Cabinet Office

HMG Security Policy Framework

The Contractual process

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	• Amended title of Chapter • New paragraph 4 concerning placing work involving or releasing Personal Data to a contractor. • Paragraph 48. Amendment to reflect that List X contractor Security Controller must register to have access to the MOD DE&S RESTRICTED website. • Paragraph 49. Amendment concerning the issue of List X Notices by non MOD Contracting Authorities. • Paragraph 50. New paragraph concerning attendance on security courses by List X Board level contacts and security staff. • Paragraph 108. Amendment to list of countries for which submission of Appendix 6 is required for approval to subcontract at the level of RESTRICTED. • Appendix 2. General amendments.

		• Appendix 6. General amendments.
V5.0	Oct 10	• In addition to some minor amendments for the purposes of clarity the following amendments have been included: • References to the MOD DE&S DHSY/PSyA undertaking security assurance and oversight responsibilities on behalf of other government department Contracting Authorities and the requirement for a Customer Service Agreement deleted. • Requirement added at paragraph 39 requiring Contracting Authorities to maintain an assurance on the security conduct of its contractors and suppliers.
V6.0	Oct 11	• Version 6.0 revised and updated for clarity. New Appendix 7 added for contractors to challenge security gradings defined in SALs.

CONTENTS

Responsibility of the Contracting Authority [1]

1. The Contracting Authority ***must*** ensure that appropriate protective security controls are in place for the protection of the assets against compromise. To determine the security controls likely to be required in any given situation, careful consideration needs to be given to the type and value of the assets involved and the nature and scale of threats to them. Such controls, which should meet the Contracting Authority's personnel, physical, document and IT security requirements, should be based upon the principles of risk assessment and management. Specific security controls, which are above the baseline controls ***must*** be clearly specified to the contractor.

2. The assessment of the threat should be based upon the Contracting Authority's own knowledge, information obtained from the Security Service, where appropriate, the local police and, from the contractor, who is likely to be aware of specific threats to its premises and assets, for example, high levels of opportunist theft or vandalism. Contracting Authorities placing large numbers of contracts may find it convenient to prepare a generic threat assessment which can be applied to the majority of contracts.

3. Whilst conditions included in a contract place the responsibility for security on the contractor, the protectively marked material remains the responsibility of the Department Contracting Authority which ***must*** ensure that such assets are protected in accordance with the Security Policy Framework (SPF), that the terms of the contract are observed and, in the case of Confidential and above assets, that such assets are not disclosed to a third party without the agreement of the Contracting Authority.

Placing a Contract or Releasing assets involving Personal Data

4. Where work involving access to Personal Data is to be undertaken on contractors premises or such information is to be provided to a contractor, the Contracting Authority ***must*** ensure that the applicable Office of Government Commerce Model Contract terms and conditions are included in the contract and that the contractor is informed of the requirements contained in the SPF for the protection of Personal Data as defined in HMG IA Standard No 6 – Protecting Personal Data and Managing Information Risk.

[1] Ultimate responsibility rests with the Department Security Officer (DSO) however the DSO may delegate the responsibility to appropriately competent Departmental security representatives.

Placing a Contract or Releasing assets at the Protectively Marked level of Restricted

5. Where work on protectively marked assets at the level of RESTRICTED is to be carried out on a contractors premises, or Restricted assets are to be released to a contractor, the Contracting Authority ***must*** give the contractor written guidance detailing the minimum requirements for the safekeeping of the RESTRICTED assets involved – see Appendices 2 and 6 as appropriate - Guidance for Contractors on the Protection of RESTRICTED Assets the former of which draws attention to the Official Secrets Acts 1911- 1989. In addition the contractor must be notified of the RESTRICTED aspects of the material in the form of a Security Aspects Letter (SAL)- see Appendix 4.

Placing a Contract or Releasing assets at the Protectively Marked level of Confidential or above

6. Where work on protectively marked assets CONFIDENTIAL or above is to be carried out on the contractor premises, the contract ***must*** include conditions concerning the "Security Measures" related to the contract such as, Appendix 1 - DEFCON 659, which clearly states that the contractor is to be compliant with the requirements of the SPF and is responsible for implementing and maintaining appropriate protective security controls. Where a Contracting Authority may require more stringent security requirements to be applied in excess of that required by the SPF, such enhanced measures must be clearly identified in the Invitation to Tender (ITT) so that the contractor can consider the implications and take into account financial provisions for any enhanced security requirements that may be required in the tender bid.

7. The Contracting Authority ***must*** be assured that before a prospective contractor is permitted to hold assets protectively marked CONFIDENTIAL and above on its own premises, that:

   a. the contractor is suitable to access and hold such assets;

   b. appropriate security controls are in place within the contractor's premises for the protection of the assets involved;

   c. the contractor's employees have been suitably cleared and authorised to have access to the assets.

These conditions are applicable for as long as protectively marked assets need to be held on the contractor's premises.

Protection of protectively marked assets

8. In so far as the protection of protectively marked assets is concerned, there are four stages to the contractual process:

- **Stage 1** - Initial discussions and checks - refer to paragraph 9
- **Stage 2 -** Security requirements - refer to paragraph 19
- **Stage 3 -** Placing the contract - refer to paragraph 36
- **Stage 4 -** In-contract monitoring - refer to paragraph 48

Stage 1 – Initial discussions and checks

9. Prior to a sending out an *ITT* - refer to paragraphs 14-18 and subsequently placing a contract involving assets protectively marked CONFIDENTIAL or above, preliminary discussions are often necessary between the Contracting Authority and prospective contractor representatives. During such discussions it may be necessary to divulge a limited amount of protectively marked information.

10. **Before** entering into initial discussions with prospective contractors representatives, the Contracting Authority should ensure that the contractor representatives concerned are appropriately security cleared, normally to Security Check (SC) level or, if applicable, have been granted a Baseline Personnel Security Standard (BPSS). It should be made clear to all involved in the discussions those aspects that are protectively marked, the levels concerned and, as preliminary discussions are not subject to contractual conditions, the fact that they are bound under the Official Secrets Acts to safeguard the protectively marked information divulged to them.

11. On satisfactory completion of Stage 1 checks, the Contracting Authority should advise the branch or section awarding the contract that there are no security objections to initial discussions taking place with those contractor representatives for whom security clearances have been approved.

12. As discussions proceed, and the nature of the proposed work is more clearly defined, the Contracting Authority should specify the 'security aspects', if only provisionally, as

clearly as possible so that the prospective contractor is able to assess the security controls, and estimate the likely costs involved.

13. At each stage in the negotiation process, the prospective contractor should be encouraged to think about the implications of providing appropriate security controls to protect the relevant protectively marked assets against compromise. Where the prospective contractor envisages difficulties or specific requirements, it should be made clear what level and type of support, if any, might reasonably be expected from the Contracting Authority.

Invitation to tender

14. To avoid legal challenge on fair trading and public law grounds, Departments and Agencies ***must*** **not** give preference to existing List X contractors over non-List X companies when preparing their ITT short list.

15. Once the Contracting Authority has identified the prospective contractors to whom it wishes to issue the ITT, it should confirm with MOD DE&S DHSY/PSyA whether the chosen contractors are currently recorded on List X. If not, and it is intended to issue an ITT for a contract that will involve assets protectively marked CONFIDENTIAL or above being held on the contractor's premises, either the Contracting Authority (MOD DE&S DHSY/PSyA in respect of Defence contracts) ***must*** undertake the due diligence/security clearance checks for provisional List X status referred to in the SPF Chapter concerning Industrial Security – Departmental Responsibilities. When these checks have been satisfactorily completed the Contracting Authority should request MOD DE&S DHSY/PSyA to add the contractor to its database of provisional List X contractors.

16. On issuing an ITT, the Contracting Authority should provide written advice, see Appendix 3 General Security Advice to Companies Bidding for Government Contracts as to the nature of general, and any specific, protective security controls that will be needed before the contract can be awarded. Such advice, where possible, should be clear and sufficient for the company to include in its tender appropriate costs for the installation of required protective security controls.

17. ITT's must not be issued and contracts must not be awarded until Stage 1 has been satisfactorily completed and either List X or provisional List X status has been confirmed by the Contracting Authority.

18. When a government contract, involving the holding of assets protectively marked CONFIDENTIAL or above on the contractor's premises, is awarded, and only after an initial visit to confirm the physical suitability of the contractors site has been undertaken by the Contracting Authority, the Contracting Authority **must** advise MOD DE&S DHSY/PSyA and request that the contractor site be formerly recorded as List X.

