58.8. Disclosure of OFFICIAL and OFFICIAL-SENSITIVE 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 any of the classified aspects of the Contract detailed in the Security Aspects Letter other than to a person directly employed by the Contractor or sub-Contractor, or service provider.

58.9. 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 shall be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with Clause 58.32.

Access

58.10. Access to OFFICIAL and OFFICIAL-SENSITIVE information shall be confined to those individuals who have a "need-to-know", have been made aware of the requirement to protect the information and whose access is essential for the purpose of his or her duties.

58.11. The Contractor shall ensure that all individuals having access to OFFICIAL-SENSITIVE information have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to OFFICIAL-SENSITIVE information. Further details and the full requirements of the BPSS can be found at the Gov.UK website at:

https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.

Hard Copy Distribution

58.12. OFFICIAL and OFFICIAL-SENSITIVE documents shall be distributed, both within and outside company premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or commercial couriers in a single envelope. The words OFFICIAL or OFFICIAL-SENSITIVE shall not appear on the envelope. The envelope should bear a stamp or details that clearly indicates the full address of the office from which it was sent.

58.13. Advice on the distribution of OFFICIAL-SENSITIVE documents abroad or any other advice including the distribution of OFFICIAL-SENSITIVE hardware shall be sought from the Authority.

Electronic Communication, Telephony and Facsimile Services

58.14. OFFICIAL information may be emailed unencrypted over the internet. OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a CESG Commercial Product Assurance (CPA) cryptographic product or a MOD approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have TLS enabled. Details of the required TLS implementation are available at:

https://www.ncsc.gov.uk/guidance/tls-external-facing-services

Details of the CPA scheme are available at:

https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

Exceptionally, in urgent cases, OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so and only with the prior approval of the Authority.

[redacted]

58.15. OFFICIAL-SENSITIVE information shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these security conditions and subject to any explicit limitations that the authority shall require. Such limitations, including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.

58.16. OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the UK and overseas. OFFICIAL-SENSITIVE information may be discussed on fixed and mobile types of telephone within the UK, but not within earshot of unauthorised persons.

58.17. OFFICIAL information may be faxed to recipients located both within the UK and overseas, however OFFICIAL-SENSITIVE information may be faxed only to UK recipients.

Use of Information Systems

58.18. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

58.19. The contractor shall ensure 10 Steps to Cyber Security is applied in a proportionate manner for each IT and communications system storing, processing or generating MOD UK OFFICIAL or OFFICIAL-SENSITIVE information. 10 Steps to Cyber Security is available at:

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

The contractor shall ensure competent personnel apply 10 Steps to Cyber Security.

58.20. 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 ex-filtrate data.

58.21. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum-security requirements for processing and accessing OFFICIAL-SENSITIVE information on IT systems.

58.21.1. Access Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of "least privilege" will be applied to System Administrators. Users of the IT System -Administrators should not conduct 'standard' User functions using their privileged accounts.

58.21.2. 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.

58.21.3. Passwords. Passwords are part of most ID&A, Security Measures. Passwords shall be 'strong' using an appropriate method to achieve this, for example including numeric and "special" characters (if permitted by the system) as well as alphabetic characters.

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

58.21.5. Data Transmission. Unless the Authority authorises otherwise, OFFICIAL-SENSITIVE information shall be transmitted or accessed electronically (e.g. point to

point computer links) via a public network like the Internet, using a CPA product or equivalent as described in Clause58.13above,

58.21.6. 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:

(e) Type of event,

(f) User ID,

(g) Date & Time,

(h) 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.

58.21.7. 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/Continuity Plan

(3). Data backup with local storage,

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

(5). Operating systems, applications and firmware should be supported,

(6). Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended Schedule. If patches cannot be applied an understanding of the resulting risk will be documented,

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

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