MINISTRY OF DEFENCE

EGAD

UNITED KINGDOM (UK) TECHNOLOGY SECURITY PLAN (TSP)

United States (US) International Traffic in Arms Regulations (ITAR) Rule Change Concerning Dual & Third Country National (DTCN) Employees

(Guidance for UK End Users and Consignees Only)

OCTOBER 2011

Published by:

BIS

Department for Business Innovation & Skills

Contents

Introduction

1. The US Department of State (DoS) has issued a final rule amending the International Traffic in Arms Regulations ("ITAR") to include a new license exemption for transfers of ~~defense~~ defence articles to Dual National or Third Country National (DTCN) employees of foreign end-users. The new rule came into force on 15 August 2011 and eliminates the need to obtain prior approval from DoS for the transfers of unclassified ~~defense~~ defence articles (including unclassified technical data) to DTCN employees of foreign business entities, foreign government entities, or international organisations that are approved end-users or consignees (including approved sub-licensees) for such ~~defense~~ defence articles.

2. However, use of the exemption is subject to satisfying certain screening and recordkeeping requirements. In particular, in lieu of prior approval, the new ITAR Section 126.18 requires eligible companies and organisations to implement "effective procedures to prevent diversion to destinations, entities, or for purposes other than those authorised by the applicable export license or other authorisation."

3. Based on comments received from Her Majesty's Government (HMG), the Export Group for Aerospace & Defence (EGAD) and others in response to the proposed rule originally published on 11 August 2010, DoS made some important amendments before issuing the final rule. Most notably, DoS has preserved the limited exemption already available under ITAR Section 124.16 for transfers of certain ~~defense~~ defence articles (including technical data) to employees from NATO and EU member states, Australia, Japan, New Zealand and Switzerland and has expanded the definition of "regular employee" to include contract employees with long term employment relationships with the foreign end-user.

4. Those foreign end users and consignees who intend to make use of the new licence exemption must have a TSP and Non-Disclosure Agreement (NDA) in place in order to comply with the rule change. This UK specific TSP has been endorsed by DoS and provides a step by step approach to ensure compliance with the rule change requirements. The information suggested in this document is for guidance only and made without any endorsement, representation or warranty. It is not intended to provide legal or professional advice, and any party seeking to relay on it should ensure that it has obtained its own legal advice to ensure it is complied in accordance with UK law.

Security Clearance

5. This guidance confirms that HMG's Security Check (SC) clearance meets the requirement of ITAR 126.18(c)(1) for a security clearance approved by the host nation government.

Diplomatic Exchange of Notes

6. HMG and the Government of the United States of America recognise that it is in both their sovereign national security interests to provide for the protection of their own and each other's defence articles and technical data. To this end, both Governments have agreed an approach confirmed in a diplomatic Exchange of Notes, which means that

HMG's pre-existing Baseline Personnel Security Standard (BPSS) constitutes a screening process meeting the screening requirements of ITAR 126.18(c)(2).

BPSS

7. This TSP and its associated NDA outlines the measures intended to implement BPSS controls for all DTCNs who are UK civil servants, members of the UK's Armed Forces, and temporary staff and employees of UK contractors, in a manner which the Government of the United States of America accepts satisfies the requirements of ITAR 124.18(c)(2) and ITAR 120.39. Controls described herein are intended to effectively manage risk by assigning and describing responsibilities within the company. Key elements that ensure an effective TSP consist of the following:

a) Integration of security procedures into the operating procedures of UK consignees and end users;
b) Appointment of individuals with duties to oversee implementation and continued observance of security procedures;
c) Communication, education, and training of employees;
d) A BPSS or personnel security screening program; and
e) NDAs.

A summary of the BPSS can be found at Enclosure 1.

Key Objective

8. The key objective is to prevent diversion of controlled US ~~defense~~ defence articles and technical data to un-authorised end-uses and end-users. Continuing personnel security is best achieved by creating a culture in which security is important and accepted (i.e. a security aware environment). The following policies, terms, and definitions are intended to guide company officials empowered with implementation of technology security rules.

