



NCSIP Position Paper

International Travel

Prepared on behalf of NCSIP with input from Committee Members by

Mohammad Qureshi/ONTARIO

2018-01-15

INTRODUCTION

As the cyber landscape continues to evolve and the capabilities of cyber intrusion continue to increase, this publication provides NCSIP's position on best practices to support international travel. Risk related to international travel should be assessed by jurisdictions based on the following:

- Travel destination;
- Travel duties, including the travellers role, responsibilities and information holdings;
- Anticipated engagements, events and activities during travel.

NCSIP POSITION

Government employees embarking on international travel face many information security risks and physical security risks. Any compromise of a travellers' device could have a negative impact on an organization, its information and its reputation. A compromise has the potential to spread to other areas of the network resulting in issues such as system performance, outages, lost productivity, loss of intellectual property, and costly recovery efforts. It is beneficial for organizations to adopt a risk-based assessment for international travel to ensure the security posture is not impacted.

Key areas of consideration include:

- 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 more 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 for their purposes (i.e. wireless, Bluetooth connectivity);
 - Leverage the device as a means of infecting government networks;
 - Access the device as a means to track your location (i.e. GPS);
 - Remotely activate the microphone on a device; and
 - Intercept communications that are sent electronically.



To support business travellers, it is important to align security practices with the perceived level of risk. The following risk levels illustrate recommended device guidelines following a risk assessment that is based on where the individual is travelling to, sensitivity of their position, and sensitivity of the information in their custody:

	High Cyber Risk Travel Minimum Requirement	Low Cyber Risk Travel Minimum Requirement
Education and Awareness	Hold briefings with travellers to raise awareness of the risk. Resources providing these briefings may vary based on available internal resources and ability to leverage external services. Share security best practices for how to work remotely and connect devices while travelling abroad.	
Device Guidelines	Issue a temporary device or a device from a travel inventory (for some jurisdiction, this is a simple cellular phone and not a smart phone)	Use the regular business device
Security Requirements	Wipe and re-format travel inventory devices as per IT procedures. Where possible: <ul style="list-style-type: none"> • Increase logging and monitoring capabilities on the travel devices and travellers user account • Use a separate network infrastructure where one is available to support travel devices 	Limit administrative privileges. Implement travel best practices

RECOMMENDATION

NCSIP members agree that it is critical to provide tools to enable secure international travel by implementing a risk assessment as part of every jurisdictions travel policy. Members also agree that the following steps should be taken before, during and after the travel period to increase the security of information stored on mobile devices and to better protect the network:

- Assess the threat: Consider the nature of the travel as well as the travellers' role, responsibilities and information holdings. Organizations should partner with their Policing departments or intelligence providers, where possible, to assess the threat.

National CIO
Subcommittee on
Information Protection



- Assess information requirements: hold briefings with the traveller to determine if the traveller needs to communicate sensitive or classified information. Inform the traveller of any known country specific customs and immigration restrictions if they plan to use encryption or VPN services for the communications.
- Educate the traveller: user education is an essential step to ensuring the travellers are aware of the threat and manage the risk accordingly. The traveller should be made aware of targeted phishing and social engineering tactics that maybe deployed to gain access to their devices or vulnerabilities associated with connecting to free/hotel Wi-Fi.
- Minimize the attack surface: wherever possible travellers' should be encouraged to leave it behind if it is not required. This applies to both devices and sensitive information.
- Report it: in the event travellers identify something suspicious they should be required to report it as soon as possible. This may include being compelled to log into the device or losing sight of it upon entry into the country.