



Critical 5

**Adapting to Evolving Threats:
A Summary of Critical 5 Approaches to Critical
Infrastructure Security and Resilience**

In partnership with the governments of:

Australia, Canada, New Zealand, United Kingdom, and United States

This narrative provides an update on the evolving risks facing critical infrastructure and discusses how Critical 5 nations have been modernizing their approaches to critical infrastructure protection. It also identifies common means to strengthen the security and resilience of their critical infrastructure domestically, while recognizing the need for a collaborative and coordinated approach across the international community given the interconnected nature of critical infrastructure.

Aussi disponible en français sous le titre : Adaptation à l'évolution des menaces : Résumé des approches en matière de sécurité et de résilience des infrastructures essentielles du Groupe des 5 Partenaires

To obtain permission to reproduce Public Safety Canada materials for commercial purposes or to obtain additional information concerning copyright ownership and restrictions, please contact:

Public Safety Canada, Communications
269 Laurier Ave. W
Ottawa Canada K1A 0P8

Communications@ps-sp.gc.ca
www.PublicSafety.gc.ca

© His Majesty the King in Right of Canada, as represented by the Ministers of Public Safety and Emergency Preparedness, 2024.

Publication date: 2024-06
Catalogue Number: PS9-35/2024E-PDF
ISBN: 978-0-660-71371-7

Table of contents

- Introduction4
- The need for resilient critical infrastructure4
- Evolving threat and hazard landscape6
- Adapting to the evolving critical infrastructure threat landscape7
 - Modernizing policy..... 7
 - Australia..... 7
 - Canada 9
 - New Zealand..... 11
 - United Kingdom 13
 - United States 14
- Definition of critical infrastructure and sector composition 16
- Developing stronger information sharing tools and partnership mechanisms 18
- Conclusion19
- Annex A: Critical 5 countries’ critical infrastructure information sheet20
 - Australia 20
 - Canada..... 23
 - New Zealand 25
 - United Kingdom..... 27
 - United States..... 30

Introduction

In 2014, the Critical 5¹ published a shared narrative entitled: Forging a Common Understanding for Critical Infrastructure. The publication established a collective interpretation of critical infrastructure concepts and definitions and was intended to facilitate the coordination of approaches to critical infrastructure protection. In the decade following its release, the geopolitical landscape has shifted, and the effects of climate change are being felt more readily. In response, Critical 5 countries are adapting their approaches to emerging hazards and threats, prompting the need to review and update their shared narrative.


This narrative provides an update on the evolving risks facing critical infrastructure and discusses how Critical 5 nations have been modernizing their approaches to critical infrastructure protection. It also identifies common means to strengthen the security and resilience of their critical infrastructure domestically, while recognizing the need for a collaborative and coordinated approach across the international community given the interconnected nature of critical infrastructure.

The need for resilient critical infrastructure

Modern societies are dependent on critical infrastructure systems to provide essential services that support lives and livelihoods. When critical infrastructure fails, it can be catastrophic, evidenced by the fact that damage to critical infrastructure and disruption of services is one of the largest contributors to economic losses from disasters.² Recognizing this, Critical 5 nations

¹ Established in 2012, the Critical 5 is an international forum comprising members from the Five Eyes intelligence sharing network (Australia, Canada, New Zealand, the United Kingdom, and the United States). The Critical 5 aims to strengthen cooperation between member countries by addressing threats to critical infrastructure, as well as to share information, practices and ideas on domestic policy and operational approaches to critical infrastructure security and resilience.

² United Nations - Department of Economic and Social Affairs. "UN DESA Policy Brief No. 139: Strengthening Disaster Risk Reduction and Resilience for Climate Action through Risk-Informed Governance | Department of Economic and Social Affairs." United Nations, United Nations, 6 Oct. 2022, www.un.org/development/desa/dpad/publication/un-desa-policy-brief-no-139-strengthening-disaster-risk-reduction-and-resilience-for-climate-action-through-risk-informed-governance.



are working to ensure that their critical infrastructure assets and systems are secure, protected, and resilient so that they may minimize and prevent disruptions when an incident occurs.

The need for such interventions is more pressing than ever before. Critical infrastructure systems are more highly interdependent and interconnected, creating the potential for individual failures to cascade into significant outages. At the same time, hazards and threats to our infrastructure systems are growing.

We also know that many of our critical infrastructures are unprepared for this new future. The COVID-19 pandemic, for example, revealed gaps in critical infrastructure business continuity planning, including inadequate stockpiles of personal protective equipment and difficulties in prioritizing and protecting key assets. Governments had to step in to prioritize critical activities to minimize economic disruptions and ensure the continued delivery of critical services.

In this context, we know that a failure to adequately invest in critical infrastructure resilience will:

- Have negative effects on the wellbeing of individuals, businesses, and communities impacted by disruptions that in many cases, could have been avoidable; and
- Impose significant costs on the economy, with the expense of recovery and service restoration generally exceeding what would have been required to prevent outages ahead of an event.

