Issue 1
October 31, 2013

Security Best Practices for Canadian Telecommunications Service Providers (TSPs)

Prepared by: Canadian Security Telecommunications Advisory Committee (CSTAC)

Contents

1. Introduction

1.1 Overview

Canadians rely on the Internet to find information, conduct business, and stay in contact with each other. According to statistics from Public Safety Canada, online sales in Canada in 2007 were estimated at more than $62 billion; and, in 2010, more than 80% of Canadian households had Internet services, with over half of those people making online purchases.[1] By 2012, 87% of Canadian businesses used the Internet.[2] Canadian telecommunications service providers (TSPs) recognize the important role that they play in helping to "build a safer, more secure and more resilient Canada." TSPs realize that the communication services they provide place them in a unique position, for "the ability to communicate" is a key requirement for other critical sectors.

Canada's *National Strategy for Critical Infrastructure* states that "Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence." TSPs are committed to ensuring the security of their infrastructure to reduce the risk of unplanned disruptions and help resolve problems.

As technologies have continued to expand and converge, the dangers from cyber threats have significantly increased. The potential damage has become more severe, and many more computer systems are likely to be affected. Malware now represents a multi-billion dollar underground economy. Today's malware is designed to be unobtrusive and undetectable, and it has a degree of sophistication as good as or better than many commercial software products. For the most part, it is designed to steal credit card information, account data, passwords, and/or business secrets.

This document defines common practices that Canadian TSPs should follow to protect critical infrastructure. It also defines the common practices that TSPs should use to safeguard their networks. Protecting the availability of the underlying communications infrastructure on which their customers depend is critical for TSPs.

1.2 Objective

The best practices defined in this document are intended as voluntary, and are designed to give guidance to TSPs on how best to secure their networks. They ensure that TSPs have a common understanding of what a secure, resilient, available communications service is and how to manage it.

1.3 Scope

As a product of the Canadian Security Telecommunications Advisory Committee (CSTAC), these best practices apply to TSPs that supply and support Canada's telecommunications critical infrastructure (CI). However, there is nothing contained in these best practices which prohibits other service providers from implementing these controls or from leveraging controls from a connected provider to meet the requirements.

[1] Statistics Canada - http://www.statcan.gc.ca/daily-quotidien/111012/dq111012a-eng.htm

[2] Statistics Canada - http://www.statcan.gc.ca/daily-quotidien/130612/dq130612a-eng.pdf

The best practices apply to wireline communications, as well as to TSPs' wireless networks, such as CDMA, HSPA, and future generation phone networks. The best practices do not apply to Wi-Fi or other ad hoc networks, but these may be added in future versions of this document.

The best practices identify the controls that any service provider should have in order to detect cyber security threats, thereby helping the service provider protect both its customers' interests and its own infrastructure.

The scope of this document includes basic controls that should be implemented for redundancy and availability, as well as other topics (such as vendor management) insofar as they relate to the objective of this document.

Areas that are explicitly outside the scope of this document include:

- availability and redundancy against significant facility loss or loss due to external factors such as natural disasters;
- security of external physical plants and buildings; and
- emergency response outside of cyber issues.

These best practices detail the features and practices that a TSP should have in its networks; however, the security resilience at the edge of the networks will vary according to the security service levels requested by customers. Nothing in these best practices limits a TSP's ability to restrict which features are available at which service levels, or to charge for those features. Many of the features listed in these best practices require a significant amount of investment and would have service levels based on customer requirements.

Throughout the best practices there are requirements to notify users if they appear to be infected with malware or if users need to take other actions. While these actions will have a benefit for customers, they are primarily intended to protect the service providers' infrastructure. TSPs are not responsible for removing infections on customers' computers.

1.4 Canadian Security Telecommunications Advisory Committee (CSTAC)

Canada's *National Strategy for Critical Infrastructure*, *Action Plan for Critical Infrastructure*, and *Canada's Cyber Security Strategy* called for government and industry cooperation to ensure the security of Canada's critical infrastructure. Within the communications sector, the response to this call was the establishment of the Canadian Security Telecommunications Advisory Committee (CSTAC).