Stage 2 – Security requirements

19. Given the possibility of rapid changes in the contractor's circumstances, the initial checks ***must*** be repeated if any changes to the contractor ownership or Executive Board structure occur, or if the contract is not awarded within one year of the provisional List X status being granted and the company is still being considered for the initial, or any other contract.

Standard conditions to be included in government contracts

20. Contracts and ITTs involving assets marked CONFIDENTIAL or above ***must*** include security conditions drawing the contractor's attention of the requirement to protect such information to a degree no less stringent than that required by the SPF and to the relevant clauses in the ***Official Secrets Act***. It must be made clear to the contractor that information received or generated as a consequence of the contract is not to be communicated to individuals other than those appropriately cleared, with a need-to-know, and authorised to work on it. These conditions provide the legal and contractual backing for the security controls the contractor will be required to implement. This requirement can be met by including DEFCON 659 see Appendix 1, or other appropriate security measures**.** Departments and Agencies may use their own contract conditions but these should include wording similar to that contained in the above to achieve the same purpose.

Security Aspects Letter

21. Where work is to be carried out on Departmental premises, security arrangements are best managed by the Contracting Authority. Such arrangements must be clearly identified in the contract.

22. Where work is to be carried out on the contractors premises a contractual Security Measures such as DEFCON 659 or other appropriate Security Measures ***must*** be included in all contracts involving protectively marked assets CONFIDENTIAL or

above. The condition should place responsibility for security firmly with the contractor. The Contracting Authority must clearly define to the contractor what is defined in the condition as the 'secret matter' associated with the contract. This must be done in the form of a Security Aspects Letter (SAL) – see Appendix 4.

23. It is important that the “Secret Matter” defined in the SAL is kept up to date and that the contractor is immediately notified of any changes. Contracting Authorities must therefore constantly keep under review the level of the “Secret Matter” defined in an SAL.

24. The contractor's obligations under the Security Measures included in a contract will primarily be concerned with the protection of protectively marked assets. It is important that before work begins on a protectively marked contract the contractor receives from the Contracting Authority a SAL which gives a precise definition and the level of protective marking for each security feature of the contract that requires special security protection.

25. In some instances the Contracting Authority may require security controls in excess of baseline controls specified elsewhere in the SPF. In such cases, these additional controls should be included in the contract .

26. The SAL, which should seldom be protectively marked higher than RESTRICTED, should be sent to the Security Controller, by name, before any work begins.

27. All individuals involved with the planning and implementation of the security aspects should fully understand the SAL and its implications. Where issues are unclear, or it imposes unacceptable or impracticable obligations on the contractor, or if, for any other reason, it is open to doubt, the contractor should take up the matter immediately with the Contracting Authority.

28. The contract and the SAL are fundamental to the List X system, in that they make the contractor responsible for achieving and maintaining required security controls for the appropriate protection of government assets. It is for the Contracting Authority, to decide how to satisfy these requirements, but recognise that such controls must meet the various baseline objectives described elsewhere in the SPF.

Doubtful Security Aspects

29. Contractors may query the protective marking of any aspect of a contract defined in a SAL. Contractors should be assured that this will in no way prejudice their interests’ vis-à-vis Government Contracting Departments. An officer receiving such a query on

a protective marking should deal with it promptly, if necessary issuing an amendment to the SAL. A template of the document to be used to challenge defined security aspects is at Appendix 7.

Security grading guide

30. With certain contracts, the Contracting Authority may define the protectively marked, aspects in a Security Grading Guide (SGG) that is referenced in the SAL, or in the contract document itself. In such a case, the SGG, or relevant part of it, should be supplied to the Security Controller of the List X contractor.

Protectively marked hardware assets

31. Hardware assets vary in size from small components to a very large assembly. Protectively marked information may be revealed in a number of ways, for example, by its shape and appearance or by some interior feature of its design which could be deduced only if the equipment in question is dismantled. The SAL (or its referenced SGG)must identify in as much detail as possible which components are protectively marked and at what level. It will then be necessary to allocate to the equipment as a whole, and to its component parts, the appropriate levels of protective marking. These may vary in different circumstances, such as during manufacture as against during use. For example, a radio transmitter might not attract a protective marking, but the frequency at which it operates could need to be protectively marked SECRET. This would mean that:

a. During manufacture and storage of the components only those components from which the frequency can be deduced need to be protected.

b. During and after assembly, the complete equipment will become SECRET and will require appropriate protection.

c. If the frequency cannot be deduced without dismantling the equipment then it may only be necessary to protect it against this possibility but not against the possibility of visual access.

32. Where the size of a protectively marked hardware asset permits it should be stored in an approved container in the same way as a protectively marked document. Where this is impracticable it will be necessary to carry out a separate risk assessment. Such an

assessment should always be conducted in conjunction with the Contracting Authority or MOD DE&S DHSY/PSyA as applicable.

International Agreements / Arrangements and procedures

33. Under various International Security Agreements/Arrangements, Memoranda of Understanding, Memoranda of Arrangement etc, the UK has certain obligations to safeguard 'classified' assets supplied by foreign governments and by International Defence Organisations (IDOs). Such Agreements/Arrangements normally include provisions for protectively marked contracts, information exchange, transmission of information and asset handling in general. The principle of the obligations contained in these undertakings is that classified assets, received from the other party, are to be protected to a level at least equivalent to that afforded to UK protectively marked information of the same classification.

34. Special obligations which arise in connection with NATO and EU contracts are dealt with in separate regulations. Security instructions for NATO are contained in *CM(2002)49* and, for EU, in *EU Council Security Regulations 2001/264/EC*. As a general rule 'classified' assets supplied by another nation or international organisation should be safeguarded in an equivalent manner to that as for UK protectively marked assets of equivalent grading. It should not therefore be necessary for Security Controllers to refer to these regulations, but where a contractor considers it has a need to do so, in the first instance, they should be advised to contact the MOD Cosmic Top Secret Atomal (CTSA) Registry, MOD, CTSA CTLB SSBC-Security.

35. Further information on International obligations can be found in the SPF Chapter concerning International Protective Security Policy.

Stage 3 – Security Oversight and Assurance of List X Contractors

Placing the contract

36. The Contracting Authority is responsible for undertaking appropriate security oversight and assurance of its contracts and protectively marked assets held by its List X contractors. The Contracting Authority should provide to MOD DE&S DHSY/PSyA.the details of contractors that it has successfully completed the List X due diligence process on and that it wishes to place on the List X database.–As necessary, the List X database will be amended to include the details of the new contractors and the record will be annotated to show the Contracting Authority who is responsible for providing security oversight.

Security oversight by the Contracting Authority

37. Once the contract has been signed, but before any work higher than RESTRICTED takes place, the Contracting Authority, designated authority, should visit the contractor to brief the Board Contact and Security Controller. The Contracting Authority ***must*** provide the Security Controller with detailed security guidance to cover all aspects of physical, document, IT, and personnel security controls. The Contracting Authority, in conjunction with the contractor, and if necessary, consulting the local Special Branch, will carry out a risk assessment based on the nature and magnitude of the threats relative to the value of the assets at risk. The Contracting Authority will advise what additional security controls, if any, are required which may include structural modifications, approved security furniture, or the installation of an Intruder Detection System (IDS) will normally have to be provided by the contractor.

38. The Contracting Authority should take all necessary steps, including site visits to obtain and maintain an assurance that the security conduct of its contractors and suppliers is and continues to be adequate for the safeguarding of protectively marked assets and are in accordance with this SPF. The DSO should be advised of any security concerns.

Personnel security

39. The Contracting Authority (for defence contractors MOD DE&S DHSY/PSyA) in consultation with the List X contractor Security Controller, will also need to confirm which employees require security clearances and the levels of clearance required.

40. Where SC and DV clearances are required, the Contracting Authority in consultation with the Security Controller, should decide who is to be responsible for undertaking the vetting process. The Security Controller is responsible for maintaining a record of security clearances approved for the contractor's employees.

41. Once the Contracting Authority is satisfied that the contractor is able to provide adequate protection for the protectively marked assets involved, the contract may be implemented and protectively marked assets held on the contractor's own premises.

42. The Contracting Authority designated authority, must continue to regularly undertake security assurance visits to the contractor for the life of the contract or as long as the contractor is required to hold protectively marked assets.

