal offence"

i. Unattended Terminals. Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. Internet Connections. Computer systems shall not be connected direct to the Internet unless protected by a firewall (a software based personal firewall is the minimum) which is acceptable to the Authority's Principal Security Advisor.

k. Disposal Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

11. Where RESTRICTED USML//REL USA and GBR Treaty Community information is to be processed on IT systems that are connected to other systems that are off of the contractors facility the IT systems concerned will require formal Accreditation by MOD Accreditors. In such circumstances advice on this must be obtained from MOD DE&S DHSY/PSYA prior to processing the RESTRICTED USML//REL USA and GBR Treaty Community information on the IT systems.

Laptops

12. Laptops holding any RESTRICTED USML//REL USA and GBR Treaty Community information are to have, as a minimum, a FIPS 140-2 approved full disk encryption solution installed.

13. Unencrypted laptops not on a secure site[3] are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt the term "drives" includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.

14. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

15. Portable CIS devices are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

Loss and/or Incident Reporting

16. Any loss of or security incident involving RESTRICTED USML//REL USA and GBR Treaty Community information, processed or generated information shall be immediately reported to the MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC), This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to MOD DE&S DHSY/PSYA and the MOD Chief Information Officer (CIO). The MOD WARP or DE&S DHSY/PSYA, as appropriate, will also advise the contractor what further action is required to be undertaken.

JSyCC WARP Contact Details

Email: CIO-DSAS-JSyCCOperations@mod.uk (UNCLASSIFIED)

Telephone: Working Hours: 030 6770 2187

Out of Hours/Duty Officer Phone: 07768 558863

[3] Secure Sites are defined as either Government premises or a secured office on the contractor premises

Fax: 01225 846904

Mail: Joint Security Co-ordination Centre (JSyCC), GOSCC, Building 405, MOD

Corsham, Westwells Rd, Wiltshire SN13 9NR.

Destruction

17. As soon as no longer required RESTRICTED USML//REL USA and GBR Treaty Community information/material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Unwanted RESTRICTED USML//REL USA and GBR Treaty Community information/material which cannot be destroyed in such a way shall be returned to the US Supplier.

Interpretation/Guidance

19. Advice regarding the interpretation of the above requirements should be sought from MOD DE&S DHSY/PSYA.

Further requirements, advice and guidance for the protection of RESTRICTED USML//REL USA and GBR Treaty Community should be sought from MOD DE&S DHSY/PSYA.

Audit

19. Where considered necessary by MOD DE&S DHSY/PSYA the Contractor shall permit the inspection of the Contractors processes and facilities to ensure compliance with these requirements.

ANNEX C

CERBERUS SPONSOR ACCOUNT APPLICATION

To enable Security Officers in Non-governmental entities in the Approved Community to request a Personnel Security Clearance (PSC) for company employees requiring access to DTCT defence articles the Security Officer **must** apply to the MOD Defence Business Services – National Security Vetting (DBS-NSV) to open a CERBERUS sponsor account. The sponsor plays a key role in confirming the requirement for PSCs for access to DTCT defence articles, for confirming the identity of the individual, and for checking any other information that may be held on him/her.

To apply for a sponsor account, the Security Officer of the Approved Community company must use the attached form (Appendix A), accompanied by a copy of the letter from DE&S DHSY/PSYA which confirmed Approved Community status. Guidance on completing the CERBERUS account application form is attached at Appendix B. When completing the form the Security Officer should request an Internet Portal Account only and disregard references to Departmental Security Authorities, which are relevant only to MOD organisations. The form, together with the DE&S DHSY/PSYA letter, should then be forwarded to the DVA either by e-mail (a scanned copy of the DE&S DHSY/PSYA letter will be acceptable) to **DVA–CS-CSMT@MOD.UK** or in hard copy to Customer Accounts Team, Room GV11, DBS-NSV, Imphal Barracks, York YO10 4AS.

Within approx 48 hours sponsors will receive an e-mail informing them how to verify and action their account; the email will also include their unique sponsor ID, which must be used on all applications and in any other dealings with the DBS-NSV.

To submit an application sponsors should access their account and initiate a clearance request. Full instructions are at:

http://www.mod.uk/NR/rdonlyres/B840A6DE-4B50-412C-A1BE-54AF6D62EF2B/0/E_Form_Portal.pdf

Alternatively if internet facilities are not available to both sponsor and vetting subject, or if preferred, sponsors can download the relevant form from the (DBS-NSV website and forward the completed hard copy to the DBS-NSV. Electronic submission will however in all cases result in a speedier service.

To access and complete hard copy forms go to:

http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/DVA/

Under the heading Related pages find Defence Business Services Publications and then under security Questionnaires find Form NSV 001 for SC. For SC the vetting subject completes Section 3 on page 1 through to and including page 29. The sponsor completes section 2 and pages 27-29. On page 2 the post should be designated non-reserved. Sponsors will be able to use their portal to monitor progress on each application.

