Public Safety Canada | Sécurité publique Canada

Canada

Building a **safe** and **resilient Canada**

Renewing Canada's Approach to Critical Infrastructure Resilience

What We Heard Report

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rnwng-cnd-pprch-crtcl-nfrstrctr-rslnc-2022/index-en.aspx

This report provides a summary of the engagement approach, the issues, and considerations heard throughout the Government of Canada's public consultations to help inform the renewal of the National Strategy for Critical Infrastructure.

Aussi disponible en français sous le titre : Renouveler l'approche du Canada envers la résilience des infrastructures essentielles : Ce que nous avons entendu — Rapport

Public Safety Canada, Communications
269 Laurier Ave West
Ottawa ON K1A 0P8
Canada

communications@ps-sp.gc.ca

Contents

Executive Summary

Since the fall of 2021, Public Safety Canada (PS) has engaged with the broader critical infrastructure (CI) community on the renewal of the 2009 *National Strategy for Critical Infrastructure* (National Strategy). Insights gathered from meetings with public and private stakeholders, online targeted consultation, and email submissions are being used to inform the development of a forward-looking vision for CI resilience.

This What We Heard Report provides a review of the key themes that emerged from engagement over the past year.

Critical Infrastructure Fundamentals

We heard that the essence of CI is adequately captured in the current definition outlined in the National Strategy, however, some respondents suggested including references to interdependencies and supply chains to the definition of CI. The majority of respondents agreed that the current ten sector configuration covers the full breadth of Canada's vital assets and systems. Others proposed that the addition of the Space and Defence sectors, among others, would be warranted to meet the changing threat landscape.

Identified Gaps in existing National Strategy Objectives

Partnership Building: We heard that partnerships could be expanded to involve municipalities and Indigenous communities in CI fora. Stronger cross-sector partnerships were top-of-mind for respondents, as was ensuring that mechanisms are in place for ongoing public-private dialogue.

All-Hazard Risk-Management: Participants described the complexity around obtaining guidance from various levels of government. They identified the need for increased coordination, coherence, and linkages across jurisdictions, as well as the need to develop a method for identifying vital CI. Key functions were proposed for government, including the establishment of data registries that could be used to identify threats and support all-hazard risk management practices.

Information Sharing: There was general consensus that the public and broader infrastructure community should be included in information sharing on risks. In addition, stakeholders voiced the desire to not only be recipients of information, but to inform the

government of the threats that they encounter. They pointed to a range of supports needed for resiliency, including the creation of a National CI Centre to act as a focal point for coordination.

Proposals for a new National Strategy Objective

Given the increasingly complex landscape of emerging threats and the interdependent nature of CI operations, respondents underscored the need to clarify and formalize CI roles, responsibilities and accountabilities. We heard that the establishment of legal obligations for designated CI could help promote accountability and enhance CI protection. Participants also underlined the government's role in providing support to CI (e.g., guidance, funding mechanisms, liability protection) to help meet any potential new requirements.

Context

Canada's National Strategy for Critical Infrastructure[1] (National Strategy) was published in 2009, and was endorsed by Federal, Provincial and Territorial Ministers responsible for emergency management. The purpose of the National Strategy is to strengthen the resiliency of critical infrastructure (CI) in Canada. It establishes a framework for cooperation in which governments and owners and operators can work together to prevent, mitigate, prepare for, respond to, and recover from CI disruptions and thereby safeguard the foundations of our country and way of life.

As part of a commitment set out in the National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure[2], Public Safety Canada (PS) undertook an examination of the National Strategy. This examination found the strategy was outdated and should be renewed in collaboration with the private sector, provinces and territories, federal partners, and other stakeholders.

The National Strategy renewal is an opportunity to shed light on what is going well, what needs to be improved, and what our vision for the future of CI resilience should be.

Engagement Overview

To ensure the representation of viewpoints from its broad base of critical infrastructure stakeholders, three approaches were used to gather input: an online targeted consultation, meetings and presentations to public and private stakeholders, and email submissions.

