Industry Security Notice

Number 2010/04

POLICY TO PROTECT PORTABLE INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) DEVICES AND MEDIA

INTRODUCTION

1. The purpose of this Industry Security Notice (ISN) is to communicate to defence contractors the MOD policy for procedural, personnel, physical and technical controls to secure ICT devices and media (e.g. Laptops, PDAs, CDROMs and USB memory sticks, external drives, etc) when they are being used off-site.

2. The direction in this ISN derives from the Security Policy Framework (SPF), issued by the Cabinet Office, in particular: Mandatory Requirement 42 which covers remote working/mobile media; Mandatory Requirement 14 which relates to personal data; and Mandatory Requirement 40 relating to encryption requirements.

3. This ISN supplements the requirements contained in the Restricted Security Conditions contained in MOD contracts that include UK Restricted aspects.

ISSUE

4. Home/remote working introduces vulnerabilities associated with off-site and portable ICT devices and media. The nature of portable ICT devices and media increases the risk to the information stored on them due to the increased chance of loss or theft compared to fixed devices.

5. The reputational damage to an organisation, whether a Government Department or Commercial Enterprise, caused by the loss of quantities of Protectively Marked information or personal data can be significant.

6. In order to protect MOD Protectively Marked information and personal data on portable ICT devices and media additional control measures are required.

DEFINITIONS

7. The following terms are used within this notice:

MOD Information – is HMG information that has been supplied by the MOD or generated by the contractor as a consequence of a MOD contract or programme.

Personal Data – as described in ISN 2010/01 and HMG IA Standard 6.

Portable ICT Devices – those systems which have no fixed secure location. The term includes laptops and other handheld devices (such as PDAs, Smart Phones and Blackberry™).

Removable Recordable Media – all media capable of storing data that do not normally form a fixed part of a device. These include all magnetic media types (e.g. floppy disks, magnetic tapes and cartridges, and external hard drives), optical media (e.g. CDs and DVDs), compact flash and solid state devices (e.g. SD cards, USB Memory Devices and PCMCIA cards).

Secure Location – facility with security measures commensurate with the Protective Marking of the information or asset.

ACTION BY INDUSTRY

MANDATORY

8. Portable ICT devices and media holding any MOD personal data or MOD information must be protected in accordance with direction given in the Policy section of this notice.

RECOMMENDED

9. Further guidance on encryption, remote working and removable media is published by MOD and a number of other HMG organisations, a selection of which are listed in the Further Information section of this notice. This guidance may prove useful to security staff, Information Assurance (IA) practitioners or other appropriate company officers when determining how to comply with the requirements of this notice.

VALIDITY

10. This notice supersedes the direction previously communicated in Industry Security Advice Bulletin (ISAB) 2008-02 and List X Notice (LXN) 2008-04, both of which are now cancelled.

11. The policy applies from the date of publication of this ISN and until rescinded.

POLICY

Portable ICT Devices

12. Portable ICT devices holding any MOD information or personal data must not be taken outside a secure location unless, as a minimum, a FIPS 140-2 approved full disk encryption solution is installed. Unencrypted portable ICT devices holding MOD personal data not at a secure location must be recalled and only used or stored in an appropriately secure location until appropriate full encryption is installed.

13. HMG contractors not engaged on MOD contracts should seek clarification from their contracting authorities but it is strongly recommended that laptops processing Protectively Marked data (PROTECT and above) are full disk encrypted.

14. The protection offered by encryption is often only enabled when the device is powered off or shutdown and not when it is left in the standby mode. Security staff should ensure that user operating procedures relating to the use of screen lock, shutdown and the physical securing devices reflect this limitation. The risk of theft or loss will determine which security precautions are appropriate.

15. Any tokens, touch memory devices or password(s) associated with the encryption package must be kept separate from the device whenever the device is not in use, left unattended or in transit.

16. In order to deter opportunist theft of ICT devices it is recommended that:

a) when being transported in vehicles they are <u>secured</u> out of sight for the duration of the journey e.g. in the boot/luggage compartment, not simply under cover in the passenger compartment,

b) they are not left unattended in any public location,

c) security staff determine workable, effective security instructions appropriate to the user's working environment.

<u>Removable Recordable Media</u>

17. Removable recordable media holding information at Impact Level 1 (IL1)[1] (PROTECT) and above must be encrypted in accordance with this policy except for the specific cases in paragraph 23.

18. Unencrypted removable recordable media containing IL1 and above information not held on a secure site must be recalled and only used or stored in an appropriately secure location until approved full encryption is installed.

