Cabinet Office

United Kingdom / United States of America Defense Trade Cooperation Treaty

Version 1.1 – July 2014

Version History

Document Version	Date Published	Summary Of Changes
1.0	April 2014	First version published on GOV.UK
1.1	July 2014	‘Version History’ addedNo other changes made.

Introduction

1. The Government of the United Kingdom of Great Britain and Northern Ireland (UK) and the Government of the United States of America (U.S.) entered into the Defense Trade Cooperation Treaty (DTCT) which was signed in Washington DC and London on 21 and 26 June 2007 respectively. The Treaty is intended to facilitate the movement of certain categories of equipment and information between pre-approved U.S. and UK government and industry facilities, and their personnel, (known as the "Approved Community") when destined for certain U.S. or UK government end-uses without the requirement for a licence or other written authorisation under the U.S. International Traffic in Arms Regulations (ITAR). A UK export license is required for UK exports/transfers to the U.S. The legally binding obligations of the DTCT are supported by an Implementing Arrangement (IA) signed on 14 February 2008 that identifies the means by which the Parties will implement the arrangements for the Treaty. Copies of the DTCT, the IA and a list of exempted U.S. Defense Articles that are excluded from DTCT arrangements, are available on the US Department of State website[1]

2. The DTCT requires the Parties to provide an appropriate degree of security protection and access control to Defense Articles received from the other Party. As U.S. origin items exported to the UK under the DTCT arrangements will not be covered by U.S. export license controls, such items will, when in the UK, be protected under Her Majesty's Government (HMG) security regulations and fall under the scope of the Official Secrets Act. All U.S. material will therefore be marked at least "RESTRICTED USML//REL USA and GBR Treaty Community" regardless of its original marking. The Treaty provides a comprehensive framework for exports and transfers" of Defense Articles whether classified (i.e. protectively marked) or not, to Government and non-governmental facilities in the "Approved Community", when such exports and transfers are in support of pre approved:

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

Security Classifications

3. The equivalent national security classification markings appropriate to Defense Articles under the provisions of the DTCT are detailed below. The original U.S. marking applied to Defense Articles by the US exporter applies and such material must not be re-marked by the UK recipient with the equivalent UK classification:

[1] www.pmddtc.state.gov/treaties/index.html

United Kingdom	United States
UK SECRET	SECRET USML//REL USA and GBR Treaty Community
See Note [2]	CONFIDENTIAL USML//REL USA and GBR Treaty Community
UK OFFICIAL-SENSITIVE	RESTRICTED USML//REL USA and GBR Treaty Community

Definitions

"Defense 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 Defense Articles from the United States Community to the United Kingdom Community;

"HMG Personnel" means those persons identified in Section 4 below;

"HMG Facilities" means those facilities identified in Section 4 below;

"Re-export" means the movement of previously Exported Defense 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 Defense 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 HMG gives notice to the United States Government that such territory shall be included within this definition for the purposes of the Treaty. HMG 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 Defense Articles within the Approved Community.

"Approved Community" means the U.S. Community and UK Community;

"United Kingdom Community" means the community identified below.

[2] US Defense Articles marked CONFIDENTIAL USML//REL USA and GBR Treaty Community are to be handled as UK SECRET

4. The United Kingdom Approved Community consists of:

a. HMG Facilities accredited by HMG identified pursuant to the IA;
b. HMG Personnel, meeting mutually agreed criteria, including, at a minimum, the appropriate United Kingdom security clearance and a need-to-know, as set out in the IA;
c. Specifically identified non-governmental United Kingdom entities and facilities that meet mutually agreed eligibility requirements, are accredited by HMG in accordance with the IA, 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 I who meet criteria set out in the IA, including, an appropriate United Kingdom security clearance and a need-to-know.

5. 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. Within Departments and Agencies in the United Kingdom Approved Community the respective Departmental Security Officer (DSO) is responsible for fulfilling the requirements of the DTCT and the provisions in the SPF. Governmental facilities will be accredited and the security requirements overseen by the HMG Department or Agency concerned (i.e. the respective DSO or representatives on their behalf) pursuant to the U.S.-UK General Security Agreement and be related to the scope of the DTCT and be maintained in a list.

7. The MOD Defence Equipment & Support – Deputy Head Security & Principal Security Adviser Organisation (MOD DE&S DHSY/PSYA) is responsible for the approval of, and ensuring compliance by, the non-governmental entities in the UK Approved Community and for this purpose will undertake compliance visits to provide an assurance of compliance with HMG obligations under the DTCT are being complied with.