Online targeted consultation - LetsTalkCriticalInfrastructure.ca

April 21, 2022 – June 1, 2022

Over 2,800 CI stakeholders, including federal, provincial, territorial and municipal (FPTM) government officials, CI owners and operators, and academia were invited to

---

[1] Public Safety Canada. *Canada's 2009 National Strategy for Critical Infrastructure.* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

[2] Public Safety Canada. *National Cross Sector Forum 2018-2020 Action Plan for Critical Infrastructure.* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr-2018-20/index-en.aspx

participate and share the link to the online consultation throughout their networks. In addition, the link was posted on the PS website and on Consulting with Canadians. Feedback was sought on issues such as: modernizing the definition of CI; prioritizing the most vital CI; and supporting risk management for complex and changing threats.

The online engagement received 120 survey responses and 9 ideas on the virtual discussion board. Based on registration information collected from the 120 respondents, 41 were from the public sector; 76 were from the private sector; and 3 were unspecified. Participants consisted of policy makers, owner-operators, industry associations, academia and more. Regional representation was diverse, with most of participants located in Ontario.

Respondents who identified as being part of the Government, Information and Communication Technology, Energy and Utilities, and Transportation sectors, made up 79% of survey submissions.

Meetings and presentations to public and private sector stakeholders

Feedback was also received through presentations and discussions at over 40 stakeholder groups and forums, including federal government committees, CI sector networks, and with individual owners and operators. Meetings with public and private sector stakeholders provided the broader CI community opportunities to offer immediate input and feedback. These meetings also allowed PS to leverage existing relationships while including stakeholders who are not directly represented under the current strategy. Additionally, PS engaged in discussions with international partners, such as members of the Five Eyes Alliance, and European Union members.

Email submissions

Members of the CI community were also invited to send their viewpoints and questions to the CI Consultations inbox (ps.cci-cie.sp@ps-sp.gc.ca). Ten emailed submissions were received which included collective input from large organizations.

What We Heard

Critical Infrastructure Fundamentals

Definition

> "The current definition could be enhanced by incorporating that how Canadians perceive critical infrastructure is a reflection of Canadian values and interests, and fosters strength in Canada's social fabric [...] Exemplifying the interdependencies would also strengthen the definition."
>
> - Participant, Online Engagement

The 2009 National Strategy defines CI as the "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence."

When asked whether the current definition of CI adequately captures the essence of CI, most survey respondents (70%) indicated that it did.

Some respondents recommended adding interdependencies to the definition. These suggestions were most often made in reference to considering supply chains, cyber/digital systems, and the natural environment. Respondents who indicated the need to include digital systems noted the value of protecting data and information, and the importance of considering procurement security for hardware and software. Those who suggested including supply chains referenced recent and ongoing issues with global supply chains that inhibit the flow of goods, as well as the importance of considering sub-contractors and vendors that provide services to CI.

Finally, we heard that the definition could be enhanced by including the notion of risk or impact. For example, respondents noted that disruptions to CI can cause significant negative impacts on the environment and Canadians.

Sector Configuration

The 2009 National Strategy for Critical Infrastructure identified ten sectors as listed below:

- Energy and Utilities
- Finance
- Food
- Government
- Health
- Information and Communications Technology (ICT)
- Manufacturing
- Safety
- Transportation
- Water

The definition and associated list of ten sectors provide a nationally agreed upon understanding of CI and form the basis for CI engagement with the federal government. Though the ten sectors may not capture the full range of Canada's CI, most respondents felt that they adequately represented the breadth of CI in Canada. However, we heard that clarity is needed to determine the assets and systems that are included under each of the sectors.

Respondents were asked to select, among several suggested new sectors, which could be considered CI, and to propose other CI sectors.

