**ANNEX A TO**
**SCHEDULE 11 TO**
**709282452**




# MEMORANDUM OF SECURITY FOR MOD CONTRACTORS

**V2 – APRIL 2014**

**CONTENTS**


| Subject | Page |
|---|---|
| Introduction | 3 |
| Security Advice | 3 |
| Conditions of Contracts relating to Security | 4 |
| Protective Markings | 5 |
| Security Grading | 13 |
| Personnel Security | 13 |
| Document Security | 13 |
| Physical Security | 16 |
| Security Breaches | 17 |

**Introduction**

1. **This Memorandum outlines the security precautions and requirements which must be taken by companies who are required to access or hold MoD classified information at the SECRET or above level; or who are taking part in tender exercise or contract negotiations where PMM at that level and may be required to be held.**

2. **To facilitate their tender, this Memorandum also provides guidance to un-cleared contractors who are invited to tender for a contract that will require access to classified information at the SECRET or above level on the minimum security requirements that they will be required to apply should a contract involving such information be placed with the company. The award of such a contract will require the contractor to be granted a Facility Security Clearance before the contract can be formally awarded.**

3. **Definitions of classifications are set out at Para 16.**

**Security Advice**

4. **During pre-contract negotiations or the life of a contract that involves MoD classified information at the SECRET or above level, general security enquiries or clarification on the requirements detailed in this Memorandum, should be addressed to the MoD DE&S Defence Equipment & Support – Infra Security Advice Centre (DE&S SAC)**

**DE&S PSyA -Security Advice Centre**
**MoD Abbey Wood**
**Poplar-1, #2004,**
**Abbeywood**
**Bristol**
**BS34 8JH**

**Tel: 030 67934378**
**Fax: 030 67934925**
**Mail to**: **DES PSyA-SecurityAdviceCentre@mod.uk**

5. **DE&S-SAC is responsible for undertaking the security implementation aspects of industrial security including overseeing the security aspects of defence contracts involving MoD classified information at the SECRET or above level undertaken by MoD contractors.**

6. **Officers of the DE&S, in their capacity as Advisers on security in industry, visit a contractor who has received his or her first contract (and intermittently thereafter) involving MoD classified information at SECRET or above level as soon as possible after the contract has been placed. They inform the contractor on the security measures which must be taken to safeguard the "SECRET Matter" of the contract in accordance with the obligations imposed by DEFCON 659A. Advisers have no powers to visit or inform a contractor until a contract at SECRET or above level has been let.**

7. **It should be noted that the level of advice and support provided will be limited until the "SECRET Matter" of the contract has been notified to the contractor.**

8. **Contractors undertaking MoD contracts involving MoD classified information at the level of OFFICIAL-SENSITIVE should contact their MoD contracting authority in the first instance for security advice.**

**Conditions of Contracts Relating to Security[6]**

9. **There are two contract conditions which relate to security. These are:**

**DEFCON 531 - Disclosure of information**

**DEFCON 659A - Security Measures**

**DEFCON 660 - Official Sensitive**

10. **DEFCON 659A is applicable only to those contracts which involve the disclosure to contractors of MoD classified information, SECRET or TOP SECRET.**

11. **This Memorandum is primarily concerned with setting out the details of the requirements on those contractors who are required to handle work, which is subject to DEFCON 659A, however, some of the information contained will also be applicable to those companies who are only handling MoD classified information at the OFFICIAL-SENSITIVE level.**

**DEFCON 531 (Disclosure of Information)**

12. **All Government contracts are subject to DEFCON 531 covers any information and requires the contractor to safeguard information provided to it by the MoD and to ensure that it's employees are aware of their responsibilities for such safeguards before they receive the information. There is a mutual obligation to treat in confidence all information disclosed in connection with or under the contract.**

**DEFCON 659A (Security Measures)**

13. **Contracts which involve MoD classified information at SECRET or above level are subject to DEFCON 659A which advises the contractor of necessary security precautions/requirements. Amongst other things DEFCON 659A draws attention to the terms of the Official Secrets Act 1911-1989 and obliges the contractor:**

