Improving the Reliability and Resilience of Canada's Digital Infrastructure

Canadian Forum for Digital Infrastructure Resilience (CFDIR)
Recommendations to the
Minister of Innovation, Science and Industry

May 1, 2023

EXECUTIVE SUMMARY

The following set of recommendations were created in response to a request from the Minister of Innovation, Science and Industry to the Canadian Forum for Digital Infrastructure Resilience (CFDIR). The request highlighted the importance of digital infrastructure in all aspects of Canadian economic and social activity. The Minister also noted the important role of the products, services, and infrastructure provided by CFDIR member organizations for both Canada's digital resilience and economy. The Minister's letter was sent November 1, 2022 with a six-month deadline.[i]

The Minister asked for a collaboratively prepared set of recommendations to improve the reliability and resilience of Canada's digital infrastructure. Presented below are:

- The method used to prepare and present our recommendations.
- Our recommendations to improve the reliability and resilience of Canada's digital infrastructure:
    - Three recommendations of a General nature
    - Twelve recommendations to ensure that Canada has Robust Networks and Systems underpinning its digital infrastructure
    - Eight recommendations to ensure that there is Coordinated Planning and Preparation to respond to threats to our digital infrastructure
    - Three recommendations concerning Strengthening Accountability to drive for resilience by our digital infrastructure stakeholders

RECOMMENDATIONS TABLE

General Topics	**Directed Towards**	
G 1: Cabinet position responsible for ensuring government-wide coherence and action on cyber security policy and technology goals.	Government	
G 2: Skills, talent and training	Government	
G 3: Maintaining and leveraging CFDIR	Government	
Robust Networks and Systems Topics	**Directed Towards**	
RNS 1: Resilience requirements for broadband funding programs	Government	
RNS 2: Incumbent ISPs' transport network leasing	Government	
RNS 3: Improving peering policies for better Internet resiliency		Industry
RNS 4: Prioritizing competition and diversity of facilities providers	Government	
RNS 5: Upstream Internet network provider bill of materials	Government	
RNS 6: Updating Internet transit procurement based on 2023 Internet standards	Government	Industry
RNS 7: Documenting the state of multiple concurrent Internet connection solutions		Industry
RNS 8: Adopting international standards and best practices	Government	
RNS 9: Supporting national resilient connectivity	Government	
RNS 10: Financial incentives for resilience	Government	
RNS 11: Designating or creating a critical infrastructure network provider	Government	
RNS 12: Interdependency of national digital infrastructure systems	Government	Industry
Coordinated Planning and Preparation Topics	**Directed Towards**	
CPP 1: Expanded emergency planning exercises		Industry
CPP 2: Emergency contacts	Government	Industry
CPP 3: Establishing a critical infrastructure resilience centre	Government	
CPP 4: Supply chain governance set	Government	Industry
CPP 5: Defence strategies and technology capability set	Government	
CPP 6: Migration to post-quantum cryptography and quantum-safe digital infrastructure	Government	Industry
CPP 7: Internet of Things security and botnets	Government	Industry
CPP 8: National industrial Internet of Things risk assessment	Government	Industry
Strengthening Accountability Topics	**Directed Towards**	
SA 1: Coordinating action between CSTAC and CFDIR	Government	Industry
SA 2: Updating Industrial Security Program requirements for IT providers	Government	
SA 3: Modernizing understanding of cyber safeguards	Government	Industry

INTRODUCTION

CFDIR is Canada's private-public forum through which industry and key federal partners work together to improve policy regarding digital infrastructure resilience. This document presents recommendations from CFDIR's industry representatives to inform the Minister of Innovation, Science and Industry regarding what steps should, as priorities, be taken to enhance Canadian digital infrastructure resilience.

In the summer of 2022, millions of Canadians experienced first-hand the difficulty of technological disruption during the Rogers outage[ii] and Hurricane Fiona. These events – during which millions of Canadians were without access to critical Internet technology, businesses were unable to accept payments and host customers, and government services were rendered inaccessible – demonstrated the urgency to improve resilience.

Digital infrastructure resilience ensures that the digital infrastructure technologies in Canadian society work at an acceptable level despite disruptions due to events such as extreme weather, human error, cyber-attacks. As the technological landscape is complex and ever-changing, achieving resilience is no simple feat. Digital infrastructure resilience is critical to support a trusted and thriving digital economy and society. From the individuals interacting with technology every day, to the companies that develop, deploy, protect, harden, monitor and sell the technology, to the government framing of regulatory and other policies, all stakeholders have active roles to play in supporting the resilience of the digital infrastructure ecosystem.

Achieving widespread digital infrastructure resilience requires a comprehensive understanding of the relevant technologies, how they operate, and how they interact with each other and with different stakeholders. Because these technologies, and the standards which they are expected to meet, are almost wholly developed by the ICT industry, industry's voice in this effort is critical.

METHODOLOGY

The Canadian Forum for Digital Infrastructure Resilience is a consensus-based and action-oriented public-private collaboration that was formed to enhance understanding of, and recommend improvements to, the resilience of Canadian critical digital infrastructure. Innovation, Science and Economic Development Canada (ISED) established CFDIR in 2020, in part to support Canada's National Strategy for Critical Infrastructure (CI). Under this strategy, ISED is the lead federal department for the information and communication technology (ICT) sector. CFDIR brings together key federal partners and industry to improve digital infrastructure resiliency.