Security guidance and education

43. In addition to advice given by the Contracting Authority the contractor ***must*** be provided access to the SPF and subsequent amendments. The ***normal*** method to access the SPF is via MOD DE&S DHSY/PSyA RESTRICTED access website to which the contractor's Security Controller ***must*** register to have access. The SPF is designed to provide advice for senior managers, security staff and line managers. It details the security requirements applicable to industry in connection with government contracts undertaken in the UK, with foreign governments and contractors and International Defence Organisations.

List X and Industry Security Notices

44. MOD DE&S DHSY/PSyA will promulgate List X Notices which address security issues specifically related to List X for defence contracts and programmes. The method of communication of List X Notices and other appropriate security education and awareness materials will be via the MOD DE&S DHSY/PSyA RESTRICTED access website. Contracting Authorities with a need to communicate security requirements in the form of a List X Notice to their own List X contractors should consult MOD DE&S DHSY/PSyA with regard to the format and serial number etc. and provide the List X Notice to MOD DE&S DHSY/PSyA for promulgation on the RESTRICTED website.

45. MOD DE&S DHSY/PSyA will also promulgate on the DE&S Principal Security Adviser's (PSyA) pages of the MOD website Industry Security Notices (ISNs). ISNs provide MOD List X and non List X contractors advice on security policy, guidance and other information that has an impact on assets protectively marked up to RESTRICTED. ISNs can be accessed at:
http://webarchive.nationalarchives.gov.uk/+/http://www.mod.uk:80/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/DESPSYA/

Security Courses

46. Board level contacts, Security Controllers and their staff should attend the protective security briefings arranged by MOD DE&S DHSY/PSyA. These will complement the training provided by the Defence Industry Security Association (DISA) to Security Controllers and their staff (see below) and other providers of recognised training.

Defence Industry Security Association

47. Board Contacts and Security Controllers and their staff are encouraged to join the Defence Industry Security Association (DISA). The Association is a private, professional association set up to encourage List X Security Controllers to exchange security information and experience. DISA represents to government the security interests and views of its membership, and is often consulted on security policy matters which may affect industry. The DISA is therefore provided the opportunity to contribute before significant changes to security requirements are introduced.

Stage 4 – In-contract monitoring

48. Whether it is the Contracting Authority or MOD DE&S DHSY/PSyA who is responsible for security oversight, regular visits should be made to the contractor throughout the period that protectively marked assets are held on the contractor's premises. The purpose of these visits is to ensure that the required protective security controls are being effectively maintained and to audit Baseline Standard procedures and associated records.

49. It is important that the contractor immediately informs the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate, when changes occur which might affect security, for example, changes of ownership, accommodation, IT, Security Controller or Board Contact.

50. On completion of the contract where there is no further need for the contractor to keep protectively marked assets on its premises, the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate, is responsible for :

    a. Ensuring that all protectively marked assets are removed or securely destroyed.

    b. Recovering any security equipment loaned to the contractor.

    c. Advising MOD DE&S DHSY/PSyA as applicable that the contractor is no longer engaged on protectively marked work.

51. Should a contract be terminated for violation of the security conditions, the Contracting Authority or MOD DE&S DHSY/PSyA, as appropriate, and the Security Division of the Cabinet Office ***must*** both be advised of the circumstances.

Subcontracting

52. Contractors may need to subcontract elements of the main contract to one or more other subcontractors. In many cases it should be possible to do so without involving the subcontractor holding or producing protectively marked material CONFIDENTIAL or above. Subcontracts may need to be placed with:

- UK contractors - refer to paragraph 62
- Overseas agents - refer to paragraph 86
- Overseas contractors - refer to paragraphs 96

International arrangements and procedures

53. Before entering into preliminary discussions or placing subcontracts for work involving 'classified' assets supplied by foreign governments and International Defence Organisations, the Contracting Authority or MOD DE&S DHSY/PSyA (in respect of defence contracts) ***must*** be consulted.

54. Special arrangements are required when subcontracting work involving 'classified' assets supplied by foreign governments and International Defence Organisations. Under various international 'Arrangements', the UK has certain obligations to safeguard such assets. These Arrangements normally include provisions for protectively marked contracts, information exchange, transmission of information and asset handling in general.

55. Special obligations which arise in connection with NATO and other International organisations contracts are dealt with in separate security regulations (see paragraphs 34 & 36 above).

Security Aspects Letter

56. Subcontractor's obligations concerning the protection of protectively marked material ***must*** be the same as those for the main contractor. It is important that before the subcontract is implemented, the main contractor sends the subcontractor a SAL which gives a precise and detailed description and the level of protective marking for each security aspect within the subcontract and a copy sent to the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate.

57. In some instances the Contracting Authority may require security controls in excess of the baseline controls specified elsewhere in the SPF. Where applicable, these additional controls must be reflected in the main sub-contract sent to the subcontractor.

58. The SAL, which normally should be protectively marked no higher than RESTRICTED, should be sent to a named individual, preferably before any work begins, to provide the basis for assessing the appropriate security controls required by the subcontract. Where the subcontractor is List X or has provisional List X status, the SAL should be sent to the subcontractor's Security Controller and a copy sent to the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate.

59. All protective markings on SALs prepared for approved overseas contractors ***must*** include the prefix 'UK' before the classification. See also further information at paragraphs 98 - 106.

60. It is important that all employees connected with the planning and implementation of the security aspects fully understand the SAL and its implications. Where issues are unclear, or it imposes unacceptable or impracticable obligations on the contractor, the subcontractor should be encouraged to seek immediate clarification from the main contractor's Security Controller. A template of the document to be used to challenge defined security aspects is at Appendix 7.

61. Where a subcontractor needs to have access to, hold or produce such assets on its own site, before inviting the subcontractor to tender or giving access to protectively marked assets, the main contractor ***must*** seek approval from the Contracting Authority. If it is proposed that the subcontractor should produce or hold on site any protectively marked hardware assets, including RESTRICTED, appropriate security controls ***must*** be considered for its control, storage, transmission and eventual disposal.

62. When it is considered by the main contractor that a proposed subcontractor is suitable to undertake the contract , the main contractor must submit an Application to Subcontract (see Appendix 5) requesting the Contracting Authority, or in case of defence contracts, MOD DE&S DHSY/PSyA to initiate appropriate List X clearance procedures.

Subcontracting work to companies and consultants in the UK

63. Before entering into preliminary discussions or placing subcontracts for work on contracts involving protectively marked assets CONFIDENTIAL or above, the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate ***must*** be consulted.

64. Subject to any expressed conditions, in the UK subcontracts may be placed with:

- Current List X contractors - refer to paragraph 67
- Non List X contractors - refer to paragraph 73
- Consultants - refer to paragraph 82

65. Until the subcontractor's premises have been granted List X status and visited by the Contracting Authority or MOD DE&S DHSY/PSyA in respect of defence contracts, no protectively marked assets CONFIDENTIAL or above can be released to the subcontractor. Protectively marked information at the level of RESTRICTED may be released and the main contractor is responsible for ensuring that the subcontractor's security controls are appropriate for the protection of such protectively marked assets against compromise. Subsequently, the main contractor ***must*** continue to ensure that protectively marked assets passed to the subcontractor are appropriately protected.

66. On completion of the subcontract the main contractor should inform the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate and unless otherwise agreed with the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate, all assets passed to the subcontractor should be returned to the main contractor for disposal. This is particularly important in the case of short term subcontracts, for example, for reprographic services, where failure to account for all assets could lead to compromise.

Further subcontracting

67. Occasionally there may be a need for a subcontractor to further subcontract work to other UK companies. In such cases, the main contractor must ensure that the appropriate procedures are followed - refer to paragraph 51.

Subcontracting work to a current List X site

68. The main contractor may subcontract work protectively marked RESTRICTED to a UK contractor with List X status, without prior reference to the Contracting Authority, unless it relates to information supplied by foreign governments (see paragraphs 52-54), however, the main contractor is expected to ensure the Contracting Authority is informed of any sub-contracted activities, so that it is aware of what activities is being undertaken where and by whom. The main contractor should consult with the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate, before subcontracting at the level of

CONFIDENTIAL or above to obtain an assurance that the List X status of the proposed subcontractor is appropriate for the level of the subcontract.