Access and Need to Know

9. The dissemination of sensitive information and assets should be no wider than is necessary for the efficient conduct of the business of the UK consignee or end user and, by implication, should be limited to those individuals who are appropriately authorised to have access to it. The "need to know" principle is fundamental to the protection of sensitive government assets.

Technology Security

10. This encompasses company policies, rules, procedures, and plans for physical security of the property, including US defense articles, of UK consignees and end users, as well as personnel security procedures for screening employees. Ensuring both physical and personnel security is the responsibility of the individual appointed as the Security Officer/Controller of the UK consignees and end users. The Security Officer/Controller may be supported in this activity by an Export Control Officer, who is the individual responsible for ensuring adherence to export licensing laws and regulations. In some instances these responsibilities may be combined into a single role. However, it is the responsibility of individuals undertaking these roles to maintain the practices necessary to

provide for security for company proprietary data and sensitive/controlled articles and technology.

Security Officer (Security Controller)

11. This is the individual responsible for both personnel and the protection of sensitive/controlled US articles and technology. This individual works closely with the Export Control Officer to develop and maintain plans to ensure security for company proprietary data and controlled articles and technology. This individual is responsible for ensuring that appropriate arrangements are in place for screening DTCN personnel.

Export Control Officer

12. This is the individual responsible for ensuring adherence to national export control laws. This individual should work closely with the company's Security Officer, who retains overall responsibility for the coordination of plans to ensure the security of company proprietary data and controlled articles and technology.

Note: In some UK consignees and end users the responsibilities of Security Officer/Controller and Export Control Officer maybe vested in the same individual.

Screening

13. The UK end user/foreign consignee is required to screen all of its DTCNs with access to ITAR-controlled material, where these do not already hold a security clearance approved by HMG. DoS have endorsed the BPSS as a screening process as it provides a suitable mechanism for checking any potential risk of diversion by its employees of proprietary data and controlled articles or technologies under the employer's control.

NDAs

14. The UK end user/foreign consignee is required to demonstrate through the execution and retention of a self-certified NDA that those DTCNs having access to ITAR-controlled technical data related to defense articles must recognise the controls that apply to that technical data and must agree that such controlled technical data will not be further disclosed, exported, or transferred in any manner not authorised. A model NDA approved by the US State Department) can be found at Enclosure 2.

Records retention and disposal

15. Records of BPSS checks will be maintained by the UK end user/foreign consignee for at least 5 years. They should be managed and retained in accordance with UK law and in particular the Data Protection Act 1998.

Frequently Asked Questions and Answers

16. A matrix of frequently asked Questions and Answers can be found as part of the overall package of UK guidance documents.

Further Information

17. For further information on this ITAR rule change and the guidance outlined in this UK TSP, please contact: Warren Bayliss, Assistant Head, International Relations Group,

Defence Equipment & Support, MoD Abbey Wood, Bristol, BS34 8JH. Tel: 0117 913 0271.

Enclosures:

1) Guidance adopted from the UK Baseline Personnel Security Standard (BPSS) as relevant here.
2) Model Non-Disclosure Agreement (NDA).

Baseline Personnel Security Standard (BPSS) Screening Guidance

Introduction

1. Subject to paragraph 3 below, HMG has taken the view that BPSS can be used by UK Government Departments, the UK's Armed Forces and UK contractors as a minimum requirement for screening all Dual and Third Country Nationals (DTCNs) who are UK civil servants, members of the UK's Armed Forces, and temporary staff and employees of UK contractors, where these individuals are to have access to US ITAR controlled material. It is for these and other employers to consider whether they adopt the same approach for all staff or for their DTCN staff alone.

2. The BPSS checks are required to address the problems of identity fraud, illegal working and deception generally. As well as posing serious risks to reputation, integrity and financial assets of the employer they may also be indicators of more serious national security concerns. Applicants must be reminded that supplying false information or failing to disclose relevant information could be grounds for refusal/dismissal and could amount to a criminal offence.

3. Those UK End Users/Consignees/Companies who choose not to adopt the BPSS may wish to utilise existing mechanisms available under the ITAR for enabling their non-security cleared DCTN staff to have authorized access to ITAR-controlled material, or implement alternative screening arrangements to meet the requirements of the International Traffic in Arms Regulation (ITAR), section 126.18(c)(2) ("ITAR 124.18(c)(2)"), issued as a final rule on 16th May 2011 on the basis that both the UK and US Governments recognise it is in their sovereign national security interests to provide for the protection of their own and the other's defence articles and technical data.