8. The following details the minimum criteria that non-governmental United Kingdom entities and facilities will be assessed against, for inclusion in the UK Approved Community referred to in paragraph 4 above:

a. That the entity or facility must have met the due diligence investigative standards for inclusion on HMG “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 (FOCI);
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 HMG;
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.

9. Non-governmental United Kingdom entities may apply to the MOD DE&S DHSY/PSYA for inclusion in the United Kingdom Approved Community if there is a requirement for the entity to receive Defense Articles under the scope of the DTCT from the United States. U.S. government endorsement, obtained via the MOD, is also required. MOD DE&S DHSY/PSYA will inform the non-governmental United Kingdom entities of the results of their application.

10. The fact that a facility is holding List X status does not mean that the facility is also automatically in the UK Approved Community. Therefore, all facilities who wish to be in receipt of U.S. Defense Articles under the DTCT must apply for DTCT United Kingdom Approved Community status using the form at Appendix 1. In addition the facility must provide any supplementary information deemed necessary by DE&S DHSY/PSYA in support of the application. An electronic version of Appendix 1 can be found attached to Industry Security Notice 2012/01 on the Gov.uk website[3].

11. 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 Defense Articles, including, the applicable requirements of the Security Policy Framework (SPF).

Access

12. Access to any United States Defense Articles exported under the Treaty will be granted only to serving members of HMG Armed Forces and 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.

[3] https://www.gov.uk/government/publications/industry-security-notices-isns

13. A Baseline Personnel Security Standard (BPSS) on its own is not acceptable for access to any United States classified Defense Articles transferred under the auspices of the DTCT.

Access Limitations

14. Access to United States Defense Articles by persons with the nationality (or dual nationality) of a country on the United States ITAR 126.1 countries is not permitted without the prior authorisation of the United States Government.

15. The relevant DSO or, in respect of non-governmental United Kingdom Approved Community entities 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 Defense Articles where national security considerations arise, including close ties to countries or entities of concern to either DTCT Party. For the U.S. a list of such countries is available on the Department of State – Directorate of Defense Trade Controls website[4].

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

Protection, Marking and Classification

17. For the purposes of the DTCT, all U.S. sourced equipment and information will be treated to at least the level of UK OFFICIAL-SENSITIVE when in the UK and will be protected as additionally required by the SPF, and fall under scope of the Official Secrets Act. United Kingdom Approved Community recipients of United States classified Defense Articles are required to provide the Defense Articles a degree of protection no less stringent than that provided to United Kingdom assets of equivalent protective marking. Such material must be safeguarded in accordance with the protective security measures applicable to UK OFFICIAL-SENSITIVE or UK SECRET information as required by the SPF. UK non-governmental Approved Community entities in receipt of USML RESTRICTED must physically protect the material in accordance with the requirements of these provisions, as applicable, and no less stringently than the provisions contained at Appendix 2.

18. UK non-governmental Approved Community entities processing U.S. Defense Articles on Computer Information Systems (CIS) must ensure that such systems are accredited to the standard required by the SPF for the equivalent level of material concerned.

[4] http://www.pmddtc.state.gov/embargoed_countries/index.html

19. All United States Defense 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 Defense 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 Defense Articles i.e. U.S. material which is UNCLASSIFIED, the standard marking or identification will read “RESTRICTED USML/REL USA and GBR Treaty Community”.

20. Where Defense Articles are returned to the United States, any Defense Articles classified as RESTRICTED USML/REL USA and GBR Treaty Community purely for the purposes of the Treaty will revert to an U.S. Unclassified state and any markings associated with this classification will be removed by the U.S. recipient. Defense Articles with other classifications remaining in the possession of the UK Approved Community facility must continue to be protected in accordance with the SPF for the classification of the Defense Article concerned and in addition:

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

21. Accordingly, on receipt of Defense Articles exported to entities in the UK 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, HMG 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. Defense Articles that are located within the United Kingdom, having been previously exported under a license or other export authorization, that are subsequently transitioned to the Treaty arrangements, will be marked, identified, transmitted, stored, and handled in accordance with the Treaty, by the holding United Kingdom Approved Community entity;
c. They comply with additional record keeping and handling requirements for Defense Articles, including:

    a. Recording dates of receipt and details of the United States exporter;
        i. Recording the location, incorporation, Transfer, Re-export, Re-transfer or destruction of the Defense Articles, to enable a full audit trail to be established regarding the handling of the Defense Articles;
        ii. Applying and maintaining appropriate markings or other identification and ensuring that these requirements are passed to any future recipient of the Defense Articles within the Approved Community;
        iii. Establishing and carrying out a self-audit regime to monitor the effectiveness of the application of relevant controls on the Defense Articles; and
        iv. Maintaining such records for a minimum of 5 years and providing such records on request to HMG, which may be provided to the United States Government.

