



## Overview of Multi-Function Cellular Phones

### Introduction

Multi-function cellular phones are often referred to as “Smartphones” and have technical capabilities far exceeding those of a traditional cellular phone. In addition to the ability to make and receive telephone calls, applications such as e-mail, calendar, and an Internet browser with mobile broadband access are common.

The COTS Security Guidance *CSEC Recommendation on the Management of Multi-Function Cellular Phones in the Government of Canada*, describes threats, vulnerabilities and best practices for smartphone deployment and use.

Employee understanding of smartphone security risks and how they must protect the smartphone and enterprise assets are essential elements of the security equation.



Employees can play a key role in ensuring that smartphone use does not pose a threat to enterprise assets.

### Smartphone Design

Smartphones require that employees be vigilant in using their devices securely. Smartphone vendors understand that employees want desktop-like functionality with greater portability.

As a result, employees need to pay attention to proper and secure use as the small size does not mean a lack of processing power, and risks to a smartphone could ultimately affect the entire enterprise network.

### Smartphone Vulnerabilities

**Loss or Theft** – Smartphones are small and easy to lose or steal. Encrypting stored data or storing data on removable media reduces the risk of data compromise. Keeping the device in a safe place is the first line of defence.

**Eavesdropping and Hijacking** – Using smartphones in crowded public places for checking e-mail or using a mobile browser increases opportunities for attackers to gain access to sensitive data in transit or stored on the smartphone, insert malware or hijack services and data. Employees should turn off Bluetooth and only use infrared connection with a trusted source. They should protect data stored on the device and their network sessions with encryption-

**Malware** – Surfing unknown sites or downloading unsigned applications expose smartphones to malware that can propagate to other smartphones and enterprise IT assets.

### Best Practices

Employees can protect private data and enterprise IT assets through conscientious attention to best practices:

**Use in Public Zones** – As much as possible, keep the smartphone turned off and physically secured. At minimum, enable automatic device lock, disable HotSync or ActiveSync, remain in undiscoverable mode, turn off Bluetooth, use passwords in accordance with departmental standards, and change passwords periodically. When connecting to the enterprise network, use a secure VPN and avoid other people “shoulder surfing” and reading information.

**Travelling** – Smartphones may be essential to maintaining contact when travelling on business. Employees should store sensitive data only on removable media secured separately and wipe the smartphone prior to travelling. Physical security includes storage in locked briefcases or room safe and usage only in controlled areas.

Employees must report the loss or theft of a smartphone immediately. They must keep their access token secure and separate from the smartphone and never share their password or PIN.