Space: Space received the most support for recognition as a distinct sector due to the essential role that space infrastructure plays in underpinning all other forms of CI and environmental monitoring. Currently, space infrastructure, like the telecommunications satellites that link Canadians from coast to coast, is considered part of the Information and Technology Communications (ICT) sector. However, space assets, systems and technology perform additional functions. Perhaps the most familiar space service is the Global Positioning System (GPS), a global navigation satellite system that broadcasts position, timing and navigation data to Canadians. Some respondents pointed to the critical services provided by space infrastructure, such as enabling navigation to northern communities with ice mapping and crop monitoring for precision agriculture. It

was noted that space assets also support scientific research, such as the study of space weather.

> "Canada is dependent on space systems for a wide range of critical daily activities. Space connects Canadians from coast-to-coast, enables and promotes routine business activities and the exchange of goods, services and information around the world, and supports national security and safety."
>
> - Participant, Online Engagement

Defence and Security: Although it was not one of the answer choices, several respondents argued in favour of creating a distinct Defence and Security sector to reflect the importance of national defence and security to Canada's safety and prosperity. As it is, defence and security falls as a subsector of Government sector and the Manufacturing sector encompasses the defence industrial base.

Community Infrastructure: Those who perceived community infrastructure as a CI sector argued that community infrastructure provides a variety of essential services, such as public health, education (daycares and schools), housing, and public works (particularly public facilities and human resources). These essential services play an important role in fostering individual and collective resilience, which enhance the resilience of the overall community. For Indigenous communities, this can include Healing and Elder Centres. The inclusion of Indigenous Priority Infrastructure as its own distinct sector was also proposed.

Academia and Research: Respondents noted academia and research's dual purpose of: (1) higher learning and research institutes, which produce intellectual property and are subject to insider threats and (2) key institutions for the production of emerging technologies (e.g., quantum, clean tech, Internet of Things, synthetic biology), which do not always fit neatly within existing CI sectors, and need to be managed, protected, and secured.

Democratic Institutions: Respondents in the affirmative selected democratic institutions in part by noting the impact of protests and other threats such as misinformation and malicious cyber activity. We heard that democratic institutions are important in maintaining the continuity of government services and avoiding social unrest. Lastly, some respondents wondered about the interplay between democratic institutions and the existing Government sector, questioning if democratic institutions are a sub-sector of the Government Sector, or vice-versa.

Natural Infrastructure: Supporters of adding a Natural Infrastructure sector argued that it is highly interdependent with all other sectors and is critical for human health and survival. In addition, natural infrastructure has multiple critical functions, such as providing core municipal and ecosystem services that protect against the impacts of climate change and extreme weather events.

Objectives of the National Strategy for Critical Infrastructure

> "Adopting a whole-of-government approach to critical infrastructure resilience; information-sharing platforms with critical infrastructure operators builds a trust for a comprehensive and shared understanding of risks and vulnerabilities; co-ordinate national policy tools, to encourage CI industries to invest and achieve in resilience objectives. This way the government is able to support and prioritize resources to protect and restore the most vital CI. Establishing standards and regulations for vital CI would enhance the overall resilience of Canada's CI."
>
> - Participant, Online Engagement

The 2009 National Strategy for Critical Infrastructure was based upon three objectives:

- Building partnerships;
- Implementing an all-hazards risk management approach; and
- Advancing the timely sharing and protection of information among partners.

Some respondents noted the importance of periodic review of the objectives of the National Strategy, given the ever-evolving context in which Canadian CI operates. Additionally, some suggested monitoring and evaluation in order to measure the effectiveness of actions taken to increase the resilience of CI. We also asked respondents whether or not the current objectives of the National Strategy are still relevant. On this question, results were split, with 56% of survey respondents saying that the objectives could remain unchanged.

The next section outlines views and feedback received from respondents on the existing objectives and how these could be improved. In turn, this input was categorized into different gap areas, for each objective as well as for the National Strategy as whole.

Identified Gaps for Objective 1: Building Partnerships

I. Broad Partnerships

> "Provinces and Municipalities need to be engaged on the specific CI that operate in their sphere of influence."
>
> - Participant, Online Engagement

We heard that partnerships could be established for many non-traditional partners, such as municipalities. Furthermore, we heard that the federal government could strengthen the existing sector networks, acting as a coordinator for sectoral and industry-specific risk analysis.

