Security Best Practice Policy for Canadian Telecommunications Service Providers (CTSPs)

V1.1 January 20, 2020

Authored by: Canadian Telecommunications Cyber Protection (CTCP) working group

for

Presentation by: Canadian Security Telecommunications Advisory Committee (CSTAC)

Contents

Revision History

The following table highlights edit changes to the document.

Editor	Date	Notes
CTCP Architecture Team	June 1, 2019	Updated content
Kevin Miller, SaskTel	Sept 17, 2019	Draft started
Marc Kneppers, TELUS	Jan 15, 2020	Minor updated based on stakeholder feedback
Marc Kneppers, TELUS	March 31, 2020	Updated reference to Information Sharing, Reporting and Privacy standard

The following table highlights major content or policy changes to the document.

Section	Contribution	Date
SS7	A general recommendation to adhere to GSMA SS7 best practices for monitoring and mitigation SS7 attacks was included as a new best practice.	March 13, 2019
BGP	A summary of Internet best practices and what is currently common and appropriate for Canadian operators.	March 13, 2019
DNS	Best practices for DNS implementation and operations, in more detail than previous.	March 13, 2019
Response	Recognition of our role in being good netizens was added. Section 5.2.1 and 5.3 add the responsibility of CTSPs for attacks that initiate in their network space and creates the expectation that CTSPs will monitor and mitigate outbound attacks that will affect other Internet entities.	March 13, 2019
Awareness	Employee and Customer cyber security awareness was added as a best practice.	April 10, 2019
Privacy	Privacy expectations with reference to applicable federal statutes were added.	February 13, 2019

Virtualization	Virtualization best practices added to section 3.1.5.	April 10, 2019

1. Introduction

1.1 Overview

Canada's communication infrastructure has become a core component of our society and individual lives. Traditionally, Canadian Telecommunications Service Providers (CTSPs) have provided Critical Infrastructure (CI) services such as basic voice telephony as well as emergency capabilities via the national 911 systems. Increasingly, however, Canadian Telecommunication Service Provider (CTSP) data services like the Internet, mobility data, and point-to-point network connections are becoming just as important to Canadians.

In light of this dependency on CTSP communication networks, we need to ensure that the services are built and provisioned securely and can withstand cyber attacks. The Canadian Center for Cyber Security (CCCS) recently published the National Cyber Threat Assessment 2018[1] and has identified a number of threats to Canadian communications which will challenge our ability to secure Canadian communications.

For CTSPs, two primary threats stand out:

- Targeting of our national CI by state-sponsored activity.
- Exploitation of the trust relationships between service providers and their customers by cyber threat actors.

This assessment shines a light on the need for secure communications networks and services.

In 2010, Canada launched the National Cyber Security Strategy which called for a national, collaborative approach to cyber defence and, among other things, increased information sharing among CI providers and CTSPs. This strategy has been updated for 2018[2] and expands this collaboration by calling for partnerships to secure vital cyber systems outside of the federal government.

[1] Canadian Center for Cyber Security, “National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age”, 2018, ,https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018; retrieved March 12, 2019

[2] Public Safety Canada, “National Cyber Security Strategy”, 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx; retrieved March 12, 2019

This is the context into which we publish the second version of the Canadian Security Telecommunications Advisory Committee's (CSTAC[3]) CTSP Best Practices Policy and Standards documents.

1.2 Objective

The goal of the CTSP Best Practice policy and standards documents are to summarize the existing best practice consensus for securing CI communications networks and to establish a baseline against which we compare our own practices and to which we hold other CTSPs.

The capabilities of CTSPs vary greatly, depending on their size and experience, and the practices outline in this document are intended to be high-level guidance that can be used to shape the implementation of specific controls at each CTSPs. While there are many authoritative best practices guides available over the Internet, not all the recommendations in those is suitable for a national CTSP and there is value in having the Canadian community agree on which of those practices should be mandatory, as they have direct relevance to Canada, and which can be optional to a provider.