CFDIR working groups are industry-led and comprise participants from CFDIR member organizations. The working groups undertake agreed-upon projects. Working group focus areas have included:

- Cloud Resilience
- Quantum Readiness
- Supply Chain Assurance
- Internet Resilience
- Internet of Things (IoT)

Definitions of *digital infrastructure, critical services*, *reliability* and *resilience* can be problematic, if one goes beyond the high level. What digital infrastructure is in scope, and does it include everything that is connected anywhere? Which services, beyond 911, are considered critical? How does one measure reliability or resilience for that digital infrastructure and for those critical services given that failures may be hard (e.g., complete outage) or soft (e.g., slow response time), widespread (e.g., national) or localized (e.g., neighbourhood or cell tower), long-lasting or momentary, and so on.

CFDIR's practical view is that critical services are those that Canadians depend upon for their livelihood, well-being and security. The digital infrastructure in scope includes at least those assets that provide such services. Reliability is the degree to which our digital infrastructure is protected from failure. Resilience is the degree to which our digital infrastructure protects critical service to users and is rapidly restored to operation when failures do occur. Canadians expect their digital infrastructure to have sufficient reliability and resilience so that their livelihood, well-being, and security are not threatened by digital infrastructure failures whatever the cause.

While cyber security is an immensely important aspect of resilient digital infrastructure, most of the recommendations from CFDIR do not specifically address cyber security. Cyber security is inherent in some topics – most notably quantum readiness, which is all about proactive responses to an impending cyber threat to digital infrastructure. CFDIR has, to this point, not attempted to comprehensively address the cyber security of digital infrastructure, and defers to the recommendations of Public Safety Canada, CSE/CCCS, and others, who provide leadership on cyber security.

The recommendations in this document were provided by CFDIR's working groups and collated by a CFDIR team, the Canadian Cyber Resilience Working Group. Following a rigorous review and approval process involving all CFDIR members, our recommendations are presented and discussed below under four headings – General Recommendations and the three categories of ISED's Telecommunications Reliability Agenda – robust networks and systems, coordinated planning and preparedness, and strengthening accountability.[iii]

- Robust Networks and Systems (RNS) Recommendations

  These are recommendations that will identify and address the digital infrastructure elements required to support Canadian digital infrastructure resilience. Digital infrastructure resilience depends on the appropriate design and construction of hardware and software systems of the underlying communication, processing, and storage assets. Digital infrastructure resilience can be enhanced to a great degree through a combination of redundancy and diversity in network interconnections, reducing the risk of disruption due to network failure or cyberattack.

- Coordinated Planning and Preparedness (CPP) Recommendations

  These are recommendations that outline how we prepare for and rapidly recover from inevitable failures. Robust Networks and Systems are necessary but not sufficient to ensure digital infrastructure resilience. Twenty-first century digital infrastructure is a complex system of systems with components that rapidly evolve. Moreover, the threats to digital infrastructure are diverse and rapidly evolving. Consequently, digital infrastructure failures are inevitable. Preparing for such events can allow services to recover rapidly despite the failure of parts of the system – a key measure of resilience.

- Strengthening Accountability (SA) Recommendations

  Recommendations of this type relate to reporting or maturity models that allow us to assess how well we are doing and what we ought to share within or between industries and their stakeholders (e.g., users, the general public, government, regulators) to educate others and ensure that our digital infrastructure is resilient and reliable from a full lifecycle perspective.

> Data and reporting are essential if we are to know that networks and systems are robust as well as whether our planning and preparedness is effectively dealing with the threats to our digital infrastructure. Accountability begins with knowing how well that infrastructure is performing, when issues arise, and how failures are addressed in a timely manner.

In some instances, recommendations may span multiple categories. We have endeavoured to group recommendations based on their primary focus without trying to constrain the recommendations as provided by industry.

RECOMMENDATIONS

GENERAL RECOMMENDATIONS

G 1: CABINET POSITION RESPONSIBLE FOR ENSURING GOVERNMENT-WIDE COHERENCE AND ACTION ON CYBER SECURITY POLICY AND TECHNOLOGY GOALS

Today, cyber security responsibilities in the Federal Government are distributed across at least 12 departments and agencies[iv]. Creating coherence across government to ensure that all departments operate with a unity of effort and purpose is essential to fostering digital resilience. These coordinated efforts must span policy and program development, procurement and the use of approval and funding powers to foster and ensure that actions and activities lead to outcomes that are cybersecure and resilient.

Canada's international counterparts have similar bodies that can serve as a frame of reference. For example, the US appointed its first White House National Cyber Director in July 2021 to serve as the President's principal advisor on cyber security[v]; the UK has a Parliamentary Under Secretary of State for Digital and Broadband who is responsible for cyber security and cyber security skills[vi]; and Australia created a standalone cyber minister in June 2022.[vii]

Recommendation: *The minister should ask Cabinet to consider the creation of a Cabinet position, taking the best aspects of each of the above models, would send a strong signal that Canada is serious about cyber security and digital resilience.*

G 2: SKILLS, TALENT AND TRAINING

The Information and Communications Technology Council[viii] and the CD Howe Institute[ix] both report on the digital and technical skill shortage facing the Canadian labour market. The importance of having a digital infrastructure workforce that is both scaled and skilled cannot be overstated.

The availability and ability of that workforce could be improved through actions that address the following:

a) Across career stages: Digital infrastructure skilling is required for current and future students in higher education as well as for those currently in the workforce who require upgrading.

b) Technical, operations, lines of business, legal, human resources, procurement, senior management, board of directors, policy makers: Digital infrastructure skilling or readiness goes far beyond technology and extends across entire organizations as they establish or augment "digital cultures" for their operations. The decreased time to market for innovation creates a digital disruption that extends to the lines-of business, legal, human resources, management, and more. Skilling must occur across the business to ensure organizational alignment.

c) Common curriculum, mainstream: There is currently no standardized curriculum for cloud computing, supply chain, quantum readiness and other digital infrastructure resilience topics across Canadian educational communities. Digital infrastructure curriculum should be standardized across the country, emphasizing security, privacy, and resilience. Furthermore, it should be "mainstreamed" (rather than included only as electives) in Computer Science, Software Engineering, Electrical Engineering, Computer Engineering and similar programs.

d) Immigration and clearances: Given the talent deficit, Canada should improve immigration processes for newcomers with digital infrastructure skills. Since many vacant positions in the digital infrastructure sector require security clearances, the government should streamline and accelerate clearance processes for new Canadians with those skills.

