
Canadian Security Intelligence Service
Service canadien du renseignement de sécurité
FAR FROM HOME
A travel security guide for government officials
FOR OFFICIAL USE ONLY
Canada

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

To request additional copies, please contact:

CSIS Communications Branch
P.O. Box 9732, Postal Station T
Ottawa, ON K1G 4G4
Telephone: 613-231-0100

3103(93/01)

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

YOUR BEST SECURITY TOOL IS YOUR SITUATIONAL AWARENESS

FOR OFFICIAL USE ONLY

THE THREAT ENVIRONMENT

SINCE 9/11 AND THE OCTOBER 2014 ACTS OF TERRORISM ON CANADIAN SOIL, THE TERRORIST THREAT LEVEL TO CANADIANS HAS CHANGED

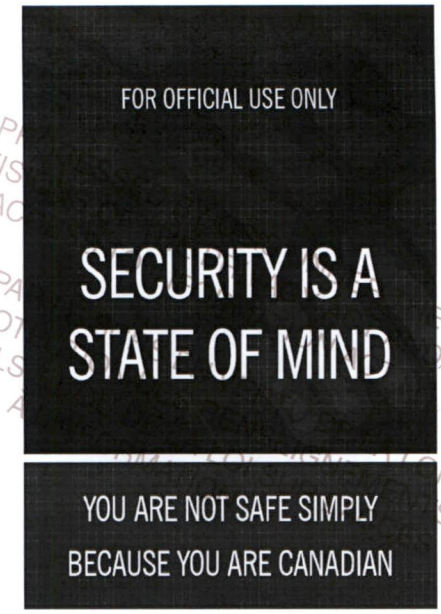
In a world that increasingly measures national power and security in economic as well as military terms, Canadian citizens travelling abroad may be the target of foreign intelligence collection activities. Many foreign governments and foreign businesses place a high priority on acquiring Government-protected information (classified, sensitive and proprietary). Since 9/11 and the October 2014 acts of terrorism on Canadian soil, the terrorist threat level to Canadians has changed. The threat you face as an official Canadian government traveller is real. This brochure describes the nature of the foreign intelligence and terrorism threats, provides basic steps you can take to mitigate the associated risk, and actions you should take to report suspicious incidents.

3103(93/01)

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

3103(93/01)



You are responsible for your own safety. The majority of safety issues can be managed appropriately through good planning, preparation, and sound security practices. The measures you take or do not take directly impact your personal safety and travel overseas.

Your best security tool is your situational awareness, which means being aware of what is going on in your environment and understanding what impact that might have on your personal safety. This could change on a daily or even hourly basis. Always remain aware of the environment and keep up to date on the potential threats in the area within which you are travelling.

The security assumptions we make about overseas travel being easy and safe are often wrong. For many of us, overseas travel has become so routine that we wrongly assume it to be low-risk. You need to take special precautions when travelling in an official capacity, especially to countries of safety and security concerns. You should receive a country-specific briefing from your Departmental Security Officer (DSO) before any trip you take as an official. Never make assumptions when travelling

3103(93/01)

overseas, always research your destination and prepare yourself for your own travel. You are always in charge of your own security.

Your vigilance should be heightened while overseas. When you travel abroad, you are vulnerable due to the limited control you exercise over the environment. Foreign governments and their agents act with greater impunity on their own soil, to say nothing of local extremists and criminals.

It is incumbent upon you to familiarize yourself with the laws, customs and culture of the country or countries you are about to visit. You may be subject to the laws and regulations of the country which you are visiting, and your Canadian citizenship will offer you little immunity, unless travelling under a diplomatic passport with the appropriate accreditations. Note, however, that even the latter does not prevent you from being targeted during your stay in the host country. Before departing you should consult the Global Affairs Canada (GAC) website for country-specific information, as well as keep copies of the contact information for the nearest Canadian Embassy, High Commission or Consulate.

Canada and Canadians are targets for many hostile actors. Canada and Canadians have been, and will continue to be, targeted by foreign intelligence agencies seeking state and industrial secrets; by extremists who see you, as a representative of a Western government, as an enemy; and by criminals who are simply looking for a quick score. In short, you are not safe simply because you are Canadian. In the eyes of those who

3103(93/01)

wish Canada harm, you are a legitimate target. Try to be a hard target by avoiding being predictable and accessible. Maintain good situational awareness.

You don't get to determine whether you're worthy of targeting. You are mistaken if you believe that the contents of your briefcase or the data in your laptop and/or smartphone are not important enough to draw the attention of a foreign intelligence agency. Because Canadians are regarded as "honest brokers" on the world stage, it doesn't mean that extremists won't target you. The fact that you are staying in good accommodations in a good area won't mean that you are less likely to be a victim.

These determinations are up to the threat actors, not you. Always try to maintain a low profile when travelling. Do not wear clothing or other items with logos openly identifying you as a foreign representative. Your dress, discipline and deportment are very important when travelling. Do not display wealth or anything that may increase your value as a target.

Do not overlook the threat posed by thieves. At the very least, briefcases, laptops, smartphones and the like are attractive to common criminals, as they are to foreign intelligence agencies. The result is the same: a security breach—one that could potentially harm you, the Canadian government and/or Canada. Be suspicious of unsolicited offers of assistance and be aware of distractions or diversions that allow unknown individuals to control or funnel your movements.

3103(93/01)

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

3103(93/01)

FOR OFFICIAL USE ONLY

VISA APPLICATIONS AND PREPARING FOR THE TRIP

YOU SHOULD BE AWARE OF THE PUBLICLY AVAILABLE INFORMATION ABOUT YOU

The gathering of information by foreign entities may begin before you even book your flights and hotels. In some countries, information gathering begins well before you arrive. The information you provide on your visa application form could be used to assess your "worthiness" as a target. Your answers contained in the questionnaire could draw a very good initial profile of who you are as a person as well as a Government of Canada employee. If you are part of a high-level delegation, assume you will receive consideration as a potential target.

In order to be successful on your trip, planning and preparation are key. A worthwhile practice is to complete 70% of your planning and preparation in Canada. Before you go anywhere, inform yourself about the general security and political situation in the country. When you arrive in the country you will be ready to put your plan into action. The remaining 30% of your effort can be spent updating and verifying your situational awareness and familiarizing yourself with the country on arrival.

3103(93/01)

Visa applications have become more comprehensive with more questions than ever before. When filling out such applications, be truthful but do not volunteer more information than needed. All visa requirements should be explored prior to booking travel given the intrusive nature of the questions. For example, some countries will request passport numbers of family members, even if they are not travelling with you. Moreover, questions on the nature of your employment can be geared to acquiring very specific details. You should be aware of the publicly available information about you. Google your name and position in advance of your visa application to find out what can be found out about you on the Internet (see the section entitled "Information gathering through open sources.")

Be prepared to answer questions at the point of entry. Before departure, ensure that you will be comfortable answering questions from the host country's customs officials about the reasons for your travel. This is especially important if you are travelling in a group, as any divergence between rationales could be used as a pretext for some kind of action on the part of local authorities.

What should you leave the country with? Alternative means for transferring information you will need while on travel status, especially that of a more sensitive nature, should be considered before you leave Canada.

3103(93/01)

Consult your Departmental Security Officer (DSO) before leaving. In consultation with your DSO, you may want to use a "disposable" telecommunication device while on travel. By disposable, we don't mean that the device is thrown away but rather that it contains no information when you leave and that, upon your return, it is completely wiped clean and the operating system re-installed. You do not want to take abroad a device packed with e-mails, contacts and documents.

Contact lists. Leave behind any address books or lists of names and contact numbers not necessary for the trip.

Communications. Keep others informed of your whereabouts for your own personal safety/security. Leave emergency contact information with your supervisor and arrange regularly scheduled check-in calls or messages at home.

Travel light. Don't saddle yourself with excess baggage because it will attract attention, curtail your mobility and mean you have more to protect.

3103(93/01)

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

3103(93/01)

What to do at any airport. Apart from following normal security procedures at airports, be vigilant and in a position to observe or watch for any type of suspicious activity – from fellow passengers, flight crews, etc.

Airline or border control agents. Assume that any detail given to airline or border control agents will be collected by the host country. It may also be shared with other countries. Keep your passport in your bag or pocket until you arrive at the border control.

Don't advertise your identity. Always conceal your bag tags. In fact, you may want to put the identifying bag tags in your checked bags and use some other type of identifier, such as a ribbon, on the handle.