Nominated [Defence] subcontractors

69. MOD contracts for defence equipment, for example, warships, missile systems etc, may propose the use of nominated subcontractors for certain aspects of the work. Where disclosure of protectively marked assets is likely to be involved, the subcontractor is likely to already be List X. Any applications to subcontract submitted to MOD DE&S DHSY/PSyA should indicate that the subcontract is required for a 'nominated subcontractor'.

70. Before issuing an ITT or prior to placing a subcontract with another UK company believed to be on List X, the contractor should confirm the subcontractor's List X status with MOD DE&S DHSY/PSyA, and confirm with the subcontractor's Security Controller that the employees involved hold appropriate security clearances. If the proposed subcontractor is not on List X an application to subcontract – Appendix 5 – ***must*** be sent to MOD DE&S DHSY/PSyA, to initiate appropriate List X clearance procedures.

71. The Contracting Authority will include conditions in the contract concerning the subcontracting of work to third party subcontractors. Unless otherwise stated, the Contracting Authority's approval is not required to place subcontracts with another UK List X contractor, providing the work is to be carried out on a site which is appropriately security approved and is List X. However, the main contractor is expected to ensure the Contracting Authority is informed of any sub-contracted activities, so that they are aware of what activities being undertaken where and by whom.

72. Once the subcontractor's competency to undertake the work and the security aspects have been confirmed, and the main contractor has the authority to continue, the subcontractor's Security Controller ***must*** be formally be notified of:

    a. The application of the Official Secrets Acts 1911 to 1989.

    b. The application of DEFCON 659 if appropriate, or other similar or special contractual requirements.

    c. The Secret Matters as covered in a SAL.

73. The contractor should also send a copy of the SAL to the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate.

Subcontracting work to a UK non List X company

Work involving protectively marked information at CONFIDENTIAL or above

74. Before issuing an ITT it may be necessary to enter into preliminary discussions with a prospective non List X subcontractor. These discussions may be entered into without the approval of the Contracting Authority providing that:

    a. There are no contractual conditions precluding such action.

    b. No information protectively marked higher than RESTRICTED is discussed.

    c. No indication is given that the subcontract will involve protectively marked material CONFIDENTIAL or above.

    d. No commitment is entered into, at this stage.

    e. It is understood by the subcontractor that discussions may be terminated without explanation.

It is important not to extend preliminary discussions until approval to subcontract has been received from the Contracting Authority.

Application to Subcontract

75. Where it would be essential to release protectively marked assets above the level of RESTRICTED before the competency of the prospective subcontractor could be assessed through tender, the main contractor ***must*** seek advice from the Contracting Authority or in the case of defence contracts, MOD DE&S DHSY/PSyA .

76. Once the subcontractor's competency to undertake the work has been confirmed, the contractor should:

    a. Where it is considered by the main contractor that a subcontractor meets the criterion to undertake the contract and is also considered to be suitable to be included on List X - the main contractor must submit an Application to Subcontract – Appendix 5, requesting the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate to initiate the List X clearance process. .

b. Arrange for Security Check (SC) clearance or BPSS as appropriate for a minimum number of the subcontractor's employees, normally two, with whom the work has been or will be discussed. When known the results of the requests for security clearance should be notified to the Contracting Authority - no further requests for the clearance of the prospective subcontractor's employees should be made until approval to subcontract has been received from the Contracting Authority. The Contracting Authority or MOD DE&S DHSY/PSyA as appropriate ***must*** be consulted immediately if security clearance for key personnel is refused as this may indicate the unsuitability of the company to work on protectively marked material.

Work involving protectively marked information at the RESTRICTED level

77. The main contractor may subcontract work protectively marked RESTRICTED, to a UK subcontractor without prior reference to the Contracting Authority (so long as the information has not been supplied by a foreign Government (see paragraph 52-54). However, the main contractor is expected to ensure the Contracting Authority is informed of any sub-contracted activities, so that they are aware of what activities being undertaken where and by whom The subcontractor ***must*** be provided with the "UK RESTRICTED Security Conditions - Guidance on the Protection of RESTRICTED Assets" - refer to Appendix 2.

Standard service sub-contracts

78. Occasionally, Standard Service Subcontracts will need to be placed for the provision of regular services such as, reprographics, the processing of film etc. In such cases, where the activity involves Confidential or above assets, when initially requesting inclusion of the prospective subcontractor on List X, the main contractor should state on the Application to Subcontract **-** refer to Appendix 5 - that approval is required for services on an 'as required basis'. The SAL must define the nature of the work relating to the highest level of protective marking involved. Individual orders, placed under the terms of the subcontract, ***must*** define the highest level of protective marking for work requested on that specific order.

79. Once the Contracting Authority's approval to subcontract has been received, the main contractor should notify a security cleared employee, preferably the individual who is to be appointed as the subcontractor's Security Controller, of the:

    a. Application of the Official Secrets Acts 1911 to 1989.

    b. The application of DEFCON 659 (Appendix 1) if appropriate, or other similar or special contractual requirements.

80. The Contracting Authority's approval is not required to place subcontracts with another List X contractor, providing the work is to be carried out on a site which is appropriately security approved and the site's List X status is adequate for the level of protectively marked assets associated with the subcontract. Before issuing an ITT or prior to placing a subcontract with another UK company believed to be on List X, the contractor should confirm the subcontractor's List X status with MOD DE&S DHSY/PSyA and confirm with the subcontractor's Security Controller that the employees involved hold appropriate security clearances. However, the main contractor is expected to ensure the Contracting Authority is informed of any sub-contracted activities, so that they are aware of what activities being undertaken where and by whom.

81. Once the subcontractor's competency to undertake the work and the security aspects have been confirmed, and the main contractor has the authority to continue, the subcontractor's Security Controller ***must*** be formally be notified of:

    a. The application of the Official Secrets Acts 1911 to 1989.

    b. The application of DEFCON 659 if appropriate, or other similar or special contractual requirements.

    c.The Secret Matters, covered in a SAL.

82. The contractor should also send a copy of the SAL to the Contracting Authority or, for defence contracts, to MOD DE&S DHSY/PSyA.

Subcontracting work to a consultant

83. From time to time contractors may need to subcontract work involving protectively marked assets CONFIDENTIAL and above, to a consultant subcontractor who:

    a. Is new to working with protectively marked assets.

b. Is an employee of a another List X contractor

c. Has previously worked for a List X contractor or government or Agency.

84. Before entering into preliminary discussions or giving access to such protectively marked assets the Security Controller ***must*** ensure that a consultant subcontractor is appropriately security cleared.

85. The main contractor's Security Controller ***must*** establish if the consultant has a current valid personnel security clearance. If the consultant has previously worked for a List X contractor, government Department or Agency the Security Controller should approach the appropriate Security Controller, or Security Branch, seeking confirmation in writing of the consultant's personnel security clearance. In the case of a consultant subcontractor employed by a university, the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate may be able to confirm their security clearance status.

86. Where authority is given for a consultant subcontractor to carry out protectively marked work at home, or in other previously approved premises, the main contractor's Security Controller remains responsible for ensuring that security controls are appropriate for the protection of protectively marked assets against compromise; and the provision of approved security furniture.

Overseas Agents

87. For the purpose of this guidance, an overseas agent is an individual employed by, or contracted to a UK company to represent its interests outside the UK. The individual will normally be a foreign national but may be a British National with permanent overseas residency. The term 'overseas agent' does not apply to a List X contractor's employee on temporary overseas detachment, who remains on the contractor's payroll.

88. Only in exceptional circumstances will the Contracting Authority approve an overseas agent to hold protectively marked assets, including RESTRICTED, since such assets are at greater risk of compromise outside the UK.

89. A List X contractor who considers that there are exceptional circumstances justifying the passing of protectively marked assets, including RESTRICTED, to an overseas agent, ***must*** seek prior written approval from the Contracting Authority. Such approval is only likely to be given if:

a. the Contracting Authority is convinced that there is a genuine 'need to know' for the assets to be released to the overseas agent

b. there is an arrangement between the UK government and the overseas agent's government, for sending protectively marked assets to that country

90. Where access to Confidential or above information is exceptionally approved to be released by the Contracting Authority and it is required to be held on the premises of the overseas agent this will **only** be acceptable when the overseas agents' premises is located in NATO and Commonwealth countries, or those countries with which the UK has a General Security Agreement/Arrangement where an assurance of the security clearance of the overseas agent's premises may be obtained. Such approval will only be granted if the premises on which the protectively marked assets are to be held have been granted an appropriate facility security clearance by the country's National Security Authority/Designated Security Authority.

