Cabinet Office

HMG Security Policy Framework

Security Requirements for List X Contractors

VERSION HISTORY

SPF VERSION	DATE PUBLISHED	SUMMARY OF CHANGES
V1.0	Dec 08	N/A
V2.0	1 May 09	N/A
V3.0	Oct 09	No significant changes to the document
V4.0	Apr 10	No significant changes to the document
V5.0	Oct 10	New paragraph 9h) detailing additional responsibility of Security Controllers to immediately report any security incident involving MOD-owned, processed or generated information to the MOD Defence Industry Warning, Advice and Reporting Point (WARP) in the Joint Security Co-ordination Centre (JSyCC).
V6.0	May 11	Paragraph 9c) Replace reference to "System Security Policy (SSP) *and* Security Operating Procedures (SyOPs)" with "Risk Management and Accreditation Document Set (RMADS)"
V7.0	Oct 11	New paragraphs 45-55 concerning Un-cleared Visitor Areas (UVAs) and other minor textual changes for the purposes of clarity.

CONTENTS

SECURITY REQUIREMENTS FOR LIST X CONTRACTORS....1

THE ROLE OF THE CONTRACTOR'S MANAGEMENT....4

Mandatory supervision requirements....4

Responsibilities of the Board Contact....6

Responsibilities of the Security Controller....6

Company security instructions....8

Notification of changes in ownership and control or closure of a List X contractor....8

Controlling visitors to List X premises....9

Types of visitors....10

Contracting Authority and visitors from other List X contractors and subcontractors....11

Security controls for meetings and conferences....11

VISITING OFFICIALS WITH A STATUTORY RIGHT OF ENTRY....12

Health and safety inspectors....12

Local authority inspectors....13

VISITORS FROM OVERSEAS....13

PREPARATION AND CONTINGENCY PLANS....20

Inspections....20

Accommodation requirements....20

Protecting sensitive assets....20

Inspection teams....21

UNITED NATIONS CHEMICAL WEAPONS CONVENTION - GUIDELINES FOR CHALLENGE INSPECTIONS OF LIST X CONTRACTORS....23

Preparation and contingency plans....23

Private Venture Defence Related Projects and Technology **24**

Exhibitions and Publicity material **24**

ADVERTISEMENTS **28**

Overseas promotion and sale of equipment and technologies **29**

OVERSEAS PROMOTION, SALE OR RELEASE OF DEFENCE EQUIPMENT OR TECHNOLOGIES **30**

US RE-EXPORT CONTROLS **31**

Transmission **32**

Licensed manufacture **32**

The role of the contractor's management

1. Contractual responsibility for the security of government assets held on the contractor's premises rests with the contractor's Board of Directors.

2. While some of the security controls required under the terms of a contract may seem inconvenient, the baseline controls discussed in this manual have been designed to flexibly provide appropriate levels of protection for sensitive government assets, wherever they are held. They can also be used to protect the contractor's own assets, technology and expertise, on which the integrity, prosperity and security of the company and its employees depend.

3. Senior managers should emphasise that security is an integral function of line management and security controls are only effective if properly planned, implemented and supervised. They should insist on the implementation of appropriate levels of security as contractually defined, and be seen to give full support to line managers and security staff involved in achieving and maintaining that objective.

4. Arrangements for meeting required security controls, are for the contractor to decide, but ***must*** always be sufficient to meet the baseline controls discussed in this Document. The Departmental Security Officer (DSO) of the Contracting Authority or MOD Defence Equipment & Support – Deputy Head Security & Principal Security Adviser Organisation (DE&S DHSY/PSYA) as applicable will be available to provide advice as to the adequacy of security controls implemented.

5. When deciding such arrangements, the contractor should bear in mind that the Contracting Authority is likely to treat any significant lapse in security, leading to the compromise of protectively marked assets, as a serious matter. Failure to fulfil security obligations in breach of contract conditions could result in contractual penalties, the termination of the contract and the removal of the contractor from List X.

Mandatory supervision requirements

6. The contractor will need to make the following appointments to satisfy mandatory requirements for the supervision of the appropriate security aspects:

a. **Board Contact** - who ***must*** be a British national and a member of the Board of Directors, with overall responsibility for security

b. **Security Controller** - a British citizen with responsibility to the Board Level Contact for the day to day security aspects - a large contractor, or a contractor with

substantial contractual obligations, may find it necessary to appoint a full time Security Controller, supported by one or more security staff - a contractor with a number of different sites, may need to appoint Local Contacts, who report to a [Group] Security Controller

The size of a contractor or its contractual obligations will vary from company to company. Some contractors decide to appoint the Managing Director as the Board Level Contact. While for smaller companies, the Board Level Contact and Security Controller may be the same person. The DSO or MOD DE&S DHSY/PSYA must be informed, where possible in advance, if the Board Level Contact or Security Controller is to change.

c. **Clearance Contact** - with responsibility for coordinating appropriate arrangements for the security clearance of employees involved with the contract - a large contractor may wish to appoint an individual to work in support of the Security Controller - a small contractor may nominate the Security Controller as the Clearance Contact

d. **IT Installation Security Officer** - IT installations and networks are particularly vulnerable to compromise and require thorough and continuous security management

e. **ATOMIC Liaison Officer** - only where the contractor requires access to ATOMIC information - this individual is to be solely responsible for the security of all ATOMIC information - the Security Controller may also be appointed ALO - the appointment of the ALO must be notified for approval, on behalf of all Contracting Authorities, to The ATOMIC Coordination Office, MOD.

f. **Crypto Custodian** - only where the contractor is required to hold government cryptographic material or equipment - this individual is to be responsible for the secure handling, that is, receipt, storage, distribution and disposal, of all cryptographic material on the contractor's site - an Alternative Crypto Custodian ***must*** also be appointed, as deputy to the Crypto Custodian - the DSO, or MOD DE&S DHSY/PSYA will notify the contractor of the procedure for appointing and registering a Crypto Custodian.

g. **Deputy Security Controller** - whilst not mandatory, companies may wish to identify an individual to act as the Deputy in the absence of the appointed Security Controller. The Deputy may also be one of the officials at c-f above.

