Ministry of Defence

Industry Security Notice

Number 2014/05

Subject: Government Security Classification Scheme

Introduction:

1. On the 2 April 2014 the United Kingdom Government implemented the new Government Security Classification (GSC) policy which replaced the Government Protective Marking Scheme (GPMS). Guidance and instruction for the application of the GSC by Ministry of Defence (MOD) contractors was issued in Industry Security Notice 2014/01.

Issue:

2. As identified in Industry Security Notice 2014/01 the GSC introduced a 3 tier security classification policy of OFFICIAL, SECRET, and TOP SECRET identified as below:

OFFICIAL
This category is for the majority of information created or processed by government and includes both routine business and some sensitive information.

SECRET
Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threats

TOP SECRET
This category of information is the most sensitive requiring the highest levels of protection from the most serious threats.

The security requirements to be applied for the each GSC tier are defined in the Security Policy Framework (SPF) much of the SPF can now be accessed on the GOV.UK website at: https://www.gov.uk/government/collections/government-security.

3. **Aim**

3.1. As part of our ongoing work on the GSC policy we will continue to engage with industry and provide information and advice as the new scheme continues to be implemented. The aim of this particular Industry Security Notice is to provide MOD contractors undertaking contracts involving security aspects at the level of OFFICIAL SENSITIVE with additional information on various aspects of the application of the GSC and clarity on some of the guidance that was included in Industry Security Notice 2014/01.

4. National Security

4.1. Contracting

New Invitations to Tender (ITT) and Contracts

4.1.1. Paragraph 9.1.2 of Industry Security Notice 2014/01 advised that the requirements applicable for OFFICIAL information may be included in a future new DEFCON. The new DEFCON 660 for contracts that involve Reportable OFFICIAL and/or OFFICIAL SENSITIVE aspects which require the issue of a Security Aspects Letter (SAL) and the issue of the Reportable OFFICIAL and OFFICIAL SENSITIVE Security Condition is currently under stakeholder consultation. Prior to the introduction of DEFCON 660 a narrative condition will be included in MOD contracts:

4.1.2. Paragraph 9.1.4 of Industry Security Notice 2014/01 identified the requirement to report to the MOD any loss or compromise of OFFICIAL information associated with contracts that have been specifically identified in a SAL as Reportable OFFICIAL. The policy regarding Reportable OFFICIAL information and the reporting requirement is being reviewed within the MOD and further information on this will be communicated when this consideration is finalised. The outcome of this consideration may impact on the wording of DEFCON 660 mentioned above and require appropriate amendments to **Annex B**.

Security Aspects Letters

4.1.3. Paragraph 9.1.7 of Industry Security Notice 2014/01 advised that MOD Project Teams will be required to review the security aspects of all contracts at the next contract amendment point, SAL annual review or, at the latest, by 1 April 2015. We have seen that some SALs have been issued by MOD Project Teams to bring the security aspects of the contract in line with the GSC classifications and we will shortly be issuing further communications to the Project Teams to remind them of the requirement. When a new SAL is received by the prime contractor, it must issue a new SAL to any sub-contractors defining the new aspects associated with the sub-contract.

4.1.4. Where new SALs have not been received by the 1 April 2015 MOD contractors are encouraged to contact the relevant MOD Project Team to enquire when the GSC compliant replacement SAL will be issued. In doing so you should inform the MOD Project Team that you are aware of the requirement placed on it to issue new SALs and that you are contacting it to request a new one for your contract at the direct request of MOD DBR-Def Sy. If an SAL is not received you should contact DBR-Def Sy STInd at the email address below providing details of the MOD Project Team and the contract.

Personnel Security Clearance Requirements and Marking of MOD Vetting Information

4.1.5. There are no changes to the existing National Security Vetting requirements for access to classified information from the 2 April 2014. A Baseline Personnel Security Standard is required for access to MOD OFFICIAL SENSITIVE material.