CSTAC is an industry and government committee, whose aim is to improve the overall security of Canada's telecommunications critical infrastructure.

The Canadian Telecom Cyber Protection (CTCP) Working Group, which reports to CSTAC, is an operational-level group that defines best practices and implements the recommendations of CSTAC related to its mandate.

2. Guiding Sources

These best practices leverage work done by other standards bodies, including:

- International Organization for Standardization (ISO) 27001, 27002, 27011, 27032, and 27035;
- Communications Security Establishment Canada's (CSEC) Technology Supply Chain Guidelines for Telecommunication Equipment and Services;
- Australia's Internet Service Providers' Voluntary Code of Practice; and
- Internet Engineering Task Force Request For Comment (RFCs) as appropriate (such as Security RFCs, Security Considerations, Ingress Filtering for Multihomed Networks).

TSPs carry a mix of traffic over their networks, including internal service provider generated traffic and external customer generated traffic. Cyber security attacks can affect both types of traffic. These best practices take into account the differing privacy concerns as they relate to these disparate networks and attempt to explain what can be monitored and addressed, and how to do so without violating customer privacy.

One of the key ways for TSPs to enhance customer safety and the stability of their portion of the Internet is to share cyber security threat information with one another. This cyber security threat information will be limited to threat characteristics and response information, and will not include individual customers. Mechanisms for sharing such threat information will be defined within CSTAC's mandate.

3. Protection of Critical Service Provider Infrastructure

3.1 Network Architecture and Design

Conceptually speaking, TSPs' networks are composed of three different layers or "planes" with different types of traffic associated with each plane. The management plane is used for communications-related to network traffic management and operations. The control plane is used for routing and signalling of network traffic. The user plane or data plane carries the network users' traffic (data communications).

Each of these planes interconnects various systems or devices and allows them to communicate. Because of the different nature of the communications across each plane, the communications of one plane are separated from those of the other planes.

3.1.1 Network Segmentation

Objective:

To ensure that service provider networks work securely and that traffic from one plane does not affect other planes, it is important to implement basic architectural features in the TSPs' networks.

The controls listed below pertain to each TSP's core network. They are not intended to be implemented on every single network component, as this may not be feasible in all network types and architectures.

Controls:

The TSPs should have the capability to:

1. Ensure that the management, control and user planes are, at a minimum, logically separated and preferably physically separated as well.
2. Provide diagrams demonstrating plane separation within their network infrastructures.

3.1.2 Management Plane

Objective:

The network management plane is the set of network segments over which both the network and associated infrastructure components are managed. This plane includes remote access to systems, as well as management functions such as backup, patch delivery and log extraction. The management plane also carries provisioning traffic, and is the network interface over which communications with back-end billing and customer care systems take place.

If the management plane is not properly protected, then the network components connected to the management plane will be compromised and exposed to attacks. Therefore, it is essential to protect the management plane components.

Controls:

The TSPs should have the capability to:

1. Isolate management functions.

2. Restrict access, allowing access to only known and approved hosts and services.

3. Filter management access to devices.

4. Use secure management protocols whenever possible.

5. Log critical events for network elements.

6. Identify the sources of malicious events.

3.1.3 Control Plane

Objective:

The Control Plane is defined as the networks over which call setup is done and management signalling is passed. These networks must be protected in order to ensure proper operation of the TSP's network.

Controls:

The TSPs should have the capability to:

1. Validate all signalling partners.

2. Validate all external input from signalling partners.

3. Drop/filter signalling outside of defined and allowed adjacencies.

4. Prevent signalling points from being addressable from the either the Data Plane or being accessible from outside of the Control Plane layer.

5. Maintain separation between the data plane and the control plane traffic.

6. Implement mechanisms to protect wireless control channels and signalling traffic.

7. Implement mechanisms to validate the end devices on their networks to ensure that no unauthorized devices are able to connect.

8. Implement egress filtering controls.

3.1.4 Data Plane

Objective:

The data plane is the routing path by which network communications arrive to the end customer. Efforts must be taken to prevent this path from delivering malicious data to the end-user and from being used as an attack path on Canadian critical infrastructure.

