



The Future of the 111 Service and the Emergency Contact System in New Zealand

Providing the critical link between the public and first responders in emergency situations

17 November 2025



Purpose

This paper provides commentary and analysis on areas to improve the 111 Service (provided by Spark) and the broader Emergency Contact System which starts with a 111 call and ends with first responders arriving on scene (if that is the appropriate response).

This paper is a joint effort between New Zealand and Australian members of NECWG, considering the similar challenges facing both countries' emergency contact systems.

Author: National Emergency Communications Working Group Australia & New Zealand (NECWG – A/NZ)

With contribution from NZ Emergency Service Organisations (ESOs): NZ Police, Fire and Emergency New Zealand, Hato Hone St John, and Wellington Free Ambulance

Version: 1.0 (final)

Date: 17 November 2025

Foreword

Emergency communications ecosystems worldwide are under increasing pressure from:

- Rapid advances in technology—both in public safety and in tools available to the public for alerts and self-protection.
- A generational shift challenging practices and operational models that have remained largely unchanged since the 1960s.
- Growing expectations driven by social media, apps, and AI that monitor health and share real-time information.

Addressing these changes demands strong leadership and clear direction to meet current needs, adapt quickly, and prepare for the future.

This paper has been prepared by the National Emergency Communications Working Group – A/NZ (NECWG) to provide commentary and analysis on areas for improvement within New Zealand’s emergency communication and contact systems. Its purpose is to generate awareness of the challenges and risks, and to promote informed discussion.

The paper does not attempt to fully prescribe solutions—the emergency communications ecosystem is too complex for that without extensive stakeholder consultation. Instead, it identifies key focus areas and offers recommendations on outcomes that will help set a path forward.

On behalf of NECWG, I commend this White Paper for your review and consideration.



Craig Anderson

Executive Chair

National Emergency Communications Working Group – A/NZ

Date: 17 November 2025

Table of contents

Purpose	2
Foreword	3
Table of contents	4
Glossary	5
Acronyms	6
Executive Summary	7
Recommendations summary	8
1. Legislation and the Regulatory Framework Need Updating	11
Recommendations Summary	13
2. Dedicated Governance and Leadership of the Emergency Contact System is required	15
Recommendation Summary	18
3. NZ Needs a Contact Strategy for the Emergency Contact System	21
Recommendations Summary	26
4. Strategic Operating Model for the Emergency Contact System	28
Recommendations Summary	33
5. Responding to Innovations and Threats	35
Recommendations summary	38
Appendix One – Current Legislative Framework - 111 Service NZ	41
Appendix Two – Drivers of Demand for 111	43
Appendix Three – 111 Call Analysis 2023, 2024 & 2025	44

Glossary

Term	Definition
111 Service	The service delivered by Spark to answer 111 calls, through their ICAP, and redirect calls to the nominated ESO or by default to Police
Critical Emergency Contact Infrastructure	The Telecommunications and Radio network (including cell & radio sites) and electricity across New Zealand, the ICAP, and ESOs' systems for managing the response to 111 calls.
Contact Option/Channel	The method for contacting ESOs for assistance. For example, voice calls, messaging, digital reporting etc.
Emergency Contact System	The end-to-end emergency system from an original 111 call (currently answered by Spark), ESOs' management of 111 calls transferred to them, through to a first responder arriving on scene (if an emergency response is required).
Emergency Communications Eco System	The Emergency Contact System and all other providers of emergency and non-emergency public safety response and the technological and societal environment in which the ESO operate.
ESOs	Emergency Service Organisations (NZ Police (Police), Fire and Emergency New Zealand (FENZ), Hato Hone St John (HHSJ) and Wellington Free Ambulance (WFA).
ICAP	The Initial Call Answer Point which is operated by Spark as their obligation (under Kiwi Share) to answer 111 calls and direct them to the required ESO.
Kiwi Share	The Crown's share in Spark which is intended to preserve basic telecom services in the community including free local calling, internet access and 111 performance.
Omni-Channel	A capability which enables an individual who has contacted ESOs to be seamlessly transferred through another contact channel within the ESO, across ESOs, or to other agencies. (Note: this is not a capability currently available)
PSAP	Public Safety Answer Point (an operating model for answering of 111 calls for service).
Telecommunications Commissioner	. A role that sits within the Commerce Commission, established under the Telecommunications Act 2001.
TSO	Telecommunications Service Obligations – established under the Telecommunications Act 2001

Acronyms

Acronym	Definition
AI	Artificial Intelligence
CAD	Computer-Aided Dispatch
CRL	Crime Reporting Line
DDOS	Distributed Denial of Service
DLI	Device Location Information
ECD	Emergency Communications and Dispatch
ECLI	Emergency Caller Location Information
EENA	European Emergency Number Association
ESCI	Emergency Communications Service and Inter-operability
ESO	Emergency Service Organisation
FENZ	Fire and Emergency New Zealand
FRV	Fire Rescue Victoria
GDPR	General Data Protection Regulation
HHSJ	Hato Hone St John
ICAP	Initial Call Answering Platform
KSO	Kiwi Share Obligation
MBIE	Ministry of Business, Innovation, and Employment
NENA	National Emergency Number Association (USA)
NECWG – A/NZ	National Emergency Communications Working Group Australia and New Zealand
NEMA	National Emergency Management Agency
NGCC	Next Generation Critical Communications
NZ	New Zealand
PSAP	Public Safety Answer Point
PSN	Public Safety Network
SMS	Short Message Service
TCF	Telecommunications Forum
TSO	Telecommunications Service Obligation
VSP	Voice Service Provider
WFA	Wellington Free Ambulance

Executive Summary

The 111 Service and broader Emergency Contact System (ECS) are critical components of New Zealand's emergency response capability. The system is under increasing pressure due to rising demand, technological change, and evolving public expectations.

Current Challenges

- No Emergency Service Organisation (ESO), including Police, has a remit for changing or improving the 111 Service, despite being responsible for public safety.
- Rising Demand: Emergency Service Organisations (ESOs) have seen significant increases in call volumes, with Police experiencing a 42% rise over the past decade.
- Technological Advances: such as autonomous calling devices and digital communication are reshaping public engagement with emergency services.
- Outdated Operating Model: The 111 Service has seen minimal change since its inception in 1958 and lacks a unified future contact strategy or oversight.

ECS Systemic Limitations

- Operates within a **complex and fragmented legislative framework** with no future strategy.
- Lacks **central governance** and **performance accountability**.
- Struggles to adapt to **emerging technologies** and **public expectations**.

Collaborative Approach

These challenges are not unique to New Zealand. This paper, developed by NECWG A/NZ in collaboration with ESOs in New Zealand and Australia, outlines five priority recommendations to improve system resilience, coordination, and service delivery.

Call to Action

A coordinated national approach is essential. These recommendations require collective leadership and support from ESOs and Government, to ensure New Zealand's Emergency Contact System remains effective, resilient, and responsive now and into the future.

The proposed reforms are expected to deliver tangible public safety benefits, including:

- A first point of contact model that contributes directly to emergency responses
- Faster emergency response through improved coordination and triage
- Seamless multi-agency coordination during complex incidents
- Greater accessibility for vulnerable and non-verbal callers
- Resilience against outages and cyber threats
- Real-time visibility and accountability for service performance
- Enhanced public trust through transparent governance

Recommendations summary

To address these challenges and increase resilience of the emergency communications ecosystem we need:

1

Legislative Reform and Establishment of an Enabling Regulatory Framework

- Research options that address the complex legislative framework to provide consistent and contemporary guidelines and regulations to manage new sources of contact (e.g. autonomous devices), growing security threats, and to improve the 111 Service resilience in New Zealand. (Refer to chapter 1 for more details)

2

Establish Governance of the 111 Service

– Propose options for a government agency, with public safety responsibilities, to establish a governance body for the 111 Service. This is to ensure:

- clear responsibility, ownership and control over how the first point of contact is managed for 111 calls and the future Emergency Contact System (ECS)
- reporting of 111 Service performance against standards
- ESOs have network visibility and are made aware of network outages which may impact the 111 Service and/or the Emergency Contact System (111 call to first responder on scene)
- prompt visibility or alerting of any 111 Service outages to the ESOs, relevant agencies and Ministers, and options for alerting the public of alternative ways to contact the ESOs for an emergency response.

(Refer to chapter 2 for more details)

3

Develop a national future focused Emergency Contact Strategy for New Zealand to provide a roadmap for service and system interoperability

- Research opportunities to respond to evolving contact options and technologies, and public expectations about how they contact ESOs. Propose a future roadmap to ensure the emergency communications ecosystem is sustainable and continuously improves.

(Refer to chapter 3 for more details)

4

Streamline and update the 111 Service operating model

- Research operating models to improve, streamline and update the 111 Service (and broader ECS), to support more effective ways of enabling public contact and multi-agency responses to emergencies.