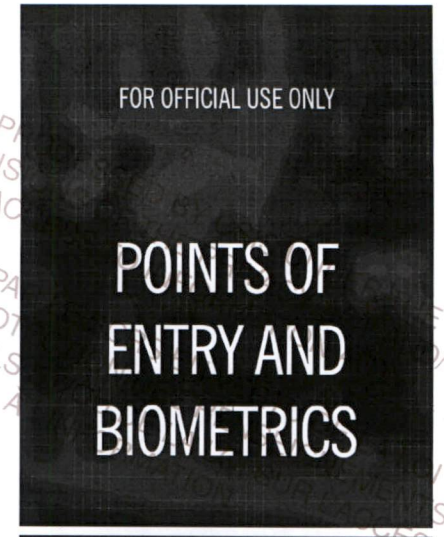
Luggage. Do not leave belongings unattended. Assume your checked luggage will be searched in transit. Do not agree to carry items for other parties unless you are certain of their nature or contents. No one should get control of your suitcases or bags. Maintain physical or visual control of your luggage at all times while in the airport. Baggage claim areas are often where criminals will target their victims. Be especially vigilant in these areas.

3103(93/01)

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

3103(93/01)



ONE SHOULD ALWAYS BE READY TO HANDLE A SECONDARY INSPECTION

Covert and overt means of targeting. Should you be identified as a potential target through the visa application process, the host intelligence agency may undertake covert or overt actions against you to further their information collection efforts.

Surveillance. Assume that in many countries, you will be subject to physical surveillance. A country-specific briefing before departure will assist in broadening awareness on this issue. Don't be paranoid but maintain a healthy level of suspicion.

A secondary search could be used as a pretext to seize or copy your files. One of these overt methods can occur right at the Point of Entry – usually an airport – where you can be selected for a secondary inspection by the local Customs Service. During this inspection, your belongings may be subject to scrutiny e.g. copied and/or seized, including whatever documents you may be carrying on your person, in your laptop, your tablet, and your smartphone.

3103(93/01)

A secondary search could indicate hostile interest. It could also simply mean that you triggered one of the many tripwires used to select passengers for secondary inspections. In either case, one should always be ready to handle a secondary inspection (prepared responses as to purpose of visit; being able to account for one's belongings and so on). You should let your superior or delegation head know you have been selected for a secondary inspection.

Be prepared to invoke your right to a consular visit. Should the questioning during a secondary search become inappropriate or lead to your detention, call the Canadian Embassy, High Commission or Consulate, as you are entitled to Consular Access. When communicating with the Embassy, High Commission or Consulate, keep your description of events to a minimum as somebody may be listening.

Biometrics are increasingly being used. Biometric measures are increasingly being used at points of entry, the purpose of which is to catch criminals and terrorists who can and often do travel using a multitude of identities and documents. At the same time, extensive information is being collected—information that could be used by a hostile intelligence service. This is especially true for individuals who travel to a given country, at different times, for both business and personal reasons; they already know who you are and what you do.

Some biometric techniques include face recognition (including 3D), iris scan and fingerprinting. In some

3103(93/01)

countries, biometrics are taken covertly via closed circuit television and cameras (CCTV). Also, a number of countries share the biometric information they collect with neighboring countries. It is possible that this information is readily available in a country where you have never travelled.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

3103(93/01)

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

3103(93/01)

FOR OFFICIAL USE ONLY

ELICITATION, CULTIVATION AND OTHER TRAPS

ALWAYS BE HEEDFUL OF DISCUSSIONS REGARDING YOUR WORK, EVEN IF SEEMINGLY BENIGN

Why would someone be interested in you? As someone working for the Government of Canada, your access to classified or privileged government and possibly private sector information makes you an attractive target for foreign intelligence services. As such, you may be the source of information or access that a foreign intelligence service needs to fulfill collection requirements which are designed to advance the foreign policy, security, and commercial/economic interests of the collector.

Contacts. Assume that any meetings you have abroad with personal contacts will come to the attention of the foreign government, even if they occur before or after the period of official meetings. Also, assume that non-governmental contacts abroad will be interviewed before your arrival or after your visit, on the nature of your travel and in relation to profile building about you or your staff.

Criminals may be interested in your information, especially if it relates to law enforcement. If your work is law enforcement-related, the information you hold or have potential access to could be of great

3103(93/01)

interest to criminal organizations interested in knowing if there are any investigations targeting them and if there are any "leaks" within their organizations.

Secrets can appear mundane. Those foreign intelligence agencies targeting Canada and Canadians are not solely after the "crown jewels" – such as a blueprint to a new fighter jet or communications infrastructure between the allies – but information that, to the Canadian person or institution holding this information or knowledge, appears unremarkable. Items such as an organizational chart may not appear to be of value but could be considered a key requirement for a hostile intelligence service.

They may be interested in gaining indirect access to an ally. Foreign intelligence agencies may also be interested in the information and access they could obtain via Canada's membership in organizations as diverse as the North Atlantic Treaty Organization (NATO), the G7 and G20, the Commonwealth, la Francophonie, the Organization of American States (OAS), the Asia-Pacific Economic Cooperation (APEC), the Organization for Economic Cooperation and Development (OECD), the United Nations (UN) and the World Trade Organization (WTO).

Gaining access to advanced U.S. technologies. Canada occupies a unique strategic position as a trusted ally of the United States, which gives privileged access to advanced U.S. technologies few others can legitimately procure.

Canada: a source of technological advances and intellectual property. Canada also participates in a system of military and strategic partnerships, and harbours a wealth of natural resources and human talent which continue to generate technological advances. These technologies are coveted by countries interested in developing their own technological and commercial opportunities while avoiding the associated research and development costs. The loss of such information diminishes Canada's competitive advantage and amounts to a transfer of wealth from Canada to another country.

HOW DOES THE GATHERING OF INFORMATION HAPPEN?

Below are some of the most common methods foreign intelligence agencies employ to collect information.

Elicitation. This is a technique used by foreign agency officers and their agents whereby they engage you in what appears to be harmless or random conversation but the aim is subtly to extract information about yourself, your work and colleagues. Warning signs are when your interlocutor:

- Appeals to your ego by flattering you;
- Emphasizes mutual interests and suggests "getting together" at a future date to pursue the mutual interest;
- Uses false statements to get you to correct them with the information you have access to;

3103(93/01)

- Volunteers information – the "give to get" principle at work. They'll share some form of sensitive information with you in the hopes you will return the favour;

- Leads you to believe he/she is very knowledgeable about your area of expertise. If they are an intelligence officer, that knowledge is likely limited and cursory, but just enough to bluff their way through a conversation.

Cultivation. Well-orchestrated approaches by hostile intelligence services begin with a period of "cultivation". A relationship is established between the representative of an intelligence service (whose true identity is unknown) and the unsuspecting person being recruited. You should be vigilant and monitor the progress of associations, particularly new relationships and those with foreign nationals. Always be heedful of discussions regarding your work, even if seemingly benign.

Unwittingly volunteering information. Never talk shop or volunteer information in front of taxi drivers, waiters and bartenders, who could be intelligence officers or informants. Every little bit of information can be useful to a competitor.

The "Vacuum Cleaner" approach or the "Mosaic Effect". Some intelligence agencies use the "vacuum cleaner" approach – they will obtain one piece of information from you and build on that with other pieces of information acquired from your colleagues or that you unwittingly

3103(93/01)

offered to other sources who are working together. You may not think that you have offered any desired information, though when pieced together the result can be quite valuable (thus creating the "mosaic effect").

The Honey Trap. Sexual entrapment, colloquially known as the "honey trap", refers to the use of an attractive individual – informed by your sexual identity and preferences – to seduce you and get you in a compromising position or one where you could be blackmailed. Honey traps often involve the clandestine recording of an intimate encounter. These recordings are either used to blackmail or publicly embarrass the victim. Foreign governments are known to employ this tactic, and employees should be aware of the potential hazards of accepting offers of companionship while travelling. There are also reports of individuals who have suspected they were drugged and who awoke to find that their hotel room had been searched, smartphone stolen and secret business documents missing.

Covert methods including intrusions. Hostile actors may decide to conduct an intrusion operation against you.

This would entail breaking into your hotel room in order to steal or copy sensitive documents in either hard or digital form. Though you may not notice that someone has surreptitiously entered your room, some travellers have returned to their rooms to find individuals searching their belongings or conducting unnecessary maintenance activities. Others have reported laptop computers showing signs of unauthorized usage or actual damage,

3103(93/01)

packages having been opened and resealed or left open, locks on briefcases and suitcases missing or showing signs of forced entry.