Controls:

The TSPs should have the capability to:

1. Validate the integrity of external traffic entering their network wherever possible.

2. Prevent traffic from spoofed (false originator) devices or sources from entering their network.

3. Prevent malicious or inappropriate traffic from entering their network. These measures include protocol, address or volume filters.

4. Prevent volumetric attacks (i.e. attacks that attempt to exceed network or device bandwidth) from affecting their infrastructure.

5. Ensure that management resources and infrastructure networks cannot be targeted by data plane traffic.

6. Use traffic restrictions based on a “blacklist” approach, where all traffic is allowed by default, but the TSP has the ability to block (or blacklist) malicious or inappropriate traffic as necessary.

7. Track malicious traffic to the originating source on their network, or to the point of entry to their network.

8. Correlate traffic sourced on their network to individual customers.

9. Ensure the integrity of traffic leaving their networks.

10. Implement mechanisms to prevent traffic with invalid characteristics.

11. Behave as responsible network citizens and take steps to avoid harm to other networks.

12. Respond to reasonable external complaints from their networks about cases of abuse that have not been prevented.

3.2 Security Controls for Core Equipment

TSP networks are made up of a variety of components, including telephone switches, home location registers, voicemail platforms and value-added service platforms, which provide services to more traditional components such as routers, switches, and other systems-based information technology (IT) components, as well as core IT services, e.g. Domain Name System (DNS) resolution, mail services via Simple Mail Transfer Protocol (SMTP), and network time syncing via Network Time Protocol (NTP).

It is necessary to ensure that these systems be designed and configured in a manner which minimizes the exposure to threat exploitation.

3.2.1 System and Component Hardening

Objective:

TSPs’ networks and their components can only function securely if all components are appropriately protected. The following recommended controls facilitate appropriate configuration of a TSP’s infrastructure components. This list is not intended as an exhaustive or mandatory list given that necessary controls are to be based on the individual components.

Controls:

Basic device hardening should be employed according to vendor guides and industry-recognized best practices, which are not listed in full here but include the following.

The TSPs should have the capability to:

1. Refer to system and device hardening guides published by reputable organizations for more detailed recommendations on the hardening of various types of systems and devices.

2. Choose an industry-recognized hardening standard, or develop in-house standards that meet the same level of effectiveness as recognized public standards and mandate the use of these standards within their organizations.

3. Mandate hardening requirements for third party service providers through contractual obligations relating to the provision and maintenance of services.

3.2.2 Domain Name System (DNS) Hardening and Security

Objective:

The DNS is a fundamental control protocol in Internet Protocol (IP) networks that is essential for connectivity to the Internet. DNS servers provided by TSPs must be secure and resilient to security events and must provide accurate data.

Controls:

The TSPs should have the capability to:

1. Ensure that they are deploying, configuring, and securing DNS infrastructure and services according to industry-recognized standards.

2. Ensure that they protect their own domain, as well as all other domains for which they are responsible.

3. As an authoritative source, ensure that they provide valid contact information.

4. Monitor DNS activity to detect and respond to abuse that could affect customers or other service providers.

5. Respond to abuse queries in a timely fashion.

6. Ensure that authoritative and resolving DNS servers are geographically diverse.

3.3 Security Testing

3.3.1 Vulnerability Assessments

Objective:

TSP environments consist of many interconnected components that make up the management, control, and data network planes. Equipment and services must be tested in a lab prior to deployment in order to ensure that they meet the vendor security specifications and to validate that the security configuration applied by the TSP does not compromise network security.

Controls:

The TSPs should have the capability to:

1. Include security testing in all system development test plans.

2. Test devices against the hardening security standards adopted.

3. Perform security testing prior to systems being granted approval to move into production.

4. Ensure that network planes are secure by conducting regular risk assessments on each plane to identify and respond to unacceptable risks.