Responsibilities of the Board Contact

7. The Board Contact is specifically responsible for:

a. exercising policy control

b. giving appropriate authority and effective support to the Security Controller

c. approving Company Security Instructions - refer to paragraphs 13-14

d. informing the DSO or MOD DE&S DHSY/PSYA of changes to the company's status, that is, ownership, control, closure - refer to paragraph 15.

Responsibilities of the Security Controller

8. It is important to note, that although the Security Controller's function under the Board Level Contact is an executive one, overall contractual responsibility remains with the Board of Directors.

9. The Security Controller is specifically responsible for interpreting, implementing and monitoring security controls for the appropriate protection of government protectively marked assets held on the contractor's site, by:

a. liasing within the company, and between the company and the DSO or MOD DE&S DHSY/PSYA

b. advising management on the interpretation and implementation of contractual and, where appropriate, legislative security controls

c. preparing and implementing the *Company Security Instructions,* ***the*** *Risk Management and Accreditation Document Set (RMADS) and* making sure that they are made available to, and understood by all appropriate employees, updating them as necessary

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 controls for a new contract or for the alteration of buildings where protectively marked 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

g. ensuring that any breach of security is immediately reported to the respective Contracting Authority and, if appropriate the regional police and that the circumstances are investigated, the outcome is recorded in the company breaches register and a full report and impact analysis is passed to the Contracting Authority

h. ensuring that **any** security incident involving MOD owned, processed or generated information is immediately reported to the MOD Defence Industry Warning, Advice and Reporting Point (WARP) in the Joint Security Co-ordination Centre (JSyCC). This will enable the JSyCC to co-ordinate a formal information security reporting process to assess any associated risks, progress incident impact, co-ordinate appropriate security enquiries and provide specific information security advice to the MoD's Chief Information Officer (CIO), Departmental Security Officer (DSO) and, where appropriate, the Security Controller, Board level contact and other senior company Executives with an evolving picture of MoD-Defence Industry information assurance (IA) and data integrity. It will also assist List X contractors to maintain their business outputs and contractual obligations whilst complying with MOD IA security procedures, build resilience into their business processes and provide respective Management Board Executives with IA incident and risk mitigation reports.

10. It is important for the Security Controller to consult widely within the company when considering security controls for a new contract or alterations to buildings requiring the co-operation and resources of several departments. Failure to discuss requirements for such controls well in advance may subsequently result in hurried and expensive remedial controls.

11. The Security Controller ***must***, as soon as possible, inform the Contracting Authority or, in respect of MOD contracts, MOD DE&S DHSY/PSYA when each contract containing Security Measures such as DEFCON 659 (refer to appendix 1, 'List X Contractual process') or other applicable Security Measures has been completed or when the List X site is **no longer** undertaking contracts that include such Security Measures.

12. Where the Contracting Authority places a separate contract with a consultant who is an employee of a List X contractor, and the work is to be carried out outside the

Contracting Authority's premises, the List X contractor's Security Controller is responsible for ensuring that security controls are appropriate to protect the protectively marked assets against compromise.

Company security instructions

13. It is important that responsibility for security aspects be given to and understood by all employees involved in handling protectively marked assets, regardless of their role or position within the company. This will help avoid lapses of security which could lead to the compromise of protectively marked assets, to embarrassment for the contractor or Contracting Authority, and breach of contract conditions, possibly resulting in contractual penalties, premature termination of the contract and removal of the contractor from List X.

14. To fulfil its contractual obligations, the contractor ***must*** provide guidance to employees in the form of Company Security Instructions. The instructions should:

a. be prepared by the Security Controller at an early stage

b. be approved by the Board Level Contact and the Contracting Authority or MOD DE&S DHSY/PSYA

c. be issued with the authority and signature of the Managing Director

d. be protectively marked at a level no higher than RESTRICTED, to help ensure full circulation and availability to all involved employees

e. publicise the appointment, details and availability of the Security Controller and their deputy and make it clear that they are available for consultation and advice on any security aspect.

Notification of changes in ownership and control or closure of a List X contractor

15. The contractor ***must*** notify its Contracting Authority or in respect of defence contracts MOD DE&S DHSY/PSYA of any change in the circumstances of the company which may have a bearing on its security status and its ability to carry out its

protectively marked contracts. In particular, the following ***must*** be immediately reported, where possible in advance:

a. proposed change of ownership and 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 protectively marked work or where access to protectively marked assets is needed

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.

16. In cases where a List X contractor is subject to a change of ownership it should not be assumed that any existing government contracts will be automatically novated to the new owners. Before such novations can take place the Contracting Authority will need to be satisfied that the new owners meet certain conditions. These include the need to be satisfied that protectively marked assets will continue to be protected to the required standard. Where assets protectively marked CONFIDENTIAL or above are involved, the new company will have to meet the criterion for List X contractor status.

17. Any intention to close down a List X contractor's company or to transfer protectively marked work from one List X site to another ***must*** be brought to the attention of the DSO or MOD DE&S DHSY/PSYA at the earliest possible time so that proper arrangements can be made for the disposal of protectively marked assets and the completion of the necessary security procedures.

Controlling visitors to List X premises

18. Visitors ***must not*** be allowed access to any protectively marked assets, unless the Security Controller is assured that such individuals have a 'need to know' and hold the appropriate security clearance and prior release approval has been granted. Where only part of a contractor's, or subcontractors premises is used on protectively marked

work, the arrangements must limit visitors without security clearance or the need to know to areas used for non protectively marked work.

19. In areas of List X premises where protectively marked work is undertaken or assets are held, the contractor, or subcontractor, ***must*** ensure that visitors do not have access to the areas or information which they have no authority to access. Accordingly the contractor or subcontractor must implement effective arrangements for the identification and control of visitors. Differing security measures are likely to be required, for example, access control systems, doors, locks or escorts.

