Canadian Radio-television and Telecommunications Commission
Conseil de la radiodiffusion et des télécommunications canadiennes

Canada

Telecommunications Resilience Analysis Benchmarks Report

June 30, 2023

REPORT SUBMITTED BY: Gartner Canada Co.

Canadian Radio-television and Telecommunications Commission Conseil de la radiodiffusion et des télécommunications canadiennes Canada

Gartner Canada Co.
1565 Carling Avenue, Ottawa, Ontario K1Z 8P9, Canada
www.gartner.com

ISBN: 978-0-660-68924-1
Cat. No.: BC92-128/2023E-PDF

The Canadian Radio-television and Telecommunications Commission (CRTC)
Ottawa, Ontario
Canada
K1A ON2
Tel: 819-997-0313
Toll-free: 1-877-249-2782 (in Canada only)
https://applications.crtc.gc.ca/contact/eng/library

Aussi disponible en français

A Report for Innovation, Science and Economic Development Canada (ISED) and the Canadian Radio-television and Telecommunications Commission (CRTC) Telecommunications Resilience Analysis Benchmarks Report

June 30, 2023
Engagement: 330081153

Table of Contents

1.0 Executive Summary

1.0 Executive Summary

As part of the Telecommunications Reliability Agenda, Innovation, Science and Economic Development Canada (ISED) in collaboration with the Canadian Radio-television and Telecommunications Commission (CRTC) is exploring potential approaches to promote reliability of telecommunications networks.

ISED and CRTC required support for undertaking a study to compile and evaluate various approaches by foreign governments, regulators, and industry to enhance the reliability and resilience against all causes of network outages. Regulatory obligations, guidelines, and compliance measures planned and/or undertaken by foreign governments must be assessed to determine their applicability to Canada.

ISED in collaboration with the CRTC engaged Gartner to perform an independent, third-party comparative analysis and benchmark for Canada against international frameworks for telecommunications reliability in selected jurisdictions.

The objective of the engagement was to provide a complete set of available policy approaches appropriate for implementation in Canada. Gartner provided benchmark-enabled support to ISED in its analysis of Telecommunications Resilience implications for Canada, by performing:

- A market scan of up to nine (9) countries of current practices, strategy, and approach to Telecommunications Resilience for foreign governments (including US, UK, Australia, South Korea, France, Germany, EU, New Zealand, and Japan) to develop a holistic picture and to identify discernible trends.
- Analysis of best practices in Telecommunications Resilience for a sub-set of down-selected countries using Gartner Research, 14 consultations across these jurisdictions, and benchmark data. The six (6) foreign governments included the US, UK, Australia, EU, New Zealand, and Japan.
- Assessment and consideration of the technology necessary to enable the analysis of trends, outlook of hypotheses, and analysis of new and existing technologies related to Telecommunications Resilience.

2.0 Introduction

2.0 Introduction

In collaboration with ISED and CRTC, Gartner leveraged its extensive research, frameworks, insights, seasoned professionals, and global experts to perform a benchmark comparison against other foreign government approaches to Telecommunications resilience.

Gartner conducted consultations, and performed a market scan using Gartner Research and Databases, and identify relevant research literature that informed the:

- Benchmark telecommunications environments globally using an all-hazards approach (e.g., natural disasters, cyber-attacks and malicious activities, human error, procedural failure, or third-party actions such as fibre/power/systems failures).
- Gartner supplied global experience in:
    - telecommunications policy and regulatory frameworks, including critical infrastructure, emergency management, and disaster recovery frameworks.
    - communications network architecture and operations (e.g., wireline/wireless/satellite network).
    - emergency services and their network architectures (9-1-1 or local equivalent, alerting and national dedicated networks e.g., FirstNet).

2.1 Telecommunications Resiliency

Telecommunications Resiliency pertains to outages and degradation of wireline, wireless, satellite and subsea communication methods.

According to CISA (The US Cybersecurity and Infrastructure Security Agency), communications resiliency means a network can withstand damages, thereby minimizing the likelihood of a service outage. Resiliency is the result of three (3) key elements: route diversity, redundancy, and protective/restorative measures.

According to European Union (EU), resilient networks are characterized by providing and maintaining an acceptable level of service in face of faults (unintentional, intentional, or naturally caused) affecting their normal operation. The main goal of resilience is for faults to be invisible to users. A wide accepted list of risks to the resilience of networks includes flash crowd events, cyber-attacks, outages of other support services, natural disasters, and system failings.

The Office of Communications (Ofcom), the United Kingdom’s regulator for communications services, outline communications resiliency as managing the risk of disruption to public networks in terms of availability, performance, and functionality.

The Australian government indicate that resilience in telecommunication networks help prevent, mitigate, and manage outages during emergencies through innovation, network hardening, satellite connections, and temporary infrastructure capabilities.

As defined by the Canadian Security Telecommunications Advisory Committee (Source: Telecommunications Network Resiliency in Canada: A Path Forward, March 2023):

- Fundamentally, network resiliency and reliability require that Canadian Telecommunications Service Providers (CTSPs) strive for always-on availability of service, to the maximum extent practicable, from a commercial, operational, and technical perspective, in the context of operating complex networks across the Canadian landscape.
- Effective network resiliency suggests that CTSPs aspire to have immediate fault-mitigation and rapid restoration mechanisms to reduce the impact of an adverse event on service delivery should the first line of connection degrade or fail. Such mechanisms may be either passive and/or active.
- CTSPs should also work toward ensuring, to the extent practicable, the deployment and maintenance of resilient communication networks for emergency recovery personnel (e.g., emergency operations, network operations centers and other CTSP personnel involved in emergency response).
- This includes striving for reliable partnerships between a CTSP and any third-party vendors that may be involved in the delivery of a CTSP’s communications service.
- Further, to the extent practicable, CTSPs should support each other during times of need, to help preserve the connectivity of all users of Canada’s telecommunications networks.

2.2 Benchmark of Best Practices

The Benchmark of Best Practices for Telecommunications Resiliency included:

- The identification of best practice alternatives to regulation to prevent/reduce telecommunications network outages; and regulatory obligations.

2.3 Final Report Goals and Objectives

The goal for the final report and the objective for the assessment was to:

- Provide benchmark-enabled support to ISED and the CRTC in its analysis of Telecommunications Resilience implications for Canada.

2.4 Information and Communication Technology Sector

For the purpose of this assessment, it is important to understand the context and definition of the Information and Communication Technology Sector. Gartner evaluated a specific type of providers within ICT. These should not be considered the only organizations and/or providers that can influence and/or support telecommunications resilience but they would be considered the primary service providers for telecommunications within the jurisdictions analyzed.

For this report, the Communication Service Providers (CSPs) sector has been classified into four categories based on type of communication infrastructure:

- **Wireless Network:** communication networks that transfer data over a between nodes without the use of wires, typically relying on radio frequencies.
- **Wireline Network – Terrestrial:** communication networks that use physical cables and fibre on land to transfer data between communication nodes.
- **Wireline Network – Sub-sea:** communication networks that use physical cables and fibre under the sea to transfer data between communication nodes.
- **Satellite Network:** communication networks that use satellites orbiting the Earth to transfer to transfer data between communication nodes.

3.0 Methodology

3.0 Methodology

For this engagement, Gartner performed a benchmark assessment and market scan of nine (9) countries and jurisdictions for current practices, strategy, and approach to Telecommunications Resilience for foreign governments. These jurisdictions included the US, UK, Australia, South Korea, France, Germany, EU, New Zealand, and Japan.

Further in the report, the analysis will dive deeper into a sub-set of the larger jurisdictional list, performing a benchmark assessment of the regulations, legislation and alternative methods required to prevent and/or reduce telecommunications network outages, voluntary codes of conduct, standards and/or best practices.

3.1 Data collection

Approach was to gather high-level data on the nine (9) countries from multiple sources to develop a holistic picture as well as to identify discernible trends. The methods used and sources referenced for this study included:

- Direct Interviews with stakeholders in the respective countries' regulatory organizations. These stakeholders included individuals currently "in-role" actively employed by the jurisdiction, regulators, or organizations influencing regulators, and individuals who previously held roles within those organizations.
- Official material published by target countries' regulatory organizations.
- Reports and articles from secondary sources.

3.1.1 Jurisdictional Profiles

Non-telecommunications characteristics of each jurisdiction were also collected to provide referential context for analytic comparisons. These characteristics included population, land area, population density, coastline, geographic features, number of CSPs, and others.

Table 1. ICT Engagement Focus – Communication Service Providers

								European Union	
	Canada	**Australia**	**United States**	**United Kingdom**	**New Zealand**	**Japan**	**South Korea**	**Germany**	**France**
Population (M)	39M	26M	340M	68M	5M	123M	52M	83M	65M
Land Area (km^2)	**10.0M**	**7.7M**	**9.4M**	0.24M	0.27M	0.38M	0.10M	0.36M	0.55M
Density (/km^2)	**4**	**3**	37	280	20	338	531	238	118
Sub-sea Connections	**21**	23	90	59	8	32	11	8	29
Number of CSPs	4+	4+	3+	4+	3+	4+	3+	4+	4+

Sources: World Population by Country 2023 (Live), The World Factbook

- Canada's land area is comparable only to the United States and Australia where network coverage, and therefore redundancy, becomes more of a concern due to sheer geography to be traversed.
- Canada's relative density aligns most closely with Australia and New Zealand and lends itself to similar potential environmental outage challenges of promoting resiliency across low to very low-density areas.
- Canada has a moderate number of sub-sea connections, compared to other global peers, allowing for redundancy should one or more connections become compromised at the same time.

For reference, Canada's characteristics are as follows:

- **Population**: At 39M, it is smaller than most scanned.
- **Land Mass**: At 10.0M km2, it is larger than all scanned.
- **Density**: At 4/km2, it is less dense than most scanned.
- **Coastline**: At 202,080 km, it is almost 10x greater than any other scanned.
- **Geographic Features**: Canada's diverse geography includes almost all geographic features from the other jurisdictions scanned, making it the most complex.
- The Largest Telecommunications Service Provider (TSP) in Canada:
  - Bell Canada, TELUS, Rogers-Shaw, and Quebecor, controlling about 90%+ of the country's telecommunications business.
  - There are some regional carriers including Videotron, SaskTel, and Eastlink.
  - Most jurisdictions scanned have 3-5 major TSPs, along with many sub-providers.

Note: The EU is currently composed of 27 Member States including Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

3.1.2 Jurisdictional Structure and Governance

Information relating to regulator mandates and governance structure was collected for each jurisdiction provide referential context for analytic comparisons. Most jurisdictions had regulators or oversight bodies that reported directly into the government.

Table 2. Jurisdictional Structures and Governance

Jurisdiction	Regulator	Mandate	Governance
Canada	Innovation, Science and Economic Development Canada (ISED)	Responsible for the *Telecommunications Act*, and in this context the department is responsible for regulating spectrum, telecommunications equipment, international submarine, and satellite licensing frameworks, as well as working with public and private sector organizations on the resiliency of telecommunications infrastructure.	Federal Department, reports to the Parliament of Canada.
	Canadian Radio-television and Telecommunications Commission (CRTC)	Regulates and supervises broadcasting and telecommunications in the public interest. The CRTC is dedicated to ensuring that Canadians have access to a world-class communication system that promotes innovation and enriches their lives.	Independent Agency, reports to the Parliament of Canada.
	Canadian Centre for Cyber Security (CCCS)	Single unified source of expert advice, guidance, services, and support on cyber security for government, critical infrastructure owners and operations, the private sector, and the Canadian public. The Cyber Centre is part of the Communications Security Establishment (CSE).	Federal Department reports to the Parliament of Canada.
United States	Federal Communications Commission (FCC)	Regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and US territories. (About the FCC)	Independent Agency, subject to the oversight of Congress.
	Cybersecurity and Infrastructure Security Agency (CISA)	Operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. Works with partners to defend against current threats and to build a more secure and resilient infrastructure for the future. (About CISA)	Operational component of the Department of Homeland Security (DHS).
	National Telecommunications and Information Administration (NTIA)	Responsible by law for advising the President on telecommunications and information policy issues, focus on broadband internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the internet	Executive Branch Agency located within the Department of Commerce.

Jurisdiction	Regulator	Mandate	Governance
		remains an engine for continued innovation and economic growth. (About NTIA)	
United Kingdom	Office of Communications (Ofcom)	Responsible for regulation of TV, radio, video on demand sectors, fixed line telecommunications companies, mobiles, postal services, and spectrum. (What is Ofcom?)	Independent Agency, reports to the UK Parliament.
	Department for Science, Innovation and Technology (DSIT)	Responsible for positioning the UK at the forefront of global scientific and technological advancement, driving innovations that change lives and sustain economic growth, delivering talent programs, physical and digital infrastructure, and regulation to support UK economy, security, and public services. (DSIT)	Federal Department, reports to the UK Parliament.
	National Cyber Security Centre (NCSC)	Responsible for providing advice and support for the public and private sector in how to avoid computer security threats. It was created out of a number of pre-existing organizations which included: Centre for Cyber Assessment (CSA), Computer Emergency Response Team UK (CERT UK), Cyber Security Information Sharing Partnership (CISP), and CovCertUK.	Its parent organization is GCHQ (Government Communications Headquarters).
Australia	Australian Competition and Consumer Commission (ACCC)	Responsible for enforcing the Competition and Consumer Act 2010 and other legislation, promoting competition, fair trading and regulating national infrastructure for the benefit of all Australians. (About ACCC)	Independent Commonwealth statutory authority, under the portfolio responsibilities of The Treasury.
	Australian Communications and Media Authority (ACMA)	Responsible for the regulation of broadcasting, radiocommunications, telecommunications and online content. Its governance and functions are prescribed by the Australian Communications and Media Authority Act 2005. (ACMA Statement of Intent)	Independent Commonwealth statutory authority, reports to the Australian Parliament.
New Zealand	New Zealand Infrastructure Commission	Two primary functions under the *Telecommunications Act* 2001 that help to ensure broadband and mobile markets are competitive. The first is to regulate certain fixed-line and mobile services by setting the price and/or access terms for that service. The second is to monitor and report on competition, performance, and developments in telecommunications markets. (NZIC / Te Waihanga Act 2019)	Independent Crown Entity, reports to the New Zealand Parliament.
Japan	Ministry of Internal Affairs and	Responsible for management and administration of the basic administration system of the country, the administration of	Accountable to the Prime Minister's Office.

Jurisdiction	Regulator	Mandate	Governance
	Communications (MIC)	local autonomy, emergency services, and application of ICT growth strategies.	
South Korea	Ministry of Science and ICT (MSIT)	Responsible for promoting inclusive economic growth through continuous technological innovation and transformation, in partnership with civil society. (MSIT Info)	Reports directly to the President of South Korea.
Germany	Bundesnetzagentur (BNetzA)	Responsible for setting the general conditions for fair competition in the electricity, gas, telecommunications and postal infrastructures sectors and act as a supervisory authority. (About BNetzA)	Independent federal authority, reports to reports directly to the Federal Ministry for Economic Affairs and Energy.
France	Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse (ARCEP)	Responsible for regulating the electronic communications, the postal sector and print media distribution. As the architect and guardian of the France's internet, fixed and mobile and postal networks, ARCEP works to ensure that these networks develop as a "common good." (ARCEP)	Independent administrative authority (IAA), reports to French Parliament.
European Union	European Union Agency for Cybersecurity (ENISA)	Responsible for increasing operational cooperation at EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross-border cyberattacks and crises.	▪ The Management Board (MB) is composed of representatives of the Member States and the EU Commission. ▪ The Executive Board is made up of five members of the MB and it is chaired by the MB Chairperson. ▪ The Executive Board is preparing decisions to be adopted by the Management Board on administrative and budgetary matters and it meets once every three (3) months.

Jurisdiction	Regulator	Mandate	Governance
	Body of European Regulators for Electronic Communications (BEREC)	Responsible for ensuring the consistent implementation of the European regulatory framework for electronic communications.	Independent body of the EU, reports to the European Commission.

3.1.3 Jurisdiction Communication Service Providers

The major telecommunications providers in each jurisdiction include:

- Canada 4+
  - Rogers
  - Bell
  - TELUS
  - Quebecor
- United States 3+
  - AT&T
  - Verizon
  - T-Mobile (Sprint is a part of T-Mobile)
- United Kingdom 4+
  - BT Group
  - Sky
  - Virgin Media
  - TalkTalk
- Australia 4+
  - Telstra Corporation Limited
  - Optus
  - Vodafone Hutchison Australia (VHA)
  - TPG Telecommunications Limited
- New Zealand 3+
  - Spark New Zealand
  - Vodafone New Zealand
  - 2degrees
- Japan 4+
  - NTT Group
  - KDDI Corporation
  - SoftBank Corp.
  - Rakuten Mobile
- South Korea 3+
  - SK Telecommunications
  - KT Corporation (formerly known as Korea Telecommunications)
  - LG Uplus
- Germany 4+
  - Deutsche Telekom AG
  - Vodafone Germany
  - Telefonica Germany (O2 – operating under the O2 brand)
  - 1&1 Drillisch AG

- France 4+
    - Orange (formerly known as France Télécom)
    - SFR (Societe Francaise du Radiotelephone)
    - Bouygues Telecom
    - Free

3.1.4 Jurisdiction Network Coverage

Unlike wireless networks, which require a continuous supply of power through transmission infrastructure (contiguous) but can also exist using intermittent transmission infrastructure, wireline networks require both power as well as contiguous physical infrastructure in the form of cables to support transmission capabilities. This makes it challenging for nations with large land masses with varied geographies or archipelagos to achieve universal coverage.

The largest countries on this list – **Canada**, the **United States** and **Australia** are yet to come close to achieving universal coverage. The US has many areas in Northern Midwest such as Montana, Dakota, Wyoming which have areas not yet brought under broadband fibre coverage. Alaska, with its challenging terrain, weather and low density is almost entirely devoid of fibre and relies on satellite and wireless technologies.

Similarly, Australia has large arid interior areas supporting small, isolated agrarian rural communities which are sans broadband coverage. Despite this, both the countries are well covered with a large majority of the population having access to broadband.

Canada shares similarities to both the US and Australia. There are many areas across the northern parts of many provinces, as well as throughout the Yukon, Northwest Territories and Nunavut, that lack fibre coverage. Even within some of those regions, satellite and wireless may be challenging due to the terrain and environment.

In contrast, the **United Kingdom** has 90% plus of its population under fibre coverage. The remaining 5-10% of the population lives in rural communities and the government is working on subsidies and incentives to private operators to cover them besides mulling over creating a public fibre network to offer universal coverage.

There is 92% of the United Kingdom's landmass covered by a good 4G signal from at least one Mobile Network Operator, while 70% of the country is covered by all four (4) operators. 5G coverage is now available from at least one operator to at least 77% of premises.

The network speeds of areas under coverage are high. As of January 2022, 64% of the United Kingdom premises had available a broadband connection with a download speed of at least 1 gigabit per second, according to the telecommunications companies' regulator, Ofcom.

Germany and **France** (excluding French overseas territories) with largely mild topography and relatively even distribution of population across the countryside boast the best coverage of broadband cables with a universal distribution across the country despite a few mountainous areas in the Alps.

Japan and **New Zealand** have most of their population in 2-3 Large Islands (New Zealand with 2 and Japan 3). There are large population centers around prominent centers with hilly interior regions with low population density and mostly rural areas. Despite this, both the countries have been able to achieve a high penetration of broadband services (Japan has a coverage rate of 99.1% of households and only 530K households are without coverage while New Zealand expects to reduce the households without coverage down to 10K in the next 2 years).

South Korea is like the United Kingdom with a small landmass and most of the population concentrated around the city of Seoul. Due to the densely concentrated and highly urbanize population, South Korea enjoys very high penetration levels across all telecommunication segments – fixed-line telephony (44% at the start of 2022), fixed broadband (46%), mobile voice and data (144%), and mobile broadband (120%).[1, 2]

Historically, South Korea had boasted some of the fastest broadband download speeds in the world (No. 2 in 2019 and No. 4 in 2020), however, according to internet speed measuring site Speedtest, as of November 2023 South Korea's average broadband download speed was 171.12 megabits per second (Mbps), ranking 34th in the world. Korea's drop in the broadband download speed rankings has been attributed to the fact that the country's wireline infrastructure was built using poorer quality hybrid fiber coaxial (HFC) cables, while countries who began building their networks after South Korea benefited by implementing faster fiber optic cables.

3.1.5 Categories of Outages

During the data collection, Gartner compiled and validated the following categories of outages:

- Environmental Factors: Natural disasters, weather, wildfires, floods, etc.
- Operational Errors: Configuration errors, procedural failures, insufficient redundancy
- Cyber Security: distributed denial of service (DDoS), ransomware, cyber-attacks, other malicious activities
- Third Party Factors: System dependencies
- Unintentional/Intentional Damage: Fibre cuts, animal damage, subsea cable cuts
- Other threats/Causes (not defined)

Understandably, jurisdictions have different resiliency focuses/scopes influenced by geographical, economic, political, and demographic differences.

3.1.6 Network Outages and Disruptions

Media Coverage Analysis

- As part of the research for this report, a review was conducted of recent outage/degradation events 9 across the jurisdictions.
- Scope of the review:
  - Events that occurred between 2018 – 2023.
  - Coverage in publicly available sources
    - Media and published reports from regulators.
- The information for each event includes several components:
  - Cause of event (operational errors, environmental factors, cyber security, third-party factors, intentional or unintentional damage).
  - Type of infrastructure impacted (wireless, wireline – terrestrial, wireline – subsea or satellite).
  - Length of outage and restoration actions.

[1] Why Korea fell 27 spots in world internet speed rankings to 32nd place last year : National : News : The Hankyoreh (hani.co.kr)

[2] Korea's internet speed ranking falls to 34th: report - The Korea Times

- Regulatory outcomes/actions.

Summary of findings related to outage types:

- Most affected type of infrastructure was wireless and wireline terrestrial.
    - The primary reason behind this was most frequently operational errors, followed by wireline and intentional damage.
- Subsea and Satellite events were less prevalent.

3.2 Deep-dive Analysis and Benchmarking

Gartner deepened and expanded the data collection for a sub-set of the larger jurisdictional list, performing a benchmark assessment of the regulations, legislation and alternative methods required to prevent and/or reduce telecommunications network outages, voluntary codes of conduct, standards and/or best practices. This sub-set deep dive included the US, UK, Australia, New Zealand, Japan, and the European Union.

3.2.1 Drivers to Improve Network Resilience

Gartner evaluated network outages and disruptions events which affected the lives and businesses of the customers receiving communication services for drivers/measures that influenced and/or improved network resilience. These included:

- Government drivers (e.g., national telecommunications regulatory compliance, encouraging investment, public safety, and emergency response).
- Industry drivers (e.g., competition, quality of service, reliability).
- Other drivers (environment/societal)

These drivers will be expanded further within the following sections.

3.2.1.1 Government Drivers to Improve Resilience

Government Drivers to Improve Telecom Resilience

Most jurisdictions have legislation enforcing mandatory incident reporting framework for service outages or disruptions. However, some jurisdictions are seeking to increase legislation and regulation to address shortcomings in service provider delivery due to preventable outages/incidents.

Table 3. Key Take-aways for Government Drivers to Improve Telecom Resilience

Defined scope for covered communication providers	▪ Categorization criteria to determine which providers are included within scope of the incident reporting framework is typically based on type of service provided or infrastructure used (e.g., satellite, wireless voice, wireless data, fixed network). ▪ For example, Germany’s framework has reporting requirements for critical infrastructure operators which are defined by network/system type (e.g., access network, backbone, sub-sea landing station, data centre).
Outage/incident thresholds	▪ Frameworks establish thresholds for reporting by type of incident (e.g., cyber security, affecting emergency calls) and/or overall impact of the incident, typically calculated by multiplying the number of customers affected by the total outage duration.
Defined reporting timelines	▪ Timelines for reporting vary across jurisdictions, between frameworks and types of incidents, however: ○ An initial notification to the regulator is typically required within 1 – 3 hours. ○ Most tiering is based on a calculation of the number of affected multiplied by the outage duration.

	○ An initial report is typically required within 2-3 days, with a final report due within weeks.
Enforcement in case of noncompliance	▪ Most jurisdictions have regulations to sanction telecommunication providers with administrative monetary penalties (AMPs) or financial penalties in case of noncompliance of service obligations and/or reporting requirements. ▪ Sanctions levied on providers is typically determined based on impact to consumers (types of services affected and number of customers affected and duration of event) and the level of negligence (was there a violation of best practices).

Drivers to Improve Network Strength & Resilience

The most common force behind improving network strength and resilience is response to outages from natural disasters and/or power failures.

Table 4. Key Take-aways for Drivers to Improve Network Strength & Resilience

Battery Backups	▪ As part of the Mobile Network Hardening Program and Strengthening Telecommunications Against Natural Disasters (STAND) program, Australia has invested in enhanced battery backup power at 467 base stations across the network. ▪ Japan has implemented mandatory backup power systems (uninterruptible power supplies and emergency generators) to protect against outages due to earthquakes and tsunamis.
Deployable Infrastructure	▪ To counter outages related to bushfires Australia has invested in deployable infrastructure such as cells on wheels (CoWs), mobile exchanges on wheels (MEoWs) and National Broadband Network Road Muster trucks.
Physical Site Hardening	▪ As part of the Mobile Network Hardening and STAND programs Australia has adopted a policy to ensure that buildings housing critical infrastructure are constructed out of fire-resistant materials. ▪ Japan's network relies heavily on buried and subsea wireline to mitigate impact of earthquakes and tsunamis.
Network Redundancy	▪ Efforts to eliminate single points of failure and build redundancy within networks was observed across all jurisdictions.

Drivers to Improve Cyber-Security and Leverage Artificial Intelligence

Historical cyber-security efforts have focused on preventing data loss/privacy at the direction of the government, however, recently providers' focus has pivoted to proactively addressing threats and leveraging emerging technology.

