PERFORMANCE AUDIT 23 JUNE 2023

Management of the Critical Communications Enhancement Program

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

audit office
OF NEW SOUTH WALES

THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

We conduct financial or 'attest' audits of state public sector and local government entities' financial statements. We also audit the Consolidated State Financial Statements, a consolidation of all state public sector agencies' financial statements.

Financial audits are designed to add credibility to financial statements, enhancing their value to end-users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to Parliament. In combination, these reports give opinions on the truth and fairness of financial statements, and comment on entity internal controls and governance, and compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These examine whether an entity is carrying out its activities effectively and doing so economically and efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities.

As well as financial and performance audits, the Auditor-General carries out special reviews, compliance engagements and audits requested under section 27B(3) of the *Government Sector Audit Act 1983*, and section 421E of the *Local Goverment Act 1993*.

GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38EC of the *Government Sector Audit Act 1983,* I present a report titled **'Management of the Critical Communications Enhancement Program'.**

Margaret Crawford PSM
Auditor-General for New South Wales
23 June 2023

RECONCILIATION COMMITMENT STATEMENT

The Audit Office of New South Wales pay our respect and recognise Aboriginal people as the traditional custodians of the land in NSW.

We recognise that Aboriginal people, as custodians, have a spiritual, social and cultural connection with their lands and waters, and have made and continue to make a rich, unique and lasting contribution to the State. We are committed to continue learning about Aboriginal and Torres Strait Islander peoples' history and culture.

We honour and thank the traditional owners of the land on which our office is located, the Gadigal people of the Eora nation, and the traditional owners of the lands on which our staff live and work. We pay our respects to their Elders past and present, and to the next generation of leaders.

auditoffice
OF NEW SOUTH WALES

Banner image: 'Yarning Circle' by Caitlin Liddle, Audit Office Indigenous Internship Program participant used with permission.

contents

Management of the Critical Communications Enhancement Program

Section one – Management of the Critical Communications Enhancement Program

Executive summary 1

Introduction 9

Performance of the enhanced Public Safety Network 15

Costing the enhanced Public Safety Network 32

Section two – Appendices

Appendix one – Response from agency 39

Appendix two – Trunked public safety radio networks 41

Appendix three – About the audit 43

Appendix four – Performance auditing 45

Section one

Management of the Critical Communications Enhancement Program

Executive summary

Public safety radio networks are critical for operational communications among Emergency Services Organisations (ESOs), which in New South Wales include:

- NSW Ambulance
- Fire and Rescue NSW
- NSW Police Force
- NSW Rural Fire Service
- NSW State Emergency Service.[1]

Since 1993, these five ESOs have had access to a NSW Government owned and operated radio communications network, the Public Safety Network (PSN), to support their operational communications. Around 60 to 70 other entities also have access to this network, including other NSW government entities, Commonwealth government entities, local councils, community organisations, and utility companies.

Pursuant to the *Government Telecommunications Act 2018* ('the Act'), the New South Wales Government Telecommunications Authority ('NSW Telco Authority') is responsible for the establishment, control, management, maintenance and operation of the PSN.[2]

Separate to the PSN, all ESOs and other government entities have historically maintained their own radio communication capabilities and networks. Accordingly, the PSN has been a supplementary source of operational radio communications for these entities.

These other radio networks maintained by ESOs and other entities are of varying size and capability, with many ageing and nearing their end-of-life. There was generally little or no interoperability between networks, infrastructure was often co-located and duplicative, and there were large gaps in geographic coverage.

In 2016, the NSW Telco Authority received dedicated NSW Government funding to commence the Critical Communications Enhancement Program (CCEP).

According to NSW Telco Authority's 2021–22 annual report, the CCEP is a transformation program for operational communications for NSW government agencies. The CCEP '…aims to deliver greater access to public safety standard radio communications for the State's first responders and essential service agencies'. The objective of CCEP is to consolidate the large number of separate radio networks that are owned and operated by various NSW government entities and to enhance the state's existing shared PSN. The program also aims to deliver increased PSN coverage throughout New South Wales.

The former NSW Government intended that as the enhanced PSN was progressively rolled-out across NSW, ESOs would migrate their radio communications to the enhanced network, before closing and decommissioning their own networks.

About this Audit

This audit assessed whether the CCEP is being effectively managed by the NSW Telco Authority to deliver an enhanced PSN that meets ESOs' requirements for operational communications.