Types of visitors

20. The type of visitor who may need access to premises where protectively marked work is undertaken or assets held include:

a. officials sponsored by the Contracting Authority

b. the MOD DE&S DHSY/PSYA

c. other List X contractor employees concerned with government programmes/ contracts

d. subcontractor employees

e. officials with statutory right of entry, for example, health and safety inspectors

f. overseas visitors

g. system and hardware engineers.

21. Other visitors may include customers, potential customers, maintenance contractors, the constituency's Member of Parliament, or students and journalists etc, who wish to examine working conditions or industrial processes. In such cases, where the disclosure of protectively marked assets may be involved, the Security Controller should seek prior approval from the DSO or MOD DE&S DHSY/PSYA .

Contracting Authority and visitors from other List X contractors and subcontractors

22. The MOD DE&S DHSY/PSYA Security Advisers and visitors sponsored by the Contracting Authority, or another List X contractor, should present little difficulty as they are generally well known to the contractor. But where there is any doubt as to their status, their 'need to know' or security clearance etc. this must be confirmed with the Contracting Authority or the appropriate List X contractor's Security Controller.

Security controls for meetings and conferences

23. Where visitors attend meetings or conferences on the contractor's premises or on premises arranged by the contractor, it is important that appropriate security controls are in place to safeguard any protectively marked assets involved before, during and after the event.

24. To this end the *Company Security Instructions* should include appropriate guidance to all employees about the implications for security when organising such events, including the following:

a. an individual attending the event should be made responsible for the security controls, even though the chairman and others attending may not be employed by the contractor

b. a list of those attending should be compiled and their 'need to know' and security clearance status confirmed by the Security Controller and passed to the individual responsible for security of the event

c. the conference room should not be susceptible to overlooking or eavesdropping - depending on the venue and the level of protectively marked discussion it may be necessary to consider a technical sweep.

d. access control to the meeting place, or conference room, should be maintained prior to and during the meeting and during breaks

e. at the start of the meeting, or conference, the chairman should explain any special security arrangements, for example, the taking away of papers, the securing of paper during breaks, the switching off of mobile telephones

f. during breaks protectively marked assets should be appropriately secured or the room should be kept locked and guarded

g. after the meeting, or conference, secure arrangements should be in place for the disposal of the protectively marked assets involved, and where they are to be passed to those attending the meeting, for transit.

Visiting officials with a statutory right of entry

25. Access to assets, protectively marked CONFIDENTIAL and above, by visiting inspectors conducting statutory inspections, should only be permitted if the inspector cannot carry out his duty without such access, and an assurance has been received from the authority employing the inspector, that the individual holds appropriate security clearance.

26. Officials from various government departments and local authorities, such as Health and Safety Inspectors, excise officers, fire inspectors etc, are empowered by statute or bylaws to enter factories, laboratories and working environments, for the purpose of inspection. On production of their credentials, issued by the authorities by which they are employed, these individuals must be given the access and facilities they require to perform their statutory duties. The problem of officials requiring access to areas where protectively marked assets are held, may often be resolved by escorting such visitors to ensure that they do not have direct access or temporarily securing or covering up the assets involved.

Health and safety inspectors

27. Under the *Health and Safety and Work Act 1974*, access to List X sites may be required as a statutory right by health and safety inspectors employed by the Health and Safety Executive (HSE) or by the Local Authority.

28. The right of entry to premises accorded to inspectors under the Act does not excuse them from compliance with the contractor's security measures for controlling visitors, such as identifying themselves and signing the visitor's book. Where the inspector wishes to take photographs, which are likely to reveal assets protectively marked CONFIDENTIAL or above, the contractor's Security Controller, having advised the inspector of the fact, should agree arrangements for the film to be processed securely, and for the photographs to be examined and correctly protectively marked prior to distribution.

29. All HSE inspectors carry credentials identifying them as HSE officials and are approved/cleared to the Baseline Standard (BS) level with some cleared to SC and DV levels to allow access to the highest level of protectively marked assets.

30. Where the Security Controller assesses that such an inspection causes specific security concerns the DSO or MOD DE&S DHSY/PSYA should be consulted, and subject to agreement, the DSO, HSE should be advised. Where necessary confirmation of the level of security clearance held by HSE inspectors should be obtained from the DSO, HSE.

Local authority inspectors

31. Local Authority Inspectors may require access to some List X sites.

32. The Inspectors are not usually security cleared but do carry credentials, which differ in design from authority to authority. These inspectors should not be given access to areas where protectively marked assets are held without prior arrangements having been made. Where difficulties arise over access by the inspectors, the Security Controller should contact the DSO, or MOD DE&S DHSY/PSYA.

Visitors from overseas

33. Except where special arrangements have been agreed and communicated to the company visitors from overseas countries ***must*** ***not*** be given access to any protectively marked assets, without the prior approval of the Contracting Authority.

34. Under various Agreements/Arrangements between the UK and foreign governments, it is the visitor's responsibility to make appropriate arrangements, through their London Embassy or High Commission, to visit a List X contractor's site where the visit involves access to any protectively marked assets. In the case of an International Defence Organisation (IDO), such as NATO, arrangements are made through the IDO Security Officer.

35. Where MOD is not the Contracting Authority, guidance on the requirements for visits by foreign nationals to List X contractors and the approval to release protectively marked information associated with the Contracting Authorities contract/programme ***must*** be obtained from the Contracting Authority DSO.