Building resilience is a positive investment for today and for the future, which generates a number of benefits, including:

- Saving lives and sustaining livelihoods;
- Maintaining social cohesion;
- Reducing economic shocks to supply chains; and
- Promoting innovative solutions and technologies to minimize damage to communities.

Evolving threat and hazard landscape

Since 2014, the geopolitical landscape has grown in complexity. Critical infrastructure now faces a wider range of threats and hazards, from naturally occurring events to human-induced disruptions of both accidental and malicious origins. Additionally, critical infrastructure assets and systems are more highly integrated than in 2014, as the technological advancements of the last decade have encouraged the adoption of digital systems by critical infrastructure owners and operators seeking to streamline service delivery.

As a result, the risk of an event triggering cascading failures across multiple interdependent sectors and having widespread domestic and international repercussions has grown significantly.

The shifting geopolitical landscape of the past decade has intensified national security concerns. Recent conflicts have illustrated how critical infrastructure can be targeted through digital or physical means to weaken a country's ability to protect itself and its citizens. Below the threshold of armed conflict, hostile threat actors deploy methods such as foreign interference campaigns, intellectual property theft, and operational disruptions to exploit critical infrastructure, resulting in substantial financial losses including maintenance and repair expenses, revenue losses, and increased security costs.

The adoption of digital and remotely operated technologies for critical infrastructure systems has also left them increasingly vulnerable to exploitation by cybercriminals and state-sponsored actors. Malicious cyber activities can have consequences, including power outages, drinking water contamination, disruption of transportation networks, and loss of life. Such disruptions can cause significant financial and reputational damage to organizations and reduce trust in institutions.

On the hazard side, climate change is escalating the frequency, intensity, and unpredictability of extreme weather events, which exert significant strain on physical critical infrastructure assets such as transportation networks, telecommunications systems, and energy infrastructure. In the absence of appropriate efforts to mitigate and adapt to the effects of climate change, these assets face a growing risk of more frequent disruptions and catastrophic failure.

Adapting to the evolving critical infrastructure threat landscape

In order to meet the challenges of both current and future threats, Critical 5 nations have had to adapt their levers to ensure critical infrastructure security and resilience through:

- Modernizing policies;
- Reviewing the definition of critical infrastructure and sector composition; and
- Developing stronger information sharing tools and partnership mechanisms.

Modernizing policy

Since 2014, Critical 5 nations have been making notable policy and program advancements to protect and secure their critical infrastructure.

Australia

In 2018, Australia implemented its primary critical infrastructure security legislation, the *Security of Critical Infrastructure Act 2018* (SOCI Act). Since then, it has undergone amendments to address emerging threats. The SOCI Act aims to strengthen the security and resilience of critical infrastructure by capturing sectors and asset classes essential to Australia. It provides a baseline level of security across 11 critical infrastructure sectors and places several obligations on entities responsible for critical infrastructure assets, including:

- The ability to impose enhanced cyber security obligations on Australia's most important critical infrastructure assets as Systems of National Significance. These are assets that, if disrupted, could have significant cascading effects on Australian society and national security;
- The reporting of operational and ownership information to the Register of Critical Infrastructure Assets, managed by the Department of Home Affairs;

- The establishment of a Critical Infrastructure Risk Management Program that requires entities to identify and mitigate the personnel, physical or natural, cyber and supply chain risks to the critical infrastructure asset;
- The requirement to report cyber security incidents to the Australian Cyber Security Centre's ReportCyber portal; and
- Responsive government assistance measures to allow the government to support industry in responding to a serious cyber incident.

The Trusted Information Sharing Network (TISN), established in 2003, is the Australian Government's primary engagement mechanism with industry on critical infrastructure. It brings together stakeholders from across the critical infrastructure community, including critical infrastructure owners and operators, supply chain entities, subject matter experts, and all levels of government. Members meet regularly within and across sector groups with the goal of enhancing the security and resilience of critical infrastructure. Australia also developed a TISN engagement platform, which is an online platform that provides a more flexible environment to support TISN engagement activity.

The *2023 Critical Infrastructure Resilience Strategy* (the Strategy) provides a national framework to guide Australia to enhanced critical infrastructure security and resilience. Developed in consultation with the critical infrastructure community, and supported by the *2023 Critical Infrastructure Resilience Plan*, the Strategy will guide Australia's critical infrastructure interests from 2023 to 2028.