- Intrusions may be conducted by the host government, a foreign intelligence service of another country or foreign business operatives.

- Intrusions are frequently accomplished with the cooperation of the hotel staff.

- Several countries, and possibly foreign companies, have the ability to overcome commercial computer intrusion-protection software and hardware.

- If you report evidence of intrusion to the hotel management or local authorities, they may deliberately want to mislead you by passing off the operation as a criminal activity.

Even if there are no obvious signs of intrusion, it does not mean that an event has not occurred in a discreet fashion.

Eavesdropping. Assume that conversations can be monitored in public places and in public transport. Eavesdropping activities can range from the strategic positioning of an unobtrusive bystander, to the use of concealed sophisticated audio and visual devices.

- Use discretion at all times

3103(93/01)

- Beware of eavesdropping at social settings where attendees feel secure and are more likely to talk about themselves and their work.

- Vulnerable venues include public and host-provided transportation, restaurants, bars, meeting facility restrooms, hotel rooms and telephones.

Concealed devices are cost efficient, low risk, and can be used in conjunction with overt devices such as traffic, security, and pedestrian-monitoring cameras.

Information gathering through open sources. Open source research goes beyond simply Googling your name and address. It entails scouring every possible source of publicly available information – such as trade publications, academic journals, websites, public registrars, etc.– that exists on you, your family and work. You'd be surprised how much open source information is accessible to someone who knows how and where to look. Even if you think you have a low profile and haven't left a digital trace behind, some information related to you, your family and friends is freely available. The gathering of such information serves to build a profile of who you are, and where you might be most easily approached either overtly or covertly. A personal, financial and professional profile of you or your business can be constructed by someone willing to invest the effort. *Remember, information about you on the Internet is almost certainly there forever.*

3103(93/01)

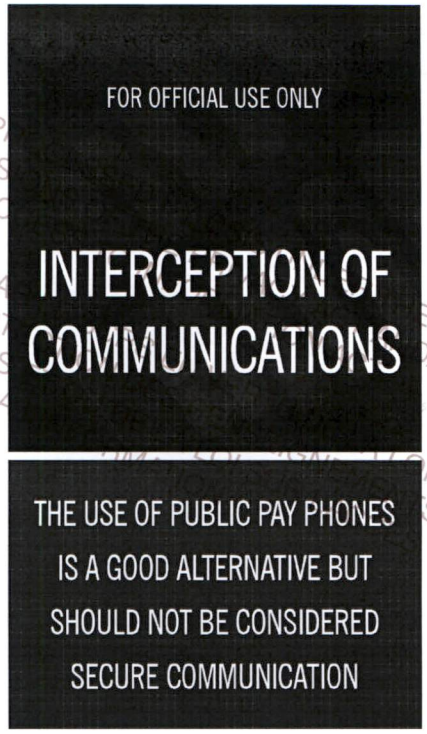
Social networks are great, except that now everybody knows your name and possibly what you look like. You might not have an account on social networks such as Facebook, Twitter, LinkedIn but a member of your family, a friend or a co-worker might, and they may have inadvertently posted information related to you. Remind your family/friends to exercise discretion when posting information about you.

Even garbage is information. All types of information can be gathered by rummaging through your trash. Be cognizant of what you throw out, especially material of a sensitive nature. Do not throw away business or personal notes in the garbage of your hotel room or meeting rooms.

Look a gift horse in the mouth. Be wary of gifts, especially electronic ones that can plug into your computer – USB keys, cameras, digital picture frames, etc. These items could be infected with Trojans and other viruses that could give someone remote access to your computer and network. Never plug in a device of unknown origin without proper virus scanning. (Please check with your own departmental security procedures.)

Private sector involved in this type of activity as well. There are private companies that are in the business of packaging open source information on people and companies for a price. These companies may also use more intrusive methods to gather information.

3103(93/01)



Intercepting your communications. Wireless communications can be monitored in any country. Assume that telecommunications will be monitored in some countries (which is why a country-specific briefing from your DSO is recommended). Local authorities have access to networks that you inherently roam while travelling. You should travel with "disposable" media, ones that don't contain classified material.

Wireless vulnerabilities. The devices you carry for the most part can connect to the Internet or be accessed wirelessly. This makes them vulnerable to cyber-attacks and hacking. Attackers can access your hard drive and everything on it; can activate your microphone or camera without your knowing; can log every key you hit and every number you enter, etc. These vulnerabilities can persist long after you return home – be vigilant and report suspicious activities.

Use good electronic hygiene. Don't let anyone plug an external device into any of your equipment.

3103(93/01)

There should be no reason for authorities to remove your equipment out of sight such as at airports, security checks and hotels. Should this happen, even for a very brief period of time, assume that the equipment has been compromised.

All types of electronic communication are vulnerable. Any type of communications (e.g. voice calls, SMS, BBM, web browsing, chat, Facebook, Twitter, etc.) can theoretically be intercepted. Yet it's worth noting that a landline, although by no means secure, is normally more difficult to intercept than a cell phone. The use of public pay phones is a good alternative but should not be considered secure communication.

Voice intercepts via the Telephone Service Provider (TSP). Authorities can monitor your telephone conversations. Not only can they gain information directly from your conversation, but also from the numbers you dial (telephone tolls). Looking at call patterns not only helps build a personal profile of someone, but a larger organizational one.

Data intercepts via the Internet Service Provider (ISP). Data can also be intercepted via technical means by the Internet Service Provider. Be it a smartphone, a tablet, desktop or laptop, these communications can all be intercepted and eventually "taken over".

Your car as a listening device. People often feel they can carry on work-related conversations in cars they rent while on business without giving any thought to the potential for eavesdropping or tracking through devices

paired to the vehicle or through manipulation of technologies embedded in the vehicles by the manufacturer.

Social engineering and phishing. Another reason to safeguard your information while travelling is that it could be used by an attacker to impersonate you and send targeted emails loaded with malicious software to employees in your department, or further afield, in the hopes of tricking recipients into opening the e-mail and attachments. This would then automatically infect their computers or networks with the malicious software. When attending conferences or training abroad be aware that attackers can use attendance lists to specifically target you with well-crafted emails – think before you click.

Storage. Don't hand in cell phones or smartphones at reception or security desks. Leave them secured at the Embassy, High Commission or Consulate.

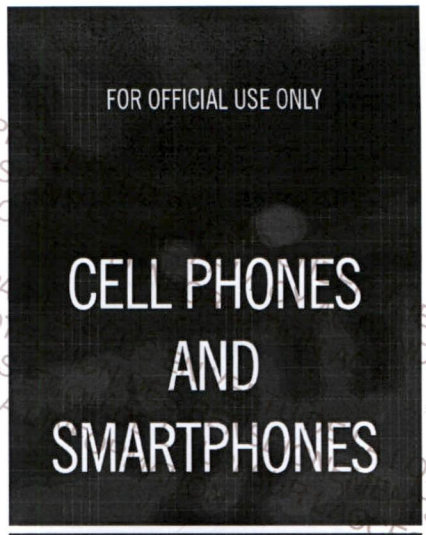
Post travel. If you brought any corporate hardware or software with you while travelling, if possible have it examined upon your return by your Information Management/Information Technology Branch for any signs of intrusion or compromise before using it at your work site.

3103(93/01)

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION

3103(93/01)



SURREPTITIOUS TRACKING OF THE WHEREABOUTS AND MOVEMENTS OF THE USER IS A PARTICULAR CONCERN

Voice Communications Interception. Eavesdropping on wireless communications is always a concern. There is inherently very little protection afforded to the wireless voice call unless expensive third party products are used for encryption. Again, authorities in the host country have access to these cellular networks.

Data Transmission Interception – BlackBerry. Apart from the general concern of the interception of data or voice communications over any wireless network, there is a particular concern that some foreign government infrastructures may be able to isolate, decrypt and store certain BlackBerry communications (i.e. Pin-to-Pin, BlackBerry Messenger and BlackBerry Group messaging) which had been considered protected with proprietary RIM encryption. This concern has been widely reported in the press.

Live Microphones in Secure Areas – Mobile phones. Bringing mobile phones into security zones presents the risk of (unintentional) live microphone transmissions. All mobile phones should be kept outside of secure areas.