Visits to Establishments where the MOD is the Contracting Authority

36. The MOD DE&S DHSY/PSYA International Visits Control Office (DE&S DHSY/PSYA IVCO), **'***Guidance Notes for List X Contractors '* - provides guidance for 'Inward & Outward Visits' to and from List X contractors working on defence contracts/programmes. Except in special agreed circumstances (see below), DE&S DHSY/PSYA IVCO is responsible for coordinating all visits by foreign nationals who require access to protectively marked assets associated with defence programmes and contracts held by the contractor, or protected areas where such activities are being undertaken within a site. However, visit requests are not required for visitors from NATO member countries, Austria, Australia, Finland, Sweden, Switzerland and New Zealand to List X sites where access to protectively marked assets will not exceed RESTRICTED and the visitor is not visiting the site for more than 21 working days in any one visit. Visit requests are required for visitors from all other countries (but see paragraphs 39-43 below). Security Controllers must, where appropriate, ensure that such visitors are escorted at all times whilst on site.

37. For visits relating to defence programmes or contracts at CONFIDENTIAL and above level any visitor who arrives at a site without having first submitted a request to DE&S DHSY/PSYA IVCO, unless the visit is carried out under the letter of Intent Framework Agreement, ***must not*** be allowed access to protectively marked assets. It is the responsibility of the UK host to ensure that approval for the visit has been obtained from DE&S DHSY/PSYA IVCO. The Parties to the Framework Agreement (FR,GE,IT,SP,SW & UK) have agreed separate international visit procedures where the visitor/s require access to defence protectively marked assets up to SECRET level that has been pre-determined as shareable - DE&S DHSY/PSYA IVCO's *Guidance Notes for List X Contractors* provides full details.

Visitors from countries of special security interest

38. A List X contractor's normal business activity may involve visits from nationals of countries of 'special security interest', for example Russia or China. Security Controllers will be notified separately of countries of special security interest.

39. It is advisable that Security Controllers keep in contact with managers likely to be involved in arranging visits from nationals of countries of 'special security interest', as a visit may be used to obtain details of advanced technology or in support of intelligence activities.

40. Prior to any visit DE&S DHSY/PSYA IVCO should be provided with the following details, where possible.

- Full Name
- Date of Birth
- Passport Number
- Who the visitor is representing

41. Visitors ***must*** be escorted when on site, and denied the opportunity for indirect access to protectively marked assets. All employees involved in discussions or presentations should be reminded of the need to guard against compromising protectively marked assets.

42. If required by the relevant Contracting Authority, on completion of the visit the Security Controller should send the DSO or MOD DE&S DHSY/PSYA a Visit Report. The requirement for a Visit Report, on a visit made to a List X contractor by a national of a country of special security interest, is not intended to monitor or limit the legitimate conduct of business. The reports are often the only indication that a visit has taken place, and also provide an important source of information for the study of hostile intelligence activity.

43. DE&S DHSY/PSYA IVCO's *Guidance Notes for List X Contractors* provides full details on the requirements for 'inward visits' in relation to defence programmes and contracts to List X contractor sites.

Un-cleared Visitor Areas (UVAs)

44. To facilitate the efficient conduct of business and to ease the administrative burden on List X facilities, Security Controllers of List X sites where MOD is the Contracting Authority can ask their Security Adviser for agreement that areas of their site are suitable for the use of overseas visitors who have not been cleared through the DE&S DHSY/PSYA IVCO process. These areas are designated as Un-cleared Visitor Areas (UVAs).

45. In order to obtain the Security Adviser's agreement the areas must, as a minimum, meet the following criteria:-

a. The List X facility will consist of those areas where protectively marked material is held or where such work is undertaken and which are physically separated from the

UVA, usually by means of automatic access controls or because it is in a separate building and where there is no possibility of protectively marked of sensitive information or conversations being accidentally viewed or overhead.

b. It is not necessary to pass through secure areas in order to reach the UVA from the point where visitors are first received.

c. Escorting arrangements are sufficient to prevent accidental overhearing of conversations about sensitive matters when visitors are using communal areas, such as staff restaurants or breakout areas.

d. The prior approval to release MOD information to the visitors has been obtained from the MOD Project Team or relevant authority.

e. Arrangements are in place to check the UVA before and after each visit to ensure that any RESTRICTED protectively marked material or personal data has been safeguarded and that following the visit the visitors have departed with all their personal property.

f. Instructions to foreign visitors being allowed access to the UVA are provided setting clear parameters and warning that failure to comply will result in the removal of the visitor from the facility.

g. Written instructions are provided to staff explaining the rules governing the UVA and its use, emphasising that under no circumstances should material marked CONFIDENTIAL or above be taken into the UVA and discussions at that level must not take place there.

h. The Security Controller must maintain records of all foreign visitors to the site and these must be made available to Security Advisers on request and to members of DE&S DHSY/PSYA IVCO.

46. There are no objections to the UVA being used for other meetings or visits (e.g. in-house or for visits by UK nationals) providing that discussions are at the RESTRICTED level or below.

47. Once the Security Adviser has agreed that a site has one or more suitable

UVAs, the List X database will be amended to indicate to DE&S DHSY/PSYA IVCO that such an arrangement is in force. A Request for Visit only needs to be submitted to obtain DE&S DHSY/PSYA IVCO clearance only where an overseas incoming visit will involve discussions at CONFIDENTIAL or above and/or where the company wishes to take a visitor to work areas outside the UVA.

48. It should be noted that DE&S DHSY/PSYA IVCO will not permit a List X site to admit an overseas visitor under the rules applying to the use of the UVA and then 'convert' the visit to a higher level. Such a situation will not count as an emergency visit and the normal rules applicable to foreign visitors will apply. If there is any doubt over the classification of the visit then clearance should be sought from DE&S DHSY/PSYA IVCO in the normal way and within the prescribed timescales.

49. The rules regarding attachments remain unchanged. Any foreign visitor who remains on site for a continuous period of 21 days or more will still require a visit request even if the level of access required is RESTRICTED or below.

50. If a company has concerns about any visit from a foreign national or where they have been advised that the countries are those where special regulations apply, it is the Security Controllers' responsibility to inform DE&S DHSY/PSYA IVCO of the details of the individuals concerned. DE&S DHSY/PSYA IVCO will then contact the appropriate authorities as necessary and provide guidance to the Security Controller.