Risk Factors

4. UK End Users/Consignees/Companies will need to decide whether a particular DTCN staff member may not be generally reliable and, if so, whether that represents a risk. Particular attention should be given to cases in which two or more adverse factors are combined. Risk factors may include the following:

- Involvement in illegal activities.
- False or unsubstantiated claims on a CV or application form.
- Unsubstantiated qualifications.
- Relevant "unspent" criminal convictions, particularly if not declared by the individual but only revealed by other sources.
- Unexplained gaps in employment history.
- Bad or false references.
- Questionable documentation (e.g. a lack of supporting paperwork or concern that documents are not genuine).

- Evasiveness or unwillingness to provide information on the part of the individual.

5. The rigorous application of the checks is dependent on effective document verification. Those carrying out the checks need to ensure that they are completely satisfied with the information that the individual has provided, and know what to do should inconsistencies emerge between that information and what the checks have discovered. In these circumstances, applicants should be allowed an opportunity to explain any discrepancies (they might be genuine errors).

Mitigating Factors

6. The following may, depending upon the circumstances, assist in an assessment of an individual DTCN's overall trustworthiness:

- The necessary identity documents have been produced and verified.
- The appropriate references (where required) have been obtained and there is nothing to suggest reservations about the individual's suitability for employment on sensitive government work.
- The individual's nationality and immigration status allows them to undertake the employment in question.
- The individual has supplied, or has given his consent to the employer obtaining a record of his criminal history, showing unspent convictions or pending prosecutions.
- There is no other information that casts doubt on the individual's suitability for access to sensitive government assets.

Continuing Personnel Management

7. UK End Users/Consignees/Companies should be alert to a number of factors which might call into question the reliability of a DTCN during the course of their employment, for example:

- Drug or alcohol abuse.
- Expressions of support for extremist views, actions or incidents, particularly when violence is advocated.
- Major unexplained changes in lifestyle or expenditure.
- Sudden loss of interest in work or overreaction or prolonged response to career changes or disappointments.
- Unusual interest in security measures, or areas of work outside the normal remit.
- Signs of stress such as excessively emotional behavior.
- Changes in working patterns (e.g. frequently working alone or at unusual hours, and reluctance to take holidays).
- Frequent unexplained absences.
- Repeated failure to follow recognised procedures.
- Unusual travel abroad.
- Relationships with or support for individuals or institutions that are generally regarded as professionally suspect.
- Sudden or marked change of religious, political or social affiliation or practice that has an adverse impact on the individual's performance of their job or attitude to security.

Continued Reliability

8. It should be recognised that all staff or employees can be vulnerable to circumstances that might compromise their attitudes and behaviour regardless of their professional standing and previous reliability. In industry, where doubt arises as to the behaviour and/or continuing suitability of an individual, it should be reported to the Security Officer.

Further Information

9. The full guide on the Pre-employment Screening of Civil Servants, Members of the Armed Forces, Temporary Staff and Government Contractors can be found at http://www.cabinetoffice.gov.uk/sites/default/files/resources/baseline-personnel-security-standard.pdf. A brief summary of the full guidance is shown below.

Baseline Personnel Security Standard (BPSS)

What is the BPSS?

The BPSS is a pre-employment check applied to all UK government employees and any third parties who are required to undergo such checks in order to comply with HMG security processes (See Annex A). It aims to provide an appropriate level of assurance as to the suitability, trustworthiness, integrity, employment legality and reliability of prospective employees. It is designed to provide an employer with an assurance that a potential employee is suitable for employment in a position that will give access to, or knowledge or custody of MOD assets. It consists of verification of a number of stages and satisfactory completion of a number of pre-determined checks. Between each stage the information collected should be reviewed and assessed, and recorded on the BPSS Verification Record, Annex B. This is the official account of the successful completion of the core checks and when they were completed, and should be retained by the employer. It is for the employer to judge whether the employee is suitable for employment in the light of the information disclosed.