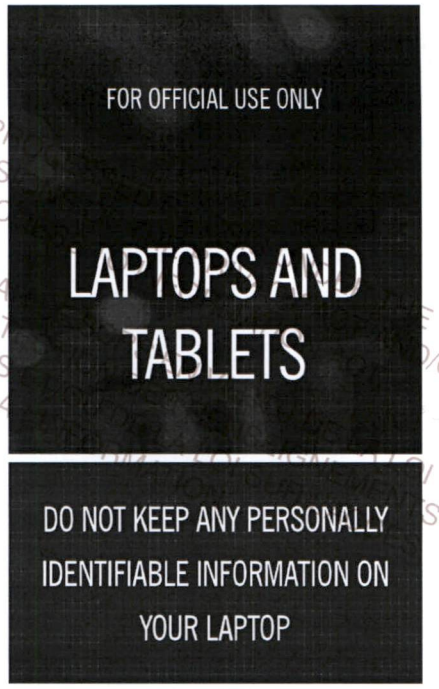
Tracking. Surreptitious tracking of the whereabouts and movements of the user is a particular concern. Smartphones provide a dedicated adversary the means to track the movements of the targeted device and its users by intercepting or acquiring GPS information transmitted or stored on the phone. Your phone has a unique signature that, once brought to the attention of an attacker, can be followed anywhere in the world.

Bluetooth and Wi-Fi Wireless. Other wireless networks available with most smartphones such as Bluetooth and Wi-Fi introduce additional interception and data loss vulnerabilities that can be exploited by an attacker. Public Wi-Fi is by its very name not private!

Lost or Stolen Smartphones and/or laptops. More so than the replacement cost, the greatest concern of a lost or stolen device is unauthorized access to the data it contains. Passwords, encryption, time lock-out and remote wipe can be used to counter this risk.

Never leave a cell phone, smartphone, or laptop unattended; compromise takes mere seconds.

3103(93/01)



Personal information. Do not keep any personally identifiable information on your laptop. A product such as "Identity Finder" can find files on your hard drive that may contain personally identifiable information. Consider leaving personal devices at home as they are as vulnerable as corporate devices and not as easily replaced.

Sensitive files. Remove them from the hard drive and put them on a disk if necessary. To ensure that the files are actually deleted from the laptop's hard drive, use a proven media sanitizing software tool. Keep the disk or USB flash drive on your person. Encrypt the files on the removable media and keep the password separate from the media.

Battery. Make sure the laptop battery is charged before you go to the airport; expect to prove that the laptop is functioning correctly. Ensure an innocuous start-up screen is in place.

Airport security. Do not send your laptop through the airport X-ray conveyor belt until it's your turn to walk through the metal detector. That way, you'll be able to pick it up promptly when it comes out the other end and prevent

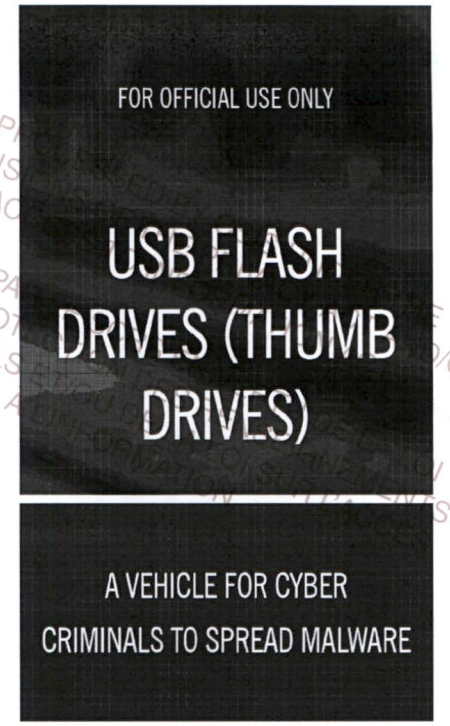
3103(93/01)

anyone from walking away with it. Never check laptop computers into a baggage claim. It is a high target item. Keep your laptop in sight at all times.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

3103(93/01)



These devices can be very small and therefore more easily lost, stolen or hidden.

Popularity. The popularity of thumb drives makes them a vehicle for cyber criminals to spread malware. They have even been targeted at the production phase, while they are being created, so a brand new product could potentially be already infected. You may wish to exercise caution when considering their use.

Running software code. A computer can run software code from a USB the moment it is plugged in. Software has been released that can make a USB thumb drive auto-execute when inserted into a Windows system, tricking Windows into treating it as a CD, and then dropping malicious software into it. Issues with data loss, bandwidth consumption, network performance, software licensing and productivity are likely signs that devices have been manipulated.

Social engineering using USB. Social engineering is made easy when a perpetrator, for example, drops several flash drives somewhere close

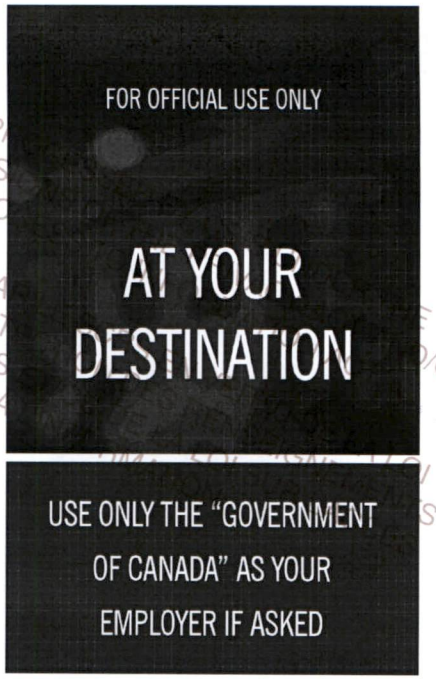
3103(93/01)

to the intended target (e.g. a hotel), and waits for an unsuspecting victim to insert it into their system, giving the perpetrator access for further manipulation.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

3103(93/01)



HOTELS

Hotel staff. Only provide the information necessary to conduct your transactions. Use only the "Government of Canada" as your employer if asked; there is no need to volunteer information. Have copies of your passport ready instead of relinquishing your passport. Always try to keep positive control of your passport.

Hotel phones and computers. Beware of the use of hotel phones and computers as authorities have access to these networks.

Answer with hello. You should answer the room telephone with a simple "hello." Again, do not volunteer information; this call could be used by someone to confirm that you are indeed in a given room.

Hotel safes and securing classified documents. Do not use the hotel safe for classified or sensitive material. Do not leave classified documents or equipment unattended in hotel rooms. Classified or sensitive material is best kept in secure storage at the Embassy, High Commission or Consulate.

3103(93/01)

Use encryption and Virtual Private Networks (VPN) if you must work using non-secure networks. When on official travel, never use an open (hotel, coffee shop, etc.) network to conduct work as these are easily intercepted (see below). It is preferable that you discuss various VPN and/or encryption methods with your Departmental Security Officer.

Never use an open or hotel network for work. Avoid using a "free" and/or unknown Wi-Fi connection as you may be accessing a network that is controlled by an intelligence agency or, more likely, a criminal. Wi-Fi is available in many locations such as airports, coffee shops and train stations. These systems are very vulnerable to abuse by hackers, competitors or foreign intelligence services. As such, it is best to avoid such systems for discussions or exchanges of sensitive or proprietary information. Ensure encryption software or features of your wireless local area network (WLAN) are installed to avoid compromise. Factory installed encryption should be changed.

Don't advertize where you're staying. If someone has your room number it makes it easier for them to target you whether they're an intelligence officer or a criminal. This is especially important for women. Please consult the GAC website for more specific information related to maintaining your personal safety. Always meet guests in the lobby and never in your room for security reasons.

Pretend that someone's always in your room. Leaving on a TV or radio, along with the lights, can give the impression that someone is in the room.

3103(93/01)

Criminals are opportunists, and will not likely "take a chance" on your room. Closing the curtains keeps prying eyes out. Leave the "Do Not Disturb" sign on your door. Never open your door to anyone without first verifying the identity of the person with the front lobby at all times. Always confirm unannounced/uninvited guests with the front desk.

What alternate exit routes are there? Always look for alternative exits in case of an emergency. In some emergencies, getting out quickly is essential—you may not have time to dither. Ensure that your room is **not** accessible at street level (below the 3rd floor) and **is** accessible to first responders (below the 7th floor where fire ladders can reach). Always have an emergency bag ready containing items such as: flashlight, passport, money, credit cards, medications, glasses, water and power bars etc.)