We addressed the audit objective by answering the following two questions:

[1] The definition of 'emergency services organisation' is set out in the *State Emergency and Rescue Management Act 1989* (NSW). In addition to the five ESOs discussed in this report, the definition also includes: Surf Life Saving New South Wales; New South Wales Volunteer Rescue Association Inc; Volunteer Marine Rescue NSW; an agency that manages or controls an accredited rescue unit; and a non-government agency that is prescribed by the regulations for the purposes of this definition.
[2] Section 15(1) of the *Government Telecommunications Act 2018* (NSW).

1. Have agreed ESO user requirements for the enhanced PSN been met under day-to-day and emergency operational conditions?
2. Has there been adequate transparency to the NSW Government and other stakeholders regarding whole-of-government costs related to the CCEP?

In answering the first question, we also considered how the agreed user requirements were determined. This included whether they were supported by evidence, whether they were sufficient to meet the intent of the CCEP (including in considering any role for new or alternative technologies), and whether they met any relevant technical standards and compliance obligations (including for cyber security resilience).

While other NSW government agencies and entities use the PSN, we focused on the experience of the five primary ESOs because these will be the largest users of the enhanced PSN.

Both the cost and time required to complete the CCEP roll-out have increased since 2016. While it was originally intended to be completed in 2020, this is now forecast to be 2027. Infrastructure NSW has previously assessed the reasons for the increases in time and cost. A summary of the findings made by Infrastructure NSW is presented in Chapter 1 of this report. Accordingly, as these matters had already been assessed, we did not re-examine them in this performance audit.

The auditee for this performance audit is the NSW Telco Authority, which is a statutory authority within the Department of Customer Service portfolio.

In addition to being responsible for the operation of the PSN, section 5 of the Act also prescribes that the NSW Telco Authority is:

- to identify, develop and deliver upgrades and enhancements to the government telecommunications network to improve operational communications for government sector agencies
- to develop policies, standards and guidelines for operational communications using telecommunications networks.

The NSW Telco Authority Advisory Board is established under section 10 of the Act. The role of the board is to advise the NSW Telco Authority and the minister on any matter relating to the telecommunications requirements of government sector agencies and on any other matter relating to the functions of the Authority. As of 2 June 2023, the responsible minister is the Minister for Customer Service and Digital Government.

The five identified ESOs are critical stakeholders of the CCEP and therefore they were consulted during this audit. However, the ESOs were not auditees for this performance audit.

Conclusion

In areas of New South Wales where the enhanced Public Safety Network has been implemented under the Critical Communications Enhancement Program, the NSW Telco Authority has delivered a radio network that meets most of the agreed requirements of Emergency Services Organisations for routine and emergency operations.

In April 2023, the enhanced Public Safety Network (PSN) was approximately 50% completed. In areas where it is used by Emergency Services Organisations (ESOs), the PSN generally meets agreed user requirements. This is demonstrated through extensive performance monitoring and reporting, which shows that agreed performance standards are generally achieved. Reviews by the NSW Government and the NSW Telco Authority found that the PSN performed effectively during major flood events in 2021 and 2022.

Where it is completed, PSN coverage is generally equal to or better than each ESO's individual pre-existing coverage. The NSW Telco Authority has a dedicated work program to address localised coverage gaps (or 'blackspots') in those areas where coverage has otherwise been substantively delivered. Available call capacity on the network far exceeds demand in everyday use. Any operational issues that may occur with the PSN are transparent to ESOs in real time.

The NSW Telco Authority consulted extensively with ESOs on requirements for the enhanced PSN, with relatively few ESO requirements not being included in the specifications for the enhanced PSN. Lessons from previous events, including the 2019–20 summer bushfires, have informed the design and implementation of the enhanced PSN (such as the need to ensure adequate backup power supply to inaccessible sites). The network is based on the Project 25 technical standards for mission-critical radio communications, which is widely-accepted in the public safety radio community throughout Australia and internationally.

There is no mechanism to ensure adequate radio coverage within new building infrastructure after the CCEP concludes, but the NSW Telco Authority and ESOs have agreed an approach to prioritise existing in-building sites for coverage for the duration of the CCEP.

The extent to which the PSN works within buildings and other built structures (such as railway tunnels) is of crucial importance to ESOs, especially the NSW Police Force, NSW Ambulance, and Fire and Rescue NSW. This is because a large proportion of their operational communications occurs within buildings.