This document will ensure that CTSPs have a common understanding of what a secure, resilient, available communications service is and how to manage it.

1.3 Scope

The guidance contained in this document is written at a high-level and generally aligns to a statement of principle or general operational practice. This guidance is then intended to be applied to the complete set of aggregate services, technology and operations from CTSPs. This includes overall wireline infrastructure (backbone networks), mobility networks, as well as the management of connected devices and users across that technology.

Where applicable, we have suggested a control target that would provide evidence that the principle has been applied, but these are not intended to serve as strict audit criteria, but rather as a starting point for a CTSPs review of its own security controls.

Where there are technologies or specifications that require more detailed treatment, CSTAC will also publish dedicated standards, and implementation guides.

[3] CSTAC, Canadian Security Telecommunications Advisory Committee, https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf10727.html; retrieved March 12, 2019

This document does not address regulated requirements, nor does it govern emergency response services. Those areas remain under federal governance with strict requirements on CTSPs.

Finally, as a product of CSTAC, these best practices apply to CTSPs that supply and support Canada's telecommunications 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.

1.4 Canadian Security Telecommunications Advisory Committee (CSTAC)

To achieve the security goals highlighted in the National Cyber Security Strategy, the Canadian Government and industry are cooperating to ensure the security of Canada's critical infrastructure. Within the communications sector, the CSTAC was established as a vehicle for this collaboration.

In the context of the communications sector, CSTAC's mission is to collaboratively anticipate threats and vulnerabilities and provide advice on realistic solutions and best practices in order to improve the security and resiliency of Canada's connected world.

The Canadian Telecom Cyber Protection (CTCP) Working Group is an operational-level group that reports to CSTAC and is the primary author of this document. CTCP defines best practice policy and standards and are responsible for implementing the recommendations.

2. Guiding Sources

The best practices used to formulate the policy and standards documents have been drawn from a number and variety of sources that deal with the specifics of each subject matter. As such, these documents leverage work done by other standards bodies, with the intention of consolidating those most applicable to CTSPs in Canada. Primary sources include:

- International Organization for Standardization (ISO) 27001, 27002, 27011, 27032, and 27035;
- National Institute of Standards and Technology (NIST) Special Publications on Information Security (SP 800) and Federal Information Processing Standards (FIPS);
- Communications Security Establishment Canada's (CSEC) Technology Supply

Chain Guidelines (TSCG) for Telecommunication Equipment and Services; and
- Internet Engineering Task Force Request For Comment (RFCs) as appropriate (such as Security RFCs, Security Considerations, Ingress Filtering for Multihomed Networks).

CTSPs 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 consider 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. Practice guides dealing with these subject matters will be denoted in their corresponding section and included in Appendix B for reference.

3. Critical Infrastructure Protection

3.1 Network Architecture and Design

Conceptually speaking, CTSPs 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 differing nature of communications across each plane, the communications of one plane are separated from those of the other planes.

Please refer to the "CSTAC Critical Infrastructure Protection Standard for CTSPs" document for the control requirements for each of the Network Architecture and Design sub-sections listed below.

3.1.1 Network Segmentation

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 CTSPs' networks.

3.1.2 Management Plane

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.

3.1.3 Control Plane

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 CTSP's network.

3.1.3.1 BGP Interconnection

BGP is the fundamental control plane for the Internet and operator networks. Operators need to be able to ensure that they maintain operational control over their BGP infrastructure and are able to ensure the integrity of the data passed through BGP.

3.1.3.2 SS7 (Signalling System 7)

SS7 is the fundamental control plane for the voice network, including SMS. It can be attacked via operator interconnects. CTSPs need to be able to ensure only legitimate access to SS7 and end-user services.

3.1.4 Data Plane

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.

