Ministry
of Defence

Industry Security Notice

Number 2022/10

Subject: **Clarification on Requirements for Remote Working with MOD Material**

Introduction

1. The UK Defence Supply Base processes a significant amount of MOD material at the OFFICIAL classification level.

2. This ISN provides clarification in respect of how to work on such material when working remotely, for instance when dealing with COVID-19 travel restrictions.

Issue

3. The typical requirements placed on the Defence Supply Base for protection of MOD material assume a situation where a majority of staff needing access are on premises, with remote working normally being handled on an exception basis.

4. This clarification provides generic requirements for Remote Working with MOD Material.

Action by Industry

5. Members of the UK Defence Supply Base needing to support Remote Working shall follow the additional stipulations below, in respect of:

- Remote Working Practices
- Discussion of MOD Information
- Securing MOD Information
- Physical Site Security
- Security Breaches

6. **Remote Working Practices.** Existing mandatory security practices shall be followed when handling MOD information classified at SECRET and above, in accordance with the Security Aspect Letter (SAL).

7. When handling MOD information classified as OFFICIAL, or OFFICIAL with need-to-know restrictions (for example, OFFICIAL-SENSITIVE), this shall:

i. follow the current company processes for approval of remote working;
ii. only be on company issued and managed devices, systems and/or services within the UK, unless export and accreditation approval have been obtained;
iii. only use a secure WiFi connection that is password protected;
iv. use a VPN (where appropriate), in line with company profile.

8. MOD information shall not be under-classified so that it can be worked on remotely.

9. Personal devices and/or accounts shall not be used to handle MOD information, this includes forwarding work email containing MOD information to personal email accounts.

10. **Discussing MOD Information.** MOD Information classified at OFFICIAL and/or OFFICIAL with need-to-know restrictions (for example OFFICIAL-SENSITIVE) may be discussed in the UK using the PSTN, mobile phones and VOIP (for example Skype).

11. When discussing MOD Information classified at OFFICIAL and/or OFFICIAL with need-to-know restrictions, the following criteria shall be met:

a. Conversations are only held with key parties, for which a direct/indirect contractual relationship exists (covered by an associated SAL or equivalent) and the recipient(s):

i. hold(s) a sufficient level of clearance for the information being discussed;
ii. has (have) a confirmed need-to-know requirement for the information being discussed.
iii. are informed of any additional procedural measures, for the safeguarding of the information, the recipient is informed at the beginning of the conversation.

b. Conversations conducted using VOIP are performed using an application approved by the company.

c. Conversations:

i. are not conducted in a public location or in a location where it could be overheard;
ii. are conducted using headphones, where necessary to enforce any need-to-know requirements;
iii. are not conducted in the vicinity of smart home speakers or devices (for example, Amazon Echo, Google Home and Smart TVs). Where this is unavoidable, ensure the devices are disconnected or switched off prior to all conversations.

d. Where there are multiple participants in a ‘virtual meeting’, it is the meeting organiser’s responsibility to confirm only authorised individuals are present on the call.

12. **Securing MOD Information.** All MOD information shall be handled in accordance with the SAL (or equivalent document), this includes:

a. adhering to any handling instructions or need-to-know restrictions;
b. minimising the amount of hardcopy produced, with the presumption of material being read on screen preferentially;
c. protecting of all MOD information in accordance with company policy, and in particular avoiding placing un-shredded material in household waste.

13. To ensure the protection of MOD information whilst travelling:

a. company device encryption must be enabled, for example: by powering off/shutting down the device;

b. any secure token associated with the company device must be carried separately, for example: not in the same bag/case as the device;

c. devices (e.g. laptops) should be carried in line with company policy;

d. all hardcopy OFFICIAL information assets should be placed in a single covered opaque envelope (with no GSC marking) or folder and placed within a bag/case;

e. all MOD information assets classified as OFFICIAL with need-to-know restrictions (for example: OFFICIAL-SENSITIVE), should not, for any period of time, be:

i. opened/accessed/viewed in a public area;

ii. left unattended for any period of time, for example: hotel, restaurant, taxi, public service vehicle, railway carriage; and/or

iii. left in an unattended motor vehicle.

14. To ensure the protection of MOD information whilst remote working:

a. Care must be taken to not draw attention to the fact that MOD information is being worked on;

b. MOD information shall be viewed only in a way that it cannot be overseen by people who are not authorised. This can be achieved by making sure:

i. the area used minimises overlooking and unexpected interruptions from people;

ii. a clear desk policy is implemented;

iii. devices are locked, or shut down when leaving it unattended for any period of time;

iv. devices and document hardcopies are not to be entrusted to the custody of a member of the public who does not hold a security clearance, for example, left with a house/flat co-resident.

c. devices holding MOD information and/or MOD information assets shall be stored in a secure location, for example: a cabinet/cupboard/drawer (preferable lockable). Where this is not possible, then a location that is concealed or not obvious shall be used, and if possible devices should be physically secured, for example by using a ‘laptop lock/cable’;

d. all MOD information assets classified as OFFICIAL with need-to-know restrictions (for example: OFFICIAL-SENSITIVE) in digital forms shall be protected by encryption;

e. all MOD information assets and MOD or company devices (provided to you for purposes of remote working) shall be returned to the company and/or MOD once remote working has ceased or disposed of in accordance with MOD and company policy.

15. **Physical Site Security.** Whilst the majority of the workforce may be remote working, it is important to ensure premises physical security controls shall be maintained.

16. **Security Breaches.** All confirmed or suspected breaches involving MOD information shall be accurately and quickly reported to your Security Officer, in line with your company procedures, for onward transmission as necessary to DefInd WARP. The report should include details of quantities, location(s), and any handling instructions or need-to-know restrictions.

Validity / Expiry Date

17. This ISN will expire when superseded or withdrawn.

MOD Point of Contact Details

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

Info & Info-Cyber Policy Team
Directorate of Cyber Defence & Risk (CyDR)
Ministry of Defence
tel: +44-20-721-83746 (PSTN)
email: UKStratCom DD-CyDR-InfoCyPol@mod.gov.uk (Multiuser)