Ministry of Defence

Industry Security Notice

Number 2025/05 (Issued 06/10/2025)

Security Aspects Letters and Contractual Security Conditions

Introduction

1. The purpose of this ISN is to explain the requirement for a Security Aspects Letter and provide an overview of the standard contractual security conditions included in MOD Contracts. This notice replaces ISN 2024/09. The content of the notice has not changed but the DSR contact email address and links contained in **Annex B** have been updated.

2. Some companies (hereafter referred to as 'Defence Suppliers') hold contracts which require them to access and/or safeguard classified assets. In order to protect classified assets, the MOD Contracting Authority (CA) shall identify the classified aspects and contractually mandate the necessary security requirements to the Defence Supplier. The Defence Supplier shall in turn flow down the relevant classified aspects and security requirements when subcontracting or collaborating with other Defence Suppliers on classified work. For the purpose of this ISN a Defence Supplier subcontracting classified work is the Contracting Authority and is responsible for issuing their own Security Aspects Letter to their Subcontractor/Supplier.

Security Aspects Letters

3. The security obligations placed upon the Defence Supplier become legally effective only when the CA has issued notice of them in writing; in cases where aspects of the pre-

contract activity (set as Invitation to Tender (ITT) for the rest of the document but covers RFI, RFQ, etc.) or Contract are graded OFFICIAL-SENSITIVE or above, this shall be achieved by means of a SAL. A SAL provides a contractual means of ensuring that security is addressed in the work that a Defence Supplier is undertaking. A SAL template is available at **Annex A**.

4. A SAL is not required if the Defence Supplier will only access classified assets graded at OFFICIAL (not OFFICIAL-SENSITIVE or above). In such cases, the Defence Supplier shall still be informed of their security obligations via security conditions included in the ITT or Contract. A SAL is also not generally required if the Defence Supplier will only have access to classified assets at MOD premises, as the CA should fulfil this notification role on a day-to-day basis.

5. The relevant security aspects about which the Defence Supplier shall be informed, are project specific and shall be compiled and included in the SAL by the CA. Security aspects that may require consideration for inclusion in a SAL include:

- general project aspects covering general points such as dates/milestones, contractual information, quantities, etc.

- performance/capabilities may cover the top-level capabilities as identified by the CA but broken down to provide more detail where available.

- it is sometimes useful to summarise the key elements of the contract at a top level before going into sub-items.

- sub-items should follow a logical progression for the breakdown of the top-level contract. A Work Breakdown Structure (WBS) may be suitable to form its basis, if available.

6. A SAL should be graded according to what it contains/can reveal but attempts shall be made to keep it at the lowest level possible, both to ease handling and to ensure that it can be distributed to the widest audience necessary, so that it is available for use by those who need it. If a SAL contains a detailed breakdown of security aspects, then it would typically be graded OFFICIAL-SENSITIVE as it identifies all the security sensitivities of a contract and therefore would be of value to an adversary. It should be noted that saying an item is SECRET does not automatically make the SAL that classification unless the existence or inclusion of that aspect is in of itself SECRET. If it is necessary to include material graded above OFFICIAL-SENSITIVE in a SAL, then it is advisable to create a separate document or annex, rather than uplifting the classification of the entire SAL.

7. The CA shall provide the SAL, together with the ITT or Contract documentation, to

the Defence Supplier. A further copy of the SAL and ITT or Contract documentation shall be sent to the Facility Security Controller of the Defence Supplier if they hold a Facility Security Clearance (FSC). The Defence Supplier shall provide a signed acknowledgment accepting the SAL before any work begins.

8. It is important that the classified assets defined in the SAL are kept up to date and that the Defence Supplier is immediately notified of any changes. The CA shall therefore keep under review the level of the classified assets defined in the SAL. The SAL shall be reviewed not less than annually, and at every contract amendment. As a contractual document, up-issue of the SAL would require contract amendment.

9. Separate SALs are required for each new contract, even if they are the same as the last contract or a task continuation. The SAL shall only contain information relevant to the work the Defence Supplier will be undertaking. Separate SALs may therefore be required for each Defence Supplier.