3.3.2 Ongoing Compliance Monitoring and Audit

Objective:

After a service or technology is implemented, it must be maintained in a secure fashion. At the core of this is a program of compliance monitoring and audits to ensure that security standards have not degraded over time in the production environment, and that systems adapt to new security standards as they are updated.

Controls:

The TSPs should have the capability to:

1. Establish a Vulnerability Management Program (VMP) containing processes and tools to scan production systems and network equipment for vulnerabilities.

2. Document processes and procedures for addressing discovered vulnerabilities.

3. Detect when new equipment has been added to networks.

3.4 Change Control Procedures

Objective:

A comprehensive Change Management Program will help to ensure that changes to production environments are managed to meet business needs. Good change management will ensure that changes are assessed for risk, approved and implemented in a controlled, consistent manner and that only authorized changes enter into production.

Controls:

The TSPs should have the capability to:

1. Maintain a Change Management Program to ensure that changes to production environments and systems are introduced in a controlled manner to help to mitigate risk and ensure that all changes comply with security requirements.

2. Ensure that the Change Management Program includes a Change Advisory Board (CAB) that has representatives from all impacted areas to ensure that changes are properly reviewed.

3. Ensure that changes are approved by management with direct responsibility for the operations of the components being changed.

4. Ensure that the change control procedures define the testing that is required to validate changes.

5. Ensure that post-change testing is conducted to validate the integrity of all pre-change security controls.

4. Network Security Monitoring and Detection Capabilities

In addition to securing the TSPs' infrastructure, it is also necessary to perform security monitoring and incident detection within the environment; even the most secure environment is still susceptible to incidents and attacks.

4.1 Requirements for TSPs to Monitor Network Infrastructure

Objective:

Service providers should be able to monitor network traffic in order to detect malicious or potentially malicious behaviours on their networks. TSPs should also work toward having the capability to search through cyber security-relevant event logs and monitoring systems for trending in order to detect anomalous behaviours for further investigation.

Controls:

The TSPs should have the capability to:

1. Monitor the infrastructure used for the provision of key services to customers.

2. Monitor critical assets from both external and internal threats.

3. Operate a security information and event management system that collects and correlates information from a variety of systems and devices.

4. Monitor multiple connections.

5. Provide volumetric monitoring of traffic.

6. Monitor for ad hoc threat indicators provided from public, private, and third party sources where feasible.

7. Monitor flows within their networks to detect anomalies.

8. Define their response plans for traffic identified as suspicious by their monitoring activities.

4.2 Types of Traffic to Monitor

4.2.1 Malware

Objective:

Malware traffic cannot always be detected on the computer that is infected because malware writers take steps to avoid detection. Mechanisms such as separate TCP/IP stacks or kernel hooks that hide malware applications in listings can defeat computer detection. There are times when a TSP can detect the signs of malware but the customer cannot. If, in the course of its monitoring duties, a TSP becomes aware of a customer who is affected by malware in this manner, the TSP should take immediate steps to inform the customer.

TSPs are not intended to be a replacement for anti-virus (AV) or other computer security tools that are normally loaded on customers' systems. TSPs are expected to be able to deal with malware traffic if it becomes excessive or is reported to them by a reputable third party.

Controls:

The TSPs should have the capability to:

1. Identify the source of malicious traffic on their network.

2. Respond to valid reports of malicious activity on their networks.

3. Monitor for different types of malicious traffic.

4. Detect malware by signature and volume characteristics.

4.2.2 Network Service Abuse

Objective:

Compromised customer systems may not individually pose a threat to the reliability or performance of critical network services and protocols such as DNS or Dynamic Host Configuration Protocol (DHCP); however, left unchecked in large numbers, these systems can negatively impact the service of other customers and/or inflate capital costs (e.g. through higher TSP capacity provisioning costs).

Controls:

The TSPs should have the capability to:

1. Monitor traffic flows from internal customers to the provider's critical infrastructure-related network services.

2. Refer detected anomalies to Incident Response procedures to address the issue.

4.2.3 Message Abuse

Objective:

Abuse of email messaging services can often result in services being blocked externally and may result in loss of reputation. It is, therefore, important for responsible TSPs to monitor email services in order to ensure that the services are being used as intended.