Municipalities were repeatedly identified as lacking representation in the current CI sector configuration and engagement structures. Respondents noted that disruptions to CI – including cascading impacts – can be felt at the community level. Therefore, measures that enhance CI resilience also directly enhance community resilience. Many respondents argued that municipalities need more support, as they often lack the financial means and ability to undertake interdependency analysis. Some respondents felt that other non-traditional CI partners, such as academia and Indigenous communities, could benefit from participating in partnership mechanisms for information sharing and awareness building and to support the undertaking of resilience enhancing activities.

II. Cross-Sector Collaboration

> “Effective risk management depends on the critical infrastructure community’s ability to engage across sectors to facilitate a shared understanding of risk and integrate a wide range of activities to manage risk [and] capture […] associated dependencies that may have cascading impacts within and across sectors.”
>
> - Participant, Online Engagement

Respondents highlighted the need for collaboration across CI Sectors and interdependency analysis. It was noted that cross-sector collaboration will help mitigate vulnerabilities in areas such as: human resources, Information Communication Technology, supply chains, the environment, and cyber systems.

Recent events, such as blockades in Ottawa and Canada-U.S. border crossings and the COVID-19 pandemic, featured prominently in stakeholder survey responses on the challenges related to CI interdependencies. Many respondents agreed the federal government could play an important role in working collaboratively with CI sectors to help improve understanding of their interdependencies ahead of an event.

We also heard that the federal government should continue to coordinate cross-sector and public-private partnerships. Some respondents encouraged the federal government to leverage its existing relationships with international allies to foster international collaboration among stakeholders.

We heard that identifying and communicating CI needs with government and other stakeholders is important for partnership building. Suggestions included:

- Enhanced partnerships across different levels of government and private industry sectors;
- Establishment of themed cross-sector working groups or forums;
- Establishment of trusted fora of key CI operators to openly discuss activities and needs outside of commercial competitive/proprietary interest;
- Establishment of clear roles and responsibilities by sector;
- Organisation of cross-sectoral meetings for specific regions;
- Fostering uptake of stakeholder-led interdependency studies; and
- Implementation of cross-sectoral exercises.

Identified Gaps for Objective 2: All-Hazard Risk Management

I. National Criticality Methodology

> "Any methodology must be adaptable to the changing needs of society. One consideration that should be integrated is the ability of CI to deal with successive or overlapping disruptions"
>
> - Participant, Online Engagement

At the community level, infrastructure can play multiple roles depending on whether there is a state of emergency. Some infrastructure could become more or less critical under specific conditions. This varying state can be described as dynamic criticality. To

support the dynamic nature of CI, various approaches were proposed by stakeholders during the consultation.

Some respondents noted that the government could take a tiered approach to CI sectors, in which highly interdependent CI sectors would be considered Tier 1, such as Energy and ICT, whereas other, less critical sectors could be Tier 2 or 3. Examples of less critical sectors included in these comments were national monuments, commercial facilities, and academia/research.

The majority of respondents (84%) thought that criteria should be developed to identify and prioritize the most vital CI sectors, organizations, and/or assets. We heard that clarity in prioritizing the order of recovery of CI in emergencies was needed. Suggestions of ways for developing a criticality methodology included: using matrix scoring grids (measuring likelihood and severity) and by type of community (large, small, remote, urban), at the provincial territorial level and federally. It was also suggested by many to use a dynamic risk-based approach, considering the following factors/metrics:

- Interruptions that cause mass casualties, sickness, injuries, or evacuations
- Population affected and community demographics
- Geography (including risk to remote, isolated locations, proximity to natural hazards)
- Potential economic damage, market maturity and dependence on foreign entities
- Single points of failure and availability of alternatives
- Scope and nature of inter-dependencies
- Lead times for replacing damaged/ageing infrastructure
- Legal impacts
- Reputation, morale, culture

Respondents also mentioned the need for coherence in what constitutes CI across provincial and territorial borders, since many CI services span across jurisdictions in Canada.

