



Ministry
of Defence

Industry Security Notice

Number 2020/05

Subject: CANADA / UK INDUSTRIAL SECURITY ARRANGEMENT - Arrangements for the Handling and Transmission of Classified and Protected Information

Introduction

1. The Government of Canada (CAN) and the Government of the United Kingdom of Great Britain and Northern Ireland (UK) reached agreement on a bilateral **Industrial Security Arrangement (ISA)** for the Protection of Classified and Protected Information which was signed on 7 September 2016. The ISA provides a government-to-government assurance for the exchange and protection of Classified and Protected Information between CAN and UK authorities and their respective suppliers.

2. The purpose of this Industry Security Notice (ISN) is to inform UK suppliers of the specific arrangements that have been mutually agreed concerning the handling and transmission procedures for Classified and Protected Information at UK OFFICIAL (UK O) – UK OFFICIAL-SENSITIVE (UK OS) and Canadian PROTECTED A & B levels between our two countries – these arrangements are effective immediately. By implementing these arrangements, Classified and Protected Information may be provided subject to release approval and on a need-to-know basis.

Arrangements

3. The following arrangements have been agreed between CAN and UK that sets out the policies, practices and procedures for the handling and transmission of Classified and Protected Information:

- a. On a government-to-government level, it is recognised that there is no CAN security classification equivalence with the UK OS classified marking. Similarly, there are no UK security classification

equivalence with the CAN PROTECTED A & B markings. However, if the information to be exchanged is strictly between two government entities, the PROTECTED A (lowest of the CAN Protected markings) shall be treated as UK OS and vice-versa. As for PROTECTED B, the CAN documents will normally be safeguarded in security containers approved for UK SECRET unless otherwise indicated on the document handling instruction cover sheet. Access to and protection of UK OS information by CAN suppliers and PROTECTED information by UK suppliers will also be subject to the following conditions:

b. UK contractors will handle and protect PROTECTED A & B information in accordance with appropriate contract clauses and handling instructions that will be provided by CAN to inform recipients of the minimum security requirements for the protection of such information. It is expected the CAN contract clauses for PROTECTED A information will necessitate protective security measures similar to those applied for the protection of UK OS classified information in line with national laws and regulations. PROTECTED B information may require more stringent protective security measures (as per para 3a above) unless otherwise supported by a handling instruction.

c. Canadian contractors will be required by contract to handle and protect UK OS classified information in accordance with the “Annex - *UK Official and UK Official-Sensitive Contractual Security Conditions*” attached to this ISN and PROTECTED A & B information in line with their national industrial security program policy.

d. In general, access to PROTECTED A & B and UK OS information will be limited to those personnel who as a minimum, have been subjected to basic recruitment checks which should establish proof of identity, nationality, right to work, employment history and a check of criminal records as permitted under UK and CAN national laws, regulations and policies. (i.e. within the UK, the Baseline Personnel Security Standard (BPSS)). Where additional checks may be required outside of the UK BPSS checks for PROTECTED B, this will be identified in CAN contract clauses and handling instructions.

e. Canadian suppliers are not required to hold a Facility Security Clearance (FSC) or any other organization screening for access to UK OS classified information. Similarly, suppliers to UK MOD are not required to hold an FSC (i.e. List X) for access to PROTECTED A & B level classified information.

f. Classified information at UK OS level may be transmitted physically by UK contractors direct to CAN contractors in accordance with national procedures, which, may include the use of commercial couriers. Such transmission is subject to obtaining the release approval from MOD sponsors. This ISN and the Security Conditions Annex attached to this ISN must be agreed by CAN contractors before UK OS level information is transmitted.

g. Transmission of CAN PROTECTED A & B information and UK OS classified information by electronic means will be protected using cryptographic devices that have been approved by the CAN and UK MOD Security Authorities. Classified information at the UK O level may be transmitted electronically in clear text subject to any 'Handling Instruction'. Specific methods of transmission will be identified in the contractual conditions.

h. When no longer required, or when the contract is completed, CAN PROTECTED A & B and UK OS information may be retained in accordance with the contractual requirements/conditions. Disposal of such information must be via nationally approved methods of destruction, standards and/or as stipulated in the contractual conditions. Such disposal/destruction methods include information in paper or electronic form.

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

4. General advice on the handling and transmission of classified information for UK suppliers can be sought from the following UK MOD 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 – Security Policy & Operations - Directorate of
Security and Resilience (SPO DSR-STInd), Level 4B, Main Building,
Whitehall, London SW1A 2HB

E: SPODSR-STInd@mod.gov.uk

Action by Industry

5. Suppliers based in the UK are required to follow the arrangements provided herein when handling CAN PROTECTED information and/or releasing UK OS classified information to Canadian suppliers. Further advice for release of classified information to a supply chain outside of the UK and Canada can be sought from the UK MOD Security Authorities listed above as necessary.

