C17 CSAE DT
Walnut 2B, #1229
MOD Abbey Wood, Bristol
BS34 8JH

File ref: SAL 707083450 v1

Date of Issue: 21 Nov 2024

CONTRACT NUMBER & TITLE: C17CSAE/707083450 CSAT Recap Phase 2

1. On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced Contract that constitute classified material.

2. Aspects that constitute OFFICIAL-SENSITIVE for the purpose of DEFCON 660 are specified below. These aspects must be fully safeguarded. The enclosed Security Condition outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
Passenger details and flight manifests	OFFICIAL SENSITIVE
Defensive Aids Suites (DAS) GFE	OFFICIAL SENSITIVE at rest
Military Global Positioning System (GPS)	OFFICIAL SENSITIVE

3. Your attention is drawn to the provisions of the Official Secrets Act 1989 and the National Security Act 2023. In particular you should take all reasonable steps to make sure that all individuals employed on any work in connection with this Contract have notice of the above specified aspects and that the aforementioned statutory provisions apply to them and will continue to apply after completion or earlier termination of the Contract.

4. Will you please confirm that:

a. This definition of the classified aspects of the referenced Contract has been brought to the attention of the person directly responsible for security of classified material.

b. The definition is fully understood.

c. The requirement and obligations set out above and in any contractual document can and will be met and that the classified material shall be protected in accordance with applicable national laws and regulations.

d. All employees of the company who will have access to classified material have either signed an OSA/NSA Declaration Form in duplicate and one copy is retained by the

Company Security Officer or have otherwise been informed that the provisions of the OSA/NSA apply to all classified information and assets associated with this contract.

5. If you have any difficulty either in interpreting this definition of the classified aspects or in safeguarding them, will you please let me know immediately.

6. Classified Information associated with this Contract must not be published or communicated to anyone without the approval of the MOD Contracting Authority.

7. Any access to classified information or assets on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Security Officer (PSyO) in accordance with DEFCON 76.

8. Contact details for the MOD Delivery Team Security Lead are included below:

Yours faithfully

Samantha Knight

Senior Cyber Security Consultant
CSAT Delivery Team Security Lead
Samantha.knight125@mod.gov.uk

Copy via email to:
ISAC-Group (MULTIUSER)
COO-DSR-IIPCSy (MULTIUSER)
UKStratComDD-CyDR-CySAAS-021

Issued 15 April 2024

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: COO-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/05/138/000003000.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:

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

Hard Copy Distribution

19. 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.

20. 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

21. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or 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 and CPA scheme are available at:

https://www.ncsc.gov.uk/guidance/tls-external-facing-services
https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

22. 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.

23. 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.

24. 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

25. 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.

26. 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

27. 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 CPA product or equivalent 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

28. Portable Electronic Devices holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 20 above.

29. Unencrypted Portable Electronic Device and drives containing personal data are not to be taken outside of secure sites[1]. For the avoidance of doubt the term *"drives"* includes all removable, recordable media e.g., memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

30. 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.

31. 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

32. 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.

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

33. 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

34. 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

35. 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.

36. 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

37. 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

38. 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

39. 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.

40. 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

41. 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.

42. 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

43. 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

44. 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

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

46. 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

47. 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.