Don't relinquish control over your key(s). This is a simple safety/security precaution.

GENERAL

Travel with disposable devices if possible. As mentioned earlier, consider travelling with clean or "disposable" devices. Even if they aren't hacked into or otherwise tampered with, they could be stolen. Laptops, cell phones, smart phones, PDA's and USB sticks – these are all mobile devices that are essential for your communications with your colleagues but they also involve risk.

3103(93/01)

- They should not be used by anyone other than the employee.
- They should not be used to connect to unprotected devices (wireless).
- They should not have unauthorized software installed on them.

Physical access to these devices allows for the extraction of data and/or the compromise of systems in support of information gathering efforts.

Consult with your IT Branch. Make sure that whatever media device you take has the latest Anti-Virus, encryption, firewall and program patches installed. Remember, your computer and/or PDA can be used as a gateway into your corporate network and from there to your "crown jewels".

We are all Westerners. In some countries the terrorist threat of kidnapping is significant, as many groups are dependent on this type of criminal activity in order to fund their operations. Consequently, you may want to look for signs of hostile reconnaissance, as well as to vary your routines and the routes you take to and from your hotel and place of work. Terrorists use the same methods as intelligence officers do in order to obtain information. They will elicit information, as well as gather it through other types of collection means. Situational awareness is your best defence.

Avoid routine patterns. Terrorists and criminals often select targets with regular and predictable schedules. You need to train yourself to vary your route while travelling abroad even on short business trips. Each day,

3103(93/01)

simply leave at a different time and vary the route you take. Routine and complacency are the two most common causes of safety and security issues.

Don't talk shop in unsecure locations. Assume your hotel room is bugged and that the list of telephone calls made from your hotel will be collected by the host country. Also, don't "talk shop" in taxis, public transportation or in public. Moreover the taxi may be outfitted with a camera and other audio-visual equipment. This equipment may be found in all taxis for driver safety reasons, but this kind of technology can have dual-uses.

Taxis. Try to arrange transportation in advance. Have someone trusted pick you up. If this is not possible, use hotel courtesy shuttles when available or research the name of reputable taxi companies. Always negotiate the taxi fare prior to departing, never share a taxi with a stranger, do not travel in taxis that are unmarked or do not have an official license prominently displayed. Always sit in the rear diagonally opposite the taxi driver. This allows you to see the hands of the taxi driver and is the most direct and safe route out of the taxi in an emergency (on the sidewalk instead of into traffic.)

Your personal data is stored on many devices. Electronics primarily refer to your phone, PDA, laptop, even MP3 if it has personal data such as pictures on it. These can prove to be treasure troves for intelligence

3103(93/01)

agencies, as well as profit generators for criminals. Avoid being distracted by your devices. Continue to pay attention to your environment while using them.

Avoid high crime areas. High crime areas are not areas one should normally visit. Should you need to enter those areas, appropriate measures should be taken – such as timed physical or telephone check-ins – to ensure your safety. Note that the "locals" will immediately detect that you are from outside the area. In case of a robbery, have a "throw away wallet or purse" ready to give away. A bag or wallet with fake credit cards and local or American money are enough to satisfy a thief and allow you to walk away from potential harm.

Criminals also seek to profit from available information. Criminals are opportunistic. They wait for you to make a mistake so they can exploit it. Their task is made easier if you volunteer information about yourself, your comings and goings, or your possessions to people you do not know. For instance, don't talk about how to use a hotel safe to store your laptop and other valuables in a taxi and then pay for it with a credit card or make mention of your name. This type of information can prove very useful to criminals, and they too are known to pay for information.

Don't be ostentatious. Be discreet about who you are, what you do and what type of valuables you're carrying.

3103(93/01)

Don't travel alone if you can. Travelling in a group is usually always safer. Criminals, like other types of predators, are less likely to target a group than a lone individual. However, the group should also seek to be discreet to avoid attracting unwanted attention.

Medication and Medical facilities. Always travel with enough prescribed medication (in their original containers) to last you for the time you are away and with a reserve supply in case your return is delayed. Make sure that you verify the legality of this medication in the country you are travelling (see the GAC travel advisory for medical information). Additionally, you should be aware of what type of medical facilities, local emergency care, means of payment, standard of care and capabilities that are available in the country (countries) where you are travelling.

Money. Always arrive with enough local currency or enough money that will work in the country within which you are travelling to get you through the first 24 hours.

Threat Response. Stay calm when confronted, assess your options, and disengage or remove yourself from the situation if possible. Always look at the hands of the aggressor and their body movements. Attract attention to yourself by yelling, screaming, or making any kind of noise. Try to create distance between you and your aggressor using furniture or vehicles. When travelling, having a whistle handy can help you attract attention in almost any environment.

3103(93/01)

TRAVEL SMART

Remember – Have a plan and a contingency plan.

Get travel insurance
Register at Travel.gc.ca
In case of emergency abroad – call collect 1-613-996-8885
sos@international.gc.ca

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

3103(93/01)

NOTES

3103(93/01)

Canadian Security Intelligence Service

Service canadien du renseignement de sécurité

Director - Directeur

CCM # 12245
UNCLASSIFIED
For Information

JUN 0 6 2012

MEMORANDUM TO THE MINISTER

THE CSIS TRAVEL SECURITY GUIDE FOR CANADIAN OFFICIALS

I am writing to share with you the first product of its kind from CSIS for Canadian officials traveling abroad. Over the years, CSIS has provided numerous security travel briefings to Ministers of the Crown and officials. This guide, developed after your office and I met with senior officials at the Prime Minister's Office, provides much of that common-sense advice in a readily available format for those traveling and engaging with foreign officials.

For Canada to remain competitive and prosperous, we must pursue our interests with our eyes open to both the risks and opportunities. Canada remains an attractive target of hostile interests precisely because of our successes in advanced technologies and privileged access to important world players like the US and the G-8. National security is not solely the responsibility of CSIS and our traditional partners; rather we all have a role to play and there are relatively simple steps we can all take to protect Canada's interests. In addition to raising the level of security awareness, the aim of this guide is to highlight the risks and how one can protect oneself and Canada against these threats.

I intend to distribute copies to my deputy head colleagues and to provide copies to your Chief of Staff to share with counterparts. You may also wish to consider dissemination to your colleagues. If so, please let me know and I will have copies forwarded to your office as appropriate.

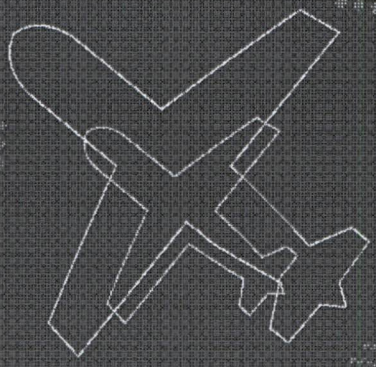
Richard B. Fadden

P.O. Box 9732, Station "T", Ottawa, Ontario K1G 4G4 C.P. 9732, Succursale "T", Ottawa (Ontario) K1G 4G4

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Far from home:
A travel security guide for government officials

For Official Use Only



Canada

3103(93/01)

A word from CSIS

It is often assumed that the protection of our national security is necessarily a complicated business, requiring specialized training, fancy technology and access to secret information.

That might be true for some of us, but all officials have a role in keeping Canada safe. We need the help of Canadians outside the professional security community, who by acquiring a basic level of security literacy serve as the country's first line of defence. The good news is that security awareness is not complicated at all, as you'll see when you read this handbook.

Don't accept gifts of USB sticks or other electronic devices; be careful what you throw in the trash; know that cell phone conversations and Internet activity can be monitored - and so on. We have addressed this guide to officials of the Canadian government who travel overseas, but it could be equally helpful to businesspeople or indeed any Canadian going abroad, particularly to countries that are aggressive collectors of intelligence.

Much of what we say falls into the category of common sense, but that doesn't mean the advice is self-evident. Even experienced travellers who occupy positions of political or public service leadership have not always understood why or how they should take precautions. I suspect this stems in part from a belief that Canada, as a peaceable and open country, is not a particularly exciting target for foreign spies. That is a wrong assumption.

Espionage is at a level on par with that experienced during the Cold War. Canada is a leader in technology, energy and other economic sectors. We also have prized political connections owing to our close relationship with the United States and to our membership in important international bodies. We are a valued target in the eyes of intelligence agencies.