(Refer to chapter 4 for more details)

5

Respond to innovations and threats

- Develop proposals for a technology road map that plans for developments in communications technology to meet public expectations, whilst ensuring appropriate security controls are in place to safeguard information and access to the Emergency Contact System.

(Refer to chapter 5 for more details)

**Legislation and the
Regulatory
Framework Need
Updating**

1. Legislation and the Regulatory Framework Need Updating

Background: Current legislation and regulatory environment

New Zealand's 111 emergency call system is a vital public service. However, the laws and regulations that support it are outdated and no longer reflect the way people use the service today.

Currently, the framework governing 111 is a patchwork of legislation, telecommunications regulations, and voluntary agreements. The legislation that regulates the 111 system, the Telecommunications Act 2001 (the Act), was developed at a time when most 111 calls were made from landlines. Today, mobile phones account for more than 89% of 111 calls, and many households and businesses no longer have landlines. It is important to note the New Zealand Emergency Service Organisations (Police, FENZ, and Ambulance) have no ownership or control over how the first point of contact is managed in emergencies when they hold the responsibility to keep people safe.

While the Act allows for the creation of emergency calling regulations, these powers have not been used. As a result, there are no clearly defined, centralised obligations for how the 111 Service must operate, particularly in the event of a service outage.

This gap came to the fore during a 2023 incident where a fault in Spark's 111 service disrupted access to emergency assistance. ESOs were not formally alerted – they discovered the outage only by checking in with one another. Spark was not required to inform any ESOs, the National Emergency Management Agency (NEMA), the Department of Prime Minister and Cabinet, the Minister/s responsible for the Ministry of Business, Innovation, and Employment (MBIE) and other Telecommunications providers, or the public. This lack of mandatory notification presents a significant risk to public safety.

Without up-to-date legislation and regulation, there is limited ability for stakeholders to plan for or respond to telecommunications outages that may affect emergency communications. This is particularly concerning given evolving technologies, such as automated emergency calls from devices like alarms, mobile apps, or smart vehicles, and increasing public expectations for reliable access to help.

To ensure the 111 Service is robust, reliable, and fit for purpose, several updates are proposed:

1. A government agency, with responsibility for public safety, establishes a governance body for the 111 Service (see chapter 2 – Governance and Leadership of the Emergency Contact System for further detail).
2. Set and monitor service delivery performance standards for the 111 Service with regular reporting to the governance body (if established).



3. Require all electricity, telecommunications and radio network providers, to provide a system that shows network availability, and provides alerts as necessary to the 111 Service governance body (if it is established) and the Emergency Service Organisations.
4. Potentially, mandate that Spark (as the owner operator of the 111 Service) immediately alerts the 111 Service governance body and the Emergency Service Organisations of any service disruptions – whether planned or unplanned.
5. Require the Telecommunications and Radio Network providers, and electricity providers, to alert the ESOs, the public, relevant government and non-government agencies, Ministers of the Crown, and the 111 Governance Body (when it is established), of any planned or unplanned outages that will impact the Emergency Contact System. I.E, the public are unable to make a call to 111 and/or the ESOs cannot receive a 111 call. It is envisaged that the Governance Body's role would be to ensure these standards are being met and hold the Electricity, Telecommunications and Radio Network providers accountable. (The proposed 111 Service Governance Body and likely the Telecommunications Commissioner (Commerce Commission) would likely need powers established through regulations.)
6. Require the ESOs to provide visibility to the public, relevant government and non-government agencies, Ministers of the Crown, and any 111 Governance Body (if established), of any planned or unplanned outages of their systems which disrupts public access to the Emergency Contact System.
7. Seek to implement enforceable standards for entities that offer products with autonomous emergency calling/contact features (such as personal alarms, fall and crash detection, etc.) to use the 111 Service responsibly (e.g. put in triage centres to ensure automated calls to 111 are genuine emergencies) to avoid wasting taxpayer funded services resources and creating false demand that impacts others' access to an emergency response. (See chapter 2 – Governance and Leadership of the Emergency Contact System and chapter 5 – Responding to Innovations and Threats, for further details)

These changes will require further policy development and consultation with key stakeholders, including the Commerce Commission, Spark, ESOs and others.

At present, the New Zealand Telecommunications Forum (TCF) publishes voluntary codes of practice, such as its Emergency Voice Calling Code, which sets out minimum requirements for voice quality and connectivity. However, these codes are not binding and do not extend to emerging industries that also rely on the 111 Service.

New Zealand's emergency call system must evolve to meet modern demands. Updating the legislative and regulatory framework will help ensure the 111 Service remains reliable, responsive, and able to support both current and future technologies. A more structured and

proactive approach will also enhance coordination and accountability during service disruptions, ultimately improving public safety.

Refer to Appendix One for a high-level overview of the complex framework under which the 111 Service operates in New Zealand.

Recommendations Summary

1. Police to establish and lead a working group to develop options which:

1.1. Outlines potential legislative and regulatory changes:

- a. for addressing the visibility of planned and unplanned outages of the telecommunications network, and/or the electricity network, and/or Sparks 111 Service, and/or the ESOs Communications and Dispatch Centres where the impact on the public is that they are unable to access the Emergency Contact System to request help in emergencies.
- b. that identify the regulatory powers a 111 Service Governance body¹ would need, if established, to have oversight of compliance of standards set for the use, operation and delivery of the 111 Service
- c. that propose enforceable standards for all entities that offer products with autonomous emergency calling/contact features (such as personal alarms, fall and crash detection, etc.) ensuring they use the 111 Service responsibly. (More information on this available in chapter 5 – Responding to Innovations and Threats)

1.2. Police to establish and lead a ‘Future of the Emergency Contact System’ working group which will drive the research and develop options to address the vulnerabilities of the ECS, in collaboration with the other ESOs, MBIE and other relevant agencies.

¹ Refer to Chapter 2



Governance and Leadership of the Emergency Contact System



2. Dedicated Governance and Leadership of the Emergency Contact System is required

Background: Current leadership and governance arrangements

Building on the regulatory challenges outlined in Chapter 1, effective governance is essential to ensure accountability, coordination, and resilience across the Emergency Contact System. Chapter 2 explores the current leadership arrangements and proposes a new governance model to address these gaps.

It is important to note that currently, the ESOs have no ownership, governance, or control over how the first point of contact for a 111 call is managed in emergencies, when they hold the responsibility to keep people safe.

Multiple agencies currently manage and deliver different aspects of the 111 Emergency Contact System. Spark operates the 111 Service through its Initial Call Answering Platform (ICAP), under the authority of the Telecommunications Act 2001. Meanwhile, ESOs are responsible for managing the emergency response once a call is received.

While the New Zealand Telecommunications Forum (TCF) provides some coordination and guidance for the telecommunications industry, its influence is limited. Participation in the TCF is voluntary, and its scope does not extend to other industries that also rely on the 111 Service, such as providers of personal alarms or devices with automated emergency calling features (e.g. mobile phones and connected vehicles).

In late 2023, a new forum was established to address some of these challenges. The Emergency Communications Service and Inter-operability (ESCI) forum brings together representatives from the ESOs' Emergency Communications and Dispatch Centres, the NEMA, Next Generation Critical Communications (NGCC), and the MBIE. While this forum provides a valuable space to share insights and discuss issues facing the Emergency Contact System, it does not hold decision-making authority or legislative power to implement changes.

Key challenge 1: Inadequate governance & legislative support for the 111 Service

Currently, there is no formal government-led strategic body with overall responsibility for governance of the 111 Service. Nor are there enabling regulations that define how the service should be managed or used. In the absence of a clear governance body, there is uncertainty about the future direction and development of this critical service.



Establishing a dedicated governance body and enabling regulations would directly contribute to improved public safety by:

Providing clarity about ownership and accountability for service delivery

- National performance standards and service level agreements are met for the 111 Service, including the availability of alternative communications channels during network outages or service disruptions.

Timely alerts and coordinated responses during outages

- Clear and timely communication is provided to the Government, ESOs² and the public on any significant planned or unplanned outages of the 111 Service as well as any broader telecommunications network issues, i.e. those that may impact the delivery of the 111 Service to the public or adversely affect the operation of the ESOs Emergency Communications and Dispatch Centres.

Set standards that support use of the 111 Service and enhance interoperability and situational awareness

- Transparent and enforceable conditions are in place to guide the use of the 111 Service by commercial and non-commercial entities delivering services to the public.
- Greater interoperability between ESOs and, potentially other emergency management agencies, to facilitate improved collaboration, coordination, and information sharing across responders. A governance body for the 111 Service could potentially set standards to support interoperability such as i3³ for ease of system integration across any future ECS.

Faster and more reliable emergency response across agencies

- A mechanism is created for individual agencies to gain support for initiatives that strengthen the continuity and resilience of ECS.
- Flexibility is built into national communications service contracts, or through legislative/ regulatory requirements, to ensure the 111 Service maintains continuity of service during periods of rapid change or increased demand.

Independent leadership models and governance structures in the North American National Emergency Number Association (NENA) and the European Emergency Number Association (EENA) has demonstrated success driving change within emergency sectors.