4.1.6. The classification of MOD vetting information that may be handled or processed by MOD contractors will vary depending on the circumstances and the information concerned. Some vetting related information will not meet the requirement for OFFICIAL SENSITIVE and should be classified and handled as OFFICIAL. This will be the case for the notifications of security clearances and NATO/EU clearance certificates. This Industry Security Notice may be taken as authority to downgrade any such notifications received since the 2 April 2014 to OFFICIAL. Some specific vetting documents will also require the additional descriptor "PERSONAL". A guide to the classifications to be applied is contained at **Annex A**. In the majority of cases vetting information must also carry the Handling Instruction "Vetting in Confidence". The Vetting in Confidence handling instruction means:

- Information can only be used for vetting purposes.
- Must be protected in accordance with the Data Protection Act 1998.
- Can only be shared within the personnel security community and on a need-to-know basis for risk management purposes.
- Must not be stored in open CIS and physical folders / team sites.
- Vetting information marked OFFICIAL SENSITIVE or OFFICIAL SENSITIVE-PERSONAL must not be transmitted over the internet (without the express permission of the information owner).
- Must not be read or worked on in public or otherwise in the sight of unauthorised persons.
- Must not be worked on, or stored on, personal (non-official) computers.
- Can be discussed over all types of telephone, but not with or within earshot of unauthorised persons.
- Must not be sent to group mail email accounts (outside of the personnel security community).
- Must not be amended or altered in any way by the recipient (this relates in particular to Notification of Clearance and NATO/EU Certificates)

4.2. **Computer Information Systems**

4.2.1. Paragraph 9.3.1 of Industry Security Notice 2014/01 advised that contractor Computer Information Systems (CIS) used to hold/process classified information at the level of Reportable OFFICIAL and/or OFFICIAL SENSITIVE will be required to be compliant with the criteria specified in the Reportable OFFICIAL and OFFICIAL SENSITIVE Security Conditions. A new version of the Reportable OFFICIAL and OFFICIAL SENSITIVE Security Condition has been produced with amended provisions concerning the encryption products for the electronic transmission and data transmission of OFFICIAL SENSITIVE information. A copy of the new MOD Security Condition is at **Annex B**.

4.2.2. Further work on the MOD CIS assurance and accreditation policy is underway, in consultation with Trade Associations; and this policy will be communicated in due course.

5. **Commercial Policy Commercial Handling Instruction**

5.1. The MOD has taken on board the concerns expressed by industry of the volume and over classification of some contracts and commercial material that is being classified as OFFICIAL-SENSITIVE COMMERCIAL. Recognising the need to identify and protect commercial sensitivities a commercial handling instruction is currently being developed to help alleviate this situation. Details of its application will be provided when finalised.

6. **Classified Patents and Designs - Security Provisions in Relation to s.22 Patents Acts 1977 and s.5 Registered Designs Act 1949**

6.1. The Intellectual Property Office (IPO) can give directions to prohibit or restrict the publication or communication of the content of a patent or design application. Under GPMS it achieved this by giving it a marking of RESTRICTED or above on advice received by the MOD. Under the GSC it has been decided that the lowest level of grading that will be given to a patent or design application subject to such directions will be OFFICIAL SENSITIVE.

6.2. As each application previously subject to a GPMS marking is reviewed in accordance with the relevant Patent and Design legislation, it will be issued with the appropriate new GSC classification. This is likely to mean that any application currently marked at CONFIDENTIAL will be remarked as SECRET on review; unless it would otherwise have been reduced to RESTRICTED on review in which case it will be marked as OFFICIAL SENSITIVE.

6.3. The dispensation that "on an exceptional basis OFFICIAL SENSITIVE may be emailed over the internet" shall not apply to patent or design applications subject to a prohibition or restriction under any circumstances. In addition applications may be subject to further handling restrictions as identified by the Security Section of the IPO in their formal notification of prohibition or restriction.

6.4. Where a contractor wishes to file an application for a patent or registered design that would be subject to a security obligation under DEFCON 14, 14a or 705[1], prior to the contract having received a new SAL, such applications shall be marked OFFICIAL SENSITIVE where they are RESTRICTED in the SAL or SECRET where they are classified CONFIDENTIAL or SECRET. They will additionally be subject to the handling restrictions set out in paragraph 6.3 above.