In the age of globalization, Canada's prosperity more than ever depends on maintaining an international profile, and that means Canadians have to venture into the world. The key is to do so safely and with eyes wide open. I want to be clear that not every country represents the kind of risk this booklet is aimed at - but better be safe than sorry.

Have a secure and successful trip.

Richard B. Fadden
Director, Canadian Security Intelligence Service

P.S. While the advice is directed at those travelling outside Canada, much of the advice is worth remembering for domestic travel as well.

Table Of Contents

THE THREAT ENVIRONMENT

In a world that increasingly measures national power and security in economic as well as military terms, Canadian citizens travelling abroad may be the target of foreign intelligence collection activities. Many foreign governments and foreign businesses place a high priority on acquiring Government-protected information (classified, sensitive and proprietary). Although the Cold War has ended, the risk of becoming an intelligence target has increased. The threat you face as an official Canadian government traveler is real. This brochure describes the nature of the foreign intelligence threat, provides basic steps you can take to mitigate the risk associated, and actions you should take to report suspicious incidents.

The security assumptions we make about overseas travel being easy and safe are often wrong. For many of us, overseas travel has become so routine that we wrongly assume it to be low-risk. You need to take special precautions when traveling in an official capacity, especially to countries of concern. You should receive a country-specific briefing from your Department Security Officer (DSO) before any trip you take as an official.

Your vigilance should be heightened whilst overseas. When you travel abroad, you are vulnerable due to the limited control you exercise over the environment. Foreign governments and their agents act with greater impunity on their own soil, to say nothing of local extremists and criminals.

Inform yourself about local laws and customs before leaving. It is incumbent upon you to familiarize yourself with the laws and customs of the country or countries you are about to visit. You may be subject to the laws and regulations of the country in which you are located, and your Canadian citizenship will offer you little immunity, unless travelling under a diplomatic passport. Note, however, that even the latter does not prevent you from being targeted during your stay in the host country. Before departing you should consult the **DFAIT website for country-specific information**, as well as keep copies of the contact information for the nearest **Canadian Embassy or Consulate**.

Canada and Canadians are targets for many hostile actors. Canada and Canadians have been, and will continue to be, targeted by foreign intelligence agencies seeking state and industrial secrets; by extremists who see you, as a representative of a Western government, as an enemy; and by criminals who are simply looking for a quick score. In short, you are not safe simply because you are Canadian. You are a legitimate target.

You don't get to determine whether you're worthy of targeting. You are mistaken to believe that the contents of your briefcase or the data in your laptop and/or Smartphone are not important enough to draw the attention of a foreign intelligence agency, or that because Canadians are "honest brokers" on the world stage, extremists won't target you, or that because you are staying in good accommodations and environs you are less likely to be the victim of a crime. **These determinations are up to the threat actors, not you**.

Do not overlook the threat posed by thieves. At the very least, briefcases, laptops, smartphones and the like are attractive to common criminals, as they are to foreign intelligence agencies. The result is the same: a security breach - one that could potentially harm you, the Canadian government and/or your country.

VISAS AND PREPARING FOR THE TRIP

The gathering of information begins before you even book your flights and hotels. In some countries, information gathering on you begins well before you arrive. The information you provide on your visa application form could be used to assess your "worthiness" as a target. Your answers contained in the questionnaire could draw a very good initial profile of who you are as a person as well as a Government of Canada employee. **If you are part of a high-level delegation, assume you will receive consideration as a potential target**.

Visa applications have become more comprehensive with more questions than ever before. When filling out such **applications, be truthful but do not volunteer more** information than needed. All visa requirements should be explored prior to booking travel given the intrusive nature of the questions. For example, some countries will request passport numbers of family members, even if they are not travelling with you. Moreover, questions on the nature of your employment can be geared to acquiring very specific details.

Be prepared to answer questions at the point of entry. Before departure, ensure that you will be comfortable answering questions from the host country's customs officials about the reasons for your travel. This is especially important if you are travelling in a group, as any divergence between rationales could be used as a pretext for some kind of action on the part of local authorities.

What should you leave the country with? Alternative means for transferring information you will need while on travel status, especially that of a more sensitive nature, should be considered before you leave Canada.

Consult your Departmental Security Officer (DSO) before leaving. In consultation with your DSO, you may want to use a "disposable" telecommunications device while on travel. By disposable, we don't mean that the device is thrown away but rather that it contains no information when you leave and that, upon your return, it is completely wiped clean and the operating system re-installed. You do not want to take abroad a device packed with e-mails, contacts and documents.

Inform yourself before leaving. Before you go anywhere, inform yourself about the general security and political situation in the country. It is recommended that you check the DFAIT website and your own department's security branch for further information. Ensure that you have the current contact information for the Canadian Embassy or Consulate in the country or countries of destination.

Contact lists. Leave behind any address books or lists of names and contact numbers not necessary for the trip.

Travel light. Don't saddle yourself with excess baggage because it will attract attention, curtail your mobility and mean you have more to protect.

AT THE AIRPORT

What to do at any airport. Apart from following normal security procedures at airports, be vigilant and in a position to observe or watch for any type of suspicious activity – from fellow passengers, flight crews, etc.

Airline or border control agents. Assume that any detail given to airline or border control agents will be collected by the host country. It may also be shared with other countries.

Don't advertise your identity. Always conceal your bag tags. In fact, you may want to put the identifying bag tags in your checked bags and use some other type of identifier, such as a ribbon, on the handle.

Luggage. Do not leave belongings unattended. Assume your checked luggage will be searched in transit. Do not agree to carry items for other parties unless you are certain of their nature or contents.

POINTS OF ENTRY AND BIOMETRICS

Covert and overt means of targeting. Should you be identified as a potential target through the visa application process, the host intelligence agency may undertake covert or overt actions against you to further their information collection efforts.

Surveillance. Assume that in many countries, you will be subject to physical surveillance. A country-specific briefing before departure will assist in broadening awareness on this issue.

A secondary search could be used as a pretext to seize or copy your files. One of these overt methods can occur right at the Point of Entry – usually an airport – where you can be selected for a secondary inspection by the local Customs Service. During this inspection, your belongings are all subject to be viewed, copied and/or seized, including whatever documents you may be carrying on your person, in your laptop and your smartphone.

A secondary search could indicate hostile interest. It could also simply mean that you triggered one of the many tripwires used to select passengers for secondary inspections. In either case, one should always be ready to handle a secondary inspection (prepared responses as to purpose of visit; being able to account for one's belongings and so on). You should let your superior or delegation head know you have been selected for a secondary inspection.

Be prepared to invoke your right to a consular visit. Should the questioning during a secondary search become inappropriate or lead to your detention, call the Canadian Embassy or Consulate, as you are entitled to Consular Access. When communicating with the Embassy or Consulate, keep your description of events to a minimum as somebody may be listening.

Biometrics are increasingly being used. Biometric measures are increasingly being used at points of entry, the purpose of which is to catch criminals and terrorists who can and often do travel using a multitude of identities and documents. At the same time, extensive information is being collected – information that could be used by a hostile intelligence service. This is especially true for individuals who travel to a given country, at different times, for both business and personal reasons; they already know who you are and what you do.

Some biometric techniques include face recognition (including 3D), iris scan and fingerprinting. In some countries, biometrics are taken covertly via closed circuit television and cameras (CCTV).

ELICITATION, CULTIVATION AND OTHER TRAPS

Why would someone be interested in you? As someone working for the Government of Canada, your access to classified or privileged government and possibly private sector information makes you an attractive target for foreign intelligence services. As such, you may be the source of

information or access that a foreign intelligence service needs to fulfill collection requirements which are designed to advance the foreign policy, security, and commercial/ economic interests of the collector.

Contacts. Assume that any meetings you have abroad with personal contacts will come to the attention of the foreign government, even if they occur before or after the period of official meetings. Also, assume that non-governmental contacts abroad will be interviewed before your arrival or after your visit, on the nature of your travel and in relation to profile building about you or your staff.

Criminals may be interested in your info, especially if it relates to law enforcement. If your work is law enforcement-related, the information you hold or have potential access to could be of great interest to criminal organizations interested in knowing if there are any investigations targeting them and if there are any "leaks" within their organizations.

Secrets can appear mundane. Those foreign intelligence agencies targeting Canada and Canadians are not solely after the "crown jewels" – say, a blueprint to a new fighter jet or communications infrastructure between the allies – but information that, to the Canadian person or institution holding this information or knowledge, appears unremarkable. Items such as an organizational chart may not appear to be of value but could be considered a key requirement for a hostile intelligence service.