3.1.5 Virtualization

Virtualization can be used to improve consolidation ratios and streamline operations; however, this must be done with a proper understanding of the security implications these decisions have on the overall security posture of the network. Not only are virtualized data centres susceptible to most of the vulnerabilities inherent with traditional data centres, but they introduce new vulnerabilities specific to this environment. Replacing many of the physical isolation mechanisms with logical equivalents may introduce unacceptable risk into the network architecture. Efforts must to taken to implement safeguards and best practices to address complex threats like system management mode rootkits, side-channel attacks, and hyperjacking, as well as practical threats like misconfigurations, compromise of the management interface, and conventional attacks on both the hypervisor and virtual machines.

3.2 Security Controls for Core Equipment

CTSP 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.

Please refer to the "CSTAC Critical Infrastructure Protection Standard for CTSPs" document for the control requirements for each of the Security Controls for Core Equipment sub-sections listed below.

3.2.1 System and Component Hardening

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

3.2.2 Domain Name System (DNS) Hardening and Security

The DNS is a fundamental control protocol in Internet Protocol (IP) networks that is essential for connectivity to the Internet. DNS servers provided by CTSPs must be secure and resilient to security events and must provide accurate data. Common DNS architectural design considerations and principles are outlined in Appendix A of the "CSTAC Critical Infrastructure Protection Standard for CTSPs" document. CSTPs should review, understand and apply these DNS architectural design considerations and principles across their respective environments.

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

The policies and standards apply to wireline communications, as well as to CTSPs' wireless networks, such as LTE 4G, 5G and future generation phone networks. DNS is

used to find core network functions and even sometimes to place calls and will take increasing importance in tomorrow's networks.

The standards identify DNS controls that any service provider should have to protect both its customers' interests and its own infrastructure. The DNS policies and standards detail the features and practices that a CTSP 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 policies or standards limit a CTSP'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 policies and standards represent the potential for significant investment to deliver the service levels to meet customer requirements.

Throughout there are recommendations to notify groups or to act, notifications to end users are informational, and CTSPs are not responsible for detecting or removing infections on subscribers' user equipment.

3.2.3 DNS Service Protection Overview

A telecommunications service provider often maintains several different DNS infrastructures for various IT contexts including internal users (employees, contractors, subcontractors) supply chain partners, customers and Internet users. The "cloud" however is driving enterprises towards a single namespace.

If the DNS namespace is not properly segregated, then there can be leakage of valuable information about a system or service in the form of the host and service names

3.2.3.1 Internal DNS

Minimize resolution visibility "horizons" to increase the difficulty level of threat actors in analysis and formulation of attacks.

Separate the business functions of the CTSP and the service provider provisioning functional namespace, such that service provider provisioning information is not exposed broadly and without necessity.

3.2.3.2 DNS

DNS services are increasingly important in the deployment of telecommunications service provider infrastructure. The exhaustion of IPv4 address space, dearth of IPv6 experience and broad-based adoption of HTTPS for inter-process communications by distributed applications are driving an increasing dependency on DNS services.

Additionally, DNS usage in non-traditional signalling, control and management planes create an abstraction between device address and service where it did not previously exist.

This scope is the telecommunications service provider's DNS infrastructure made visible to its clients, customers, subscribers, and some supply chain partners.

CTSPs should engage with network element management and operational support systems teams to ensure that DNS deployments are resilient, and that DNS provides valid service location information.

3.2.3.3 5G DNS

CTSPs 5G networks will use proposed 3GPP standards that replace many LTE core and RAN interfaces with Services Based Interfaces (SBI). SBIs use uniform resource locators and HTTPS to exchange messages. While the 3GPP standard may not specify name-based interfaces, virtualization flexibility and exhausted and conflicting IP address space will undoubtedly cause pressure to create last-minute DNS services. 5G distributed network core rollouts should assure scale and reliability if DNS is deployed as part of the CTSP's 5G network.