**a. to allow only individuals approved by the MoD and with a valid "need to know" to have access to the "SECRET Matter";**

**b. to safeguard the "SECRET Matter" strictly at all times to the standard prescribed;**

**c. to make sure that employees with access to the "SECRET Matter" are aware of and observe the security obligations imposed on the contractor and to report any default on their part;**

---

[6] DECONS 531, 659A can be found on the DE&S AOF Commercial Toolkit at: http://www.aof.dii.r.mil.uk/aofcontent/tactical/toolkit/content/defcons/defcon.htm

**d. not to award subcontracts involving disclosure of "SECRET Matter" without the MoD's written consent, and to include security conditions as defined in Appendix to DEFCON 659A;**

**e. to allow the MoD to inspect the contractor's security arrangements;**

**f. to allow no information in any form whatever to be published, or circulated except as necessary for the work, without the MoD's written consent.**

14. **DEFCON 659A contractually obligates the contractor to be compliant with the security requirements contained in the UK Governments national security regulations contained in the Security Policy Framework (SPF), issued by the Cabinet Office. All Government contractors handling classified information at the level of SECRET and TOP SECRET must be aware of their security obligations under the SPF. A public version of extracts from SPF is available at Security Policy Framework | Cabinet Office. Those companies who are awarded contracts which require them to hold SECRET or above classified information at one or more of their facilities (referred to as List X or a Facility Security Clearance (FSC)), will be required to register with the DE&S SAC via the address below for access to the full version of the SPF. mailto: DES PSyA-SecurityAdviceCentre@mod.uk**

15. **If the contract involves the processing or holding of classified information of any level on an Electronic Information System, the advice of the MoD Defence Assurance and Information Security (DAIS) must be sought before any classified information is placed on the Electronic Information System mailto:cio-dsas- industrycontactpoint@mod.uk**

**Classified Markings**

16. **Whenever it is important to national security to safeguard material or information, one of the following protective markings will be used:**

**OFFICIAL-SENSITIVE**

**Asset Value - consequence of compromise**

**The compromise of assets marked OFFICIAL-SENSITIVE would be likely to:**

- **adversely affect diplomatic relations**
- **cause substantial distress to individuals**
- **make it more difficult to maintain the operational effectiveness or security of UK or allied forces**
- **cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies**
- **prejudice the investigation or facilitate the commission of crime**
- **breach proper undertakings to maintain the confidence of information provided by third parties**
- **impede the effective development or operation of government policies**
- **breach statutory restrictions on the disclosure of information (except the Data Protection Act - which can be addressed by other impact statements and/or the e-Government Security Framework)**
- **disadvantage government in commercial or policy negotiations with others**
- **undermine the proper management of the public sector and its operations.**

**Level of protection**

**The level of protection provided for assets marked OFFICIAL should:**

**promote discretion in order to avoid unauthorised access.**

**Baseline objectives Storage and control**

**For the storage and control of OFFICIAL assets do everything possible to:**

- **make accidental compromise or damage unlikely during storage, handling, use, processing, transmission or transport**
- **deter deliberate compromise or opportunist attack**
- **dispose of or destroy in a manner to make reconstruction unlikely.**

**Information assets:**

- **Handle, use and transmit with care**
- **Take basic precautions against accidental compromise or opportunist attack.**

**Physical assets:**

- **Control, use and transport with care**
- **Take basic precautions against accidental compromise or opportunist attack.**

**Baseline objectives disposal and destruction**

**Information assets:**

- **Make reconstitution unlikely.**

**Physical assets:**

- **Dispose of with care or destroy to make reconstitution unlikely.**

| | |
|---|---|
| **Access requirements** | **In addition to a 'need to know' access to classified information at the level of OFFICIAL-SENSITIVE requires individuals to have satisfied the requirements of the Baseline Personnel Security Standard (BPSS).** |
| **Application requirements** | **The handling caveat OFFICIAL-SENSITIVE should only be applied to OFFICIAL assets containing additional sensitivity so that additional procedural and handling requirements can be applied to enforce the 'need-to-know'.:** |
| **Telephone** | **OFFICIAL and OFFICIAL-SENSITIVE information may be discussed on all types of telephone within the UK, but not with (or within) earshot) of unauthorised persons.** |