In November 2023, Australia released the 2023-2030 Australian Cyber Security Strategy. Under "Shield Four" of the Strategy, the Government has committed to protecting Australia's critical infrastructure and essential government systems so it can withstand and bounce back from cyber-attacks, by:

- Clarifying the application of the SOCI Act to ensure critical infrastructure entities are protecting their data storage systems and managed service providers are uplifting their security settings;

- Delivering best practice guidance, exercises, advice on regulatory settings by working with industry to co-design security obligations for telecommunications providers and exploring options to incorporate cyber security regulation as part of expanded requirements for the aviation and maritime sectors;
- Establishing a framework to ensure compliance with security obligations and capture secondary consequences from cyber incidents by exploring powers to direct an entity to take specific actions to manage the consequences of a nationally significant incident;
- Expediting implementation of the most interdependent and important critical infrastructure in Australia to support the development of a bespoke, outcomes-focused partnership between the Government and Systems of National Significance entities;
- Uplifting Government cyber security by enabling the National Cyber Security Coordinator to oversee the implementation and reporting of cyber security across the whole of government and conducting reviews of the cyber maturity of Government agencies to position the Australian Government as a world-class trusted digital government; and
- Pressure-testing national defenses by expanding the national cyber security exercise program led by the National Cyber Security Coordinator to identify gaps in cyber defenses and build incident response playbooks.

Canada

Canada is in the process of modernizing its approach to critical infrastructure. In 2022, Canada launched a public consultation on its 2009 *National Strategy for Critical Infrastructure* to inform decision-making on securing and protecting its critical infrastructure. While work continues on charting a revised policy approach to critical infrastructure protection, the Government of Canada has also tabled legislation and implemented policies aimed at addressing threats to critical infrastructure.

Canada has taken strides to improve its cyber security, including that of our critical infrastructure. In 2018, Canada launched its *National Cyber Security Strategy* (NCSS), which aims to advance cyber security and resilience, support cyber innovation, and foster

collaboration among stakeholders. The NCSS prompted the creation of the Canadian Centre for Cyber Security, which works closely with domestic and international partners and serves as a trusted resource on cyber security. It also created the National Cybercrime Coordination Unit of the Royal Canadian Mounted Police (RCMP) to expand the RCMP's capacity to investigate cybercrime. Due to rapid advancements to digital infrastructure, Canada is currently in the process of updating its NCSS.

In 2022, Canada tabled Bill C-26, which, at the time of writing, is at consideration in committee in the House of Commons. Bill C-26 includes the *Critical Cyber Systems Protection Act*, which would designate federally regulated entities from four priority sectors (i.e., energy, finance, telecommunications, and transportation) to protect their critical cyber systems. If enacted, this legislation would create a registry of designated critical infrastructure entities that would be subject to cyber security obligations.

To address economic security threats, Canada is introducing amendments to the *Investment Canada Act* that will bolster Canada's visibility on investments, enhance transparency, support greater investor certainty, and ensure Canada has strong authorities to take action quickly and where required. Key amendments include new filing requirements prior to the implementation of investments in prescribed business sectors, improved information sharing with international counterparts, and expanded ministerial authority to extend the national security review of investments, impose conditions during a national security review, and accept undertakings to mitigate national security risk.

At the same time, Canada is in the process of exploring options to modernize its tools to counter foreign interference as the threat rapidly evolves. As part of a public consultation launched in November 2023, opinions were sought regarding potential amendments to several Canadian laws including:

- New foreign interference offences to the *Security of Information Act*;
- Updating the sabotage offence in the *Criminal Code* to strengthen deterrence of intentional harm to critical infrastructure;
- Introducing a review mechanism in the *Canada Evidence Act* for cases involving sensitive information; and

- Amending the *Canadian Security Intelligence Service Act* to include the ability for Canadian Security Intelligence Service to disclose sensitive information to those outside the Government of Canada.

In 2023, Canada also launched the first public report of the National Risk Profile, its first strategic, national-level risk assessment. The report is based on input and evidence from whole-of-society stakeholders across Canada and provides a foundation for understanding disaster risk from the three costliest hazards facing Canadians: earthquakes, wildland fire, and floods. It aims to broaden public awareness of disaster risk, identify gaps in the Canadian emergency management system at a national level and provide evidence to support existing federal risk assessment and climate change adaptation efforts.

Efforts have also been made to strategically reduce the risks that come with climate change impacts. In 2022, Canada launched its first *National Adaptation Strategy*. A key objective of the *National Adaptation Strategy* is to ensure that all infrastructure systems in Canada are climate-resilient and undergo continuous adaptation to adjust for future impacts to deliver reliable, equitable, and sustainable services to all of society. The *National Adaptation Strategy* aims to incorporate climate change resilience into all new federal infrastructure funding programs and ensure the provision of robust guidance, codes and standards that cover the top climate change risks for key public infrastructure systems.

New Zealand

New Zealand's commitment to improving the resilience of critical infrastructure is reflected across a range of strategies and policies, including:

- Rautaki Hanganga o Aotearoa 2022, New Zealand's first Infrastructure Strategy, which recommends a coordinated approach to managing risks to infrastructure resilience;
- New Zealand's first National Adaptation Plan 2022, which sets out a series of actions to enable critical infrastructure asset owners to undertake the actions needed to remain resilient to the impacts of climate change, and adapt to a changing climate;
- National Security Strategy 2023, which includes resilient critical infrastructure as a key economic security objective, and

- National Cyber Security Strategy, which prioritizes efforts to support critical infrastructure in building cyber resilience and protecting the security of their systems.

