July 2024

Public Safety Mission Critical Communication: Is this Critical Infrastructure?

This paper highlights how emergency communications are dealt with in terms of critical infrastructure across several jurisdictions.

It has been produced by the Collaborative Coalition for International Public Safety, CC:IPS, a collective who, together, pledge to promote, support and improve emergency communications services utilising the most current and commonly accepted technologies, standards, and best practices.

Global Statement

Through this paper, our goal is to provide Public Safety practitioners worldwide with information to understand the critical nature and role of emergency communications, including 3-digit emergency call systems such as 000/112/911/999, within their own national Critical Infrastructure (CI) framework. A document that shares various countries' positions is an important first step in enabling others to benchmark their own stance and the implications.

Objective of this Paper

To understand where mission critical communications are recognised and protected in legislation as an “ecosystem” that comprises the critical infrastructure and human resources that combine to provide the capabilities Public Safety Agencies need to respond to and protect lives, and property in a manner that meets public expectations and those of First Responders personal safety health and wellbeing.

The objective of the paper is to provide information about how mission critical communication systems and infrastructure are dealt with by different governments. It does not set out to make recommendations; instead, it is for the reader to use the information provided as background research.

The definition of Critical Infrastructure differs between jurisdictions; for example, Australia summarises Critical Infrastructure as *'those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect the nation’s ability to conduct national defence and ensure national security.’*

Summary of Findings

Emergency call systems have varying degrees of complexity with their many components. On this basis, organisations (which can include governments, emergency agencies, etc…) that are considering designating certain parts of Critical Infrastructure, should carefully consider key aspects, such as single points of failure and the stakeholders which are critical to it.

There are views from different jurisdictions that emergency call systems should be Critical Infrastructure. This, however, is rarely the case. The findings in this paper are summarised in the following table. The information is based upon that available at the time of research.

Country	Summary
Australia	Emergency communications is NOT designated as critical infrastructure
Canada	9-1-1 infrastructure IS designated as critical infrastructure; emergency communications is not.
European Union	Emergency communications are NOT considered as critical infrastructure. However, the facilities required to provide emergency communications (i.e. electronic communications networks and services) ARE considered as critical infrastructure/essential services in EU legislation. As these are specified in a Directive at EU level (with a supplementing Delegated Regulation defining the essential services) they must be transposed into national law at Member State level.
New Zealand	Emergency communications is NOT designated as critical infrastructure
United Kingdom	Public Safety communications are NOT designated as critical infrastructure (current Airwave TETRA nation mission critical network & future ESN (Emergency Services Network) 4G LTE based network)
USA	Emergency communications and 911 is designated as Critical Infrastructure in two of the 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States. Those two sectors are Emergency Services Sector (ESS) and the Communications Sector.
Latin America	In the examples of Ecuador and Costa Rica, Cyber Security and Critical Infrastructure are closely linked – with Public Safety one of the key pillars in Ecuador.

Other Considerations – Artificial Intelligence

Researching this paper has brought clarity that Critical Infrastructure, Cyber Security, and now, Artificial Intelligence must be considered as a "linked" set of initiatives.

For example, on 20 December 2023, the U.S.A. Federal Communications Commission announced it has chartered the ninth Communications Security, Reliability, and Interoperability Council (CSRIC IX) with a working group that will examine how Artificial Intelligence (AI) and Machine Learning can enhance the security, reliability, and integrity of communications networks in a non-discriminatory, transparent, and socially responsible manner. The CSRIC will be co-chaired by the Cybersecurity and Infrastructure Security Agency (CISA).

Country Findings

The remainder of this paper considers findings on a country-by-country basis, providing links to key source documentation where appropriate.

1. Australia

As part of Australia's Cyber Security Strategy 2020 [1], the Australian Government introduced critical infrastructure law reforms with the aim to further protect and improve the resilience of Australia's critical infrastructure.

Australia's Cyber Security Strategy 2020 is currently being reviewed to cover the period 2023-2030 [2] and may lead to a further review of the related legislation. Submissions to this review closed on 15 April 2023 and the University of Melbourne CDMPS made the attached Submission.