² ESOs should ideally have visibility of the ECS network rather than receiving large volumes of notifications of minor and short-lived outages across the entire telecommunications and power networks which will be difficult to sift through to identify those outages which impact the ability of the public to call 111 and/or ESOs to receive 111 calls.

³ i3 is a standard used across North America and Europe for technology which enables ease of systems integration and interoperability across providers (ESOs, Telecommunications Companies etc) who operate within the ECS.



In addition to the above, a governance body would directly contribute to improved public safety by ensuring:

Key challenge 2: Non-enforceable Network Standards

The network performance standards set by TCF are not enforceable. This means telecommunications providers may make network changes without considering the impact on the Emergency Contact System or providing visibility/alerting the ESOs.

For example, earlier this year, telecommunications provider 2 Degrees made changes to their radio network without alerting ESOs.

This caused a 20-minute radio network outage in the Police, and Fire and Emergency New Zealand (FENZ) Emergency Communications and Dispatch Centres.

As a result, Police and FENZ dispatchers were unable to use the radio voice console to talk to first responders. Instead, they were forced to use a much slower and less flexible dispatch process that should only have been necessary as a system of last resort.

Whilst the outage had a clear negative impact on this critical public service for a 20-minute period, there were no repercussions for 2 Degrees as they had not breached any regulations or obligations.

If the ESOs had visibility or been alerted of this planned outage in advance, they could have worked to minimise the negative impacts to service delivery and emergency response times.

Note: This would not be solved by the Public Safety Network (PSN) being delivered by the NGCC. The PSN relies heavily on the NZ Telecommunications infrastructure.

Without regulations that mandate formal engagement between telecommunications providers and ESOs for planned outages or network changes, emergency services are limited in their ability to plan ahead. This introduces unnecessary risks to the Emergency Contact System and undermines the ability of ESOs to protect the public and support first responders.

Even in cases where telecommunications providers do consult with ESOs for planning outages and upgrades, there is no requirement to adjust the timing of outages based on ESO needs or feedback. As a result, ESOs must attempt to negotiate the best possible outcome, often relying on forecasted low-demand periods to minimise potential impacts. This reactive approach places undue strain on the system and limits the ability to manage risk proactively.

Recommendation Summary

2. Development of Governance Options for the 111 Service - Emergency Service Organisations (ESOs), MBIE, and other relevant agencies should develop a comprehensive set of options that assess opportunities, benefits, and risks related to the establishment of a governance framework for the 111 Service in New Zealand. The options should include clarity about the:

2.1 Role, Functions and Establishment – of a governance body, with appropriate powers and responsibility for public safety, to have oversight of the 111 Service. The options must clearly set out a defined role and functions for a proposed governance body, and guidance of how such a governance body could be established

2.2: Key Design Principles – the governance framework options should consider:

- a. **Structure** - the governance body's structure must enable informed decision-making based on:
 - i. Practical operational knowledge and experience
 - ii. Understanding of system challenges
 - iii. Awareness of real-world implications of regulations and service standards
- b. **Representation** – membership could include:
 - i. Each Emergency Service Organisations (Police, FENZ, HHSJ and WFA), with an ESO as the chair of the governance body
 - ii. Ministry of Business, Innovation and Employment
 - iii. Spark (as the current 111 Service provider)
 - iv. Other telecommunications providers
 - v. The Telecommunications Commissioner (Commerce Commission)
 - vi. A representative from the Electricity Authority
- c. **Functions and Powers**- the governance body should have the authority to:
 - i. Oversee the Emergency Contact System
 - ii. Ensure a controlled and coordinated approach to planned outages affecting the 111 Service and ESOs emergency responses
- d. **Enforceable Standards** – define the governance body's authority to set enforceable standards, potentially through regulation, to ensure:



- i. Accountability and proper use of 111 by commercial entities leveraging publicly funded ESOs for their services
- ii. Compliance with service delivery performance standards, including reporting requirements
- iii. A coordinated approach to planned outages across the telecommunications, electricity and ESO systems

The background of the slide features a complex network diagram. It consists of numerous nodes, represented by small circles, connected by thin, light blue lines. The nodes are distributed across the slide, with a higher concentration in the upper right and lower left areas. Some nodes are colored red, while others are purple. The overall structure suggests a web of connections or a system of interrelated components.

Contact Strategy for the Emergency Contact System

3. NZ Needs a Contact Strategy for the Emergency Contact System

Background: The need for an Emergency Contact Strategy

With governance structures under consideration, the next critical step is to define how the public interacts with emergency services. Chapter 3 introduces a forward-looking contact strategy to ensure accessibility, clarity, and responsiveness in line with evolving public expectations and technology.

Emergency communications services are critical for everyone in New Zealand. They provide real-time access to emergency assistance during incidents and disasters, enabling the right response at the right time. These services help reduce harm, prevent further damage, and can mean the difference between life and death.

To ensure these services continue to meet the needs of the public, a National Strategy for the Emergency Contact System is required. This strategy should optimise communications channels, align with modern expectations, and ensure the public clearly understands how to access emergency help.

As technology evolves, emergency events become more complex, and public expectations shift – particularly with the rise of digital communications. There is an increasing need for a unified forward-looking strategy. Currently, confusion about the role of 111 leads to significant call volumes that do not require emergency assistance. This has been partially addressed through the introduction of alternative services such as the Police non-emergency number 105, and the free mental health support line, 1737 (available 24/7).

Any efforts to streamline emergency contact options must avoid a fragmented or confusing approach. Whilst acknowledging the operational independence of the ESOs and Spark as the 111 Service provider, a nationally consistent contact strategy is essential to provide clarity and confidence to the public – particularly as we prepare for generational changes in workforce skills, expectations, technology and communications preferences.

The contact strategy will need to guide future investments and planning, and support the implementation of new technologies and communications channels, while accommodating the unique needs and structures of each ESO. Without a shared strategy, emergency communications risk falling out of step with public expectations and may fail to fully support community needs.

The community's expectations of how they contact and interact with ESOs is shifting, in line with a digital-first mentality. Today, access to emergency communications services in New Zealand is predominantly via voice channels (i.e. landline, mobile or satellite phones). While alternative contact channels exist, they are limited and often outdated.

For example, the 111 Text Service developed by NZ Police in 2012 enables registered users who are hearing or speech-impaired, to request help via SMS text messaging). Police operate this service on behalf of all the ESOs. However, it is not part of the official Spark-operated 111 platform (due to its absence from scope when the telecommunications provider was privatised); it relies on outdated technology; and it suffers from frequent outages and usability issues.

Whilst the NZ Police plan to make improvements, the limitations of the current 111 Text Service highlight an opportunity to integrate more modern and reliable digital contact options under a refreshed 111 Service framework.

There is a reasonable expectation that people who cannot make a voice call to 111, due to physical or situational limitations, would anticipate a contemporary range of emergency contact options to be available.

The development of a forward-looking Emergency Contact Strategy must begin now. It is vital to ensure the 111 Service, and any future ECD, is capable of meeting the evolving needs and expectations of all New Zealanders across generations and communications preferences.

A forward-looking contact strategy will help ensure:

- Direct access to emergency services for all community members
- Alternative communication methods for those unable to speak
- Improved responsiveness through familiar digital platforms
- Reduced harm and faster triage during emergencies

Globally there are examples of enabling standards to learn from such as the NENA i3⁴ standards that can facilitate these inputs. These include standards across an IP based network, supporting multimedia across voice, messaging, photos or video, smart routing using GPS, interoperability as well as cyber security measures.

Omni-Channel Capability is becoming the norm in other industries and there is a public expectation that the Emergency Service Organisations will have this capability too.

Other industries across telecommunications, transport, healthcare, social services, or banking, are moving towards more omni-channel servicing approaches, setting expectations for being able to engage across multiple channels. Omni-channel capability would enable someone who has been answered through one mechanism of contact to be seamlessly moved through one or more other channels of communication depending on the situation and their needs. For example, if a member of the public chooses to make an online non-emergency report for an emergency event that is happening now, (e.g. where they or others

⁴ https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-010.3b-2021_i3_stan.pdf



are in danger), with the use of modern intelligent technology, their request for help could be pushed into the Emergency Communications and Dispatch mechanism of the appropriate ESO/s and first responders dispatched as required. Conversely, those members of the public who call 111 for a non-emergency event could be seamlessly moved to another more appropriate channel to avoid entry to the ESOs Emergency Communications and Dispatch mechanism. The ability to develop omni-channel capability is dependent on investment in ESOs and the Emergency Contact System and ability to connect the public across the wider Government and Non-Government network. True Omni-channel capability is a long-term goal. (Omni-Channel is different from introducing new contact options (channels)).

Entities are designing contact channels that are intended to be received directly by ESOs, but ESOs are not able to receive the contact. It is important entities are required to engage with the ESOs constructively before offering new contact/channel options to their customers for making requests for an emergency response from the ESOs. This includes offering applications and devices which autonomously call/contact 111 if an alarm is activated such as fall and crash detection, and the ability for the public to use methods such as messaging 111 with an expectation the ESOs will receive the message and respond.