Consistent with the direction provided in these national strategies, New Zealand is working to update its settings to deliver a more resilient critical infrastructure system, including by:

- Improving access to funding and financing for infrastructure investments;
- Uplifting the infrastructure sector's approach to asset management to improve service delivery;
- Developing a climate adaptation framework to support investment decisions, cost-sharing, and management of climate risks;
- Streamlining resource management processes, and
- Establishing a standardized, robust approach to consideration of natural hazards risk in land use planning.

New Zealand is also considering a new systems-based regulatory approach, which would complement existing sectoral regulation with a comprehensive set of resilience requirements for all critical infrastructure. The intent of this regulatory reform is to better position the critical infrastructure system to manage all hazards and threats (including long-standing natural hazard risks, the effects of climate change and a growing range of national security threats). Potential features of a new regulatory approach that were consulted on in 2023 include:

- Improved information sharing between government and critical infrastructure on hazards, threats, and vulnerabilities, to enable critical infrastructure entities to make well-informed investment decisions;
- Collection of information by government on matters like ownership and control, and cyber incidents, to expand government's awareness of vulnerabilities and threats that critical infrastructure entities are exposed to;
- Enforceable minimum resilience standards, to reduce the likelihood and impact of adverse events that could disrupt the delivery of essential services across the critical infrastructure system, and

- Last resort, step-in powers for Government to support critical infrastructure entities in managing significant national security threats (such as cyber incidents).

More broadly, in 2021, the *Overseas Investment Act* was amended to enhance the New Zealand Government's ability to manage national security and public order risks posed by overseas investments in critical infrastructure. This includes the ability to screen investments in a number of critical infrastructure sectors irrespective of the dollar value of the investment or amount of equity being obtained.

United Kingdom

Since 2014, the United Kingdom has adapted and developed its approach to Critical National Infrastructure, with two new sectors, Space and Defence, being added in 2015.

In 2018, the United Kingdom developed a new systems thinking methodology—the Criticalities Process—to identify and categorize critical infrastructure assets and their supporting systems. This new standardized approach enables a consistent and shared understanding of the most critical infrastructure in the United Kingdom.

The United Kingdom has built upon the Criticalities Process, by creating a new digital tool, the Critical National Infrastructure (CNI) Knowledge Base. Knowledge Base takes Criticalities information and allows risk owners to view critical national infrastructure on a map or as a network graph and enables visualization of interdependencies and relationships between assets to understand potential cascading impacts of risk. Both tools have become essential in supporting the United Kingdom Government in providing targeted and practical guidance to make better-informed risk management decisions.

Furthermore, to embed resilience into policy-making, the United Kingdom Government published the Resilience Framework in December 2022, which marked the United Kingdom Government's first articulation of its strategic approach to resilience. Focusing on the foundational building blocks of resilience, the Framework enables the United Kingdom Government to better prevent, mitigate, respond to and recover from the risks the nation faces. Within the Resilience Framework the United Kingdom Government committed to introducing CNI standards by 2030. The 2023 Resilience Framework Update (published on 4 December 2023) highlights the progress that has been made across the various resilience commitments.

In addition, the United Kingdom passed the Telecommunications (Security) Act 2021, which places stronger security-related duties and responsibilities on the telecoms industry. It requires telecom providers to have measures in place to identify and defend their networks from cyber threats, as well as prepare for any future risks. In the same year, the United Kingdom also introduced the *National Security and Investment Act*, which enables the United Kingdom to identify and manage investment risks to national security, including Critical Infrastructure.

Recognizing the importance that developments in cyber will have on United Kingdom CNI, the United Kingdom implemented the National Cyber Strategy in 2022. This Strategy strengthens United Kingdom cyber security so that the United Kingdom is able to pursue and promote interests with confidence. In particular, the National Cyber Strategy 2022 sets outcomes for CNI (in the private and public sector) to better understand and manage cyber risk, whilst minimizing the impact of cyber incidents when they occur.

The United Kingdom has also unveiled a new “New Position, Navigation and Timing” (PNT) Framework in 2023, which includes a crisis plan in the event current PNT services are unavailable, as well as the creation of a dedicated government unit to ensure critical services can operate without disruption.

In addition, two new Technical Authorities have been created to support and improve the security and resilience of Critical National Infrastructure. In 2016, the United Kingdom formed the National Cyber Security Centre to provide a unified national response to cyber threats. In 2023, the United Kingdom created the National Protective Security Authority to provide expert, intelligence-led advice to sensitive sectors including critical infrastructure stakeholders.

United States

Since 2014, the United States’ critical infrastructure security and resilience doctrine has shifted towards centralizing the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency (DHS/CISA) to manage joint and cross-sector coordination across the Federal Government, establishing measurable risk reduction goals, and addressing urgent strategic threats.