There is no mechanism to ensure the adequacy of future in-building coverage for the PSN in new or refurbished buildings after the CCEP concludes. Planning, building, and fire regulations are silent on this issue. We note there are examples in the United States of how in-building coverage for public safety radio networks can be incorporated into building or fire safety codes.

In regard to existing buildings, it is not possible to know whether a building requires its own in-building PSN infrastructure until nearby outside radio sites, including towers and antennae, have been commissioned into the network. Only then can it be determined whether their radio transmissions are capable of penetrating inside nearby buildings. Accordingly, much of this work for in-building coverage cannot be done until outside radio sites are finished and operating.

In March 2023, the NSW Telco Authority and ESOs agreed on a list of 906 mandatory and 7,086 non-mandatory sites for in-building PSN coverage. Most of these sites will likely be able to receive radio coverage via external antennae and towers, however this cannot be confirmed until those nearby external PSN sites are completed. The parties also agreed on an approach to prioritising those sites where coverage is needed but not provided by antennae and towers. Available funding will likely only extend to ensuring coverage in sites deemed mandatory, which is nonetheless expected to meet the overall benchmark of achieving 'same or better' coverage than what ESOs had previously.

There is a risk that radio interoperability between ESOs will not be maximised because the NSW Telco Authority has not settled with ESOs how encryption will be used across the enhanced PSN.

End-to-end encryption of radio transmissions is a security feature that prevents radio transmissions being intercepted or listened to by people who are not meant to. The ability of the PSN to provide end-to-end encryption of operational communications is of critical importance to the two largest prospective users of the PSN: the NSW Police Force and NSW Ambulance. Given that encryption excludes other parties that do not have the requisite encryption keys, its use creates an obstacle to achieving a key intended benefit of the CCEP, that is a more interoperable PSN, where first responders are better able to communicate with other ESOs.

Further planning and collaboration between PSN participants are necessary to consider how these dual benefits can be achieved, including in what operational circumstances encrypted interoperability is necessary or appropriate.

The capital cost to the NSW Telco Authority of the CCEP, originally estimated at $400 million in 2016, was not made public until the 2021–22 NSW Budget disclosed an estimate of $1.325 billon.

The estimated capital cost to complete all stages of the CCEP increased over time. This increasing cost was progressively disclosed to the NSW Government through Cabinet processes between 2015–16 and 2021–22.

In 2016, the full capital cost to the NSW Telco Authority of completing the CCEP was estimated to be $400 million. This estimated cost was not publicly disclosed, nor were subsequent increases, until the cost of $1.325 billion was publicly disclosed in the 2021–22 NSW Budget (revised down in the 2022–23 NSW Budget to $1.293 billion).

There has been no transparency about the whole-of-government cost of implementing the enhanced PSN through the CCEP.

In addition to the capital costs incurred directly by the NSW Telco Authority for the CCEP, ESOs have incurred costs to maintain their own networks due to the delay in implementing the CCEP. The ESOs will continue to incur these costs until they are able to fully migrate to the enhanced PSN, which is expected to be in 2027. These costs have not been tracked or reported as part of transparently accounting for the whole-of-government cost of the enhanced PSN. This is despite Infrastructure NSW in 2019 recommending to the NSW Telco Authority that it conduct a stocktake of such costs so that a whole-of-government cost impact is available to the NSW Government.

1. Key findings

Where available and used by ESOs, the enhanced PSN has met user requirements regarding coverage and availability

At the time of this audit, the enhanced Public Safety Network (PSN) was approximately 50% completed, with full completion currently expected in 2027. The performance of the enhanced PSN cannot be conclusively assessed while it is still being delivered. However, the performance data and experience to date suggest that, when it is completed, the enhanced PSN will likely be effective in meeting the majority of ESO requirements for coverage and availability.

The enhanced PSN generally meets the benchmark of 99.95% availability for all sites. Individual sites also consistently meet the agreed requirement that no more than 1 in 1,000 calls should be delayed (or queued) by more than one second.

On current plans, the geographic coverage of the enhanced PSN will exceed any radio coverage previously available to ESOs. Moreover, the NSW Telco Authority is actively working with ESOs to identify and resolve individual coverage gaps, including reprioritising sites to 'fill in' coverage gaps (or 'blackspots') in defined geographical areas. This should enable ESOs to fully migrate to the PSN in these areas.