They may be interested in gaining indirect access to an ally. Foreign intelligence agencies may also be interested in the information and access they could obtain via Canada's membership in organizations as diverse as the North Atlantic Treaty Organization (NATO), the G8, G20, Commonwealth, Francophonie, Organization of American States (OAS), Asia-Pacific Economic Cooperation (APEC), the Organization for Economic Cooperation and Development (OECD), the United Nations (UN) and the World Trade Organization (WTO).

Gaining access to advanced US technologies. Canada occupies a unique strategic position as a trusted ally of the United States, which gives privileged access to advanced U.S. technologies few others can legitimately procure.

Canada: a source of technological advances and intellectual property. Canada also participates in a system of military and strategic partnerships, and harbours a wealth of natural resources and human talent which continue to generate technological advances. These technologies are coveted by countries interested in developing their own technological and commercial opportunities while avoiding the associated research and development costs. The loss of such information diminishes Canada's competitive advantage and amounts to a transfer of wealth from Canada to another country.

How does the gathering of information happen?

Below are some of the most common methods foreign intelligence agencies employ to collect information.

Elicitation. This is a technique used by foreign agency officers and their agents whereby they engage you in what appears to be harmless or random conversation but the aim is subtly to extract information about yourself, your work and colleagues. Warning signs are when your interlocutor:

- Appeals to your ego by flattering you;
- Emphasizes mutual interests and suggests "getting together" at a future date to pursue the mutual interest;
- Uses false statements to get you to correct them with the information you have access to;
- Volunteers information – the "give to get" principle at work. They'll share some form of sensitive information with you in the hopes you will return the favour;
- Leads you to believe he/she is very knowledgeable about your area of expertise. If they are an intelligence officer, that knowledge is likely limited and cursory, but just enough to bluff their way through a conversation.

Cultivation. Well-orchestrated approaches by hostile intelligence services begin with a period of "cultivation". A relationship is established between the representative of an intelligence service (whose true identity is unknown) and the unsuspecting person being recruited. You should be vigilant and monitor the progress of associations, particularly new relationships and those with foreign nationals. Always be heedful of discussions regarding your work, even if seemingly benign.

Unwittingly volunteering information. Never talk shop or volunteer information in front of taxi drivers, waiters and bartenders, who could be intelligence officers or informants. Every little bit of information can be useful to a competitor.

The "Vacuum Cleaner" approach or the "Mosaic Effect". Some intelligence agencies use the "vacuum cleaner" approach – they will obtain one piece of information from you and build on that with other pieces of information acquired from your colleagues or that you unwittingly offered to other sources who are working together. You may not think that you have offered any desired information, though when pieced together the result can be quite valuable (thus creating the "mosaic effect").

The Honey Trap. Sexual entrapment, colloquially known as the "honey trap", refers to the use of an attractive individual – informed by your sexual identity and preferences – to seduce you and get you in a compromising position or one where you could be blackmailed. Honey traps often involve the clandestine recording of an intimate encounter. These recordings are either used to blackmail or publicly embarrass the victim. Foreign governments are known to employ this tactic, and employees should be aware of the potential hazards of accepting offers of companionship while travelling. There are also reports of individuals who have suspected they were drugged and who awoke to find that their hotel room had been searched, smartphone stolen and secret business documents missing.

Covert methods including intrusions. Hostile actors may decide to conduct an intrusion operation against you.

This would entail breaking into your hotel room in order to steal or copy sensitive documents in either hard or digital form. **Though you may not notice that someone has** surreptitiously entered your room, some travellers have returned to their rooms to find individuals searching their belongings or conducting unnecessary maintenance activities. Others have reported laptop computers showing signs of unauthorized usage or actual damage, packages having been opened and resealed or left open, locks on briefcases and suitcases are missing or showing signs of forced entry.

- Intrusions may be conducted by the host government, a foreign intelligence service of another country or foreign business operatives.
- Intrusions are frequently accomplished with the cooperation of the hotel staff.
- Several countries, and possibly foreign companies, have the ability to overcome commercial computer intrusion-protection software and hardware.
- If you report evidence of intrusion to the hotel management or local authorities, they may deliberately want to mislead you by passing off the operation as a criminal activity.

Even if there are no obvious signs of intrusion, it does not mean that an event has not occurred in a discreet fashion.

Eavesdropping. Assume that conversations can be monitored in public places and in public transport. Eavesdropping activities can range from the strategic positioning of an unobtrusive bystander, to the use of concealed sophisticated audio and visual devices.

- Beware of eavesdropping at social settings where attendees feel secure and are more likely to talk about themselves and their work.
- Vulnerable venues include public and host-provided transportation, restaurants, and bars, meeting facility restrooms, hotel rooms and telephones.
- Concealed devices are cost efficient, low risk, and can be used in conjunction with overt devices such as traffic and pedestrian-monitoring cameras.
- Use discretion at all times.

Information gathering through open sources. Open source research goes beyond simply Googling your name and address. It entails scouring every possible source of publicly available information – such as trade publications, academic journals, websites, public registrars, etc.– that exists on you, your family and work. You'd be surprised how much open source information is accessible to someone who knows how and where to look. Even if you think you have a low profile and haven't left a digital trace behind, some information related to you, your family and friends is freely available. The gathering of such information serves

to build a profile of who you are, and where you might be most easily approached either overtly or covertly. A personal, financial and professional profile of you or your business can be constructed by someone willing to invest the effort.

Social networks are great, except that now everybody knows your name... You might not have an account on social networks such as Facebook, Twitter, LinkedIn but a member of your family, a friend or a co-worker might, and they may have inadvertently posted information related to you.

Even garbage is information. All types of information can be gathered by rummaging through your trash. Be cognizant of what you throw out, especially material of a sensitive nature. Do not throw away business or personal notes in the garbage of your hotel room or meeting rooms

Look a gift horse in the mouth. Be wary of gifts, especially electronic ones that can plug into your computer – USB keys, cameras, digital picture frames, etc. These items could be infected with Trojans and other viruses that could give someone remote access to your computer and network. Never plug in a device of unknown origin without proper virus scanning.

Private sector involved in this type of activity as well. There are private companies that are in the business of packaging open source information on people and companies for a price. These companies may also use more intrusive methods to gather information.

INTERCEPTION OF COMMUNICATIONS

Intercepting your communications. Wireless communications can be monitored in any country. Assume that telecommunications will be monitored in some countries (which is why a country-specific briefing from your DSO is recommended). Local authorities have access to networks that you inherently roam while travelling. You should travel with "disposable" media, ones that don't contain classified material.

Wireless vulnerabilities. The devices you carry for the most part can connect to the Internet or be accessed wirelessly. This makes them vulnerable to cyber attacks and hacking. Attackers can access your hard drive and everything on it; can activate your microphone or camera without your knowing; can log every key you hit and every number you enter, etc.

Use good electronic hygiene: Don't let anyone plug an external device into any of your equipment.

There should be no reason for authorities to remove your equipment out of sight such as at airports, security checks and hotels. Should this happen, even for a very brief period of time, assume that the equipment has been compromised.

All types of electronic communication are vulnerable. Any type of communications can theoretically be intercepted. Yet it's worth noting that a landline, although by no means secure, is normally more difficult to intercept than a cell phone. The use of public pay phones is a good alternative.

Voice intercepts via the Telephone Service Provider (TSP). Authorities can monitor your telephone conversations. Not only can they gain information directly from your conversation, but also from the numbers you dial (telephone tolls). Looking at call patterns not only helps build a personal profile of someone, but a larger organizational one.

Data intercepts via the Internet Service Provider (ISP). Data can also be intercepted via technical means by the Internet Service Provider. Be it a smartphone, a tablet, desktop or laptop, these communications can all be intercepted and eventually "taken over".

Your car as a listening device. People often feel they can carry on work-related conversations in cars they rent while on business without giving any thought to the potential for eavesdropping or tracking through devices paired to the vehicle or through manipulation of technologies embedded in the vehicles by the manufacturer.

Social engineering and phishing. Another reason to safeguard your information while travelling is that it could be used by an attacker to impersonate you and send targeted emails loaded with malicious software to employees in your department, or further afield, in the hopes of tricking recipients into opening the e-mail and attachments. This would then automatically infect their computers or networks with the malicious software.

Storage. Don't hand in cell phones or smartphones at reception or security desks. Leave them secured at the Embassy.