**SECRET**

| | |
|---|---|
| **Asset Value - consequence of compromise** | **The compromise of assets marked SECRET would be likely to:**<br>- **raise international tension**<br>- **seriously damage relations with friendly governments**<br>- **threaten life directly or seriously prejudice public order or individual security or liberty**<br>- **cause serious damage to the operational effectiveness or security of UK or allied forces**<br>- **cause serious damage to the continuing effectiveness of highly valuable security or intelligence operations**<br>- **cause substantial material damage to national finances or economic and commercial interests.** |
| **Level of protection** | **The level of protection provided for assets marked SECRET should:**<br>- **make unauthorised access highly unlikely**<br>- **ensure that actual or attempted compromise will be detected and make it highly likely that those responsible will be identified.** |

**Baseline objectives - storage and control**

**For the storage and control of assets marked SECRET, do everything possible to:**

- **make accidental compromise or damage highly unlikely during storage, handling, use, processing, transmission or transport**
- **limit knowledge of planned movement of physical assets**
- **offer a degree of resistance to deliberate compromise by a professional or violent attack**
- **detect actual or attempted compromise and help identify those responsible**
- **dispose of or destroy in a manner to make retrieval or reconstruction highly unlikely and prevent identification of constituent parts.**

**Information assets:**

- **Handle, use and transmit to minimise the chance of accidental compromise**
- **Offer a degree of resistance to deliberate compromise by a professional attack**
- **Where possible, detect actual or attempted compromise and help identify those responsible.**

**Physical assets:**

- **Control, use and transport to minimise the possibility of accidental compromise**
- **Offer a degree of resistance to deliberate compromise by a professional attack**
- **Limit knowledge of planned movements**
- **Detect actual or attempted compromise and help identify those responsible.**

**Baseline objectives - Disposal and destruction**

**Information assets:**

- **Make retrieval or reconstitution highly unlikely**
- **Detect actual or attempted compromise and help identify those responsible.**

**Physical assets:**

- **Make reconstitution highly unlikely**
- **Prevent identification of constituent parts**
- **Detect actual or attempted compromise and help identify those responsible.**

**Access requirements**

**For occasional access to assets marked SECRET the following level of clearance is required:**

- **a Baseline Standard (BPSS).**

**For regular access to assets marked SECRET the following level of clearance is required:**

- **Security Check**

**Application requirements**

**The protective marking SECRET should only be applied to sensitive assets which relate to the following areas of activity:**

- **National Security**
- **International relations**
- **Defence**
- **Public order and civil rights**
- **Economic interests.**

**TOP SECRET**

**Asset Value - consequence of compromise**

**The compromise of assets marked TOP SECRET would be likely to:**

- **threaten directly the internal stability of the UK or friendly countries**
- **lead directly to widespread loss of life**
- **cause exceptionally grave damage to the effectiveness or security of UK or allied forces**
- **cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations**
- **cause exceptionally grave damage to relations with friendly governments**
- **cause severe long term damage to the UK economy.**

**Level of protection**

**The level of protection provided for asset marked TOP SECRET should:**

- **ensure that there is no unauthorised access**
- **ensure that actual or attempted compromise will be detected and those responsible will be identified.**

**Baseline objectives – storage and control**

**For the storage and control of assets marked TOP SECRET do everything possible to:**

- **prevent accidental compromise or damage during storage, handling, use, processing, transmission or transport**
- **strictly limit knowledge of planned movement of physical assets to those with 'need to know'**
- **offer a degree of resistance against compromise by a sustained and sophisticated or violent attack**
- **detect actual or attempted compromise and make it likely that those responsible will be identified**
- **dispose of or destroy in a manner to prevent reconstruction or identification of constituent parts.**