II. Evidence Based Risk Management

> "[There is need for] standard industry communication and reporting systems for use across the various sector to identify potential risks, threats and to report incidents. These systems could be managed/accessed by industry and public safety

> organizations to interact, communicate (disseminate information) and mine for information/data."
>
> - Participant, Online Engagement

Respondents emphasised the need for all-hazards risk management to be evidence-based, and for governments to engage in risk foresight analysis in order to offer proactive support to CI on emerging risks.

The establishment of registries, to be maintained by PS, using data from obligatory CI reporting (e.g., incident, business continuity plans, response and recovery plans, ownership, and cyber practices), and voluntary reporting by other CI, was suggested. These registries could be analysed to identify threats, share timely information, and guide CI owners and operators.

We heard that a progressively more complex landscape of emerging threats, combined with the increasingly interdependent nature of CI operations, warrant more support from the federal government. The increasing probability of overlapping risks (i.e., more than one events occurring simultaneously) also featured prominently in survey responses.

Specifically, many respondents voiced the need for assistance in understanding existing and emerging risks to their activities. Some signalled a desire for the government to engage in more all-hazards risk assessments and analysis, and share the results of these analyses in a timely fashion. This risk analysis could include actionable information to guide their institution's response. Respondents listed the following risks as needing more investigation:

- Cyber risks, including hardware and software procurement risks, malicious cyber activities, and cyber-physical risks;
- Emerging risks, such as pandemics, climate change and extreme weather events, and protests; and,
- Risks specific to interdependencies, such as the risk of cascading impacts, risks to Information and Communication Technology (ICT) networks, supply chains, cyber systems, and risks to the natural environment.

Identified Gaps for Objective 3: Information Sharing

I. Community Awareness

> "There also should be a public facing […] component so that Canadians understand the importance of CI and its interdependencies"
>
> - Participant, Online Engagement

We heard that educating and spreading awareness to the broader CI community and to the public is important. Ideas included community risk education campaigns and public information campaigns, to provide the general public with guidance and information on various threats (for example, malicious cyber activity in the context of international conflicts or global pandemics).

Another suggestion was the creation of a public repository of information that would be accessible to the broader CI community and the general public. Information shared through this medium could include guidance on threats and vulnerabilities, declassified risk information (potentially pulled from CI risk and incident reports), best practices developed by larger CI entities, and guidance to communities on identifying CI. It was proposed that information sharing should be multi-directional, as opposed to being a government service to stakeholders. CI stakeholders wish to be involved in decision-making through dedicated timely and actionable information sharing mechanisms.

II. Support Tools

> "Develop, in partnership with ten CI Sector Leads and the private sector ([for] financing and subject matter expertise), dedicated knowledge centres for high-risk areas and emerging issues. This can be done in partnership with academic institutions as well as private sector professional services organizations so [as not to] limit industry service providers the ability to be competitive."
>
> - Participant, Online Engagement

Respondents noted that government support is crucial for their resilience. When asked about the types of support that they require, respondents made a variety of suggestions, including financial supports, information sharing, and issue management.

In terms of support to CI based on risks, respondents expressed the need for the following types of support:

- Capability development: education and training; exercises
- Guidance Documents: roles and responsibilities by sector; guidance by sector; evidence-based guidance documents (e.g., on specific threats); and guidance on emerging risks
- Assessments: impact; resilience; and capability assessments
- Tools: best practices registry; modelling tools; and risk registry
- Training or funding for specialized workforces (e.g., cybersecurity experts)

III. Coordination

> "[There is a] lack of concentration of responsibilities, information and authority given the span of industries, jurisdictions and unofficial bodies. CISA is a good example where authority is concentrated, responsibility clear, and information sharing (within government and to the public) seems to be occurring at a much more rapid pace, of high quality, and effectively disseminated in real time to organizations who need it... This may be a model to consider."
>
> - Participant, Online Engagement

We heard that joint leadership is needed to better coordinate guidance, issue and incident management. Clarity and coherence on the roles and responsibilities of CI actors across jurisdictions is also necessary.

