Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

# Travelling Overseas with Electronic Devices

JUNE 2019

## Introduction

The targeting of electronic devices used by personnel during overseas travel is a real and persistent threat. Electronic devices likely to be targeted include, but are not limited to, corporate and personal laptops, phones, tablets and removable media such as USB drives and SD cards. The compromise of electronic devices could impact the ongoing operation and security of an organisation's business.

Generally, the risks associated with electronic device usage during overseas travel are:

- The compromise of electronic devices could give an adversary access to sensitive information (including user credentials). This could immediately impact the integrity, confidentiality or operational security of an organisation's business activities.
- The compromise of electronic devices could allow an adversary to propagate into any connected networks putting additional sensitive information on such networks at risk. This could have a long-lasting impact on the integrity and confidentiality of an organisation's business activities.
- The compromise of electronic devices belonging to personnel of enduring interest, such as an organisation's senior personnel, could result in immediate or ongoing operational security or safety concerns for targeted personnel.

## Securing electronic devices before overseas travel

The following measures should be implemented before travelling personnel depart:

- If appropriate, issue travelling personnel with newly provisioned accounts and electronic devices from a pool of dedicated travel devices to be used solely for work-related activities. Further, advise travelling personnel against taking their own personal electronic devices, especially if the devices are rooted or jailbroken.
- If appropriate, apply SCEC-endorsed tamper seals to key areas of electronic devices, such as hard drive bays, removable media slots and other external interfaces in addition to educating travelling personnel on an associated inspection regime to detect any attempted tampering.
- Record details of electronic devices such as product type, serial number and International Mobile Equipment Identity (IMEI) in an inventory of electronic devices being taken.
- Ensure electronic devices are running a vendor supported operating system that is fully patched and securely configured with all non-essential accounts, information and functionality removed.
- Configure remote locate and wipe capabilities of electronic devices and ensure they are encrypted, including when locked if possible, and using pre-boot authentication.

# Securing electronic devices during overseas travel

The following measures should be implemented during overseas travel:

- Report any loss, suspected compromised or unusual behaviour (including the type, date and time) for electronic devices, including multi-factor authentication tokens, to the organisation's designated security personnel as soon as possible.
- Assume any electronic devices that have been taken out of sight for inspection by foreign government officials, or have been lost or stolen and later found or returned, to be potentially compromised.
- Never lend electronic devices to untrusted people, even if only briefly (e.g. to check the weather or sports results).
- Never allow untrusted people to charge their electronic device using your electronic device (e.g. charge their phone using your laptop).
- Never use chargers supplied by third parties or charge electronic devices at designated charging stations or USB charging outlets. Only use genuine chargers supplied with electronic devices.
- Never place electronic devices, including multi-factor authentication tokens, in check-in luggage. Further, never leave electronic devices, including multi-factor authentication tokens, or luggage containing such items, unattended, even in hotel safes.
- Store authentication credentials (e.g. passwords and/or multi-factor authentication tokens) separately to electronic devices they are used to authenticate to.
- Avoid connecting electronic devices to any open or untrusted Wi-Fi networks. Regardless, use an approved Virtual Private Network (VPN) connection to encrypt all internet traffic. Alternatively, use per-application VPNs for all web browsing, email and instant messaging applications.
- Use encrypted Voice over IP (VoIP) applications for making calls instead of calls in the clear over foreign telecommunication provider networks.
- Disable any communication capability for electronic devices when not in use (e.g. cellular data, Wi-Fi, Bluetooth and Near Field Communication (NFC)).
- In locations where sensitive conversations take place, power-down electronic devices and remove them from close proximity to the sensitive conversations.
- Avoid re-using removable media after connecting it to other organisation's electronic devices as they may not provide the same level of security as your organisation or their electronic devices could be compromised.
- Ensure removable media provided by other organisations for data transfers are appropriately checked prior to being connected to your electronic devices noting some malware residing on removable media may not be detectable.
- Never use any gifted electronic devices, especially removable media, when travelling overseas or when returning to Australia. If required, purchase electronic devices from established and reputable local businesses.

# Securing electronic devices after overseas travel

The following measures should be implemented after travelling personnel return:

- If appropriate, reset user credentials used with electronic devices, including those used for remote access to the organisation's networks.

- If appropriate, monitor user accounts of personnel that had recently travelled overseas for indicators of compromise. In particular, pay close attention to failed logon attempts using user credentials that have been recently reset.
- Sanitise all removable media used by travelling personnel and decommission multi-factor authentication tokens that left the physical possession of travelling personnel.
- Sanitise and reimage electronic devices as per organisational procedures.

If at any point following overseas travel significant doubts exist as to the integrity of an electronic device's firmware or hardware, the electronic device should be sanitised, reimaged and redeployed for purposes that do not pose a risk to either sensitive information or enduring personnel of interest.

The choice to decommission electronic devices for any reason should not be taken lightly given the considerable financial burden this may place on organisations.

# Further information

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

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

Additional platform-specific guidance is available to assist organisations in the secure configuration of electronic devices. This guidance is available at https://www.cyber.gov.au/publications/.

# Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).