[1] DEFCONs 14,14a and 705 have not yet been updated and still refer to GPMS classifications.

7. **International Policy – Protection of OFFICIAL SENSITIVE and Third Party RESTRICTED information**

7.1. The Agreements with International Organisations and bilateral Security Agreements/Arrangements with international partners are being amended to reflect that UK OFFICIAL SENSITIVE information equates with International RESTRICTED information. Annex E to Industry Security Notice 2014/01 identified the additional protective security requirement over and above those applied to OFFICIAL SENSITIVE information that must be applied to Third Party RESTRICTED information.

7.2. Whilst it is permissible in exceptional circumstances with the prior approval of the MOD information owner and where there is a demonstrable and pressing business requirement for UK OFFICIAL SENSITIVE information to be emailed unencrypted over the internet to UK recipients, OFFICIAL SENSITIVE information must **not** be transmitted unencrypted to recipients located overseas. Whilst it is recognised that internet transmissions to UK recipients may be routed via various global satellites this restriction is not for technical security reasons but because international partners will treat OFFICIAL SENSITIVE to their standards for national RESTRICTED information which does not permit unencrypted transmission.

Action by Industry:

8. This Industry Security Notice should be read in conjunction with Industry Security Notice 2014/01 and is issued to provide further information, guidance and clarification for MOD contractors on the requirements and implementation of the GSC and identifies the action that should be taken when a new GSC compliant SAL is not issued by the MOD Project Team. It may be utilised for internal use and promulgation as appropriate.

Validity / Expiry Date:

9. There is no expiry date to this Industry Security Notice.

MOD Points of Contact Details:

Ministry of Defence
DBR-Def Sy STInd
Zone I
Main Building
Whitehall
London
SW1A 2HB

Email: DBR-DefSy-STInd@mod.uk

22 October 2014

ANNEX A

Government Security Classification System – Classification of MOD Vetting Information Accessed by Industry

Type of Information / asset	GSC marking	Reasons
Completed Aftercare Incident Report (AIR)	**OFFICIAL SENSITIVE-PERSONAL** or higher classification as required by circumstance plus **Handling instruction: Vetting-in-Confidence**	Will contain particularly sensitive information - some of which may be unproven and therefore potentially personally damaging; some information may be potentially damaging to the Department (particularly where security breaches are involved).
Notification of NSV clearance	**Handling instruction: Vetting-in-Confidence**	Only contains name, date of birth, clearance level and validity date. In some circumstances, it will refer to restrictions, but it will not provide the reason for the restrictions.
Notification of withdrawal / denial of clearance	Letters to the individual should be addressed as "Personal for". Letters to the employing or sponsor company should be **OFFICIAL SENSITIVE** and include the **Handling instruction: Vetting-in-Confidence**.	Letters to the Vetting subject, and particularly those sent to a home address, should not carry a security marking but should be marked "Personal for". Letters to third parties (e.g. company Security Officer/Line Manager), should be marked **OFFICIAL-SENSITIVE** plus the **Handling instruction**.
NATO clearance Certificates	**Handling instruction: Vetting-in-Confidence**	Same as for Notification of NSV clearance.
EU clearance Certificates	**Handling instruction: Vetting-in-Confidence**	Same as for Notification of NSV clearance.
Transfer Request Form - DBS NSV Vetting Form 101	**Handling instruction: Vetting-in-Confidence**	Contains personal information, full name including any previous surname, DOB, POB, staff/service no, nationality, rank. Also vetting information, level, case ref no, date issued and expiry date.

The information identified above that does not bear the classification of OFFICIAL-SENSITIVE or higher is classified OFFICIAL but may not be marked it should be treated accordingly.

Reportable OFFICIAL and OFFICIAL SENSITIVE Security Condition for UK Contracts

Definitions

1. The term "Authority" means a Ministry of Defence (MOD) official acting on behalf of the Secretary of State for Defence.