For example, when Telco advertised their new cell phone satellite service, shortly after Cyclone Gabrielle, announcing people would be able to use satellite coverage to text 111 when the usual cell phone coverage was not available.

At no stage had that Telco engaged with the ESOs or Spark 111 to determine if Spark (as the 111 Service provider) had the capability to receive satellite text messages.

Challenges to navigate with new channels and technologies

Despite the accessibility benefits that new channels and technologies bring, there are several challenges with implementation including incident validation, service availability consistency, potential delays to dispatch, demand fluctuations and demand capacity. These challenges need to be considered in any decision to bring on new contact channels.

Key Challenge 1: Validating incident location and context

ESO/s require three critical pieces of information to respond effectively to an emergency:

- The **location** of the incident
- The **nature** of the emergency
- Any **immediate safety threats** (such as the presence of safety hazards)

Gathering this information can be significantly more difficult when using non-voice communication channels, such as text messaging. These limitations may affect the



accuracy or timeliness of the response and could pose risks to both public and first responder safety.

The location of an incident, from either a landline or mobile call, is easily identifiable from owner records and/or using the Emergency Caller Location Information (ECLI) function that is available off every modern Smartphone. This provides, to a high level of accuracy, the location of the caller, allowing ESOs to immediately identify any other conditions known about the location. Location is currently not natively available through non-voice contacts and requires the person to validate this manually. Without a valid or validated location, emergency services cannot be effectively directed to the incident. It is important to note that the system recognises the location of the Smartphone, which may or may not be the location of the incident as the caller could be removed from the scene or calling on behalf of someone else, therefore needs a level of validation for responders.

Understanding the nature of the incident is critical so emergency services can prioritise or dispatch the correct resources to address the incident. Currently voice calls are the preferred form of communication for 111 calls to Police. It allows staff to hear the tone of voice and relevant background noise when determining the level of risk and the appropriate response. Police are keen to trial video links. The trial would be limited to emergency events where visuals would provide improved situational awareness and there are no increased safety concerns for the caller in using video. Guardrails would be put in place with any video trial to ensure there is no breach of legislation (e.g., the Search and Surveillance Act and Privacy Act), and other concerns such as evidential requirements have been considered. Ambulance and Fire ESOs may also use live video calls to assess risk, injuries and events, and to better determine the appropriate response.

Key Challenge 2: Disparate implementation creating unrealistic expectations of service capability

There is an expectation that 111 Service capabilities will be consistently available to the community, wherever they are and no matter which ESO they are engaging with. This can present a challenge when seeking to implement new contact channels, as pilot programmes are often developed in individual ESOs before being rolled out more broadly if appropriate. The roll out approach of any new channels would need to be carefully considered to avoid confusion in the community and reduce the potential for service failure.

Key Challenge 3: Demand fluctuations driven by alternative channels

A deep understanding is required of the implications for ESOs should new contact channels be engaged to receive information and requests for services. This includes the richness (or not) of the information the channels provide, and the resourcing required to manage them.



For example, when New Zealand Police launched the non-emergency 105 calling number, it was anticipated that a significant portion of non-urgent calls to the 111 service would be redirected to the new channel. While this shift occurred to some extent, demand for the new 105 service quickly exceeded expectations. Within the first 12 months of operation, the volume of non-emergency calls reached the resourcing limits of the 105 non-emergency team.

By making it easier for the public to contact Police for non-emergency matters, the 105 service inadvertently increased the demand on Police resources. This outcome highlighted the need for careful resource planning when introducing new communication channels.

Prior to the launch of 105, the Crime Reporting Line served a similar function with call volumes peaking at 1,585,210 in FY 2019/20, coinciding with the COVID pandemic. In the first three years of the 105 service, annual call volumes remained high, fluctuating between 1.273 and 1.284 million calls.

Emerging channels, such as live streaming and image, could be made only accessible through a link that is text to a member of the public reporting an emergency incident - where it is considered safe to enable a live stream. The member of the public would need to accept the link before the ESO could see what is happening through the camera on the caller's mobile device. Live streaming may be best provided to a two up emergency unit travelling to an incident, with the passenger viewing the footage for situational awareness.

There are challenges with the use of contact options such as live streaming due to implications for the Search and Surveillance Act 2012, recording requirements for evidentiary purposes, resource requirements and responsibilities to view material, and the risks of putting the public in harm's way 'to get a better angle'. However, as noted above Police Emergency Communications and Dispatch are considering undertaking a trial of this technology, with appropriate guardrails, to assess the place of video calls for emergencies.

Key Challenge 4: Limitations of existing foundational technologies

To introduce new contact options and enable omnichannel communication capabilities, investment in core systems is essential. These upgrades will allow the Emergency Contact System to leverage current and emerging technologies such as machine learning and intelligent systems to better manage demand and prioritise urgent public needs.

The 111 Service and ESOs need a clear roadmap, grounded in a national emergency contact strategy. This strategy must support the development of capabilities that ensure value for communities while maintaining fiscal responsibility and long-term sustainability.

While the introduction of new contact channels presents opportunities to improve public access and responsiveness, it also introduces complexity. A forward-looking, coordinated strategy is needed to guide development and investment.

Benefits of expanding contact channels to emergency services include:

1. Direct access to emergency services for all community members, eliminating reliance on third party intermediaries that may delay analysis and response.
2. Alternative communication methods for individuals who cannot safely speak or be heard during emergencies.
3. Opportunities to diversify the emergency communications workforce.
4. Increased accessibility via familiar, everyday communications platforms.

Recommendations Summary

3. Police to lead, in consultation with the ESOs, MBIE, and other relevant agencies, the development of full options for:

3.1. A national Emergency Contact Strategy - for the Emergency Contact System, which is forward looking and considers both current and future developments in communications technology and public expectations. The strategy would ideally be ratified by the proposed 111 Service Governance yet to be established, and should include:

- a. research into community needs and contact preferences for various emergency scenarios.
- b. demand forecasting for emerging communication channels over time
- c. a plan to establish a true omnichannel capability enabling seamless movement between communications channels as needed.
- d. exploration of workforce and operating models, technology infrastructure and data requirements
- e. a roadmap with detailed investment requirements
- f. identification of priority development areas



Strategic Operating Model for the Emergency Contact System

4. Strategic Operating Model for the Emergency Contact System

Background: Current operating context

To support the contact strategy and governance reforms, a modernised operating model is required. Chapter 4 outlines the limitations of the current system and presents opportunities to streamline operations, improve interoperability, and enhance service delivery.

Emergency incidents often require coordination between multiple agencies, placing significant pressure on the existing 111 system. ESOs' ability to coordinate effectively is currently hindered by outdated systems, limiting real-time information sharing and collaborative response efforts.

Despite increasing demand and more complex emergencies, the 111 Service still operates under a model established in 1958. This linear, voice-only model routes calls based on the caller's request or defaults to Police if the caller is uncertain. With minimal investment, this model has not evolved to meet modern expectations or emergencies.

Limitations of the current model:

- Limited system integration and information sharing reduce the ability to coordinate during complex or multi-agency events.
- Demand and demographic changes, including a growing and aging population and more frequent emergencies, increase strain.
- Technology gaps hinder service efficiency and resilience.
- Reliance on workarounds to deliver accessible 111 services. For example, the use of NZ Relay (a translation service for people with communications difficulties, including having limited English) to provide accessible 111 services to hearing and speech-impaired communities. NZ Relay lacks emergency risk assessment capabilities which can result in adverse impacts for the service-user.
- Vulnerability during crises such as pandemics, cyber-attacks, natural disasters, and other large-scale emergency events.

One common factor exists across all these issues; they will not be resolved in isolation. A modernised, collaborative, and resilient emergency communication system is essential for maintaining public safety.

A modernised operating model will:

- Enable real-time information sharing and coordinated dispatch

- Reduce duplication and improve speed of response
- Support AI-driven triage and multilingual accessibility
- Strengthen public and first responder safety during complex events

Key challenge 1: Lack of systems integration, information sharing and interoperability

There is no consistent integration or interoperability between systems used by ESOs, limiting coordinated responses.

ESOs currently operate separate systems for gathering, prioritising, and sharing emergency information. This creates barriers to effective coordination and situational awareness.

Integration across public safety platforms is essential to provide unified, timely responses.

