Ministry of Defence

Industry_Security_Notice

Number 2018/06

Subject:_**Australia-UK_Security_Arrangement Arrangements_for_the_Handling_and_Transmission_of _Defence_Classified_Information**

Introduction

1. The Department of Defence of Australia (AUS DoD) and the Ministry of Defence of the United Kingdom of Great Britain and Northern Ireland (UK MOD) have signed a new bilateral security Arrangement for the Protection of Defence Classified Information which came into effect on 9 November 2018. The Arrangement provides a government-to-government assurance for the exchange and protection of defence classified information between the AUS DoD, UKMOD and their respective suppliers.

2. The purpose of this Industry Security Notice (ISN) is to inform suppliers of the specific arrangements that have been agreed concerning the handling and transmission procedures for defence classified information at UK OFFICIAL-SENSITIVE (UK OS) and Australian PROTECTED (AUS P) levels between our two countries – these arrangements take effect immediately. By implementing these arrangements, such classified information may be disclosed or released on a need to know basis and in accordance with the principle of originator control, by the originating party to the recipient party.

Arrangements

3. The following arrangements have been agreed between the AUS DoD and UK MOD that sets out the policies, practices and procedures for the handling and transmission of defence classified information:

- On a government-to-government level, AUS P classified information corresponds directly to UK OS classified information and will be handled and protected in accordance with respective national laws and regulations. However, access to and protection of such classified information by Australian and UK suppliers will be subject to the following conditions:

a. Suppliers to UK MOD will handle and protect AUS P as UK OS but will also apply the additional measures of protection outlined in the UK Cabinet Office document "*Guidance Protecting International RESTRICTED Classified Information"* or successor document found at: www.gov.uk

b. Australian suppliers will be required to handle and protect UK OS classified information in accordance with the "Annex - *UK Official and UK Official-Sensitive Security Conditions"* attached to this ISN.

c. Access to AUS P and UK OS classified information will be limited to those personnel who as a minimum, have been subjected to basic recruitment checks which should establish proof of nationality, identity and confirms that they satisfy all legal requirements for employment and verification of their employment record. Criminal records checks should also be undertaken as required under UK national laws, regulations and policies.

d. Australian suppliers are not required to hold a facility security clearance for access to UK OS classified information. Suppliers to UKMOD are not required to hold a facility security clearance for access to AUS P.

e. Classified information at UK OS level may be transmitted physically by suppliers to UK MOD (subject to release approval from MOD sponsors) direct to Australian suppliers in accordance with national procedures which, may include the use of commercial couriers. The Security Conditions Annex attached to this ISN should be appended to the classified material as part of the required security measures.

f. Transmission of AUS PROTECTED and UK OS classified information by electronic means will be protected using cryptographic devices that have been approved by the AUS DoD and UK MOD Security Authorities.

g. Suppliers to UK MOD will handle and protect Australian sensitive information at the level of **Australian OFFICIAL:Sensitive** to the same degree as UK classified information at the level of UK OFFICIAL. Information at the UK OFFICIAL and Australian OFFICIAL:Sensitive levels may be transmitted electronically in clear text.

h. Suppliers to UK MOD will handle and protect Australian legacy sensitive information at the level **FOR OFFICIAL USE ONLY** to the same degree as UK classified information at the level of UK OFFICIAL.

- The physical transfer of classified information/material as freight between the UK and Australia will be subject to approval of a Transportation Plan/Movement Security Plan by the AUS DoD and UK MOD respective Security Authorities.

- General advice on the handling and transmission of classified information can be sought from the following national Security Authorities:

UK Competent Security Authority
Defence Equipment and Support – PSyA-Security Advice Centre, Poplar -1, ~2004, MOD Abbey Wood, Bristol BS34 8JH
E: DESPSyA-SecurityAdviceCentre@mod.gov.uk

UK Designated Security Authority
Ministry of Defence – Directorate of Security and Resilience (DSR-STInd), Level 4, Zone B, Main Building, Whitehall, London SW1A 2HB
E: DSR-STind@mod.gov.uk

Action_by_Industry

4. Suppliers to the UK MOD are advised to follow the arrangements provided herein when handling AUS P classified information and/or releasing UK OS classified information to Australian suppliers. Further advice can be sought from the Security Authorities listed above as necessary.

Validity_/_Expiry_Date

This ISN is valid with immediate effect and remains so until further notice.