Recommendation: *Government, industry and academia work together on a priority basis to develop and implement an aggressive plan to ensure that Canada has at its disposal the talent pool needed to build, install, upgrade, maintain and protect Canada's digital infrastructure.*

G 3: MAINTAINING AND LEVERAGING CFDIR

CFDIR is a forum for ensuring that resilience is continuously considered, designed, implemented, and maintained in Canada's digital infrastructure. It is a relatively new forum but has already brought together many ICT companies and thought leaders, and its working groups are actively working to improve the resilience of Canada's digital infrastructure. The Government should avoid creating additional groups or forums with a similar mandate and ensure that the role of CFDIR is recognized within all relevant departments.

Recommendation: *ISED should continue its strong support CFDIR and leverage CFDIR work as much as possible.*

ROBUST NETWORKS AND SYSTEMS RECOMMENDATIONS

RNS 1: RESILIENCE REQUIREMENTS FOR BROADBAND FUNDING PROGRAMS

Recommendation i: *All governments should require applicants seeking support from broadband funding programs to demonstrate how their proposed investments in broadband infrastructure would enhance the resilience of broadband networks. This applies to funding programs such as ISED's program Connect to Innovate: Rural and Remote, and programs offered by the CRTC, and the Ministry of Indigenous Affairs.*

Recommendation ii: *The federal government should ensure that regional ISPs have access to transport services to the nearest Internet exchange point (IXP) to increase their resilience. This can be achieved by providing transport directly to critical infrastructure services like Domain Name Servers (DNS) resolution.*

Recommendation iii: *The federal government, for the next round of Universal Broadband Fund applications and any future broadband funding programs should consider how transport to regional ISPs is supported in the funding program; how the resilience of the Internet connection to the regional ISP is achieved; how to ensure that there are no single points of failure in the provisioned Internet access; and how to ensure there is sufficient capacity in terms of Internet transit and transport services.*

RNS 2: INCUMBENT ISPS' TRANSPORT NETWORK LEASING

Many Canadian Internet Service Providers (ISPs) interconnect with only one upstream provider, often physically located far away from the ISP's area of operation. This single interconnection is a potential single point of failure that leaves that ISP vulnerable to outages suffered by their upstream provider. Sometimes the lack of alternative interconnect options is due to the upstream network providers refusing to sell transport connectivity to other providers or to Internet Exchange Points served by other providers.

Recommendation: *The Minister should request that the CRTC initiate a public proceeding to determine the extent of the refusal of some upstream providers (notably large incumbent ISPs) to sell affordable transport to smaller ISPs, and if there are regulatory or other means to remedying the situation.*

RNS 3: IMPROVING PEERING POLICIES FOR BETTER INTERNET RESILIENCY

Major Internet Exchange Points have been established to enable ISPs in Canada to exchange internet traffic (which is referred to as "peering"). However, most of Canada's large incumbent ISPs will not peer openly in existing IXPs, to the detriment of smaller ISPs who may already have established a presence in these IXPs. That is, the incumbent ISPs would rather serve Canadian organizations as customers than directly peer with them at an IXP.

As a result of the efforts of these incumbent ISPs, which carry most of Canada's traffic, to avoid Canadian IXPs, the bulk of Canadian consumer-to-consumer traffic and consumer-to-enterprise traffic is routed by Canada's incumbents via the US (and US IXPs) rather than through Canada. The performance of some services in Canada, such as private web conferencing and the like, is impeded by traffic being routed north-south rather than east-west, meaning that Canadian consumers as well as smaller Canadian ISPs are disadvantaged.

Recommendation: *CFDIR should initiate a conversation with the Canadian Security Telecommunications Advisory Committee (CSTAC) about how to improve the relationship between the Canadian IXPs and incumbent ISPs with the goal of:*

- *Encouraging a more permissive peering policy by those ISPs and a gradual transition to keeping more traffic in Canada.*
- *Peering with any critical infrastructure networks that are present at the IXP so they can rapidly begin to exchange traffic in these IXPs with all IXP members in the event of an outage.*

RNS 4: PRIORITIZING COMPETITION AND DIVERSITY OF FACILITIES PROVIDERS

The continued expansion of telecommunications and cable network facilities enhances the redundancy, and therefore the resilience, of the Canadian Internet. Competition among facilities providers that results in a diverse array of providers building and operating their networks is integral to the redundancy and resilience of Canada's Internet.

Recommendation: *The Canadian Radio-television and Telecommunications Commission and Innovation, Science and Economic Development Canada should continue to support and create favourable conditions for competition among network operators for key Internet facilities, including but not limited to back-haul, transport and last-mile.*

RNS 5: UPSTREAM INTERNET NETWORK PROVIDER BILL OF MATERIALS

Just as a construction company can list the materials and components used to build a structure for the structure's owner, ISPs providing network access in Canada should be required to make available, on demand, a list of their upstream Internet network providers. This would allow Canadian consumers and enterprises to better understand the components that make up their Internet access, to identify and mitigate against potential single point of failure, and to assist in determining their own level of Internet access resilience. This requirement would increase transparency and awareness of the Internet network access dependencies, resulting in improved decision-making and risk management for consumers and enterprises.