10. 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 Defence Supplier, or if, for any other reason, it is open to doubt, the Defence Supplier shall take up the matter immediately with the CA.

11. A Defence Supplier may query the classification of any aspect of a contract defined in a SAL. The Defence Supplier should be assured that this will in no way prejudice their interests with the CA. Any CA receiving such a query on a classification shall deal with it promptly, if necessary, issuing an amendment to the SAL.

12. The contract and SAL are fundamental to the protection of classified assets, in that they make the Defence Supplier responsible for achieving and maintaining the required security controls for the appropriate protection of government assets. It is for the CA, to decide how to satisfy these requirements, but recognise that such controls shall meet the various baseline objectives described in GovS:007.

13. With certain contracts, the CA may define the classified aspects in a Security Grading Guide (SGG) that is referenced in the SAL.

14. The SAL (or its SGG) shall identify in as much detail as possible which components are classified and at what level. This is because classified information can 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. It will then be necessary to allocate the appropriate levels of classification to the equipment as a whole and to its component parts. These may vary in different circumstances, such as during manufacture as against during use. For example, a radio transmitter might not attract a classification, but the frequency at which it operates could need to be classified

SECRET. This would mean that:

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

- during and after assembly, the complete equipment will become SECRET and therefore an accountable item that will require appropriate protection.

- 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.

15. Where the size of a classified hardware asset permits, it should be stored in an approved container in the same way as a classified document. Where this is impracticable, it will be necessary to carry out a separate risk assessment. Such an assessment shall always be conducted in conjunction with the CA.

16. For certain international collaborative projects, there may be an applicable Project Security Instruction (PSI) agreed amongst the project participants, which may include special security procedures. For the Defence Supplier to comply with the PSI, it needs to be included in the contract or elsewhere in the contractual documentation by the CA. Defence Suppliers shall flow down relevant clauses of the PSI to their Subcontractors/Suppliers.

Contractual Security Conditions

17. The Defence Supplier shall flow down all applicable contractual security conditions issued by the CA when subcontracting or collaborating with other Defence Suppliers on classified work. Defence Suppliers shall also seek permission to subcontract or collaborate with other Defence Suppliers when required in accordance with the Subcontracting or Collaborating on Classified MOD Programmes ISN. Below is a summary of the standard MOD Contractual Security Conditions.

18. DEFCON 660 OFFICIAL-SENSITIVE Security Requirements specifies the measures to be taken to protect OFFICIAL-SENSITIVE material including the requirements to flow down security requirements to any Subcontractor/Supplier. DEFCON 660 shall be included in all contracts containing OFFICIAL aspects (including those that are subject to DEFCON 659A and/or other security conditions). A copy of the OFFICIAL and OFFICIAL-SENSITVE Security Conditions included at **Annex B** shall also be provided for all contracts and subcontracts.

19. DEFCON 531 Disclosure of Information requires the Defence Supplier to safeguard material provided by MOD and to ensure that its employees are aware of their responsibilities before they receive information. There is a mutual obligation to treat in confidence all information disclosed in connection with or under the contract.

20. DEFCON 658 Cyber requires the Defence Supplier to implement cyber security measures to safeguard MOD Information. Defence Suppliers shall be compliant and ensure the compliance of their supply chain with respect to DEFSTAN 05 -138 by flowing down DEFCON 658. Where this condition is invoked, the MOD will assess and set the associated cyber risk profile to which the Defence Supplier must work, with flow down risk profile determined by the Defence Supplier completing an online Risk Assessment using the Supplier Cyber Protection Service Tool.

21. Contracts involving the disclosure of material at SECRET or above are subject to DEFCON 659A Security Measures, obligating Defence Suppliers to comply with security requirements contained in GovS007: Security. DEFCON 659A takes precedence over DEFCON 531. DEFCON 659A must not be referenced in contracts placed with Overseas Defence Suppliers. Overseas security conditions/clauses for ITTs and contracts shall be obtained from the ISAC.