CTSPs should engage with 5G teams to ensure that DNS deployments in a distributed 5G core have a resilient DNS services architecture based on the information found in the "CSTAC Critical Infrastructure Protection Standard for CTSPs" document for 5G DNS Service Protection control requirements.

3.2.3.4 DNS – User Equipment Plane Resolution Control

Some DNS information is intended for LTE evolved packet core network elements to place calls for user equipment (UE).

Control the resolution path of DNS traffic such that only trusted forwarders and information is provided to the UE.

3.2.3.5 DNS – Control Plane & User Equipment Plane Separation

Some DNS information is intended for LTE evolved packet core network elements to place calls for user equipment (UE).

3.2.3.6 Resiliency across DNS Service

Multiple techniques can be used to ensure resiliency of the DNS service.

3.2.3.7 DNS Monitoring

Several sections in the "CSTAC Critical Infrastructure Protection Standard for CTSPs" document call for DNS alerting and suspicious event logging. While this may be suitable for investigative response purposes, it is prudent to detect anomalous activity that can be indications and warnings of imminent risks presented to DNS infrastructure.

3.2.3.8 DNS Configuration Management

Changes to DNS zone files, and server configurations should support configuration management practices that align with the CTSP's change and service management processes and provides the linkage from technical realm to the business. This allows effective detection and response of aberrations that originate in the divide between the business authorization and technical implementation.

3.2.3.9 Network Considerations for Externally Accessible DNS

The Domain Name Service (DNS) is a critical service that must be made accessible to external users (authoritative: Internet; resolvers: customers) and internal users (authoritative and resolvers). The DNS service must be able to respond rapidly to requests with low latency to ensure the responsiveness of the Internet. This has grown more so in the recent years with the explosion of the number of links embedded in each web page a user access. In addition, DNS service is the target of multiple types of attacks. Different methods can be used to secure them at different levels: network, application, monitoring, etc. The standards listed in the "CSTAC Critical Infrastructure Protection Standard for CTSPs" document details the network aspects that must be considered for an efficient deployment of the DNS service.

3.2.3.10 DNS Network Considerations for IPv6

With the depletion of available IPv4 addresses, the world is slowly shifting to IPv6. IPv4 and IPv6 will need be supported by the DNS service in order to enable migration to IPv6, with the complexity and length of IPv6 addresses, the importance of the DNS service is even higher for IPv6.

3.2.3.11 DNS Query Logging

DNS resolution infrastructure should be designed to provide resolution telemetry and security events information to external systems, such that it minimizes the impact on availability.

3.2.3.12 DNS Cache Poisoning

DNS query logs provide data that can provide information indicating the source of cache poisoning attacks using various methods. Often the attackers are indicated when their IP address is associated with a lack of entropy in the source port higher-than-expected frequency of answers, and ratios of queries to answers.

3.2.3.13 DNS Cache Stretching

Authoritative servers may be bombarded by resolvers if the remote authority is offline.

3.2.3.14 DNS – Detection and Defense

Opportunities for defensive and detective DNS controls will help to prevent and detect activity such as Botnet activity within CTSP environments. Defensive controls will protect DNS infrastructure against threats that attempt to use it as an attack or amplification method.

Due to the widespread ability of DNS traffic to traverse different networks malicious code can use DNS for Botnet command and control (C2) instructions. Detective DNS controls will help CTSPs to identify and control such DNS command and control traffic.

3.2.3.15 DNS – Privacy Protection

DNS metadata in aggregation can create the potential for privacy breaches. Manage data collection closely to avoid unintended privacy consequences of increased DNS security monitoring and event collection.

Consider DNS resolution traffic in the context of an adversary monitoring it upstream and model the aggregate information disclosure over a period of time. Consider policy, technical and/or contractual safeguards that reduce the likelihood that an adversary or unauthorized party could finely associate individuals to other entities in violation of Canada's Personal Information and Electronic Documents Act, the organization's Privacy Policy, and/or the service providers' terms of service or terms of use.