Personnel security clearance/approvals for overseas agents and their employees

91. Where the overseas agents' premises has been granted a facility security clearance the responsibility for granting the personnel security clearance of the overseas agent and any employees rests with the National Security Authority/Designated Security Authority of the country concerned.

92. Where the requirement is for the overseas agent to have access to CONFIDENTIAL or above information only on the premises of the UK List X site such access may only be granted following an assurance that the individual has been granted an appropriate security clearance by their National Security Authority/Designated Security Authority. Where no foreign security clearance exists access may be granted only when the List X contractor undertakes a BPSS and the full requirements have been successfully satisfied.

Safeguarding protectively marked assets sent to an overseas agent

93. The following actions ***must*** be taken to safeguard protectively marked assets sent to an overseas agent:

a. All protectively marked assets approved for sending to overseas agents ***must*** be transmitted in accordance with procedures agreed between the UK and receiving governments.

b. A record of all protectively marked material held by an overseas agent should be kept by both the List X contractor and the overseas agent.

c.Instructions ***must*** be provided to the overseas agent that the protectively marked assets may only be discussed with an appropriately cleared representative of the government of the country in which the overseas agent is operating - where there is any doubt about the official status of such an individual, the overseas agent should consult the local British Embassy, Consulate or High Commission.

94. It is important that an overseas agent does not pass protectively marked assets to a third party foreign government. In such cases the List X contractor should first seek the written approval of the Contracting Authority. Only if approval is received, may such assets be released and ***must*** only be transmitted through approved/official government-to-government channels.

Access to protectively marked assets by overseas agents in the UK

95. A request for an overseas agent to visit the List X contractor for briefing ***must*** be referred to the Contracting Authority for approval.

96. An overseas agent visiting the UK for a briefing by the contractor may be given access to protectively marked assets providing the contractor is assured that the overseas agent has a 'need to know' and is appropriately security cleared or has been granted a BPSS.

Subcontracting work to companies outside the UK

Work involving protectively marked information at CONFIDENTIAL level or above

97. The Contracting Authority's approval is required before releasing any protectively marked assets, or proceeding with any discussions, ITT or subcontracting with companies outside the UK.

98. When it is considered necessary to subcontract protectively marked work CONFIDENTIAL or above to companies outside the UK, the main contractor ***must***:

a. Conduct all preliminary discussions as above with the exception that, the approval of the Contracting Authority is needed before releasing any protectively marked assets, including RESTRICTED assets.

b. Send the Contracting Authority or in the case of defence contracts to MOD DE&S DHSY/PSyA an Application to Subcontract – Appendix 5.

99. The Contracting Authority or MOD DE&S DHSY/PSyA as appropriate will notify the main contractor in writing of its approval or refusal for the release of protectively marked assets and subsequently, to subcontract. Where approval is given, a reference to standard conditions of contract relating to the security aspects or to the UK Official Secrets Acts is not appropriate, the Contracting Authority will provide relevant wording of the security conditions to be included in the subcontract.

100. Two copies of the ITT or subcontract and two copies of the SAL must be sent to the Contracting Authority. The Contracting Authority will arrange for the National/Designated Security Authority of the country concerned to oversee the security aspects of the work to be undertaken on the contract.

Work involving protectively marked information at RESTRICTED level

101. With the prior written approval of the Contracting Authority (in respect of the MOD the authority is the relevant Project Team), the main contractor may subcontract work involving protectively marked information at RESTRICTED level to an overseas subcontractor. With the exception of those destinations outlined in paragraph 102 below, the application to subcontract may be in the form of a simple written request or the Application to Subcontract at Appendix 5. If approval is granted the main contractor ***must*** provide the subcontractor with guidance on the protection of UK RESTRICTED Information - Appendix 6.

102. Because of how RESTRICTED information is required to be treated in the countries concerned an application for approval to subcontract work involving MOD information at RESTRICTED level to contractors in Australia, , Czech Republic, Egypt, Estonia, Greece, Hungary Israel, , Japan, Luxembourg, Romania and the Slovak Republic also require prior security approval. An Application to Subcontract - Appendix 5 ***must*** therefore be submitted to MOD DE&S DHSY/PSyA. Should approval be granted the main contractor ***must*** provide the subcontractor with guidance on the protection of UK RESTRICTED Information - Appendix 6.

Preliminary discussions, collaboration or teaming agreements or joint ventures with companies outside the UK

103. In so far as preliminary discussions, collaboration or teaming agreements with companies overseas are concerned, for example, the Euro Fighter project, the contractor ***must*** send the Contracting Authority an Application to Subcontract- Appendix 5. The Contracting Authority will notify the contractor in writing of its approval or refusal to proceed.

104. No protectively marked assets should be released, ITT issued or discussions relating to protectively marked work conducted, including RESTRICTED, until written approval has been received.

105. Where a contractor currently engaged in contract work involving protectively marked assets is contemplating a merger with one or more companies in a 'joint venture', the Security Controller ***must*** advise in writing to the Contracting Authority or MOD DE&S DHSY/PSyA before the merger or discussions concerning the contract takes place. The other companies involved ***must*** not be given access to any protectively marked assets or be informed of the terms of the contract until written approval has been received from the Contracting Authority or MOD DE&S DHSY/PSyA as appropriate.

Arrangements relating to feasibility studies, project definition, development, production and support of protectively marked defence equipment

106. These arrangements are normally in the form of a Memorandum of Understanding which relates to major collaborative defence projects involving two or more nations and their respective defence contractors. National security laws and regulations apply to all parties although detailed Project Security Instructions may be developed when necessary.

List of Appendices

Appendix 1

DEFCON 659
Security Measures

Definition

1. In this Condition:

a) 'Secret Matter' means any matter connected with the Contract, or its performance which is designated in writing by the Authority as 'Top Secret', 'Secret', or 'Confidential', and shall include any information concerning the content of such matter and anything which contains or may reveal that matter.
b) 'Employee' shall include any person who is an employee or director of the Contractor or who occupies the position of a director of the Contractor, by whatever title given.

The Official Secrets Acts

2. The Contractor shall:

a) take all reasonable steps to ensure that all Employees engaged on any work in connection with the Contract have notice that the Official Secrets Acts 1911-1989 apply to them and will continue so to apply after the completion or termination of the Contract; and
b) if directed by the Authority, ensure that any Employee shall sign a statement acknowledging that, both during the term of the Contract and after its completion or termination, he is bound by the Official Secrets Acts 1911-1989 (and where applicable by any other legislation).

Security Measures

3. Unless he has the written authorisation of the Authority to do otherwise,
neither the Contractor nor any of his Employees shall, either before or after the completion or termination of the Contract, do or permit to be done anything which they know or ought reasonably to know may result in Secret Matter being disclosed to or acquired by a person in any of the following categories:

a) who is not a British citizen;
b) who does not hold the appropriate authority for access to the protected matter;
c) in respect of whom the Authority has notified the Contractor in writing that the

Secret Matter shall not be disclosed to or acquired by that person;

d) who is not an Employee of the Contractor;

e) who is an Employee of the Contractor and has no need to know the information for the proper performance of the Contract.

4. Unless he has the written permission of the Authority to do otherwise, the Contractor and his Employees shall, both before and after the completion or termination of the Contract, take all reasonable steps to ensure that:

a) no photograph of, or pertaining to, any Secret Matter shall be taken and no copy of or extract from any Secret Matter shall be made except to the extent necessary for the proper performance of the Contract;

b) any Secret Matter is at all times strictly safeguarded in accordance with the Security Policy Framework and upon request, is delivered up to the Authority who shall be entitled to retain it.

A decision of the Authority on the question of whether the Contractor has taken or is taking reasonable steps as required by this Clause, shall be final and conclusive.

5. The Contractor shall:

a) provide to the Authority:

i. upon request, such records giving particulars of those Employees who have had at any time, access to any Secret Matter that is required to be kept in accordance with sub-Clause 4.b);

ii. upon request, such information as the Authority may from time to time require so as to be satisfied that the Contractor and his Employees are complying with his obligations under this Condition, including the measures taken or proposed by the Contractor so as to comply with his obligations and to prevent any breach of them;

iii. full particulars of any failure by the Contractor and his Employees to comply with any obligations relating to Secret Matter arising under this Condition immediately upon such failure becoming apparent;

b) ensure that, for the purpose of checking the Contractor's compliance with the obligation in sub-Clause 4.b), a representative of the Authority shall be entitled at any time to enter and inspect any premises used by the Contractor which are in any way connected with the Contract and inspect any document or thing in any such premises, which is being used or made for the purposes of the Contract. Such representative shall be entitled to all such information as he may reasonably require.