Specifically, some respondents made the case for an authoritative centralized agency or national CI centre that would act as a one-stop-shop for CI support and coordination. Respondents noted the need for such a centre to coordinate CI activities by:

- Acting as a hub for CI capability support (e.g., education and training, guidance, exercises, assessments, and lessons learned);
- Coordinating issue management through timely and actionable information sharing, FPTMI (Federal, Provincial, Territorial, Municipal and Indigenous) Stakeholder coordination, and Sectoral/Lead Federal Department coordination;
- Helping collaborate among CI stakeholders and subject matter experts in academia and other specialized workforces;
- Providing a harmonized view of the multi-jurisdictional CI incentives landscape;
- Providing coherent support for designated CI;
- Having advanced data analytics capabilities; and

- Providing emergency management support for CI (timely support, incident response, prioritization, emergency management training, response and recovery management) and coordinate emergency response for CI across jurisdictions.

Identified Gap from 2009 Objectives: Critical Infrastructure Protection

I. Identification and Protection

> "To maintain a resilient infrastructure of lifelines that interconnect other critical services, yes - vital CI should be designated, with standards and governance to help ensure that appropriate protection, response and recovery plans are in place."
>
> - Participant, Online Engagement

The overwhelming majority of survey respondents (85%) agreed that the most vital CI should be designated and have required to meet certain obligations. In this context, "designation" refers to the formal identification of CI entities and/or assets for the purposes of providing oversight and support.

We heard that regulations would help to provide a benchmarked standard of service in the CI system, thereby enhancing the resilience of the CI system as a whole. Many noted that set baseline levels of protection would provide their organizations with trust in their upstream dependencies, consequently enabling them to adjust their business continuity, response, and recovery plans. Respondents also noted the important role that government could play in establishing robust standards and governance to help ensure that obligations are met, and that appropriate protection, response, and recovery plans are in place.

As was exemplified earlier when discussing a national criticality methodology, respondents again proposed a mix of factors for identifying vital CI, including the infrastructure's importance to life and health, national security (or the impact of its failure on national security), and the presence of single points of failure (e.g., the one access road to a remote community).

Furthermore, many said that highly interdependent systems should be formally designated and regulated, given their potential to cause cascading failures across other CI and have harmful impacts on communities and Canadian society. These respondents identified the Transportation, Energy and Utilities, and Information and

Communication Technology sectors for this purpose. In addition, cyber systems and space infrastructure were noted as having the same high level of interdependencies with other CI sectors, therefore also potentially requiring regulation to protect the overall CI system.

II. Obligations and Reporting

> "Accountability includes ownership, practices, privacy, self-monitoring, reporting and oversight."
>
> - Participant, Online Engagement

We heard that creating a national regulatory framework for CI would increase the overall resilience of the system, thereby enhancing safety and trust. Some cautioned coherence with existing regulatory bodies and jurisdictions, in order to avoid an overly cumbersome regulatory environment and redundant reporting burden.

Some obligations suggested by respondents include:

- Mandatory standards and service standards
- International (ISO) standards
- Reporting on incidents
- Cyber practices
- Participation in exercises
- Response and recovery plans
- Business continuity plans
- Providing ownership information

A few respondents also recommended the mandatory reporting of IP addresses and geolocation information for the explicit purpose of facilitating timely emergency response.

If the most vital CI were to be designated, respondents suggested that the government leverage existing best practices reported by CI stakeholders to help to build consensus on approach, responsibility, and end state, thereby enabling smaller and non-designated CI to meet the standards established by larger more mature CI.

While many respondents agreed that reporting is an important part of a regulatory framework, many cautioned on the importance of ensuring that data is secured. They

recommended that any information shared to the broader public should be scrubbed of identifying and proprietary information, or that these data should be aggregated.