The Federal Government's Parliamentary Joint Committee on Intelligence and Security [3] is responsible for legislation relevant to critical infrastructure and national security. The key legislation is the Security of Critical Infrastructure (SOCI) 2018 [4] which includes the development of the category of "System of National Significance" [5] which may be declared by the Minister for Home Affairs

The SOCI Act legislation identifies the following 11 critical infrastructure sectors and asset classes within those sectors

- Communications
  - a critical telecommunications asset
  - a critical broadcasting asset
  - a critical domain name system
- Data storage or processing
- Defence industry
  - a critical defence industry asset
- Energy
  - a critical electricity asset
  - a critical gas asset
  - a critical energy market operator asset
  - a critical liquid fuel asset
- Financial services and markets
  - a critical banking asset
  - a critical superannuation asset
  - a critical insurance asset
  - a critical financial market infrastructure asset
- Food and grocery
  - a critical food and grocery asset
- Health care and medical
  - a critical hospital
- Higher education and research
  - a critical education asset

[1] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
[2] 2023-2030 Australian Cyber Security Strategy Discussion Paper (homeaffairs.gov.au)
[3] Parliamentary Joint Committee on Intelligence and Security – Parliament of Australia (aph.gov.au)
[4] Security of Critical Infrastructure Act 2018 (legislation.gov.au)
[5] Systems of National Significance and Enhanced Cyber Security Obligations Legislative Handbook (cisc.gov.au)

- Space technology
- Transport
  - a critical port
  - a critical freight infrastructure asset
  - a critical freight services asset
  - a critical public transport asset
  - a critical aviation asset
- Water and sewerage
  - a critical water asset

The SOCI legislation was amended in 2021 seeking to make risk management, preparedness, prevention and resilience, business as usual for the owners and operators of critical infrastructure assets and to improve information exchange between industry and government to build a more comprehensive understanding of threats.

In addition to the SOCI Legislation the Telecommunications and Other Legislation Amendment Act 2017 , known as the Telecommunications Sector Security Reforms (TSSR), created a regulatory framework to better manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities.

In Australia the key government agency(s) responsible for critical infrastructure, cyber security, and emergency management is the Department of Home Affairs [6], the Cyber and Infrastructure Security Centre (CISC) [7] and the National Emergency Management Agency [8] A key reference is the SAFECOM Strategic Plan 2023 [9]

In November 2023, to acknowledge the importance of critical infrastructure, it was announced by the CISC that the month of November would be Australia's annual "Critical Infrastructure Security" month[10]. And on 1 November 2023, the Department of Home Affairs released the Cyber and Infrastructure Security Centre's (CISC) first Critical Infrastructure Annual Risk Review [11]. The Review [12] provides a summary of the potential security risks that Australia's critical infrastructure providers may face. Further, on 13 November 2023, the Minister for Home Affairs announced that "telecommunications" will be recognised as "critical infrastructure" – the Minister saying, "these rules, frankly, should have been in place years ago".

In announcing this decision, the Minister also said that telecommunications companies will be brought under the Security of Critical Infrastructure Legislation (SOCI Act) that will allow telecommunications companies to be subject to new world's best practice standards that will require them to meet these standards.

Consultation on the further reform of the SOCI Act will commence at the end of January 2024.

---

[6] Department of Home Affairs
[7] Cyber and Infrastructure Security Centre (cisc.gov.au)
[8] Home | National Emergency Management Agency (nema.gov.au)
[9] SAFECOM Strategic Plan, March 2023 (cisa.gov)
Additional Resource: Submission to Australia's 2023-2030 Cyber Security Strategy - 15 April 2023 (FINAL).pdf

[10] https://www.cisc.gov.au/news-media/archive/article?itemId=1134
[11] https://www.cisc.gov.au/news-media/archive/article?itemId=1132
[12] Critical Infrastructure Annual Risk Review First Edition 2023 (cisc.gov.au)

2. Canada

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

The Government of Canada uses a risk-based approach for strengthening the resiliency of Canada's vital assets and systems such as our food supply, electricity grids, transportation, communications, and public safety systems.

- The *National Strategy* [13] establishes a collaborative, federal-provincial-territorial and private sector approach built around partnerships, risk management and information sharing and protection.
- The *Action Plan* [14] is the blueprint for how the Strategy will be implemented to enhance the resilience of Canada's CI.

The national strategy speaks to the safety of all Canadians but likewise makes no mention of emergency communications.

Given that disasters most often occur locally, the National Strategy recognizes that, in an emergency, the first response is almost always by the owners and operators, the municipality or at the provincial/territorial level. The federal government fulfils national leadership responsibilities relating to emergency management, respecting existing federal, provincial, and territorial jurisdiction and legislation. The federal government is also responsible for helping provinces/territories if the province/territory has requested the assistance. The National Strategy is based on the recognition that enhancing the resiliency of critical infrastructure can be achieved through the appropriate combination of security measures to address intentional and accidental incidents, business continuity practices to deal with disruptions and ensure the continuation of essential services, and emergency management planning to ensure adequate response procedures are in place to deal with unforeseen disruptions and natural disasters.