Recommendation: *ISPs providing network access in Canada should be required to make available to customers, on demand, a list of their upstream Internet network providers.*

RNS 6: UPDATING INTERNET TRANSIT PROCUREMENT BASED ON 2023 INTERNET STANDARDS

According to APNIC Labs, the Government of Canada does not require certain key standards and protocols for its Internet access deployments. APNIC Labs provides research, measurement, and technical reports on the use of certain key Internet standards and protocols, such as IPv6, DNSSEC and RPKI ROA validation (The Canadian Government operates its networks using autonomous number AS2675):

- https://stats.labs.apnic.net/ipv6/AS2675
- https://stats.labs.apnic.net/dnssec/AS2675
- https://stats.labs.apnic.net/roa/AS2675

Recommendation: *The Government of Canada should review its requirements for Internet transit procurement and ensure that its own networks and those of critical infrastructure providers conform to the most current standards and best practices.*

This review should consider items such as the following:

- Support for full dual-stack IPv4 and IPv6 transit for protocol redundancy.
- That transit capabilities include peering arrangements with relevant Canadian IXPs who have an appropriately permissive peering policy.

  - For example, peering with critical infrastructure providers inside Canada.
  - At a minimum, peering with DNS providers like .CA, .COM, and root servers.

- That Internet service providers:
  - List their upstream Internet network providers to assist in understanding their level of redundancy and resiliency.
  - Have service level agreements covering availability and quality of service for both IPv4 and IPv6 traffic.
  - Adopt best practices, such as MANRS, BCP38 (Network Ingress Filtering), DNSSEC validations, RPKI.
  - Demonstrate commitment to ongoing implementation of key Internet standards, protocols, technologies, and best practices as they advance.

RNS 7: DOCUMENTING THE STATE OF MULTIPLE CONCURRENT INTERNET CONNECTION SOLUTIONS

Stakeholders should work together to develop a guide for multi-homing Internet solutions. A business or even a residence is "multi-homed" when it has concurrent Internet connections from more than one ISP. Multi-homing is a very complicated topic and solutions diverge based on resiliency requirements.

Such a guide could include information on the different types of multi-homing solutions available for different types of users (e.g., home, small business, enterprise), the pros and cons of each solution, and recommendations for choosing the right solution based on individual needs and requirements. Cost is an important factor to include in each of the scenarios. The guide should document the various options available to automate the switchover from the primary to the backup connection to eliminate downtime.

The development of the guide would involve experts in the field, such as network engineers, ISPs, and government representatives, to share their knowledge and experiences. They could also conduct surveys and research to better understand the current state of multi-homing Internet solutions in Canada and identify gaps in knowledge or areas where more information is needed.

Once the guide has been developed, it could be disseminated through various channels, such as online resources, training programs, and workshops, to ensure that individuals and organizations have access to the information they need to make informed decisions about their Internet solutions.

Recommendation: *Industry should create a guide to multi-homing Internet solutions and ensure that it is disseminated.*

RNS 8: ADOPTING INTERNATIONAL STANDARDS AND BEST PRACTICES

Canada lags in the adoption of compliance standards for a number of areas of digital infrastructure, such as cloud services, IoT, supply chain and quantum computing. The federal government's specification of bespoke requirements for suppliers not only adds friction to any service delivery initiative, these Canada-unique requirements add cost and technical debt. Financial services, the energy sector, transportation and other regulated critical infrastructure participants have embraced international standards such as ISO, SSE SOC, Cloud Security Alliance and others to demonstrate sufficiently high levels of assurance for the adoption of these services in their communities.

Recommendation: *The Government of Canada should move to adopt international standards and clearly communicate which standards it supports in procuring cloud services and other digital infrastructure. The Government of Canada should consider existing standards from the US and EU. The Government of Canada should also actively participate in international standards development activities for those standards that are adopted.*

RNS 9: SUPPORTING NATIONAL RESILIENT CONNECTIVITY

Canada's critical infrastructure, including digital infrastructure, has a significant north/south dependency. There are many vital points in Canada where damage arising from environmental or other causes to one location could significantly impact a variety of critical services at a regional or wider scale. Often there is a bias on a particular modality of communication. This may change due to the priorities of the local telecom providers and their infrastructure ambitions.

Recommendation: *The Government of Canada should look to increase geographic route diversity from east to west within Canada for critical digital infrastructure, considering a portfolio of communications media, including fibre, wireless (4G, 5G, Whitespace WiFi) and LEO Satellite to support resilience.*

RNS 10: FINANCIAL INCENTIVES FOR RESILIENCE

Resilience often requires additional investment as failsafe, redundant, duplicative paths and employees are required to ensure continued operation of services under difficult conditions.

Recommendation: *The Government of Canada should consider incentives for organizations to improve their resilience to failures in their primary provider's network.*

RNS 11: DESIGNATING OR CREATING A CRITICAL INFRASTRUCTURE (CI) NETWORK PROVIDER

Many of Canada's CI providers rely upon the public Internet provided by an ISP. In the event of a major Internet disruption at their ISP, a CI provider could fall back to a designated Critical Infrastructure Network Provider to maintain connectivity between CI systems that are key to providing critical services.

Recommendation: *The Government of Canada should evaluate the feasibility and benefits of designating or creating a trusted Critical Infrastructure Network Provider operating such an emergency CI backbone. Designated CI providers must connect to this CI backbone, using a zero-trust architecture.*

RNS 12: INTERDEPENDENCY OF NATIONAL DIGITAL INFRASTRUCTURE SYSTEMS

There is a growing interdependency among the systems comprising Canada's digital infrastructure. It is therefore difficult to understand how our digital infrastructure normally operates, and extremely difficult to anticipate the impact of failures. The issue should not be ignored.