MOD_Point_of_Contact_Details

Ministry of Defence
Directorate of Security and Resilience (DSR-STInd), Level 4, Zone B, Main Building, Whitehall, London SW1A 2HB
E: DSR-STind@mod.gov.uk
T: 0207 218 4263

ANNEX

UK_OFFICIAL_and_UK_OFFICIAL-SENSITIVE_Security_Conditions_for_Classified_Contracts

Purpose

1. The document provides guidance for Contractors where information and material provided to or generated by the Contractor is classified as UK OFFICIAL and UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not well understood, further advice should be sought from the **Defence Security and Vetting Service, Australian Department of Defence (DS&VS), Campbell Park Offices, PO Box 7951, Canberra BC ACT 2610, Australia**.

Definitions

2. The term **"Authority"** for the purposes of this Annex means a UK Ministry of Defence (MOD) official acting on behalf of the Secretary of State for Defence.

3. The term **"Contract"** for the purposes of this Annex means an agreement between two or more parties creating and defining enforceable rights and obligations under domestic law between those parties.

4. The term **"Contractor"** for the purposes of this Annex means any individual, organisation, or other entity, including sub-Contractors, who is negotiating or has entered into a Classified Contract.

5. The term **"Need-to-Know"** for the purposes of this Annex means the principle that access to Classified Information should be limited those who need to use such information in order to perform their official or contracted duties.

6. The term **"Service Provider"** for the purposes of this Annex means a company that provides services to a contractor which may enable that company to access Classified Information. Examples of this include managed service providers of information infrastructure.

Facility Security Clearance

7. The UK does not require a Facility Security Clearance (FSC) to be held by Australian facilities handling UK information classified as UK OFFICIAL-SENSITIVE.

Security_Grading

8. All aspects associated with Contracts involving the provision or generation of information or material classified as UK OFFICIAL are to be classified UK OFFICIAL. Some aspects are more sensitive and are classified as UK OFFICIAL-SENSITIVE. The Security Aspects Letter, issued by the Authority specifically defines the UK OFFICIAL-SENSITIVE information that is furnished to the Contractor, or which is to be developed by it, under this Contract. The Contractor will mark all UK OFFICIAL-SENSITIVE documents

which he or she originates or copies during the Contract clearly with the UK OFFICIAL-SENSITIVE classification.

Security_Conditions

9. The Contractor will take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and will continue so to apply after the completion or earlier termination of the Contract.

Protection_of_UK_OFFICIAL_and_UK_OFFICIAL-SENSITIVE_Information

10. The Contractor must protect UK OFFICIAL and UK OFFICIAL-SENSITIVE information 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 Contractor will take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.

11. Where Contractors are asked to apply Industry Security Notice (ISN) 2017/01 requirements to industry owned IT and communication systems used to store, process or generate UK Ministry of Defence information (including those systems containing UK OFFICIAL and/or UK OFFICIAL-SENSITIVE information) they will contact and consult with the Australian Department of Defence, DS&VS on these requirements. ISN 2017/01 details UK Ministry of Defence Assurance and Risk Tool (DART) registration, IT security accreditation processes, risk assessment and risk management requirements. The ISN is available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594320/DART_ISN_-_V2_3.pdf

12. All UK OFFICIAL and UK OFFICIAL-SENSITIVE material including documents, ICT media and other material must be physically secured to prevent unauthorised access. When not in use UK OFFICIAL and UK OFFICIAL-SENSITIVE documents/material must be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE documents/material must be stored under lock and key and be placed in a lockable room, cabinets, drawers or safe and the keys/combinations must be subject to a level of control.

13. Disclosure of UK OFFICIAL and UK OFFICIAL-SENSITIVE information must be strictly controlled in accordance with the "Need-to-Know" principle. Except with the written consent of the Authority, the Contractor must not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Contractor or sub-Contractor, or Service Provider.

14. Except with the consent in writing of the Authority the Contractor is not to make use of the Contract or any information issued or furnished by or on behalf of the Authority otherwise than for the purpose of the Contract, and, save as provided for in paragraph 13 above, the Contractor must not make use of any information or material, or part thereof, for any other purpose.

15. Subject to any intellectual property rights of third parties, nothing in this Security Condition restricts the Contractor from using any specifications, plans, drawings and other documents generated outside of this Contract.

16. 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 must be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 38 below.