The Strategy recognizes that primary responsibility for strengthening the resiliency of critical infrastructure rests with the owners and operators. Federal, provincial, and territorial levels of government are also working to protect their own critical infrastructure and to support owners and operators in addressing this challenge.

Canada's list of 10 sectors:

- Energy and utilities
- Finance
- Food
- Transportation
- Government
- Information and communication technology

[13] *The National Strategy*
[14] *The Action Plan*

- Health
- Water
- Safety
- Manufacturing

3. European Union (EU)

In European Union Directive 2022/2557 on the resilience of critical entities, 'Critical Infrastructure' is defined as "*an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service*". In the same legislation, an essential service is "*a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment*"

The list of critical entities listed in the Annex to Directive 2022/2557 are listed below. In addition, Commission Delegated Regulation (EU) 2023/2450 supplementing Directive (EU) 2022/2557 elaborates further by defining a non-exhaustive list of essential services. Those essential services relevant to emergency communications are listed under the relevant critical entities (from Annex to Directive 2022/2557) below:

1. Energy
    - Electricity
    - District heating and cooling
    - Oil
    - Gas
    - Hydrogen
2. Transport
    - Air
    - Rail
    - Water
    - Road
    - Public Transport
3. Banking
4. Financial market infrastructure
5. Health
6. Drinking water
7. Waste water
8. Digital infrastructure

(non-exhaustive list of essential services from Delegated Regulation (EU) 2023/2450 under Digital Infrastructure)

- provision and operation of internet exchange point service (providers of Internet Exchange Points);

- provision of domain name system (DNS) service excluding services related to root name servers (DNS service providers);
- operation and administration of top-level domain (TLD) name registries (TLD name registries);
- provision of cloud computing services (providers of cloud computing services);
- provision of data centre service (providers of data centre services);
- provision of content delivery networks (providers of content delivery networks);
- provision of trust services (trust service providers);
- provision of publicly available electronic communications services (providers of electronic communications services);
- provision of public electronic communications networks (providers of public electronic communications networks);

9. Public administration
10. Space
11. Production, processing, and distribution of food

The critical entities falling under the scope of this legislation are subjected to cybersecurity risk-management measures and reporting obligations under the Directive 2022/2555 (NIS 2 Directive). The directive also applies to:

1. Postal and courier services
2. Waste management
3. Manufacture, production, and distribution of chemicals
4. Production, processing, and distribution of food
5. Manufacturing
   - Manufacture of medical devices and in vitro diagnostic medical devices
   - Manufacture of computer, electronic and optical products
   - Manufacture of electrical equipment
   - Manufacture of machinery and equipment n.e.c.
   - Manufacture of motor vehicles, trailers, and semi-trailers
   - Manufacture of other transport equipment
6. Digital providers
7. Research

Article 108 of the European Electronic Communications Code (Directive 2018/1972): “Member States shall take all necessary measures to ensure the fullest possible availability of voice communications services and internet access services provided over public electronic communications networks in the event of catastrophic network breakdown or in cases of force majeure. Member States shall ensure that providers of voice communications services take all necessary measures to ensure uninterrupted access to emergency services and uninterrupted transmission of public warnings."

Note: A "Directive" is a legislative act that sets out a goal that EU Member State must achieve. However, it is up to the individual Member State to devise its own laws on how to reach those goals. Directives are binding on Member States, but they are written in such a way as to leave some flexibility to the Member State to implement it in the manner best suited to its own national circumstances (i.e. transposition of the European Directive into nation law at Member State level).

Romania:

The 112 network in Romania has:

- Equipment uninterruptible power supplies;
- The electrical supply of PSAPs originates from 2 different power station of the national grid, acting as primary and secondary means of energy sources, and a power generator with minimum 24 hours of autonomy without refilling the tank as contingency;
- To ensure the business continuity of the 112 service, the following additional measures are applied in case of failures in different counties:
  - activation of backup routes to another county PSAP;
  - handling emergency calls by operators from another PSAP;
  - technical and operational activation of backup centres located in other locations than the affected PSAP;
  - automatic or manual (through specific reconfigurations) routing of emergency calls/communications to another PSAP;

In the public operator's infrastructure, the measures taken for power outage are specific to the operator's policy rather than mandated nationally, but the following general aspects are implemented:

- Communication sites are equipped with UPS/power stations/batteries which, depending on their importance in the architecture of their networks, provides hours of autonomy;
- Depending on the situation and priorities to make the intervention, field teams can install mobile power generators;
- Depending on the situation and specific needs, specific actions are taken to reduce the energy consumption, for instance:
  - Closing some services (i.e. shutting down some of the 2G equipment that are large power consumers);
  - Closing some sites whose services may be ensured by another sites (depending on the load and importance).