In New Zealand, the “Report of the Government Inquiry into the Response to the North Island Severe Weather Events” in January and February 2023 identified “A nationally consistent common operating platform is required that is mandated through legislation, funded, and used by all councils and government agencies. It is important that information is consolidated at local, regional, and national levels and shared in real-time between councils, emergency agencies, and NEMA. Relevant tasking from the 111 system also needs to be integrated. (Paragraph 70, page 19)”

Under the heading “Review the 111 system to ensure it is effective in an emergency”, the Report of the Government Inquiry into the Response to the North Island Severe Weather Events also notes the issues with the 111 Service were: *“Further exacerbated as each emergency provider has their own system with no way of integrating or reconciling tasking between them. Police have advised they use a Computer-Aided Dispatch (CAD) system where all requests for help and events from the 111 service can be recorded and prioritised. Similarly, each emergency service provider has their own events recorded in their own systems.”* (paragraph 211)

The report goes on to say; “The Inquiry’s observation is that the emergency 111 system is complex and confusing. It is difficult to ascertain where responsibility for ‘ownership’ of the system sits. The problem is not in the disaggregation of 111 calls to Police, FENZ, Wellington Free Ambulance, and Hato Hone St John, but rather the lack of interoperability between these systems in a major or severe event. Situational awareness and the ability to respond was compromised leaving many people and communities fearing for their safety and that of their families.” (paragraph 213)

The inquiry closes with a recommendation that “Government commission a comprehensive review of the 111 system to ensure an effective, transparent, and interoperable service that can effectively draw on the resources of all emergency services, even in times of high demand. Any improved 111 system should be able to interface with the common operating



platform for emergency management that the Inquiry is recommending. This will ensure the best situational awareness possible in emergency events.”

This Government Inquiry into the North Island Severe Weather Events (2023) underscored the need for:

- A common operating platform for emergency coordination.
- Integration between the 111 Service and local, regional, and national systems.
- Transparent and unified system ownership to avoid confusion during major emergencies.

“We need to work smarter not harder. Interoperability is also critical to meet public expectations.” Comment NECWG Industry Engagement Forum – May 2025

Key challenge 2: Lack of modern technology to support service delivery

The current Emergency Contact System in New Zealand operates on a **linear call transfer model**, where calls are queued and answered strictly in the order they arrive. While simple, this “first in, first served” approach is highly limiting during high-demand situations. For example, when a major incident occurs, dozens of people—or even automated alerts from devices like Apple or Google—can simultaneously dial 111 for the same event. This surge creates a temporary **denial of service**, preventing other callers with unrelated emergencies from getting through. The system lacks the ability to differentiate between duplicate reports and genuinely new, critical incidents.

There is a significant opportunity to modernise this process by introducing **dynamic call handling powered by AI and machine learning**. Instead of treating all calls equally, intelligent prioritisation could identify critical emergencies, consolidate duplicate reports, and route calls based on urgency and resource availability. Such a system would ensure that life-threatening situations are addressed immediately, while still capturing valuable information from secondary callers without overwhelming Emergency Service Organisations (ESOs). Moving away from a rigid linear model toward a **smart, adaptive contact system** is essential for resilience in an era where technology-driven alerts and mass reporting are increasingly common.

Artificial Intelligence (AI) Opportunities

Opportunities exist to improve public and first responder service using AI and other smart technology in ESOs’ Emergency Communications and Dispatch (ECD) Centres.

AI and smart technology could help human agents (Communicators, Dispatchers, Shift Commanders etc.) to perform their roles more effectively and efficiently, improving service delivery.

Leveraging AI capabilities, the Emergency Contact System could offer multi-lingual services enabled by real-time translation, increased risk identification through AI call listening and word prompts and assisted offence coding and note taking. This would free up agent time to focus on call taking and more.

These capabilities are based on the premise that the core systems in the 111 service and ESOs ECD Centres are modern products capable of AI and smart technology integration.

Limited investments in these technologies are a barrier to improved operations, connectivity, and operating models.

Key challenge 3: Lack of Integration in Community Awareness

Currently, New Zealanders need to recall a variety of help line numbers depending on the nature of their situation. However, individual perceptions of what constitutes an emergency vary. For example, during a storm, one neighbour might view a fallen tree as a serious emergency, while another may see it as a minor issue. This subjectivity often leads individuals to call 111 – the most widely known and simplest number – even when their situation might be better handled by a non-emergency service. When their issue is redirected, it can feel like their emergency is being dismissed.

The linear operating model of the Emergency Call System often requires people to disconnect from one service and contact another, adding to the caller's frustration and confusion. A 'no wrong door' approach, enabled by omnichannel technology, would allow the public to be redirected seamlessly to the right service – emergency or non-emergency – without needing to disconnect and call again. However, consideration must be given to avoiding becoming a contact service for all government agencies.

This will require strategic planning and investment, which could be led by the 111 Service Governance body (per recommendation 2.1 in chapter 2 – Governance and Leadership of the Emergency Contact System) and the development of a full contact strategy for the Emergency Contact System (per recommendations 3.1 in chapter 3 – Contact Strategy for the Emergency Contact System).

Key challenge 4: Aligning ways of working across agencies

Police, Fire and Emergency NZ, and the NZ Ambulance Service operate in different ways based on their experience in managing different situations. Supporting more integrated ways of working would likely require a level of cross-skilling and alignment in emergency response procedures.

In considering a common operating model, it is important to note the independence of each of the Emergency Service Organisations (ESOs) and to ensure their ability to manage their own business is maintained or enhanced. We acknowledge that each constituent ESO is part



of a collective system and service, and that each needs to accommodate their wider organisation's national objectives and outcomes within their own strategic and operational management frameworks.

Any operating model change would need to ensure any nuances are maintained and managed appropriately in any continuity or contingency planning and execution. Increasing collaboration should strengthen the emergency services response overall without hampering individual parts.

A shared operating model would reduce duplication and hand-offs, improving speed, efficiency, and coordination. Greater alignment would also benefit coordination with local councils, utility providers, and national agencies during major events.

One potential Public Safety Answer Point (PSAP) model - would be to have a trained public agency team that collects and forwards information to relevant ESOs that:

- Minimise the need to ask callers to repeat information.
- Simultaneously alerts all relevant ESOs during multi-agency incidents

This would:

- Enhance response times and coordination.

This PSAP model would need to be staffed by fully trained ESO ECD staff to ensure appropriate expertise. As noted above/below the work on a potential PSAP is in its infancy.

In taking this forward there will need to be an exploration of how capability is transformed over time with sustainable funding models.

Recommendations Summary

4. Police to lead development of new 'Operating Model Options'

4.1 To streamline and improve the 111 Service, in consultation with the other ESOs and Spark, with the aim to:

- a. **Improve Service Delivery and Safety** – the proposed new operating models should ensure there is a significant improvement for public and first responder safety.
- b. **Improve Information Sharing** - improvements to interoperability and systems integration will enable appropriate information sharing for an emergency response which requires more than one ESO to attend.
- c. **Assess Inputs** – such as the current workforce, funding, processes and technology implications to inform points 4.1 and 4.2.
- d. **Consultation with Stakeholders** – the options paper for a new Operating Model must be prepared in collaboration with the community and emergency service stakeholders, including the current provider of the 111 Service.

4.2 The proposed operating model improvements should be developed in the context of the varying governance and organisational models of New Zealand. Options for consideration may include:

- a. **Calls to the ESO for emergency or non-emergency events which require an ESO response** will be directed to the appropriate channel within the ESO for an emergency or non-emergency response.
- b. **Where the call is not for ESOs, callers will be advised to redirect their request to other services** such as mental health, tenancy support agencies, local councils etc.
- c. **Use of AI for triage**, translation and low-risk administrative tasks (e.g. patient transport booking, burn-off notifications)
- d. **Clear protocols for secure information** sharing supporting response determination, priority, and coordination.
- e. **Research into community preferences** for emergency contact methods.



Responding to Innovations and Threats

5. Responding to Innovations and Threats

Background: The rise in cyber threats and autonomous devices

As the Emergency Contact System evolves, it must also be safeguarded against emerging threats. Chapter 5 addresses the critical need for resilience, cybersecurity, and appropriate frameworks to protect the infrastructure and data that underpin emergency communications.

Emergency agencies and associated organisations have some provisions in place to safeguard data, technology, and infrastructure in response to rising threats and challenges. Examples of existing provisions include:

- Airgaps between critical systems and the internet.
- On-premises infrastructure with controlled access provisions.
- Dual communications and dual electricity feeds into critical communications facilities.
- Active monitoring for cyber-attack or infiltration attempts.
- Physical security (fencing, security access-controlled doors etc.) of remote or isolated communications equipment.
- Encryption of data transmitted over public domain communications networks.

While these protections are in place in some agencies, not all apply them consistently. Inconsistent security standards pose a risk.

Significant effort has been applied by various agencies, organisations, and governments to determine appropriate guidelines for the protection of critical environments. These include:

- Essential Eight Maturity Model (patching, multi-factor authentication, restricted access etc.)
- New Zealand Information Security Manual
- Compliance with the New Zealand Privacy Act 2020
- Cybersecurity Best Practices developed by the United States' Cybersecurity & Infrastructure Security Agency
- [General Data Protection Regulation \(GDPR\)](#) – alignment where possible with this European standard for privacy and security

These are in addition to individual agency and organisation policies that may be aligned to one or more of these items.



The expansion and increasing reliance and dependency on internet or online technology means we are vulnerable to threats of cyber-attacks, denial of service, data breaches, and network failures that could be initiated within New Zealand or from overseas.