In 2015, the United States began publishing Sector-Specific Plans, which establish goals and priorities for each sector that address their current risk environment, such as the nexus

between cyber and physical security, interdependence between various sectors, risks associated with climate change, aging and outdated infrastructure, and the need to ensure continuity in a workforce that is rapidly approaching retirement³.

In November 2018, recognizing the convergence of the physical and cyber worlds, the United States passed the *Cybersecurity and Infrastructure Security Agency Act*, which redesignated the DHS's National Protection and Programs Directorate as the CISA. CISA leverages an integrated approach to security by working with businesses, communities, and government at every level to help make the United States' critical infrastructure more resilient to cyber and physical threats. CISA, as the National Coordinator for critical infrastructure security and resilience, coordinates national efforts to manage physical risks to critical infrastructure and collaborates across government and private sector stakeholders who own and operate the majority of critical infrastructure in the country.

The *Fiscal Year 2021 National Defense Authorization Act* codified Sector-Specific Agencies, previously defined in Presidential Policy Directive 21 (PPD-21), as Sector Risk Management Agencies (SRMAs); and authorized how the DHS and SRMAs work with each other to protect critical infrastructure.

On April 30, 2024, the White House published the National Security Memorandum (NSM-22) on Critical Infrastructure Security and Resilience. This memo builds on the important work that the DHS/CISA and agencies across the federal government have been undertaking in partnership with America's critical infrastructure communities for more than a decade. It also replaces Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, which was issued more than a decade ago to establish national policy on critical infrastructure security and resilience.

The threat environment has significantly changed since PPD-21 was issued, shifting from counterterrorism to strategic competition, advances in technology like Artificial Intelligence, malicious cyber activity from nation-state actors, and the need for increased international

³ Cybersecurity and Infrastructure Security Agency - CISA. "2015 Sector-Specific Plans: CISA.", 15 Dec. 2015, www.cisa.gov/2015-sector-specific-plans.

coordination. This change in the threat landscape, along with increased federal investment in U.S. critical infrastructure, prompted the need to update PPD-21 and issue the new memo.

NSM-22 will help ensure United States critical infrastructure can provide the nation a strong and innovative economy, protect American families, and enhance collective resilience to disasters before they happen, strengthening the nation for generations to come. This NSM specifically:

- Empowers DHS to coordinate the national effort to secure United States critical infrastructure, with CISA acting as the National Coordinator for the Security and Resilience of United States Critical Infrastructure. . The Secretary of Homeland Security will be required to submit to the President a biennial National Risk Management Plan that summarizes United States government efforts to mitigate risk to the nation’s critical infrastructure.
- Reaffirms the designation of 16 critical infrastructure sectors and establishes a federal department or agency responsible for managing risk within each of these sectors.
- Elevates the importance of minimum security and resilience requirements within and across critical infrastructure sectors, consistent with the National Cyber Strategy, which recognizes the limits of a voluntary approach to risk management in the current threat environment.

Definition of critical infrastructure and sector composition

While definitions of critical infrastructure may vary slightly across Critical 5 nations, key underlying commonalities have not changed substantially since the publication of the 2014 shared narrative.

“Critical infrastructure, also referred to as critical national infrastructure, can be broadly defined as the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations.”

This definition continues to support a common framework to shape international engagement on critical infrastructure.

All Critical 5 nations continue to use a sector-based approach. This facilitates sector and cross-sector collaboration among stakeholders and can be used as a high-level analytical framework for identifying critical services and functions as well as the assets and systems that enable them. Some countries also identify subsectors of critical infrastructure or prioritize specific vital assets and systems for greater protection.

Emerging national and economic security threats alongside rapid technological advancements have prompted Critical 5 nations to expand their understanding of what constitutes critical infrastructure. Areas of additional focus and effort by some Critical 5 nations have included:

- Higher Education and Research: Plays a vital role in the development of a skilled workforce, technological innovation, and economic growth. It also allows for the advancement of new technologies that are essential to critical infrastructure, such as healthcare and information technology;
- Data Storage: Data storage is an essential service for individuals, businesses, and government. It is also crucial for critical infrastructure stakeholders to access critical information when much of it is stored in the cloud; and
- Space: The reliance on data and services originating from space-based assets (e.g., positioning, navigation and timing services provided by global navigation satellite systems) and the unique threat environment facing space-based assets have prompted some Critical 5 members to consider recognizing space as an independent sector.

Sector composition will continue to evolve as technology and the threat landscape changes, ensuring that the most essential services are subject to appropriate regulatory requirements and other protections.

Developing stronger information sharing tools and partnership mechanisms

The Critical 5 values partnerships and information sharing with critical infrastructure owners and operators, as well as national, regional, and local government counterparts. Engaging in multiple formats, such as engagement forums and web-based information sharing platforms, allows industry stakeholders and government to collaborate on topics including assessing and identifying the criticality of infrastructure, identifying cross-sector dependencies, and developing best practices for managing vulnerabilities to common risks.