Germany:

In Germany PSAPs are classed as Critical Infrastructure. They are all prepared by backup energy systems. PSAPs in general will have a diesel generator and fuel supplies that enables operation for several days. More information is available on this link to the BBK (Federal Office for Civil Protection and Disaster Relief).

Netherlands:

Information about the Netherlands Critical Infrastructure from the Ministry of Justice and Security can be found on the factsheet here. "Communication with and between emergency

services through the 112-emergency number" is listed in the B-category of critical infrastructures in the Netherlands.

4. United Kingdom

The following information is taken from the UK Government's National Technical Authority for Physical and Personnel Protective Security website: https://www.npsa.gov.uk/critical-national-infrastructure-0

The UK Definition of Critical National Infrastructure is such that not everything within a national infrastructure sector is judged to be 'critical'. The UK government's official definition of CNI is:

"*Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*

a) Major detrimental impact on the availability, integrity, or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - considering significant economic or social impacts; and/or

b) Significant impact on national security, national defence, or the functioning of the state."

National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example).

In the UK, there are 13 national infrastructure sectors - each sector has one or more Lead Government Department(s) (LGD) responsible for the sector, and ensuring protective security is in place for critical assets. The sectors are:

- Chemicals
- Civil Nuclear
- Communications
- Defence
- Emergency Services
- Energy
- Finance
- Food
- Government
- Health
- Space
- Transport
- Water

Several sectors have defined 'sub-sectors'; Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard.

The UK Cabinet Office used to produce a Public Summary of Sector Security & Resilience Plans – the last one available openly being published in 2018. Two pages are of interest – page 14 which is about Emergency Services and page 12 which is about Communications.

5. United States of America

Cybersecurity & Infrastructure Security Agency (CISA) is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience – more information on their role in the Communications Sector can be found at: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector

The Communications Sector is closely linked to other sectors, including:

- The Energy Sector, which provides power to run cellular towers, central offices, and other critical communications facilities and relies on communications to aid in monitoring and controlling the delivery of electricity.
- The Information Technology Sector, which provides critical control systems and services, physical architecture, and Internet infrastructure, and relies on communications to deliver and distribute applications and services.
- The Financial Services Sector, which relies on communications for the transmission of transactions and operations of financial markets.
- The Emergency Services Sector, which depends on communications for directing resources, coordinating response, operating public alert and warning systems, and receiving emergency 9-1-1 calls.
- The Transportation Systems Sector, which provides the diesel fuel needed to power backup generators and relies on communications to monitor and control the flow of ground, sea, and air traffic.

The mission of the Emergency Services Sector (ESS) is to save lives, protect property and the environment, assist communities impacted by disasters, and aid recovery during emergencies – more information on the role of CISA in the Emergency Services Sector can be found at: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/emergency-services-sector

Five distinct disciplines compose the ESS, encompassing a wide range of emergency response functions and roles:

- Law Enforcement
- Fire and Rescue Services
- Emergency Medical Services
- Emergency Management
- Public Works

The ESS also provides specialized emergency services through individual personnel and teams. These specialized capabilities may be found in one or more various disciplines, depending on the jurisdiction:

- Tactical Teams (i.e., SWAT)
- Hazardous Devices Team/Public Safety Bomb Disposal

- Public Safety Dive Teams/Maritime Units
- Canine Units
- Aviation Units (i.e., police and medevac helicopters)
- Hazardous Materials (i.e., HAZMAT)
- Search and Rescue Teams
- Public Safety Answering Points (i.e., 9-1-1 call centres)
- Fusion Centres
- Private Security Guard Forces
- National Guard Civil Support

The US Emergency Services Sector (ESS) is a community of millions of trained personnel along with the physical and cyber resources that enable them to provide a wide range of prevention, preparedness, response, and recovery services during both steady-state and incident management operations. The ESS includes geographically distributed facilities and equipment and highly skilled personnel that provide services in both paid and volunteer capacities. The sector is organized primarily at the Federal, State, local, tribal, and territorial (SLTT) levels of government, such as city police departments, county sheriff's offices, Department of Defense police and fire departments, and town public works departments. The ESS also includes private sector resources such as industrial fire departments, private security organizations, and private emergency medical services (EMS) providers.