Recommendation: *The Government of Canada, with industry collaboration, should build a comprehensive program to understand and manage the interdependent deployment of the technological systems that make up Canada's digital infrastructure. Such a program should begin with the systems that are relied on by Canada's CI sectors. This program could consider, among other things, the need for post-quantum cryptography-safe (PQC) and quantum-safe technologies and should include meaningful input and support from all of Canada's CI sectors.*

COORDINATED PLANNING AND PREPAREDNESS RECOMMENDATIONS

CPP 1: EXPANDED EMERGENCY PLANNING EXERCISES

Our digital infrastructure is sophisticated and highly interdependent. Expanding emergency planning exercises to include additional stakeholders will better reflect how emergencies affect all of society, and how digital infrastructure intersects with every sector. This will increase resilience in the event of an emergency.

These emergency planning exercises could consider low-likelihood but high-impact "zero-day" failure scenarios to drive a thoughtful assessment of the interconnectedness of many sectors and equip government and industry to better address unexpected but serious failure scenarios. The goal would be to widen the scope from the planning exercises that are already done at an individual business or ISP level, or even the CSTAC level, and include wider industry and other participation.

Recommendation: *CSTAC and CFDIR should jointly develop a plan for conducting emergency planning exercises. This should be coordinated with appropriate programs in the Government of Canada.*

CPP 2: EMERGENCY CONTACTS

One of the challenges of managing during an outage is that some communications channels are likely not available, even to the very technicians dealing with the outage. The CCCS should work with CFDIR to determine who should be included as emergency contacts, the mechanism for ensuring that this information is kept private (e.g. TLP AMBER+STRICT), the obligation for stakeholders (such as network and CI providers) to keep their information up to date, and the mechanism for using the contact information under various digital-infrastructure failure scenarios.

Recommendation: *The CCCS, with input from CFDIR and others, should establish and maintain a list of emergency contacts which includes details for all possible communication channels so that stakeholders can be informed of incidents and coordinate their response.*

CPP 3: ESTABLISHING A CRITICAL INFRASTRUCTURE (CI) RESILIENCE CENTRE

The Government of Canada has no central coordination centre for critical infrastructure resilience. There are many interdependencies that cross federal departmental mandates. As a result, it is difficult to make progress on cross-departmental imperatives to measure and improve the resilience of Canada's digital infrastructure.

Recommendation: *The Government of Canada should establish a CI resilience centre to address the gaps in Canada's CI resilience and work across departmental mandates. The scope of the CI resilience centre should also include cyber resilience and should be tied to the National Infrastructure Assessment.*

CPP 4: SUPPLY CHAIN GOVERNANCE SET

The Government of Canada has an existing model to ensure positive policy outcomes when multiple government entities each apply their own unique mandates, authorities, resources, and programs for supply chain risk management. This model relies on important success factors: 1) whether and to what extent the individual agencies are operating under a unified strategy and vision, with a defined action plan; 2) the extent to which each relevant agency is aware of and able to complement other agencies' activities in a coordinated manner; and 3) the extent to which the coordinating structure enables collaboration with other government and non-government partners.

The whole-of-government alignment is critical for ensuring the disparate agencies of the Government of Canada are aligned in their focus and actions to mitigate digital supply chain risks, and for providing a centralized point of contact for outreach and collaboration with provincial, territorial, municipal governments, critical infrastructure owners and operators and their key suppliers, academia, and international digital supply chain risk management efforts.

Recommendation: *The federal government, through one or more lead departments (SSC, CCCS/CSE, PSPC, ISED, PSC, Transport Canada and/or TBS), should provide appropriate resources to establish a new Government of Canada Supply Chain Centre of Excellence or coordination agency. The Centre (or coordination agency) should be designed to integrate supply chain risk management efforts from across the Government of Canada with those of provinces, municipalities, territories, First Nations organizations, and Canadian industry. This Centre should be tasked with the following:*

1. *Serve as a central and shared knowledge resource for supply chain risk management activities carried out by individual agencies and coordinate cross-government digital supply chain risk management activities.*
2. *Develop a coordinated vision, strategy, and action plan for Canada's digital supply chain risk management activities, including opportunities for enhanced collaboration across federal agencies and engagement with non-governmental stakeholders and guidance to non-government stakeholders on the key activities and points of contact for relevant government agencies.*
3. *Review significant digital supply chain-related incidents (SolarWinds, Log4j) and develop after-action reviews and recommendations, including identification of cyber defence strategies and key technologies that, taken together, could help prevent or mitigate future attacks.*
4. *Work with relevant agencies to review existing government-wide security architectures and technical reference requirements, and update as appropriate to account for critical system defence strategies, practices and technology capabilities that could prevent, mitigate, or lessen the impact of future supply chain attacks or vulnerabilities.*
5. *Distribute supply chain risk management intelligence products from CCCS and other organizations to partners in provinces, municipalities, territories, First Nations organizations, and Canadian industry.*
6. *Identify and/or design potential Government of Canada procurement policy levers that could be applied to encourage the adoption of digital supply chain risk management best practices by ICT suppliers to the government.*
7. *Develop a Canada-specific Supply Chain Risk Management Maturity Model ensure that organizations make resource decisions about their supply chain assurance programs tailored to their risk profile and to encourage knowledge sharing. This may incorporate elements drawn from existing Supply Chain Maturity Models e.g., NIST Cybersecurity Framework, Supply Chain Risk Leadership Council's (SCRLC) Maturity Model.*
8. *Develop additional recommendations for engaging small and medium enterprises, as appropriate.*
9. *Identify critical knowledge of vulnerabilities, determine where additional research and funding is required, and develop new strategies to address existing risks. This organization would integrate and coordinate both public and private sector efforts into an ongoing national supply chain risk management strategy.*
10. *Fund and/or conduct research to test the security of enterprise email, telecom, data centre, workplace technology devices, and services; help identify vulnerabilities and develop mitigation measures; and support efforts to certify the security of critical technologies.*
11. *Develop, in collaboration with industry, a new industry Supply Chain Integrity certification and accreditation program that would assist in both making industry supply chains more resilient and secure, and through certification, provide a competitive advantage by demonstrating to consumers via a certification mark that their products are resilient and secure. Industry testing labs would apply for accreditation to offer this SCI service to industry, which could be based on*

certifying compliance to existing SCI standards, e.g., ISO/IEC 27036[x], ATIS-I-0000090 5G Network Assured Supply Chain.[xi]