For example, in Australia in 2022, Fire Rescue Victoria (FRV) experienced a significant cyber-attack on its information and computer technology systems, including emergency response dispatch systems.

This cyber-attack forced firefighters to rely on mobile phones, radios, and pagers to respond to emergencies. Additionally, the attack potentially resulted in sensitive information about current and former employees of FRV, board members, individual contractors, secondees and job applicants being accessed or stolen.

Inconsistent use of cybersecurity guidelines and safeguards leave organisations open to exploitation, the impacts of which may be felt well beyond the borders of the impacted entity.

In New Zealand, differing standards of security meant that when Police led the development of a Treasury business case on behalf of all the NZ ESOs, the document could not be shared between Police and the Ambulance providers due to differing security standards. (In this case an embedded security standard in the Treasury business case template prevented its transmission via email to the Ambulance Services Hato Hone St John (HHSJ) and Wellington Free Ambulance (WFA).

Moreover, infrastructure and facilities supporting emergency communications are not consistently treated as critical infrastructure across agencies.

End-to-end infrastructure and facilities supporting the Emergency Contact System should be classified as critical, with this status reflected in legislation and policy. The infrastructure includes electricity and telecommunications networks across New Zealand, the 111 Service, the ESOs core systems in their ECD Centres, and the ESOs ECD facilities. This classification would ensure the end-to-end infrastructure and facilities are given priority during and following major events which impact on the ability of the Emergency Contact System to continue to operate.

There is a need for consistent and contemporary guidelines and enabling regulations to respond to innovations and threats

There is little doubt that in New Zealand, there is an opportunity to improve emergency communications security and regulatory frameworks. This will ensure they are both contemporary and responsive to changing needs and circumstances.

The frameworks should accommodate current, new and developing technologies and include sufficient legislative or regulatory safeguards to address the risks associated with



third party devices, apps and systems seeking to connect directly to national emergency 111 communications services. The regulation should protect that service (and consequently the ESOs) from Distributed Denial of Service (DDOS) attacks.

An appropriate regulatory environment should, incorporate or control changed capability expectations and services (e.g. App development in emergency / health monitoring and alerting, and autonomous 111 calling/contact systems into the emergency communications ecosystem).

Ideally, these guidelines and policies will be, where appropriate, agreed internationally. Understanding the regulatory framework in place or under development in the European Union, Ireland and other Five Eyes nations, particularly for commercial entities use of the Emergency Contact System, will help to inform the development of regulations.

The Emergency Contact System depends on resilient infrastructure

Classifying ECS infrastructure as critical will:

- Ensure priority restoration during disasters
- Protect against cyber threats and DDOS attacks
- Maintain continuity of emergency services during outages
- Safeguard public access to help when it's needed most

Reviewing the resilience of the telecommunications and radio networks, and the electricity supply, that the public and ESOs rely on for the Emergency Contact System to operate is a vital piece of work. Questions may need to be raised about what redundancy is available when parts of the network fail.

For example, back up battery power for many cell towers may only allow for up to two hours of emergency power. Two hours seems insufficient when significant emergencies such as the Auckland floods and Cyclone Gabrielle, and other recent weather events, result in protracted power outages.

With 89% of all 111 calls made on mobile phones, there needs to be a significant improvement in the resilience and redundancy for the cellular (and radio) network.

The 111 Governance Body (when it is established) could lead the with work with key stakeholders to develop requirements and standards for the resilience and redundancy of the infrastructure that the Emergency Contact System is reliant on. The recommendations below directly address some of the concerns raised about the infrastructure and facilities that support the provision of the Emergency Contact System in New Zealand

In Easter 2025 Ex-Tropical Cyclone Tam hit Northland which resulted in several cell phone towers switching to the emergency battery power supply, but this ran out after just two hours.

With 89% of 111 calls made on cell phones and reducing landline telephone connections in homes this meant that whilst the 111 Service was operating many of the people in Northland could not make 111 calls or receive emergency alerting messages. When the ESOs engaged with the chair of the TCF post the event, it became apparent that at no stage had consideration been given to the fact that large numbers of people rely on the cell phones to call 111.

Recommendations summary

5. Police to lead and develop, together with the ESOs, options on how to improve response to innovations and threats, which addresses:

5.1 Optimising Operations - through contemporary, safe and secure systems that support ESOs ability to optimise their operations, to manage requests for service for emergency events, and support both first responders and public safety. Consideration should be given to:

- a. **Fiscally sustainable investment** - in modern systems is essential for the Emergency Communications and Dispatch Centres across all the New Zealand ESOs
- b. **Prioritisation of modernising ESOs ECD systems** – to enable optimisation each ESOs operating model and adoption of new technology innovations to meet the needs of the public.
- c. **Development of clear road maps for the core technology solutions in ESO's ECD systems (within fiscal constraints)**, ensuring they can adapt to future innovations, improve inter-operability with ESOs and strengthen data security in response to growing threats.
- d. **Cyber Security** – set out requirements for all ESOs and other providers within the Emergency Contact System (e.g. Telecommunications providers and electricity companies) to meet or exceed the minimum cybersecurity guideline and safeguards for their ECD systems to minimise the risk of loss of sensitive data and distributed denial of service attacks.

5.2. Classification of Infrastructure and Facilities as Critical – include in the options the need for the infrastructure and facilities that support the provision of Emergency Contact System and the system itself are classified, in appropriate legislation, as critical. The driver is to ensure legislation and

policy adequately recognises the Emergency Contact System (including the 111 Service, telecommunications networks, and ESO core ECD systems) as critical to public and first responder safety and are given priority during and following major events which may threaten delivery of the 111 Service and the ESOs Emergency Communications and Dispatch Centres.

5.3. Note the Civil Defence Emergency Management Act 2002 (the Act) is likely the most relevant legislation in which the Emergency Contact System (ECS) infrastructure and facilities should be classified as critical.

In 2025 the Emergency Management Bill is being progressed to make changes to the Act. The ESOs will provide agency feedback on the Bill and request the classification of the Emergency Contact System and supporting infrastructure as critical assets.

5.4. Note that ESO may require additional baseline funding to achieve 5.1, 5.2 and 5.3. Keeping up with changes in technology requires ongoing investment in modern systems may be beyond the ability of ESOs to meet from baseline funding. Where this is the case there will be a need for appropriate business casing through the Treasury for funding.

Modernising the full end-to-end Emergency Contact System is critical to support evolving needs and expectations of the public including evolving commercial products which rely on taxpayer funded ESOs for delivery. The appropriate regulatory environment which incorporates, or controls changed capability expectations and services is detailed in chapter 1 – Legislation and the Regulatory Framework Needs Updating.



Appendix



Appendix One – Current Legislative Framework - 111 Service NZ

The following is a very high-level overview of the complex framework under which the 111 Service operates in New Zealand.

Kiwi Share:

- In 1990 when Telecom was sold, the Crown retained ownership of 1 special share – called the ‘Kiwi Share’.
- The kiwi share is intended to preserve basic telecom services in the community – including free local calling, internet access and 111 performance.
- The kiwi share obligations (KSO) were described in clause 5 of the first schedule of Telecom’s constitution. KSO only related to emergency calls from fixed residential lines, but, that this is amended to cover all ‘voice services’ (see below).

In 2001 two things occurred:

- The Telecommunications Act 2001 took effect – creating ‘telecommunications service obligations’ (TSO), and Telecommunications Commissioner (within Commerce Commission)
- The Kiwi Share was updated by a new deed – the 2001 deed was stated to be a TSO and while in place the KSO (clause 5) did not operate.

In 2011 the ‘kiwi share’ deed was updated, to reflect the move away from copper and other changes in technology. A revised TSO deed was made. This carried over the same 111 obligations from the 2001 deed.

In 2018 the Telecommunications (New Regulatory Framework) Amendment Act 2018 – required Commerce Commission to create a 111 Contact Code, which is deemed to be a TSO – essentially, focused on vulnerable⁶ customers having access to 111 emergency service in case of electricity failure (based on move away from copper). The 111 Contact Code only relates to fixed landline connections. Currently 89% of all 111 calls are made from mobile devices which are not included in the 111 Contact Code.

In December 2024, there was an amendment to the TSO deed that includes the following extract:

- ii. ensure that its contract with any Supplier, in relation to the Alternative Residential Voice Service, requires the Supplier to:
 - a. provide Chorus with all information Chorus requires to meet its reporting obligations to the Crown under clause 6A.2(c) below;



- b. comply with the 111 Contact Code (being the code made by the Commerce Commission under section 238 of the Telecommunications Act 2001, or any equivalent replacement); and
- c. comply with parts G and H of the New Zealand Telecommunications Forum Incorporated TCF Emergency Code Call code (or any equivalent replacement), as if they were a Voice Service Provider (VSP) under that Code.