Post travel. If you brought any corporate hardware or software with you while travelling, if possible have it examined upon your return by your Information Management / Information Technology Branch for any signs of intrusion or compromise before using it at your work site.

CELL PHONES AND SMARTPHONES

Voice Communications Interception

Eavesdropping on wireless communications is always a concern. There is inherently very little protection afforded to the wireless voice call unless expensive third party products are used for encryption. Again, authorities in the host country have access to these cellular networks.

Data Transmission Interception - BlackBerry

Apart from the general concern of the interception of data or voice communications over any wireless network, there is a particular concern that some foreign government infrastructures may be able to isolate, decrypt and store certain BlackBerry communications (i.e. Pin-to-Pin, BlackBerry Messenger and BlackBerry Group messaging) which had been considered protected with proprietary RIM encryption. This concern has been widely reported in the press.

Live Microphones in Secure Areas - Mobile phones

Bringing mobile phones into security zones presents the risk of (unintentional) live microphone transmissions.

Tracking

Surreptitious tracking of the whereabouts and movements of the user is a particular concern. Smartphones provide a dedicated adversary the means to track the movements of the targeted device and its users by intercepting or acquiring GPS information transmitted or stored on the phone.

Bluetooth and Wi-Fi Wireless

Other wireless networks available with most smartphones such as Bluetooth and Wi-Fi introduce additional interception and data loss vulnerabilities that can be exploited by an attacker.

Lost or Stolen Smartphones and/or laptops

More so than the replacement cost, the greatest concern of a lost or stolen device is unauthorized access to the data it contains. Passwords, encryption, time lock-out and remote wipe can be used to counter this risk.

Never leave a cell phone, smartphone, or laptop unattended; compromise takes mere seconds.

3103(93/01)

LAPTOPS

Personal information. Do not keep any personally identifiable information on your laptop. A product such as "Identity Finder" can find files on your hard drive that may contain personally identifiable information.

Sensitive files. Remove them from the hard drive and put them on a disk if necessary. To ensure that the files are actually deleted from the laptop's hard drive, use a proven media sanitizing software tool. Keep the disk or USB flash drive on your person.

Battery. Make sure the laptop battery is charged before you go to the airport; expect to prove that the laptop is functioning correctly. Ensure an innocuous start-up screen is in place.

Airport security. Do not send your laptop through the airport X-ray conveyor belt until it's your turn to walk through the metal detector. That way, you'll be able to pick it up promptly when it comes out the other end and prevent anyone from walking away with it. Never check laptop computers into a baggage claim. It is a high target item. Keep your laptop in sight at all times.

USB FLASH DRIVES (thumb drives)

These devices can be very small and therefore more easily lost, stolen or hidden.

Popularity. The popularity of thumb drives makes them a vehicle for cyber criminals to spread malware. They have even been targeted at the production phase, while they are being created, so a brand new product could potentially be already infected. You may wish to exercise caution when considering their use.

Running software code. A computer can run software code from a USB the moment it is plugged in. Software has been released that can make a USB thumb drive auto-execute when inserted into a Windows system, tricking Windows into treating it as a CD, and then dropping malicious software into it. Issues with data loss, bandwidth consumption, network performance, software licensing and productivity are likely signs that devices have been manipulated.

Social engineering using USB. Social engineering is made easy when a perpetrator, for example, drops several flash drives somewhere close to the intended target (e.g. a hotel), and waits for an unsuspecting victim to insert it into their system, giving the perpetrator access for further manipulation.

AT YOUR DESTINATION

HOTELS

Hotel staff. Only provide the information necessary to conduct your transactions. Use only the "Government of Canada" as your employer.

Hotel phones and computers. Beware of the use of hotel phones and computers as authorities have access to these networks.

Answer with hello. You should answer the room telephone with a simple "hello." Again, do not volunteer information; this call could be used by someone to confirm that you are indeed in a given room.

Hotel safes and securing classified documents. Do not use the hotel safe for classified or sensitive material. Do not leave classified documents or equipment unattended in hotel rooms. Classified or sensitive material is best kept on your person or in secure storage at the Embassy.

Use encryption and Virtual Private Networks if you must work using non-secure networks. When on official travel, never use an open (hotel, coffee shop, etc.) network to conduct work as these are easily intercepted (see below). It is preferable that you discuss various VPN and/or encryption methods with your Department Security Officer.

Never use an open or hotel network for work. Avoid using a "free" and/or unknown WiFi connection as you may be accessing a network that is controlled by an intelligence agency or, more likely, a criminal. WiFi is available in many locations such as airports, coffee shops and train stations. These systems are very vulnerable to abuse by hackers, competitors or foreign intelligence services. As such, it is best to avoid such systems for discussions or exchanges of sensitive or proprietary information. Ensure encryption software or features of your wireless local area network (WLAN) are installed to avoid compromise. Factory installed encryption should be changed.

Don't advertize where you're staying. If someone has your room number it makes it easier for them to target you whether they're an intelligence officer or a criminal. This is especially important for women. Please consult the DFAIT website for more specific information related to maintaining your personal safety.

Pretend that someone's always in your room. Leaving on a TV or radio, along with the lights, can usefully give the impression that someone is in the room. Criminals are opportunists, and will not likely "take a chance" on your room. Closing the curtains keeps prying eyes out. Leave the "Do Not Disturb" sign on your door.

What alternate exit routes are there? Always look for alternative exits in case of an emergency. In some emergencies, getting out quickly is essential - you may not have time to dither.

Don't relinquish control over your key(s). This is a simple safety precaution. If you leave the card at the front desk, you lose control over access to your room.

General

Travel with disposable devices if possible. As mentioned earlier, consider traveling with clean or "disposable" devices. Even if they aren't hacked into or otherwise tampered with, they could be stolen. Laptops, cell phones, smart phones, PDAs and USB sticks – these are all mobile devices that are essential for your communications with your colleagues but they also involve risk. a) They should not be used by anyone other than the employee b) they should not be used to connect to unprotected devices (wireless) and c) they should not have unauthorized software installed on them. Physical access to these devices allows for the extraction of data and / or the compromise of systems in support of information gathering efforts.

Consult with your IT Branch. Make sure that whatever media device you take has the latest Anti-Virus, encryption, firewall and program patches installed. Remember, your computer and/or PDA can be used as a gateway into your corporate network and from there to your "crown jewels".

We are all Westerners. In some countries the terrorist threat of kidnapping is significant, as many groups are

dependent on this type of criminal activity in order to fund their operations. Consequently, you may want to look for signs of hostile reconnaissance, as well as to vary your routines and the routes you take to and from your hotel and place of work. Terrorists use the same methods as intelligence officers do in order to obtain information. They will elicit information, as well as gather it through other types of collection means. Security awareness is your best defence.

Avoid routine patterns. Terrorists and criminals often select targets with regular and predictable schedules. You need to train yourself to vary your route while traveling abroad even on short business trips. Each day, simply leave at a different time and vary the route you take.

Don't talk shop in unsecure locations. Assume your hotel room is bugged and that the list of telephone calls made from your hotel will be collected by the host country. Also, don't "talk shop" in a taxi – the driver may be an intelligence officer or an informant. Moreover the taxi may be outfitted with a camera and other audio-visual equipment. This equipment may be found in all taxis for driver safety reasons, but this kind of technology can have dual uses.

Your personal data is stored on many devices. Electronics primarily refer to your phone, PDA, laptop, even MP3 if it has personal data such as pictures on it. These can prove to be treasure troves for intelligence agencies, as well as profit generators for criminals.

Avoid high crime areas. High crime areas are not areas one should normally visit. Should you need to enter those areas, appropriate measures should be taken – such as timed physical or telephone check-ins – to ensure your safety. Note that the "locals" will immediately detect that you are from outside the area.

Criminals also seek to profit from available information. Criminals are opportunistic. They wait for you to make a mistake so they can exploit it. Their task is made easier if you volunteer information about yourself, your comings and goings, or your possessions to people you do not know. For instance, don't talk about how to use a hotel safe to store your laptop and other valuables in a taxi and then pay for it with a credit card or make mention of your name. This type of information can prove very useful to criminals, and they too are known to pay for information.

Don't be ostentatious. Be discreet about who you are, what you do and what type of valuables you're carrying.

Don't travel alone if you can. Traveling in a group is usually always safer. Criminals, like other types of predators, are less likely to target a group than a lone individual. However, the group should also seek to be discreet to avoid attracting unwanted attention.