6. If at any time either before or after the completion or termination of the Contract, the Contractor or any of his Employees discovers or suspects that an unauthorised person is seeking or has sought to obtain information directly or indirectly concerning any Secret Matter, the Contractor shall forthwith inform the Authority of the matter with full particulars thereof.

Subcontracts

7. If the Contractor proposes to make a subcontract which will involve the disclosure of Secret Matter to the subcontractor, the Contractor shall:

a) submit for approval of the Authority the name of the proposed subcontractor, a statement of the work to be carried out and any other details known to the Contractor which the Authority shall reasonably require;

b) incorporate into the subcontract the terms of the Appendix to this Condition and such secrecy and security obligations as the Authority shall direct. In the appendix 'Agreement' shall mean the 'Subcontract', 'First Party' shall mean the 'Contractor' and 'Second Party' shall mean the 'Subcontractor';

c) inform the Authority immediately he becomes aware of any breach by the subcontractor of any secrecy or security obligation and, if requested to do so by the Authority, terminate the subcontract.

Termination

8. The Authority shall be entitled to terminate the Contract immediately if:

a) the Contractor is in breach of any obligation under this Condition; or

b) the Contractor is in breach of any secrecy or security obligation imposed by any other contract with the Crown;

where the Authority considers the circumstances of the breach jeopardise the secrecy or security of the Secret Matter.

ANNEX TO DEFCON 659
Security Measures

Provisions to be included in relevant Subcontracts

Definition

1. In this Condition:

a) 'Secret Matter' means any matter connected with the Agreement, or its performance which the First Party informs the Second Party in writing has been designated by the Authority as 'Top Secret', 'Secret', or 'Confidential', and shall include any information concerning the content of such matter and anything which contains or may reveal that matter;

b) 'Employee' shall include any person who is an employee or director of the Second Party or who occupies the position of a director of the
Second Party, by whatever title given;

c) the 'Authority' means the Secretary of State for Defence.

The Official Secrets Acts

2. The Second Party shall:

a) take all reasonable steps to ensure that all Employees engaged on any work in connection with the Agreement have notice that the Official Secrets Acts 1911-1989 apply to them and will continue so to apply after the completion or termination of the Agreement; and

b) if directed by the First Party or the Authority, ensure that any Employee shall sign a statement acknowledging that, both during the term of the Agreement and after its completion or termination, he is bound by the Official Secrets Acts 1911-1989 (and where applicable by any other legislation).

Security Measures

3. Unless he has the written authorisation of the Authority to do otherwise, neither the Second Party nor any of his Employees shall, either before or after the completion or termination of the Agreement, do or permit to be done anything which they know or ought reasonably to know may result in Secret Matter being disclosed to or acquired by a person in any of the following categories:

a) who is not a British citizen;
b) who does not hold the appropriate authority for access to the protected matter;
c) in respect of whom the Authority has notified the Second Party in writing that the Secret Matter shall not be disclosed to or acquired by that person;
d) who is not an Employee of the Second Party;
e) who is an Employee of the Second Party and has no need to know the information for the proper performance of the Agreement.

4. Unless he has the written permission of the Authority to do otherwise, the Second Party and his Employees shall, both before and after the completion or termination of the Agreement, take all reasonable steps to ensure that:
a) no photograph of, or pertaining to, any Secret Matter shall be taken and no copy of or extract from any Secret Matter shall be made except to the extent necessary for the proper performance of the Agreement;
b) any Secret Matter is at all times strictly safeguarded in accordance with the Security Policy Framework and upon request, is delivered up to the Authority who shall be entitled to retain it.

A decision of the Authority on the question of whether the Second Party has taken or is taking reasonable steps as required by this Clause, shall be final and conclusive.

5. The Second Party shall:

a) provide to the Authority:
i. upon request, such records giving particulars of those Employees who have had at any time, access to any Secret Matter that is required to be kept in accordance with sub-Clause 4.b);
ii. upon request, such information as the Authority may from time to time require so as to be satisfied that the Second Party and his Employees are complying with his obligations under this Condition, including the measures taken or proposed by the Second Party so as to comply with his obligations and to prevent any breach of them;
iii. full particulars of any failure by the Second Party and his Employees to comply with any obligations relating to Secret Matter arising under this Condition immediately upon such failure becoming apparent;
b) ensure that, for the purpose of checking the Second Party's compliance with the obligation in sub-Clause 4.b), a representative of the First Party or the Authority shall be entitled at any time to enter and inspect any premises used by the Second Party which are in any way connected with the Agreement and

inspect any document or thing in any such premises, which is being used or made for the purposes of the Agreement. Such representative shall be entitled to all such information as he may reasonably require.

6. If at any time either before or after the completion or termination of the Agreement, the Second Party or any of his Employees discovers or suspects that an unauthorised person is seeking or has sought to obtain information directly or indirectly concerning any Secret Matter, the Second Party shall forthwith inform the Authority of the matter with full particulars thereof.

Subcontracts

7. If the Second Party proposes to make a subcontract which will involve the disclosure of Secret Matter to the subcontractor, the Second Party shall:

a) submit for approval of the Authority the name of the proposed subcontractor, a statement of the work to be carried out and any other details known to the Second Party which the Authority shall reasonably require;
b) incorporate into the subcontract the terms of this Condition and such secrecy and security obligations as the Authority shall direct;
c) inform the Authority immediately he becomes aware of any breach by the subcontractor of any secrecy or security obligation and, if requested to do so by the Authority, terminate the Agreement.

Termination

8. The First Party shall be entitled to terminate the Agreement immediately if:

a) the Second Party is in breach of any obligation under this Condition; or

b) the Second Party is in breach of any secrecy or security obligation imposed by any other contract with the Crown;

where the Authority considers the circumstances of the breach jeopardise the secrecy or security of the Secret Matter and notifies its contractor accordingly.

Appendix 2

UK Restricted Security Conditions - Guidance for UK Contractors on the Protection of UK Restricted Assets

Definitions

1. The term "Authority" means the Contracting Authority.

Security Grading

2. The Authority shall issue a RESTRICTED Aspects Letter which shall define the RESTRICTED matter that is furnished, or which is to be developed, under this Contract. The Contractor shall mark all RESTRICTED documents which he or she originates or copies during the Contract with the equivalent national grading.

Official Secrets Acts

3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract have notice that these statutory provisions apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

Protection of RESTRICTED Information

4. RESTRICTED information shall be protected in a manner to promote discretion in order to avoid unauthorised access. The Contractor shall take every effort to prevent the loss or compromise of the information or deliberate or opportunist attack.

5. Disclosure of RESTRICTED information shall be strictly in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than a person directly employed by the Contractor or sub-Contractor or Service provider.

6. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the

Authority and must be returned on completion of the Contract or if directed by the Authority, destroyed in accordance with paragraph 23.

7. When not in use RESTRICTED documents shall be stored under lock and key.

Access

8. Access shall be confined to those individuals who have a "need-to-know" and whose access is essential for the purpose of his or her duties.

9. The Contractor shall ensure that all individuals having access to RESTRICTED information meet legal requirements in respect of immigration and the right to work in the UK and have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to RESTRICTED information. Further details and the full requirements of the BPSS can be found at the Cabinet Office website within the Security Policy Framework at Mandatory Requirement 23: http://www.cabinetoffice.gov.uk/spf

Transmission of RESTRICTED Information

10. RESTRICTED documents shall be transmitted, both within and outside company premises in such a way as to make sure that no unauthorised person has access. They may be sent by ordinary post in a single envelope. The word RESTRICTED must **NOT** appear on the envelope. The envelope should bear a company stamp that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

11. Advice on the transmission of RESTRICTED documents abroad or any other general advice including the transmission of RESTRICTED hardware should be sought from the Authority.

Use of Communications and IT Systems

12. The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure that they are blocked.

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

14. The following describes the minimum Accreditation security requirements for processing and accessing RESTRICTED information on IT systems.