DBS-NSV PSC action normally takes approximately 4 weeks. When completed, the DVA will provide the Approved Community Security contractor Security Officer with the PSC certificate for their employees. The PSC will be valid for 3 years. If the employee continues to require access to DTCT defence articles the company Security Officer must undertake the same process to re-validate the PSC prior to the date of its expiry.

After clearance has been given, the sponsor is responsible for actively managing the individual and for reporting any matters of potential security concern to the DBS-NSV. Failure to do so may lead to CERBERUS sponsorship status being removed

ANNEX C - APPENDIX A

MINISTRY OF DEFENCE

Helpdesk Opening Times
Mon – Thurs 0800 - 1700
Fri 0800 - 1500
Telephone: 01904-662644
Fax: 01904-662765
Email: dva-cs-csmt-gm@mod.uk

CERBERUS SPONSOR ACCOUNT – APPLICATION FORM

Surname		**Role Within Organisation**	
Forename(s)		**Require Internet Portal Account**	
Date Of Birth		**If Yes Insert E-Mail Address**	
Place Of Birth		**Require Restricted Portal Account**	
Country Of Birth		**If Yes Insert E-Mail Address**	
Department		**Require Sponsor Account**	
Organisation Name			
Phone Number Incl Area Code			
Full Address and Postcode			

For guidance on how to complete this form please see the guidance notes for Cerberus sponsor accounts.

Guidance notes to assist you in completing this form are available on the DVA Internet site.

Defence Vetting Agency
www.mod.uk/dva

Guidance Notes For Completion Of The Cerberus Sponsor Account Application Form.

This document gives an explanation of the terminology used for Cerberus sponsor account access and permissions.

e-Form Portals

There are two e-Form portals available for sponsoring National Security Vetting (NSV) applications. They provide the means to submit and monitor NSV applications electronically through Cerberus CMS.

Restricted Portal: This portal is accessed via the Restricted Land Interconnect (RLI) or Government Secure Internet (GSI). Some OGD customers will access the restricted network using other approved tools such as CJX, PNN and GSX etc. Sponsors must register for an account to access this portal, the sponsor and subjects must both have access to a restricted network to use this account. In addition, the restricted portal will allow sponsors to submit Vetting Status Information (VSI) enquires.

Un-restricted (Internet) portal: This portal can be accessed via the internet. Sponsors must register for an account to access this portal. The information saved on the internet portal is protected by secure encryption to Impact Level 3(IL3).

Sponsors: To act as a sponsor for NSV applications on Cerberus, sponsors must first register for a portal account(s) with the DBS-NSV and be allocated a unique sponsor ID.

- The unique sponsor ID will need to be entered on all electronic and hard copy applications.

- When contacting the DBS-NSV Helpdesk, the call advisor will request the sponsor ID from the caller. This will be used to verify the caller.

Sponsor Account Application form: This is at Appendix B. All boxes detailing personal and organisation information on the registration form must be completed in full to enable the sponsor account to be created.

<u>Access to e-Form portals</u>

- If you have access to a secure network i.e. the RLI or GSI, you can apply for a restricted portal account. This means that all information submitted via this

portal is done so across a restricted network. For the restricted (RLI/GSI) portal please provide your role email address.

Example: DVA-CS-example-email@MOD.UK if you do not have a role email but have another restricted email address you may use this.

- If you do not have access to a secure network, you should apply for an unrestricted internet portal account. **For the unrestricted internet portal, please provide your unclassified work email address, which may be your company email address.**

- If you have access to the restricted and unrestricted networks you can apply for access to both e-Form portals.

- Sponsors of staff/contractors who have access to the restricted and un-restricted networks can use either of the e-Form portals to register a subject for NSV; however an application must be started and completed on the same portal.

- For sponsors of staff/contractors who do not have access to the RLI/GSI you should use the un-restricted internet portal to register the subject.

ALL PERSONAL INFORMATION IS PROTECTED AT IMPACT LEVEL 5 (UP TO SECRET)

Department/Organisation

- For Approved Community companies the department would be MOD and organisation would be the company name. When typing in full address please ensure you include the full details of the site.

Sponsor Account.

Sponsor access through the restricted (RLI\GSI) and unrestricted (Internet) portals allows registered users to sponsor vetting applications and to view Application Status Information (ASI) on both the internet and restricted portals for all cases they have initiated only. Sponsors using the restricted portal will also have access to the Vetting Status Information (VSI) facility but not those using the Internet portal.

Account Authorisation.

All account requests must be submitted with a copy of the Approved Community status letter provided to the company by DE&S DHSY/PSYA.

If you have any further queries that are not answered by this guidance, please email them to: DVA-CS-CSMT-GM@mod.uk.