CPP 5: DEFENCE STRATEGIES AND TECHNOLOGY CAPABILITY SET

Recommendation: *The Government of Canada should review existing government-wide security architectures and technical reference requirements, and update as appropriate to account for critical system defence strategies, practices and technology capabilities that could prevent, mitigate, or lessen the impact of supply chain attacks or vulnerabilities. Those architectures and reference requirements should be disseminated to industry as models for adoption, to the extent feasible and scalable. Specific actions would include:*

1. *Adopting Zero Trust Architectures;*
2. *Assisting Government of Canada departments and agencies with Implementing Software Assurance and Supply Chain Transparency measures*
    a. *Maintaining a robust supplier inventory that provides a complete view of suppliers' security posture;*
    b. *Establishing a collaborative ecosystem with suppliers of information sharing, risk reduction and remediation, and incident management;*
    c. *Deploying and utilizing Software Bill of Materials (SBOM) as part of an organization's asset management practices, vulnerability management practices, and/or software license management practices;*
    d. *Employing a secure continuous integration/continuous delivery (CI/CD) approach that focuses on integrating security tools early into the engineering lifecycle e.g. static, dynamic, and software composition analysis tools.*
3. *Integrating endpoint detection and response (EDR) technologies with Artificial Intelligence (AI)/Machine Learning (ML)-based monitoring of critical platforms and products to help protect against sophisticated supply chain attacks;*
4. *Utilizing Principles-Based Assurance policies which provide flexible cyber security objective-based guidance to organizations, e.g., European Union General Data Protection Regulation (EU GDPR);*
5. *Maintaining a robust asset and supplier inventory with explicit points of contact to enable immediate, coordinated action to be undertaken during an incident to secure an organization's environment; inform upstream consumers and downstream providers; and request, collaborate on, or enforce remediation/mitigation in the organization' own supply chain;*

6. *Maintaining an accurate, up-to-date inventory of an organization's internet-facing assets and those within their supply chain, to facilitate swifter remediation and incident response;*
7. *Applying widely accepted guidelines or standards for Secure Development Lifecycle (SDLC) Management ex.:*
    a. *NIST SP 800-218 "Secure Software Development Framework";*
    b. *OWASP "Software Component Verification Standard";*
    c. *Cloud Native Computing Foundation "Software Supply Chain Best Practices";*
    d. *Open Source Security Foundation "Supply Chain Levels for Software Artifacts (SLSA)";*
    e. *ISO/IEC 27034 "Application Security"*
8. *Disseminating to industry updated Government of Canada-wide security architectures and technical reference requirements as models for adoption, to the extent feasible and scalable.*

CPP 6: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY AND QUANTUM-SAFE DIGITAL INFRASTRUCTURE

The most common forms of cryptography, that are used in public-key infrastructure, Internet browsing and IoT devices, are also the most vulnerable to quantum-based attack. Much of our critical infrastructure will become vulnerable to hostile actions because of current cryptography. Due to the foundational nature of cryptography, failures will be systemic and devastating, and rapid recovery will likely be impossible.

Determinations regarding security against cyber threats against long-lasting infrastructure elements should take into account the upcoming and future quantum threat to cryptography and thus cybersecurity. Canada must prepare and respond proactively, putting in place measures that will support an orderly transition to cryptographic agility and quantum-resistant cryptography.

To improve the security and reliability of Canada's digital infrastructure, it is important to adopt new technologies that can withstand potential threats from quantum computing. This includes using standardized post-quantum cryptography and quantum-safe products and services that have been tested and proven effective employing internationally recognized certifications and testing methods. By creating a trusted supply chain of these technologies, Canada can protect its critical infrastructure and even export them to allied nations. Each of Canada's critical infrastructure sectors should assess its vulnerabilities and create a plan to mitigate the quantum threat with PQC solutions.

Recommendation: *The Canadian government and critical infrastructure providers should take the following actions, in close alignment with international PQC standardization efforts and recognizing the need for Canadian policies in this area to be in general alignment with those of our principal allies - the US, the EU and the UK:*

1. *Establish a task force or working group to oversee the implementation of PQC and quantum-safe infrastructure. This group should include experts from industry, academia, and federal government agencies to ensure a coordinated approach.*
2. *Work with industry partners to develop and test PQC and quantum-safe products, services, and solutions. This can include funding research and development initiatives, as well as providing incentives for private companies to invest in these technologies.*
3. *Develop a plan to create a trusted supply chain of quantum-safe technologies, including those made in Canada, that can be used domestically and exported to allied nations, confirming to an appropriate standard.*
4. *Conduct a comprehensive risk assessment across all sectors of Canada's critical infrastructure to identify vulnerable systems and prioritize remediation efforts.*
5. *Educate and train federal government officials, industry partners, and the public on the importance of PQC and quantum-safe infrastructure, as well as the potential risks associated with not implementing these solutions.*
6. *Develop policies and regulations that require the use of PQC and quantum-safe infrastructure in critical infrastructure sectors.*
7. *Monitor and evaluate the effectiveness of PQC and quantum-safe infrastructure over time and make adjustments as needed to ensure the ongoing security and reliability of Canada's digital infrastructure.*

All of Canada’s 10 Critical Infrastructure sectors should be active participants in this endeavour, with all CI-sector companies completing a quantum-risk assessment by year end 2024, and preparing a comprehensive remediation plan by year end 2025.