Table 5. Key Take-aways for Drivers to Improve Cyber-Security and Leverage Artificial Intelligence

Data loss/Privacy concerns	▪ Potential release of customer data, intellectual property, financial information, and sensitive/proprietary organizational information motivates providers to invest in cybersecurity.
Operational impact	▪ Cyber-attacks pull internal resources away from productive activities (for incident response, investigation, and remediation), and in some cases can do damage to physical infrastructure.
Financial /Reputational	▪ Outages and service degradation can lead to financial losses, legal exposure, and reputational damage. ▪ The press and publicity relating to hacks, malware events, and other cyber-activities can be influential drivers, encouraging more proactivity in this area.
Self-healing /Autonomous Networks	▪ Artificial intelligence (AI) in networking revolves around predictive analytics. It aims to resolve a problem/issue before it happens by understanding the design goal of the network and its policies; and looking at predefined metrics, traffic flows, trends, and patterns, while comparing against network baselines. ▪ The results are improved availability (>25%) and an overall reduction in operational and unintentional outages.

Drivers to Improve Network Coverage

Most jurisdictions have taken a hybrid approach to expanding network coverage. Measures include universal service obligations (USOs) and emergency service obligations. This specifically refers to the expansion of network coverage, typically through infrastructure, rather than the addition or expansion of redundancy of networks. However, redundancy could be a key consideration for all network expansions to ensure that resiliency is built into the network from the outset.

Table 6. Key Take-aways for Drivers to Improve Network Coverage

Industry Lead Initiatives	▪ Allow the TSPs to identify market and drive Initiatives to Improve Coverage in commercially feasible regions. ▪ Allow profits to incentivize the TSPs to meet the demands of customers, enhance their service offerings, and drive revenue growth through improved network coverage.
Government Supported Initiatives	▪ Intervene and support investment in regions where it is not commercially feasible for the market to service (i.e., rural regions with rugged terrain and low populations) ▪ Support new investment in infrastructure such as low earth orbit satellite, additional cell towers, and wireline infrastructure. ○ UK Government estimates around 10% of premises across the UK are not commercially viable for industry, has supported

	unserved areas through Building Digital UK's Superfast Broadband Program which will see delivery of full fibre network to these areas ○ US has launched programs such as the Broadband Equity, Access, and Deployment Program (BEAD) and Enabling Middle Mile Broadband Infrastructure Grant Program to increase broadband access to unserved and underserved communities.

Canada

Overview of Resiliency Legislation and Regulatory Frameworks (including Pending)

- The Canadian Radio-television and Telecommunications Commission (the Commission) mandate is to regulate and supervises telecommunications in the public interest and dedicated to ensuring that Canadians have access to a world-class communication system that promotes innovation and enriches their lives.
- The CRTC's mandate is established legislation and is focused on achieving policy objectives established in the *Telecommunications Act* and Canada's Anti-Spam Legislation (CASL).
- Paragraph 7b) of the *Telecommunications Act* includes a policy objective related to reliability, that can be taken into account in decision-making related to existing regulatory and legislative frameworks.
- As a result, the Commission has mandated or required implementation of Resilience and Reliability of Telecom Networks and Services in various policy proceedings that resulted in Decisions or Orders on technical and operations resiliency and reliability.
- The Commission has approved or mandated the implementation of various recommendations on technical, operational and procedural resiliency requirements and best practices developed by CRTC Interconnection Steering Committee (CISC) and its various working groups, largely the Network Working Group (NTWG), Emergency Services Working Group (ESWG) and in the Business Process working Group (BPWG).
- Proposed security-related amendments to the *Telecommunications Act* under Bill C-26 Part 1 that, if passed, would establish new authorities that enable the Government to take action to promote the security of the Canadian telecommunications system, which could include taking measures related to resiliency more broadly.
- A new policy objective would be added to promote the security of the Canadian telecommunications system, enabling the Minister of Industry and the Commission to consider this objective when exercising their respective powers under the *Telecommunications Act*.
- New order making powers for the Minister of Industry could be used to direct TSPs to take a broad range of action, subject to consultation, to secure the telecommunications system against the threat of interference, manipulation, or disruption.

Initiatives to Improve Network Strength and Resilience

- ISED has established the Canadian Security Telecommunications Advisory Committee (CSTAC) and the Canadian Forum for Digital Infrastructure Resilience (CFDIR) to advance common priorities, share information and develop best practices.
- The Telecommunications Reliability Agenda was released in September 2022 to assure that networks are reliable and resilient not just in the face of cyber-attacks but also natural disasters and human error that might cause extended network disruptions. The agenda was launched following an outage in July 2022 from one of Canada's top three

(3) telecommunications companies that lasted 15 hours or more for millions of subscribers.

- The Memorandum of Understanding on Telecommunications Reliability has now been fully operationalized following the negotiation of bilateral emergency roaming agreements and the development of internal emergency communications action plans.
- CSTAC recommendations to strengthen network resiliency were published in March 2023. ISED and government partners are in the process of reviewing these recommendations.
- Similarly, CFDIR recommendations to improve reliability and resilience of Canada's Digital Infrastructure were published in May 1, 2023. ISED and government partners are in the process of reviewing these recommendations.

Initiatives to Improve Cybersecurity

- Current initiatives fall under Canada's National Cyber Security Strategy and National cyber Security Action Plan. They are also supported by Canada's National Strategy for Critical Infrastructure and Action Plan for Critical Infrastructure.
- Proposed legislation tabled in Bill C-26 Part 2 proposes to enact the Critical Cyber Systems Protection Act (CCSPA), which would establish a regulatory framework across the telecom, finance, transport, and energy sectors.
    - The CCSPA lists vital services and systems in schedule 1, and schedule 2 would list classes of operators of those services and systems. Designated operators would have obligations under the CCSPA in relation to their critical cyber systems that underpin vital services and systems.
    - Presently, schedule 1 lists telecommunications services. The Minister of Industry would act as regulator for the telecom sector under the CCSPA.
    - Designated operators would be required to:
        - establish a cyber security programs
        - Mitigate supply-chain/third-party risks
        - Report cyber security incidents to the Communications Security Establishment, and notify the sector regulator
        - Comply with any Cyber Security Directions (order making power)

Initiatives to Improve Coverage

- ISED established Canada's Connectivity Strategy in 2019 with the objective that all Canadian's have access to broadband at speeds of 50/10 Mbps by 2030 and expanded mobile wireless coverage. ISED broadband programs including the Universal Broadband Fund (UBF) and Connect to Innovate (CTI) assist in supporting this initiative.

United States

Overview of Resiliency Legislation and Regulatory Frameworks

- FCC (Federal Communications Commission) is the primary United States (US) telecom regulatory body.
- 3 primary Acts and an Order cover regulation *(Communications Act of 1934, Telecommunications Act of 1996, FCC's 2015 Open internet Order, and Digital Equity Act 2021).*
- The Acts regulate virtually all aspects of the communications and broadcasting industry, including assignment of frequencies, rates and fees, standards, competition, terms of

subscriber access, commercials, broadcasting in the public interest, government use of communications systems.

- The Acts also provide for more detailed regulation and oversight via the FCC.
- The Acts encourage competition and entry into the industry, while regulating virtually all aspects of the communications and broadcasting industry

Initiatives to Improve Network Strength and Resilience

- The *Bipartisan Infrastructure Law* provides $65 billion in funding to help achieve the goal to connect everyone in America to affordable, reliable high-speed internet led by four agencies: the National Telecommunications and Information Administration (NTIA), the Federal Communications Commission (FCC), the Department of the Treasury, and the US Department of Agriculture (USDA).
- The Department of Homeland Security (DHS) Science and Technology Directorate's Secure and Resilient Mobile Network Infrastructure and Emergency Communications Research and Development Program provides direct research and development support for Cybersecurity and Infrastructure Security Agency (CISA) priorities to secure and make resilient 5G infrastructure, and emergency communications capabilities.
- This will help secure mobile network infrastructure for federal government missions and use-cases the capabilities of first responders' communications systems.
- The National Emergency Communications Plan (NECP) is the US's strategic plan to strengthen and enhance emergency communications capabilities.
- *Homeland Security Act of 2002*, Title XVIII requires that CISA develop the NECP to provide recommendations for supporting emergency response in the event of disasters.
- The Public Wireless Supply Chain Innovation Fund entails an investment of $1.5 billion in the development of open and interoperable networks, fostering competition, lowering costs, supporting innovation, and strengthening the 5G supply chain. A driving factor for this fund is to promote Open Radio Access Network (RAN) adoption. While this doesn't directly influence resilience, having additional entrants and flexibility across multiple manufacturers provides resilience through diversification and development of redundancy.

Initiatives to Improve Cybersecurity

- The Executive Order 13800 from 2017, on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", requires the Secretaries of Commerce and Homeland Security to "jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."

Initiatives to Improve Coverage

- The *Access Broadband Act of 2021* was established to increase access to high-speed internet by expanding broadband networks to communities in need.

United Kingdom

Overview of Resiliency Legislation and Regulator Frameworks

- Ofcom is the regulator and competition authority for the United Kingdom (UK) communications industries. It regulates the Television and Radio sectors, fixed line telecommunications, mobiles, postal services, plus the airwaves over which wireless devices operate.

- The *Communications Act 2003* is the primary legislation. The Act regulates communications providers by means of general authorizations which are required to be complied with as a condition of operating in the market.
- It requires an effective functioning Public Telephone Network, and in the event of catastrophic network breakdown, its availability/uninterrupted access for Emergencies.
- It also empowers Ofcom to implement conditions requiring providers to assist central and local government in times of emergencies.

Initiatives to Improve Network Strength and Resilience

- The UK Telecommunications Security Code of Practice is a framework established through the *Telecommunications (Security) Act* 2021 with three (3) layers: strengthened security duties on public telecommunication providers, specific security measures/requirements, and technical guidance.
- This code of practice provides detailed guidelines to large and medium-sized providers of public telecommunication providers on the preferred approach to showing compliance.
- In cases of non-compliance, Ofcom can issue a notification of contravention, identify any remedial action to be taken, and interim steps to address security gaps.
- Ofcom can also issue AMP/financial penalties. The size of the financial penalties is up to 10% of their turnover if they fail to comply with sufficient effort.
- TSPs may comply with duties and requirements by adopting different solutions or approaches than those specified in the code of practice, with Ofcom's approval.

Initiatives to Improve Cybersecurity

- The British Government National Cyber Security Centre provides advice and support for the public and private sector in how to avoid computer security threats.

Initiatives to Improve Coverage

- The United Kingdom Government's overarching strategic priority is to promote efficient competition and investment in digital networks. Promoting investment is prioritized over interventions to further reduce retail prices in the near term, recognizing longer-term benefits.
- The Government has identified a set of outcomes for achieving this strategic priority:
    - Greater regulatory stability and clarity, through the availability of longer five-year market review periods and a framework providing confidence for fair returns.
    - Regulation only where and to the extent necessary to address competition concerns and ensure the interests of consumers are safeguarded.
    - Where appropriate, a geographically differentiated approach to regulation. For areas where there is competition, there would be less need for regulation.
- The UK Government estimates that at least a third of the UK's premises are likely to be able to support three (3) or more competing gigabit-capable networks, up to half should support two or more competing networks, and there may be parts of the country that, while commercially viable for at least one operator, may not benefit from investment.
- The proposed new Electronic Communications Code (EECC) provides powers to designate areas where no operator has indicated plans to deploy and indicate additional funding will be required to ensure national coverage.
- This strategy relies on getting five things right:
    - Making the cost of deploying fibre networks as low as possible by addressing barriers to deployment, which both increase costs and cause delays;

  - Supporting market entry and expansion by alternative network operators through easy access to Openreach’s ducts and poles, complemented by access to other utilities’ infrastructure (for example, sewers);
  - Stable and long-term regulation that incentivizes competitive network investment;
  - An ‘outside in’ approach to deployment that means gigabit-capable connectivity across all areas of the UK are achieved at the same time through Government supported investment; and
  - A switchover process to increase demand for full fibre services.
- Full fibre delivery will be prioritized through the existing BDUK’s Superfast Broadband Programme, which has already provided access to over 200k premises in predominantly rural areas.
- The 2019 Telecommunications Supply Chain Review identified the need to manage and mitigate risks from high-risk vendors, introduce a new robust security framework for telecommunications, and create a more diverse and competitive supply base for telecommunications networks (5G diversification).
- The Government undertook important decisions to limit and exclude high risk vendors in United Kingdom’s telecommunications infrastructure and brought forward legislation to place those decisions on a statutory footing.
- This included supporting incumbent suppliers, attracting new suppliers, and accelerating open-interface solutions and deployment so that UK is not reliant on any single vendor.
- The UK has developed Open RAN principles, Open RAN principles - GOV.UK (www.gov.uk), which directly refer back to the Diversification Strategy, as well as ongoing government-supported work on Open RAN R&D and testing, such as SmartRAN Open Network Interoperability Centre (SONIC) Labs - Case study - GOV.UK (www.gov.uk).

Australia

Overview of Resiliency Legislation and Regulator Frameworks

- The Australian Communications and Media Authority (ACMA) is the primary telecom regulator in Australia.
- The Australian Competition and Consumer Commission (ACCC) is responsible for competition regulation.
- The ACCC assesses and enforces terms of access to the National Broadband Network (NBN), sets wholesale prices and wholesale terms of access for declared services, tracks and reports on prices and competition, and investigates claims of anticompetitive conduct.
- The *Telecommunications Act 1997* is the primary act which governs telecom in Australia covering carriers (i.e., infrastructure owners and operators) and other entities that provide services to end users, referred to as carriage service providers.
- The *Telecommunications (Consumer Protection and Service Standards) Act 1999* establishes universal service and other public interest telecom services.

Initiatives to Improve Network Strength and Resilience

- The Mobile Network Hardening Program is an Australian Government initiative (with funding) that assists the mobile network operators, infrastructure providers and managers to improve the resilience of regional mobile network telecom infrastructure to:
  - prevent outages in the event of a Natural Disaster;
  - strengthen the resilience of telecommunications facilities to allow them to operate for longer during bushfires and other Natural Disasters; and

  - enable the rapid restoration of services following an outage.
- The first stage enhanced battery backup power at 467 base stations to at least 12 hours.
- The second stage delivered more than 530 resilience upgrades at mobile base station sites for:
  - deployment of portable and permanent generators;
  - upgrading of battery systems, addition of battery extension devices;
  - improvement of transmission resilience within regional mobile network clusters to reduce single points of network failure; and
  - physical hardening of sites against bushfire damage.
- Strengthening Telecommunications Against Natural Disasters (STAND) initiative was a temporary grant provided in 2022. Its intent was to improve resilience in communities affected by severe brushfires or at risk of natural disasters, and to enhance service restoration by quickly deploying temporary facilities to address gaps caused by outages.
- The Telecommunications Disaster Resilience Innovation (DRI) Program for 2022-2025 promoted development of new technologies for resilience particularly in regional, remote and First Nations communities.
  - Round 1 was resilience against the impacts of power outages.
  - Round 2 was innovative technologies improving resiliency for natural disasters.
- These programs were intended to assist against increasing climate risks, including against an anticipated increase in the frequency and severity of natural disasters.
- The Australian Government co-invested with the telecom industry to purchase portable communications facilities including cells on wheels (CoWs), mobile exchanges on wheels (MEoWs), NBN Road Muster trucks, and portable satellite kits, for positioning in disaster affected areas to restore services quickly.
- The Government has also been providing upgraded connectivity at rural fire service depots and evacuation centres through Sky Muster satellite connections.

Initiatives to Improve Cybersecurity

- The Australian Cyber Security Centre (ACSC) of the Australian Signals Directorate (ASD) leads the Australian Government’s efforts to improve cyber security.
- The ACSC is a hub for private/public sector collaboration and information-sharing which:
  - responds to cyber security threats and incidents as Australia’s computer emergency response team (CERT);
  - private/public sector collaboration sharing threats and increase resilience;
  - increases awareness of cyber security in governments, industry, and community;
  - provides cyber security information, advice, and assistance to all Australians.
- The *Security of Critical Infrastructure Act 2018* was amended in 2021 to add obligations for Carriers and Carriage Service Providers including:
  - telling the ACSC if a cyber-security incident has a relevant impact on a critical infrastructure asset;
  - giving the Cyber and Infrastructure Security Centre of the Department of Home Affairs (Home Affairs) certain information about critical infrastructure assets so it can be included in a register.

Initiatives to Improve Coverage

- Australia’s NBN 2009 policy aimed to address Australia’s broadband availability and performance and to facilitate the structural separation of Telstra by providing an optic fibre alternative to its copper network.
- The NBN is being built and run by a government-owned enterprise, nbnTM.
- A fundamental policy setting is that nbnTM provides only wholesale services to retail service providers (RSPs) and does not serve end-users.

- The original NBN plan was to reach 93% of premises with an optic fibre connection. The remaining 7% of premises would be served by either a new satellite service or terrestrial fixed wireless service.
- The NBN regulatory framework was set up with two Acts:
  - *National Broadband Network Companies Act 2011*
  - *Telecommunications Legislation Amendment (National Broadband Network Measures—Access Arrangements) Act 2011*
- Recently, the Australian Government committed to invest $2.4 billion to enable an additional 1.5 million homes and businesses currently served by Fibre to the Node (FTTN) to upgrade to Fibre to the Premises (FTTP).
- FTTP is viewed as better than FTTN (higher speeds/reliability), and both are better than copper as they are faster, better over long distances, have greater bandwidth, are more scalable, and are more reliable/stable.
- These upgrades will help deliver faster broadband speeds, better reliability, are more energy efficient and support the provision of additional data capacity.

New Zealand

Overview of Resiliency Legislation and Regulator Frameworks

- The Ministry of Business, Innovation and Employment (MBIE), the New Zealand Commerce Commission and the Telecommunications Carrier Forum (TCF), play key roles in the legislation, regulation, and provision of telecommunications services for New Zealand.
- The *Telecommunication Act 2001* acts as the basis for regulation and legislation and enables the Commission to regulate the provision of telecommunication services.

Initiatives to Improve Network Strength and Resilience

- The Rural Capacity Upgrade program will see existing cell towers upgraded and new towers built in rural areas experiencing poor performance, as well as fibre, additional very high bit-rate digital subscriber line (VDSL) coverage and other wireless technology deployed in congested areas.
- The Remote Users Scheme will equip as many remote households as possible with the connectivity infrastructure needed to access broadband services.
- The Mobile Black Spots Fund (MBSF) is providing greater mobile coverage on approximately 1,400 kilometres of state highways and in over 168 tourism locations where no coverage currently exists.

Initiatives to Improve Cybersecurity

- The primary government body involved in setting up cybersecurity policy in New Zealand is Department of the Prime Minister and Cabinet (DPMC).
- The Cyber Security Emergency Response Plan (CSERP) sets the framework for the government’s response to a cyber security emergency. This outlines roles, responsibilities, the government approach, coordination, and ensures services and operations are restored swiftly and appropriate lessons are identified and acted upon.
- The CSERP is part of New Zealand’s broader National Security System (NSS), is maintained by the DPMC and is authored in collaboration with other agencies with a role in cyber security.

Initiatives to Improve Coverage

- The Ultra-Fast Broadband (UFB) program was setup to provide around 87% of New Zealanders, in over 390 towns and cities, access fibre by the end of 2022.
- Almost $1.8 billion has been invested in the Ultra-Fast Broadband (UFB) infrastructure.
- Crown Infrastructure Partners was established as a Crown company initially to manage the Government's investment in UFB.
- Ultra-Fast Broadband (UFB) uses fibre optic cables to deliver fibre-to-the-premises. It is most suitable in urban areas with higher population densities.
- Following the effective rollout of fibre and additional submarine cable links, New Zealand is now well above the Organisation for Economic Co-operation and Development (OECD) average and similarly placed to the US with internet speeds averaging 33Mbps.

Japan

Overview of Resiliency Legislation and Regulator Frameworks

- The Ministry of Internal Affairs and Communications (MIC) is the telecommunications regulator (specifically the Telecommunications Bureau).
- Its role includes formulating policies, issuing licenses, managing radio frequencies, promoting competition, protecting consumer rights, and ensuring smooth operations.

Initiatives to Improve Network Strength and Resilience

- Japan has a robust earthquake early warning system that issues alerts to the public and helps prevent disruptions to telecommunications infrastructure.
- Multiple-address wireless communication, house receivers and radios are used to transmit information to local communities through sirens and speakers and other means.
- L-Alert is a system which converts information from public organizations into XHL, email and other formats, and transmits it to the media and communications companies.
- Japan uses movable and deployable ICT resource units (MDRU), which have comms, information processing and storage devices mounted on a mobile container or vehicle.
- Regional government bureaus have founded fixed stations, many which have portable satellite communications systems.
- Telecommunication providers in Japan are required to have backup power systems in place, including uninterruptible power supplies (UPS) and emergency generators.
- To minimize and protect against earthquakes/disasters, a significant portion of the telecommunication infrastructure, including fibre optic cables, is installed underground.

Initiatives to Improve Cybersecurity

- The Cybersecurity Policy for Critical Infrastructure Protection is a common action plan shared between the government, responsible for promoting independent measures, and CI operators which independently carry out relevant protective measures.
- Japan's *Basic Act on Cybersecurity* stipulates critical infrastructure operators, and some telecom carriers, shall endeavor to voluntarily and proactively secure cybersecurity and to cooperate with cybersecurity measures implemented by government.
- Under the Telecommunications Business Act, service operators have obligations to protect the secrecy of telecommunications, and to maintain/operate facilities in compliance with technical standards established by the MIC.
- The NSS is the principle for Japan's national security strategy, defining diplomatic and defense strategies in response to the new security environment.
- The NDS defines the Japan Self-Defense Force's (JSDF) defense strategy, setting goals for national security and outlining approaches and means to achieve them.

- The Defense Buildup Program indicates a medium- to long-term development plan that includes the level of defense capability and the procurement plan.

Initiatives to Improve Coverage

- The 2020 national coverage rate for household fibre optic broadband was 99.1%.
- The current government aims to increase the area under fibre coverage to more than 99.9% of the country's landmass by 2028.

European Union

Overview of Resiliency Legislation and Regulator Frameworks

- The Body of European Regulators for Electronic Communications (BEREC) is the regulator for the European Union (EU). It consists of representatives from the national regulatory authorities (NRAs) of each EU member state.
- Its primary role is to promote the consistent application of the EU regulatory framework for electronic communications, ensure competition, and safeguard the interests of consumers and end-users.
- BEREC provides guidance and advice to the European Commission, assists in the development of common approaches to regulation, and contributes to the harmonization of the telecommunications sector across the EU. The BEREC Regulation outlines the tasks, powers, and composition of BEREC.
- The European Electronic Communications Code (EECC) is a comprehensive regulatory framework for electronic communications in the European Union. The EECC sets out rules for electronic communications networks and services, spectrum management, access to networks, consumer protection, and competition. It requires providers to ensure the security and integrity of their networks, implement appropriate security measures, and have incident response capabilities in place.

Initiatives to Improve Network Strength and Resilience

- Electronic communication providers in the EU are required to notify incidents that have a significant impact on the continuity of electronic communication services to the telecommunications NRAs in each EU member state.
- Every year the NRAs report a summary to the European Union Agency for Cybersecurity (ENISA), covering a selection of these incidents (the most significant incidents, based on a set of agreed EU-wide thresholds).
- The mandatory reporting of incidents had a specific focus on security incidents with a significant impact on the functioning of each category of telecommunication services.
- Over the years, the regulatory authorities have agreed to focus mostly on network/service outages (type A incidents – Service outage, e.g., continuity, availability – an outage caused by a cable cut caused by a mistake by the operator of an excavation machine used for building a new road would be categorized as a type A incident).
- This would exclude from the scope of these reports targeted attacks, e.g., those involving the use of Signaling System 7 (SS7) protocol vulnerabilities, SIM Swapping frauds, or even more extended attacks that nevertheless do not cause outages.
- Telecommunications security incidents that are reported to national authorities are only the major incidents, i.e., those with significant impacts. Smaller incidents, affecting small percentages of population such as SIM Swapping attacks are not reported.
- In addition, there are more services within the scope of the EECC, including not only traditional telecommunications operators but also, for example, over-the-top (OTT)

providers of communications services (such as messaging services like Viber and WhatsApp).

- Annual reporting guidelines combine quantitative and qualitative parameters as well as the notification of security incidents affecting not only the services of fixed and mobile internet and telephony, but also number-based interpersonal communications services and/or number independent interpersonal communications services (OTT communications services).

Initiatives to Improve Cybersecurity

- The European Union focused on regulating cyber resiliency of electronic communication providers within the EU's telecommunications regulatory framework.
- It expanded through the Directive on Security of Network and Information Systems (NIS Directive) to Operators of Essential Services and Digital Service Providers that include particularly digital infrastructure providers and cloud computing services.
- The European Union Agency for Cybersecurity (ENISA) is an independent and key agency of the EU, with a primary mission to enhance cybersecurity in Europe and help Member States and EU institutions in their efforts to improve their resilience to cyberthreats.
- The NIS Directive is EU-wide legislation on cybersecurity, with the objective of achieving a high common level of cybersecurity for all Member States. One of the three (3) pillars of the NIS Directive is the implementation of risk management and reporting obligations.
- ENISA evaluates and measures each year the NIS impacts on cybersecurity.
- NIS2 entered into force in 2023, and improves the existing cyber security level by:
  - Creating the necessary Cyber Crises Liaison Organisation Network (CyCLONe).
  - Increasing the harmonization level of security requirements/reporting obligations.
  - Encouraging introduction of supply chain, vulnerability management, core internet and cyber hygiene in member state national cybersecurity strategies.
  - Bringing in peer reviews for enhancing collaboration and knowledge sharing.
  - Including more sectors which means that more entities are obliged to take measures to increase their level of cybersecurity.
- The Cyber Resilience Act puts in place minimum cybersecurity requirements for products and software that are placed on the single market regardless of where they are produced.
- While it will be possible to make self-declarations of conformity for 90% of the products, for about thirty products, the conformity examination will have to be carried out by a third party. The Commission will be able to request the withdrawal from the market of a product that presents a cyber risk.
- The EU continues to ensure the implementation of the 5G cybersecurity toolbox to deploy secure networks. All Member States have unanimously agreed to exclude so-called high-risk providers from their networks (CORE and RAN).