22. Control of Defence Supplier employees at MOD Establishments who need access to classified material, or where they cannot be isolated from access to classified material, is covered in Section 10 of DEFCON 76 Conditions that Apply to Work at UK Government Establishments. DEFCON 76 shall be included in all contracts where work is performed by Defence Supplier employees at MOD establishments and obligates such employees to comply with any establishment security policies/regulations.

Validity / Expiry Date

23. This ISN will expire when superseded or withdrawn.

MOD Point of Contact Details

24. The point of contact in respect of this ISN is:

Industry Security Assurance Centre (ISAC)
Ministry of Defence
email: ISAC-Group@mod.gov.uk (Multiuser).

Annexes:

A. SAL Template

B. OFFICIAL and OFFICIAL-SENSITVE Security Conditions

Annex A

SAL TEMPLATE

For the attention of . . . . . .(insert name of Facility Security Controller or senior management contact in the cases of non-FSC 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 classified material. 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 classification. Material passed to you will bear the classification appropriate to it. However, to assist you in allocating any necessary classification 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 classification to apply to the various aspects of the tender / subcontract / order.

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

ASPECTS	CLASSIFICATION

(Note: Add more rows as required)

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 classification 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 Advisor[1].

6. A copy of this letter has been sent to your Security Advisor.[2]

---

[1] *Reference to the Security Advisor should only be made in SALs addressed to FSC Suppliers.* Note: If the Contracting Authority for the main contract requires that protective security controls above the baseline defined in GovS 007 be applied to this subcontract these should be set out in a separate paragraph in the SAL.

[2] Delete paragraph if SAL is being provided to a Non- FSC or Overseas Supplier.

Annex B

UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS

Purpose

1. This document provides guidance for Defence Suppliers where classified material provided to or generated by the Defence Supplier is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (Email: DOS-DSR-IIPCSy@mod.gov.uk).

Definitions

2. The term "Authority" for the purposes of this Annex means the UK MOD Contracting Authority.

3. The term "Classified Material" for the purposes of this Annex means classified information and assets.

Security Grading

4. The SENSITIVE marking is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the 'need to know'. The Security Aspects Letter, issued by the Authority shall define the UK OFFICIAL-SENSITIVE material that is provided to the Defence Supplier, or which is to be developed by it, under this Contract. The Defence Supplier shall mark all UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading. The Defence Supplier is not required to mark documents graded UK OFFICIAL unless they are transmitted overseas or generated by a Defence Supplier based outside the UK in a third-party country.

Security Conditions

5. The Defence Supplier shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex. The Defence Supplier shall make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

6. Where a Defence Supplier is based outside the UK in a third-party country the national rules and regulations of the third-party country take precedence over these conditions only if the third-party country has an extant bilateral security agreement or arrangement with the UK.

7. The Authority shall state the data retention periods to allow the Defence Supplier to produce a data management policy.

8. If you are a Defence Supplier located in the UK, your attention is also drawn to the provisions of the Official Secrets Act 1989 and the National Security Act 2023.

Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material

9. The Defence Supplier shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to 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 Defence Supplier shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.

10. Once the Contract has been awarded, where the Defence Supplier is required to store or process UK MOD classified information electronically, they shall comply with the requirements specified in ISNs, Defence Condition 658 and Defence Standard 05-138. Details can be found at the links below:

https://www.gov.uk/government/publications/industry-security-notices-isns.
https://www.dstan.mod.uk/toolset/05/138/000004000.pdf
https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down

11. All UK classified material including documents, media and other assets shall be physically secured to prevent unauthorised access. When not in use UK classified material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be controlled.

12. Disclosure of UK classified material shall be strictly controlled in accordance with the *"need to know"* principle. Except with the written consent of the Authority, the Defence Supplier shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Defence Supplier or Subcontractor.

13. Except with the consent in writing of the Authority the Defence Supplier shall not make use of the Contract or any classified material issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 9 above, the Defence Supplier shall not make use of any article or part thereof similar to the articles for any other purpose.

14. Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Defence Supplier from using any specifications, plans, drawings and other documents generated outside of this Contract.

15. 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 37.

Access

16. Access to UK classified material shall be confined to those individuals who have a *"need-to-know"*, have been made aware of the requirement to protect the material and whose access is essential for the purpose of their duties.

17. The Defence Supplier shall ensure that all individuals requiring access to UK OFFICIAL and UK OFFICIAL-SENSITIVE material have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Defence Supplier; 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 UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

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

Hard Copy Distribution

18. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed internally and externally of Defence Supplier premises. To maintain confidentiality, integrity and availability, distribution shall be controlled such that access to documents is only by authorised personnel. They may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must not appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

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

Electronic Communication and Telephony and Facsimile Services

20. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using a UK 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

21. Exceptionally, in urgent cases UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the prior approval of the Authority. However, it 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 require. Such limitations including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the information.

22. UK OFFICIAL and UK OFFICIAL-SENSITIVE information may be discussed verbally on corporate telephones and other corporate electronic devices with persons located both within the country of the Defence Supplier and overseas. UK OFFICIAL-SENSITIVE information should only be discussed where there is a strong business need to do so.

23. UK OFFICIAL information may be faxed to recipients located both within the country of the Defence Supplier and overseas, however UK OFFICIAL-SENSITIVE information may be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

Use of Information Systems

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

25. The Defence Supplier should ensure **10 Steps to Cyber Security** (Link below) is applied in a proportionate manner for each IT and communications system storing, processing or generating UK OFFICIAL or UK OFFICIAL-SENSITIVE information.

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

26. 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. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing UK OFFICIAL and UK 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 are to 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 are to be "strong" using an appropriate method to achieve this, e.g., including numeric and "special" characters (if permitted by the system) as well as alphabetic characters.

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

e. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g., point to point computer links) via a public network like the Internet, using a UK MOD approved cryptographic technique as described in paragraph 20 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:

(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.

(3) The accounting records are to have a facility to provide the System Manager with a hard copy of all or selected activity. There also must 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 must 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 are to 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 are to 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" will 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".*

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 must not be connected direct to the Internet or "un-trusted" 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).

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

Portable Electronic Devices

27. Portable Electronic Devices holding any UK OFFICIAL-SENSITIVE information shall be encrypted in accordance with Defence Standard 05-138.

28. Unencrypted Portable Electronic Device and drives containing personal data are not to be taken outside of secure sites[3]. For the avoidance of doubt the term *"drives"* includes

[3] Secure Sites are defined as either Government premises or a secured office on the Defence Supplier premises.

all removable, recordable media e.g., memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

29. 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.

30. Portable Electronic Devices holding the Authorities' data 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 Portable Electronic Device 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

31. The Defence Supplier shall immediately report any loss or otherwise compromise of any Defence Related Classified Material to the Authority. The term Defence Related Classified Material includes any information or asset that has been given a security classification by the UK MOD. The term also includes classified information and assets held by UK Defence Suppliers which are owned by a third party e.g., NATO or another country for which the UK MOD is responsible.

32. In addition, any loss or otherwise compromise of Defence Related Classified Material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP). This will assist the UK MOD in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD's Chief Information Officer (CIO) and, as appropriate, the Defence Supplier concerned. The UK MOD Defence Industry WARP will also advise the Defence Supplier what further action is required to be undertaken.

UK MOD Defence Industry WARP Contact Details
Email: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)
RLI Email: defencewarp@modnet.r.mil.uk (MULTIUSER)
Telephone (Office hours): +44 (0) 3001 583 640
Mail: Defence Industry WARP, DE&S PSyA Office
MOD Abbey Wood, NH2 Poplar-1 #2004, Bristol, BS34 8JH

33. Reporting instructions for any security incidents involving Defence Related Classified Material can be found in the Incident Reporting Industry Security Notice at:

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

Subcontracts

34. Where the Defence Supplier wishes to subcontract any elements of a Contract to Subcontractors within its own country or to Subcontractors located in the UK such subcontracts will be notified to the Authority. The Defence Supplier shall ensure that these Security Conditions are incorporated within the subcontract document.