III. Incentives

> "Financial support is needed to assist in the transition to a regulatory framework. Support can be direct or indirect. Direct support may include assistance in staffing, systems integration, monitoring equipment, disaster planning, etc. Indirect support will establish new college and university curricula focusing on CI and the impact on society."
>
> - Participant, Online Engagement

When asked about the types of incentives that vital CI should receive to help offset the impact of mandatory requirements, respondents suggested grants, interest-free loans, cost-sharing, tax incentives, funding for regulatory compliance, and regulatory concessions.

In addition, respondents noted that liability protection would be necessary for those CI that would be subject to any reporting obligations. Other suggestions included public recognition of the owner/operator for its compliance, and preferential ability to bid on government contracts.

Some respondents also listed government supports that could help them achieve regulatory compliance. These included guidance on standards and obligations, emergency management planning assistance, support with obtaining the assistance of specialized skills (e.g., financial support for hiring cybersecurity experts), and training.

Lastly, a few respondents noted the occasional need for penalties in response to regulatory non-compliance. These included fines, the loss of tax breaks, and restrictions on the owner and operator's ability to bid on government contracts.

Glossary

All-Hazards Risk Management: the process of identifying, analyzing and evaluating risks using an all-hazards approach. An all-hazards approach takes into account all types of hazards, whether accidental, intentional or natural.

Assets: refers to a property or a resource such as a building, equipment, a facility, intellectual property, documents or data of value to the owner. A bridge, hospital patient data, facility operating manuals, a hydro dam, a municipal vehicle and a pipeline are examples of CI assets.

Climate Change: a long-term shift in the average weather conditions of a region, such as its typical temperature, rainfall, and windiness. Climate change means that the range of conditions expected in many regions will change over the coming decades. There will also be changes in extreme conditions.

Community Infrastructure: includes the structures, places and organizations that support the lives and well-being of residents in a community. Local parks, libraries and homeless shelters are examples of community infrastructure.

Critical: to have a decisive or crucial importance in the success, failure, or existence of something. Criticality exists on a spectrum with some infrastructure being more critical or important than others. The criticality of an infrastructure refers to its relative importance in terms of the consequences that its failure would have on the population and its vital resources.

Critical Infrastructure (CI): refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. CI includes both physical and digital infrastructure. Physical infrastructure refers to the built environment, including buildings, vehicles, computer hardware and other assets. Digital infrastructure refers to electronic systems and assets, like data and software.

Cross-sector: refers to more than one sector, and typically to all ten CI sectors in Canada. For instance, the National Cross Sector Forum is a cross-sector forum with representation from all ten CI sectors.

Cybersecurity: refers to the protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cybersecurity includes the body of technologies, processes, practices, responses and mitigation measures designed to protect networks, computers, programs and data from damage or unauthorized access so as to ensure confidentiality, integrity and availability.

Democratic Institutions: refers to the rules, organizations, processes and systems that underpin an accountable government of elected representatives.

Designation: refers to the identification of critical infrastructure assets or entities, based on different approaches such as risk analysis, criticality assessment and applying cross-cutting and sectoral criteria. Designation can serve different purposes, such as implementing regulatory obligations for CI protection, or developing an inventory to support risk management and incident response.

Emergency: a present or imminent event that requires prompt coordination of actions concerning persons or property to protect the health, safety or welfare of people, or to limit damage to property or the environment.

Emergency Management (EM): the management of emergencies concerning all-hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery.

Global Navigation Satellite System (GNSS): a constellation of satellites providing positioning, navigation and timing services. Global Positioning System (GPS) is an example of a GNSS.

Governance: refers to a system through which decisions are made pertaining to the operation of an organization. A system of governance decides how objectives are set and achieved, how risk is monitored and addressed, and how performance is optimized.

Hazard: refers to a potentially damaging physical event, phenomenon or human activity that may cause the loss of life or injury, property damage, social and economic disruption or environmental degradation. A hazard can be natural, intentional or accidental.