CPP 7: INTERNET OF THINGS SECURITY AND BOTNETS

Large-scale IoT botnets like MIRAI pose a significant threat to critical infrastructure networks. These botnets are made up of compromised IoT devices, such as routers and cameras, that can be remotely controlled by cybercriminals to launch distributed denial of service (DDoS) attacks. These attacks can overload a network with traffic, causing it to slow down or even crash, which can have serious consequences for critical infrastructure sectors such as healthcare, finance, and energy. IoT botnet

attacks can also compromise the security and integrity of data transmitted over these networks, leaving sensitive information vulnerable to theft or manipulation.

The size and complexity of these botnets, combined with the growing number of unsecured IoT devices, make them a particularly challenging threat to address. Without effective measures in place to secure these devices and networks, the risk of large-scale IoT-based botnet DDoS attacks will continue to grow, potentially causing significant harm to critical infrastructure and the economy as a whole.

Recommendation: *The Canadian government and critical infrastructure operators, to mitigate the threat of large-scale IoT botnets like MIRAI, should consider the following actions focused on attacks originating within Canada:*

1. *Increase awareness: The government should increase awareness of the risks associated with IoT devices and botnet attacks through public awareness campaigns and education initiatives. This will help to promote best practices for securing IoT devices and networks.*
2. *Develop regulations: The government should develop regulations that require the use of secure IoT devices and networks in critical infrastructure sectors. This can include requirements for regularly updating firmware, implementing strong access controls, and other security measures.*
3. *Collaborate with industry: The government should collaborate with industry partners to develop best practices and standards for securing IoT devices and networks. This can include working with device manufacturers to ensure that devices are designed with security in mind.*
4. *Invest in research: The government should invest in research to better understand the threat of IoT botnets and develop effective mitigation strategies. This can include funding research initiatives focused on developing new security technologies and techniques.*
5. *Build capacity: The government should build capacity within its own organizations and with critical infrastructure sectors to ensure that they have the skills and knowledge necessary to effectively manage the risks associated with IoT botnets.*
6. *Develop response plans: The government should develop response plans that outline how it will respond to potential IoT-based botnet DDoS attacks on critical infrastructure networks. This can include early detection and mitigation measures to prevent attacks from spreading and causing significant damage.*
7. *Foster international cooperation: The government should foster international cooperation to address the global threat of IoT botnets. This can include working with other countries to develop common standards and best practices for securing IoT devices and networks.*

CPP 8: NATIONAL INDUSTRIAL INTERNET OF THINGS RISK ASSESSMENT

There is very little information on, or an inventory of the quantity and security of connected devices already deployed in the Critical Infrastructure sectors. Many of the current connected devices were deployed with insecure technologies and associated monitoring, support and maintenance. It is believed that many of these devices have out-of-date software and indeed may not even be upgrade-able. These devices likely do not have proper zero trust practices and adequate crypto in place.

Yet, we are actively deploying connected devices across the Canada's CI sectors, including Water, Safety, Health, Finance, Transportation, Energy and Utilities, Food, Manufacturing, Government, and Information and Communication Technology. These devices include sensors, networking gear, SCADA, ICS, smart cities, payments and more.

The number of IoT devices is dramatically increasing, as are CPU and network speeds. They are also leveraging an increasing level of open-source components in their deployment, which can carry additional software supply chain-risk resulting in large scale vulnerabilities.

Best practices dictate that cybersecurity is designed into the architecture, deployment, and operations of these devices. It is believed that there is a low level of cybersecurity prevention, detection and response tools and mechanisms in place today and a thorough risk analysis would help the Canadian government and private sector develop robust and evidence-based policy, standards, procedures and guidelines to better protect Canadian IoT infrastructure across CI sectors. As part of this exercise, it would be important to look across the IT and associated operational technologies (OT) to understand the vulnerabilities of these systems.

Recommendation: *The Government of Canada should perform a national industrial Internet of Things Risk Assessment, across all Canadian Critical Infrastructure sectors, within 2 years, to help identify the key risks of IoT across the CI sectors.*

The completed risk assessment will then help enable, as a next step, the identification and implementation of risk-mitigation strategies and measures, to help reduce threats for the key industrial IoT risk areas identified. Part of the emerging best practices should include the sharing of best practices and outstanding threat intelligence to enhance resilience in the areas with high-risk / high-impact vulnerabilities.

STRENGTHENING ACCOUNTABILITY RECOMMENDATIONS

SA 1: COORDINATING ACTION BETWEEN CSTAC AND CFDIR

The Internet in Canada is more than ISPs. It also includes the mission-critical digital infrastructure elements such as the Domain Name Servers, content providers, enterprise networks, hyperscale service providers, cloud service providers, and much more. The Canadian Security Telecommunications Advisory Committee has already provided recommendations to the Minister to improve Canadian digital infrastructure resilience. CFDIR is providing its recommendations in this document.