Initiatives to Improve Coverage

- Connecting Europe Facility (CEF) is a program aimed at promoting the development of high-performing, sustainable, and interconnected digital infrastructures across member states. It provides financial support for projects related to broadband deployment, 5G networks, public Wi-Fi, and other digital services, with the goal of improving coverage and connectivity.
- Broadband Europe promotes connecting European citizens and businesses with very high-capacity networks, including Gigabit connectivity for all the main socio-economic drivers, uninterrupted 5G coverage for all urban areas and major terrestrial transport

paths, and access to connectivity offering at least 100 Mbps for all European households.

- The ambition of the Europe Digital Decade is that by 2030 all European households are covered by a Gigabit network, and all populated areas are covered by 5G.

3.2.1.2 Industry Drivers to Improve Resilience

Competition, consumers, market trends, and technology drive industry investment in telecommunications resilience. Across the jurisdictions, efforts tend to be reactive with evidence of proactivity when network access has been impeded/disrupted or the impact is felt commercially/reputationally.

Table 7. **Key Take-aways for Industry Drivers to Improve Telecom Resilience**

Competition	▪ Resilience can provide a competitive advantage in the telecommunications industry. Providers that can offer reliable and robust connectivity solutions are more likely to attract and retain customers. By enhancing resilience, telecom providers differentiate themselves.
Increasing reliance on connectivity and technology	▪ Businesses and individuals depend heavily on seamless and reliable connectivity for communication, data transfer, and accessing critical services. This dependence drives the need for resilient telecommunications to ensure uninterrupted connectivity, even in the face of disruptions.
Customer expectations	▪ Businesses and consumers expect connectivity. Network outages and service disruptions can have financial and reputational implications for service providers, driving customers to the competition.
Remote work and digital transformation	▪ The COVID-19 pandemic accelerated the adoption of remote work and digital transformation across businesses, organizations, and governments. As more organizations continue with remote work, and rely more on cloud-based services, the need for telecommunications resiliency is even more critical.
Future technologies	▪ The deployment of emerging technologies such as 5G, Internet of Things, and AI will place additional demands on telecommunications. Industry will continue to invest in these technologies and support those revenue streams.
Industry collaboration/ Peer-pressure	▪ The development of industry standards and best practices through industry groups, both within a jurisdiction, as well as multi-jurisdictional (e.g., ENISA in the European Union) will continue to foster advancements and improvements in resilience.

Largest Telecommunications Service Providers (TSP)/Internet Service Providers (ISP):

As noted in Section 3.1.3 Jurisdictional Communication Service Providers, all jurisdictions scanned have three (3) or more major service providers/carriers delivering telecommunications services.

Drivers for industry are across all motivators. Overall, the drivers for the telecommunications industry to improve resilience revolve around meeting customer expectations, differentiating against competition, complying with regulations, safeguarding against cybersecurity threats, ensuring business continuity, and capitalizing on market opportunities.

Service providers have greatest motivation to improve where there is financial benefit, short- and long-term.

3.2.1.3 Other Drivers to Improve Resilience

Other drivers include elements such as environmental and/or climate change, the impact of COVID-19/remote work and digital transformation. Environment/climate tends to be more unexpected and affects availability and performance.
Environmental and Climate Change drivers are usually more unexpected while typically cause more significant affects. Natural disasters can have devastating effects on countries and their citizens, exacerbated by disruptions and loss of telecommunications.

Table 8. Key Take-aways for Other Environmental/Societal Change Drivers

Increased frequency and intensity	▪ Rising sea levels, storms, and coastal erosion can threaten coastal telecommunication infrastructure. Additionally, heatwaves, prolonged droughts, and wildfires can damage network equipment. ▪ Countries are experiencing these conditions with greater occurrence and severity. ▪ E.g., Australia continues to suffer from more frequent and more severe network disruptions due to weather events and wildfires.
Adaptation to changing conditions	▪ Environmental drivers also necessitate adaptation to changing conditions. Telecommunications providers may need to modify network infrastructure or deploy additional resources in areas prone to specific environmental risks. ▪ E.g., New Zealand has been more proactive in its response to handling the fallout of natural disasters as was evidenced in the recent cyclone Gabrielle, seeing an increased penetration of satellite devices in the rural and isolated communities.
Monitoring and early warning systems	▪ Organizations' abilities to monitor and predict environmental changes to greater accuracies will enable increased proactivity in addressing vulnerabilities and plan for future resilience measures for telecommunications networks. ▪ E.g., Japan witnesses strong and frequent earthquakes, accompanying Tsunamis, volcanic eruptions, hurricanes, and strong Typhoons. Japan has developed disaster information

	sharing systems and frameworks, satellite communication for redundancy, mobile towers, and early response teams.
Remote work and digital transformation	- The COVID-19 pandemic accelerated the adoption of remote work and digital transformation across businesses, organizations, and governments. As more organizations continue with remote work, and rely more on cloud-based services, the need for telecommunications resiliency is even more critical.

The **United States** with its diverse geography experiences a wide range of natural disasters including hurricanes, wildfires, tornadoes, floods, winter storms, and earthquakes. As such the US has developed several frameworks and initiatives in response including the Disaster Information Reporting System (DIRS), a voluntary reporting system, the National Infrastructure Protection Plan to enhance critical infrastructure, the Wireless Resiliency Cooperative Framework (encouraging wireless providers to coordinate during emergencies) and other State and local initiatives (e.g., task forces, regulations/guidelines). The US also has specific initiatives to address hazards such as hurricanes and wildfires (e.g., Wireless Emergency Alerts [WEA], Fire Management Assistance Grants [FMAGs]).

The **United Kingdom** has experienced severe storms and flooding events in recent years, causing significant damage and disruption. In winter months, the UK has encountered extreme cold waves bringing heavy snowfall, sub-zero temperatures, and strong winds, leading to challenges for infrastructure and utilities. The UK is not typically prone to large-scale natural disasters like earthquakes or tsunamis. Like most countries the UK has several early warning systems in place to mitigate against severe weather activities.

Australia has suffered network disruptions due to weather events and wildfires and historically has lagged the other nations on this study in terms of network resilience in the face of natural disasters. There is less infrastructure to cater to rural areas and not many government initiatives to address this. Though that has changed in the last decade with government stepping up with spending on programs such as the Telecommunications Disaster Resilience Innovation Program and creating broadband infrastructure. Moreover, Australia’s countryside has a high penetration of satellite communication devices and infrastructure in the countryside which adds to the network resilience.

Like Australia, **New Zealand** also lagged other countries on this list till recently, but the NZ Government has stepped up and is incentivizing private companies to create resilient infrastructure. Additionally, the government is also proactive in its response to handling the fallout of natural disasters as was evidenced in the recent cyclone Gabrielle. Like Australia, New Zealand too has a high penetration of satellite devices in the rural and isolated communities.

Japan is the county on the list most prone to disasters. Situated on the Pacific ring of fire, Japan witnesses strong and frequent earthquakes due to tectonic activity, accompanying Tsunamis as well as volcanic eruptions. Japan also has a hurricane season and witnesses strong Typhoons. Due to this Japan has a very strong infrastructure in place to tackle these challenges – pervasive early warning and detection systems across the county, disaster information sharing systems and frameworks, satellite communication networks for redundancy, mobile transmission towers and early response teams always on standby with the private telecommunications operators. Moreover, Japan's undersea cables are situated in bays which are relatively less prone to natural disasters. Network Resilience of Japan in the face of the specific threat posed by natural disasters is exemplary.

The **European Union** with its diversity across 27 member countries, has a wide range of environmental and climate issues. Several countries in Europe have faced severe storms and flooding over the past several years, notably UK, Germany, Poland, France, and others. Wildfires have been more prevalent as well, notably across Greece, Portugal, Spain, Italy, and Sweden. Winter storms and cold waves have affected several parts of Europe as well, with greater frequency. Each country has its own mechanisms and resources in place to respond to natural disasters often in coordination with the EU's Civil Protection Mechanism and Emergency Response Coordination Center (ERCC), which facilitates cooperation among member states during emergencies. The EU has also developed the EU Adaptation Strategy that sets out how the European Union can adapt to the unavoidable impacts of climate change and become climate resilient by 2050. The Strategy has found principal objectives: to make adaptation smarter, swifter, and more systemic, and to step up international action on adaptation to climate change.

Gartner has developed research for enterprises seeking to mitigate the risks of climate change. Climate adaptation creates business resilience in response to a changing climate. Organizations, including Telecommunications providers, need to use scenario models and risk assessments to identify and respond to climate threats while protecting revenue and the enterprise's reputation.

Another driver affecting all jurisdictions is the impact of the COVID-19 pandemic and the acceleration of the adoption of remote work and digital transformation across businesses, organizations, and governments. As more organizations continue with remote work, and rely more on cloud-based services, the need for telecommunications resiliency is even more critical. This increased demand and traffic, particularly high-speed internet connectivity, can strain network capacity. Shifting usage patterns can place lead to changes in peak usage times and higher bandwidth requirements during specific periods of the day, reducing maintenance windows for service providers. The decentralization of the workforce has placed higher demands on widespread infrastructure for reliability, redundancy, and resilience, where previous focuses may have been on urban centers and city downtown centres.

3.2.2 Regulatory Obligations

Telecommunications Service Providers (TSPs) are subject to various regulatory obligations typically established in legislation by each jurisdiction through legally binding rules and regulations. These obligations may take the form of laws, regulations, rules, permits, licenses, reporting requirements, or other forms of legal mandates. They often include provisions for monitoring, enforcement, and penalties for non-compliance.

Compliance and conformance measures can be imposed due to a TSP's failure to provide service during an outage or when service targets are missed on recovery. They are also typically imposed if a TSP is non-compliant to regulatory obligations in providing emergency services. These measures all work to prevent, reduce, and assist recovery from network outages.

Table 9. Key Take-aways for Regulatory Obligations

Essential communication services accessible to all citizens	▪ All jurisdictions have adopted some form of a universal service obligation and/or emergency service obligation. ▪ Select TSPs are responsible for providing basic services (typically voice, Internet access, and emergency services) to all citizens. ▪ Costs for this is typically funded in part by imposing a levy on the TSPs who are not charged under the service obligation. ▪ Most universal service obligations relate to voice service however, some are starting to introduce broadband service as a basic service.
Outage notification systems/incident reporting controls	▪ Most jurisdictions have a mandatory incident reporting framework, with variations, but have three (3) common elements. 1. Defined scope of covered communication providers - typically categorized based on type of service provided or infrastructure. 2. Outage/incident thresholds – categorized by type of incident and/or impact of the incident (the number of customers affected multiplied by the total duration of the outage event). 3. Defined reporting timelines – timeline for initial notification typically 1-3 hours depending on severity of issue incident.
Penalties	▪ Many jurisdictions have regulations to sanction TSPs with AMP/financial penalties in case of noncompliance. • Sanctions levied are determined based on impact of the violation on consumers (types of services affected, number of customers affected and duration of event) and level of negligence (was there a violation of best practices). ▪ However, none of the jurisdictions interviewed had defined frameworks for determining values of potential fines.

Canada

Universal Service Obligation

The Universal Service Obligation (USO) in Canada aims to ensure that all Canadians have access to affordable and reliable telecommunications services, including both voice and broadband internet. The CRTC has set specific targets for these services to be available to all Canadians, regardless of their location.

Regarding voice services, the CRTC has established a universal service objective that requires all Canadians to have access to reliable and affordable internet access and local voice services, including access to emergency services.

Emergency Calls

Canada has developed specific Telecom Regulatory Policies which sets out the Commission’s 9-1-1 action plan for reliability and resiliency of the 9-1-1 networks, including notification to 9-1-1 call centres of network outages that may affect them.

All carriers that are 9-1-1 network providers must take all reasonable measures to ensure that their 9-1-1 networks are reliable and resilient to the maximum extent feasible. This should have an adequate combination of industry best practices that should generally include:

- 9-1-1 network design principles.
- 9-1-1 operation and maintenance practices.
- Contingency plans for disaster or outage recovery of 9-1-1 networks.
- 24/7 monitoring of 9-1-1 networks.

The Commission also established a framework for notification process to ensure that (i) parties that are directly required to take action to restore service are able to do so quickly, and (ii) parties can inform the public of alternative measures to access emergency services if the time to repair the outage is lengthy.

In terms of next generation 9-1-1 (NG9-1-1) services, this includes the ability to (i) reroute traffic to alternative public safety answering points (PSAPs) in the event that a PSAP is not able to respond to 9-1-1 calls; (ii) maintain reliability and performance of the network even when demarcation points, call handling systems, and telephones are separated by a large geographical distance; and (iii) procure interoperable equipment and services from different vendors that all adhere to the Commission-approved National Emergency Number Association (NENA) i3 Standard for NG9-1-1 (i3 standard).

The Commission also directed NG9-1-1 network providers to include in their NG9-1-1 service agreements specific mandatory requirements for PSAPs to interconnect with the NG9-1-1 networks to ensure compatibility between the NG9-1-1 networks and PSAP networks, as well as to ensure reliability, resiliency, and security measures for NG9-1-1 and interconnecting networks.

Outage Notification and Incident Reporting

The Commission has launched a process to develop a framework to improve the reliability and resiliency of telecommunications networks. In the first stage of this process, the Commission launched a Notice of Consultation proceeding to seek comments on a proposal to require all Canadian carriers to notify the Commission, ISED, and other relevant authorities of major service outages; and to submit a comprehensive post-outage report to the Commission.

On an interim basis pending the outcome of the Notice of Consultation 2023-39 proceeding, the Commission directed all Canadian carriers, on an interim basis, to provide the following information to the Commission, effective 8 March 2023:

- Carriers must notify the Commission within two hours of when the carrier becomes aware of a “major service outage,” defined for the purposes of this interim measure, as any outage affecting (i) more than 100,000 subscribers or a material portion of the carrier’s subscribers for more than one hour, (ii) subscribers that are in a geographic area served only by the affected carrier, (iii) critical infrastructure, (iv) major transport facilities, or (v) a 9-1-1 network.
- Carriers must provide to the Commission, within 14 days of the day the Commission was notified of a major service outage (as required by item a above), a comprehensive report detailing (i) the causes of the outage, (ii) the steps taken to resolve the outage, (iii) how emergency and accessibility services (including those tailored for Deaf, hard-of-hearing, or visually impaired persons) were specifically affected by the outage, and (iv) plans put in place to prevent similar outages in the future.

The Commission also indicated it will initiate additional public proceedings to address network resiliency in broader terms (e.g., network resiliency principles, emergency services (9-1-1), public alerting, consumer communication, consumer compensation, accessibility, technical measures, and the imposition of administrative monetary penalties).

The information about the service outages in Canada is posted in the public domain on the following CRTC webpage: CRTC: General Information - Service Outages: 8000-C12-201909780.

Remediation Plans

Like other jurisdictions, the CRTC can apply various remediation plans to address issues and ensure compliance from TSPs. While the specific plans can vary based on the nature of the problem, measures and actions include requirements to meet coverage obligations, improve service levels, or investment in infrastructure to improve service quality. Most remediation plans include mandatory monitoring and reporting to ensure plans are adhered to and outcomes are realized within the outlined timeframes. In some cases, additional audits may be identified.

Additionally, there is proposed legislation tabled in Bill C-26. Parts 1 and 2 include Administrative Monetary Penalties (AMPs) and offence regimes for non-compliance (provisions are subject to Parliamentary consideration).

Administrative Monetary Penalties/Fines and Penalties

The CRTC has the ability to apply **Administrative Monetary Penalties** (AMPs) to telecommunications service providers. As indicated above, there is proposed legislation tabled in Bill C-26. Parts 1 and 2 include AMPs and offence regimes for non-compliance (provisions are subject to Parliamentary consideration).

User Compensation

Canada does not have an obligation for telecommunication providers to compensate customers for service outages. Entitlement to compensation is dictated by the specific circumstances of the outage and the contractual agreement between service providers and their customers.

United States

Universal Service Obligation

Universal service is a cornerstone of the law that established the Federal Communications Commission (FCC), the *Communications Act of 1934*. Since that time, universal service policies have helped make telephone service ubiquitous, even in remote rural areas. Today, the FCC recognizes high-speed internet as the 21st Century's essential communications technology and is working to make broadband as ubiquitous as voice, while continuing to support voice service.

The Act established principles for universal service that specifically focused on increasing access to evolving services for consumers living in rural and insular areas, and for consumers with low incomes.

Emergency Calls

The Wireless Communications and Public Safety Act of 1999 (911 Act) took effect in October 1999 with the purpose of improving public safety by encouraging and facilitating the prompt deployment of a nationwide, seamless communications infrastructure for emergency services. One provision of the 911 Act directs the FCC to make 911 the universal emergency number for all telephone services.

The FCC has taken several steps to increase public safety by encouraging and coordinating development of a nationwide, seamless communications system for emergency services. The FCC has designed and established transition periods to bring the nation's communications infrastructure into compliance.

To deliver emergency help more quickly and effectively, the carriers and public safety entities are upgrading the 911 network on a regular basis. For example, most 911 systems now automatically report the telephone number and location of 911 calls made from wireline phones, a capability called Enhanced 911, or E911.

The FCC also requires wireless telephone carriers to provide 911 and E911 capability, where a Public Safety Answering Point (PSAP) requests it. Once it is implemented fully, wireless E911 will provide an accurate location for 911 calls from wireless phones.

Other FCC rules regulate 911 for Voice over Internet Protocol (VoIP), mobile satellite services, telematics, and telecommunications devices for the Deaf (TDD). The 911 requirements are an important part of FCC programs to apply modern communications technologies to public safety.

Outage Notification and Incident Reporting

Within the scope of FCC’s mandate, the organization is responsible for administration of two separate telecommunication outage notification/incident reporting databases and reporting systems, Network Outage Reporting System (NORS) and Disaster Information Reporting System (DIRS).

NORS is a mandatory reporting system that allows the FCC to collect information on significant communications service disruptions that could affect homeland security, public health or safety, and the economic well-being of the nation. The scope of communication providers covered under the NORS mandate includes wireline, cable, satellite, wireless, interconnected VoIP, and Signaling System 7 providers. NORS framework includes thresholds/guidelines that determine if the provider is required to an incident or not. These guidelines include but are not limited to incidents that disrupted 900,000 user-minutes or incident that impacted E911 services. Under the Mandatory Disaster Response Initiative, providers are required to report outages and restoration activities through FCC portals (i.e., NORS).

Reporting Guidelines for communication providers are as follows:

- Wireline, cable, satellite, wireless and Signaling System 7 providers:
    - Submit a NORS notification within 120 minutes of receiving preliminary information about the outage,
    - Submit an initial outage report within three (3) calendar days of the outage,
    - Submit a final report no later than 30 days are the discover of the outage.
- VoIP Providers:
    - Submit a NORS notification either within 240 minutes after discovering an outage that potentially affects a 911 facility or within 24 hours of discovering an outage which affects potentially 900,000 user minutes and results in a complete loss of service or potentially affects any special offices and facilities (which include any facility enrolled in the Telecommunications Service Priority (TSP) Program at priority Levels 1 and 2).
    - Submit a final report within 30 days of discovering the outage.
- Covered 911 service providers, or providers that aggregate 911 traffic from an originating service provider and deliver it to a 911 call center:
    - Must notify the designated official at the 911 call center no later than 30 minutes after discovering an outage that affects a 911 call center.

    - Must also communicate additional material information to the affected 911 call center as it becomes available, but no later than two hours after the initial contact.

Information and data collected by NORS is used by the Public Safety and Homeland Security Bureau’s Cybersecurity and Communications Reliability Division (CCR) to assess the impact of major outages, identify trends, and create best practices that can prevent or mitigate future outages.

DIRS is a voluntary web-based reporting/notification system that the FCC established in the wake of the Hurricane Katrina natural disaster. The purpose of DIRS is to enable the collection of operational status and restoration information from communications providers (including wireline, wireless, broadcast, cable, interconnected VoIP, and broadband service providers) during major disasters and subsequent recovery efforts. Additionally, DIRS providers communication providers with a channel to request assistance during these events.

The FCC compiles the data and provides network status information to federal emergency management officials as well as publishes public reports of aggregated restoration information. The FCC’s analysis of DIRS data informs restoration efforts led by federal partners and the agency’s own assessments of communications reliability during disasters.

DIRS is only activated by the FCC preceding an anticipated major emergency, like a major hurricane, or following an unpredictable disaster. The FCC announces DIRS activations through public notices and emails to DIRS participants.

Remediation Plans

In addition to the CCR’s role as administrators of the NORS and DIRS reporting systems, the CCR is also responsible for promoting network improvements through incident investigations, stakeholder-driven processes, and rulemakings. As a result of the incident investigation the CCR may issue a compliance plan to the TSPs involved in the incident.

The structure and content within a compliance plan differs depending on the circumstances surrounding the incident, however, the goal of all compliance plans is to ensure the Largest TSPs staff understand the causes of the incident and are aware of mitigating factors. Typically, compliance plans address topics such as operating procedure, development of compliance manuals and checklists, continuous improvement plan (training and review of compliance material), overview of best practices and remediation roadmap (time frame is typically between 30 - 90 business days).

Administrative Monetary Penalties/Fines and Penalties

- Fines related to network outages that blocked 911 calls: The FCC issued $6 million in fines across AT&T, CenturyLink (now Lumen Technologies), Intrado and Verizon. The fines generally focus on whether the providers were able to support 911 calls as well as whether they alerted the FCC and 911 operators in a timely manner about outages.
- Fines for Non-Utilization of Allocated Spectrum: Verizon Communications Inc. VZ.N and its Straight Path Communications Inc. unit paid a $614 million civil penalty to the FCC. The telecommunications regulator said the settlement resolved an investigation into allegations that Straight Path failed to use the spectrum it was awarded, and in doing so violated the FCC’s rules in connection with approximately 1,000 licenses.

User Compensation

Under US law, there is no general obligation for telecommunication providers to compensate customers for service outages. The FCC does not mandate automatic compensation, rather, entitlement to compensation is dictated by the specific circumstances of the outage and the contractual agreement between service providers and their customers.

United Kingdom

Universal Service Obligation

The *Communications Act 2003* also provides for provisions to ensure quality of service to customers in the form of the Telephony Universal Service Legislation and it sets out a minimum set of services that must be provided to everyone, on request, at an affordable price.

In March 2018, the Government introduced legislation, *The Electronic Communications (Universal Service) (Broadband) Order 2018*, for a broadband universal service obligation, to give homes and businesses the right to request a decent and affordable broadband connection.

Emergency Calls

Ofcom also has a monitoring program to see whether telecommunications providers are complying with their emergency call obligations as the United Kingdom (UK) migrates from an analog to digital phone system.

Digital voice services use the same fibre cables as broadband services, improving voice quality for customers and reducing cost, complexity, and energy consumption for Telecommunications Service Providers (TSPs).

The only change that end-users should expect to see is that they plug their handset into their router rather than a specific socket in the wall.

Since digital calls are reliant on electricity, Telecommunications Service Providers (TSPs) will be required to make their power systems more reliant as well.

Outage Notification and Incident Reporting

Under Section 105K of the *Telecommunications (Security) Act 2021*, requires providers to inform Ofcom any security compromises, which are defined as “anything that compromises the availability, performance or functionality of the network or service.”

Note for this assessment, the scope is for telecommunication providers and not Operators of Essential Services (OES). It should be noted that OES can have a significant impact and influence on telecommunications resilience and should be considered as part of a wider resilience strategy (e.g., Ofcom has guidance for OES under their digital sub-sector for Domain Name System (DNSs), top-level domains (TLDs) and Internet exchange points (IXPs), EU and Germany include thresholds for such domains as DNSs, TLDs and IXPs).

Under Section 105A of the *Telecommunications (Security) Act 2021*, the scope of security compromise includes several situations including network or service outages, and cybersecurity incidents. Security compromises that are deemed reportable to Ofcom are defined as follows:

- Any security compromises impacting service availability, which meet the thresholds set out in the table below.
- Any security compromises affecting networks or services involved in connecting emergency calls (e.g., Call Handling Agent platforms, emergency call routing) and leading to a reduction in the usual ability to answer or correctly route calls.
- Any security compromises that the provider is aware of that has a link to a potential loss of life.
- Any security compromises involving significant cyber security breaches.
- Any security compromises reported to other Government agencies or departments.

- Any security compromises that providers are aware of being reported in the media (local, national or trade news sources).

Table 10. Fixed network numerical thresholds

Network/service type	Minimum number of end customers affected	Minimum duration of service loss or major disruption
Fixed network providing access to the emergency services	1,000	1 Hour
Fixed network providing access to the emergency services	100,000	Any Duration
Fixed voice or data service/network offered to retail customers	10,000 or 25% (see Note 2 below)	8 Hours
Fixed voice or data service/network offered to retail customers	100,000	1 Hour

Notes on table above:

1. A customer is affected if the main functions of a network or service are not available to them due to the security compromise.
2. This threshold should be interpreted as either 10,000 end customers or 25% of the provider's total number of end customers on the affected service, whichever is the lowest number.

Table 11. Mobile network numerical thresholds

Network/service type	Minimum number of end customers affected	Minimum duration of service loss or major disruption
Mobile network providing access to the emergency services	1,000	1 Hour
Mobile network providing access to the emergency services[2]	100,000	Any Duration
Mobile virtual network operator voice or data service/network offered to retail customers[3]	25% (see Note 3 below)	8 Hours
Mobile network operator voice or data service/network offered to retail customers	See notes[4]	

Notes on above:

1. A customer is affected if the main functions of a network or service are not available to them due to the security compromise.
2. A Mobile virtual network operator (MVNOs) should report security compromises affecting its end customers, even where security compromises are the result of a failure in its host mobile network operator's (MNO's) network. In this case, the third party's details should be provided.