The significance of this is that it specifically brings the 111 contact code AND parts G and H of the 2022 TCF Emergency Calling Code (G. Availability and quality of emergency calls; and H. Caller Information) under the coverage of the 2011 Kiwi Share deed. Those parts are, therefore, considered to be part of a TSO and are themselves enforceable obligations under the Telecommunications Act.

In terms of the Telecommunications Act, TSO deeds are enforceable by the Commerce Commission. There is a list of enforcement cases relating to breaches by telco providers of the 111 Contact Code. The list of TSO deeds is contained on the Commerce Commission website⁷ – the Spark TSO (aka Telecom TSO) is included and is still in effect.

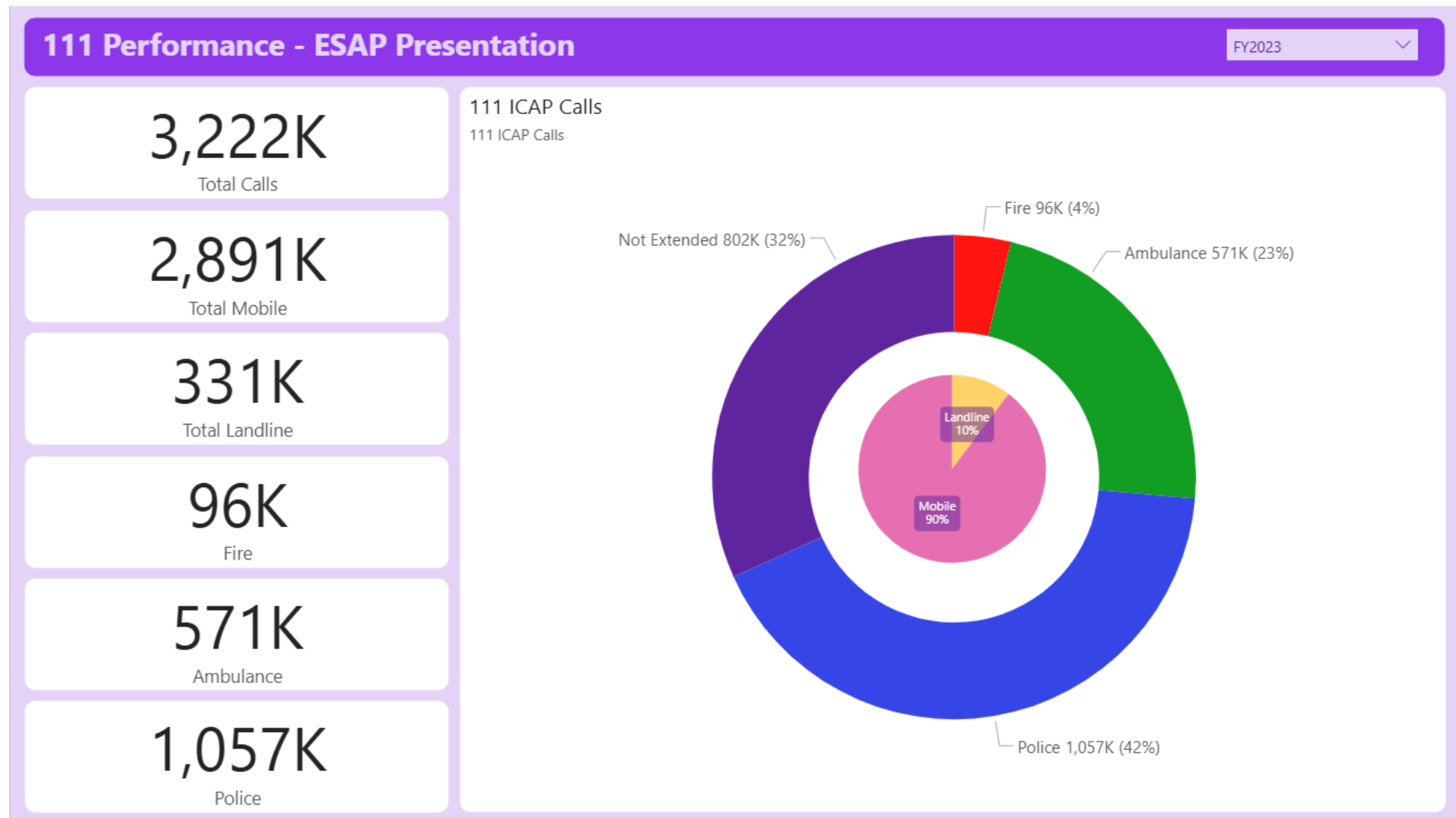


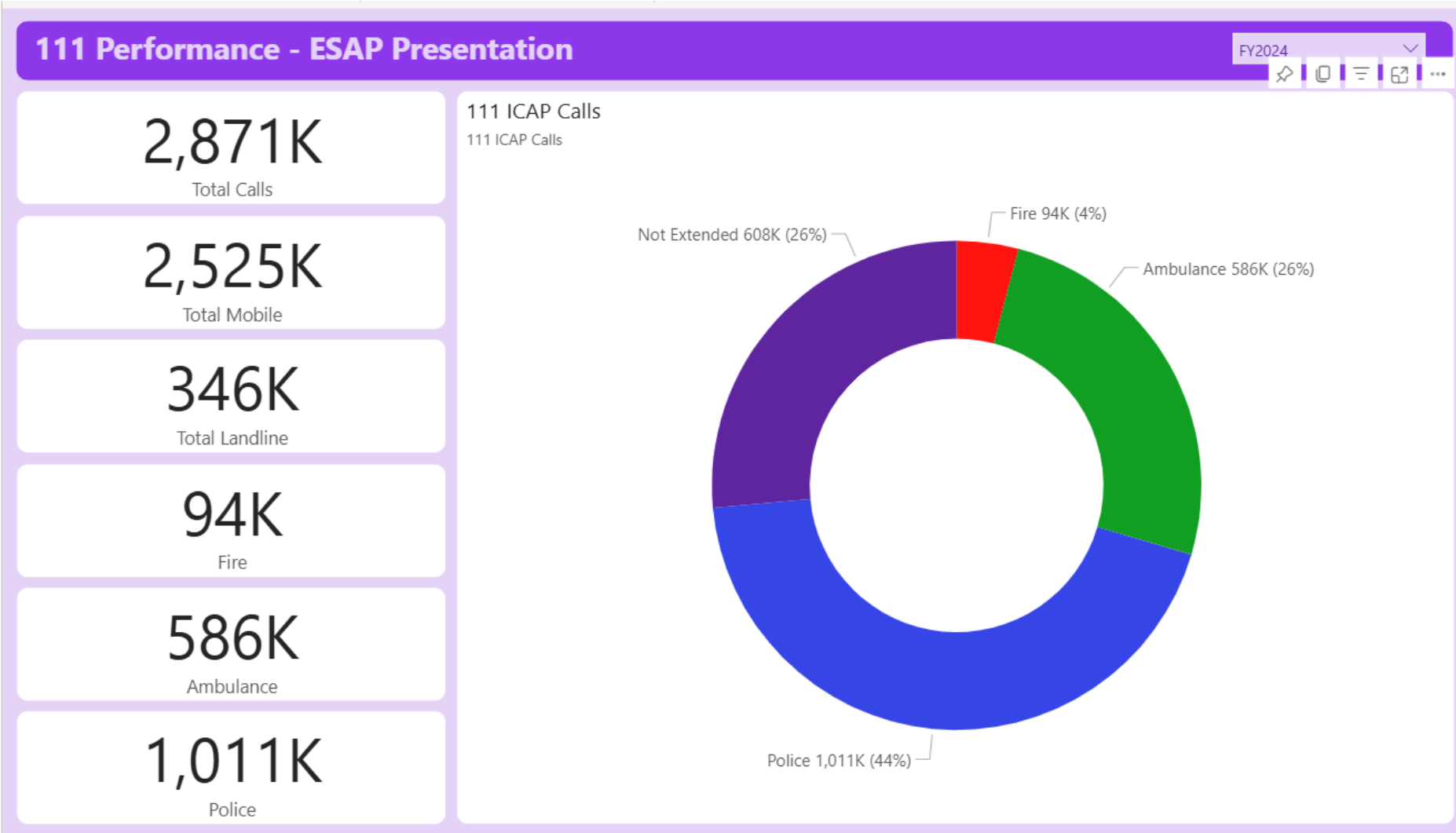
Appendix Two – Drivers of Demand for 111