Controls:

The TSPs should have the capability to:

1. Monitor for misuse, including specific monitoring of outbound message volumes and high numbers of intended message recipients, if they are providing email services.

2. Ensure that customers that exceed message volume and high-number thresholds are identified and follow-up action is taken.

3. Ensure that third party service agreements for outsourced message services include controls and processes for monitoring and responding to message abuse.

4.2.4 Outbound Spam

Objective:

Email-related services should be monitored for outbound spam messages from individual customer IP addresses. The indicators used for detection can be drawn from trusted third parties, such as Senderbase, which tracks counts on outbound spam messaging.

Controls:

The TSPs should have the capability to:

1. Monitor for high volumes of spam-related traffic coming from individual customer IP addresses in order to notify those customers of a potential infection, or take other actions to stop such traffic.

5. Security Incident Response Capabilities

5.1 TSPs' Incident Response Capabilities

Objective:

To ensure that TSPs have the capacity to deal with security incidents, both internal and external to the service provider, the TSPs need to have defined and repeatable processes. The TSP must also have a team of individuals who are capable of handling security incidents as they occur. This team could be a highly distributed functional team or a centralized security incident response team (e.g. security operations centre).

Controls:

The TSPs should have the capability to:

1. Manage cyber security incidents via a defined, tested, and repeatable program.

2. Implement a governance structure for their cyber security incident management program.

3. Respond to operational security incidents occurring during normal and off-hour times.

4. Engage with defined contacts for reporting abusive behaviour, which is monitored and responded to appropriately.

5.2 Response Procedures for Issues Affecting Customers

5.2.1 Incidents Involving Customers' Information Technology (IT) or Home Computers

Objective:

There will be times when a TSP becomes aware of a security breach or malware that is affecting a customer's computer, whether as a victim of an attack or as the perpetrator of an attack (either knowingly or unknowingly). When a TSP becomes aware of such a breach in a customer's system or data, the TSP should notify all affected customers or partners immediately in order to protect the customer from further damage.

Additionally, TSPs should, where technically feasible, contain the impact of the attack by whatever means possible. This could include remediating and mitigating the malicious traffic (see Section 5.3 below) or suspending the customer until such time as the threat is remediated.

Controls:

The TSPs should have the capability to:

1. Define their process for customer notifications.

2. Track customer notifications, including methods and frequency of notifications issued.

3. Validate third party incident information before acting on it.

4. Protect the information source in customer notifications when the source is a confidential third party.

5. Identify and respond to known breaches or potential loss situations affecting customers.

5.2.2 Breach of Customer Information

Objective:

When a TSP becomes aware of an incident that has caused a breach of customer's personal information or information regarding the network configuration, the TSP should notify all affected customers or partners immediately in order to protect those customers and partners from subsequent fraud.

Controls:

The TSPs should have the capability to:

1. Define notification procedures that can be implemented in a short period of time (a maximum of two days) in order to protect their customers and partners.

2. Document and communicate internally who is responsible for contact with customers, partners and the general public.

3. Establish a trusted prearranged method for communicating incident or breach of information with customers.

4. Establish security mechanisms to ensure that customers and partners can authenticate communications coming from the TSP.

5.3 Remediation and Mitigation of Malicious or Inappropriate Traffic

Objective:

There are certain circumstances where some types of traffic might be damaging to customers and/or the TSP. For example, a Denial of Service (DoS) attack against one customer could impact the service provider or other customers. Some types of malware can cause excessive network traffic and have a similar effect as a Distributed Denial of Service (DDoS) attack. In order to protect the TSP's infrastructure, its customers, and the Canadian telecommunications critical infrastructure, TSPs need to have the capacity to filter or to drop traffic that is causing significant damage to others.

Note: *This section concerns traffic that the TSP deems to be malicious or harmful to its network, and is intended for the mitigation and remediation of such traffic. It does not oblige TSPs to block content that a third party finds objectionable or that harms a third party, but merely states the controls that should be in place, should the TSP decide to take action.*

Controls:

The TSPs should have the capability to:

1. Determine what categories of malicious traffic that they would be willing to throttle, filter, or block, and ensure that they have the capability to take these actions.