3. This threshold should be interpreted as 25% of the provider's total number of end customers on the affected service.
4. Due to the inherent difficulty in determining the exact number of end customers affected by a security compromise in mobile networks, Ofcom has agreed a reporting process with each of the four UK mobile operators which is based on their individual definitions of a major service failure (MSF). Network MSFs are security compromises which have a significant impact on the network and are raised to senior management within the MNO. The ultimate intention is to ensure reporting of mobile security compromises which cause similar levels of customer disruption to those reportable on fixed networks. The agreements are intended to ensure consistency between MNOs in reporting and in the calculation of customer impact. Ofcom will periodically review the criteria for reporting with MNOs to maintain this consistency between MNOs and between mobile and fixed networks.

The *Telecommunications (Security) Act 2021* further delineates security compromises into urgent and non-urgent categories. Security compromises should be considered as “urgent” if they meet any of the following criteria:

- All security compromises involving significant cyber security breaches that are reportable under the "Reportable security compromises” criteria above and which require urgent remedial action.
- Security compromises affecting services to 10 million or more end users.
- Security compromises affecting services to end users which exceed 3 million user hours. This should be based on the combination of duration of service loss/disruption and the number of end customers affected.
- Security compromises attracting national mainstream media coverage, regardless of whether they meet the quantitative thresholds in Tables 1, 2 and 3
- Security compromises affecting critical Government or Public Sector services (e.g., widespread impact on 999, 3-digit non-emergency numbers, emergency services communications).
- Any single security compromise that is likely to affect the provision of wholesale services to both fixed and mobile communications providers in a given geographical area.

Requirements for reporting urgent security compromises include:

- Providing an initial notification to Ofcom within 3 hours of the provider becoming aware of the security compromise.
- Providing a full report within 72 hours of the initial notification.

Security compromises should be considered as “non-urgent” where the combination of duration of service loss/disruption and the number of end customers affected is above 250,000 user-hours lost. Requirements for reporting non-urgent security compromises include providing a report within 72 hours of becoming aware of the security compromise.

All security compromises below the 250,000 user-hours lost threshold would be considered “non-major” and are excluded from the 72-hour reporting requirement. Non-major security compromises can be reported in batches which commenced in a calendar month before the second Monday of the following month of the incident/compromise.

Remediation Plans

Like other jurisdictions, Ofcom will apply various remediation plans to address issues and ensure compliance from TSPs. While the specific plans can vary based on the nature of the problem, measures and actions include requirements to meet coverage obligations, improve service levels, or investment in infrastructure to improve service quality. Most remediation plans include mandatory monitoring and reporting to ensure plans are adhered to and outcomes are realized within the outlined timeframes. In some cases, additional audits may be identified.

Administrative Monetary Penalties/Fines and Penalties

Ofcom derives its enforcement powers from the *Communications Act 2003* and other legislation. When assessing fines or penalties, Ofcom considers factors such as the seriousness of the breach, the extent of harm caused, the duration and impact of the outage, and the provider’s previous compliance history. Ofcom aims for proportionate and deterrent penalties that reflect the severity of the non-compliance or breach. There are statutory limits on the fines or penalties that Ofcom can impose. These limits vary depending on the specific regulatory framework and the nature of the violation. For instance, under the General Conditions of Entitlement, which outline the obligations for communications providers, the maximum penalty per contravention is set at 10% of the provider’s relevant turnover. Before imposing fines or penalties, Ofcom typically engages in a consultation process with the provider, allowing them to respond to the allegations and present their case.

User Compensation

Ofcom have implemented an automatic compensation scheme for broadband and landline customer to get money back from their provider when within some conditions, without having to ask for it. Approximately 10 providers have signed up to the scheme. This provides compensation for delayed repairs following a loss of service, missed repairs or provision appointments, and delays to the start of a new service.

Australia

Universal Service Obligation

The Universal Service Obligation (USO) is a long-standing consumer protection that ensures everyone has access to landline telephones and payphones regardless of where they live or work.

Telstra is responsible for delivering the USO and must provide standard telephone services (STS) on request to every premises in Australia within reasonable timeframes. This is both a legislative and contractual obligation. The Department of Infrastructure, Transport, Regional Development, Communications, and the Arts monitors how Telstra meets the USO. The USO is law under the *Telecommunications (Consumer Protection and Service Standards) Act 1999*. In December 2018 the Government announced the USO would be incorporated into a new, wider Universal Service Guarantee (USG), including both broadband and voice.

Emergency Calls

The Australian Communications and Media Authority (ACMA) also mandates TSPs to provide emergency call service to customers (*Telecommunications [Emergency Call Service] Determination 2019* and the Emergency Call Service Requirements Industry Code C526:2011), failure of which is met with steep fines (such as the $400,000 fine paid by TPG Telecommunications Service Provider [TSP] in 2014 after an ACMA investigation into a complaint made by a customer who tried to call 000 in 2011 when their partner had a heart attack).

TSPs are also mandated to notify customers at least five working days in advance about any service disruptions as per the Australian Telecommunications Consumer Protections (TCP) Code and telecommunications operators and Internet Service Provider (ISP) have been fined (nominally) or been formally admonished by the ACMA as part of the mild regulator response.

Outage Notification and Incident Reporting

Australia telecommunication regulators do not have a mechanism for telecommunication outage notification or incident reporting. The Australian Cyber Security Centre (ACSC) requires cyber security incident reporting for critical infrastructure owners and operators.

Remediation Plans

Like other jurisdictions, ACMA will apply various remediation plans to address issues and ensure compliance from TSPs. While the specific plans can vary based on the nature of the problem, measures and actions include requirements to meet coverage obligations, improve service levels, or investment in infrastructure to improve service quality. Most remediation plans include mandatory monitoring and reporting to ensure plans are adhered to and outcomes are realized within the outlined timeframes. In some cases, additional audits may be identified.

Administrative Monetary Penalties/Fines and Penalties

Critics have alleged that Australian regulators have limited both imposing fines and the quantum of fines imposed. Though this has been changing recently. Besides the obligation to provide services, TSPs and ISPs have also been fined the by the Australian Competition and Consumer Commission (ACCC) when found to be providing substandard services to customers. The ACCC has in the recent past penalized the National Broadcasting Network (NBN) for congested or slow services.

User Compensation

The Australian Customer Service Guarantee Standard (CSG Standard) protects customers from poor service. It tells telecommunications companies how fast they must connect or fix landlines. It also sets the compensation they must pay if they miss those timelines. The CSG Standard covers phone services and appointments at user’s location including connecting a service and repairing a fault or service problem (i.e., customer can’t make or receive calls, are repeatedly cut off, have severe interference that affects the service, or are unable to use the service). The standard does not cover mobile phone and internet services. There are many conditions and dependencies to this guarantee. Notably the CSG does not apply if a network outage or disruption is the result of a natural disaster or extreme weather, planned maintenance or upgrade work, or damage to their facility or network by a third party. In the case of a mass service disruption, the telecommunications company must follow the rules in the Standard. Within 10 days of the start of the disruption they must write to everyone who is affected or publish a notice on their website and in the local newspaper and notify ACMA and the Telecommunications Industry Ombudsman about the disruption.

New Zealand

Universal Service Obligation

The telecommunications service obligations (TSO) regulatory framework established under the *Telecommunications Act 2001* enables specific telecommunications services to be available and affordable.

A TSO is established through an agreement under the *Telecommunications Act 2001* between the Crown and a TSO provider.

Currently there are 2 TSO providers:

- Spark (supported by Chorus) is the TSO provider for the local residential telephone service, which includes charge-free local calling.
- Concentrix is the provider for the New Zealand relay service for deaf, hearing-impaired, and speech-impaired people.

Costs for subsiding telecommunications services supplied under TSOs are funded through the Telecommunications Development Levy. This levy is collected from the telecommunications industry.

The New Zealand Commerce Commission works out the TSO charge paid to a TSO provider and the proportion of the Telecommunications Development Levy each provider is liable for.

Emergency Calls

Emergency calls in New Zealand are made by calling 111. A main component of the emergency calling system is the Initial Call Answering Platform (ICAP) for the first answering of 111 calls.

Spark operates the ICAP so emergency calls are first answered at a Spark call centre. Genuine emergency calls are then forwarded to the appropriate Emergency Service Provider (Police, Fire, Ambulance). Although telecommunications service providers are not obliged to provide emergency call services, they are encouraged to inform their customers about emergency call access and how to make emergency calls.

The Telecommunications Forum sets minimum standards for emergency call services through its industry code of practice, the Emergency Calling Code.

Outage Notification and Incident Reporting

New Zealand regulators do not have a mechanism for telecommunication outage notification or incident reporting.

Remediation Plans

Like other jurisdictions, the New Zealand Commerce Commission will apply various remediation plans to address issues and ensure compliance from telecommunication service providers. While the specific plans can vary based on the nature of the problem, measures and actions include requirements to meet coverage obligations, improve service levels, or investment in infrastructure to improve service quality. Most remediation plans include mandatory monitoring and reporting to ensure plans are adhered to and outcomes are realized within the outlined timeframes. In some cases, additional audits may be identified.

Administrative Monetary Penalties/Fines and Penalties

The New Zealand Commerce Commission does not specifically impose fines or penalties for outages; however, it does have the authority to enforce compliance with various regulatory requirements.

User Compensation

There were no specific automatic compensation frameworks for telecommunication outages identified in New Zealand.

Japan

Universal Service Obligation

The *Telecommunications Business Act (*TBA) defines Universal Telecommunication services as services which are essential to the lives of Japanese people. Under a *Telecommunications Business Act* ordinance, services for telephone calls, public and private, urgent calls to police and fire stations are included in the Universal Services.

To allocate part of the costs of universal services, contributions named universal service fees are collected from mobile phone companies, fixed phone companies and IP phone companies, and the contributions are distributed to NTT EAST and NTT WEST, who are the universal service providers. The amount of the contributions is between ¥2 to ¥3 per month per telephone number, and the contributions are passed on to the end users in most cases.

Broadband is not deemed as a universal service currently, but the Ministry of Internal Affairs and Communications is considering designating broadband a universal service.

Emergency Calls

The primary emergency number in Japan is 110 for reporting crimes or seeking police assistance. For medical emergencies or requesting an ambulance, the number is 119. These emergency numbers are widely recognized and accessible throughout the country.

Under the *Disaster Countermeasures Basic Act*, the government is responsible for establishing and maintaining a robust emergency response system. This includes ensuring that emergency call services are available to the public. The Act sets guidelines for the establishment and operation of emergency call centers, ensuring that they are adequately staffed, equipped with the necessary technology, and capable of coordinating emergency responses.

Outage Notification and Incident Reporting

Japan's TBA provides the Ministry of Internal Affairs and Communications (MIC) with a mandate to collect information on telecommunication related outages or accidents and incidents. The TBA outlines two categories of accidents and incidents that TSPs are required to report to MIC, these include 1) serious accidents or 2) accidents and incidents requiring quarterly reporting.

The TBA defines serious accidents as:

- Accidents in which a failure in telecommunications facilities (i.e., machines, equipment, wires and cables or other electrical facilities for conducting telecommunications) occurs results in the suspension or quality deterioration of the services, provided that the number of affected users who have been affected and the duration fall under the criteria specified in the classification of telecommunications services listed in the table below.

Table 12. TBA Criteria for Defining Serious Accident

Classification of Telecommunication Services	Hours	Number of Users Affected
1. Voice transmission services with emergency calls	1 Hour	30,000
2. Voice transmission services without emergency calls	2 Hours 1 Hour	30,000 100,000
3. Mobile phones (excluding telecommunications services listed in the above 1 and 2) with cellular low power wide area (LPWA) services (radio facilities that meet the conditions specified in Article 49-6-9, Paragraphs 1 and 5 or Paragraphs 1 and 6 of the Order of MIC No.18 of 1950: Regulating Radio Facilities) and unlicensed LPWA services stipulated in Article 1, Paragraph 2, Item 18 of the Reporting Rules	12 Hours 2 Hours	30,000 100,000
4. Internet-related services that do not receive payment from users as compensation for the provision of telecommunications services (excluding telecommunications services listed in the above items 1 to 3)	24 Hours 12 Hours	100,000 100,000
5. Telecommunications services other than those listed in the above 1 to 4	2 Hours 1 Hour	30,000 100,000

Accidents in which a failure in important telecommunications facilities (e.g., satellites, submarine cables, or other similar important telecommunications facilities) causing all communications disabled for two hours or more.

The TBA defines accidents and incidents as an accidents and incidents requiring quarterly reporting when:

- Accidents in which a failure in telecommunications facilities occurs and the provision of all or part of telecommunications services resulting in the suspension or quality deterioration of the services, provided that the number of affected users who have been affected is 30,000 or more or the (duration is two hours or more).
- Accidents in which a failure in facilities other than telecommunications facilities occurs, the provision of telecommunications services is interfered, and the number of users affected by the accident is 30,000 or more or the duration is two hours or more.
- Incidents which information leakage on telecommunications facilities may interfere with the provision of telecommunications services.
- Accidents and Incidents caused by a failure in terminal system transmission line facilities (limited to those interconnected to mobile terminal facilities at one end) interconnected to users' telecommunications facilities at one end over the radio.
- Accidents caused by a failure in station-installed remote accommodation devices or feeder/line-point remote accommodation devices, where the scope of the impact is limited to a part of those who use the line accommodated by the device.
- Accidents caused by a failure in a digital subscriber line access multiplexer (DSLAM), where the scope of the impact is limited to some of the users of the line accommodated by the device.

Remediation Plans

Like other jurisdictions, MIC will apply various remediation plans to address issues and ensure compliance from telecommunication service providers. While the specific plans can vary based on the nature of the problem, measures and actions include requirements to meet coverage obligations, improve service levels, or investment in infrastructure to improve service quality. Most remediation plans include mandatory monitoring and reporting to ensure plans are adhered to and outcomes are realized within the outlined timeframes. In some cases, additional audits may be identified.

Administrative Monetary Penalties/Fines and Penalties

There were no specific frameworks identified for Administrative Monetary Penalties or Fines and Penalties applied by MIC.

User Compensation

There were no specific automatic compensation frameworks for telecommunication outages identified in Japan.

European Union

Universal Service Obligation

In the context of the European Union (EU), USO refers to the Universal Service Directive (USD). The USD is an EU directive that aims to ensure the availability of basic communication services to all EU citizens, regardless of their geographical location or personal circumstances.

The USD sets out certain obligations for EU member states and TSPs including access to basic communication services: Member states must ensure that affordable and high-quality services, such as voice telephony, broadband internet, and directory assistance, are available to all users.

Emergency Calls

112 became the single European emergency number in 1991. The European Electronic Communications Code ensures that Europeans can call the European emergency number 112 wherever they are in Europe. The Roaming Regulation obliges roaming service providers to send an SMS to people travelling to another EU country with information about the European emergency number 112. 112 functions alongside existing national emergency numbers. Denmark, Estonia, Finland, Malta, the Netherlands, Portugal, Romania, and Sweden have opted for 112 as their only national emergency number.

Outage Notification and Incident Reporting

The regulatory requirement for reporting by TSPs in the EU is governed by the EU regulatory framework for electronic communications. This framework includes several directives and regulations that outline the obligations and reporting requirements. This includes:

- Outage/Incident Reports – including nature, scope and impact of the outage or incident (e.g., duration, geographical scope, number of affected users). This reporting must also include the steps taken and/or plans to restore service(s).
- Outage/Incident Follow-up Reports – providing updates on the progress of service restoration efforts and any measures taken to prevent future incidents.
- Annual Transparency Reports – including network coverage, quality of service, tariffs, and market share.

- Quality of Service (QoS) Reports - including indicators such as call drop rates, setup times, speeds, and service performance metrics.
- Security Incident Reporting – security incidents and breaches reported to the national regulatory authorities (NRA), and in some cases to the Computer Security Incident Response Teams (CSIRTs) or other relevant bodies.

The specific reporting requirements and procedures vary among EU member states: they have the flexibility to implement the EU regulatory framework into their national legislation. E.g., Germany does have mandatory reporting requirements relating to security breaches/outages.

To strengthen cyber security at the European level, the EU Network and Information Security Directive (NIS Directive) was published in in June 2017. The updated NIS 2.0 directive came into force in 2023.

E.g., Germany

The competent regulatory/supervisory authority in these cases is the Federal Network Agency (Bundesnetzagentur). It requires mandatory reporting of security incidents from all telecommunication providers.

In addition, larger operators that are considered as Critical Infrastructures operators additionally must report to Germany's Federal Office for Information Security. The definition of Critical Infrastructures is concretized by 1-7 of the Regulation on the Designation of Critical Infrastructures pursuant to the *Federal Office for Information Security Act*. Specific threshold values define when a critical infrastructure operator is subject to regulation.

Telecommunications companies will be more strongly regulated in the future (*IT Security Act*). They will be obliged to warn their customers if they detect misuse of a customer connection. In addition, where possible, they are obliged to disclose potential solutions with those affected.

Table 13. German Critical Infrastructure Operator Threshold Values

Network/system type	Threshold
Access Network	100,000 users
Backbone	100,000
Subsea cable landing station	1 sea cable
Internet exchange point (IXP)	100 connected application servers
Domain Name System (DNS) Resolver	100,000 participants in access network
Authoritative DNS Server	250,000 domains
Top-level domain (TLD) Registry	250,000 domains
Data center	3.5 MW power
Server farm	10/15 thousand instances
Content Delivery Network	75 TB data/year

Note: these threshold values were obtained through the jurisdictional scan. However, more details on the thresholds may be available.

E.g., France

In France, the framework for telecommunications outage notification and incident reporting falls under the Regulatory Authority for Electronic Communications, Postal Services and Press Distribution (*Autorité de régulation des communications électroniques, des postes et de la distribution de la presse*). The French Postal Services and Electronic Communications Code (*Code des communications électroniques et des postes*) includes requirements for telecommunication operators around conditions of continuity, quality, availability, security and integrity of the network and service, the standards and specifications of the network and service, and the free transfer of emergency calls and the transfer of communication from public authorities related to imminent dangers.

France has the National Agency for Information system Security (*Agence nationale de la sécurité des systèmes d'information* [ANSSI]). Within the French *Critical Infrastructures Information Protection Law (*CIIP Law*)*, the ANSSI shall be notified by operators of incidents occurring on their critical information systems. Types of incidents to be notified have been specified by sectoral orders.

Remediation Plans

Like other jurisdictions, the EU member countries apply various remediation plans to address issues and ensure compliance from telecommunication service providers. Most remediation plans are left up to the member states. While the specific plans can vary based on the nature of the problem, measures and actions include requirements to meet coverage obligations, improve service levels, or investment in infrastructure to improve service quality. Most remediation plans include mandatory monitoring and reporting to ensure plans are adhered to and outcomes are realized within the outlined timeframes. In some cases, additional audits may be identified.

Administrative Monetary Penalties/Fines and Penalties

While the EU can impose fines on companies that breach telecommunications regulations and for ongoing non-compliance, most Administrative Monetary Penalties or Fines and Penalties are the responsibility of the member countries.

User Compensation

There were no specific automatic compensation frameworks for telecommunication outages identified that apply across the EU.

3.2.3 Voluntary Industry Measures

Regulators and industry groups across almost all deep dive jurisdictions have also developed voluntary guidance for service providers. These include standard operating procedures, guidelines, best practices, and recommendations relating to the reliance of telecommunications networks and services. These measures all work to prevent, reduce, and assist recovery from network outages.

Table 14. Key Take-aways for Voluntary Industry Measures

Collaboration	▪ In most cases regulators collaborate with working groups of industry stakeholders or established resiliency steering committees to develop the guidelines and recommendations they issue. Sharing lessons learned and information about emerging threats and vulnerabilities facilitates knowledge exchange and implementation of effective resiliency strategies. ▪ Public statements made by government or regulators and voluntary codes of conduct developed collaboratively help guide service providers to better resiliency.
Guidelines and Industry Recommendations	▪ Types of guidelines and recommendations issued by the regulators and industry groups vary largely. ▪ However, topics most frequently covered under these guidelines and recommendations include the following: disaster recovery plans, network security and resilience, backup power and network redundancy.
Development and Adoption of Best Practices	▪ While regulators in most jurisdictions issue some form of guidelines, recommendations or best practices, the traditional approach has been light touch. ▪ In most jurisdictions industry has been left to identify and implement best practices within their telecommunications networks. ▪ However, due to the rapid pace of technology innovation, some regulators have identified the need introduce more prescriptive guidance and conduct compliance assessments.
Voluntary Outage/Incident Reporting System	▪ Of the six jurisdictions, the US is the only regulator that has implemented a voluntary outage/incident reporting system. ▪ The voluntary reported system is activated during major disasters and enables communications providers to quickly report service degradations and request assistance.

United States

Standard Operating Procedures, Guidelines and Recommendations

The FCC has established a committee called Communications Security, Reliability, and Interoperability Council (CSRIC) to provide recommendations to the FCC regarding ways the FCC can help to ensure security, reliability, and interoperability of communications systems.

Scope of CSRIC's recommendations focus on a range of public safety and homeland security-related communications matters, including: (1) the reliability of communications systems and infrastructure; (2) 911, Enhanced 911 (E911), and Next Generation 911 (NG911); (3) emergency alerting; and (4) national security/emergency preparedness (NS/EP) communications, including law enforcement access to communications.

Recommendations address the prevention and remediation of detrimental cybersecurity events, the development of best practices to improve overall communications reliability, the availability and performance of communications services and emergency alerting during natural disasters, terrorist attacks, cybersecurity attacks or other events that result in exceptional strain on the communications infrastructure, the rapid restoration of communications services in the event of widespread or major disruptions, and the steps communications providers can take to help secure end-users and servers.

Every two years, since 2009, CSRIC has been rechartered to address new issues as assigned by the Federal Communications Commission's Chairman. In response to these tasks, CSRIC produces reports that address various aspects of the issues as directed, including recommendations and best practices. (CSRIC Reports)

The US has also developed DIRS, a voluntary reporting system.

United Kingdom

Standard Operating Procedures, Guidelines and Recommendations

With respect to network resilience, United Kingdom has not developed specific binding standards or requirements, but follows a community driven approach to develop recommendations and guidelines. It is recommended that providers implement the guidelines on telecommunications infrastructure resilience issued by the Electronic Communications Resilience and Response Group. This group is made up of the major network operators, UK and devolved governments and Ofcom as regulator. Ofcom has developed a threat intelligence-led penetration testing scheme which simulates a well-resourced cyber-attack from a nation state or large organized crime groups and may exercise its statutory powers to require a provider to undergo testing in order identify and address any security vulnerability or other weaknesses in a provider's functions, processes, policies, systems, or networks.

Besides this, all Operators of essential services (OES) that fall under the *Network and Information Systems Regulations 2018* must comply with various notification requirements that are still based on EU's NIS Directive of 2018. These mainly include:

- (High-Level) Security requirements for operators of essential services; and
- Incident reporting duties for operators of essential services.

Following a consultation in 2022 the government announced its intention to update these regulations to improve the UK's cyber resilience. The changes included adding managed service providers (MSPs) into scope of the regulations for:

- Improving cyber incident reporting to regulators;
- Establishing a cost recovery system for enforcing the NIS regulations;
- Giving the government the power to amend the NIS regulations in future to ensure they remain effective; and
- Enabling the Information Commissioner to take a more risk-based approach to regulating digital services.

In 2018, Ofcom imposed communications providers to offer at least one solution to ensure a minimum of one-hour back-up power for telecom infrastructure during power outages.

Australia

Standard Operating Procedures, Guidelines and Recommendations

Australian regulators generally do not issue standard operating procedures, industry guidelines or recommendation relating to reliability and resilience of telecommunication networks. The current approach is to rely on competition within the market to identify best practices and improve resilience within networks.

However, in the past regulators such as the ACMA have conducted investigations and released reports relating to the reliability and resilience of the nation's telecommunication networks. The investigations and reports are typically completed on an ad hoc basis and in response to a major incident. One recent example of this would be ACMA report (in conjunction with Communications Alliance and AMTA) on the impacts of the 2019–20 bushfires on the telecommunications network. This report provided a detailed analysis of information obtained from the carriers relating outages and degradation events caused by to the 2019-20 bushfires and offers observations about network resilience and the use of remediation measures to restore services. The report did not make any recommendations or identify any best practices relating to resilience.

New Zealand

Standard Operating Procedures, Guidelines and Recommendations

The New Zealand Telecommunications Forum (TCF) and Internet Service Providers Association of New Zealand (ISPANZ) provide resources, guidance, and forums for collaboration among telecommunications providers. They promote best practices, share knowledge, and advocate for the interests of their members.

The TCF's Code Compliance Framework (CCF) is central in ensuring the protection of consumers and maintaining the validity of self-regulation by the telecommunications industry. The CCF sets out the processes, roles, and responsibilities of the TCF and code signatories for monitoring and reporting on compliance with TCF Codes. Administration of the CCF is undertaken by the TCF Code Compliance Officer in accordance with the procedures set out in the CCF Operations Manual.

There are three (3) types of Codes within the TCF - Regulated Codes, Mandatory Codes and Voluntary Codes. A Regulated Code is any Code of practice regulated under the *Telecommunications Act 2001* as determined by the Minister or the Commerce Commission from time to time. A Mandatory Code is a Self-Regulated Code that the TCF Board decides is compulsory for all TCF Members to become signatories to, as part of their TCF membership. A Voluntary Code is a Self-Regulated Code which TCF Members and other Parties may choose to sign up to.

Industry guidelines do not require signatories or compliance but often form the foundation document to binding agreements between telecommunications providers.