The four elements of the BPSS are:

Stage 1 - The Identity Check

Verification of identity is essential before any individual can begin their employment. Identity can be verified by physically checking a range of appropriate documentation (e.g. passport or other photo ID together with bills, bank statements etc) or by means of a commercially available ID verification service (see Annex B)

Stage 2 - Nationality/Immigration Check

Annex C should be completed by the employee and retained by the employer. Nationality and immigration status can be verified by physically checking appropriate documentation

or, in exceptional circumstances only; by means of an independent check of UK Border Agency (UKBA) records (see Annex D).

Stage 3 - Employment and/or Academic History (including references)

As a minimum the past 3 years' employment or academic history must be verified by checking with previous employers. Annex E provides a template for seeking references from previous employers named by the employee, or alternatively references can be followed up by means of a commercially available CV-checking service. Annex F should only be used in exceptional circumstances, where there are unresolved gaps or doubts remain about an individual's employment history. When signed by the individual, it authorises HMRC to disclose to the employer any or all personal data relating to the individual.

Stage 4 - Criminal Record Declaration

Under the terms of the Rehabilitation of Offenders Act 1974, it is reasonable for employers to ask individuals for details of any 'unspent' criminal convictions. In order to check this record employers must obtain a basic disclosure via Disclosure Scotland www.disclosurescotland.co.uk/ for residents of England, Wales and Scotland or Access Northern Ireland www.accessni.gov.uk, for residents of Northern Ireland Basic disclosures, which contain details of convictions considered "unspent" under the Act, can be obtained either by the individual or, with consent, by the employer. A fee is payable for this service.

If discrepancies are found in any documentation or information supplied by the individual, further enquiries should be conducted and the individual given the opportunity to explain

Transfer of documentation

Where an individual transfers from one organisation to another, the receiving department, agency or contractor must be satisfied that the BPSS has been met. To help do this, they may request from the supplying organisation copies of the completed BPSS Verification Record.

If a period of 1 year has lapsed since employment, the individual's identity and immigration status must be confirmed

Renewal of the BPSS

The immigration status of migrant employees must be checked before the current leave expires or within twelve months of the previous check, whichever is the sooner. These checks must be repeated until the employer is able to demonstrate that the employee can remain in the UK or until employment comes to an end.

This page has been intentionally left blank.

ANNEX A

EXAMPLE OF A PRE-APPOINTMENT TIMETABLE

1. Identify requirement. →

2. Advertise requirement with job criteria, including the need as part of the process to: (i) satisfy basic eligibility criteria/certain conditions of employment (e.g. nationality rules/right to work); and (ii) provide appropriate documentation to verify ID, nationality, employment and/or academic history, criminal record (unspent convictions only). →

3. Receive expressions of interest. ↓

4. Check basic eligibility criteria (some people may be rejected at this stage) and issue application pack, including verification forms with a caveat that this information will be checked prior to any subsequent offer of employment but will <u>not</u> be used as part of the sift. ←

5. Receive applications and completed verification forms. ←

6. Sift applicants (based on suitability for the job) and issue invitations for test and/or interview, including the need to bring with them photo and/or other permissible ID verification documents. ↓

7. Test and/or interview, where ID and other previously provided details can be verified/checked face-to-face. →

8. Selection on merit and offer of employment, subject to completion of any outstanding checks. Complete verification record form and advise Security Units for any NSV requirement and, in respect of migrants, inform appropriate department of the need to recheck documents that retain the excuse against a liability for a civil penalty for employing an illegal migrant worker

ANNEX B

Approved Access No:

BASELINE PERSONNEL SECURITY STANDARD VERIFICATION RECORD

1. Employee/Applicant details

Surname:……..……
Forenames:……...

Address:……
.....

Tel No: ……..……..

Date of birth:……

Place of birth:……..……..

Nationality:……

Former or dual nationality:……

(with dates if applicable)

2. Certification of identity

a…….
…….

b……...
…….

c…….
…….

d…….
…….....

3. References (if taken)

a.Referee:……..

Relationship:……..

Address:…….

Length of association:…….

b.Referee:……..

Relationship:……..

Address:…….

Length of association:…….

c.Referee:……

Relationship:……..

Address:…….

Length of association:…….