Access

17. Access to UK OFFICIAL and UK OFFICIAL-SENSITIVE information will 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 their duties.

18. The Contractor must ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE information have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where permissible under national/local laws, regulations and policies. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS).

Hard_Copy_Distribution

19. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed, both within and outside company premises, only in such a way as to make sure that no unauthorised person has access. It 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 should 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. Additional advice on the distribution of UK OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of UK OFFICIAL-SENSITIVE hardware can be sought from the Authority, and/or from DS&VS.

Electronic_Communication_and_Telephony_and_Facsimile_Services

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

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

Details of the CPA scheme are available at:

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

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 must 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 requires. Such limitations including any regarding publication, further circulation or other handling instructions will be clearly identified in the email sent with the material.

23. UK OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the country of the Contractor and overseas. UK OFFICIAL-SENSITIVE information may be discussed on fixed and mobile telephones only where there is a strong business need to do so and only with the prior approval of the Authority.

24. UK OFFICIAL information may be faxed to recipients located both within the country of the Contractor and overseas, however UK OFFICIAL-SENSITIVE information may be faxed only where there is a strong business need 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 Contractor must ensure **10 Steps to Cyber Security** is applied in a proportionate manner for each IT and communications system storing, processing or generating MOD UK OFFICIAL or UK OFFICIAL-SENSITIVE information. 10 Steps to Cyber Security is available at:

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

The Contractor is to ensure competent personnel apply 10 Steps to 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.

28. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing 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, for example, 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 21 above.

f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

(1). The following events are to 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,

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.

Laptops

29. Laptops holding any UK MOD supplied or Contractor generated UK OFFICIAL-SENSITIVE information are to be encrypted using a CPA product or equivalent as described in paragraph 21 above.

30. 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.

31. 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.

32. Portable CIS devices holding MOD 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 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

33. The Contractor is to immediately report the loss of any UK OFFICIAL or UK OFFICIAL-SENSITIVE information to the Authority and to DS&VS (Security Incident Centre).

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

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/293480/ISN2014_02_Incident_Reporting.pdf

any security incident involving any UK MOD owned, processed or Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE information is to be immediately reported to the UK 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 UK MOD's Chief Information Officer (CIO) and, as appropriate, the company concerned. The UK 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@mod.gov.uk **- Email: For those without access to the RLI:** CIO-DSAS-SyCCOperations@mod.gov.uk

Telephone: Working Hours: +44 (0)30 677 021 187

Out of Hours/Duty Officer Phone: +44(0)7768 558863

Fax: +44(0)1480 446328

Mail: Joint Security Co-ordination Centre (JSyCC), X007 Bazalgette Pavilion, RAF Wyton, Huntingdon, Cambs PE28 2EA.

DS&VS Security Incident Centre Contact Details Email: Security.IncidentCentre@defence.gov.au

Telephone: Working Hours: (02) 6266 3331

Out of Hours/Duty Officer Phone: 0416 060 347

Sub-Contracts

35. Where a Contractor has sub-contracted any elements of a Contract to a sub-Contractor within Australia or to Contractors located in the United Kingdom, such sub-Contracts will be notified to the Authority. When sub-contracting to a sub-Contractor located in either Australia or to the UK, the Contractor must ensure that these Security Conditions are incorporated within the sub-Contract document. The prior approval of the Authority is to be obtained should the Contractor wish to sub-Contract any UK OFFICIAL-SENSITIVE elements of the Contract to a sub-Contractor facility located in another (Third Party) country. The first page of Appendix 5 (MOD Form 1686 (F1686)) of the Security Policy Framework Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at Appendix 5 at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf

36. If the sub-Contract is approved, the Authority will provide the Contractor with the Security Conditions that should be incorporated within the sub-Contract document.

Publicity_Material

37. Contractors wishing to release any publicity material or display hardware 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 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 UK MOD, the military services or any other government department.

Destruction

38. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE information/material must 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 is to 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 UK OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way is to be returned to the Authority.

Interpretation/Guidance

39. Advice regarding the interpretation of the above requirements should be sought from the Authority or from DS&VS.

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

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

Audit

41. Where considered necessary by the Authority or by DS&VS, the Contractor is to provide evidence of compliance with these Security Conditions and/or permit the inspection of the Contractors processes and facilities by representatives of the national security authorities of the Authority or DS&VS to ensure compliance with these