Industry and government engagement forums support partnership building and information sharing across the critical infrastructure community. For example, New Zealand engages through the national-level Lifelines Council and regional lifelines groups, as well as sector-specific information exchanges that are facilitated by the National Cyber Security Centre, while the United Kingdom holds industry forums led by the Critical National Infrastructure and Systems Lead Government Departments and the National Protective Security Agency.

Awareness and outreach campaigns, such as the United States' and Australia's annual Infrastructure Security Month, the United States' Critical Infrastructure Partnership Advisory Council, Cybersecurity Advisory Committee, and the National Infrastructure Advisory Council are leveraged to promote resources and tools that can help critical infrastructure owners and operators build security and resilience. In future years, Critical 5 nations intend to collectively host an official, branded month of focus and action on critical infrastructure security.

Lastly, some Critical 5 nations use web-based information sharing platforms to allow industry and government to share timely information in a secure environment such as Australia's Trusted Information Sharing Network engagement platform and Canada's Critical Infrastructure Information Gateway.

Conclusion

Over the past decade, Critical 5 nations have been adapting their policy approaches as the hazard and threat environment has rapidly evolved. Climate change, cyber threats, and growing national security risks have led all Critical 5 countries to introduce or consider changes to what constitutes critical infrastructure as well as the regulatory and non-regulatory tools available to critical infrastructure providers to enhance their resilience. This recognizes that collectively investing in critical infrastructure resilience is essential, as failure to do so can be unnecessarily costly in the event of disruption or loss of service.

Critical 5 nations continue to share knowledge, experience, and expertise on issues of common interest, which will better equip this community to respond to the growing and evolving risks. The strength of the relationship among the Critical 5 forum has proven to be valuable as we continue to learn from each other on key issues of mutual interest.

Annex A: Critical 5 countries' critical infrastructure information sheet

Australia

Definition of critical infrastructure:

Critical infrastructure is considered to be physical facilities, systems, assets, supply chains, information technologies and communication networks, which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic well-being of Australia as a nation or its states or territories, or affect Australia's ability to conduct national defence and ensure national security.⁴

List of sectors:

- Energy
- Communications
- Data storage or processing
- Defence industry
- Financial services and markets
- Food and grocery
- Healthcare and medical
- Higher education and research
- Space technology
- Water and sewage
- Transport

⁴ "Critical Infrastructure Resilience Strategy". Cyber and Infrastructure Security Centre Website, Department of Home Affairs & Australian Government, 2023, www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy.

Policy approach to managing critical infrastructure security and resilience:

Security of critical infrastructure in Australia is legislated. The critical infrastructure policies and frameworks in Australia are managed by the Department of Home Affairs, with some aspects of the regulation falling under other Australian Government agencies.


The Department of Home Affairs is responsible for the *Security of Critical Infrastructure Act 2018*, which is the primary legislation relating to critical infrastructure security. Other critical infrastructure security framework in place includes:

- *Aviation Transport Security Act 2004*, which protects Australia’s civil aviation infrastructure from acts of unlawful interference (primarily terrorism);
- *Maritime Transport and Offshore Facilities Security Act 2003*, which protects Australia civil maritime transport, and offshore facilities from acts of unlawful interference (primarily terrorism); and
- Part 14 of the *Telecommunications Act 1997*, which formalizes information sharing arrangements between government and industry to better protect Australia’s networks from acts of sabotage, espionage, and foreign interference.

Stakeholder engagement program and supports:

Engagement with industry is central to Australia’s critical infrastructure security and resilience model. Since late 2022, Australia has been undertaking a significant expansion of the ways in which it engages with owners and operators to assist them manage risk and increase compliance. This has involved hosting Australia’s inaugural Cyber and Infrastructure Security Conference and Critical Infrastructure Security Month; experimenting with new mediums and formats—such as: webinars, town halls, and podcasts; launching a dedicated social media presence for owners and operators; hosting in-person “community of best practice” events; and planning a program of engagement with Corporate Leaders, Company Directors, and Board members.

The Trusted Information Sharing Network (TISN) is a platform for all levels of Australian industry and government to engage and enhance the security and resilience of critical



infrastructure. In addition to a secure online platform, the TISN is comprised of sector groups which enable critical infrastructure owners and operators to share information on threats and vulnerabilities and collaborate on appropriate measures to mitigate risk and boost resilience. Membership of the TISN doubled in 2023.

Australia regularly publishes a range of risk assessment material to aid owner and operator understanding of the threat environment and to encourage owners and operators to think critically about their risk exposure.

Australia's National Office of Cyber Security Exercise Program runs exercises on a priority basis with critical sectors. These exercises are designed to test established processes in the event of a cyber security incident which impacts industry and requires interaction with government to manage flow-on consequences. They are collaborative, discussion-based exercises which demonstrate opportunities for enhancement and further alignment in the event of an incident.

Canada

Definition of critical infrastructure:

The *National Strategy for Critical Infrastructure* defines critical infrastructure 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.