d. There are access controls appropriate to the level of classification of the Defense Articles and their status under the DTCT, including password protection for electronically held Defense Articles, and that such Defense Articles be contained on information systems that have been accredited in accordance with HMG standards and guidelines appropriate to the classification of the Defense Articles;
e. 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 HMG, 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
f. Defense Articles are not to be Re-transferred or Re-exported without the prior authorization of both the United States Government and HMG, and be in compliance with the process for seeking such authorizations. Members of the United Kingdom Approved Community may seek such authorizations from the United States Department of State, Directorate of Defense Trade Controls, directly or through the original United States exporter.

Transmission

22. The transmission or transportation of United States classified Defense 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 Defense 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 Defense Articles in clear text is not permitted. Encryption devices approved by the UK or U.S. governments for the transmission of classified information must be used for such transmissions.

Transfers

23. Non-governmental entities in the Approved Community in receipt of Defense Articles exported to it under the DTCT and wishing to transfer such Defense Articles to a UK non-governmental entity not already in the Approved Community as part of an existing contract or new contract must sponsor the proposed recipient for Approved Community status. Such transfer cannot occur under the DTCT arrangements until DE&S DHSY/PSYA has advised that Approved Community status has been granted.

Re-transfers and Re-exports

24. All Re-transfers or Re-exports of Defense Articles will require authorization by HMG. 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 U.S. Government approval is also a consideration in reviewing export licence applications that may be required under the export control process of HMG.

25. HMG procedures relating to the Re-transfer or Re-export of Defense 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 U.S. Government approval has been obtained; and
b. It is made a condition of relevant open licences that U.S. Government approval must have been obtained.

26. HMG will require a United Kingdom Approved Community member seeking to Re-transfer or Re-export to first approach the United States Department of State, Directorate of Defense Trade Controls, directly or through the original exporter, to obtain United States Government approval before seeking approval from HMG.

27. For Re-transfers, in view of the above paragraphs, the approval to Re-transfer Defense Articles received under the DTCT to United Kingdom non Approved Community entities shall only be considered by HMG 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 Defense Articles.

28. For Re-exports, of Defense 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 HMG. HMG audit procedures will check that relevant licence conditions have been met, including checks to ensure F680 clearance has been obtained as required.

29. In the event of authorization from HMG, the proposed Re-transfer or Re-export may take place. The Defense 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, HMG, in place of the terms of the Treaty.

30. In the event that an entity seeking HMG 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.

31. Re-transfer or Re-export of Defense 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 DTCT.

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

33. Further to the above paragraphs, the following exceptions to the Re-transfer and Re-export authorization provisions of the DTCT apply:

a. Exports or Transfers of Defense Articles from non-governmental entities of the United States 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 IA, via United Kingdom Armed Forces transmission channels, or other transmission channels approved by the DTCT Parties; and
b. Exports or Transfers of Defense Articles from non-governmental entities of the United States 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 IA, via United Kingdom Armed Forces transmission channels, or other transmission channels approved by the by the DTCT Parties.

34. Where a contractor employee from a non Approved Community facility works at either an HMG or a non governmental Approved Community facility as a regular employee and the contracting company that has seconded the individual has no role in the work that the individual performs (other than providing that individual for that work) and the contracting company would not have access to any DTCT Defense Articles, then the contracting company does not need to be a member of the non governmental Approved Community. The contract employee would, for purposes of the DTCT, be treated as if they were HMG personnel.

35. However, if the contractor employee working at the HMG or non governmental Approved Community facility requires to provide any DTCT Defense Articles to his/her employer then, before this can happen, the contract employee's company must either be authorised as a member of the United Kingdom non governmental Approved Community or there must be a Re-transfer authorization in place in accordance with paragraphs 24-33 above for the company to receive the DTCT Defense Articles.