19. Where removable recordable media is created specifically for release to the public, encryption is not required. Such media should be marked 'For Public Release'.

COMPLIANCE

20. CESG's position is that Impact Level 3 information requires protection by products assessed by CESG as suitable for RESTRICTED coupled with supply of CESG key material. However, they recognise there may be difficulty meeting greatly increased demand for approved products and key material in the short-term and acknowledge that pragmatic decisions will need to be taken when selecting products. To this end, commercial grade encryption products which have been approved to the FIPS 140-2 standard are an acceptable alternative where the CESG Baseline product cannot be procured within reasonable timescales.

21. The existing encryption policy requirements for Impact Level 4 and above information remain unchanged.

[1] Impact Levels are defined in HMG IA Standard No. 1 – See Further Information section of this notice.

22. A full list of the approved CESG encryption products to protect Protectively Marked material and sensitive data can be found in either the CESG Approved Products List or the MOD ICS Catalogue. Defence Information Assurance Note 15 Lite (included as an Annex to ISN 2010/01) details a number of additional encryption products which are acceptable for use to protect MOD information. Guidance on which encryption products are suitable for encrypting optical media should be sought from the appropriate Government contact in the Points of Contact section of this notice.

23. In certain circumstances removable recordable media may be used without encryption:

a. data transfer purposes of information between systems, if used within the same secure location e.g. building, computer room or server room,

b. system back-ups (retained for business continuity purposes) retained within the same secure location, or stored within a different secure location (including transfer between secure locations) or

c. digital cameras exclusively (such media should be secured when not in use).

Where encryption is not used the risk must be reflected in a Risk Assessment (taking account of any aggregation effect) and where appropriate documented in the system RMADS[2] and approved by the system accreditor.

24. Where the encryption policy for portable ICT devices or removable media handing MOD information or personal data cannot be met the circumstances must be reported to the Contracting Authority so that a Risk Balance Case (RBC) can be produced and assessed by MOD security advisors.

FURTHER INFORMATION

25. Further information, aimed at security staff, IA practitioners or other appropriate company officers, is available from the following sources.

Information Commisioner's Office (www.ico.gov.uk)
Framework Code of Practice for Sharing Personal Information
Approach to Encryption
Data Security Tips

Department for Business Innovation and Skills (www.bis.gov.uk)
Information Security Section
Business Links Information Security Guidance (www.businesslink.gov.uk)

[2] Risk Management and Accreditation Document Set.

Cabinet Office
HMG Security Policy Framework (SPF) outlines the mandatory security requirements and management arrangements to which all Departments and Agencies (defined as including all bodies directly responsible to them) must adhere.
http://www.cabinetoffice.gov.uk/intelligence-security-resilience/intelligence-and-protective-security.aspx
Security Policy 2: Protective Marking and Asset Control. Mandatory Requirement 14.
Security Policy 4: Information Security and Assurance. Mandatory Requirement 40.
Security Policy 4: Information Security and Assurance. Mandatory Requirement 42.

CESG (www.cesg.gov.uk)
CESG offers a range of products and services including technical consultancy and advice, policy documentation, product evaluation and training, primarily to UK government and the armed forces, the wider public sector, and industries forming part of the Critical National Infrastructure, such as power and water. Non-Governmental organisations with a current Government contract may receive information from CESG under sponsorship of the contracting authority; details on the procedure can be found on their website or via the CESG enquiries desk.

Impact Level Tables:
http://www.cesg.gov.uk/publications/media/policy/is1_risk_assessment.pdf#page=47
http://www.cesg.gov.uk/policy_technologies/policy/media/business_impact_tables.pdf
Approved Products List: http://www.cesg.gov.uk/products_services/iacs/caps/index.shtml

HMG IA Standard No. 4 – Communications Security and Cryptography.
HMG IA Standard No. 6 – Protecting Personal Data and Managing Information Risk.
Good Practice Guide 5 – Securing Data at Rest on Laptops.
Good Practice Guide 10 – Remote Working.

MOD
http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/DESPSYA/
ISN 2010/01 - Handling MOD Personal Data. (includes DIAN 15 Industry Lite Version – Encryption of CIS Media).

POINT OF CONTACT

26. The MOD point of contact for clarification on the scope of this notice is:

DBR-DefSy-InfoSy Pol
Level 1, Zone I
MOD Main Building
London, SW1A 2HB

27. For guidance regarding the use of portable CIS and media for processing or storing non-MOD information the relevant contracting authority should be consulted.