Japan

Standard Operating Procedures, Guidelines and Recommendations

The Telecommunications Carriers Association (TCA) in Japan is an industry association representing major telecommunications carriers. They develop and promote industrywide guidelines and best practices including network security, service quality, disaster preparedness, and consumer protection. The Council for Safety and Reliability's committee promotes coordination of carrier activities including sharing of various information among carriers with the objective of securing the safety and reliability of telecommunications system.

The MIC prepares and issues reports that identify causes of incidents/events. Findings from these reports are considered guidelines however, there is no legal enforcement behind it.

European Union (EU)

Standard Operating Procedures, Guidelines and Recommendations

The European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit, standardization organization in the field of information and communications. ETSI supports the development and testing of global technical standards for systems enables by Information and Communication Technologies (ICTs), applications, and services including fixed, mobile, radio, converged, broadcast and internet technologies.

ETSI was set up by the European Conference of Postal and Telecommunications Administrations (CEPT). ETSI is the officially recognized body with a responsibility for the standardization of ICT. It is one of the three (3) bodies, the others being the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC), officially recognized by the European Union (EU) as a European Standards Organization (ESO). The role of the European Standards Organizations is to support EU regulation and policies through the production of Harmonised European Standards and other deliverables. The standards developed by ESOs are the only ones that can be recognized as European Standards.

A key publication is the "Emergency Communications (EMTEL): Overview of Emergency Communications Network Resilience and Preparedness". The report provides guidelines and recommendations to maximize the level of preparedness and resilience of emergency communication services based on identified risks for involved technologies. The guidelines include concepts such as component level resilience, path/route diversity and separation, fault tolerance, disaster recovery, service diversity, network segmentation, and isolated operations.

E.g., Germany

The Federal Network Agency (*Bundesnetzagentur*), in agreement with the Federal Office for Information Security and the Federal Commissioner for Data Protection and Freedom of Information, has drawn up a Catalogue of Security Requirements for the operation of telecommunications and data processing systems and for the processing of personal data as a basis for the security concept. The catalogue classifies operators of public telecommunications networks as having an increased risk potential and defines particular security requirements that need to be implemented.

A list of critical functions for public telecommunications networks and services identifies the critical functions whose components are covered by the regulation. The Technical Guideline TR-03163 'Security in Telecommunications Infrastructure', contains the relevant certification schemes for such critical components in public telecommunications networks with an increased risk potential.

In addition to public telecommunication services, specific regulations exist for digital service providers and internet service providers. Specific Recommendations for internet service providers have been developed by Germans Federal Office for Information Security reflect the state of the art (best current practice) which is referred to in higher level documents.

3.2.4 Other Initiatives and Technologies to Improve Resilience

There are also other initiatives and technologies that are contributing to improving resilience that are either not directly related to telecom resilience efforts or are delivering primary benefits adjacent and/or outside of commercial telecommunications or across multiple industries. These could be considered when looking at a comprehensive and complete approach to resilience.

Table 15. Key Take-aways for Other Initiatives and Technologies

Low Earth Orbit (LEO) Satellites	▪ Traditional telecommunications networks rely on ground-based infrastructure which is more susceptible to physical damage through intentional sabotage or climate change related events. LEO satellites are less susceptible to localized/terrestrial issues. ▪ In case of an outages or disruption in the ground-based infrastructure, LEO satellites can be used to quickly restore connectivity and ensure communication continuity, providing the telecommunications networks with an additional layer of resiliency.
Public Safety Broadband Networks (PSBN)	▪ While intended specifically for use by public safety agencies and first responders, this network sometimes has an indirect effect of improved resilience to commercial networks. ▪ Infrastructure hardening and redundancy that are required from the wireless carrier participants/operators for the Public Safety Broadband Networks are sometimes shared with networks and infrastructure delivering services for commercial users.
Power Resiliency	▪ In areas with frequent power outages, telecommunication providers may establish localized power solutions including dedicated backup systems with generators, longer lasting batteries, or solar power installations at individual cell towers/network equipment sites. ▪ As well multiple interconnected network nodes and redundant pathways are established to reroute traffic in case of power failures at specific locations.
Neutral Host/Open Radio Access Network (ORAN) Adoption	▪ Alternate approaches to telecommunications network architecture include the adoption of more open and interoperable solutions. ▪ This approach aims to introduce greater flexibility, interoperability, and innovation by decoupling hardware, software and specific vendors or providers.

Alternative: Low Earth Orbit Satellites

Low Earth Orbit (LEO) satellites circle the Earth at an altitude below 2,000 km (approximately 1,243 miles), which enables them to provide better performance and lower latency than older generations of geostationary satellites.

Traditional telecommunications networks rely on ground-based infrastructure (such as cell towers or terrestrial and subsea cables) to transmit signals for communications, which makes them susceptible to physical damage through intentional sabotage or climate change related events. LEO satellites, on the other hand, operate mainly in space and therefore are less susceptible to such localized issues. In case of an outages or disruption in the ground-based infrastructure, LEO satellites can be used to quickly restore connectivity and ensure communication continuity, providing the telecommunications networks with an additional layer of resiliency. In addition to the benefit of enhanced resilience, other benefits of LEO satellites include:

- Wide Coverage: LEO satellites proximity to Earth allows them to provide broader coverage and reach even remote or underserved areas where traditional telecommunications infrastructure is limited or absent.
- Flexibility and Scalability: LEO satellite networks can be rapidly deployed and expanded to accommodate increased demand or to provide temporary coverage during emergencies. This flexibility makes them ideal for responding to sudden surges in communication needs, such as during natural disasters or major events.

While jurisdictions can use LEO satellites for TSPs services to take advantage of the potential benefits, establishing a large constellation is complex and costly endeavor. Most TSPs prefer to partner with existing LEO broadband internet providers to avoid the overhead and costs of building from scratch.

Alternative: Public Safety Broadband Network

- A Public Safety Broadband Networks (PSBN) provides additional resilience and robustness to a country’s first responders.
- This network can sometimes improve resilience to commercial networks (and commercial users), where infrastructure hardening, and redundancy are required from the wireless carrier participants/operators.
- The costs are usually very significant.
- Most jurisdictions continue to face challenges with coverage and resiliency on the PSBN.

A PSBN is a communication network designed specifically for use by public safety agencies, such as law enforcement, firefighters, emergency medical services, and other first responders.

Traditionally, public safety agencies have relied on separate and fragmented communications that were not always interoperable. These systems included land mobile radio systems (LMRS), and other legacy technologies. However recently several jurisdictions have established their own PSBN, typically using Long-Term Evolution (LTE) or similar wireless networks. Some of these PSBNs are also seeking to leverage recent advances in LEO Satellite Communications. PSBNs typically provide high-speed data, voice, and video capabilities. Drivers for nationwide PSBN initiatives include no broadband service, no interoperability between agencies, and high cost of services.

PSBNs provide resiliency and robustness for public safety, intended to enhance the effectiveness and efficiency of emergency response efforts by providing dedicated and advanced communication capabilities to first responders.

European projects reviewed typically use a multi-carrier shared-network model, where there are several carriers in charge of provisioning of public safety services and the network is shared between public safety users and MNO's (Mobile Network Operators) regular customers.

Overall, there are different business models for MNOs in existing projects, and none of these models has achieved a clearly dominant position. The share of public safety users on a jurisdiction’s Public Safety Broadband Network is typically 0.4% to 0.8%.

The following chart provides an overview of some examples of international Public Safety Broadband Networks.

Table 16. International Public Safety Broadband Network Examples

	United States	United Kingdom	Australia	France	Belgium	South Korea
Type	Single-Carrier	Multi-Carrier shared	Multi-Carrier shared	Hybrid/Multi-Carrier	Multi-Carrier shared	Dedicated Public Safety Network
Spectrum	Single-Carrier Spectrum	No Dedicated Spectrum	Multi-Carrier Spectrum	Multi-Carrier Spectrum	Multi-Carrier Spectrum	Limited Spectrum
Radio Access Network (RAN)	Single-Carrier RANs	Multi-Carrier RANs	Multi-Carrier RANs	Multi-Carrier RANs	Multi-Carrier RANs	Private RANs
Infrastructure	Commercial Grade	Commercial Grade	Commercial Grade	Public Safety Grade Cores	Commercial Grade	Public Safety Grade Core
Interoperability	Some challenges	-	High Level	High Level		High Level

Commercial-grade core networks are primarily designed to support general consumer and business communication needs. Public safety-grade cores are specifically tailored to support the delivery of mission-critical services, high availability, and robust security features.

PSBN Interoperability refers to the ability of different networks to seamlessly communicate and exchange information with each other more so than standard networks. Priority and pre-emption of public safety users across networks is applied to ensure robust and resilient service delivery.

United States

AT&T FirstNet

The US FirstNet is a shared network with priority access and preemption. This network was initiated through United States (US) federal legislation in 2012 through the assignment of 10 MHz of spectrum (currently 20 MHz, 10 MHz paired) in the 700 MHz (Band 14) and the creation of a government oversight body referred to as FirstNet.

Once FirstNet was established, it took steps to enable nationwide interoperability requirements, canvas the industry through an extensive request for information (RFI) process, and perform consultation with and compile data from all 56 US states and territories, and issue an objectives-based request for proposals (RFPs).

The roll-out of broadband data over LTE is currently positioned as an overlay system to existing LMR voice systems with separate funding allocated to both agencies.

United Kingdom

Emergency Services Network

Like the United States, the United Kingdom has begun deployment of a nationwide PSBN known as the Emergency Services Network (ESN), to replace the Airwave system for police, fire, and ambulance services in Great Britain (England, Wales, and Scotland) and transform how they operate.

ESN will enable fast, safe, and secure voice, video, and data across the 4G network and give first responders immediate access to life-saving data, images and information in live situations and emergencies on the frontline.

Investment in ESN will also mean improvements to 4G network coverage, which will allow 999 calls to be made from any 4G enabled mobile phone in some of the most remote and rural parts of Great Britain where it was not previously possible.

ESN's critical mobile technology will mean communication between the emergency services will take priority over other network traffic, even at peak times in busy urban locations. It will mean the emergency services and other first responders can share vital data, information, and expertise quickly and securely from the frontline when it is needed most.

However, the ESN differs from FirstNet in that it will replace the UK's existing mission-critical Push-To-Talk (PTT) two-way radio system, thereby providing mission-critical voice in addition to data to all emergency services. EE's existing commercial network and spectrum will be used to provide services for the ESN, as no new spectrum has been allocated.

Although announced in 2015, the ESN project has experienced significant delays and costs (£2bn on ESN and £2.9bn to maintain Airwave). The Home Office has ended its contract with Motorola early (challenges brought to the Competition and Markets Authority).

Australia

Telstra's LTE Advanced Network for Emergency Services

Australia has been operating its LTE Advanced Network for Emergency Services (LANES) offering with prioritized access to its commercial LTE network since 2016, adding mission-critical push-to-talk in 2017 that was enabled by its existing LTE Broadcast capabilities for delivering PTT calls to groups.

The government set aside spectrum at 800 MHz and 4.9 GHz for public safety mobile broadband. LANES offers a basic prioritized access service as well as one that allows organizations which need emergency communications to use their own LTE spectrum combined with "an option to extend onto the Telstra LTE spectrum".

Australia performed a detailed study which examined a fully commercial model, a dedicated public safety model, and two hybrid variations. The study concluded that a commercial model was the best approach due to the reduced cost and complexity. Additionally, they concluded that it would be best to align with international standards such as LTE and with the spectrum allocations of others in the Asia–Pacific Telecommunications Community.

Australia's Public Safety Broadband Network (PSBN) still has numerous areas with poor or no connectivity. Around 15 per cent of major roads do not have mobile coverage and around 30% of the rail network has poor or no coverage. There are 4,000 reported mobile black spots. NSW Connectivity Strategy is focused on addressing these gaps.

Lessons Learned for deploying capability outside of the commercial footprint:

- Some areas of Australia do not have commercial mobile coverage at present but are covered by land mobile radio networks. There is limited scope to reuse existing infrastructure in these areas, the cost of rolling out a permanent mobile broadband network assessed as very high.
- The cost of building a new base station site was estimated to be three times more than deploying new equipment to an existing base station, requiring a targeted approach. Lower-cost options considered: transportable base station equipment and satellite broadband.
- Plans to deliver $40M in funding to extend/improve mobile phone coverage and competition in regional and remote Australia, by co-funding new or upgraded telecommunications infrastructure in 54 target locations.

France

Réseau Radio du Futur

France has begun awarding tenders for aspects of network development. 19 MHz of the 700MHz spectrum was reserved for use for public protection and disaster relief (licenses taken up in 2019).

With the Réseau Radio du Futur (RRF), France seeks to acquire a high-speed communication network (4G/5G) common to all security and rescue carriers, allowing them to communicate instantly with each other while benefiting from new features such as: video calls, live position sharing, sending electrocardiograms, and interoperability.

The RRF is the State's response to modernizing communication for security and emergency first responders. Today, most use radio equipment designed in the early 1990s, specific to each force, and which does not allow the transmission of large quantities of data or real-time images from the field.

France plans for an investment of more than 700 million euros from the Ministry of the Interior toward RRF. The Ministry of the Interior began construction of the future network in September 2022. The construction and then the tests of a first version of the RRF are forecast to extend over a period of 19 months.

Belgium

ASTRID

ASTRID’s mission is to establish, run, maintain, and implement widening of a radio communications network for voice and data transmissions for Belgian emergency and security services (Blue Light Mobile: single SIM gives access to three (3) Belgian operators and operators in four (4) neighboring countries in a priority and secure environment, automatically switches, works with tablets, pagers, drones, and cameras).

As part of ASTRID, STI Engineering has supplied a total of 189 high-powered very high frequency paging transmitters to Belgium. Stage one of the system refresh commenced in 2015, with an additional 89 sites upgraded in 2021.

Many agreements needed to be entered into with commercial operators (SLAs/guarantees for: coverage, priority access and communication service), planned auction of 700 MHz frequencies.

The initial contract in 2015 depended on STI undertaking development and manufacturing process changes to comply with all European directives, including CE marking and the Direction of the restriction of the use of hazardous substances in electrical and electronic equipment. Transmitters were delivered for stage one in 2015, with stage two delivered Q1 2021.

As an official advisory body, the Users' Advisory Committee represents ASTRID users, and it is responsible for making recommendations. ASTRID respects privacy data protection and has oversight in place to ensure compliance with the *General Data Protection Regulation* (GDPR).

South Korea

SAFENET

SafeNet enables policemen, firefighters, and other groups of public officials to communicate using dedicated terminals. It provides a single communication network on a national scale supporting one channel of command and control, and integrated response at disaster sites.

South Korea, through its Ministry of Public Safety and Security, has also selected an existing commercial mobile network operator to provide emergency services to all Public Safety users in South Korea.

A request for proposal was issued for rollout SafeNet. Samsung has won a contract to provide user devices. The national government has dedicated 20MHz of the 700MHz band. A trial of SafeNet was conducted during the 2018 winter Olympics.

Users will be transitioning from a variety of two-way radio systems onto the new system which will provide mission-critical voice and data like the UK's ESN (dedicated frequencies in 700MHz channels). The system will use existing commercial network (towers, backhaul), as well as dedicated Public Safety RF equipment and spectrum. Therefore, Public Safety priority over commercial users is not necessary.

The chosen operator is paid by the Ministry of Public Safety and Security to provide the service. The government has pledged $1.5 billion to build the network, South Korea also plans to launch a maritime public safety LTE network.

Alternative: Open Radio Access Network/Neutral Host

Open Radio Access Network (RAN) adoption refers to the implementation and deployment of telecommunications networks that adhere to the principles and specifications of an open and interoperable RAN architecture. Traditionally, RAN refers to the equipment and technology that connects devices to the core network of a wireless provider.

Open Radio Access Network adoption represents a shift from the traditional closed and proprietary RAN solutions offered by specific vendors to a more open and disaggregated approach. It aims to introduce greater flexibility, interoperability, and innovation in the RAN domain by decoupling hardware and software components.

4.0 Appendix

4.0 Appendix

4.1 Government Drivers to Improve Network Resilience – Details

Canada

Overview of Resiliency Legislation and Regulator Frameworks

Examples of CRTC Regulations to improve Resilience and Reliability of Telecom Networks and Services

Section – A

CRTC Regulatory policies and Decisions

The Canadian Radio-television and Telecommunications Commission (“the Commission) mandate is to regulate and supervises telecommunications in the public interest and dedicated to ensuring that Canadians have access to a world-class communication system that promotes innovation and enriches their lives. This CRTC’s mandate is established legislation and is focused on achieving policy objectives established in the *Telecommunications Act* and Canada’s Anti-Spam Legislation (CASL).

The *Telecommunications Act* states following policy objectives:

a. 7(b): to render reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada.
b. 7(c): to enhance the efficiency and competitiveness, at the national and international levels, of Canadian telecommunications.

As a result, Commission has mandated or required implementation of Resilience and Reliability of Telecom Networks and Services in various policy proceedings that resulted in Decisions or Orders on technical and operations resiliency and reliability requirements for the implementation of regulated specific wholesale or retail telecom services.

Following are some examples:

1. *Northwestel Inc. – Review of regulatory framework*, Telecom Regulatory Policy CRTC 2011-771, 14 December 2011, which include reliability of the services offered by Northwestel.
2. *Northwestel Inc. – Regulatory Framework, Modernization Plan*, Telecom Regulatory Policy CRTC 2013-711, 18 December 2018, which looks into the network redundancy and reliability of Northwestel network.
3. In Telecom Regulatory Policy 2018-123, the Commission requested that development of business rules and minimum targets for competitor quality of service indicators related to high-speed access (HSA) installation and repair appointments met, as well as average timelines for HSA installation and repair appointments.
4. *Development of the Commission’s Broadband Fund*, Telecom Regulatory Policy CRTC 2018-377, 27 September 2018, considered improving affordability and reliability of telecom services.
5. As part of the Broadband Fund Projects, the Commission considers the projects that enhances telecom network reliability. For example: *Broadband Fund – Acceptance of*

statement of work for TELUS Mobility's access and mobile project in northern Alberta, Telecom Order CRTC 2022-188, 19 July 2022.

6. Telecom Decision CRTC 2022-343: Northwestel Inc. – Application to modify the approval process for the company's retail Internet service tariffs
Article 114: "streamline the tariff approval process for Northwestel's terrestrial residential Internet services in a targeted way, to promote the timely availability of reliable and affordable telecommunications services of high quality in all regions of the Far North that respond to the economic and social needs of users."
7. *Northwestel Wholesale Connect Service – Final rates*, Telecom Order CRTC 2018-338, 31 August 2018, which is the tariff approval of CRTC 21480 - Carrier Access Tariff. See Service Level Agreement (SLA) requirements on Page 31, 6(b):

(b) SLA Targets

Metric	Basic CoS Targets	Medium CoS Targets	High CoS Targets	Highest CoS Targets
Service Availability	99.9%	99.9%	99.9%	99.9%
Packet Loss	N/A	<2%	<1%	<1%
Latency	N/A	<200ms	<150ms	<80ms
Jitter	N/A	<50ms	<25ms	<25ms

Section – B

CRTC Interconnecting Steering Committee Reports and Decisions

The Commission has approved or mandated the implementation of various recommendations on technical, operational and procedural resiliency requirements and best practices developed by CRTC Interconnection Steering Committee (CISC) and its various working groups, largely the Network Working Group (NTWG), Emergency Services Working Group (ESWG) and in the Business Process working Group (BPWG).

The following are some examples:

1. In Telecom Decision CRTC 2022-264, "the Commission **approves** the Business Process Working Group's consensus Task Identification Form (TIF) report BPRE096b and the updated Canadian Data Interchange Guideline and directs telecommunications service providers to migrate to the use of Transport Layer Security 1.3 for exchanging data over Application Statement 2 links by 30 June 2023".
2. *CISC Business Process Working Group – Reports and guidelines related to the implementation of a new competitor quality of service regime*, Telecom Decision CRTC 2021-340, 14 October 2021.
3. *Implementation of a new competitor quality of service regime*, Telecom Decision CRTC 2020-408, 22 December 2020.
4. *CISC Emergency Services Working Group – Consensus report on matters related to compatibility, reliability, resiliency, and security for next-generation 9-1-1*, Telecom Decision CRTC 2019-353, 22 October 2019.
5. *CISC Network Working Group – Non-consensus report on quality of service metrics to define high-quality fixed broadband Internet access service*, Telecom Decision CRTC 2018-241, 13 July 2018.

6. *CISC Emergency Services Working Group – Consensus report ESRE0077 regarding cybersecurity best practices for public safety answering points in a Canadian 9-1-1 ecosystem*, Telecom Decision CRTC 2018-79, 23 February 2018.
7. *CISC Emergency Services Working Group – Consensus report regarding a Next-Generation 9-1-1 network architecture standard for Canada*, Telecom decision CRTC 2015-531, 30 November 2015.
8. **Telecom decision CRTC 2015-432** CISC Network Working Group – Consensus report on recommendations to deal with telephony denial of service attacks against public safety answering points
9. **NTRE076.docx**: TIF 41 - Final Report on Risks of Telephony Denial of Service and Distributed Denial of Service attacks from 5G and IP Networks
10. **NTRE043.doc**: Consensus Report, Network Congestion Mitigation Recommendations Regarding Implementation of Communication Notification Service (CNS)
11. **NTRE061.pdf**: Develop recommendations as to the appropriate metrics and reporting to define high-quality fixed broadband Internet access service.
12. **NTRE054.docx**: Telephony Denial of Service attacks against PSAPs Consensus Report.
13. **NTRE046.doc**: IP to IP Interconnection Guidelines
14. **NTRE055.docx**: Technical Specifications - Wireless Public Alerting Service (WPAS) Specifications

---

Section – C

Resiliency and reliability of 9-1-1 networks

1. *9-1-1 action plan*, Telecom Regulatory Policy CRTC 2014-342, 25 June, where the Commission indicated that it would review the reliability and resiliency of the 9-1-1 networks, including notification to 9-1-1 call centres of network outages that may affect them.
2. *Matters related to the reliability and resiliency of the 9-1-1 networks*, Telecom Regulatory Policy CRTC 2016-165, 2 May 2016, para 30 – 33:

   30. The Commission imposes the following obligation as a condition pursuant to Section 24 of the *Telecommunications Act* (the Act) on all carriers that are 9-1-1 network providers:

   > *9-1-1 network providers must take all reasonable measures to ensure that their 9-1-1 networks (as defined in Footnote12) are reliable and resilient to the maximum extent feasible.*

   31. To assist parties in interpreting what measures would be reasonable with respect to their individual networks, 9-1-1 network providers should use an adequate combination of industry best practices that should generally include the following:

   - 9-1-1 network design principles, Footnote13 e.g. critical component backups configured in a geo-redundant fashion, diverse interconnections from originating networks to the 9-1-1 networks (including backup solutions), location (or site) diversity, transport network diversity (i.e. physically diverse routes with no single points of failure), network available 99.999% of the time, minimum P.01 voice trunk grade of service, Footnote14 and backup power provisions lasting a minimum of 24 hours for central office switches and 72 hours for tandem switches.

- ○ 9-1-1 operation and maintenance practices (e.g., route diversity auditing or a change management process to protect route diversity).
- ○ contingency plans for disaster or outage recovery of 9-1-1 networks to minimize, to the extent feasible, the likelihood and duration of unforeseen, service-impacting 9-1-1 network outages (i.e., 9-1-1 network outages that result in 9-1-1 calls not being delivered to the appropriate PSAP).
- ○ 24/7 monitoring of 9-1-1 networks such that 9-1-1 network performance issues, including outages, are quickly detected, and resolved.

32. The Commission will address any complaints or issues raised regarding the reliability and resiliency of a particular 9-1-1 network on a case-by-case basis and take enforcement actions if required.

33. The Commission encourages PSAPs to implement mitigating strategies of their own to improve the reliability and resiliency of their infrastructure and procedures, such as providing 9-1-1 network providers physically diverse entries for 9-1-1 transmission facilities into the PSAP building, having a backup (or evacuation) site with diverse entries, and having a call-handling arrangement with a partner PSAP to handle calls on each other’s behalf during outages.

3. In TRP 2016-165, para 51, the Commission set out the goal of the notification process:

51. The overall goal of providing 9-1-1 service outage notifications is to ensure that (i) parties that are directly required to take action to restore service are able to do so quickly, and (ii) parties can inform the public of alternative measures to access emergency services if the time to repair the outage is lengthy.

In para 65, the Commission requests that the ESWG do the following:

- develop 9-1-1 service outage notification processes and mechanisms for 9-1-1 network providers and TSP carriers based on the principles and scenarios defined above, and
- report its recommendations to the Commission within six months of the date of this decision.

In response, ESWG submitted report ESRE0076 which was approved in Telecom Decision CRTC 2017-389.

ESWG updated the notification process for Next-generation 9-1-1 in its report ESRE0098.

4. *Next-generation 9-1-1 – Modernizing 9-1-1 networks to meet the public safety needs of Canadians*, Telecom Regulatory Policy CRTC 2017-182, 1 June 2017, which sets out obligations regarding reliability and resiliency, security, and component and data sovereignty.
5. *CISC Emergency Services Working Group – Consensus report ESRE0077 regarding cybersecurity best practices for public safety answering points in a Canadian 9-1-1 ecosystem*, Telecom Decision CRTC 2018-79, 23 February 2018.
6. *CISC Emergency Services Working Group – Consensus report on matters related to compatibility, reliability, resiliency, and security for next-generation 9-1-1*, Telecom Decision CRTC 2019-353, 22 October 2019.
7. *Modification of the next-generation 9-1-1 framework to accommodate hosted call handling solutions for public safety answering points*, Telecom Decision CRTC 2022-284, 17 October 2022, para 22:

22. Interventions relating to the additional flexibility provided by the IP-based NG9-1-1 network reflect the Commission's objective to employ standards-based solutions that allow for flexibility. In terms of NG9-1-1, this includes the ability to (i) reroute traffic to alternative PSAPs in the event that a PSAP is not able to respond to 9-1-1 calls; (ii) maintain reliability and performance of the network even when demarcation points, call handling systems, and telephones are separated by a large geographical distance; and (iii) procure interoperable equipment and services from different vendors that all adhere to the Commission-approved National Emergency Number Association (NENA) i3 Standard for NG9-1-1 (i3 standard).