As the ESS focuses on protecting other sectors and the public, unique challenges arise in addressing the security and resilience of the ESS as critical infrastructure. The incapacitation of any of the assets, networks, or systems in this sector, whether physical or virtual, could cause significant harm or loss of life, public health issues, and/or long-term economic loss.

The ESS consists of systems and networks composed of physical, cyber, and human components.

6. Latin America

To give insight into Latin America, the examples of Ecuador and Costa Rica are used as typical approaches.

Ecuador:

Definition of Critical Infrastructure in Ecuador: According to Ecuador's National Cybersecurity Policy issued by Ecuador's Ministry of Telecommunications, to achieve a safe digital cyberspace that guarantees the rule of law, protects the State's critical services and infrastructures, and provides security to the population in cyberspace, the Government outlined a plan of action based on 7 pillars:

- Cybersecurity Governance
- Information Systems and Incident Management
- Protecting Digital Critical Services and Infrastructures
- Sovereignty and Defence
- Public Safety and Citizen Security
- Cyberspace Diplomacy and International Cooperation
- Cybersecurity Culture and Education

The actions in these pillars seek to prioritize institutional strengthening and effective coordination of multiple actors by the Government. Government and private entities must cooperate responsibly to achieve a safe digital cyberspace. The link between Cyber Security and Critical Infrastructure is defined by the National Cybersecurity Strategy, which needs to be sustained by each government and achieve results.

The Law on Public and State Security includes critical infrastructure protection with the national Critical Infrastructure strategy developed by the Ministry of Telecommunications.

The key agencies responsible for critical infrastructure, cybersecurity, and emergency response are the Ministry of Telecommunications, Ministry of Defence, and Integrated Security Service ECU 911.

There is also a Council of Public and State Security, composed of: President, Vice president, President of the National Assembly, President of the Supreme Court of Justice, Coordinating Minister for Security, Minister of National Defence, Minister of the Interior, Minister for Foreign Affairs, Chief of the Joint Command of the Armed Forces and Commander General of the National Police.

Costa Rica:

The United Nations Office for Disaster Risk Reduction identifies that Costa Rica's critical infrastructure includes sectors agreed upon with the National Commission of Risk Prevention and Emergency Response (CNE). These sectors are: (i) electricity, (ii) oil, (iii) roads and bridges, (iv) railways, (v) water and sanitation, (vi) health, (vii) education, and (viii) the postal service.

These sectors are seen as critical to the country's functioning and resilience, ranging from essential services such as health and education to key infrastructure such as energy, transport, and communications. The protection of these sectors is crucial to ensure the security, well-being, and sustainable development of Costa Rica.

Further information can be found in the Qualitive assessment of critical infrastructure in Costa Rica | UNDRR

The link between cybersecurity and critical infrastructure in Costa Rica has been significantly strengthened through the National Cybersecurity Strategy 2023-2027. This strategy recognizes the importance of protecting the digital systems and technological infrastructure that support essential services for the country. It focuses on strengthening cybersecurity governance and improving infrastructure protection and national cyber resilience. Protecting critical infrastructure is one of the main challenges identified, including cyber defence, and strengthening cybersecurity-related standards, organizations, and technologies.

This integrated approach indicates the interdependence between physical security and cybersecurity, highlighting how the protection of critical assets encompasses not only physical measures but also defence against digital threats. By protecting critical infrastructure from cyberattacks, Costa Rica seeks to ensure the continuity and reliability of essential services such as energy, water, health, and transportation, which are critical to national security and the well-being of its citizens. Whilst there is no specific law on critical infrastructure, a cybersecurity bill addressing critical infrastructure is currently underway.

In addition, the national strategic plan for 2050, although not focused exclusively on critical infrastructure, contemplates improvements in infrastructure for connectivity and the transition to a decarbonized, digital, and decentralized economy, which also contributes to national security in the long term.

This integrated approach indicates that Costa Rica recognizes the need for a holistic national security strategy that includes the protection and strengthening of critical infrastructure, considering both physical and digital threats, to ensure the continuity and efficiency of essential services and the overall security of the country.

In Costa Rica, the key government agencies responsible for critical infrastructure, cyber security, and emergency management are:

- National Emergency Commission (CNE)
- Cyber Incident Response Teams (CSIRT) of the Ministry of Science, Innovation, Technology and Telecommunications
- Ministry of Public Security
- Costa Rican Electricity Institute (ICE)
- Ministry of Health
- Costa Rican Social Security Fund (CCSS)