51. Companies are under no obligation to set-up a UVA for their facilities; however, if they do so, they will be expected to oversee the administration of the UVA themselves. Abuse of these arrangements by a site could result in the DE&S withdrawing their agreement to the UVA and a consequent reversion to the full DE&S DHSY/PSYA IVCO visit arrangements taking place.

52. If a MOD List X contractor without an existing approved UVA wishes to use the UVA procedure it should consider whether it believes it already has a suitable facility. If it does, the Security Controller should submit a request to the Security Adviser to approve existing arrangements. The submission should enclose any relevant plans, draft instructions to visitors and draft instructions to staff.

53. Unless the reception area/gatehouse is immediately adjacent to the proposed UVA, details should also be provided of exactly how and by what route visitors will be escorted between the two. The Security Adviser may request amendments or ask to visit the site before a decision on approval is made. Approval should not be anticipated.

54. If a site wishes to have a UVA, but this will involve the adaptation of existing premises, the Security Adviser should be consulted at an early stage to ensure that any changes will meet the required standard. Once any necessary work has been completed the Security Adviser will assess the adaptation against the criteria set out above

Overseas visits by List X contractor employees

55. List X contractors may undertake government work that requires its employees to make visits overseas, that involves access to UK protectively marked assets, or 'classified' assets belonging to foreign governments or International Defence Organisations (IDO's), for example, NATO.

56. There are various international Agreements/ Arrangements that allow for the exchange of protectively marked or classified assets. Under these Agreements/Arrangements, prior to such visits, the UK is obliged to provide assurances that the individuals involved hold appropriate levels of security clearance and have been briefed on their security responsibilities. For such visits relating to defence programmes and contracts, DE&S DHSY/PSYA IVCO is responsible for providing such assurances except in respect of visits to the Parties to the Framework Agreement relating to sharable information for which separate procedures apply - paragraph 37 refers.

57. Where MOD is not the Contracting Authority, guidance on the requirements for visits by List X employees overseas falls to the Contracting Authority as does responsibility for providing such assurances to the host nation.

58. Whilst the Contracting Authority's approval may not be required for visits overseas which do not involve any protectively marked assets, British diplomatic representatives in the country to be visited can often provide considerable help if a visit is associated with potential exports. Business people may therefore wish to inform the relevant British Embassy/ High Commission of any such visit to establish if any assistance can be provided. Forms for this purpose are available from DE&S DHSY/PSYA IVCO.

59. Employees of a List X contractor, who are travelling for defence purposes with a group of government, or military, personnel, are responsible for submitting their own Request for Visit applications to DE&S DHSY/PSYA IVCO. They cannot be included upon the same Request for Visit as the government, or military, personnel.

Protection of UK protectively marked assets overseas

60. Where a List X contractor's employee is travelling overseas as a member of a party or delegation, the Contracting Authority organising the visit is responsible for the appropriate security arrangements.

61. Before an overseas visit by a List X contractor's employee takes place the Security Controller should:

a. brief the individuals involved as to the threats they may encounter and the security controls they are required to observe.

b. Ensure that written approval is obtained from the Contracting Authority where it is necessary for the individual to disclose UK protectively marked assets during an overseas visit

c. Make arrangements for any protectively marked assets to be sent by approved diplomatic channels to await collection where the individual is personally carrying protectively marked assets the procedures for casual couriers should be followed.

62. During the visit, the individual should take care to appropriately protect any protectively marked assets in their safekeeping. Except when they need to have such assets with them for the purposes of their work, they should arrange to have them stored securely. With the approval of the Contracting Authority, this may be on the premises of the organisation being visited or the approved contractor's agent.

63. Protectively marked assets ***must*** ***never*** be left unattended in hotel rooms or hotel safes. Where appropriate levels of protection cannot be guaranteed, protectively marked assets should be left in the care of the nearest British Embassy, High Commission or Mission.

Protection of foreign classified assets received during a visit

64. Classified material CONFIDENTIAL and above, handed to a visiting individual, should only be accepted where it is possible to hand it, on the same day, to the nearest British Embassy, Consulate or High Commission for official transmission to the UK. Where this is not possible the originator should be requested to send the asset through diplomatic channels in accordance with local national security regulations. In exceptionally urgent circumstances where it may be necessary for the visitor to hand-

carry CONFIDENTIAL or above material to the UK in relation to a defence contract/programme, approval must be sought and granted by MOD DE&S DHSY/PSYA.

Conventional Forces in Europe Treaty - Guidelines for challenge inspections of List X contractors

65. Under the *Conventional Forces in Europe (CFE) Treaty*, former Warsaw Treaty Organisation Inspection Teams may carry out Challenge Inspections at UK industrial sites to satisfy themselves that Treaty Limited Equipment (TLE) is not stored there. TLE includes Main Battle Tanks, Armoured Infantry Combat Vehicles, Artillery greater than 100mm calibre, fixed wing permanently land-based Combat Aircraft and permanently land-based Combat Helicopters.

Preparation and contingency plans

66. List X contractors need to prepare contingency plans refer to paragraph 67-70 which detail how they will protect protectively marked assets in the event of their sites being chosen for inspection.

Inspections

67. Contractors will receive between 5 and 8 hours notice of a Challenge Inspection from Joint Arms Control Implementation Group (JACIG), who will send a forward detachment to advise and discuss any relevant issues. An inspection is normally, though not always, carried out during normal working hours and could last up to 8 hours, made up of several visits which could take place on any day of the year.

Accommodation requirements

68. The number of visitors involved in an inspection could total up to 35, that is, Inspectors, JACIG's forward detachment and escorts, representatives from the local police and Army District, drivers, interpreters etc. The contractor will be required to provide an on site office, or room, for both the Inspection Team and JACIG as well as accommodation for the other visitors. Food may be required for all visitors, on repayment.

Protecting sensitive assets

69. At the majority of sites, contractors should be able to protect sensitive assets by 'managed access' techniques, that is:

a. shrouding protectively marked machinery and equipment - disguising tell tale bulges and shapes

b. implementing a clear desk policy

c. switching off computer screens

d. providing vantage points from where inspectors can satisfy themselves that no TLE are stored in a building, without giving them the opportunity to explore it.

