DECEMBER 2012

Technical advice: Travelling overseas with an agency issued electronic device

1. This product has been developed to assist IT security staff to secure agency devices and information before employees travel overseas. It should be read in conjunction with the advice provided in the document *Travelling Overseas with an electronic device*. Additionally, this document should be considered in conjunction with an agency developed risk assessment for high threat travel situations and with Department of Foreign Affairs and Trade travel advice. For devices carrying classified information please consult the *Australian Government Information Security Manual* (ISM).

Mitigation Strategies

2. Government employees travelling overseas face additional information security risks. The following advice provides steps IT security staff should take before agency employees travel in order to maximise the security of devices and the information held on them. This is general advice which may not be applicable to every device.

a. Update the operating system and all software applications installed on the device before the trip and while away. It is important to note most updates are fixes for identified vulnerabilities and should be applied as soon as they become available. If using a Windows operating system, automatic updates should be used. However if using automatic updates this should be done through connection to a Virtual Private Network (VPN) back to the agency.

b. Minimise administrative privileges on the device to only users who need them. You should restrict the user's rights in order to permit them to only execute a specific set of predefined functions as required to complete their duties.

c. Enable application whitelisting to only allow approved programs to run, while all other programs are blocked from running by default. Solutions include Microsoft AppLocker. For tablets and smartphones use mobile application management to specify which applications are allowed to be used.

d. Install an agency approved antivirus product on the device. 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. This will reduce the risk of the device being compromised by malicious software.

e. Where possible, install a firewall to protect against malicious or unauthorised incoming network traffic, preferably one from DSD's Evaluated Products List.

f. Disable unnecessary features or software; minimising software on the device reduces opportunities to exploit and gain access to the device through software vulnerabilities.

g. For all hardware and software, implement passphrase policies as per the ISM or, if available, a device-specific DSD hardening guide (as passphrase policies may differ from the generic advice in the ISM). This includes preventing the user changing their passphrase more than once a day.

h. Use the data execution prevention functionality, preferably hardware, which will run additional checks to ensure that certain types of vulnerabilities are harder to exploit.

3. Base-line the device prior to departure and again on return to look for any signs of compromise. This involves auditing what is installed and running on the device and how it is configured prior to travelling and doing the same when it returns. Ensure that any changes to the device have been approved and authorised. If you note anything of concern report the incident to the Cyber Security Operations Centre who will advise of further action you can take.

4. Once you have base-lined the device upon return it is important to wipe or reset the device. This should be done even if nothing suspicious is noted.

Encryption

5. DSD recommends that information on all mobile devices be encrypted. Refer to the ISM for evaluated products and approved algorithms.

6. Encryption at rest: All mobile devices should be encrypted in order to mitigate the risk of unauthorised access to information. Agencies using encryption to secure data at rest should implement evaluated products and approved algorithms and should use either:

a. full disk encryption; or

b. partial disk encryption where the access control will only allow writing to the encrypted partition.

7. 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.

8. It is important to ensure that the device's data is protected when traversing a network. Ensure your browser supports only approved SSL cyphers as specified in the ISM. Ensure that appropriate network security settings are implemented and are consistent with ISM requirements.

Networks

9. Configure wireless security settings so that the device is not allowed to connect to ad-hoc wireless networks.

10. Devices should not be allowed to connect to wireless networks, except when temporarily connecting to facilitate the establishment of a VPN. All web browsing and email should be conducted through the agency's VPN.

11. Disable split tunnel VPNs. These can allow access to internet systems via an unsecured connection while connected to your agency's network through a VPN. This can bypass the normal security controls implemented by your agency on its Internet connection and increase the risk of the VPN being attacked from unsecured networks.

12. Disable Bluetooth pairing by default. This can be enabled if required but should be done prior to departure.

Further information

13. The *Australian Government Information Security Manual* assists in the protection of official government information that is processed, stored or communicated by Australian Government systems: http://www.dsd.gov.au/infosec/ism/index.htm

14. DSD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies can be found at:
http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

15. DSD creates device-specific guidance such as hardening guides which should also be read in conjunction with this document. These documents can be found at:
http://www.dsd.gov.au/publications/index.htm

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.