35. The prior approval of the Authority shall be obtained should the Defence Supplier wish to subcontract any UK OFFICIAL-SENSITIVE elements of the Contract to a Subcontractor facility located in another (third party) country. The first page of MOD Form 1686 (F1686) is to be used for seeking such approval. The MOD Form 1686 can be found in the "Subcontracting or Collaborating on Classified MOD Programmes ISN" at the link below:

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

36. If the subcontract is approved, the Defence Supplier shall flow down the Security Conditions in line with paragraph 34 above to the Subcontractor. Defence Suppliers located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

Physical Destruction

37. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE 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. Advice shall be sought from the Authority when the classified material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Defence Supplier to be necessary or desirable. Unwanted UK OFFICIAL-SENSITIVE classified material which cannot be destroyed in such a way shall be returned to the Authority.

Private Venture Activities

38. Private Venture (PV) funded (i.e., non-MOD funded) defence related projects and technology fall within one of the following three categories:

a. Variants. Variants of standard defence equipment under research, development or in production, e.g., aircraft, military vehicles or ships, etc. with non-standard equipment or fitments, offered to meet special customer requirements or to avoid security or commercial difficulties associated with the sale of an item in-Service with UK Armed Forces.

b. Derivatives. Equipment for military or civil use that is not based on standard Service designs but is dependent upon expertise or technology acquired in the course of defence contracts.

c. Freelance. Equipment of defence importance that is in no way based on information gained from defence contracts.

39. UK Defence Suppliers shall ensure that any PV activity that falls into one of the above categories has been formally security graded by the MOD Directorate of Security and Resilience. Please see PV guidance on the following website further information: https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets

Publicity Material

40. Defence Suppliers wishing to release any publicity material or display assets that arises from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Defence Supplier'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 UK Government.

41. For UK Defence Suppliers where the exhibition assets relate to multiple Delivery Teams or for Private Venture defence related classified material where there is no defined Delivery Team, the Defence Supplier shall request clearance for exhibition from the Directorate of Security and Resilience. See the MOD Exhibition Guidance on the following website for further information:

https://www.gov.uk/government/publications/private-venture-pv-grading-and-exhibition-clearance-information-sheets

Export sales/promotion

42. The Form 680 (F680) security procedure enables MOD to control when, how, and if defence related classified material is released by UK Defence Suppliers to foreign entities for the purposes of promotion or sales of equipment or services. Before undertaking any targeted promotion or demonstration or entering into any contractual commitments involving the sale or release of defence equipment, information or technology classified UK OFFICIAL-SENSITIVE or above to a foreign entity, a UK Defence Supplier shall obtain F680 approval from the Export Control Joint Unit (ECJU) MOD Team. This includes assets classified UK OFFICIAL-SENSITIVE or above either developed to meet a UK MOD requirement or Private Venture (PV) equipment, as formally advised in a Security Aspects Letter (SAL) issued by the relevant Authority, or PV Security Grading issued by the MOD Directorate of Security and Resilience. Guidance regarding the F680 procedure can be found at:

https://www.gov.uk/government/publications/ministry-of-defence-form-680-procedure-guidance

43. If a Defence Supplier has received an approval to subcontract, under an MOD Form 1686 (F1686), for development/production of parts of an equipment, that approval also permits the production of additional quantities for supply to an export customer, when the Defence Supplier has MOD Form 680 approval for supply of the complete equipment, as long as:

a. they are identical, except for component obsolescence, to items produced under the UK programme that the approval to subcontract relates to; and

b. no additional OFFICIAL-SENSITIVE or above material is required to be released to the overseas Subcontractor.

Interpretation/Guidance

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

45. Further requirements, advice and guidance for the protection of UK classified material at the level of UK OFFICIAL and UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

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

Audit

46. Where considered necessary by the Authority the Defence Supplier shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Defence Supplier's processes and facilities by representatives of the Defence Supplier's National/Designated Security Authorities or the Authority to ensure compliance with these requirements.