[redacted]

58.21.9. 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.

58.21.10. Internet Connections. Computer systems shall not be connected direct to the Internet or 'untrusted' systems unless protected by a firewall (a software based personal firewall is the minimum but risk assessment and management must be used to identify whether this is sufficient).

58.21.11. 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

58.22. Laptops holding any MOD supplied or contractor generated OFFICIAL-SENSITIVE information are to be encrypted using a CPA product or equivalent as described above.

58.23. Unencrypted laptops not on a secure site are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the Authority for consideration. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites. For the avoidance of doubt the term "drives" includes all removable, recordable media (e.g., memory sticks, compact flash, recordable optical media e.g. CDs and DVDs), floppy discs and external hard drives.

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

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

Loss and Incident Reporting

58.26. The contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIAL-SENSITIVE information to the Authority.

58.27. Accordingly, in accordance with Industry Security Notice 2014/02 as may be subsequently updated at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/293480/ISN2014_02_Incident_Reporting.pdf

any security incident involving any MOD owned, processed, or Contractor generated OFFICIAL or OFFICIAL-SENSITIVE information defined in the contract Security Aspects Letter shall 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.

[redacted]

JSyCC WARP Contact Details

Email: For those with access to the RLI: [redacted]
Email: For those without access to the RLI: [redacted]
Telephone: Working Hours: [redacted]
Out of Hours/Duty Officer Phone: [redacted]
Fax: [redacted]
Mail: [redacted]

Sub-Contracts

58.28. The Contractor may Sub-contract any elements of this Contract to Sub-contractors within the United Kingdom notifying the Authority. When sub-contracting to a Sub-contractor located in the UK the Contractor shall ensure that 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 OFFICIALSENSITIVE elements of the Contract to a Sub-contractor located in another country. The first page of Appendix 5 (MOD Form 1686 (F1686)) of the Security Policy Framework Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at Appendix 5 at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367494/Contractual_Process_-_Appendix_5_form.doc.

If the Sub-contract is approved, the Authority shall provide the Contractor with the security conditions that shall be incorporated within the Sub-contract document.

Publicity Material

58.29. Contractors wishing to release any publicity material or display hardware that arises from this contract shall seek the prior approval of the 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 MOD, Services or any other government department.

Private Venture

58.30. Any defence related Private Venture derived from the activities of this Contract are to be formally assessed by the Authority for determination of its appropriate classification. Contractors are to submit a definitive product specification for PV Security Grading in accordance with the requirement detailed at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414857/20150310_PV_Ex_Guidance_Document.pdf

Promotions and Potential Export Sales

58.31. Contractors wishing to promote, demonstrate, sell or export any material that may lead to the release of information or equipment classified OFFICIAL-SENSITIVE (including classified tactics, training or doctrine related to an OFFICIAL-SENSITIVE equipment) are to obtain the prior approval of the Authority utilising the MOD Form 680 process, as identified at:

https://www.gov.uk/mod-f680-applications.

Destruction

58.32. As soon as no longer required, OFFICIAL and OFFICIAL-SENSITIVE information/material shall be destroyed in such a way as to make reconstitution unlikely, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

Interpretation/Guidance

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

58.34. Further requirements, advice and guidance for the protection of MOD information at the level of OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

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

Audit

58.35. Where considered necessary by the Authority, the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractors processes and facilities by representatives of the Authority to ensure compliance with these requirements.

59. Entire Agreement

59.1. This Contract constitutes the entire agreement between the Parties relating to the subject matter of this Contract. This Contract supersedes all prior negotiations, representations, and undertakings, whether written or oral, except that this Clause 59.1 shall not exclude liability in respect of any fraudulent misrepresentation.

60. Continuing Obligations

60.1. Save as otherwise expressly provided in this Contract or as already taken into account in the calculation of any payment on termination pursuant to this Contract:

4.2.6 termination of this Contract shall be without prejudice to any accrued rights or obligations under this Contract prior to termination; and

4.2.7 termination of this Contract shall not affect the continuing rights and obligations of the Contractor and the Authority under:

(1) Condition 54 (TUPE), Condition 32 (Background Information), Condition 34 (Documents, Drawing and Information), Condition 17 (Financial Consequences of Termination), Condition 33 (Retention of Records), DEFCON 530 (Dispute Resolution (English Law)), DEFCON 609 (Contractor's records)

(2) any other provision of this Contract which is expressed to survive termination, or which is required to give effect to such termination or the consequences of such termination.

61. Gainshare

61.1. Should either the Authority or the Contractor propose either a change to the Contract or an improved way of working which it is believed will result in a benefit to both the Authority and the Contractor, following discussions the Contractor shall raise a detailed proposal, including full details of the proposed benefit that would accrue to the Authority in approving the