Other information (i.e. verification of employment history (past 3 years); verification of nationality and immigration status, whether and when such immigration status needs to be rechecked and by whom; disclosure of unspent criminal record; academic certificates seen; additional checks carried out etc.):

I certify that in accordance with the requirements of the Baseline Personnel Security Standard:

I have personally examined the documents listed at 2 above and have satisfactorily established the identity of the above named employee/applicant.

I have obtained the references (if taken) and information listed at 3 and 4 above and can confirm that these satisfy the requirements.

Name:……..

Appointment/Post:……..

Signature:……..

Date:……

Important: Data Protection Act (1998). This form contains “personal” data as defined by the Data Protection Act 1998. It has been supplied to the appropriate HR or Security authority **for the purpose of the Baseline Personnel Security Standard but** in the event of a breach of ITAR on the part of the individual, may be shared with others, including the US Government in accordance with UK law.

ANNEX C

Note: If you are appointed, documentary evidence will be sought to confirm your answers. Your answers will be checked against UK immigration and nationality records.

BASELINE PERSONNEL SECURITY STANDARD

NATIONALITY AND IMMIGRATION STATUS FORM

Full name:
……..

Alias(es)/Other name(s) used:
……..
……

Date of birth: ……Male or Female: …….

Current/last known
address:……..
……
Nationality at birth:
……..

Present nationality (if different):
……

Have you ever possessed any other nationality or citizenship?
YES/NO

If YES, please specify:

……..

……

Are you subject to immigration control?

YES/NO

If YES, please specify: ……..

……

Are you lawfully resident in the UK?

YES/NO

Are there any restrictions on your continued residence in the UK?

YES/NO

If YES, please specify:

……..

……..

Are there any restrictions on your continued freedom to take employment in the UK?

YES/NO

If YES, please specify:

……..

……..

If applicable, please state you Home Office / Port reference number here:

……

Declaration: I undertake to notify any material changes in the information I have given above to the HR or Security branch concerned.

Signature: ……Date: …….

Important: Data Protection Act (1998). This form asks you to supply "personal" data as defined by the Data Protection Act 1998. You will be supplying this data to the appropriate HR or Security authority where it will be processed for the purpose of a check against the UK's immigration and nationality records **but** in the event of a breach of ITAR on the part of the individual, may be shared with others, including the US Government in accordance with UK law. The HR or Security authority will protect the information which you provide and will ensure that it is not passed to anyone who is not authorised to see it.

By signing the declaration on this form, you are explicitly consenting for the data you provide to be processed in the manner described above. If you have any concerns, about any of the questions or what we will do with the information you provide, please contact the person who issued this form for further information.

For official use only:

Reference:

(Organisation stamp)

ANNEX D

EE1 UKBA IMMIGRATION EMPLOYMENT ENQUIRY FORM CONFIDENTIAL

To: Home Office Evidence & Enquiry Unit Information and Property Management Directorate 12th Floor, Lunar House 40 Wellesley Road CROYDON CR9 2BY Fax No: 0208 196 3946/3047	From: Fax No:

PART 1 [for completion by the requesting officer] **– APPLICANT'S DETAILS**

Family name:	Last known address:	
Other names:		
Nationality:	Date of birth:	Gender:
Enquiry:	HO Reference No:	
	Port Reference No:	
Enquirer's Name:	Telephone Number:	

PART 2 [for completion by UKBA] **– CONFIRMATION OF IMMIGRATION STATUS**

Any trace of the individual?	YES / NO	

Are they entitled to seek paid employment?	YES / NO	If so, from what date: / /
Does the above named have restrictions on their employment?	YES / NO	If so, what are the restrictions?
Additional information including HO number, aliases and address if different:		
Name (Block Capitals): Date: / /	Home Office authorisation stamp or signature:	

ANNEX E

BASELINE PERSONNEL SECURITY STANDARD

EMPLOYMENT HISTORY REPORT FORM

(The draft covering letter shown below may be used together with the Baseline Personnel Security Standard Employment History Report Form overleaf. Alternatively, organisations may wish to include the Report Form with their normal letter requesting employment history).