Consider the implementation of DNS technical configurations, vendor selection criteria or contractual safeguards that reduce the information queries to the minimum required when performing recursive queries.

Protect confidentiality of queries and answers across untrusted networks where endpoints are under the providers' control through the implementation of technical configurations, vendor selection criteria or contractual safeguards on DNS infrastructure.

3.2.3.16 DNS – Cryptography Security

Organizations should use cryptographic methods to ensure the integrity of source resource records data and authenticity of answers provided to client resolvers.

3.2.3.17 DNS – Net Neutrality

Organizations should enable subscribers to select and route DNS request to resolvers of their choice.

3.3 Security Testing

Please refer to the “CSTAC Critical Infrastructure Protection Standard for CTSPs” document for the control requirements for each of the Security Testing sub-sections listed below.

3.3.1 Vulnerability Assessments

CTSP 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 CTSP does not compromise network security.

3.3.2 Compliance Monitoring and Audit

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.

3.4 Change Procedures

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.

Please refer to the “CSTAC Critical Infrastructure Protection Standard for CTSPs” document for the Change Procedure Control requirements.

4. Network Security Monitoring and Detection

In addition to securing the CTSPs' 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.

Please refer to the "CSTAC Network Security Monitoring and Detection Standard for CTSPs" document for the control requirements for each of the Network Security Monitoring and Detection sub-sections listed below.

4.1 Requirements for CTSPs to Monitor Network Infrastructure

Service providers should be able to monitor network traffic in order to detect malicious or potentially malicious behaviours on their networks. CTSPs 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.

4.2 Types of Traffic to Monitor

4.2.1 Malware

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 CTSP can detect the signs of malware but the customer cannot. If, in the course of its monitoring duties, a CTSP becomes aware of a customer who is affected by malware in this manner, the CTSP should take reasonable actions to inform the customer.
CTSPs are not intended to be a replacement for antivirus (AV) or other computer security tools that are normally loaded on customers' systems. CTSPs are expected to be able to deal with malware traffic if it becomes excessive or is reported to them by a reputable third party.

4.2.2 Network Service Abuse

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 CTSP capacity provisioning costs).

4.2.3 Message Abuse

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 CTSPs to monitor email services in order to ensure that the services are being used as intended.

4.2.4 Outbound Spam

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.

5. Security Incident Response

Please refer to the “CSTAC Security Incident Response Standard for CTSPs” document for the control requirements for each of the Security Incident Response Capabilities sub-sections listed below.

5.1 Incident Response Capabilities

To ensure that CTSPs have the capacity to deal with security incidents, both internal and external to the service provider, the CTSPs must have defined and repeatable incident response processes. The CTSP must maintain a team of individuals who are capable of handling security incidents as they occur.

5.2 Response Procedures for Issues Affecting Customers

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

There will be times when a CTSP becomes aware of a significant security incident involving a customer's device or where a customer's device is having a significant impact on the CTSP's network or other providers' networks. In these circumstances, the CTSP should notify the customer in a timely manner to minimize further damage from the incident.

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

5.2.2 Breach of Customer Information

When a CTSP becomes aware of an incident that involves a breach of customer's personal information or other sensitive information, the CTSP will notify all affected customers as soon as feasible in order to reduce the likelihood of the breached information being used for subsequent personal or financial harm against customers. Breach notification is required as part of PIPEDA, which includes a mandatory requirement that organizations provide notice to affected individuals and the Privacy Commissioner of Canada under circumstances where "the breach creates a real risk of significant harm to the individual".

5.3 Remediation and Mitigation of Malicious or Inappropriate Traffic

There are circumstances where some types of traffic might be damaging to customers and/or the CTSP. For example, a Denial of Service (DoS) attack against one customer could impact services provided by the service provider, other customers, or even other CTSPs. To protect the CTSP's infrastructure, its customers, and the Canadian telecommunications critical infrastructure, CTSPs need to have the capacity to filter or to drop traffic that is causing significant damage to themselves or others.