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

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

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

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

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

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

e. **Data Transmission:** RESTRICTED information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using commercial encryption devices accepted by the Authority. Advice on encryption requirements for the transmission of RESTRICTED information shall be sought from the Authority However, in cases where there is a pressing business need, telephone conversations, video conferencing or facsimile transmissions containing RESTRICTED information may be in clear text. In cases where a pressing business need has been identified, both parties need to accept that there exists the potential for a risk of compromise. When taking a decision to communicate RESTRICTED information in this way they should be aware of the impact of disclosure.

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

(1) The following events shall always be recorded:

I. All log on attempts whether successful or failed.

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

III. The creation, deletion or alteration of access rights and privileges.

IV. The creation, deletion or alteration of passwords.

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

I. Type of event,

II. User ID,

III. Date & Time

IV. Device ID

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

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

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

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

(2) Defined Business Contingency Plan

(3) Data backup with local storage

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

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

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

I. "Unauthorised access to this computer system may constitute a criminal offence"

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

j. **Internet Connections**: Computer systems shall not be connected direct to the Internet unless protected by a firewall which is acceptable to the Authority's Security Officer.

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

Laptops

15. Laptops holding any information supplied or generated as a consequence of the contract are to have, as a minimum, a FIPS 140-2 approved full disk encryption solution installed.

16. Unencrypted laptops not on a secure site[2] are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Business Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration.

17. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt the term "drives" includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.

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

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

Loss

20. Any loss of RESTRICTED information shall be reported without delay to the Authority.

Sub-Contracts

[2] Secure sites are defined as either Government premises or secured offices on the contractor premises

21. The Contractor may Sub-contract any elements of this Contract to Sub-contractors within the United Kingdom notifying the Authority. When doing so these security conditions shall be incorporated within the Sub-contract document. The prior approval of the Authority shall be obtained should the Contractor wish to Sub-contract any elements of the Contract to a Sub-contractor in another country.

Publicity Material

22. Contractors wishing to release any publicity material or display hardware that arises from this contract, whether directly or indirectly, must seek the prior approval of the Contracting Authority. Publicity material includes open publication in the contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the Authority, or any other government department. For Private Venture Defence Related Material to be released at exhibitions, contractors must seek the prior approval of DBR-DefSy(S&T/Ind).

Destruction

23. As soon as soon as no longer required RESTRICTED information/material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Unwanted RESTRICTED information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation

24. Advice regarding the interpretation of the above requirements should be sought from the Authority.

Audit

25. Where considered necessary by the Authority the Contractor shall permit the inspection of the Contractors processes and facilities to ensure compliance with these requirements.

Appendix 3

General Security Advice For Companies Bidding for Government Contracts Involving Assets Protectively Marked CONFIDENTIAL or above

1. The contract to which this Invitation to Tender relates will require the successful bidder to hold government material bearing a protective marking of **CONFIDENTIAL** or above on its premises. If you decide to submit a bid and are subsequently awarded the contract you will be required to protect these assets to standards laid down by HM Government. To achieve these standards you may need to provide, in addition to your existing security controls, certain other controls and procedures which could involve you in additional expense. Such controls will depend upon the particular requirements of the contract and the nature of your site. If you are awarded the contract a Security Adviser will be appointed who will visit you and advise you of these details but, in advance of this, the following paragraphs are intended to give you a broad indication of what will be required.

Physical Security

2. To safeguard the government material **out of working hours** you will be required to store the material in approved lockable containers (filing cabinets, cupboards etc). In certain circumstances one container may be provided to you on free loan but you will be required to insure it against possible damage or loss. These containers will need to be housed in a 'secure area', that is, an area with a defined perimeter. This secure perimeter may be either the outer walls, doors and windows or a complete building, or the walls and doors which form an area within a building. The perimeter will need to be protected by good quality locks on in-use doors, window locks where appropriate, and supplementary locking devices on emergency exits. If the material is marked **SECRET** and above, it is probable that either an alarm system or patrolling guards will be required to provide an adequate level of protection during silent hours.

3. If you already have an alarm system installed by a reputable company it will probably be satisfactory although it may require some minor upgrading. In some circumstances for the system to be acceptable you may also need to be able to provide a response to an alarm within 15 minutes. Most companies achieve this by having their system connected to a central station which alerts a nominated key-holder and the local police.

4. In some circumstances more complex measures, for example, window bars, secure rooms etc, may be required, but it may only be possible to determine such requirements

when the Security Adviser visits.

5. During working hours you will need to provide access control which will prevent unauthorised persons having access to the protectively marked material either deliberately or inadvertently. Depending on the nature of the contract and your site, this may vary between confining the work to a lockable office to installing access control locks to all of the doors providing access to a designated area or building. You will also need to have measures for controlling the movements of visitors within your site.

Document Security

6. Apart from storing material in approved containers when not in use you will need to set up a system of document control which will ensure that a record is kept of all material bearing the higher levels of protective marking held at your site, including any which you produce yourself. The system will also need to keep track of such material if it moves within your site and will have to ensure that any such material which leaves your site does so properly packaged and transported by approved means. The system will also need to ensure that only approved persons have access to protectively marked material.

Finally you will need to carry out spot checks at regular intervals to ensure that the material recorded as being on your site is present.

Personnel Security

8. All persons requiring access to the protectively marked material must be specifically authorised to do so. Such authorisation may necessitate certain specified checks being carried out by the Contracting Authority or their agent. As a minimum you will be required to satisfy yourself of the identity of the individual by having sight of specified documents such as passports, birth certificates etc, and their reliability by obtaining references from previous employers and/or other nominated persons. You will be required to keep records of all those employees who have been authorised.

9. In certain cases the Contracting Authority may refuse to authorise individuals who are not British Nationals or whose reliability is doubtful because, for example, they have a significant criminal record.
10. Full details of these procedures will be given to you by your Security Adviser.

Computer Security

11. The requirements for security controls relating to computer systems are particularly dependent upon the system or equipment in use and the nature of the contract.

12. In general the same basic rules apply in these circumstances as apply to the protection of documents, that is, controls must be in place to ensure that only authorised persons can gain access to protectively marked data, and the data, whether on magnetic media or within the machine or network, must be safeguarded when not in use. The easiest way of achieving the required state is to use stand-alone PCs, fitted with removable hard disks and located within the secure area. Small networks confined to the secure area are also usually easy to accommodate, provided that the hard disks and or other forms of magnetic media are readily removable. Networks extending outside the secure area may require additional technical controls, particularly if there are off-site links are less likely to be acceptable. In all the above situations some security software is also likely to be needed. You are strongly advised not to purchase any computing equipment in support of the contract in advance of the initial visit by your Security Adviser.

13. If the contract does require you to hold protectively marked material on computer you will also be required to produce certain standardised supporting documentation and obtain accreditation of all IT systems holding such material.

Organisation

14. To manage government security issues within your company you will be required to nominate two individuals, a Security Controller to be responsible for all day-to-day aspects and a Board Level Contact who accepts responsibility for security on behalf of the company and to whom the Security Controller will report. In all except very large companies the Security Controller's task is unlikely to be a full-time one and in smaller companies the roles of the Board Level Contact and the Security Controller are frequently combined. Larger agencies may wish to nominate a Clearance Contact to deal with the paperwork involved in maintaining personnel security.

Appendix 4

SECURITY ASPECTS LETTER

Messrs . . . . . .
. . . . . .
. . . . . .
For the attention of . . . . . .(insert name of Security Controller or senior management contact in the cases of non-List X or overseas companies)

Dear . . . . . .

SUBJECT AND TENDER / SUBCONTRACT / ORDER NO.:

1. The above tender / subcontract / order arises from a United Kingdom government contract and will involve your company holding UK protectively marked material (replace "protectively marked" with "classified" for overseas companies). It is a condition of this tender / subcontract / order that this material must be protected. The standard of protection required has been notified to you separately and varies with the level of protective marking. Material passed to you will bear the protective marking appropriate to it. However to assist you in allocating any necessary protective marking to material which your company may produce during the course of the tender / subcontract / order and thus enable you to provide the appropriate degree of protection to it, this letter formally advises you of the correct protective marking to apply to the various aspects of the tender / subcontract / order.

2.The aspects of the tender / subcontract / order which require to be protectively marked are:-

Aspect* **Protective Marking*** (provide full and detailed information)

3. If the subcontract / order contains a Condition of Clause referring to "Secret Matter" this Secret matter is defined as the Aspects listed above.