**Information assets:**

- **Handle, use and transmit to prevent accidental compromise**
- **Offer a degree of resistance to compromise by a sustained and sophisticated attack**
- **Where possible detect actual or attempted compromise and make it likely that those responsible will be identified.**

**Physical assets:**

- **Control, use and transport to take every possible precaution against accidental damage**
- **Offer a degree of resistance to deliberate compromise by a sustained and sophisticated attack**
- **Strictly limit knowledge of planned movements to those with a 'need to know'.**
- **Detect actual or attempted compromise and make it likely that those responsible will be identified.**

**Baseline objectives - Disposal and destruction**

**Information assets:**

- **Do everything necessary to prevent retrieval or reconstitution**
- **Detect actual or attempted compromise and make it likely that those responsible will be identified.**

**Physical assets:**

- **Do everything necessary to prevent retrieval**
- **Prevent identification of constituent parts**
- **Detect actual or attempted compromise and make it likely that those responsible will be identified.**

**Access requirements**

**For access to assets marked TOP SECRET the following level of clearance is required:**

- **Developed Vetting (DV) for regular access**
- **In some cases a Security Check (SC) may be sufficient for supervised or occasional / limited access.**

**Application requirements**

**The protective marking TOP SECRET should only be applied to sensitive assets which relate to the following areas of activity:**

- **National Security**
- **International relations**
- **Defence**
- **Public order and civil rights**
- **Economic interests.**

**Atomic and national caveat (UK EYES only OR Discretion) markings**

17. **Documents which bear the restrictive markings ATOMIC or UK EYES ONLY or DISCRETION in conjunction with classification, require special treatment as regards their handling, custody and who can have access to them. Contractors in receipt of this type of information should seek guidance on their protection from the DE&S SAC in the first instance or their MoD Contracting Authority.**

**Security grading**

18. **Documents concerned with a classified tender or contract may be originated by the contractor themselves. These should be graded in accordance with the definition of information to be given security protection.**

19. **Documents should be graded according to the sensitivity of their own content and not according to the grading of other documents to which they may refer. Mere reference to classified document does not itself necessarily warrant a classification. Security is not enhanced by over-grading and cases of doubt should be referred to the Technical or Contracting Authority.**

**Personnel security**

**Need to know**

20. **Disclosure of MoD classified information must be strictly in accordance with the "need to know" principle. It must be confined to those members of your staff whose access to the information is essential for the preparation of the tender or execution of the contract.**

**Authority for Access**

21. **Any individual requiring access to UK MoD classified information at the level of OFFICIAL-SENSITIVE or above must, as a minimum, be subject to the HMG Baseline Personnel Security Standard (BPSS). Further information on the BPSS is available at Security Policy Framework | Cabinet Office. A BPSS is not acceptable for access to classified information CONFIDENTIAL or above provided to the UK by a foreign government or International Organisation such as NATO.**

22. **For access to foreign government or International Organisation classified information at the level of CONFIDENTIAL or above or more sensitive to MoD classified information, additional security controls, referred to as National Security Vetting (NSV) will need to be applied. If this is the case, security clearance must be sought from the Defence Business Service-National Security Vetting (DBS-NSV) organisation. The level of authority for access will be defined by those responsible for the issue of the tender for contract or contracting authority.**

23. **List X facilities will be able to sponsor requests for National Security Vetting themselves; companies or facilities not on List X will need to arrange for their requests for NSV to be sponsored by their Contracting Authority or other pre-defined MoD authority.**

24. **Information on the operation of NSV for MoD contractors is available at Ministry of Defence | About Defence | What we do | Security and Intelligence | DBS National Security Vetting.**

**Document security**

**Definition**

25. **The word "document" is used to cover any form of recorded information; including written and electronic media or classified material.**