List of sectors:

Energy and utilities

Finance

Food

Government

Health

Information and communication technology

Manufacturing

Safety

Transportation

Water

Policy approach to managing critical infrastructure security and resilience:

Canada's current approach is guided by the *National Strategy for Critical Infrastructure* and its accompanying three-year Action Plans. Published in 2009, the National Strategy provided a definition of critical infrastructure and created 10 sectors. Public Safety Canada provides a central governance and policy coordination function while individual sector networks—a group of public-private stakeholders within a given sector—are organized by responsible lead federal departments and agencies. Canada's approach to critical infrastructure security and resilience is based on collaborative, voluntary actions and participation, ranging from information sharing to tools and programs.

Stakeholder engagement program and supports:

Canada has various engagement programs and supports available to its critical infrastructure stakeholders. For example, Canada works closely with internal and external partners to enhance critical infrastructure resilience through:

- Public-private sector collaboration through various engagement mechanisms such as the National Cross Sector Forum which promotes information sharing across the sector networks;
- Lead Federal Department and Federal-Provincial-Territorial working groups bring together representatives to collaborate on all-hazard and cross-sector issues;
- Information sharing to stakeholders to support risk management action, including via Canada's Critical Infrastructure Information Gateway, a secure information sharing platform, working with internal and external partners to enhance critical infrastructure cyber security, including through training and threat briefings;
- Exercises to support critical infrastructure planning and response efforts; and
- Online and on-site assessments to identify/address vulnerabilities and help owners and operators enhance the security and resilience of their organization from an all-hazards perspective.

New Zealand

Definition of critical infrastructure:

As of January 2024, New Zealand does not have a legislated definition of critical infrastructure – the closest is those entities currently listed as ‘lifeline utilities’ in Schedule 1 of the *Civil Defence Emergency Management Act 2002*.

Reflecting the changing technological and risk landscape, the New Zealand Government is considering adopting a new principles-based definition of critical infrastructure as part of broader work to enhance the resilience of New Zealand’s critical infrastructure system.

List of sectors:

Broadcasting

Energy

Telecommunications

Transport

Water (fresh, waste and storm water)

Policy approach to managing critical infrastructure security and resilience:

New Zealand largely regulates critical infrastructure entities on a sector-by-sector basis. These sectoral regulatory regimes tend to have a focus on safety, security, and affordability, which often have overlaps with resilience.

There are limited exceptions to this sector-by-sector approach, most clearly in relation to emergency preparedness and response. The *Civil Defence Emergency Management Act 2002*⁵ requires lifeline utilities to “ensure that [they are] able to function to the fullest possible extent, even though this may be at a reduced level, during and after an emergency”, but this is not an enforceable requirement.

⁵ Department of Internal Affairs. Civil Defence Emergency Management Act 2002 - New Zealand Legislation, Department of Internal Affairs, 2002, www.legislation.govt.nz/act/public/2002/0033/51.0/DLM149789.html.

Stakeholder engagement program and supports:

New Zealand government agencies support critical infrastructure owners and operators in preparing for, and mitigating the consequences of, potential hazards and threats through awareness and capability building. For example:

- The National Emergency Management Agency provides leadership in reducing risk, as part of which it engages with lifeline utilities on managing sector readiness, response and recovery from emergencies;
- The National Institute of Water and Atmospheric Research and the Earthquake Commission, Toka Tū Ake EQ, provide information on natural hazard exposures, including geotechnical and real-time natural hazards data; and
- The National Cyber Security Centre as part of the Government Communications Security Bureau engages directly with critical infrastructure owners and operators, providing guidance, threat alerts and specialist technical capabilities to raise their cyber resilience. The National Cyber Security Centre also helps critical infrastructure respond to, and recover from, significant cyber security incidents.

In addition to the support provided by government agencies, the New Zealand Lifelines Council (comprised of representatives from government and the private sector) focuses on connecting critical infrastructure owners and operators across sectors and facilitates engagement with a range of stakeholders working to improve New Zealand's infrastructure resilience.

United Kingdom

Definition of critical infrastructure:

Critical National Infrastructure (CNI): The United Kingdom Government official definition is: “Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), where the loss or compromise of which could result in:

- Major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
- The Significant impact on national security, national defence, or the functioning of the state.”

List of sectors:

Chemicals

Civil nuclear

Communications

Defence

Emergency services

Energy

Finance

Food

Government

Health

Space

Transport

Water

Policy approach to managing critical infrastructure security and resilience:


The United Kingdom's Cabinet Office, and respective Devolved Administrations, are responsible for providing overarching governance and cross-sector policy guidance for their countries. In terms of United Kingdom critical national infrastructure oversight, the United Kingdom Government oversees a decentralized and sector-led model of CNI. Each sector is overseen by the relevant Lead Government Department, whilst different stakeholders such as the Cabinet Office, National Technical Authorities, Regulators, Owners and Operators and Devolved Administrations all play specific roles in the functioning of the United Kingdom's CNI landscape.