> *Note: This section concerns traffic that the CTSP deems to be harmful to its network, or harmful to other providers' networks and is intended for the mitigation and remediation of such traffic. It does not oblige CTSPs to block content that a third party finds*

objectionable, but merely states the controls that should be in place, so the CTSP can act when warranted.

6. Information Sharing, Reporting and Privacy

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

Please refer to the "CSTAC Information Sharing, Reporting and Privacy Standard for CTSPs" document for the control requirements for each of the Information Sharing, Reporting and Privacy sub-sections listed below.

6.1 Sharing of Information for Telecommunications Critical Infrastructure Protection

CTSPs that are actively engaged in Cyber security information sharing protect both customers and Canadian critical infrastructure. CTSPs will ensure they are sharing cyber threat information with each other and government. CTSPs 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 CTSPs 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.

6.2 Establishment of Mechanisms for Information Sharing

All CTSPs 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.

6.3 Privacy

The privacy rights of Canadians are protected by several federal and provincial Acts and Commissions, including:

1. the Privacy Act, which covers how federal government handles personal information;
2. the Personal Information Protection and Electronic Documents Act (PIPEDA), which covers how private businesses[4] handle personal information;
3. the Canadian Radio-television and Telecommunications Commission (CRTC) Act, which covers the licensure and regulation of electronic communication services; and
4. Provincial and Territorial Legislation for municipalities, universities, schools, and hospitals.

These legal requirements take full precedence over the guidelines listed in these best practices. CTSPs 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 not needed for abuse or trouble resolution. The CTSP serving a customer must be able to identify the user who is the

[4] Non-commercial entities and activities are generally regulated by their respective provinces/territories.

source or target of malicious 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 CTSPs have in protecting citizens' rights, there are additional best practices that should also be applied.

7. Vendor Management

Please refer to the "CSTAC Vendor Management for CTSPs" document for the control requirements for each of the Vendor Management sub-sections listed below.

7.1 Equipment Supply Chain

CTSPs 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.

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

7.2 Vendor Security Management

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

8. Awareness

Creating an effective security awareness program is key to securing any organization, large or small. Demystifying security and educating users about their role in protecting your organization helps cultivate a robust first line of defence.
Using the NIST, ISO and/or PCI frameworks to guide and build out your security awareness program is an effective way to ensure users are educated on key security topics.

Please refer to the "CSTAC Awareness Standard for CTSPs" document for the control requirements for each of the Awareness sub-sections listed below.

8.1 Policy and Standards

The organization develops and documents security policies and standards. Once created, policies and standards are promoted and made easily available to users.

8.1.1 Policy and Standards creation

Provide concise information regarding the organization's security guidelines, procedures and expectations for users.

8.1.2 Policy and Standards Maintenance

Review and update policy and standards on a regular basis, there by providing the most relevant and up to date information to users.

8.2 Training

8.2.1 Basic Security Awareness Training

Organization provides basic security awareness training to all system users, at all levels of access and seniority.

8.2.2 Specialized / Role-based Training

Provide role-specific security training to users with access to sensitive data and/or those who are potentially exposed to more frequent security risks as part of their role.

8.2.3 Ongoing Training

Conduct ongoing, mandatory user training (for instance, annually), focused on the evolving threat landscape and/or security threats known to be a continuous challenge for organizations (e.g. phishing).

8.2.4 Records and Metrics

Ensure assigned mandatory training is completed within specified timelines.

8.3 Security Awareness Program

8.3.1 Program Creation

Implement and organization-wide security awareness program that complements the training program and provides users with information about the latest threats, day-to-day security best practices, etc. on an on-going basis.

8.3.2 Program Efficacy Metrics

Use metrics and user feedback to measure program impact.