**Recording of Classified Documents**

26. **The receipt, circulation, despatch and disposal of documents marked as SECRET and above, whatever their origin must be recorded in such a way that the whereabouts of a document, and each copy of it can readily be determined. In the event of such a document being created within the Company, this should be recorded in a similar way to those received from outside, being initially recorded as "incoming" at the point where it is created. The registers in which the records are maintained should aim to conform to the layout indicated below.**

**Documents-in Register**

27. **Columns for:**

- **Date of receipt**
- **Received from**
- **Originator if different from column ii**
- **Date of documents**
- **Reference No.**
- **Copy No (where appropriate)**
- **Title or Subject**
- **Protective marking**
- **Where held**
- **Date receipt sent (where appropriate)**
- **Date of spot check.**

**Documents-out Register**

**28. Columns for:**

- **Date of despatch**
- **Addressee**
- **Date of document**
- **Reference No.**
- **Copy No (where appropriate)**
- **Title or subject**
- **Protective marking**
- **Receipt No**
- **Date receipt returned**

**Transmission within Company Premises**

**29. Transmission of classified information documents within a company's premises must be safeguarded to ensure that no unauthorised person has access. Documents should be passed from one building to another in sealed envelopes or locked cases or boxes.**

**Transmission Outside Company Premises within UK**

**30 General instructions for the marking of envelopes containing documents protectively marked SECRET or above are as follows:**

**(a). Both inner and outer envelopes should bear a company stamp that clearly indicates the full address of the office from which it was sent.**

**(b). The document reference number and date of origin should be indicated on the inner envelope.**

**(c). Outer envelopes should be clearly addressed to a person, company or branch of a Government Department. For the MoD, it is essential that the branch, room number and full address of the building are also included: failure to include these details will cause considerable delays and may result in a breach of security. There must be no mention of the security classification on the outer envelope.**

**(d). Inner envelopes, similarly addressed, should be marked with the security protective marking.**

**(e). National caveat markings must not appear on either the inner or the outer envelopes containing documents so marked. The inner envelope, which must carry the documents protective marking but not the national caveat, should be addressed to an individual who is known to be permitted to have access to the contents, using the format:**

**EXCLUSIVE TO .....**

**31. Classified documents should be sent by post as follows:**

**OFFICIAL-SENSITIVE**

**By ordinary post in a single envelope which should bear no security protective marking. No receipt necessary.**

**SECRET**

**By Parcelforce 24 hour service under double cover, both covers being addressed to the intended recipient. The inner cover only should be marked SECRET. A receipt form bearing only the date and reference number of the document should be enclosed with a request that it signed and returned immediately to the sender. If this receipt is not returned within 10 days, enquiries should be made of the addressee.**

**TOP SECRET**

**By hand of Defence Courier only.**

**There are special rules governing the transmission of documents marked ATOMIC. Instructions will be issued as necessary by the Technical Authority.**

**Transmission Overseas**

**No classified documents may be transmitted overseas without the prior approval of the Contracting Authority. If approval is given the documents must be forwarded to the Contracting Authority for transmission through official Government channels. To identify to the overseas recipient that the**

**material is owned by the UK the classification contained on documents to be sent overseas must be pre-fixed "UK".**

**Removal of Documents from Company Premises**

**32. Classified documents may occasionally have to be taken off the premises for meetings in the UK. A record of the documents should be kept in the Company and used to check the documents when they are returned.**

**33. Classified documents taken off the premises must be carried in a locked brief case bearing a label with the Company's address and telephone number in case of loss.**

**34. Persons taking classified documents off the premises should be informed that they must keep the documents under their personal care at all times, must never read them in a public place (e.g. a restaurant or railway carriage must never leave them, even in a locked briefcase, in an unattended car or public place or entrust them to the safe custody of a member of the public; that they have an obligation to safeguard the documents and are liable to prosecution under the OSA if they handle them carelessly.**

**If the documents are lost they must immediately report the fact to the Company.**

**35. No classified document may be taken overseas without the prior approval of the Authority and DES Infra Security.**

**Destruction**

**36. Classified waste must be segregated and stored under secure conditions and its collection and destruction by burning or crosscut shredding must be carried out under supervision. Arrangements can often be made to return protectively marked waste to the Authority for destruction.**