Recommendation: *The chairs of CFDIR and CSTAC should meet to discuss areas where it would be beneficial to collaborate on actions taken based on the two sets of recommendations to the Minister.*

SA 2: UPDATING THE INDUSTRIAL SECURITY PROGRAM REQUIREMENTS FOR IT PROVIDERS

Recommendation: *The government should modernize the Industrial Security Program run by Public Services and Procurement Canada in recognition of the security, privacy and resilience controls employed in the delivery of cloud services.*

SA 3: MODERNIZING UNDERSTANDING OF CYBER SAFEGUARDS

While the cyber security threat actors have advanced in their approaches to exploiting corporate networks, many enterprises have failed to implement the fundamental security controls espoused for over 40 years. Federal government and private sector procurements continue to use requirements that are aligned with decades old approaches to IT services delivery. Clearly a different approach needs to be taken beyond the hundreds of pages of controls along with the associated compliance and audit regimes.

Recommendation: *The Government of Canada should review the existing cyber resilience and IT security guidance for outdated approaches and revise with modern principles to address today's threat and resilience needs.*

CLOSING THOUGHTS

CFDIR remains focused on activities to improve the resilience of Canada's digital infrastructure and is pleased to offer these CFDIR Industry representatives' recommendations to the Minister of Innovation, Science and Industry. The technologies, architectures, infrastructures, products and services and solutions, vertical markets and business models and processes represented within CFDIR members are extremely diverse. This diversity reflects the depth and breadth of Canada's digital infrastructure.

In the short time since its creation in early 2020, CFDIR has brought together many ICT companies and thought leaders. CFDIR working groups have made meaningful contributions to efforts to identify and understand the gaps and weaknesses that must be addressed to increase the resilience of Canada's digital infrastructure. ISED is encouraged to continue their first-rate and much appreciated support for this forum.

The digital infrastructure technology and risk landscape is highly dynamic. CFDIR is exploring setting up two new working groups: one that could focus on Artificial Intelligence/Machine Learning, and a separate one that could coordinate the ICT sector's response to cyber threats and events. CFDIR will also consider whether and how to continue the Canadian Cyber Resilience Working Group beyond its May 1st, 2023 mandate. We anticipate that this working group activity will bring further insight to the topic of Canadian digital infrastructure resilience.

CFDIR will continue to work on the most pressing challenges facing Canada's digital infrastructure resilience. There are many *horizontal* technology domains beyond those currently addressed by CFDIR working groups, such as artificial intelligence or secure software development. There are also technologies that are more specific to *vertical* markets, such as connected vehicles and transportation. These topics may be addressed by CFDIR working groups in the future. For now, we are prepared to discuss any of our current recommendations to assist in understanding and implementation.

CFDIR would like to thank the Minister of Innovation, Science and Industry for this opportunity to provide recommendations to improve Canada's digital infrastructure resilience and we look forward to working with the Minister's team on actions and follow-up from these recommendations.

ACRONYMS AND ABBREVIATIONS

4G	Fourth Generation (Cellular Wireless)
5G	Fifth Generation (Cellular Wireless)
AI/ML	Artificial Intelligence/Machine Learning
APNIC Labs	Asia Pacific Network Information Centre Labs
BOTNET	roBOT NETwork (attack)
CFDIR	Canadian Forum for Digital Infrastructure Resilience
CI	Critical Infrastructure
CI/CD	Continuous Integration/Continuous Delivery (software development process)
CPP	Coordinated Planning and Preparedness
CRTC	Canadian Radio-television and Telecommunications Commission
CSTAC	Canadian Security Telecommunications Advisory Committee
DDOS	Distributed Denial of Service (attack)
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EDR	Endpoint Detection and Response
ICS	Industrial Control System
ICT	Information and Communication Technology (sector)
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ISP	Internet Service Provider
IXP	Internet eXchange Point
LEO	Low Earth Orbit (Satellite)
MANRS	Mutually Agreed Norms for Routing Security
MIRAI	Japanese word for "future" (botnet)
OT	Operational Technology
PQC	Post-Quantum Cryptography
RNS	Robust Networks and Systems
ROA	Route Origin Authorization
RPKI	Resource Public Key Infrastructure

SA	Strengthening Accountability
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition (industrial control)
SCRLC	Supply Chain Risk Leadership Council's (maturity model)
SDLC	Secure Development Lifecycle
SSE SOC	Security Service Edge

[i] https://ised-isde.canada.ca/site/mobile-plans/en/minister-champagnes-letter-canadian-forum-digital-infrastructure-resilience

[ii] Global News, Rogers Outage July 8, https://globalnews.ca/tag/rogers-outage-july-8-2022/

[iii] Innovation, Science and Economic Development Canada, (September 7, 2022), A Telecommunications Reliability Agenda, https://ised-isde.canada.ca/site/mobile-plans/en/telecommunications-reliability-agenda

[iv] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx

[v] https://thehill.com/policy/cybersecurity/562601-chris-inglis-formally-sworn-in-as-national-cyber-director/

[vi] https://www.gov.uk/government/ministers /parliamentary-under-secretary-of-state--109

[vii] https://www.arnnet.com.au/article/698646/labor-creates-standalone-cyber-minister-new-cabinet-line-up/

[viii] Paul Stasny, (August 26, 2021), ICTC Labour Market Outlook: Additional Demand for Digital Talent to Reach 250,000 By 2025, Information and Communications Technology Council, https://www.ictc-ctic.ca/news-events/ictc-labour-market-outlook-additional-demand-for-digital-talent-to-reach-250000-by-2025

[ix] CD Howe Institute, (August 23, 2022), *The Knowledge Gap: Canada Faces a Shortage in Digital and STEM Skills,* https://www.cdhowe.org/public-policy-research/knowledge-gap-canada-faces-shortage-digital-and-stem-skills-0

[x] https://www.iso.org/ standard/82905.html

[xi] https://access.atis.org/apps/group_public/download.php/66150/ATIS-I-0000090.pdf