8.4 Security Community and Industry Contracts

Establish and maintain contact with select, trusted groups, organizations and/or associations within the security community.

8.5 External Security Awareness Program

Where possible and appropriate educate customers and other stakeholders on their role in ensuring their own security when interacting with your organization.

Annex A — Glossary

- BGP Border Gateway Protocol
- CCCS Canadian Centre for Cyber Security
- CDMA Code Division Multiple Access
- CI Critical Infrastructure
- CIP Critical Infrastructure Protection
- CLI Command Line Interface
- CSEC Communications Security Establishment
- CRTC Canadian Radio-television and Telecommunications Commission
- CSTAC Canadian Security Telecommunications Advisory Committee
- CTCP Canadian Telecom Cyber Protection Working Group
- CTSP Telecommunications Service Provider
- DDoS Distributed Denial of Service Attack
- DHCP Dynamic Host Configuration Protocol
- DNS Domain Name System
- DoS Denial of Service Attack
- FIPS Federal Information Processing Standards
- 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
- IETF Internet Engineering Task Force
- 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
- NIST National Institute of Standards and Technology
- OPC Office of the Privacy Commissioner of Canada
- PIPEDA Personal Information Protection and Electronic Documents Act
- QOS Quality of Service
- RFC Request for Comments
- 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
- TBS Treasury Board of Canada Secretariat
- TSCG Technology Supply Chain Guidelines
- 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 Centre for Cyber Security

The Canadian Centre for Cyber Security (CCCS) is the National CERT (Computer Emergency Response Team), and the Government of Canada CIRT (Computer Incident Response Team), working in close collaboration with government departments, critical infrastructure, Canadian businesses and international partners to respond to and mitigate cyber events. The CCCS, formed in October 2018, is a consolidation of existing operational groups from Public Safety Canada, Shared Services Canada, and the Communications Security Establishment IT Security branch.

https://cyber.gc.ca; retrieved April 10, 2019

Canadian Security Telecommunications Advisory Committee

The Canadian Security Telecommunications Advisory Committee (CSTAC) was created to support two key Government of Canada initiatives; the National Strategy for Critical Infrastructure and Canada's Cyber Security Strategy. CSTAC allows the private and public sectors to exchange information and collaborate strategically on current and evolving issues that may affect the telecommunications infrastructure, including cyber security threats.

https://www.ic.gc.ca; retrieved April 10, 2019

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.

https://www.nist.gov/; retrieved March 12, 2019

Center for Internet Security

The Center for Internet Security (CIS) is a non-profit entity that publishes standards and guidelines on the use of hardening techniques for security IT systems against attacks. CIS standards are refined and verified by a volunteer global community. The CIS also publishes scoring tools that can be used to assess network components against the standards.

https://www.cisecurity.org/; retrieved April 10, 2019

Cybertip.ca

The Canadian Centre for Child Protection (CCCP) is a charitable organization dedicated to reducing child victimization by providing national programs and services to the Canadian public. The CCCP operates *Cybertip.ca,* Canada's national tip line for reporting the online exploitation of children.

https://www.cybertip.ca; retrieved April 10, 2019

Internet Engineering Task Force

The Internet Engineering Task Force (IETF) is an open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite. It has no formal membership or membership requirements.

https://www.ietf.org/; retrieved April 10, 2019

International Organization for Standardization

The International Organization for Standardization (ISO) is an international standard-setting body composed of representatives from various national standards organizations. The ISO 27000 series deals with matters of Information Security Management Systems.

https://www.iso.org/; retrieved April 10, 2019

Office of the Privacy Commissioner

The Office of the Privacy Commissioner of Canada (OPC) oversees legal compliance with the handling of personal information held by the Government of Canada, as well as the proper application of the Personal Information Protection and Electronic Documents Act (PIPEDA), which deals with personal information held in federally regulated private sector industries.

https://www.priv.gc.ca; retrieved April 10, 2019

The Treasury Board of Canada

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