Validity / Expiry Date

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

MOD Point of Contact Details

7. Ministry of Defence, Security Policy & Operations - Directorate of Security and Resilience (SPO DSR-STInd), Level 4B, Main Building, Whitehall, London SW1A 2HB
E: SPODSR-STInd@mod.gov.uk

UK / Canadian Industrial Security Arrangement (ISN 2020/05)
UK OFFICIAL and UK OFFICIAL-SENSITIVE Contractual Security
Conditions

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 UK Designated Security Authority (address details at paragraph 4 above) or the Director International Industrial Security - Designated Security Authority - Public Services and Procurement Canada - 2745 Iris Street, Ottawa, K1A 0S5 - Canada, TPSGC.dgsssiprojetintl-dobissintlproject.PWGSC@tpsgc-pwgsc.gc.ca as appropriate.

Definitions

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

Security Grading

3. All aspects associated with this Contract are 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 shall mark all UK OFFICIAL or UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract clearly with the UK OFFICIAL or UK OFFICIAL-SENSITIVE classification.

Security Conditions

4. The Contractor shall take all reasonable care and adhere to the controls outlined in the Contract and listed in this Annex. The Authority must state the data retention periods to allow the Contractor to produce a data management policy.

Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Information

5. The Contractor shall 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 shall take all reasonable steps to prevent the loss or compromise of the information whether accidentally or from deliberate or opportunist attack.

6. Once the Contract has been awarded, where Contractors are required to store or process information electronically, they are required to register the IT system onto the UK MOD Defence Assurance Risk Tool (DART). Details on the registration process can be found in the 'Industry Security Notices (ISN)' on Gov.UK website. ISNs 2017/01, 04 and 06, Defence Conditions 658 and Defence Standard 05-138 details the DART registration, IT security accreditation processes, risk assessment/management and Cyber security requirements which can be found in the following links:

[https://www.gov.uk/government/publications/industry-security-notices-isns.](https://www.gov.uk/government/publications/industry-security-notices-isns)

<http://dstan.gateway.isg-r.r.mil.uk/standards/defstans/05/138/000002000.pdf>

<https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down>

7. All UK OFFICIAL and UK OFFICIAL-SENSITIVE material including documents, media and other material must be physically secured to prevent unauthorised access. When not in use UK OFFICIAL and UK OFFICIAL-SENSITIVE documents/material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE documents/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 subject to a level of control.

8. 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 shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Contractor or sub-Contractor.

9. Except with the consent in writing of the Authority the Contractor shall not 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, same as provided for in paragraph 8 above, the Contractor shall not make use of any article or part thereof similar to the articles for any other purpose.

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

11. 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 32.

Access

12. Access to UK OFFICIAL and UK 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 their duties.

13. The Contractor shall ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE information have undergone basic recruitment checks. This should include establishing proof of identity and nationality; 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 and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf

Hard Copy Distribution

14. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may 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 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.

15. 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 UK Designated Security Authority and/or the Canadian DSA.

Electronic Communication and Telephony and Facsimile Services

16. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information will normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product; a MOD approved cryptographic technique such as Transmission Layer Security (TLS) or a product mutually agreed between the sender and recipient. 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>

17. 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 material.

18. 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.

19. UK OFFICIAL information may be emailed/faxed to recipients located both within the country of the Contractor 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

20. 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.

21. The Contractor 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 MOD UK OFFICIAL or UK OFFICIAL-SENSITIVE information. The Contractor should ensure competent personnel apply 10 Steps to Cyber Security.

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

22. 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.

23. 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 and should be eight or more characters in length, 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 16 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.

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

24. Laptops holding any UK MOD supplied or Contractor generated UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 16 above.

25. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites¹. 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.

26. 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.

27. 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

¹ Secure Sites are defined as either Government premises or a secured office on the contractor premises.

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

28. 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) below. 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: DefenceWARP@mod.gov.uk (OFFICIAL with no NTK restrictions)

RLI Email: defencewarp@modnet.rli.uk (MULTIUSER)

Telephone (Office hours): +44 (0) 30 6770 2185

JSyCC Out of hours Duty Officer: +44 (0) 7768 558863

Mail: JSyCC Defence Industry WARP

X007 Bazalgette Pavilion,

RAF Wyton, HUNTINGDON, Cambridgeshire, PE28 2EA.

29. Reporting instructions for any security incidents can be found in Industry Security Notice 2017/03 as may be subsequently updated at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651683/ISN_2017-03_-_Reporting_of_Security_Incidents.pdf

Sub-Contracts

30. Where the Contractor wishes to sub-contract any elements of a Contract to sub-Contractors within its own country or to Contractors located in the UK such sub-contract will be notified to the Contracting Authority. The Contractor shall ensure that these Security Conditions are incorporated within the sub-contract document.

31. For MOD contracts, the prior approval of the Authority shall 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://www.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf

32. If the sub-contract is approved, the Contractor will flow down the Security Conditions in line with paragraph 30 above to the sub-Contractor. Contractors located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

Publicity Material

33. 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.

Physical Destruction

34. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE information/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 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 shall be returned to the Authority.

Interpretation/Guidance

35. Advice regarding the interpretation of the above requirements should be sought from the UK Designated Security Authority or the Canadian DSA as identified in paragraph 1 of this Annex.

36. Further requirements, advice and guidance for the protection of UK 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

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