Formal reviews that considered the performance of the enhanced PSN during a series of natural disasters have been positive, particularly from the flood events in northern NSW in 2021 and 2022. Reviews from the 2019–20 bushfires resulted in changes to the CCEP's design for the enhanced PSN, including provision of:

- greater resilience in power supply to sites, including larger backup batteries and additional mobile generators
- additional mobile radio assets
- improved interjurisdictional interoperability.

Outside of major events and disasters, the enhanced PSN has ample capacity, with overall network routine usage averaging around five per cent of capacity, and most individual sites running below 15% of their capacity. While congestion can occur during major events, such as during the northern New South Wales flood event of February to March 2022, this can be mitigated using mobile radio assets.

Despite targeting an important risk, a draft network congestion management plan has not been finalised and tested

In addition to the technical and infrastructure solutions for heightened capacity and congestion management, a draft PSN Traffic Mitigation Plan has been prepared for managing how access is prioritised if the network is congested or capacity is exceeded.

When finalised, this plan is intended to outline the:

> …traffic mitigation principles, levels, procedures and policies that must be followed by all agencies in the event of network congestion.

This plan has been in draft form since June 2019 and consequently has not been tested in simulations or other scenario-based training.

There is no mechanism to ensure adequate radio coverage within new building infrastructure after the CCEP concludes, but the NSW Telco Authority and ESOs have agreed an approach to prioritise existing in-building sites for coverage for the duration of the CCEP

A key piece of work scheduled for later delivery under the CCEP is to complete in-building coverage for the enhanced PSN (that is, coverage within built structures that cannot be penetrated by external radio transmission).

In-building coverage is an important issue for NSW Police Force, Fire and Rescue NSW, and NSW Ambulance because a large proportion of their operational communications occurs within buildings and other infrastructure, such as railway tunnels. More in-building coverage would be a significant benefit of the CCEP to these agencies, which have principally relied on alternative forms of communication that may not always reach mission critical standards of reliability where existing in-building coverage is unavailable.

Beyond the completion of the CCEP, there is no ongoing mechanism in New South Wales to consider the need for future coverage for the enhanced PSN within new or refurbished building infrastructure. Unlike in the United States, for example, building and fire regulations in Australia do not require developers or builders to address this issue during approvals for building design or construction.

In regard to existing building infrastructure, the need for additional sites that provide in-building coverage can only be determined once nearby outdoor radio sites are finished, and the coverage provided by these sites is tested within buildings.

In March 2023, the NSW Telco Authority and ESOs agreed on a list of 906 mandatory and 7,086 non-mandatory sites for in-building PSN coverage. Of the 906 mandatory sites, the NSW Telco Authority has estimated that around 650 will receive coverage from nearby external towers and antennae, meaning that between 200 and 250 sites will require specific infrastructure or other solutions to ensure adequate in-building coverage. The NSW Telco Authority has estimated that around 140 (two per cent) of the non-mandatory sites would require their own infrastructure to receive adequate coverage.

The governance mechanisms for the ongoing operation of the enhanced PSN are unclear in how they ensure that ESOs participate in future operational decisions about the network

As sections of the CCEP are completed, the former NSW Government mandated that ESOs progressively decommission their own radio networks and migrate to the enhanced PSN. The NSW Telco Authority will remain responsible for the operation and maintenance of the PSN. The PSN will transform from being a supplementary source of radio communications, to being the only source of mission critical radio communications for ESOs. The ESOs will depend entirely on the NSW Telco Authority to provide their primary mission critical communications. This greater degree of dependency heightens the need for governance mechanisms to support transparency, trust, and collaboration between parties for the ongoing operation of the enhanced PSN after the CCEP has concluded.

The comprehensive governance arrangements the NSW Telco Authority has put in place for implementation of the CCEP provides a collaborative approach, with ESO's included in making key decisions about the CCEP. This is facilitated primarily by a Program Steering Committee, which is the highest decision-making body for the CCEP. This committee is chaired by a Deputy Secretary from the Department of Customer Service and comprised of senior executives of the NSW Telco Authority and all ESOs, and serves functions such as:

- considering, acknowledging, and providing guidance on high impact issues and risks to enable the achievement of CCEP benefits
- providing strategic guidance, support, and high-level oversight to assist the CCEP in achieving its outcomes.

It will be important that a similar governance mechanism is available to allow ESOs to participate in key operational and service delivery decisions for the enhanced PSN on a permanent basis after the CCEP concludes.

