Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

JULY 2012

MOBILE TECHNOLOGIES IN INTERNATIONAL TRAVEL

Guidance for Government of Canada IT Security Managers

ITSB-88

INTRODUCTION

This guidance publication outlines best practices to support the development of departmental travel IT Security policies for travel ranging from routine low risk business travel to high risk travel requirements.   Risk should be assessed by the department based on such factors as the:

- travel destination;
- travel duties, including the travelers role, responsibilities and information holdings; and
- anticipated engagements, events and activities during travel.

SECURITY CONSIDERATIONS

Government employees embarking on international travel face many Information Technology (IT) security risks. As an IT Security manager, it is important that you inform travelers of security best practices.   Any compromise of their device could have a negative impact on your department, its information and its reputation. A compromise has the potential to spread to other areas of the network resulting in issues such as: downgrades in system performance, outages, lost productivity and costly recovery efforts. It is beneficial for departments to adopt a risk-based functionality posture while safeguarding against threats.

Consider these key points:

- Travelers face a wide variety of threats, including those associated with wireless technologies.
- Individuals holding more senior positions within government and/or those that work with valuable information may be at higher risk.
- Capabilities exist which allow threat actors to:
  - identify and target mobile devices;
  - deliver malicious code to the device;
  - use the network connections of the device (e.g.: wireless, Bluetooth) for their purposes;
  - leverage the device as a means of infecting other GC department networks;
  - access the device as a means to track your location (e.g.: GPS);
  - remotely activate the microphone on a device; and
  - intercept many types of communications that are sent electronically.

Note: It is the departments' responsibility to assess the level of risk associated with travel requirements. The following best practices serve as general recommendations only. Departments should select best practices to enhance their security posture as they deem necessary. For example, if the travel risk is assessed as low, a department may still choose to implement additional security recommendations to enhance their security posture.

GUIDANCE ON RISK MANAGEMENT FOR INTERNATIONAL TRAVEL

To support business travelers, it is important to align security practices with the perceived level of risk. The following scenarios illustrate recommended device guidelines, security requirements and IT dependencies associated with high and low risk travel.

	HIGH RISK TRAVEL	LOW RISK TRAVEL
Device Guidelines	Issue a temporary device or a device from a travel inventory.	Use the regular business device.
Security Requirements	Wipe and re-format travel inventory devices as per departmental procedures and implement travel best practices as noted in this bulletin. Where possible: ▪ Use a separate network infrastructure to support travel devices. ▪ Increase logging and monitoring capabilities on the travel devices.	Limit administrative privileges. Implement travel best practices as noted in this bulletin.
Dependencies	Procure temporary devices to be used for high-risk travel and/or establish a travel inventory of pre-configured devices. Consider using a commercial service to avoid any possible connection to the departmental network.	None

RECOMMENDATIONS FOR INTERNATIONAL TRAVEL

To further enhance the risk scenarios, the following table outlines steps departments should take **before, during** and **after** the travel period to increase the security of the information stored on mobile devices and to better protect the departmental network.

- Assess the threat: Consider the nature of the travel as well as the travelers' role, responsibilities and information holdings.
- Assess information requirements: Determine if the traveler needs to communicate sensitive or classified information. Inform the traveler of any known country specific customs and immigration restrictions if they plan to use encryption or high-assurance products. Consult the Departmental Security Officer (DSO) or Departmental COMSEC Authority (DCA).
- Educate the traveler: User education is an essential step to ensuring that travelers are aware of the threat and manage the risk accordingly. Implement a mandatory travel briefing for international travel, and refer them to the publication; *Mobile Technologies in International Travel: Guidance for Government of Canada Business Travelers (ITSB-87)*.

HIGH RISK TRAVEL

Issue the traveler with a travel inventory device or a temporary device that will be returned after travel and implement the following security practices:

- Prepare travel devices with only the minimum data required for the trip:
  - ensure applications installed on the mobile devices have the latest patches;
  - disable unnecessary features or software (e.g.: WiFi, infrared ports, Bluetooth);
  - update the web browser with strict security settings;
  - implement a locked-down travel profile on the Blackberry Enterprise Server (for Blackberry devices); and
  - ensure that the traveller has contact information to report security issues / incidents.
- Consider using a commercial service to avoid any connection to the departments' network.
- Prepare for incident handling:

  - increase logging and monitoring capabilities; and
  - image the device using a mobile device management (MDM) application to allow for comparisons.
- When they return:
  - recall travel inventory device or temporary device;
  - if an incident is suspected, report the event to the Government of Canada Cyber Threat Evaluation Centre (GC CTEC) (ctec@cse-cst.gc.ca) as per the GC IT Incident Management Plan (IT IMP); and
  - re-image the device and/or replace the SIM card as per department procedures (following incident reporting).
- Implement additional security features noted below.

BEST PRACTICES - BEFORE THEY TRAVEL

Employees frequently travel to low risk locations and it would be difficult to assess security requirements on a case-by-case basis. As a general baseline, departments should strive to implement the following best practices for mobile devices, including:

- Install up-to-date anti-virus protection, spyware protection, OS security patches, and a firewall and ensure that the user cannot disable these features.
- Configure devices to run anti-virus software on storage devices on access (e.g.: USB) upon installation and explain the procedures to the traveler.
- Limit and restrict administrative privileges and have the traveler update passwords before and after travel.
- Ensure that proper network security settings are implemented for devices such as laptops.
- Verify that mobile devices such as laptops are not able to access the internet at the same time the user is accessing the department's internal network.
- Ensure proper security settings are implemented for VPN accesses (if applicable).
- Prepare for Incident Handling:
  - increase logging and monitoring capabilities (when applicable);
  - install a mobile device management (MDM) application to assist with the identification of security compromises. MDMs allow departments to compare device images before and after travel to identify discrepancies; and
  - ensure that the traveler has contact information for the IT Service Desk.

BEST PRACTICES - WHILE THEY TRAVEL

- When possible, maximize your monitoring capabilities for devices that are associated with international travel and look for unusual activity and anomalies, such as:
  - unauthorized connection attempts;
  - connection attempts which occur at unusual times; and
  - unusual and unauthorized VPN activity (e.g.: split tunnels).
- Be available to respond to IT user questions and concerns while they travel (e.g.: lost device, security concerns);

BEST PRACTICES - WHEN THEY RETURN

- Assist employees in resetting their credentials after they return, including both remote and local accesses.
- Consult the user to obtain information about any reported issues, unusual device behaviour or any other security concerns.

- Follow incident handling procedures:
  - examine the device for the presence of malicious software before connecting to a GC network;
  - continue to monitor for unusual behaviour, including the remote access accounts of employees who returned from travel to ensure unauthorized accesses are not occurring;
  - compare the current image with the baseline image (if available) to identify signs of compromise;
  - re-image the device before returning it to the travel inventory;
  - test removable memory devices such as CD-ROMs, DVDs and USB sticks that were received during travel before plugging them into the network; and
  - if an incident is suspected, report the event to the Government of Canada Cyber Threat Evaluation Centre (GC CTEC – ctec@cse-cst.gc.ca) as per the GC IT Incident Management Plan (IT IMP).

ADDITIONAL INFORMATION

For additional information about proactive mitigation measures, please consult the CSEC Top 35 Mitigation Measures. For more information about the advice and guidance contained in this publication contact IT Security.

IT Security Client Services
Communications Security Establishment Canada
PO Box 9703, Terminal
Ottawa, ON K1G 3Z4

Email: itsclientservices@cse-cst.gc.ca
Telephone: 613-991-7654