Dear [ ],

SUBJECT:

You may be aware that we are required to verify employment history to help confirm the reliability of persons who may have access to Government assets. The person named above who (is an employee of) / (has applied for employment with) this organisation comes within the terms of this procedure.

S/he has given us your name as a (previous employer). It would be appreciated, therefore, if you would be good enough to let us have (confirmation (with dates) of his/her employment with you) by completing the attached Report Form and returning it to us by no later than [insert date]. Your reply will be treated in the strictest confidence.

Your cooperation and understanding in this matter will be greatly appreciated.

Yours sincerely,

[Signed]

SUBJECT:

1. How long did the subject work for you and in what capacity?

From:…….....
To:……..

Capacity(i.e. appointment/post)……..……

2. Are you related to the subject? If so, please state your relationship.

……

3. Over what period have you known the subject?

From:……..
To:……...

Name:……

Signature:…….
Date:……...

Contact
address:……
….. Tel No:…….

Email:……..

Company Name and Address (Stamp if applicable):

Important: Data Protection Act (1998). This form contains “personal” data as defined by the Data Protection Act 1998. It has been supplied to the appropriate HR or Security authority for the purpose of the Baseline Personnel Security Standard **but** in the event of a breach of ITAR on your part, may be shared with others, including the US Government in accordance with UK law. The HR or Security authority must protect the information provided and ensure that it is not passed to anyone who is not authorised to see it.

ANNEX F

HMRC RECORD CHECK FORM – APPLICATION IN RESPECT OF THE HMG BASELINE PERSONNEL SECURITY STANDARD

[TEMPLATE – TO BE REPRODUCED LOCALLY ON HEADED/CRESTED PAPER]

I authorise HM Revenue & Customs to disclose any or all personal data which they have access to or hold about me to the [insert name of requesting organisation] in connection with my current or prospective employment, directly or indirectly, by the [insert name of employing organisation].

I declare that the information I have given is true and complete to the best of my knowledge. I understand that any false statement may disqualify me from employment or, if employed, lead to dismissal. In the event of a breach of ITAR on my part, I agree that it may be shared with others, including the US Government in accordance with UK law.

Title: | | National Insurance Number: | |

Surname: | | Forename(s): | |

Any previous name(s) used:

Current address (including postcode):

Previous address (including postcode):

Date of birth: / /

Signature: Date: / /

Return to address (to be completed by requesting organisation):

Name of sponsoring department/organisation:

If you have any queries regarding the completion of this form, please contact HM Revenue & Customs, Data protection SAR Unit (Tel: 0191 225 3098).

Enclosure 2

Model Non-Disclosure Agreement (NDA)

[End User/Consignee Name]

[Address] [Date]

Non-Disclosure Agreement for the purposes of ITAR Section 124.18(c)(2) – authorisation for disclosure to dual-national and third country national ("DTCN") employees

I ---------- , duly authorised by [*name of UK end user/consignee*] hereby certify that [*name of UK end user/consignee*] has taken and will take all necessary steps to ensure any technical data relating to defense articles on the US Munitions List to which [*name of UK end user/consignee]* will have access to by virtue of licenses granted under the International Traffic in Arms Regulations (Title 22 Code of Federal Regulations Parts 120-130) (the "ITAR")

(i) will only be provided to those of its DTCN employees who either

a. hold a security clearance approved by the United Kingdom Government, or

b. have been screened for employment under the United Kingdom Government's Baseline Personnel Security Standard (BPSS); and

(ii) will not be further disclosed, re-exported, or transferred by those employees in any manner or in any way that represents a risk of diversion inconsistent with the relevant terms of the license, or of any subsequent authorization issued by the US Department of Defense Trade Controls, disclosed to [*name of UK end user/consignee*] by the licensor.

I further certify that [*name of UK end user/consignee*] will keep records of those of its DTCN employees who have been screened pursuant to paragraph (i)(b) in accordance with the requirements of the UK Technology Security Plan and the Data Protection Act 1998. In the event of a civil or criminal violation [insert name of UK end user/consignee] will make those records available to Her Majesty's Government in accordance with UK law, including the Data Protection Act 1998 and the protocols and agreements referred to in the Exchange of Notes agreed between the United States Government and Her Majesty's Government dated 11 August 2011. .

Signed,

[give position]