36. If a contractor is employed to provide a service (e.g. maintenance of equipment) at an HMG or non governmental Approved Community facility and their employees providing the required services/maintenance are required to have access to DTCT Defense Articles, before such access can happen, the contractor must either be authorised as a member of the United Kingdom non governmental Approved Community or for the contractor employees to receive access to the DTCT Defense Articles there must be a Re-transfer authorization in place in accordance with paragraphs 24-33 above.

Compliance

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

38. 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.

39. Any material violations by United Kingdom Approved Community members 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.

40. Within Departments and Agencies such violations must be reported to the DSO who shall inform the MOD DE&S DHSY/PSYA. UK Approved Community non governmental members must report any violation to the MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC) who will advise MOD DE&S DHSY/PSYA who, in both circumstances, will notify the United States Government as appropriate. The details of the JSyCC are:

JSyCC WARP Contact Details

Email: For those with access to the RLI: CIO-DSAS-JSyCCOperations

Email: For those without access to the RLI: CIO-DSAS-JSyCCOperations@mod.uk

Telephone: Working Hours: 030 677 021 187

Out of Hours/Duty Officer Phone: 07768 558863

Fax: 01480 446328

Mail: Joint Security Co-ordination Centre (JSyCC), X007 Bazalgette Pavilion, RAF Wyton, Huntingdon, Cambs PE28 2EA

41. United Kingdom Community members must inform their employees and personnel who may be handling Defense Articles of the above requirements; and

42. 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.

Notification of changes in ownership, control or closure of a UK Non-Governmental Approved Community Site

43. The Facility Security Officer or Board Level Contact of UK non-governmental Approved Community facilities must immediately notify MOD DE&S DHSY/PSYA of any change in the circumstances of the company/facility that may have a bearing on its Approved Community status. In particular, the following must be immediately reported in advance of the event occurring:

a. Proposed change of ownership or control, including any foreign acquisition which will raise the stock-holding by any foreign interest to 5% or more of the total company stock.
b. Appointment of new Board Directors.

c. Appointment of a person, who is not a full UK citizen, or who holds dual nationality, to a position within the company where that person may be able to influence the appointment of employees to those areas of the company which are engaged on involving U.S. DTCT Defense Articles.
d. Purchase by a person, who is not a full UK citizen, of sufficient shares in the company which would enable that person to appoint, or influence the appointment of individuals to positions where access to protectively marked assets or a secure area is involved.

44. In cases where a non-governmental Approved Community facility is subject to a change of ownership it should not be assumed that Approved Community status will continue as any such changes will need to be re-considered by MOD DE&S DHSY/PSYA and the U.S. government.

Compliance Inspections

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

Appendix 1: Application for a Non-Governmental United Kingdom entity to join the DTCT Approved Community

FULL NAME & ADDRESS OF FACILITY TO BE CONSIDERED (include "Trading As" name if different)	**FULL NAME & ADDRESS OF HEAD OFFICE (IF DIFFERENT)** (include "Trading As" name if different)
Post Code:	Post Code:

Tel N$^{o:}$
Fax N$^{o:}$

In accordance with the Data Protection Act 1998, the

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

DETAILS OF INDIVIDUAL TO BE FACILITY SECURITY CONTROLLER	**DETAILS OF BOARD MEMBER TO BE COMPANY BOARD LEVEL CONTACT**
Surname:	Surname:
Full Forenames:	Full Forenames:
DoB:	DoB:
Place of Birth:	Place of Birth:
Country of Birth:	Country of Birth:
Nationality/ties:	Nationality/ties:
Full Work Address (including Post Code):	Full Work Address: (including Post Code):
Tel N$^{o:}$	Tel N$^{o:}$
Fax N$^{o:}$	Fax N$^{o:}$
e-Mail:	e-Mail:

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 INCORPORATED, PLEASE GIVE DETAILS OF ALL ASSOCIATED COMPANIES, SUBSIDIARIES, PARENT OR HOLDING COMPANIES, INCLUDING FULL NAME AND ADDRESS AND COUNTRY IN WHICH REGISTERED.