8. In Telecom Decision CRTC 2019-353**,** the Commission directed NG9-1-1 network providers to include in their NG9-1-1 service agreements specific mandatory requirements for PSAPs to interconnect with the NG9-1-1 networks to ensure compatibility between the NG9-1-1 networks and PSAP networks, as well as to ensure reliability, resiliency, and security measures for NG9-1-1 and interconnecting networks.

Section – D

CRTC Service Outage Reporting Requirement

In *Development of a regulatory framework to improve network reliability and resiliency – Mandatory notification and reporting about major telecommunications service outages*, Telecom Notice of Consultation CRTC 2023-39, 22 February 2023, the Commission launched a process to develop a framework to improve the reliability and resiliency of telecommunications networks. In the first stage of this process, the Commission launched a Notice of Consultation proceeding to seeks comments on a proposal to require all Canadian carriers, on a going-forward basis and as a condition of service imposed pursuant to Section 24 of the *Telecommunications Act*,

- to notify the Commission, ISED, and other relevant authorities of major service outages; and
- to submit a comprehensive post-outage report to the Commission.

On an interim basis pending the outcome of this proceeding, the Commission directed all Canadian carriers (as defined in the *Telecommunications Act*), on an interim basis, to provide the following information to the Commission, effective 8 March 2023:

- Carriers must notify the Commission within two hours of when the carrier becomes aware of a “major service outage,” defined for the purposes of this interim measure, as any outage affecting (i) more than 100,000 subscribers or a material portion of the carrier's subscribers for more than one hour, (ii) subscribers that are in a geographic area served only by the affected carrier, (iii) critical infrastructure, (iv) major transport facilities, or (v) a 9-1-1 network.
- Carriers must provide to the Commission, within 14 days of the day the Commission was notified of a major service outage (as required by item a above), a comprehensive report detailing (i) the causes of the outage, (ii) the steps taken to resolve the outage, (iii) how emergency and accessibility services (including those tailored for Deaf, hard-of-hearing, or visually impaired persons) were specifically affected by the outage, and (iv) plans put in place to prevent similar outages in the future.

The Commission also indicated it will initiate additional public proceedings to address network resiliency in broader terms. Those proceedings may deal with issues including network resiliency principles, emergency services (9-1-1), public alerting, consumer communication, consumer compensation, accessibility, technical measures, and the imposition of administrative monetary penalties.

Information about causes of recent outages in Canada:

The information about the service outages in Canada is posted in public domain on the following CRTC webpage: CRTC: General Information - Service Outages: 8000-C12-201909780.

Since March 2023, Carriers have submitted outage notifications to the Commission has required. Following is an aggregated summary of the causes of service outages.

Table 17. Causes of Major Service Outages from 8th March 2023 to Present

Causes of Service outages	Number of Service outages reported due each cause
Procedural error (e.g., Software or Hardware updates…)	4
3rd party actions (e.g., fibre cuts)	2
Weather events (including those that caused power outages)	5

United States

Overview of Resiliency Legislation and Regulator Frameworks

The FCC (Federal Communications Commission) is the primary telecommunications regulatory body of the United States (US). The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and US territories. An independent US government agency overseen by Congress, the Commission is the federal agency responsible for implementing and enforcing America’s communications law and regulations.

The ***Communications Act of 1934*** combined and organized federal regulation of telephone, telegraph, and radio communications. The Act created the FCC to oversee and regulate these industries. The Act is updated periodically to add provisions governing new communications technologies, such as broadcast, cable, and satellite television.

The *Communications Act*, as amended, is an expansive statue regulating US telephone, telegraph, television, and radio communications. Its seven subchapters regulate virtually all aspects of the communications and broadcasting industry, including assignment of frequencies, rates and fees, standards, competition, terms of subscriber access, commercials, broadcasting in the public interest, government use of communications systems. The Act also provides for more detailed regulation and oversight via the establishment of the FCC.

The ***Telecommunications Act of 1996*** was the first major overhaul of telecommunications law in almost 62 years after the *Communications Act*. The goal of this law is to let anyone enter any communications business – to let any communications business compete in any market against any other. This law has provisions to empower the FCC to create fair rules for this new era of competition.

FCC's Open Internet Order 2015 enacts strong, sustainable rules grounded in multiple sources of legal authority to protect the Open Internet and ensure that Americans reap the economic, social, and civic benefits of an Open Internet today and into the future.

The ***Digital Equity Act of 2021*** was established by the *Bipartisan Infrastructure Law*, also called the *Infrastructure Investment and Jobs Act* (Sections 60301-60307). Under the legislation, the National Telecommunications and Information Administration (NTIA) will use the data on "covered populations" (Census Bureau and NTIA gathered and analyzed federal data to identify and quantify the eight different "covered populations" defined by the Digital Equity Act of 2021, which overall have historically experienced lower rates of computer and internet use) and the relative availability and adoption of broadband as inputs into its funding formula to allocate funding to states (including the 50 states, the District of Columbia, and Puerto Rico) for Digital Equity Planning and Capacity Grants. Census Bureau and NTIA provide the *Digital Equity Act* data through its Population Viewer and data files so users can identify and help address the needs of unserved and underserved populations.

As a part of the *Consolidated Appropriations Act of 2021*, the ***Access Broadband Act of 2021*** was established to increase access to high-speed internet by expanding broadband networks to communities in need. In addition, the legislation requires NTIA to release estimates of the economic impact of such broadband deployment efforts on local economies, including any effect on small businesses or jobs. To address this requirement, the Census Bureau and NTIA created the **Access Broadband Dashboard** for policymakers and the public to assess how changes in broadband availability and adoption could influence local economies.

Initiatives to Improve Network Strength and Resilience

The ***Bipartisan Infrastructure Law*** provides $65 billion in funding to help achieve the goal to connect everyone in America to affordable, reliable high-speed Internet.

Four agencies are leading this effort: the National Telecommunications and Information Administration (NTIA), the Federal Communications Commission (FCC), the Department of the Treasury, and the United States Department of Agriculture (USDA).

There are many different programs under the umbrella of this national initiative:

- Affordable Connectivity Program: This program helps those in need pay for high-speed Internet service and technology.
- Broadband Equity, Access, and Deployment (BEAD) Program: Builds high-speed Internet infrastructure where needed, supports job training, provides the equipment needed, and drives partnerships to get everyone online.
- Broadband Infrastructure Program: A program for states and Internet providers to support high-speed Internet infrastructure projects. It aims to expand Internet service in areas that lack access.
- Capital Projects Fund: This program helps state governments fund capital projects and infrastructure. It works to expand high-speed Internet to deliver vital services.
- Connecting Minority Communities Pilot Program: This program helps colleges and institutions that serve minority and tribal communities. It provides funds to buy Internet equipment and hire staff to help with technology.
- *Digital Equity Act* Programs: The *Digital Equity Act* provides $2.75 billion to establish three (3) grant programs that promote digital equity and inclusion. They aim to ensure that all people and communities have the skills, technology, and capacity needed to reap the full benefits of the digital economy.

- Enabling Middle Mile Broadband Infrastructure Program: This program expands middle mile infrastructure. It aims to reduce the cost of connecting unserved and underserved areas.
- ReConnect Loan and Grant Program: This program helps expand high-speed Internet access in rural areas. Funds support construction, facilities, and equipment.
- State Digital Equity Planning Grant Program: A $60M formula grant program for states, territories, and tribal governments to develop digital equity plans.
- Tribal Broadband Connectivity Program: This program helps tribal communities expand high-speed Internet access and adoption on tribal lands.

Secure and Resilient Mobile Network Infrastructure and Emergency Communications Research and development Program

The Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Secure and Resilient Mobile Network Infrastructure and Emergency Communications Research and Development Program provides direct Research and Development (R&D) support for critical Cybersecurity & Infrastructure Security Agency (CISA) priorities related to its mission to secure and make resilient 5G infrastructure, mobility for government mission use, and emergency communications capabilities.

The solutions developed through these interrelated program R&D areas will help secure legacy and next-generation mobile network infrastructure for federal government missions and use-cases and help secure and enhance the capabilities of the critical communications systems used by the nation's first responders.

The wide-ranging Secure and Resilient Mobile Network Infrastructure and Emergency Communications R&D Program is managed by S&T's Office of Mission Capability and Support and is engaged in the following complementary R&D efforts:

- Secure and Resilient Mobile Network Infrastructure R&D Project; and
- Emergency Communications R&D Project.

National Emergency Communications Plan

The National Emergency Communications Plan (NECP) is the US's strategic plan to strengthen and enhance emergency communications capabilities. The NECP navigates the complex mission of maintaining and improving emergency communications capabilities for emergency responders and serves as the US's roadmap for ensuring emergency communications interoperability at all levels of government.

Title XVIII of the *Homeland Security Act of 2002*, as amended, requires that the CISA develop the NECP to "provide recommendations regarding how the United States should support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of disasters and to ensure, accelerate, and attain interoperable emergency communications nationwide." The law also directs CISA to develop and periodically update the NECP in coordination with federal, state, local, territorial, tribal, and private sector stakeholders.

Supply Chain Diversification

The US government recently launched the Public Wireless Supply Chain Innovation Fund with the primary objective of diversifying supply chains. This fund entails an investment of $1.5 billion in the development of open and interoperable networks.

The objective of the Innovation Fund is to foster competition, lower costs for consumers and network operators, support innovation across the global telecommunications ecosystem, and strengthen the 5G supply chain. More specifically the first round seeks to expand and improve testing to demonstrate the viability of new approaches and remove barriers to adoption to wireless such as open radio access networks (Open RAN). Research and development and testing activities included within the first round will include:

- Expanding industry-accepted testing and evaluation (T&E) activities to assess and facilitate the interoperability, performance, and/or security of open and interoperable, standards-based 5G radio access networks; and
- Developing new or improved testing methodologies to test, evaluate, and validate the interoperability, performance, and/or security of these networks, including their component parts.

The overall objectives include unlocking opportunities for innovative companies, particularly small and medium enterprises, to compete in a market historically dominated by a few suppliers, some of which present a high security risk.

Initiatives to Improve Cybersecurity

Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” was issued May 11, 2017. In Section 2 (d), the executive order requires the Secretaries of Commerce and Homeland Security to “jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets).”

United Kingdom

Overview of Resiliency Legislation and Regulator Frameworks

The Office of Communications (Ofcom) is the regulator and competition authority for the United Kingdom (UK) communications industries. It regulates the TV and radio sectors, fixed line telecommunications, mobiles, postal services, plus the airwaves over which wireless devices operate.

The Communications Act 2003 which replaced almost all the former *Telecommunications Act 1984*, is the primary legislation that set up Ofcom as the regulator for the broader communications industry and implemented the new European regulatory framework which came into force in July 2003. Instead of the former licensing regime of the *Telecommunications Act*, the new Act regulates communications providers by means of general authorizations which are required to be complied with as a condition of operating in the market.

Section 51 defines the subject matter that can be included by Ofcom in the general Conditions of Entitlement. Section 51(1)(c) specifies “conditions making such provision as OFCOM consider appropriate for securing the proper and effective functioning of public electronic communications networks” and thereby empowers Ofcom to implement Article 23 of the Universal Service Directive, entitled Integrity of the Network. It has done so through Condition 3 of the Conditions of Entitlement:

> **3. Proper and Effective Functioning of the Network**
>
> 3.1 The Communications Provider shall take all reasonably practicable steps to maintain, to the greatest extent possible: (a) the proper and effective functioning of the Public Telephone Network provided by it at fixed locations at all times, and (b) in the event of catastrophic network breakdown or in cases of force majeure the availability of the Public Telephone Network and Publicly Available Telephone Services provided by it

> at fixed locations, and (c) uninterrupted access to Emergency Organizations as part of any Publicly Available Telephone Services offered at fixed locations.
>
> 3.2 The Communications Provider shall ensure that any restrictions imposed by it on access to and use of a Public Telephone Network provided by it at a fixed location on the grounds of ensuring compliance with paragraph 3.1 above are proportionate, non-discriminatory, and based on objective criteria identified in advance.
>
> 3.3 For the purposes of this Condition, "Communications Provider" means a person who provides a Public Telephone Network at a fixed location and/or provides Publicly Available Telephone Services at a fixed location.

Section 51(1)(e) of the specifies "conditions requiring or regulating the provision, availability and use, in the event of a disaster, of electronic communications networks, electronic communications services and associated facilities" and thereby empowers Ofcom to implement conditions requiring providers to assist central and local government in times of emergencies.

This is specifically allowed (though not mandated) by paragraph 12 of Annex A to the Authorization Directive and continues previous obligations on Public Telephone Operators in their former licenses.

The provisions to ensure resilience in the face of natural disasters:

> **5. Emergency Planning**
>
> 5.1 Subject to paragraph 5.3, the Communications Provider shall, on the request of and in consultation with:
>
> > (a) the authorities responsible for Emergency Organizations; and
> >
> > (b) such departments of central and local government as Ofcom may from time to time direct for the purposes of this Condition,
>
> make arrangements for the provision or rapid restoration of such communications services as are practicable and may reasonably be required in Disasters.
>
> 5.2 Subject to paragraph 5.3, the Communications Provider shall, on request by any person as is designated for the purpose in any such arrangements, implement those arrangements in so far as is reasonable and practicable to do so.
>
> 5.3 Nothing in this Condition precludes the Communications Provider from:
>
> > (a) recovering the costs incurred in making or implementing any such arrangements; or
> >
> > (b) making the implementation of any such arrangements conditional upon being indemnified by the person for whom the arrangements are to be implemented for all costs incurred as a consequence of the implementation.
>
> 5.4 For the purposes of this Condition:
>
> > (a) "Communications Provider" means a person who provides a Public Telephone Network and/or provides Publicly Available Telephone Services; and
> >
> > (b) "Disaster" includes any major incident having a significant effect on the general public; and for this purpose, a major incident includes any incident of contamination involving radioactive substances or other toxic materials.

Telecommunications Security Code of Practice

The framework established through the ***Telecommunications (Security) Act 2021*** **('the TSA')** comprises three (3) layers:

1. Strengthened overarching security duties on public telecommunication providers. These are set out in new Sections 105A and 105C of the Act as amended by the TSA.
2. Specific security measures (hereafter referred to as 'requirements'). These are set out in the *Electronic Communications (Security Measures) Regulations 2022* ('the Regulations') and detail the specified measures to be taken in addition to the overarching duties in the Act.
3. Technical guidance. This code of practice provides detailed guidelines to large and medium-sized providers of public electronic communications networks or public electronic communications services (hereafter referred to as 'public telecommunication providers') on the government's preferred approach to demonstrating compliance with the duties in the Act and the requirements within the Regulations.

Non-compliance with the new security duties in the Act and/or requirements in the Regulations:

- In cases of non-compliance with the new security duties and/or specific security requirements, Ofcom will be able to issue a notification of contravention to providers setting out that they have not complied, and any remedial action to be taken. Ofcom also can direct telecommunication providers to take interim steps to address security gaps during the enforcement process.
- In addition, in cases of non-compliance, including where a provider has not complied with a notification of contravention, Ofcom can issue financial penalties. The size of the financial penalties that Ofcom can impose in those instances has been updated through the TSA.
- Further information on how Ofcom will use its powers and regulate the framework will be contained within its procedural guidance.

These new regulations developed with the National Cyber Security Centre and Ofcom set out specific actions for UK public telecommunication providers to fulfill their legal duties in the Act. Ofcom has been given the power to fine them up to 10% of their turnover if they fail to comply with sufficient zeal. However, Ofcom recognizes that the guidance set out in the code of practice is not the only way for providers to comply with the new security duties and specific security requirements. TSPs may choose to comply with those new security duties and specific security requirements by adopting different technical solutions or approaches than those specified in the code of practice. In these cases, Ofcom may require the provider to explain the reasons why they are not acting in accordance with the provisions of the code of practice to assess whether they are still meeting their legal obligations under the security framework.

United Kingdom Wireless Infrastructure Strategy

Initiatives to Improve Cybersecurity

The National Cyber Security Centre is an organization of the British Government that provides advice and support for the public and private sector in how to avoid computer security threats. Based in London, it became operational in October 2016.
No major initiatives noted.

Initiatives to Improve Coverage

The UK Government's overarching strategic priority is to promote efficient competition and investment in world-class digital networks. Investment is key to improving consumer outcomes, in terms of choice, service quality, innovation and price over the longer-term. It is the

Government's view that promoting investment should be prioritized over interventions to further reduce retail prices in the near term, recognizing these longer-term benefits.

The Government has identified a set of outcomes with a view to achieving this strategic priority:

- Greater regulatory stability and clarity, through the availability of longer five-year market review periods and a framework whereby firms making large, risky investments can have confidence that any regulation reflects a fair return on investment commensurate to the level of risk.
- Recognizing the convergence of business and consumer uses of networks, through unified access market reviews, where appropriate.
- Regulation only where and to the extent necessary to address competition concerns and ensure the interests of consumers are safeguarded as fibre markets become more competitive.
- Recognition of the differences in local market conditions across the UK, though, where appropriate, a geographically differentiated approach to wholesale regulation. For areas where there is actual or prospective competition between networks, we would expect there to be less need for regulation.
- Flexibility for firms to develop new approaches to reduce deployment costs and manage risks through commercial arrangements.

The most effective way to deliver nationwide full fibre connectivity at pace is to promote competition and commercial investment where possible, and to intervene where necessary. The UK Government estimates that:

- At least a third (with the potential to be substantially higher) of the United Kingdom's premises are likely to be able to support three (3) or more competing gigabit-capable networks.
- Up to half (or lower if there are more than three (3) network areas) of premises are likely to be in areas that can support competition between two gigabit-capable networks.
- There are likely to be parts of the country (c.10% of premises) that, while commercially viable for at least one operator, may not benefit from investment.
- The Government will use 'Competition for the market' mechanisms to secure investment in areas. The proposed new Electronic Communications Code (EECC), for example, provides powers to designate areas where no operator has indicated plans to deploy; and
- In the final c.10% of premises, the market alone is unlikely to support network deployment and additional funding of some description will be required to ensure national coverage.

This strategy relies on getting five things right:

1. Making the cost of deploying fibre networks as low as possible by addressing barriers to deployment, which both increase costs and cause delays.
2. Supporting market entry and expansion by alternative network operators through easy access to Openreach's ducts and poles, complemented by access to other utilities' infrastructure (for example, sewers).
3. Stable and long-term regulation that incentivizes competitive network investment.
4. An 'outside in' approach to deployment that means gigabit-capable connectivity across all areas of the United Kingdom are achieved at the same time, and no areas are systematically left behind; and
5. A switchover process to increase demand for full fibre services.

Those areas that are likely to be unviable commercially for full fibre deployment will require additional funding of some kind. The British Government estimates this will include around 10% of premises across the United Kingdom. These, often rural, areas must not be forced to wait until the rest of the country has connectivity before they can access full fibre networks. Widespread connectivity creates opportunities for small businesses to tap into a global customer base and for people to work more efficiently.

The British Government aims to pursue an 'outside in' strategy, meaning that while network competition serves the commercially feasible areas, the Government will support investment in the most difficult to reach areas at the same time. The additional funding from whatever source is likely to be region of c.£3 billion to c.£5 billion. To make sure that fibre delivery in these areas starts early, we will prioritize delivery of full fibre networks through the existing Building Digital UK (BDUK)'s Superfast Broadband Programme, which has already made Fibre to the premises (FTTP) available to over 200,000 premises in predominantly rural areas by March 2018.

Phase 3 of the Superfast Broadband Programme is seeking to address superfast coverage in as much of the remaining 5% of the country as possible, and Government will now maximize the number of premises to be covered with full fibre. The UK Government has already identified around £200 million within the existing Superfast Programme that can be used for this purpose.

5G Diversification Strategy

The British Government undertook a comprehensive review of the supply arrangements for the United Kingdom's telecommunication Critical National Infrastructure (CNI). The 2019 Telecommunications Supply Chain Review identified the need to: manage and mitigate risks from high-risk vendors, introduce a new robust security framework for telecommunications, and create a more diverse and competitive supply base for telecommunications networks.

The Government undertook important decisions to limit and exclude high risk vendors in United Kingdom's telecommunications infrastructure and brought forward legislation to place those decisions on a statutory footing. The 5G Diversification Strategy sets out targeted and ambitious plans to diversify the global telecommunications supply market, focusing on the following key areas of activity:

- Supporting incumbent suppliers to ensure their resilience and ability to supply the market in the near term, while supporting their transition into the emerging market structure.
- Attracting new suppliers into the UK market to build resilience and competition, prioritizing deployments that are in line with the longer-term vision.
- Accelerating open-interface solutions and deployment so that UK is not reliant on any single vendor and begin to realize its long-term vision for a more open and innovative market.
- Competitive and vibrant telecommunications supply market.
- The UK has developed Open RAN principles, Open RAN principles - GOV.UK (www.gov.uk), which directly refer back to the Diversification Strategy, as well as ongoing government-supported work on Open RAN R&D and testing (e.g., SmartRAN Open Network Interoperability Centre (SONIC) Labs - Case study - GOV.UK (www.gov.uk))

Australia

Overview of Resiliency Legislation and Regulator Frameworks

The Australian Communications and Media Authority (ACMA) is the primary telecommunications regulator in Australia. The Australian Competition and Consumer Commission (ACCC) is responsible for competition regulation.

The ACCC:

- assesses and enforces terms of access to the National Broadband Network in a special access undertaking (SAU) from NBN Co.;
- enforces Telstra's structural separation undertaking (SSU) and the plan to migrate Telstra's customers to the National Broadband Network (NBN);
- sets wholesale prices and wholesale terms of access for declared services;
- tracks and reports on prices and competition in the communications sector;
- investigates claims of anti-competitive conduct in the communications sector.

The Ministry/Department responsible for telecommunications related initiatives and oversight is the Department of Infrastructure, Transport, Regional Development, Communications, and the Arts.

The *Telecommunications Act 1997* is the primary act which governs telecommunications in Australia. The object of the Act is to protect the long-term interests of end users of carriage services and ensure accessible and affordable services for Australians. The Act distinguishes between carriers (i.e., infrastructure owners and operators) and other entities that provide services to end users, referred to as carriage service providers or Communications Service Providers.

The *Telecommunications (Consumer Protection and Service Standards) Act 1999* establishes Australia's regime for universal service and other public interest telecommunications services.

Initiatives to Improve Network Strength and Resilience

Incentives and grants programs funded by the Australian government, the Department of Infrastructure, Transport, Regional Development, Communications, and the Arts, include:

The **Mobile Network Hardening Program** is an Australian Government initiative that assists the mobile network operators, infrastructure providers and infrastructure managers to improve the resilience of Australia's regional mobile network telecommunications infrastructure to:

- prevent outages in the event of a Natural Disaster;
- strengthen the resilience of telecommunications facilities to allow them to operate for longer during bushfires and other Natural Disasters; and
- enable the rapid restoration of services following an outage.

Round 1 of the Program was funded through the Government's Strengthening Telecommunications Against Natural Disasters Programme, announced in January 2020. As part of the Government's Better Connectivity Plan for Regional and Rural Australia, announced in the 2022–23 Budget, the Government committed funding for further rounds of the program. This new funding is part of the Government's commitment to improve communications resilience in rural, regional, and remote Australia under the Better Connectivity Plan.

Round 1 of the Mobile Network Hardening Program is providing $23.5 million (GST inclusive) in funding to Optus, Telstra and TPG, the mobile network operators, across two stages to deliver approximately 1,000 projects to strengthen the resilience of regional telecommunications infrastructure.

The first stage is funding to Optus, Telstra and TPG to enhance the battery backup power at 467 base stations funded under the first two rounds of the Government's Mobile Black Spot Program. These upgrades will increase backup operation at these base stations to at least 12 hours. To date, 461 upgrades have been completed with the remaining sites scheduled to be completed in 2023.

The second stage is funding for Optus, Telstra and TPG to deliver over 530 resilience upgrades at mobile base station sites across Australia. These upgrades comprise:

- the deployment of new portable and permanent generators to supply additional backup power during power outages.
- the upgrading of battery systems to increase backup power capacity.
- the addition of battery extension devices to enhance existing backup power capacity at key sites within mobile networks.
- the improvement of transmission resilience within regional mobile network clusters to reduce single points of network failure.
- the physical hardening of sites against bushfire damage.

The Government committed up to $16.5 million (GST inclusive) to Round 2 of the Mobile Network Hardening Program to fund additional project that improve the resilience of mobile network infrastructure in rural, regional, and remote Australia.

The Government consulted with members of the public, the telecommunications industry and government stakeholders on the design of this round, including draft Grant Opportunity Guidelines.

A Temporary Telecommunications Infrastructure Deployment Grant was provided by the Australian government in 2022. The grant opportunity was announced as part of the **Strengthening Telecommunications Against Natural Disasters (STAND) Program**. Up to $7.7 million was available for this grant opportunity. (Note: the grant is now closed and is no longer available.) The objectives of the program were:

- Increase and improve telecommunications resilience in communities recently affected by severe bushfires or at risk of natural disasters in the future.
- Enhance the capability to restore services to areas affected by bushfires or natural disasters by quickly deploying temporary facilities to address gaps caused by outages.

The **Telecommunications Disaster Resilience Innovation (TDRI) Program** will promote the development of new technologies to provide solutions for telecommunications disaster resilience, particularly in regional, remote and First Nations communities.
The $50 million commitment was announced and funded under the Australian Government's Better Connectivity Plan for Regional and Rural Australia and will run from 2022–25. Funded projects will improve the preparedness of Australia's telecommunications networks against increasing climate risks, including against an anticipated increase in the frequency and severity of natural disasters in Australia.