Impact Assessment: a planning and decision-making tool used to assess the potential positive and negative effects of proposed projects. Impact assessments consider a wide range of factors and propose measures to mitigate projects' adverse effects. They also consider components of follow-up programs (for projects that are allowed to proceed), which verify the accuracy of an impact assessment and the effectiveness of mitigation measures.

Interdependency: refers to two or more things, assets, systems or people relying on one another. There are interdependencies within and across CI sectors, meaning that sectors rely on each other to deliver the goods and services essential to Canadians. The interdependent nature of CI sectors means that a failure in one sector has the ability to impact other sectors.

Lead Federal Department: federal department or agency that supports information sharing and collaboration within a CI sector.

Multi-Sector Network: a forum that brings together working-level representatives from each of the ten CI sectors to discuss topics related to CI resilience. These annual meetings provide a platform to examine Canada's CI priorities from a cross-sector and multi-jurisdictional perspective; facilitate the timely exchange of relevant information on CI risks and emerging issues; and foster cross-sector partnerships among CI owners and operators.

National Cross Sector Forum: a network that brings together senior leaders from each of the ten CI sectors, federal, provincial and territorial governments to set priorities, discuss cross-sector and interdependencies issues and foster information sharing and best practices across sectors. The NCSF focuses on issues that promote an all-hazards approach to CI risk management.

Natural Infrastructure: refers to the use of preserved, restored or enhanced ecosystem features and materials (e.g., water, native vegetation, sand and stone) to deliver infrastructure outcomes and targeted community services.

Owners and Operators: the businesses, government organizations, individuals or other entities that own, operate, maintain and/or provide CI assets, systems and services. CI in Canada is owned, operated and provided by the private, public and not-for-profit sectors.

PNT: Position, navigation and timing information is used to understand where we are on the surface of the earth (position), to decide how to get to where we need to go (navigation) and to synchronize networks, or for timestamping (timing). Global navigation satellite systems (GNSS) are used extensively for providing this precise PNT information

Processes: refers to the actions or steps taken to achieve an outcome. For example, the changing of coloured lights follow a process to allow traffic flow.

Resilience: the capacity of a system, community or society to adapt to change or to a disturbance while keeping an acceptable level of function. Improving CI resilience means enhancing the ability of CI to continue to provide Canadians with the goods, services and infrastructure they need in the face of hazards.

Risk: the combination of the likelihood and the consequence of a specified hazard being realized. Risk refers to the vulnerability, proximity or exposure to hazards, which affects the likelihood of adverse impact structure.

Risk Management: refers to a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on, and communicating risk issues, is an integral part of good management.

Sector Networks: enable discussion and information sharing among sector-specific industry stakeholders and governments on sector network priorities and emerging issues. Each sector network is led by a federal government department or agency, which is responsible for determining the membership of the sector network. For example, the Department of Finance leads a Finance Sector Network with representatives of Canada's major financial institutions.

Security: the degree to which a person, organization or thing, such as infrastructure, is free from intentional harm or disruption and the ability to continue to reliably function in safety. Security can also refer to the integrity and privacy of information. For instance, cyber security measures are required to keep research data secure against unauthorized access and manipulation.

Stakeholder: a party or organization with an interest, role or responsibility related to the objectives of another organization or institution. Stakeholders involved in the renewal of the National Strategy for CI broadly include the federal, provincial, territorial and

municipal governments, private sector CI owners and operators, as well as academia and think tanks with subject matter expertise in CI security and resilience

Systems: refers to multiple things or people that interact to perform a role or produce an output. A system can be relatively simple, like an organization's information management software system, to complicated, like an industrial control system that monitors water quality at a water treatment facility.

Threat: the presence of a hazard and an exposure pathway; threats may be natural or human- induced, either accidental or intentional.

Vulnerability: refers to the conditions determined by physical, social, economic and environmental factors or processes, which increase susceptibility of something to the impact of hazards. It is a measure of how well prepared and equipped infrastructure is to decrease the impact of or cope with hazards.