2. Identify the conditions under which throttle, filter, or blocking actions will be taken on malicious traffic, and which of their networks these actions will protect.

3. Consider traffic filtering and blocking as a last resort when protecting critical networks to prevent the possibility of affecting legitimate traffic.

4. Identify the authoritative intelligence sources on malicious traffic.

5. Issue a publicly stated policy on malicious traffic remediation and mitigation.

6. State their policies on malicious traffic remediation and mitigation within their customer Service Level Agreements (SLAs).

6. Information Sharing and Reporting

Information sharing and reporting are crucial components of protecting critical infrastructure. The extent, the breadth, and the complexity of today's threats are such that cooperation among TSPs is necessary to protect the Canadian critical infrastructure.

In addition to direct information sharing with other Canadian TSPs and government, TSPs should participate in third party working groups and trust groups relevant to their business needs and security responsibilities. These groups offer collaboration and information-sharing opportunities that significantly enhance an organization's ability to prepare and to respond to cyber security events.

Examples of some currently established working groups and trust groups include:

1. Messaging Anti-Abuse Working Group (MAAWG),
2. Forum for Incident Response and Security Teams (FIRST),
3. Microsoft Security Response Alliance (MSRA),
4. Canadian Telecommunications Cyber Protection (CTCP), and
5. North American Network Operators' Group (NANOG).

Additionally, there are a number of established individual based trust groups in which TSPs should actively encourage their staff to participate.

Membership requirements for these groups vary, including fee-based (e.g. MAAWG and FIRST) and contributory participation (e.g. MSRA and CTCP). Regular face-to-face participation is a requirement of all these groups.

Information sharing communities (formal or informal, open or private) may have their own restrictions, including but not limited to Non-Disclosure Agreements (NDAs), vetting and web-of-trust requirements (e.g. withdrawal of attestations of trustworthiness).

Information-sharing between service providers, federal departments and agencies and other relevant entities must respect information classification levels set by information owners, adhere to relevant legislation (e.g. the *Access to Information Act*) and the Treasury Board of Canada's guidelines on information sharing.

6.1 Sharing of Information for Telecommunications Critical Infrastructure Protection

Objective:

To ensure that TSPs are actively engaged in cyber security information sharing for the protection of both their customers and the Canadian critical infrastructure.

The TSPs should have the capability to:

Controls:

1. Both receive and take action on threat information from other network operators and incident response organizations.

2. Document and implement information-sharing practices for sharing threat information with other third parties.

3. Participate in the Canadian Telecommunication Cyber Protection (CTCP) Working Group, if they are responsible for telecommunications critical infrastructure, as defined by Industry Canada.

6.2 Establishment of Mechanisms for Information Sharing

Objective:

All TSPs should have a set of common capabilities to support secure information sharing. These capabilities are minimum requirements in order to securely exchange threat and incident information. While there are more advanced mechanisms, not all organizations will have access to these; hence, a base level of capabilities is necessary. In addition to securing the data, the mechanisms used should also provide for authenticating the sender to the recipient of the information in order to avoid phishing or other impersonation attacks.

Controls:

The TSPs should have the capability to:

1. Support appropriate security mechanisms designed for the secure exchange of information as dictated by the forums in which the information is being shared.

2. Establish and enforce internal policies on classification, privacy and distribution of information, which include requirements for the collection, use, disclosure, retention, and disposal of information.

3. Establish and enforce an acceptable use policy and/or terms of service policies for customers, especially for abuse management.

4. Limit the information shared to only that required to resolve issues, and avoid sharing of personal information.

7. Vendor Management

7.1 Equipment Supply Chain

TSPs act as vendors to their customers. However, they are also customers themselves, as they procure systems and technology from vendors in order to build the infrastructure that provides service to Canadians.

Objective:

In order to reduce threats to their infrastructure and customers, TSPs should make reasonable efforts to ensure that network equipment is secure.