The program will be delivered through two competitive grants rounds:

- Round 1 focuses on funding innovative solutions that will strengthen the resilience of telecommunications against the impacts of power outages. This focus recognizes that power outages remain one of the most common causes of all telecommunications outages during periods of disaster.
- Round 2 focuses on other innovative telecommunications technologies (excluding power-based solutions, which will be funded in Round 1) that will improve the resiliency,

redundancy, and availability of telecommunications during and/or following a natural disaster.

To **boost temporary infrastructure capabilities**, the Australian Government has co-invested with the telecommunications industry to purchase portable communications facilities such as cells on wheels (CoWs), mobile exchanges on wheels (MEoWs) and National Broadband Network Road Muster trucks, which can be positioned in disaster affected areas to allow communications services to be restored quickly.

The investment means that temporary communications infrastructure is ready to hit the road when needed, allowing Australians to keep in contact with family and essential services, and making sure essential food, water and fuel purchases can occur.

Funding has been provided to NBN Co. to purchase five (5) extra Road Muster satellite trucks and twelve (12) portable satellite kits to provide connectivity where needed during emergencies. These have all been delivered and stationed at strategic locations around Australia to better respond to emergency events.

Provision of Satellite Connections to Emergency Services and Evacuation Centres

The Government has been providing upgraded connectivity at fire service depots and evacuation centres across Australia to support their essential work and provide emergency connectivity for communities.

The funding has seen NBN Co. install Sky Muster satellite connections to rural and country fire service depots and designated evacuation centres across Australia**.**

Initiatives to Improve Cybersecurity

The Australian Cyber Security Centre (ACSC) leads the Australian Government’s efforts to improve cyber security.

The ACSC is a hub for private and public sector collaboration and information-sharing on cyber security, to prevent and combat threats and minimize harm to Australians. We provide advice and assistance across the whole economy, including critical infrastructure and systems of national interest, federal, state, and local governments, small and medium businesses, academia, not-for-profit organizations, and the Australian community.

Specifically, the ACSC:

- responds to cyber security threats and incidents as Australia’s computer emergency response team;
- collaborates with the private and public sector to share information on threats and increase resilience;
- works with governments, industry, and the community to increase awareness of cyber security; and
- provides cyber security information, advice, and assistance to all Australians.

Department of Home Affairs Cyber Security Policy Division staff are co-located with ACSC staff to collaborate in providing policy advice for government.

The Australian Government’s amended the *Security of Critical Infrastructure Act 2018* (SOCI Act) in December 2021. Carriers and Carriage Service Providers (CSP) now have new security obligations, including:

- telling the Australian Cyber Security Centre of the Australian Signals Directorate (ASD) if a cyber-security incident has a relevant impact on a critical infrastructure asset (from July 7, 2022)

- giving the Cyber and Infrastructure Security Centre of the Department of Home Affairs certain information about critical infrastructure assets so it can be included in a register (from October 7, 2022).

The first 12 months (from July 8, 2022) is considered a learning and familiarization phase. The CISC will focus on education, support and working with entities to understand the reporting thresholds as they relate to each sector.

During this time, enforcement action may occur only for egregious non-compliance, such as failure to report critical incidents, rather than the timeliness of reporting or whether a report contains a sufficient level of detail.

The enforcement mechanisms under Sections 68 and 101 of the *Telecommunications Act* that relate to non-compliance with a license condition, or a service determination apply to the new instruments.

Initiatives to Improve Coverage

Australia's NBN was announced in 2009. The policy aimed to address Australia's broadband availability and performance and to facilitate the structural separation of Telstra by providing an optic fibre alternative to its copper access network.

The NBN is being built and run by a government-owned enterprise, NBN Co. (now known as nbnTM). A fundamental policy setting is that nbnTM provides only wholesale services to retail service providers (RSPs) and does not serve end-users. This policy is set out in legislation so any proposed change would need to be brought before parliament.

The original NBN plan was to reach 93 per cent of premises with an optic fibre connection. The remaining 7 per cent of premises would be served by either a new satellite service or terrestrial fixed wireless service (that is, a service to a fixed location, like a home, rather than a mobile service).

The NBN regulatory framework was set up with two Acts:

- *National Broadband Network Companies Act 2011*; and
- *Telecommunications Legislation Amendment (National Broadband Network Measures—Access Arrangements) Act 2011.*

Recently the Australian Government committed to invest $2.4 billion to roll out more fibre to communities across Australia. The new investment will enable an additional 1.5 million homes and businesses currently served by Fibre to the Node (FTTN) to upgrade to Fibre to the Premises (FTTP).

FTTP is viewed as better than FTTN (higher speeds/reliability), and both are better than copper as they are faster, better over long distances, have greater bandwidth, are more scalable, and are more reliable/stable.

These upgrades will help deliver faster broadband speeds, better reliability, are more energy efficient and support the provision of additional data capacity.

New Zealand

Overview of Resiliency Legislation and Regulator Frameworks

In New Zealand (NZ) various government bodies as well as agencies are for regulating the telecommunications space. The Ministry of Business, Innovation and Employment (MBIE), the Commerce Commission and the Telecommunications Carrier Forum (TCF), play key roles in the legislation, regulation, and provision of telecommunications services for NZ.

The Telecommunication Act 2001 acts as the basis for regulation and legislation. The Act enables the commission to regulate the provision of telecommunication services in the country.

Initiatives to Improve Network Strength and Resilience

The **Rural Capacity Upgrade Programme** will see existing cell towers upgraded and new towers built in rural areas experiencing poor performance, as well as fibre, additional VDSL coverage and other wireless technology deployed in congested areas.

As part of the initiative, 13 private sector contractors have signed contracts with Crown Infrastructure Partners to carry out the work. The programme will be funded with the $47 million from the Government’s COVID-19 Response and Recovery Fund.

The **Remote Users Scheme** will equip as many remote households as possible with the connectivity infrastructure needed to access broadband services. Through Budget 2022, $15 million was allocated toward funding the Remote Users Scheme, as part of the broader $60 million rural connectivity package announced earlier in the year.

The **Mobile Black Spot Fund (MBSF)** is providing greater mobile coverage on approximately 1,400 kilometres of state highways and in over 168 tourism locations where no coverage currently exists. The programme will have a direct impact on public safety, by providing greater mobile coverage on stretches of state highway. It will also enhance visitor experiences by providing new coverage in tourism locations.

Crown Infrastructure Partners is managing the contractual arrangements for the MBSF.

Initiatives to Improve Cybersecurity

The primary government body involved in setting up cybersecurity policy in New Zealand is Department of the Prime Minister and Cabinet (DPMC).

New Zealand has a cyber security plan in place. The Cyber Security Emergency Response Plan (CSERP) sets the framework for the government’s response to a cyber security emergency to ensure that:

- agencies and officials understand their roles and responsibilities in the event of a cyber security emergency.
- the private sector understands the government’s approach.
- the response is coordinated, appropriate and effective during a cyber security emergency; and
- following a cyber security emergency, services and operations are restored swiftly and appropriate lessons are identified and acted upon.

The CSERP has informed New Zealand’s response to cyber security emergencies since 2013. Throughout its existence, it has been updated to deliver the goals of the Cyber Security Strategy, adapt to the changing environment and reflect lessons learned from incidents and exercises.

The CSERP is part of New Zealand’s broader National Security System (NSS), is maintained by the Department of the Prime Minister and Cabinet (DPMC) and is authored in collaboration with other agencies with a role in cyber security.

Initiatives to Improve Coverage

The **Ultra-Fast Broadband (UFB)** Programme was one of the largest and most ambitious infrastructure projects ever undertaken in New Zealand. It saw around 87% of New Zealanders, in over 390 towns and cities, able to access fibre by the end of 2022.

Almost $1.8 billion has been invested in the UFB infrastructure to ensure as many New Zealanders as possible can experience the social and economic benefits of faster broadband. Crown Infrastructure Partners (previously Crown Fibre Holdings) was established as a Crown company initially to manage the Government's investment in UFB.

The UFB uses fibre optic cables to deliver fibre-to-the-premises. It is most suitable in urban areas with higher population densities. It is superior to the copper technology that was rolled out in New Zealand over the last century. UFB users can access speeds of close to 1,000 Megabits per second.

The UFB initiative dates to 2008 in response to global telecommunication trends in Southeast Asia and the relative low quality of internet in New Zealand.

The quality of New Zealand's broadband has improved significantly in recent times. A decade ago, average internet speed in New Zealand lagged the UK and Australia. Following the effective rollout of fibre and additional submarine cable links, New Zealand is now well above the Organisation for Economic Co-operation and Development (OECD) average and similarly placed to the US with internet speeds averaging 33Mbps.

Japan

Overview of Resiliency Legislation and Regulator Frameworks

The Ministry of Internal Affairs and Communications (MIC) is the telecommunications regulator (specifically the Telecommunications Bureau). Its role includes formulating policies, issuing licenses, managing radio frequencies, promoting competition, protecting consumer rights, and ensuring smooth operations.

Initiatives to Improve Network Strength and Resilience

Multiple Initiatives to Improve resilience during emergencies and Natural Disasters

- **Earthquake Early Warning System:** Japan has a robust earthquake early warning system that detects seismic activities and issues alerts to the public through various communication channels, including mobile phones, television, and radio. This system provides valuable seconds to minutes of warning before the arrival of seismic waves, allowing people to take protective measures and helping to prevent disruptions to telecommunications infrastructure.
- **Provision of disaster and evacuation information through multiple-address wireless communications:** Multiple-address wireless communication is a system which can promptly and accurately transmit information to local communities through sirens and speakers and other means at the time a disaster strikes. Specifically, siren loudspeakers and house receivers are classified as multiple-address wireless communication. House receivers and emergency radios are distributed to people in areas which the sound of sirens cannot reach.
- **Provision of early warning and other disaster information through disaster information email.**
- **Disaster information sharing through a particular system (J-Alert):** The disaster information sharing information system (J-Alert) is a system which converts information from public organizations into XHL, email and other formats, and transmits it to the

media and communications companies. J-Alert can efficiently and swiftly transmit information from all the participants in the system in a certain format

- **Securing of communications in afflicted areas through movable and deployable Information and communication technology resource unit:** A movable and deployable ICT resource unit (MDRU) is a mobile information and communication technology unit for communications when disasters strike. It consists of communications devices, and information processing and storage devices mounted on a mobile container or vehicle. An MDRU can be brought to disaster-afflicted areas within a short time after a disaster and serve as a telephone/communications infrastructure.
- **Securing of communications in afflicted areas through portable satellite communications systems:** A portable satellite communications system takes moving pictures of disaster afflicted areas and sends the data via a satellite to disaster headquarters and other relevant offices, which take advantage of the pictures to make countermeasure plans.
- Regional development bureaus of the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) have founded fixed stations, in which several portable satellite communications systems are stationed to prepare for disasters.
- **Backup Power Systems**: Telecommunication providers in Japan are required to have backup power systems in place to maintain the operation of critical infrastructure during power outages caused by disasters. These backup systems include uninterruptible power supplies (UPS) and emergency generators.
- **Underground Fibre Optic Cables**: To protect against damage from earthquakes and other disasters, Japan has a significant portion of its telecommunication infrastructure, including fibre optic cables, installed underground. This helps to minimize the risk of disruptions to communication networks during emergencies.

Initiatives to Improve Cybersecurity

Since 2005, the “Cybersecurity Policy for Critical Infrastructure Protection” has been set as a common action plan shared between the government, which bears responsibility for promoting independent measures by critical infrastructure operators relating to critical infrastructure cybersecurity and implementing other necessary measures, and critical infrastructure operators which independently carry out relevant protective measures, and the new edition was published in 2022.

- The *Basic Act on Cybersecurity* stipulates Japan’s basic policy on cybersecurity as well as the fundamental responsibilities of the national and local governments. Under the Basic Act on Cybersecurity, critical infrastructure operators, including certain telecommunications carriers, shall endeavor to voluntarily and proactively secure cybersecurity and to cooperate with cybersecurity measures implemented by the national and local governments.
- Under the *Telecommunications Business Act*, telecommunications service operators shall have obligations to protect the secrecy of telecommunications, and to maintain and operate certain telecommunication facilities in compliance with the applicable technical standards established by the Ministry of Internal Affairs and Communications. These technical standards include certain requirements for network security.
- On December 16, 2022, the Japanese government approved a cabinet decision on security-related strategic documents: the National Security Strategy (NSS), National Defense Strategy (NDS), and Defense Buildup Program (DBP). The NSS is the principle for Japan’s national security strategy for the next 10 years, defining diplomatic and defense strategies in response to the new security environment. The NDS, renamed from the National Defense Program Guideline, defines the Japan Self-Defense Force’s (JSDF) defense strategy for the next decade, setting goals for national security and outlining approaches and means to

achieve them. The DBP, renamed from the Mid-term Defense Program, indicates a medium- to long-term development plan that includes the level of defense capability and the procurement plan.

Initiatives to Improve Coverage

The national coverage rate for fibre optic broadband services for households was 99.1% as of the end of March 2020, and services are not available for almost 530 thousand households in Japan. Based on the prefectural coverage rate for fibre optic broadband services, development of the fibre optic broadband network has been delayed in prefectures that have many remote islands or mountainous regions.

The current government aims to increase the area under fibre coverage to more than 99.9% of the country's landmass by 2028.

European Union

Overview of Resiliency Legislation and Regulator Frameworks

The Body of European Regulators for Electronic Communications (BEREC) is the regulator for the European Union (EU). It consists of representatives from the national regulatory authorities (NRAs) of each EU member state.

Its primary role is to promote the consistent application of the EU regulatory framework for electronic communications, ensure competition, and safeguard the interests of consumers and end-users.

BEREC provides guidance and advice to the European Commission, assists in the development of common approaches to regulation, and contributes to the harmonization of the telecommunications sector across the EU.

Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. An adequate level of protection must be ensured and the detrimental effects of disruptions on the society and citizens must be limited as far as possible.

The European Union Agency for Cybersecurity (ENISA), Executive Director, Juhan Lepassaar states that "The resilience of our EU critical infrastructures and technologies will highly depend on our ability to make strategic investments. I am confident that we have the competence and skills driving us to achieve our goal, which is to ensure we will have the adequate resources at hand to further develop our cybersecurity capacities across all economic sectors of the EU."

The European Union started in 2009 and focused on regulating cyber resiliency of electronic communication providers within the EU's telecommunications regulatory framework since the reform of the telecommunications package, and then expanded it through the NIS Directive to Operators of Essential Services (OES) and Digital Service Providers (DSP) that include particularly digital infrastructure provider and cloud computing service.

Initiatives to Improve Network Strength and Resilience

Electronic communication providers in the EU are required to notify security incidents that have a significant impact on the continuity of electronic communication services to the telecommunications NRAs in each EU member state.

Every year the NRAs report a summary to ENISA, covering a selection of these incidents, i.e., the most significant incidents, based on a set of agreed EU-wide thresholds. This is the 11th year ENISA is publishing an annual incidents report for the telecommunications sector. ENISA started publishing these annual reports in 2012. Mandatory incident reporting has been part of the EU’s telecommunications regulatory framework since the 2009 reform of the telecommunications package: Article 13(a) of the Framework directive (2009/140/EC) came into force in 2011.

The mandatory reporting of incidents under Article 13(a) had a specific focus on security incidents with a significant impact on the functioning of each category of telecommunication services. Over the years, the regulatory authorities have agreed to focus mostly on network/service outages (type A incidents – Service outage, e.g., continuity, availability – an outage caused by a cable cut caused by a mistake by the operator of an excavation machine used for building a new road would be categorized as a type A incident).

This would exclude from the scope of these reports targeted attacks, e.g., those involving the use of SS7 protocol vulnerabilities, SIM Swapping frauds, or even more extended attacks that nevertheless do not cause outages. The relevant update of the EU telecommunications rules, namely the European Electronic Communications Code (EECC), that was expected to be harmonized in Member States by the end of 2020, includes a broader scope on the requirements for incident reporting in Article 40. These requirements explicitly include, for example, breaches of confidentiality. 2021 is the second time ENISA has also received three (3) type B reports of incidents (breaches of confidentiality).

It is important to note that the telecommunications security incidents that are reported to national authorities are only the major incidents, i.e., those with significant impacts. Smaller incidents, affecting small percentages of population such as SIM Swapping attacks are not reported.

Under Article 40 of the EECC the incident reporting requirements have a broader scope, including not only outages but also, for instance, breaches of confidentiality. In addition, there are more services within the scope of the EECC, including not only traditional telecommunications operators but also, for example, over-the-top (OTT) providers of communications services (such as messaging services like Viber and WhatsApp). In 2020, the annual reporting guideline was updated to include new thresholds for annual summary reporting to ENISA. These combine quantitative and qualitative parameters as well as the notification of security incidents affecting not only the services of fixed and mobile internet and telephony, but also number-based interpersonal communications services and/or number independent interpersonal communications services (OTT communications services).

Initiatives to Improve Cybersecurity

The EU also expanded this telecommunications regulation to Operators of Essential Services (OES) and Digital Service Providers (DSP) that include particularly digital infrastructure provider and cloud computing service.

The NIS Directive represents the first EU-wide legislation on cybersecurity, with the objective of achieving a high common level of cybersecurity for all Member States. One of the three (3) pillars of the NIS Directive is the implementation of risk management and reporting obligations.

The ENISA is evaluating and measuring each year NIS impacts on cybersecurity. ENISA 2022 report marks the third iteration of ENISA's NIS Directive Investments report, which collects data on how Operators of Essential Services and Digital Service Providers identified in the European Union’s NIS Directive invest their cybersecurity budgets and how this investment has been influenced by the NIS Directive.

Cybersecurity Investments in the EU: Is the Money Enough to Meet the New Cybersecurity Standards? (NIS Investments 2022)

On January 16, 2023, the Directive (EU) 2022/2555 (known as NIS2) entered into force replacing Directive (EU) 2016/1148. ENISA considers that NIS2 improves the existing cyber security status across EU in different ways by:

- creating the necessary cyber crisis management structure (CyCLONe);
- increasing the level of harmonization regarding security requirements and reporting obligations;
- encouraging Members States to introduce new areas of interest such as supply chain, vulnerability management, core internet and cyber hygiene their national cybersecurity strategies;
- bringing novel ideas such as the peer reviews for enhancing collaboration and knowledge sharing among the Member States;
- covering a larger share of the economy and society by including more sectors which means that more entities are obliged to take measures to increase their level of cybersecurity.

The Cyber Resilience Act, which we presented last November 2022, puts in place minimum cybersecurity requirements for products and software that are placed on the single market regardless of where they are produced. It includes telecommunications players. In doing so, Europe is filling a legal vacuum. The Act will raise the level of cybersecurity "by default" in all products and introduce a concept of "cybersecurity by design."

While it will be possible to make self-declarations of conformity for 90% of the products, for about thirty products, the most critical in terms of cyber risk – such as industrial firewalls, routers, or operating systems – the conformity examination will have to be carried out by a third party. And the Commission will be able to request the withdrawal from the market of a product that presents a cyber risk.

This legislation has the potential to set a global standard for cybersecurity. Indeed, the new cybersecurity policy announced by the US a month ago draws heavily on NIS and the Cyber Resilience Act.

The EU continues to ensure the implementation of the 5G cybersecurity toolbox to deploy secure networks. All Member States have unanimously agreed to exclude so-called high-risk providers from their networks (CORE and RAN). But while 23 Member States have passed laws to this effect, only 7 have implemented them and excluded in one way or another those providers that they considered to pose a security risk.

Initiatives to Improve Coverage

The 2nd generation of the Connecting Europe Facility (CEF-2 programme) “Digital” strand (2021-2027) aimed to support and catalyze investments in digital connectivity infrastructures of common interest. The programme has a total budget of €2,065 billion, of which €1,7 billion is managed by the Health and Digital Executive Agency (HaDEA). Actions foreseen to be supported under CEF-2 Digital include:

- Deployment of very high-capacity networks, including 5G systems, capable of providing Gigabit connectivity in areas where socio-economic drivers are located (e.g., schools, universities, hospitals, transport hubs, public administrations), and access to those networks;
- Uninterrupted coverage of 5G systems on all major transport paths, including the trans-European transport networks;

- Deployment of new or significant upgrade of existing backbone networks including submarine cables, both within and between the EU Member States and third countries; and
- Implementation of digital connectivity infrastructures related to cross-border transport and energy projects and/or the support of operational digital platforms directly associated to these infrastructures.

The first generation of the Connecting Europe Facility (CEF-1), “Telecom” strand (2014-2020) facilitated the cross-border interaction between public administrations, businesses, and citizens, by deploying Digital Service Infrastructures, connectivity in local communities (WiFi4EU) and broadband networks (through equity and loan instruments).

With a budget of approximately €1 billion, of which €203 million is now managed by HaDEA, the programme supported two types of digital services:

- Reusable digital services that can be integrated into/combined with other projects, covering eIdentification, eSignature, eInvoicing, eDelivery and Automated Translation (building blocks); and
- Specific digital service infrastructures covering areas such as cyber security, eHealth, European Platform for Digital Jobs and Skills, Business Registers Interconnection System, Europeana, eProcurement, Electronic Exchange of Social Security Information, Public Open Data, European e-Justice Portal, Safer Internet, and online dispute resolution.

Broadband Europe promotes the EU Commission's strategy on Connectivity for a European Gigabit Society by 2025 as well as the vision set by the Digital Decade for Europe’s digital transformation by 2030 to connect European citizens and businesses with very high-capacity networks.

This Gigabit Society vision for 2025 relies on three (3) main strategic objectives:

1. Gigabit connectivity for all the main socio-economic drivers;
2. Uninterrupted 5G coverage for all urban areas and major terrestrial transport paths; and
3. Access to connectivity offering at least 100 Mbps for all European households.

The ambition of the Digital Decade is that by 2030 all European households are covered by a Gigabit network, and all populated areas are covered by 5G.

4.2 Regulatory Outcomes of Network Outages and Disruptions

Cyber Security

Table 18. Cyber Security Outages/Degradations

REGION	DATE	INFRASTRUCTURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
European Union	26/09/20	Wireless	In September of 2020, the telecommunications service provider (TSP) Magyar Telekom (subsidiary of Deutsche Telekom) experienced an outage caused by a distributed denial of service (DDOS). As per Magyar, the volume of the attack was 10 times higher than amount of traffic typically seen in DDOS events.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
European Union	03/05/22	Satellite	In May of 2022, the TSP Orange experienced an outage event when services from Viasat (an american satellite operator) were interrupted by a 'cyber event'. The outage effected approx. 40K satellite internet subscribers across the European Union.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
South Korea	29/01/23	Wireless	In January 2023, the South Korean TSP LG U+ experienced network disruptions of its mobile data services. The disruption event lasted on total of 63 minutes on average and the cause of the outage is said to be DDoS attack.	The Ministry of Science and Information and Communication Technology and Korea Internet and Security Agency started an investigation into recent data breaches and outages. Ministry issued a strong warning to LG U+, regarding the lack of basic breach response system. Ministry also demanded LG U+ implement responsible corrective measures and push for policy improvements, including regulation revisions regarding major TSP breach response systems.

Environmental Factors

Table 19. Environmental Outages/Degradations

REGION	DATE	INFRASTRUCTURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
New Zealand	07/12/19	Wireless and Wireline – Terrestrial	In December of 2019, the New Zealand TSP Spark experienced an outage caused by extreme rainstorms and flooding. Outage occurred when a fibre-optic cable was severed between the cities of Ashburton and Timaru, leaving thousands of customers without service.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
Australia	17/01/20	Wireless and Wireline – Terrestrial	In January 2020, Australia experienced a severe bushfire season which caused outages across all major TSP networks. According to the ACMA nearly 1,400 telecommunications facilities were directly or indirectly affected during the summer bushfires, during which the average outage was three and a half days and the longest was 23 days. Root cause for majority of outages was electricity supply failures, National Broadband Network (NBN) deployed generators to restore power to services once immediate bushfire event had passed.	In April of 2020, the AMCA released a report detailing the impacts of the 2019 - 2020 bushfires on the TSPs network. Observations include root cause analysis and restoration actions analysis. No recommendations or legislative actions provided.
New Zealand	27/01/23	Wireless and Wireline – Terrestrial	In January 2023, Auckland New Zealand experienced a severe weather event that caused small, localized flooding. Flooding led to outages in the TSPs (Chorus and Spark) networks caused by electrical supply failures.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
New Zealand	13/02/23	Wireless and Wireline – Terrestrial	In February of 2023, New Zealand was hit by Cyclone Gabrielle which caused major outages and	In immediate response to the event, TSPs and emergency response teams worked to fix impacted networks. Relying

REGION	DATE	INFRASTRUC TURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
			widespread damage across the country. This event effected all major New Zealand TSPs (Vondafone, 2degrees, etc.) who experienced widespread outages due to infrastructure damage and/or loss of power to cell sites.	largely on the deployment of backup generators to impacted sites. Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).

Operational Errors

Table 20. Operational Outages/Degradations

REGION	DATE	INFRASTRUC TURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
United Kingdom	06/12/18	Wireless	In December 2018, the TSP O2 suffered a major network failure which resulted in a loss of data services for the majority of its customers across its 2G, 3G and 4G networks. Root cause of the failure was identified as an expired software certificate.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
New Zealand	13/03/19	Wireless	In March of 2019, the TSP Spark experienced an outage that left customers in a region of Auckland without voice, mobile data, and SMS services for three (3) days. Cause of outage was identified as issue with the Chorus fibre link that links the regions cell tower to rest of the Spark network.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
United Kingdom	17/10//19	Wireless	In October of 2019, the British TSP Three experienced an outage which effected the voice, text, and data services for millions of its customers. The cause of was identified as an error that occurred during routine repairs to Three’s 3G network infrastructure.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).