Inspection Teams have no right of access to rooms or buildings, with entrances less that 2 metres wide, unless such rooms or buildings contain TLEs.

70. Where 'managed access' cannot adequately protect protectively marked assets, rooms or buildings can be designated Sensitive Points Within a Site (SPWS). When the JACIG escorting team arrives at the site it must be advised of any SPWSs and the justification for their designation. Contractors must not declare a SPWS when other safeguarding methods can be used, nor must SWPS be designated for reasons of purely commercial sensitivity.

71. Prior to the visit the contractor should consider the following controls:

a. keys for every locked building, room or container with an opening more than 2 metres wide should be made available, if required

b. all the contractor's guides should be fully briefed and thoroughly familiar with the contractor's site and products, and the location of buildings, rooms and containers liable for inspection

c. removing all information including, notices, posters, telephone directories etc, which could reveal anything about the contractor or the employees, from the office or room allocated for use by the inspectors

Inspection teams

72. It should be assumed that each Inspection Team (IT) will include at least one intelligence officer, to collect information, unrelated to the inspection, in the defence, commercial and technical fields. It is also probable that one inspector will be a R & D expert familiar with the contractor's, or equivalent, products.

73. Inspection Teams are authorised to use the following equipment during their inspections:

- binoculars
- still cameras
- laptop computers
- passive night vision equipment
- dictaphones
- flashlights
- video cameras
- magnetic compasses
- tape measures

74. During the introductory briefing by the contractor the Inspection Team should only be given information it has a right to know, or needs for the purpose of the inspection, for example:

a. a brief description of the company

b. the layout of the site, with a site plan

c. the description and location of any TLE stored on the site.

There should be no mention of equipment exempt from the Treaty because of its R&D or manufacturing status, in the introductory briefing.

75. For the visit the contractor's employees should be aware that the inspectors:

a. will have studied the contractor and its products beforehand and will know exactly what they are looking for

b. may try to catch the contractor and its employees off guard by varying the time of their arrival, or by returning after they have left the site, where the inspection time does not exceed the stipulated 8 hours

c. may pretend not to understand English, or will understand more than they admit to, so that they can eavesdrop on conversations or internal radio communications

d. will attempt to take surreptitious photographs or video footage

e. will talk to any employee and will compare notes after the visit, so all employees should expect tricky questions, to which they should respond politely and courteously while not volunteering more information than is necessary.

United Nations Chemical Weapons Convention - Guidelines for challenge inspections of List X contractors

76. Under the United Nations Weapons Convention, which bans the manufacture or possession of toxic chemicals and imposes controls on a range of chemicals, every building in the UK may be subject to a Challenge Inspection at short notice initiated by another Signatory State. Challenge Inspections aim to check the UK's compliance with the Convention and are conducted by international inspectors from the Organisation for the Prohibition of Chemical Weapons.

Preparation and contingency plans

77. Challenge Inspections to industrial sites are most unlikely but cannot be ruled out. Inspections will be penetrating and detailed, although the Convention acknowledges the right of States to protect national security and commercial confidentiality. It is possible that some inspectors and observers may attempt to use an inspection for collecting intelligence.

78. The Department of Energy and Climate Change (DECC) is the National Authority for coordination of the UK's response to the Convention. It provides advice to all firms, whether on List X or not, and will help if a Challenge Inspection is mounted. Such advice may be obtained from: The CWC National Authority, Non-Proliferation, Office of Nuclear Development, DECC.

79. List X contractors need to draw up contingency plans detailing how they will protect protectively marked assets in the event of a Challenge Inspection. They may also wish to include in the plans how to protect sensitive company assets. At the majority of site protectively marked assets can be safeguarded by 'managed access' techniques, similar to those suggested for dealing with CFE Challenge Inspections - refer to paragraph 55. Under the Chemical Weapons Convention, rooms and buildings with entrances narrower than 2 metres are not excluded from inspection.

80. For Challenge Inspections under the Convention, MOD have not made any special arrangements to support List X contractors and will presume that site and contact details are the same as for CFE, unless MOD DE&S DHSY/PSYA has been otherwise advised.

Private Venture Defence Related Projects and Technology

81. Private Venture funded defence related projects and technology fall within one of the following three categories:

a. Variants. Variants of standard defence equipment under research, development or in production, e.g. aircraft, military vehicles or ships, etc. with non-standard equipment or fitments, offered to meet special customer requirements or to avoid security or commercial difficulties associated with the sale of an item in-Service with UK Armed Forces.

b. Derivatives. Equipment for military or civil use that is not based on standard Service designs but is dependant upon expertise or technology acquired in the course of defence contracts.

c. Freelance. Equipment of defence importance that is in no way based on information gained from defence contracts.

82. The contractor ***must*** ensure that any Private Venture that falls into one of the above categories has been formally security graded. MOD DefSy(S&T/Ind) is the only department within the MoD that can provide formal security gradings for Private Venture Projects and Technology. Guidance on how to apply for Private Venture security gradings with MOD DefSy(S&T/Ind) is on the MoD website www.mod.uk and is also available from the contractor's Security Controller.

Exhibitions and Publicity material

83. Contractors wishing to release publicity material, publish a paper, give a lecture in any audio or visual form or exhibit publicity material or hardware at an exhibition ***must*** seek the prior approval of the relevant Authority, where the publicity material or hardware originates from or is related to:

a. Any government contract either directly or indirectly.

b. A Defence related *Private Venture Project* - aspects of which may warrant

protection in the national interest.

84. In this context the release of publicity material includes:

a. open publication of the contractor's publicity material

b. through the media

c. at exhibitions, that is, any exhibition attended by the public even if organised or sponsored by a military unit, branch of MOD or other Contracting Authority

d. as the subject, or as part of, a lecture

e. in scientific, technical papers made available to public institutions or individuals

f. symposia

g. any other occasion where members of the general public have access to the information.