Controls:

The TSPs should have the capability to:

1. Define security standards for procurement of systems, devices, and software.

2. Ensure that relevant security standards are included in purchase agreements, Requests for Proposals (RFPs), and contracts.

3. Require third parties to test and verify all equipment, systems, and software in accordance with well-known best practices (e.g. Common Criteria).

4. Avoid doing business with vendors who do not meet security standards unless the vendors are willing to address the issues or mitigating controls can be introduced.

5. Define procedures to ensure that vendors are following the standards defined by the TSP.

6. Support a compliance verification program to ensure that vendors are following the standards defined by the TSP.

7. Ensure that hardening requirements are passed to suppliers.

7.2 Vendor Security Management

Objective:

Telecommunications vendors often provide significant levels of support to TSPs. TSPs should, therefore, implement security controls on vendors accessing their equipment.

Controls:

The TSPs should have the capability to:

1. Limit vendor access to only those systems for which vendors provide support.

2. Demonstrate that the practices of their telecommunications vendors do not impact or degrade the level of security of the TSPs' infrastructures.

3. Monitor vendor activity to ensure the integrity and security of their networks.

4. Ensure that security hardening requirements are included in Service Level Agreement (SLA) clauses with third party providers.

8. Privacy

Objective:

The privacy rights of Canadians are protected by several federal and provincial Acts, as well as privacy regulations imposed by the Canadian Radio and Telecommunications Commission (CRTC). These legal requirements take full precedence over the guidelines listed in these best practices. TSPs that follow these best practices are also expected to maintain the same level of commitment concerning privacy toward their customers.

Specifically, sharing of personal information is rarely needed for abuse or trouble resolution. The TSP serving a customer must be able to identify the user who is infected or performing abuse activities, but this information should not be shared with other entities unless disclosure is done in accordance with the requirements of the provider's Privacy Policies and Terms of Service.

While the relevant legislation outlines the privacy rights of citizens, along with the responsibilities that TSPs have in protecting citizens' rights, there are additional best practices that should also be applied.

Controls:

The TSPs should have the capability to:

1. Ensure that the solutions and services that they provide adhere to all applicable privacy legislation.

2. Ensure that they deal with privacy concerns promptly and transparently.

3. Evaluate any actions that they take to protect the security of their network against the privacy trade-offs to their customers.

Annex A — Glossary

BGP	Border Gateway Protocol
CDMA	Code Division Multiple Access
CIP	Critical Infrastructure Protection
CLI	Command Line Interface
CSEC	Communications Security Establishment Canada
CSTAC	Canadian Security Telecommunications Advisory Committee
CTCP	Canadian Telecom Cyber Protection Working Group
DDoS	Distributed Denial of Service Attack
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service Attack
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
HSPA	High Speed Packet Access
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MD5	Message Digest 5
QOS	Quality of Service
RFP	Request for Proposal
RPF	Reverse Path Forwarding
SIM	Subscriber Identity Module
SSH	Secure Shell
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TSP	Telecommunications Service Provider
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
VAS	Value Added Service
VLAN	Virtual Local Area Network
Wi-Fi	Wireless Fidelity

Annex B — Resources

Canadian Cyber Incident Response Centre

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice for cyber security incidents.

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) publishes standards and guides for U.S. Government Information Processing systems and other pertinent security information.

Center for Internet Security

The Center for Internet Security (CIS) publishes standards for hardening various types of equipment for networks and computers. It also publishes scoring tools that can be used to assess network components against the standards.

Cybertip.ca

Cybertip.ca is Canada's national tip line for reporting online exploitation of children.

Office of the Privacy Commissioner

The Office of the Privacy Commissioner of Canada (OPC) oversees compliance with both the *Privacy Act*, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The OPC provides data breach notification guidance under PIPEDA. See Key Steps for Organizations in Responding to Privacy Breaches and the Privacy Breach Incident Report Form.

The **Treasury Board of Canada**

The Treasury Board of Canada has published guidelines on information sharing with and by Government of Canada agencies. These guidelines should be respected when federal departments are involved.