4. You are requested to acknowledge receipt of this letter and to confirm that the level of protective marking associated with the various aspects listed above have been brought to the attention of the person directly responsible for the security of this tender / subcontract / order, that they are fully understood, and that the required security controls in the contract security conditions can and will be taken to safeguard the material concerned.

5. If you have any difficulty in interpreting the meaning of the above aspects or in safeguarding the materials, will you please let me know immediately and send a copy of your letter to your Security Adviser[3].

6. A copy of this letter has been sent to your Security Adviser.[4]

[3] *Reference to the Security Adviser should only be made in SALs addressed to List X companies.*
Note: If the Contracting Authority for the main contract requires that protective security controls above the baseline defined in the Security Policy Framework be applied to this subcontract these should be set out in a separate paragraph in the SAL.
[4] Delete paragraph if SAL is being provided to a Non List X or overseas contractor.

Appendix 5

APPLICATION TO SUB-CONTRACT OR COLLABORATE ON PROTECTIVELY MARKED WORK (ALSO KNOWN AS F1686)

PART 1

A	From: full name and address of contractor submitting application Telephone no:		
B	This application concerns: (tick appropriate box)		
1	A sub-contractor in the United Kingdom	☐	Complete Parts 1, 2 & 3
2	A sub-contractor overseas	☐	Complete Parts 1, C and D, Part 3
3	A pre-contract collaboration/teaming agreement with overseas contractor	☐	Complete Parts 1, C, Part 3
C	Full name and address of selected company		
D	Full name and address of selected manufacturer (if different from C)		
E	Registration no. of the company & VAT no.: Reg No: VAT No:		

F	Names under which the company has previously traded (if applicable):

G	Full name, address, registration and VAT no. of parent and/or holding company:
H	Full name, address, registration and VAT no. of each company holding more than one fifth of the paid up shares, preference shares or loan capital.
I	Date of formation of business and brief history:
J	Representative(s) (maximum of two) of sub-contractor with whom proposed work has been/will be discussed:

	Full name:	Full name:
	AA number (if known):	AA number (if known):
	Position in company:	Position in company:

PART 2

K	Please provide in the boxes below details of Chairman, Deputy Chairman, all Directors (indicating specifically those who hold executive appointments), and Company Secretary. Information should also be provided for individuals holding more than one fifth of the paid up shares, preference shares or loan capital.

1. SURNAME a) Now				
(b) At birth if different from (a)				
(c) All other surnames used				
2. FULL FORENAMES				
3. PLACE OF BIRTH Including county, state and country				

4. DATE OF BIRTH				
5. NATIONALITY (a) Now				
(b) At any time if different from (a)				
(c) If naturalised state number & date of certificate				
6. ADDRESS (a) Full permanent address				
7. POSITION IN COMPANY				

PART 3

L	Does the information relate to:	1	UK government contract?	☐	Complete M to Q
		2	Private venture work?	☐	Complete M to P
		3	NATO contract?	☐	Complete M to R
		4	Collaboration discussions	☐	Complete M to P
M	Maximum level of release of protectively marked material:				

N	Name and/or reference of project:		
O	Description of work to be carried out:		
P	Full name and address of project authority: Telephone no:	Q	Contracting authority: Contract no:
R	Name of NATO contracting authority:		

Name of Security Controller: ……..

Signature: …… Date: …….

Appendix 6

UK Restricted Security Conditions - Guidance for Overseas Contractors on the Protection of UK Restricted Assets

Definitions

1. The term "Authority" means the Contract Authority.

Security Grading

2. The Authority shall issue a Security Aspects Letter (SAL) which shall define the UK RESTRICTED matter that is furnished, or which is to be developed, under this Contract. The Contractor shall mark all UK RESTRICTED documents that he or she originates or copies during the Contract in accordance with the SAL.

Protection of UK RESTRICTED Information

3 UK RESTRICTED information shall be protected in a manner to promote discretion in order to avoid unauthorised access. The contractor shall take every effort to prevent the loss or compromise of the information or deliberate or opportunist attack.

4. Except with the consent in writing of the Authority, the Contractor shall not disclose the Contract or any of its provision to any person other than a person directly employed by the Contractor or sub-Contractor or Service Provider.

5. Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any information issued or furnished by or on behalf of the Authority otherwise than for the purpose of the Contract, and, save as provided for in Clause 6 the Contractor shall not make use of any article or part thereof similar to the Articles for any other purpose.

6 Subject to any rights of Third Parties, nothing in this Condition shall, restrict the Contractor from using any specifications, plans, drawings and other documents generated outside of this Contract.

7 Any samples or patterns or any specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and must be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 22.

8. When not in use UK RESTRICTED documents shall be stored under lock and key.

Access

9. Access to UK RESTRICTED information shall be confined to those individuals who have a “need-to-know” and whose access is essential for the purpose of his or her duties.

10. The Contractor shall ensure that all individuals requiring access to UK RESTRICTED information have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws and regulations. This is in keeping with the core principles set out in the HMG Baseline Personnel Security Standard (BPSS).

Loss

11. Any loss of a UK RESTRICTED document shall be reported without delay to the Authority.

Dispatch of Information

12. UK RESTRICTED documents shall be transmitted in such a way as to make sure that no unauthorised person has access. Postal transmissions outside of the company must be in at least one envelope/package; Commercial Couriers may be used. The word “RESTRICTED” must **not** appear on the envelope.

Use of Communications and IT Systems

13. The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure that they are blocked.

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

15. The following describes the minimum Accreditation security requirements for processing and accessing UK RESTRICTED information on IT systems.

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

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

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

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

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

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

e. **Data Transmission**: UK RESTRICTED information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using commercial encryption devices accepted by the Authority. Advice on encryption requirements for the transmission of UK RESTRICTED information shall be sought from the relevant UK security organisation via the Authority. However, where there is a pressing business need, telephone conversations, video conferencing or facsimile transmissions containing UK RESTRICTED information may be in clear text. In such circumstances where a pressing business need has been identified, both parties need to accept that there exists the potential for a risk of compromise. When taking a decision to communicate UK RESTRICTED information in this way they should be aware of the impact of disclosure..

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

(1) The following events shall always be recorded:

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

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

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

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

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

(a) Type of event,

(b) User ID,

(c) Date & Time

(d) Device ID

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

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

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

(1) Provide general protection against normally foreseeable accidents/mishaps and known

recurrent problems (e.g. viruses and power supply variations)

(2) Defined Business Contingency Plan

(3) Data backup with local storage

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

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

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

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

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

j. **Internet Connections**: Computer systems shall not be connected direct to the Internet unless protected by a firewall (a software based personal firewall is the minimum).

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

Laptops

16. Laptops holding any information supplied or produced as a consequence of the contract are to have, as a minimum, a FIPS 140-2 approved full disk encryption solution installed.

17. Unencrypted laptops not on a secure site[5] are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed.

18. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt the term "drives" includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.

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

20. Portable CIS devices holding data belonging to the Authority are not to be left

[5] Secure sites are defined as either Government premises or secured office on the contractor premises

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

Sub-Contracts

21. The Contractor may sub-contract any elements of this Contract to Sub-contractors within its own country or the United Kingdom. When doing so, these security conditions shall be incorporated within the Sub-contract document. The prior approval of the Authority shall be obtained should the Contractor wish to sub-contract any elements of the Contract to a contractor in a third country.

Destruction

22. As soon as soon as no longer required, UK RESTRICTED information/material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Unwanted UK RESTRICTED information/material that cannot be destroyed in such a way shall be returned to the Authority.

Interpretation

23. Advice regarding the interpretation of the above requirements should be sought from the Authority

Appendix 7

Doubtful Security Grading

From:..... To .....

Subject Contract Reference Number

Dear Sir

1. We acknowledge receipt of your letter/report on the above subject which is receiving attention. The reason for the security grading of ..... defined in the SAL is not, however, clear to us.

2. From our knowledge of the subject and the written definition of the secret matter in the SAL, reference ……..... we consider that a grading of ..... is more appropriate.

3. I would be grateful if you could review this security grading and confirm in writing if this it is considered correct or issue a revised SAL if it is determined that a different grading is more appropriate so that we know precisely what information must be safeguarded under DEFCON 659.

Yours faithfully

Copy to:

Contracting Authority or in respect of defence contracts to MOD DE&S DHSY/PSyA