85. Approval for the exhibition of hardware and release of publicity material should be sought from the relevant Authority responsible for the information/equipment programme. For MOD related information in relation to contracted activity the DE&S Project Team (PT) should be approached to obtain clearance. For defence related activity where the information relates to multiple PTs or for Private Venture information where there is no defined PT, the contractor should approach MoD DefSy(S&T/Ind) to obtain clearance for exhibition of hardware and related publicity material. The contractor should give as much notice of the requirement as possible so that any security implications can be assessed and advice given. To this end, it is important that the guidance provided in this section be drawn to the attention of the contractor's employees responsible for product marketing.

86. A request for approval to release publicity material should take into account that:

a. the material involved must not bear any protective marking

b. the proposal should be clearly headed with the purpose or event, for example,

"Publicity material for the Farnborough Air Show"

87. Where any part of the material or hardware discussed in the proposal, for example, photographs, graphics etc, have been previously approved for inclusion in publicity, this should be stated and the reference given:

a. where closely related material has been previously approved for inclusion in publicity, this should be stated and the reference given

b. in the case of authored papers, two copies of the full text and supporting illustrations should accompany the submission - any photographs should be actual prints and not photocopies, each marked with an identifying number - one copy of films or videos should accompany the submission

c. the date by which approval is required should be stated.

88. In the case of authored papers one of the two copies submitted with the application will be returned with advice on any changes needed to make the material suitable for release.

89. The approval could take 3 weeks from the date of the application's receipt, but in exceptional circumstances, e.g. urgent press releases, the release for earlier approval ***must*** be clearly stated in the submission and every effort will be made to meet an earlier deadline. Where a proposal includes a large volume of material it may be possible to save time by giving the Contracting Authority advanced warning.

90. The main contractor should normally be responsible for initiating proposals for all aspects of a contract, but if subcontractors are to act independently the main contractor must ensure that they act in compliance with these instructions. Publicity material prepared by a PR firm under subcontract should also be submitted by the main contractor who is responsible for ensuring that any protective marking or publicity policy guidelines established for specific projects or contracts are applied.

91. For release of information contained in a patent application subject to a *Prohibition Order (Patents Act)* application should first be made to the Patents Office.

92. Where the contractor is in any doubt about the level of protective marking of the asset involved, which is most likely to occur in the case of a *Private Venture Project* **-** advice should be sought in the first instance from the relevant Authority, MOD DE&S DHSY/PSYA or MOD DefSy(S&T/Ind).

Exhibitions

93. It is important that company staff responsible for the preparation of exhibition displays are carefully supervised to ensure that no material or equipment which has not been approved by the relevant Authority is accidentally included. Companies should be aware that from time to time exhibitions are monitored for compromise of protectively marked information and equipment. As such, company staff manning exhibition displays should have access to the clearance references, as a minimum, in order to address any queries raised by government staff carrying out this monitoring.

94. An export licence may be required for goods to be shown abroad at exhibitions and demonstrations although models for exhibitions, unless incorporating actual components, may not require a licence. However obtaining licences can avoid delays in shipment resulting from HM Revenue & Customs or UK Border Agency enquiries. Advice should be sought on a case by case basis from the Department for Business, Innovation and Skills (BIS). In cases where a request for an export licence is made it is important that the submission for exhibition clearance is made to the relevant Authority prior to, or at the same time as, the export licence application.

95. Responsibility for the security protection of the exhibits rests with the main contractor presenting them.

Protectively marked equipment

96. Special precautions are necessary if, exceptionally, authority is given to display protectively marked (including RESTRICTED) equipment. Wherever possible, protectively marked features of components should be removed from material to be displayed. If this is not possible external features of exhibits should be shrouded or disguised. If it is not practicable to remove protectively marked internal features of an exhibit whose external features are not protectively marked, the exhibit as a whole should be physically protected to a level appropriate to the protective marking of its internal features.

97. Exhibits ***must*** be protected in transit in accordance with the rules of the transmission of protectively marked hardware and any supplementary advice which may be issued by the Contracting Authority.

98. Companies ***must*** provide sufficient personnel to protect exhibits during periods when the exhibition is open to the general public. Although the organisers of the exhibition will usually supply a general guard during other periods, it may be necessary to supplement this protection using company staff or approved contract guards,

depending on the status of the organisers and any special instructions which may be issued by the relevant Authority.

99. Other special physical security precautions may also be required during closed hours. Where size permits items should be locked away in security containers which, themselves, may need to be fixed to the stand or floor. Where this is not possible exhibits should normally be fastened to the stand or floor and should be fitted with some form of locked cover and sealing device. The covers or seals should be inspected each morning, and any evidence of tampering reported immediately to the exhibition organisers and the relevant Contracting Authority.

100. Prior to any exhibition staff in charge of company arrangements and those in charge of exhibits should be carefully briefed about the protectively marked aspects of the equipment with which they are concerned, and the security controls which are required.

Advertisements

101. No advertisements, including those for the recruitment of staff, should draw undue attention to protectively marked projects. Where necessary, reference may be made to material already cleared for open publication but otherwise the relevant Authority should be consulted before publication.

102. No mention of the existence or membership of List X, and no reference to the security status of the company or its employees, should be included in any advertisement.

Questionnaires and media enquiries

103. Contractors receiving requests or questionnaires seeking information about their business from organisations concerned with the compilation or publication of directories, registers, marketing or business surveys, or from the media, should consider carefully the implications of disclosure and, if necessary, consult their relevant Authority or MOD DE&S DHSY/PSYA before providing details or discussing aspects of protectively marked work or advanced technology.

104. This guidance is not intended to discourage contact with the media but only to protect sensitive information or technology, the disclosure of which might be damaging to national security. Where the company Security Controller has any doubts about a

particular approach, they should consult the relevant Authority or MOD DE&S DHSY/PSYA as appropriate.