REGION	DATE	INFRASTRUCTURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
European Union	23/11/20	Wireless	In March of 2019, the TSP Vodafone experienced a widespread outage effecting more than 100K users within its German Network. Outage lasted approximately five hours for most customers and the cause of was identified as a failure of control equipment.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
South Korea	01/10/21	Wireless and Wireline – Terrestrial	In October 2021, the South Korean TSP KT Corp experienced widespread outages of internet and phone services due to a routing error. Routing error was caused by the mistake of an employee of a KT subcontractor. Network restored within 1 hour.	In accordance with its own compensation policy, KT paid ~ 40 billion won ($33.97 million) in compensation to customers of its wired and wireless services. Additionally, KT said it would incorporate a testbed that will simulate the routing process before they are performed, to prevent any recurrence, and expand an existing system that blocks routing error dissemination.
Japan	14/10/21	Wireless	In October of 2021, the Japanese TSP Nippon Telegraph and Telephone (NTT) Docomo experienced a network outage that affected approximately 12.9 million users. Outage caused by malfunction during work on NTT Docomo's network of payment equipment, and affected users had no access to voice or data services for up to 29 hours.	The Ministry of Internal Affairs and Communications (MIC) described incident as having enormous societal impact and stated that sufficient steps must be taken to ensure it does not happen again. NTT Docomo issued an incident report and introduced a new system to separately control mobile phones when system failures occur.
New Zealand	03/02/22	Wireless	In February of 2022, the TSP 2degree experienced an outage that effected thousands of customers across New Zealand. Customers affected reportedly had no access to the TSP’s network for over an hour. The cause of outage is unknown but was reported as an	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).

REGION	DATE	INFRASTRUCTURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
			"internal issue" by a 2degree representative.	
Japan	05/07/22	Wireless	In July 2022, the Japanese TSP KDDI Corporation experienced a network outage that affected nearly 22.78 million voice over long term evolution (VoLTE) service customers and 7.65 million data (4G/5G) customers over a period of three (3) days. Outage occurred during routine maintenance when a router for VoLTE calls was replaced but lead outage of texting and phone call (including emergency line) services.	KDDI issued a report on the incident to the MIC on July 29, 2022. Report provided an overview of the incident (cause, scope, and impact), outline of recurrence prevention measures and a description of a refund for provided to effected customers (~200 Yen/customer).
New Zealand	10/04/22	Wireless	In October of 2022, a technical issue led to thousands of 2degree customers being unable to access calling, text, or data services. Outage lasted approximately 2 hours before being resolved.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
Japan	17/12/22	Wireless	In December of 2022, the Japanese TSP NTT Docomo suffered an outage in their data network due to a malfunction of communications equipment. Outage only effected mobile data services and did not affect voice call services.	The MIC issued a "stern warning" to NTT Docomo and issued guidance, instructing NTT to implement various measures to prevent recurrence.
Australia	01/03/23	Wireless	In March of 2023, the TSP Optus experienced an outage that effected rural areas including Copmanhurst, Whiteman Creek, Jackadgery. Hundreds of customers were unable to make phone calls or send/receive text messages, additionally the	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).

REGION	DATE	INFRASTRUCTURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
			Copmanhurst Rural Fire Service (RFS) were unable to ACTIV apps which alert them when emergencies occur and allow them to communicate directly with one another when responding to call outs.	
Japan	03/04/23	Wireline – Terrestrial	In April of 2023, the Japanese TSPs NTT East and West experienced a network outage that impacted 446K internet lines and 233K landlines. Services impacted included calls to emergency services such as 110 and 119. Cause of outage was reported as "equipment failure" and services were restored within approximately 3 hours.	During an online press conference officials from NTT acknowledge the outage as a "serious incident" under law. The communications ministry may issue administrative orders; however, the incident is still currently under investigation.
United Kingdom	04/04/23	Wireless	In April 2023, the British TSP Virgin Media experienced an outage that effected more than 50K customers’ access to broadband internet services. Root cause of issue was identified as a technical issue.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
European Union	14/04/23	Wireless	In April 2023, the TSP Vondafone experienced an outage effecting its mobile phone network in the Netherlands. Outage effected impacted customers’ ability to make calls, including emergency services. Outage causse was identified as an internal malfunction.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
Australia	17/04/23	Satellite	In April 2023, satellite provider Inmarsat experienced an outage on its I-4 F1 satellite which provides L-band services for East Asia and the Pacific region. Cause of outage was power loss	On April 19 Inmarsat confirmed that all safety services and broad band global area network services had been restored. However, no public penalties or reporting provided by regulators.

REGION	DATE	INFRASTRUCTURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
			due to loss of power from one of its solar arrays. Outage impacted variety of services provided by the satellite including GPS signals used by horticultural systems, maritime safety systems and the shipping industry.	
United States	25/04/23	Wireless	In April of 2023, Shenandoah Telecommunications Company (Shentel) experienced an outage of emergency 911 routing services in, Wyoming, Lewis, and McDowell counties. Outage caused by operational error while Shentel was replacing Session Border Controllers and transitioning customers to a new 911 routing service.	To settle this matter, Shentel was required by the FCC to implement a compliance plan and pay a $227,200 civil penalty.
Australia	09/05/23	Wireless	In May of 2023, the Australian TPS Telstra Group Limited experienced a major outage impacting customers across New South Wales and Queensland. Customers impacted experienced issues making and receiving calls and text messages. However, Telstra stated that calls to triple-0 and mobile data usage were not affected by the outage. Outage caused by issue with a planned upgrade to the network which caused flow-on effects.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).

Third Party Factors

Table 21. Third Party Factors Outages/Degradations

REGION	DATE	INFRASTRUC TURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
United States	15/06/20	Wireless	In June of 2020, T-Mobile experienced an outage impacting customers' experience accessing VoLTE and texting services. The original cause of outage was suspected to be due to a DDoS attack, however, root cause was identified as an overload issue caused by a leased fibre circuit failure from a third-party provider in the Southeast. Issue was resolved the same day as of 10:03 pm PST.	On June 15th, 2020, the FCC announced that it will launch an investigation. The investigation concluded with a compliance plan and $19,500,000 settlement payment.
Japan	12/09/22	Wireless	In September of 2022, the Japanese TSP Rakuten Mobile, Inc. experienced a network disruption that affected 110K phone service customers and 1.3 million customers with a data transmission disruption. The cause of the outage was software malfunction in equipment at a data center.	The MIC issued a warning to the Communications Service Provider and inspected data centre to ensure corrective measures are being put in place.
Australia	20/04/23	Wireless	In April 2023, the Australian TSP MATE experienced a major outage effecting broadband and mobile internet services of customers across Australia. Most notable disruptions are occurred in New South Wales, Victoria, and Western Australia states. Cause of outage was due to a technical fault affecting a data center in Sydney.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).

Unintentional/Intentional Damage

Table 22. Unintentional/Intentional Damage Outages/Degradations

REGION	DATE	INFRASTRUCTURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
South Korea	15/11/18	Wireless and Wireline – Terrestrial	In November of 2018, the South Korea's TSP KT Corp, experienced an outage which effected landline, mobile and internet networks in parts of Seoul. The outage was caused by a fire in a basement where KT's base transceiver station was located. The fire took 10 hours to fully extinguish, and the outage lasted approximately 24 hours total.	To discuss countermeasures, KT and South Korean Broadband officials attended a government meeting on Sunday morning that also involved the Ministry of Science and ICT and the Korea Communications Commission. KT set aside compensation for affected individuals and committed to putting together stringent measures to prevent a recurrence.
New Zealand	11/05/20	Wireless	In May 2020, the TSP Spark experienced an outage of mobile voice, text and data services after a bad actor committed an act of arson on a cell tower. Spark is deployed a temporary cell tower tomorrow to provide additional capacity to the local area while the permanent cell tower was repaired.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
European Union	27/04/22	Wireline – Terrestrial	In April 2022, France’s telecommunication network experienced a major outage that was linked to a coordinated act of vandalism. Across France customers were left without access to the broadband network when multiple underground cables were damaged by malicious actors.	Following the incident an investigation was launch by local police and the French Telecoms Federations. The investigation has not resulted in any regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).
New Zealand	13/05/22	Wireline – Terrestrial	In May 2020, the TSP Chorus experienced an outage of its fibre internet services after a rodent had chewed through fibre cables. The outage effected approximately	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).

REGION	DATE	INFRASTRUC TURE TYPE	OUTAGE DESCRIPTION	OUTCOME DESCRIPTION
			1000 customers and lasted a total of 33 hours.	
United Kingdom	21/10/22	Wireline - Subsea	In October 2022, TSPs in Shetland experienced an outage that effected landline, mobile and internet services. The cause of the outage was a cut in a subsea cable that connects the island with the Scottish mainland network. Damage to cable was suspected to be caused accidentally by a UK-registered trawler.	Declared as a major incident, this network outage was reported Ofcom under the *Telecommunications (Security) Act of 2021*. Ofcom's review noted that restoration of the services was achieved by increasing power output at the source. Over the next ten days, repairs were carried out across both the primary and secondary fibre cables to the islands, leading to a permanent restoration of services. Additionally, as part of its R100 Programme, the Scottish Government has laid 16 new subsea cables6 which is connecting 15 Scottish islands to faster and more reliable broadband services.
European Union	16/02/23	Wireline - Terrestrial	In February 2023, the TSP Deutsche Telekom experienced an outage that effected major airline Lufthansa Group and caused major delays and flight cancellations. Outage was caused when Builders working for state-owned railway company Deutsche Bahn unintentionally cut out four cables that were buried more than 16 feet deep.	Unable to verify if outage resulted in regulatory actions (e.g., incident reports, investigations, legislative actions, recommendations, fines).

4.3 Scan of Jurisdictional Low Earth Orbit Satellite Initiatives

This Low Earth Orbit (LEO) Satellite scan across the jurisdictions is a current snapshot of some of the LEO coverage examples observed across the jurisdictions assessed. Note, this is a very dynamic and changing capability, and Gartner expects that the information provided here will be outdated within a matter of weeks (vs. months or years). The assessment was evaluated across basic categories of internet, messaging, and voice capabilities.

Table 23. Scan of Jurisdictional LEO Satellite Initiatives

Region	Description of Ongoing LEO Satellite Initiatives
Unites States	▪ The Federal Communications Commission (FCC) has approved licenses for deployment of LEO satellite constellations from the following companies: SpaceX, Telesat, Kepler, LeoSat and Project Kuiper. These licenses authorize the companies to provide satellite internet services to US entities. ▪ In January of 2022, the FCC granted Virginia based company, Lynk, the first license to offer satellite-direct-to-standard-phone communications (SCS). SCS is an acronym defined by FCC (Supplemental-Coverage-From-Space). The industry seems to be now using Direct to Device (D2D); however, this could change again. ▪ In 2022 Lynk conducted pre-commercial tests where they successfully used SCS to connect 6000 devices to send and receive messages. Current objective is to launch commercial services in the spring of 2023. ▪ AT&T has asked the FCC for permission to use SCS technology from AST SpaceMobile on some of its commercial spectrum. AT&T has conducted satellite-direct-to-phone tests with AST SpaceMobile on Band 14 spectrum, but the nationwide spectrum license for the airwaves belongs to the FirstNet Authority. ▪ In August 2022, SpaceX and T-Mobile announced a plan to deliver space-to-ground service to mobile phones in areas not covered by T-Mobile's cellular network.
United Kingdom	▪ In April of 2023, the Department of Science, Innovation and Technology announced that London-headquartered OneWeb (in partnership with BT and Clarus) will deploy its low-Earth orbit (LEO) internet satellite technology to provide satellite internet services to customers on Shetland Islands and Lundy Islands. The OneWeb trial was announced as part of the department's Wireless Infrastructure Strategy.
Australia	▪ In March 2022, Telstra, and UK based OneWeb signed a 10-year deal that requires Telstra to build and maintain three new teleports in Australia to provide ground support in the southern hemisphere for OneWeb's growing fleet of low-earth orbit satellites.
New Zealand	▪ In 2023, two of New Zealand's largest telecommunications providers, One NZ and 2degrees have signed deals with satellite providers (SpaceX and Lynk respectively). Initial services will be limited to text messages with voice and data service to follow.
Japan	▪ In December 2022, KDDI and SpaceX launched the first mobile tower in Japan powered by SpaceX and began offering satellite internet services commercially in Hatsushima. KDDI plans to expand coverage to a total of 1,200 remote towers. ▪ In November 2022, Japan's fourth largest telecommunications network operator Rakuten Mobile was issued with preliminary experimental test station license to carry out a series of mobile communication tests and preliminary verification in Japan. In April 2023, Rakuten Mobile and US-based satellite designer and manufacturer AST SpaceMobile completed the world's 'first' successful two-way voice call with standard mobile phones using the BlueWalker 3 (BW3) satellite.

European Union	▪ As part of the EU's Secure Connectivity Programme the European Parliament and the European Council, announced plans to deploy an EU satellite constellation called 'IRIS^2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite)". (Deutsche Telecom and Orange Consortium) ▪ The EU's Secure Connectivity Programme will follow an incremental approach with the goal of delivering initial services (internet and direct to phone) in 2024 and reach full operational capability by 2027.

4.4 References

United States

- Federal Communications Commission | The US (fcc.gov)
- About the FCC | Federal Communications Commission
- *Telecommunications Act of 1996* | Federal Communications Commission (fcc.gov)
- Laws & Regulations - Telecommunications Industry: A Research Guide - Research Guides at Library of Congress (loc.gov)
- *Telecommunications Act* of 1996 | Federal Communications Commission (fcc.gov)
- FCC Releases Open Internet Order | Federal Communications Commission
- Digital Equity Act of 2021 (census.gov)
- Programs | Internet for All
- FCC Acts to Improve Network Resiliency During Disasters | Federal Communications Commission
- Executive Order on Improving the Nation's Cybersecurity | The White House
- Federal Funding | BroadbandUSA (doc.gov)
- Secure and Resilient Mobile Network Infrastructure and Emergency Communications R&D Program | Homeland Security (dhs.gov)
- Emergency Communications R&D Project | Homeland Security (dhs.gov)
- Emergency Communications | Cybersecurity and Infrastructure Security Agency CISA
- Statewide Communication Interoperability Plans Workshops | CISA
- Biden-Harris Administration Launches $1.5 Billion Innovation Fund to Develop a More Competitive and Diverse Telecommunications Supply Chain | National Telecommunications and Information Administration (ntia.gov)
- Wireless Innovation Fund Notice of Funding Opportunity | National Telecommunications and Information Administration (ntia.gov)
- Connect America Fund (CAF) | Federal Communications Commission (fcc.gov)
- Lifeline Program for Low-Income Consumers | Federal Communications Commission (fcc.gov)
- E-Rate - Schools & Libraries USF Program | Federal Communications Commission (fcc.gov)
- Rural Healthcare Program | Federal Communications Commission (fcc.gov)
- 911 and E911 Services | Federal Communications Commission (fcc.gov)
- AT&T, Verizon, others fined for 911 outages | Light Reading
- Verizon, Straight Path pay $614 million civil penalty to U.S. FCC: statement | Reuters
- Data Protection Laws and Regulations Report 2022-2023 US (iclg.com)
- New US Privacy Law May Give Telecoms Free Pass on $200 Million Fines (vice.com)
- VIII. Privacy — Telephone Consumer Protection Act (fdic.gov)
- Data Protection Laws and Regulations Report 2022-2023 US (iclg.com)

United Kingdom

- Home - Ofcom
- What is Ofcom? - Ofcom
- Telecoms security: proposal for new regulations and code of practice - GOV.UK.
- Telecommunications Networks – a vital part of the Critical National Infrastructure, v1.1 - EC-RRG (publishing.service.gov.uk)
- Future_Telecoms_Infrastructure_Review.pdf
- E02781980_Telecommunications_Security_CoP_Accessible.pdf
- Ofcom fines O2 £150,000 for providing inaccurate and incomplete information - Ofcom
- Ofcom fines O2 £10.5m for overcharging customers - Ofcom
- Ofcom fines Sepura £1.5m for breaking competition law - Ofcom

- Ofcom fines BT £42,500 over inaccurate information
- The Electronic Communications (Universal Service) (Broadband) Order 2018 (legislation.gov.uk)
- Statement: Delivering the Broadband Universal Service - Ofcom
- UK government imposes its own security obligations on telecoms sector - Telecoms.com
- Regulation of VoIP Services: Access to the Emergency Services - Ofcom
- Emergency Services Network: overview - GOV.UK (www.gov.uk)
- Investment in telecoms innovation and R&D - GOV.UK (www.gov.uk)
- 5G Supply Chain Diversification Strategy - GOV.UK (www.gov.uk)
- UK Wireless Infrastructure Strategy - GOV.UK (www.gov.uk)

Australia

- Homepage | ACMA
- Fines, warnings and the ACMA’s 2021-22 priorities: The telco industry in May (holdingredlich.com)
- Telstra pays $1.5 million penalty for breaching customer rights | ACMA
- Australian telecommunications firms fined $22.1 mln for false internet speed claims | Reuters
- TPG forced to pay $2m fine after High Court loss - Telco/ISP - iTnews
- NBN Co faces $30-a-day fines for unfixed faults - Telco/ISP - iTnews
- Telstra Triple Zero outage: Report reveals 1400 calls were unable to be connected (smh.com.au)
- iTWire - Telstra could face big fine over triple-zero outage
- Strengthening Telecommunications Against Natural Disasters (STAND) - Temporary Telecommunications Infrastructure Deployment | business.gov.au
- Telecommunications Disaster Resilience Innovation Program | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- USO | ACMA
- Universal Service Obligation | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- National Broadband Network | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- NBN legislative framework | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- National Broadband Network – Parliament of Australia (aph.gov.au)
- NBN Co welcomes $2.4 billion Government investment to enable 1.5 million more homes and businesses to upgrade to full fibre nbn | nbn
- Provision of Satellite Connections to Emergency Services and Evacuation Centres | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- Boosting temporary infrastructure capabilities | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- Cyber Security | Australian Signals Directorate (asd.gov.au)
- Telecommunications security reforms | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- Cyber-security-incident-reporting.pdf

New Zealand

- Ministry of Business, Innovation & Enterprise: Emergency Call Services
- Emergency Calls in New Zealand | 2degrees
- Universal Service Obligation | Department of Infrastructure, Transport, Regional Development, Communications and the Arts

- *Telecommunications Act 2001* No 103 (as at 01 September 2022), Public Act – New Zealand Legislation
- A review of New Zealand Telecommunications: Legislation, Regulations and Recommendations | Telsoc
- Govt releases vision for New Zealand's digital connectivity future | Ministry of Business, Innovation & Employment (mbie.govt.nz)
- Homes, businesses to benefit from upgrade to rural broadband | Beehive.govt.nz
- More rural broadband for regional communities | Beehive.govt.nz
- Govt delivers connectivity for rural and remote households | Beehive.govt.nz
- Broadband and mobile programmes | Ministry of Business, Innovation & Employment (mbie.govt.nz)
- New Zealand - Data Protection Overview | Guidance Note | DataGuidance
- Consolidated Telecommunications Information Privacy Code 2020 | Legal research | DataGuidance
- New Zealand - Data Protection Overview | Guidance Note | DataGuidance
- New Zealand's Cyber Security Emergency Response Plan | Department of the Prime Minister and Cabinet (DPMC)

Japan

- *Telecommunications Information Privacy Code 2020*
- Japan: *Telecommunications Business Act* amendments introducing new regulations for cookies and user identification information - Baker McKenzie InsightPlus
- Key telecommunications laws, regulations and policies in Japan - DLA Piper Telecommunications Laws of the World (dlapiperintelligence.com)
- New Japanese Regulation on Telecomunications Businesses Provided by Foreign Business Operators | PwC Japan Group'
- Telecoms, Media & Internet Laws and Regulations Report 2023 Japan (iclg.com)
- Ribbon Deploys Colt Japan's Emergency Calling Service | Ribbon Communications
- *Disaster Countermeasures Basic Act* - Climate Change Laws of the World (climate-laws.org)
- Access System Technologies for Service Diversification | NTT Technical Review (ntt-review.jp)
- National center of Incident readiness and Strategy for Cybersecurity | NISC
- Japan to bring fiber-optic networks to 99.9% of households by 2028 | The Japan Times

European Union

- The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament
- NIS Directive — ENISA
- For Telcos — ENISA
- Telecom Security Incidents 2021 — ENISA
- Cyber Resilience Act | Shaping Europe's digital future
- Connecting Europe Facility (CEF Digital) | EU Funding Overview
- Support for Broadband rollout | Shaping Europe's digital future
- NIS Investments 2022 — ENISA
- NIS Investments Report 2021 — ENISA
- NIS Investments Report 2020 — ENISA
- Enabling and managing end-to-end resilience — ENISA
- ENISA Report Highlights Resilience of Telecom Sector in Facing the Pandemic — ENISA

Jurisdictional Structure and Governance – references:

- What We Do | Federal Communications Commission

- About CISA | CISA
- About NTIA | National Telecommunications and Information Administration
- What is Ofcom? - Ofcom
- Department for Science, Innovation and Technology - GOV.UK
- About the ACCC | ACCC
- ACMA-statement-of-intent-pdf.pdf
- New Zealand Infrastructure Commission/Te Waihanga Act 2019 No 51 (as at 01 September 2022), Public Act Contents – New Zealand Legislation
- Information Brochure on the MSIT
- Bundesnetzagentur - About us
- Arcep | Arcep
- Why Korea fell 27 spots in world internet speed rankings to 32nd place last year
- Korea's internet speed ranking falls to 34th: report

Government Drivers to Improve Resilience – references:

- Biden-Harris Administration Launches $1.5 Billion Innovation Fund to Develop a More Competitive and Diverse Telecommunications Supply Chain | National Telecommunications and Information Administration (ntia.gov)
- E02781980_Telecommunications_Security_CoP_Accessible.pdf
- Provision of Satellite Connections to Emergency Services and Evacuation Centres | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- Cyber Security | Australian Signals Directorate (asd.gov.au)
- Telecommunications security reforms | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- National Broadband Network – Parliament of Australia (aph.gov.au)
- NBN legislative framework | Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- NBN Co welcomes $2.4 billion Government investment to enable 1.5 million more homes and businesses to upgrade to full fibre nbn | nbn
- Homes, businesses to benefit from upgrade to rural broadband | Beehive.govt.nz
- New Zealand's Cyber Security Emergency Response Plan
- Japan Sets Aside $450 Million Fund for 6G - Telecom Review Asia Pacific
- The Booklet of Best Practicesof resilient ICT systems in JAPAN
- Japan to bring fiber-optic networks to 99.9% of households by 2028 | The Japan Times
- EU Adaptation Strategy

Regulatory Obligations – References:

- Universal Service | Federal Communications Commission (fcc.gov)
- 911 and E911 Services | Federal Communications Commission (fcc.gov)
- AT&T, Verizon, others fined for 911 outages | Light Reading
- Verizon, Straight Path pay $614 million civil penalty to U.S. FCC: statement | Reuters
- Telecommunications service obligations | Ministry of Business, Innovation & Employment (mbie.govt.nz)
- The Customer Service Guarantee | ACMA
- Automatic compensation: What you need to know - Ofcom
- Emergency call services | Ministry of Business, Innovation & Employment (mbie.govt.nz)
- Bundesnetzagentur - Public safety
- BSI - Legal basis
- Telecoms, Media & Internet Laws and Regulations Report 2023 Japan (iclg.com)
- Ribbon Deploys Colt Japan’s Emergency Calling Service | Ribbon Communications

- EUR-Lex - l24108h - Affordable telecommunications services - users' rights
- Communications Security, Reliability, and Interoperability Council | Federal Communications Commission
- CSRIC_WG 9_Backup_Power_Reccomendations__11-24-2014.pdf
- Inventory of Reports
- Our network security and network resilience work - Ofcom
- Guidance: Protecting access to emergency organisations when there is a power cut at the customer's premises
- The NIS Regulations 2018 - GOV.UK
- Impacts of the 2019-20 bushfires on the telecommunications network | ACMA
- Federal Network Agency - Security requirements
- Code Compliance | NZ Telecommunications Forum
- ETSI TR 102 445 V1.2.1 (2023-04) Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness

Voluntary Industry Measures – References:

- Communications Security, Reliability, and Interoperability Council | Federal Communications Commission
- Communications Security, Reliability, and Interoperability Reports | Federal Communications Commission
- Disaster Information Reporting System (DIRS) | Federal Communications Commission
- Electronic Communications Resilience and Response Group
- ETSI TR 102 445 V1.2.1 (2023-04) Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness

Other Initiatives and Technologies – References:

- FCC approves SpaceX, Telesat, LeoSat and Kepler internet constellations - SpaceNews
- International Bureau Grants Kuiper Satellite Modification | Federal Communications Commission
- Engadget - Amazon secures key FCC approval to deploy its Project Kuiper broadband satellites
- FCC grants Lynk first license for commercial satellite-direct-to-phone service - Urgent Comms
- Lynk announces deployments, plans for spring satellite-direct-to-phone commercial service - Urgent Comms
- Nextivity supports satellite-direct-to-phone operations on FirstNet spectrum, looks to upgrade HPUE next year - Urgent Comms
- Ars Technica - A Virginia company has connected mobile phones directly to satellites
- Arts Technica - Forget 5G wireless, SpaceX and T-Mobile want to offer Zero-G coverage
- https://www.uktech.news/deep-tech/oneweb-trials-20230411
- Telstra signs 10-year teleport support deal with OneWeb | ZDNET
- One NZ and 2degrees sign up with satellite providers
- KDDI launches the 1st Mobile Tower powered by SpaceX's Starlink in Japan
- Rakuten Mobile given preliminary licences to test LEO
- Rakuten Mobile and AST SpaceMobile claim a 'first' with ground-breaking mobile broadband call
- Welcome IRIS²: Infrastructure for Resilience, Interconnectivity and Security by Satellite
- Deutsche Telekom and Orange head up consortium in bid for EU satellite constellation