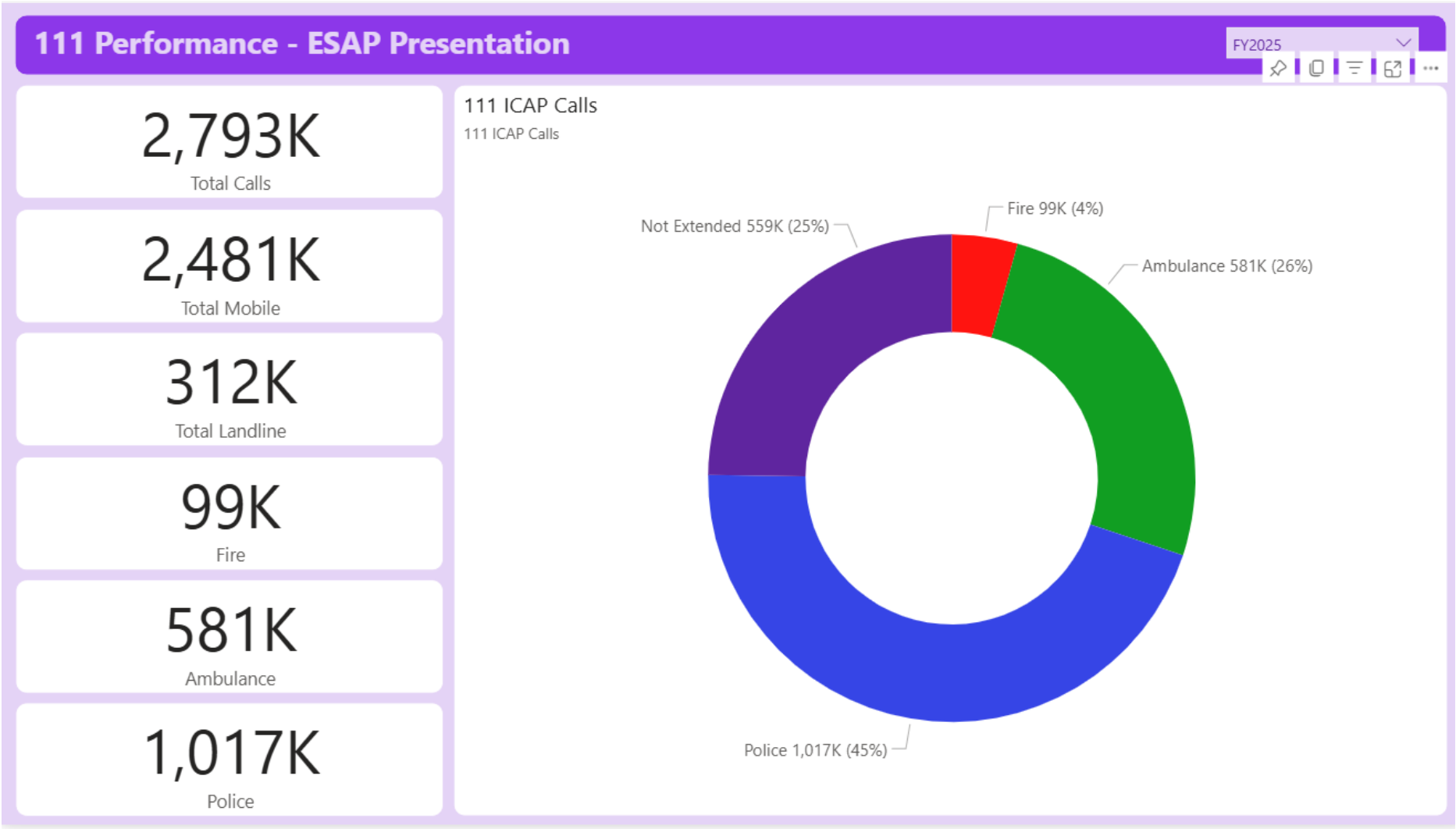
111 Demand is fuelled by:

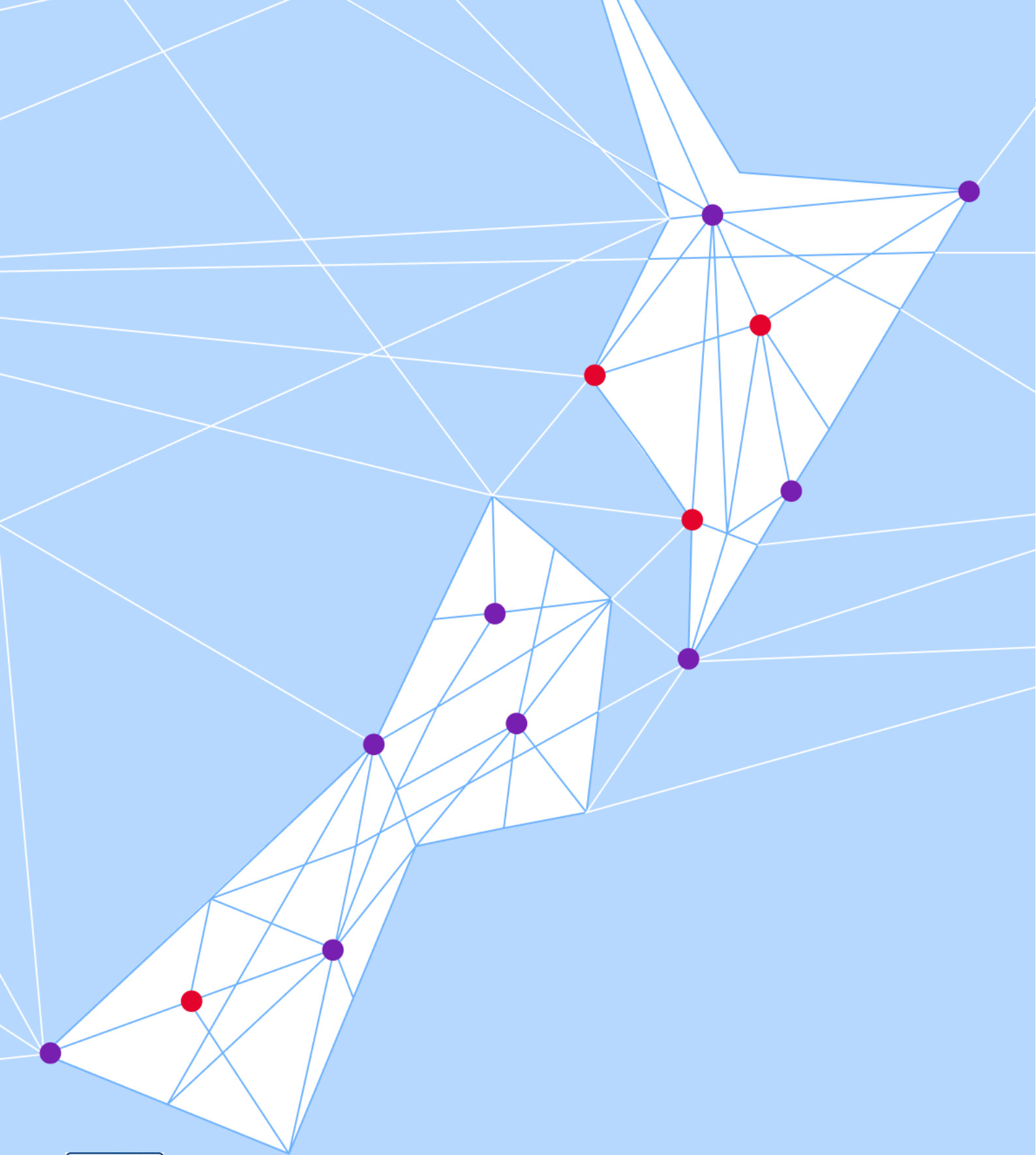
- **Increases in emergency events:** Communities are facing more diverse, frequent, and extreme emergencies including extreme weather events such as the Auckland floods in January 2023 and Cyclone Gabrielle in February 2023, and tropical cyclone Tam in mid-April 2025.
- **Shifts in societal expectations:** Communities are more mobile meaning they can travel and access places in which they expect the same level of communications capability that they would enjoy at home. The significant shift to mobile technology also means the community have more accessibility to services to raise a request rather than having to locate a fixed line service to contact emergency services.
- **Increases in population:** New Zealand's population growth between June 2014 to December 2024 was 18.5% to 5.357 million, it is projected the NZ population will reach between 5.82 and 5.85 million by 2033.
- **Increasing number of non-genuine or accidental calls:** The widespread use of mobile phones, 'smart' devices, and personal alarm devices and/or autonomous devices that can detect risk to a person (i.e. a fall or because of a car crash) has led to an influx of 111 calls. Many of these calls are either non-genuine or notifications of minor incidents that do not require emergency response. In the year ending June 2025, in New Zealand, Spark 111 had almost 2.8 million 111 calls presented to them. Approximately 25% of those calls were not sent on to an ESO and were determined to be either non-genuine, accidental or abandoned 111 calls.
- **The increasing complexity of emergency calls:** 111 calls often involve multiple factors, requiring coordination across ESOs and specialised responders. These calls might involve emergency mental health crises, complex medical needs, criminal offences and victims of crime, fires and chemical hazards requiring single or multi ESO responses or multi-jurisdictional incidents. These require sophisticated call handling and coordinated dispatch, public and first responder safety risks, informed decision-making, clarity of command and control and at times safe forward points.

Appendix Three – 111 Call Analysis 2023, 2024 & 2025









The paper has been a joint effort between New Zealand and Australian members of the National Emergency Communications Working Group - A/NZ (NECWG) given the similar challenges facing both systems.