As the Lead Government Departments are responsible for their own sector, they develop their own guidance, regulation and legislation to support in protecting and strengthening the security and resilience of their CNI. The Cabinet Office also leads on implementing overarching bills, legislations, strategies, and frameworks to support the sectors and provide coherence and consistency across the CNI sectors.

As the United Kingdom is made up of four different legislatures and executives, each with a different range of powers, the CNI approach can vary between Devolved Administrations and the United Kingdom. However, the four administrations of Scotland, Wales, Northern Ireland and the United Kingdom work in partnership to ensure policy approaches and legislation is complementary. The policy approach to Critical National Infrastructure is nuanced, in that some areas are partly reserved (to the Government of the United Kingdom), and some aspects and sectors are devolved (to the administrations of Scotland, Wales and Northern Ireland).

Stakeholder engagement program and supports:

CNI sector engagement is led by Lead Government Departments and devolved administrations. Lead Government Departments may differ in their approach across the sectors, but include industry forums, one-to-one engagement, or one to many guidance. Technical authorities (such as the National Cyber Security Centre and the National Protective Security Authority) provide best practice security guidance and advice to critical national



infrastructure systems owners and operators including holding information exchange forums with industry.

In June 2023 the United Kingdom Government published the most transparent ever National Risk Register, which includes all information in the classified National Security Risk Assessment unless it could not be released for national security or commercial reasons. The document is aimed at providing detailed information for those with formal contingency planning responsibilities at national and local level. The approach to transparency on risk means that everyone, from risk practitioners to academics, can now see directly how the United Kingdom Government identifies and assess risks.

In the 2023 Annual Statement, we also announced a new United Kingdom Resilience Academy (UKRA). The UKRA will provide training and play a leading role in setting standards for resilience learning; creating and promoting good practice guidance documents and regularly convening resilience practitioners to encourage collaboration.

United States

Definition of critical infrastructure:

Under the *USA Patriot Act of 2001*, the United States defines critical infrastructure as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters⁶.

List of sectors:

- Chemical
- Commercial facilities
- Communications
- Critical Manufacturing
- Dams
- Defence industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities and services
- Health and public health
- Information and technology
- Nuclear reactors, materials and waste
- Transportation
- Water and wastewater

⁶ Analysis of the USA PATRIOT Act." USA PATRIOT ACT - Title 10, Section 1016, 2004, www.seattlewebcrafters.com/usapatriotact/t10sec1016.php.

Policy approach to managing critical infrastructure security and resilience:

In the United States, critical infrastructure security is built on a partnership between government and private industry that combines the implementation of policy, regulatory, and voluntary actions to manage risk. Both public and private entities own and operate the nation's critical infrastructure. The effort to secure the nation's critical infrastructure requires a whole-of-government approach and coordination and collaboration across multiple intergovernmental and industry stakeholders. The *Cybersecurity and Infrastructure Security Agency Act of 2018* (CISA), requires the Director of CISA to "coordinate a national effort to secure and protect against critical infrastructure risks" consistent with a comprehensive national plan (currently the National Infrastructure Protection Plan 2013).

The responsibility for fulfilling policy goals is distributed across multiple federal agencies with statutory responsibility as "Sector Risk Management Agencies." Each of the 16 critical infrastructure sectors have a designated Sector Risk Management Agency with authorities, expertise, and capability aligned to that sector.

This existing national infrastructure security framework provides a collaborative partnership model for consolidating information and expertise from government and industry. Working with critical infrastructure sectors, the Federal Government ensures the security and resilience of the nation's infrastructure through the use of tools and resources like bi-directional threat information sharing, real-world exercises, incident response training and guidance, federally led risk assessments and analysis, and subject matter expertise. Active engagement with public and private sector partners informs this national framework and its associated tools and resources, which those partners rely on for the security of their systems and assets.

Stakeholder engagement program and supports:

The United States has developed and implemented numerous information sharing programs to promote resources and tools that help our partners build security and resilience. These programs include awareness and outreach campaigns like the annual Cybersecurity Awareness Month, the annual Critical Infrastructure Security and Resilience Month, and broader national awareness programs that offer partner toolkits. These programs allow for

sharing substantive information with the private sector and with state, local, tribal, and territorial governments.

The United States, through CISA, fosters relationships with international partners to promote collaborative information sharing, cyber security best practices, and partnership models across the globe, as it is recognized that cyber security threat actors are not constrained by geographic boundaries. In addition, the Cyber Innovation Fellow Initiative is an opportunity for senior technical experts from across the private sector to apply to embed on CISA's cyber security teams for their professional development benefit, and to the benefit of CISA's growing mission space⁷. The United States also has a variety of Public-Private Partnership Councils and Committees that work towards the goal of enhancing the security and resilience of the nation's critical infrastructure.

⁷ CISA. Cyber Innovation Fellows Initiative: CISA, 2023, www.cisa.gov/topics/partnerships-and-collaboration/cyber-innovation-fellows-initiative.