Details:	Details:

Details:	Details:

Details:	Details:

Please provide the 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
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 & Date of Certificate			
Full Permanent Address (incl Post Code)			
Since (Date)			
Position in Company (Title)			
Signature*****			

*** SIGNATURE BY COMPANY DIRECTOR'S INDICATES THEIR AGREEMENT TO THE CONSENT STATEMENT ON PAGES A1-10 & 11 BELOW.**

PLEASE CONTINUE OVERLEAF AND ON CONTINUATION SHEETS AS NECESSARY

DIRECTORS' CONTINUATION SHEET

	Director	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 & Date of Certificate			
Full Permanent Address (incl Post Code)			
Since (Date)			
Position in Company (Title)			
Signature*****			

*** SIGNATURE BY COMPANY DIRECTOR'S INDICATES THEIR AGREEMENT TO THE CONSENT STATEMENT ON PAGES A1-10 & 11 BELOW.**

PLEASE CONTINUE ON CONTINUATION SHEETS AS NECESSARY

DIRECTORS' CONTINUATION SHEET

	Director	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 & Date of Certificate			
Full Permanent Address (incl Post Code)			
Since (Date)			
Position in Company (Title)			
Signature*****			

*** SIGNATURE BY COMPANY DIRECTOR'S INDICATES THEIR AGREEMENT TO THE CONSENT STATEMENT ON PAGES A1-10 & 11 BELOW.**

PLEASE CONTINUE ON CONTINUATION SHEETS AS NECESSARY

DIRECTORS' CONTINUATION SHEET

	Director	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 & Date of Certificate			
Full Permanent Address (incl Post Code)			
Since (Date)			
Position in Company (Title)			
Signature*****			

*** A SIGNATURE INDICATES CONSENT TO BACKGROUND CHECKS BEING MADE WITH OTHER UK GOVERNMENT AGENCIES. IT ALSO INDICATES CONSENT TO THE NAME AND TITLE OF THE INDIVIDUAL BEING RELEASED TO THE UNITED STATES GOVERNMENT FOR IT TO CONDUCT BACKGROUND CHECKS INTO:**

1). **ANY INDICTMENTS OR CONVICTIONS OF US EXPORT CONTROL LAWS; AND**
2). **ANY CLOSE TIES THROUGH BIRTH OR OTHER ASSOCIATIONS TO:**
   - **A. COUNTRIES SUBJECT TO NATIONAL OR INTERNATIONAL ARMS EMBARGOES OR;**
   - **B. COUNTRIES, ORGANISATIONS OR ENTITIES THAT SUPPORT TERRORISM.**

PLEASE CONTINUE ON CONTINUATION SHEETS AS NECESSARY

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 UNITED KINGDOM 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 OR THE UNITED STATES GOVERNMENT ARE TO BE LISTED BELOW.

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

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

If necessary please continue on a separate sheet.

PLEASE PROVIDE INFORMATION ON ANY VIOLATIONS OF UNITED KINGDOM EXPORT CONTROL LAWS OR REGULATIONS AS CONSIDERED BY HER MAJESTY'S GOVERNMENT BY DIRECTORS OF THE COMPANY OR ANY OTHER INDIVIDUALS HOLDING MORE THAN ONE FIFTH OF PAID UP SHARES, PREFERENCE SHARES, OR LOAN CAPITAL.

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

If necessary please continue on a separate sheet.

Do you have any current contracts 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 any UK or US Defence contracts currently being undertaken or pursued by the company

DECLARATIONS

DECLARATION - To be signed by the Company Secretary, Legal Director or other senior company official **not** the Security Controller nominated on page A1

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.

I confirm that, as a duly authorised officer of the company, I acknowledge on behalf of the company that it will comply with the provisions of the Security Policy Framework, as amended, in accordance with Section 10 of the Implementing Agreement (IA), and I acknowledge the conditions identified in Section 11(4)(b) of the Implementing Agreement (IA) as set out below.

(i) Information and statements provided to one Participant regarding Defense Articles exported, Transferred, Re-transferred, or Re-exported may be provided to the other Participant;

(ii) Defense Articles may not be Re-transferred or Re-exported without the prior approval of the Participants;

(iii) The United States Government considers any Re-transfer or Re-export of Defense Articles, without prior permission of the Participants, to be a violation of the United States International Traffic in Arms Regulations, Arms Export Control Act, and related laws;

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

(v) United Kingdom Approved Community members must, within five days of the event, provide written notification to Her Majesty's Government of a material change in a United Kingdom Approved Community member, 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. A United Kingdom Approved Community member must provide Her Majesty's Government 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 of ownership or control of the United Kingdom Approved Community member;

(vi) Any material violations of the procedures established pursuant to the terms of the Treaty 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;