The Queen's award for technological achievement

105. The Awards Office invites applications from UK 'Industrial Units', annually, for consideration of an Award under the following criteria for technological achievement:

A significant advance leading to increased efficiency in the application of technology to a production or development process in British industry, or the production for sale of goods which incorporate new and advanced technological qualities.

106. Whilst there is no intention of inhibiting List X firms from making applications for an Award, any submission which has, or may have, security connotations should be cleared by the relevant Authority.

Overseas promotion and sale of equipment and technologies

Export controls

107. The Government imposes strategic export controls on the sales of certain military and dual-use items for several reasons including:

- National security
- International security policy and objectives
- International treaty obligations and commitments
- Concerns about the spread of terrorism, regional instability or the use of internal repression
- Concerns about the development of WMD and delivery systems

108. Strategic export controls are implemented through secondary legislation introduced under the *Export Control Act 2002.* The latest legislation, The Export Control Order 2008 (“the 2008 Order”) consolidates the main Orders previously made under the 2002 Act so that domestic legislation on strategic export controls (other than legislation relating to particular sanctions or embargoes) is now in place. The secondary legislation now lists a wide range of military and dual-use goods that are subject to export controls and which may require an export licence to most destinations as well as those goods subject to trade controls. See also:

http://www.decc.gov.uk/en/content/cms/what_we_do/uk_supply/energy_mix/nuclear/nonprolif/chemical_bio/chemical_bio.aspx

109. If a contractor is unclear whether or not an export licence is required advice should be sought from the Export Control Organisation Helpline at the Department of Business Innovation & Skills (BIS) (Tel: 020 7215 8070/4594).

110. More details on strategic export controls, and information on BIS-ECO can be accessed at http://www.berr.gov.uk/whatwedo/europeandtrade/strategic-export-control/index.html

Overseas promotion, sale or release of defence equipment or technologies

111. A contractor ***must not*** promote or sell protectively marked defence equipment or technology without the prior approval of the MoD's Equipment Capability – Export Policy and Assurance (EPA) department.

112. A contractor ***must*** complete and obtain approval via *MOD Form 680* (F680) before undertaking any targeted marketing, promotion and demonstration or entering into any contractual commitments involving the sale or release of protectively marked defence equipment or technology overseas. This includes Private Ventures that bear a protective marking (RESTRICTED or above), and any defence equipment or technologies, including Private Ventures, that have not been formally security graded. A Form 680 is still required when a contractor wishes to undertake the targeted promotion or demonstration of protectively marked (RESTRICTED or above) equipment or technologies at an UNCLASSIFIED level.

113. However, a contractor can show and promote a protectively marked (RESTRICTED or above) product at an exhibition without obtaining a F680, providing they have previously obtained exhibition clearance for that product (see the Publicity Material section). This includes talking to exhibition attendees within the physical boundaries of the exhibition, providing the scope of the discussions are constrained within the exhibition clearances received. However, if the contractor wanted to talk to a specific customer outside the parameters of the exhibition clearance or at a higher classification, an approved F680 must be in place beforehand. This does not apply to Government sponsored (i.e. UKTI) special events where F680 for Promotion to the countries involved must be obtained.

114. A F680 is not normally required for the targeted export of equipment or technologies that the MOD has security graded UNCLASSIFIED, unless: in relation to Open General Export Licence – Military Goods For Demonstration (due to its specific reference to F680 as a requirement); including a requirement for HMG support; or, the contractor is attending a HMG sponsored/funded event. In these cases, F680 approval will be required irrespective of whether the equipment or technology has been formally graded or not.

115. MOD F680 can be obtained from the UK MoD website http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/EquipmentandLogisticsPublications/Form680/ModForm680Procedure.htm This website also contains guidance on completing the MOD F680 and how it is processed.

116. The system is designed to prevent unauthorised disclosure of information, and help contractors in marketing their products. It also assists the processing of subsequent export license applications for potential or actual sales. Contractors should allow as much notice as possible for the processing of applications.

117. The UK Government has Bilateral Security Agreements/Arrangements (see Annex B to Chapter on International Protective Security Policy) with many countries which place obligations not to release classified information/material received from the other country without their prior written approval. Where information/equipment has been supplied by another country or contains foreign components you must satisfy yourselves that you have taken into account the undertakings that you or the UK Government have made to the overseas government concerned not to export without the approval of the owner/originating country including where the foreign content is subject to particular controls. If you are exporting classified items originating from another country you ***must*** provide with the F680 application the written agreement from that country to release the classified information/technology or re-export the goods. You ***must*** also take into account any classifications applied to any foreign content by the originating nation.

US re-export controls

118. Contractors involved in re-exporting products should note that where such products, or components within, are of US origin, or where manufactured using US technology, the US claims control over [re]exports from other countries, including the UK. In such cases, under US export regulations, a US re-export licence is required, even if a UK export licence is needed, or has been granted. Although such US regulations do not form part of UK law, contractors who do not comply may be at a

serious disadvantage in any subsequent dealings with the US government or US companies.

119. Companies requiring advice on US export controls or experiencing difficulties with US regulations should contact: BIS, North America Section Policy Unit.

120. Guidance on licensable items or restricted destinations under US regulations should be sought from the: Commercial Section, US Embassy.

Transmission

121. Products permanently, or temporarily exported, for example, for overseas exhibitions, ***must*** not be transmitted through, or carried by a carrier belonging to a country to which their sale is embargoed.

122. For the transmission of goods protectively marked CONFIDENTIAL or above a security transportation plan is required to be approved by the DSO or MOD DE&S DHSY/PSYA as appropriate.

Licensed manufacture

123. Authority to promote or sell an item of defence equipment does not automatically imply agreement for licensed manufacture of that equipment in the same country, because the manufacturing process involved invariably leads to an additional transfer of technology. The issues relating to technology transfer must be considered.

124. Contractors seeking clearance for licensed manufacture should follow the promotion procedures above making it clear in their application that it is a proposal for local manufacture.