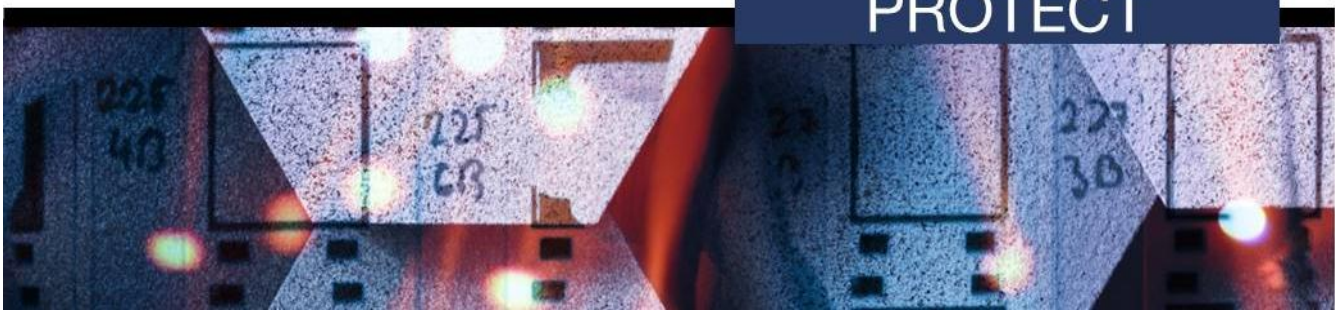

DECEMBER 2012

Travelling Overseas with Electronic Devices (Technical Guidance)

Introduction

1. This publication has been developed to assist IT security staff to secure electronic devices and information before employees travel overseas. It should be read in conjunction with the guidance in the *Travelling Overseas with Electronic Devices (User Guidance)* publication available from the Australian Cyber Security Centre (ACSC) website.
2. For devices carrying classified information, the *Australian Government Information Security Manual* (ISM) contains further guidance.

Mitigation strategies

3. The following mitigation strategies should be implemented before employees travel overseas in order to maximise the security of devices and the information held on them. This is general guidance which may not be applicable to every device.
    a. Update the operating system and all applications on devices. Most updates are fixes for identified security vulnerabilities and should be applied as soon as they become available.
    b. Restrict administrative privileges on devices to only users who need them. Restrict user's rights in order to permit them to only execute a specific set of predefined functions as required to complete their duties.
    c. Implement application whitelisting on devices, such as Microsoft AppLocker, to only allow approved programs to run. For tablets and smartphones, use Mobile Application Management tools to specify which applications are allowed to be run.
    d. Install antivirus software on devices. Virus pattern signatures should be checked for updates several times per day and installed as soon as they become available. All storage should be regularly scanned for malicious code.
    e. Where possible, install a firewall to protect against malicious incoming network traffic.
    f. Disable unnecessary features or software; minimising software on devices reduces opportunities to gain access to devices through software-based security vulnerabilities.
    g. Implement passphrase policies as per the ISM or device-specific hardening guides.

Device encryption

4. All devices should be encrypted to mitigate the risk of unauthorised access to information if a device is lost or stolen. In doing so, organisations should use either full disk encryption or partial disk encryption where access controls will only allow writing to encrypted partitions.

5. Full disk encryption provides a greater level of protection than file based encryption. While file based encryption may protect individual files there is a risk that unencrypted copies of the file may be left in temporary locations used by the operating system. Full disk encryption also allows operating system and software files to be more easily protected from an adversary with physical access.

Network connections

6. Configure wireless security settings on devices such that they can't connect to ad-hoc wireless networks. Further, configure devices such that split tunnelling is disabled when users connect back to the organisation via a Virtual Private Network (VPN) to browser the Web or access their emails. Finally, disable Bluetooth pairing by default. This can be enabled if required but should be done prior to the departure of employees on overseas travel.

Further information

7. The *Australian Government Information Security Manual* (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

8. The *Strategies to Mitigate Cyber Security Incidents* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

9. Additional platform-specific hardening guides are available on the Australian Cyber Security Centre website to assist organisations in the secure configuration of devices. This guidance is available at https://www.acsc.gov.au/publications/.

Contact details

10. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).