**Telephone conversations**

**37. Classified information at the level of OFFICIAL and OFFICIAL-SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not with (or within) earshot) of unauthorised persons. However SECRET and TOP SECRET must not be discussed on the telephone at all.**

**E-mail**

**38. OFFICIAL and OFFICIAL-SENSITIVE information may be emailed to UK recipients over the internet in accordance with the Security Conditions. However, OFFICIAL-SENSITIVE information may be emailed only where there is a strong business need to do so and only with the prior approval of the Authority, and subject to any explicit limitations that it shall require. Such limitations including any regarding publication and further circulation shall be clearly identified in the covering email. Classified information at the level of SECRET and TOP SECRET must not be passed over the internet unless appropriately encrypted.**

**Physical Security**

**39. The physical security measures required at a company's premises will depend upon the nature and classification of the work. Safes or steel cupboards / filing cabinets to an approved standard will be required for storing classified documents and appropriate hardware. The DE&S Security Adviser should be consulted about the approved containers.**

**Additional precautions which may be necessary include:**

**(a). provision of segregated areas for carrying out classified work;**

**(b). 24 hour guard patrols or the provision of monitored alarm systems are required for work which is classified SECRET or above.**

**(c). modification of perimeter defences including security of windows and doors.**

**Storage within Company Premises**

**40. When not in use MoD classified information SECRET or above must be locked in approved security containers or when the size renders this impracticable in a room or area which has been given adequate protection to make it secure. All OFFICIAL-SENSITIVE marked material including documents, media and other material must be physically secured to prevent unauthorised access. It is recommended as a minimum that OFFICIAL-SENSITIVE material is placed in a lockable room, cabinets, drawers or safe and the keys/combinations are subject to a level of control.**

**41. No indication of the security grading of the contents should appear on the outside of the container. Occasional inspections should be made to ensure that the rules contained in this Memorandum for safeguarding of classified documents are being observed.**

**Security of Keys and Combination Lock Settings**

**42. Security keys are those which operate the locks fitted to:-**

**(a). security containers for the storage or circulation of protectively marked documents;**

**(b). doors of secure rooms or areas.**

**43. Only persons authorised to have access to classified information protected by a particular security key should have access to security key(s).**

**44. When not in use, security keys should be kept in a container with a combination lock. When this is not possible and security keys have to be taken off the company's premises, they must never be carried loose in a pocket or handbag but must always be on a key ring attached to a chain, and must never leave the possession of the owner. The keys themselves should bear no marking or label which could indicate the premises where they are used.**

**45. Security keys must never be taken out of the United Kingdom.**

**46. Combination locks should be set by, and knowledge of the setting should be confined to, those members of staff who have authorised access to the contents of the container. A written record of each setting, for use in an emergency, should be held in a sealed envelope in a secure container of at least equivalent security standard. Only staff with authorised access to the**

**contents of the container should have access to the record of re-setting. Except for such a record, combination settings must NEVER be written down.**

**Keys**

**47. If a security key is lost or if there is reason to suspect that an unauthorised person may have access to a key, the following action must be taken forthwith:**

**a. clear the container and ensure that it remains cleared until such time that a new lock has been fitted.**

**b. investigate the circumstances of the loss;**

**c. where the investigation reveals that the classified material protected by the key may have been compromised, the JSyCC should be contacted immediately (See para 49).**

**Security Breaches**

**Loss and Incident Reporting**

**48. Any security incident involving any MoD owned, processed or generated information must be immediately reported to the MoD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC). This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the MoD's Chief Information Officer (CIO) and, as appropriate, the company concerned. The MoD WARP will also advise the contractor what further action is required to be undertaken.**

**JSyCC WARP Contact Details**

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

**Further Advice**

**50. Further advice on the content of this Memorandum may be obtained from the DE&S SAC via the points of contact details at paragraph 4 above.**