Security Grading

2. The Authority shall issue a Security Aspects Letter which shall define the OFFICIAL SENSITIVE and Reportable OFFICIAL information that is furnished to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all OFFICIAL SENSITIVE documents which it originates or copies during the Contract clearly with the OFFICIAL SENSITIVE classification. However, the Contractor is not required to mark information/material related to the contract which is only OFFICIAL.

Official Secrets Acts

3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911-1989 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 (including sub-contractors) have notice that these statutory provisions, or any others provided by the Authority, apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

Protection of Reportable OFFICIAL and OFFICIAL SENSITIVE Information

4. The Contractor shall protect Reportable OFFICIAL and OFFICIAL SENSITIVE information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

5. Reportable OFFICIAL and OFFICIAL SENSITIVE information shall be protected in a manner to avoid unauthorised access. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

6. All OFFICIAL SENSITIVE material including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use OFFICIAL SENSITIVE documents/material shall be stored under lock and key. As a minimum, when not in use, OFFICIAL SENSITIVE material shall be stored in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security and control.

7. Disclosure of 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.

8. 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 paragraph 31.

Access

9. Access to Reportable 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.

10. 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/security-policy-framework.

Hard Copy Distribution of Information

11. Reportable 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 Reportable 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.

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

Electronic Communication, Telephony and Facsimile Services

13. Reportable OFFICIAL information may be emailed unencrypted to recipients over the internet when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions. OFFICIAL SENSITIVE information shall normally be transmitted over the internet encrypted using a Foundation Grade or equivalent product. Information about Foundation Grade products and the CESG Commercial Product Assurance scheme is available at: http://www.cesg.gov.uk/servicecatalogue/Product-Assurance/Pages/Product-Assurance.aspx. 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.

14. 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.

15. 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.

16. OFFICIAL SENSITIVE information may be faxed to UK recipients.

17. Reportable OFFICIAL information may be discussed with and faxed to recipients located overseas.

Use of Information Systems

18. 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 proportionate security mitigations are applied to prevent a successful attack.

19. 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.

20. The following describes the minimum security requirements for processing and accessing OFFICIAL SENSITIVE information on IT systems.

a. 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.

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

1. (1) Up-to-date lists of authorised users.
2. (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 ‘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.

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

e. 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 Foundation Grade product or equivalent as described in paragraph 13 above,

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,

3. (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,

4. 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-now.

5. 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),
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,

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.

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

6. “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 or 'untrusted' systems unless protected by a firewall (a software based personal firewall is the minimum) which is acceptable to the Authority's Principal Security Advisor.

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

21. Laptops holding any MOD supplied or contractor generated Reportable OFFICIAL and OFFICIAL SENSITIVE information are to be encrypted using a Foundation Grade product or equivalent as described in paragraph 13 above..

22. 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 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.

23. 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.

24. 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

25. The contractor shall immediately report any loss or otherwise compromise of Reportable OFFICIAL and OFFICIAL SENSITIVE information to the Authority.

26. Any security incident involving any MOD owned, processed, or contractor generated Reportable 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.

JSyCC WARP Contact Details

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.

Sub-Contracts

27. 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 Reportable

[2] Secure Sites are defined as either Government premises or a secured office on the contractor premises

OFFICIAL or OFFICIAL SENSITIVE 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 form can be found at Appendix 5 at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/299557/Contractual_Process.pdf

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

28. 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

29. 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 to DBR-DefSy(S&T/Ind) for PV Security Grading in accordance with the requirement detailed at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/300050/pv_grading_flyer_apr14.pdf

Promotions and Potential Export Sales

30. 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

31. As soon as no longer required, Reportable 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

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

33. Further requirements, advice and guidance for the protection of MOD information at the level of Reportable OFFICIAL and OFFICIAL SENSITIVE may be found in Industry Security Notices at: https://www.gov.uk/government/publications/industry-security-notices-isns

Audit

34. 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.