(vii) Any additional information, records, or documents relating to compliance with the procedures established pursuant to the terms of the Treaty, and this Implementing Arrangement, will be provided to Her Majesty's Government upon request of either Participant. United Kingdom Approved Community members will also endeavour to obtain any additional information, records, or documents relating to compliance with the procedures established pursuant to the terms of the Treaty, and this Implementing Arrangement, held by a foreign subsidiary, parent or affiliated company upon request by either Participant;

(viii) No objection will be made by the United Kingdom Approved Community member to any reasonable request by either Participant to undertake an investigation, review records, or inspect any premises in accordance with the established mechanisms of cooperation;

(ix) United Kingdom Approved Community members .will inform their employees and personnel who may be handling Defense Articles of these requirements; and

(x) In the case of removal from the United Kingdom Approved Community, the nongovernmental United Kingdom entity or facility 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.

By signing and submitting this application to join the United Kingdom Approved Community, I confirm that the Company is aware of the terms and conditions attached to United Kingdom 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 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 in this form may also, if required, be passed to the United States Government Authorities involved in the DTCT Approved Community approval process.

By signing this form you are thereby confirming that you understand the above and that you give your explicit consent to the processing of any sensitive personal data of which you are the data subject contained in this form in the manner stated.

Appendix 2: Security Requirements for the Protection of Restricted USML Defense Articles

1. USML Defense Articles transferred to the non-governmental UK Approved Community which are to be handled as OFFICIAL-SENSITIVE will be marked "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 Defense 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. The Contractor shall protect RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

4. RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles information shall be protected in a manner to avoid unauthorised access. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

5. All RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles documents/material shall be stored under lock and key. As a minimum, when not in use, RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles shall be stored in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security and control.

6. Disclosure of All RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles information shall be strictly in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose any of the classified aspects of the Contract detailed in the Security Aspects Letter other than to a person directly employed by the Contractor or sub-Contractor, or Service Provider.

Access

7. Access to RESTRICTED USML//REL USA and GBR Treaty Community Defense 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 organisation (DBS-NSV), have a "need-to-know", and whose access is essential for the purpose of his or her duties.

8. 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[5].

Transmission of USML RESTRICTED Defense Articles

9. RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles in any form shall be distributed, 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 or Commercial Couriers in a single envelope. The words RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles shall **not** appear on the envelope. The envelope should bear a stamp or details that clearly indicates the full address of the office from which it was sent

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

Use of Communications and IT Systems

11. The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

12. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/255911/HMG_Baseline_Personnel_Security_Standard.pdf

13. The following describes the minimum security requirements for processing and accessing RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles information on IT systems.

a. Access Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “least privilege” will be applied to System Administrators. Users of the IT System (Administrators should not conduct ‘standard’ User functions using their privileged accounts.

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 ‘strong’ using an appropriate method to achieve this, for example including 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. Unless the Authority authorises otherwise, RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using commercial encryption devices accepted by the Authority. Advice on encryption requirements for the transmission of RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles information shall be sought from the Authority.

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).
5. Operating systems, applications and firmware should be supported
6. Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

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.

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 or ‘untrusted’ systems 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.

Laptops

14. Laptops holding any supplied or contractor generated RESTRICTED USML//REL USA and GBR Treaty Community Defense Articles information are to be encrypted using a Foundation Grade product of equivalent, for example FIPS 140-2 approved full disk encryption.

15. Unencrypted laptops not on a secure site[6] 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.

16. 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.

17. 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 Incident Reporting

18. 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 relevant Department/Agency DSO who shall inform the MOD DE&S DHSY/PSYA. UK Approved Community non-governmental facilities shall inform 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. The contact details of the MOD JSyCC WARP are:

JSyCC WARP Contact Details

Email: For those with access to the RLI: CIO-DSAS-JSyCCOperations
Email: For those without access to the RLI: CIO-DSAS-JSyCCOperations@mod.uk
Telephone: Working Hours: 030 677 021 187
Out of Hours/Duty Officer Phone: 07768 558863
Fax: 01480 446328
Mail: Joint Security Co-ordination Centre (JSyCC), X007 Bazalgette Pavilion, RAF Wyton, Huntingdon, Cambs PE28 2EA

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

Destruction

19. 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 U.S. Supplier.

Interpretation/Guidance

20. Advice regarding the interpretation of the above requirements should be sought from MOD DE&S DHSY/PSYA, Tel: 030679 34378.

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

Audit

22. 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.

Any enquiries regarding this publication should be sent to us at GSSmailbox@cabinet-office.x.gsi.gov.uk
You can download this publication from www.gov.uk.