One option that could satisfy this need is the Operations Service Delivery Governance forum, one purpose of which is to '…facilitate collective governance of the PSN for operational matters, supporting a common purpose in representation of all PSN users'. The intent of this forum appears to be to foster formal engagement with the ESOs on the operation of the enhanced PSN. However, the audit was provided with incomplete terms of reference for this forum, which did not clarify:

- those matters on which ESOs could make decisions
- how decisions would be made, including decision rules
- what escalation processes were available in the event of dispute
- the standing of any made decisions, including whether decisions of the forum could be overruled.

The potential cloning of unauthenticated radio terminals poses a risk to the security of communications over the enhanced PSN and needs to be addressed as a matter of urgency

All ESOs required that the enhanced PSN should have the capability to authenticate terminals (which includes radio handsets, desk-based consoles, and radios in vehicles). This capability prevents the 'cloning' of terminals by validating their authenticity, thereby preventing individuals or organisations accessing the enhanced PSN without authorisation.

While around 98% of existing handsets are capable of being authenticated, the NSW Telco Authority has not expedited the mandatory authentication of these handsets. Only around 42% are currently authenticated. The NSW Telco Authority has also not implemented effective interim strategies to mitigate the risk of unauthenticated terminals accessing the network.

The NSW Telco Authority has not settled arrangements with ESOs to ensure that, where required, encrypted radio calls can be made between first responders from different agencies

Among the intended benefits of the enhanced PSN are improved security of calls through the optional use encryption, as well as improved interoperability of communications between ESOs.

Interoperability includes the capability for first responders to make and receive calls between different ESOs during operations that require a multi-agency response.

Functionally, there can be an inherent incompatibility between encryption and interoperability. While the former is intended to restrict who can participate in a call, the latter is intended to foster greater sharing of information. In effect, unless carefully managed, encryption can inhibit interoperability in those operational circumstances where secure communications are required during multi-agency incidents or campaigns.

If encryption is used across the PSN without a strategy to deal with this incompatibility, there is a risk that the intended benefit of interoperability will not be realised. Encrypted interoperability requires the sharing of encryption keys, and therefore effective coordination and cooperation is required between ESOs and the NSW Telco Authority.

Further work is necessary by the NSW Telco Authority, in collaboration with the ESOs, to identify in what circumstances encryption and interoperability are each required (including in combination) by each ESO, and what technical and governance measures are needed (such as rules and agreements around the sharing of encryption keys). The NSW Telco Authority has approved a Radio Encryption and Authentication program, which, if implemented, may support addressing this issue.

While the increasing capital cost of the CCEP was known to key decision-makers in the former NSW Government, it was not communicated to Parliament or the community until the 2021–22 NSW Budget

In 2016, the NSW Telco Authority determined an initial estimate that the total capital cost directly incurred by it to complete the CCEP would be $400 million. This estimate increased over time. When the 2021–22 NSW Budget was delivered, the estimated total capital cost was revealed as $1.325 billion (subsequently revised down in the 2022–23 NSW Budget to $1.293 billion).

The initial and updated costs were provided to the former NSW Government through Cabinet processes between 2015–16 and 2021–22.

However, the initial total cost of the program and its growth over time were not made transparent to Parliament or the community until the then estimated total capital cost of $1.325 billion was included in the 2021–22 NSW Budget papers. Before this time, budget papers and media releases did include information about some estimated costs, though these amounts were only partial costings for the program, such as for the first three stages or for individual work items.

The full cost of the enhanced PSN has not been tracked or reported during the program

In addition to the capital costs incurred by the NSW Telco Authority for the CCEP, costs have been incurred by the ESOs due to delays in implementing the CCEP. These costs include maintaining their own radio equipment, infrastructure and networks. As ESOs will need to continue to maintain their own networks until they fully migrate to the enhanced PSN (expected in 2027), these costs will continue to be incurred.

These costs incurred by ESOs have not been tracked to determine the whole-of-government cost of the enhanced PSN. This is despite a review conducted by Infrastructure NSW in 2019 that included the 'critical recommendation' that the NSW Telco Authority:

> …coordinate a stocktake of the costs of operational bridging solutions implemented by PSAs [ESOs] as a result of the 18-month delay, so that a whole-of-government cost impact is available to the NSW Government.

It should be noted that forecast completion of the CCEP was delayed from 2020 to 2027 and that further ‘operational bridging solutions’ have been needed by the ESOs to maintain their own radio networks.

We have estimated that the full cost to government of implementing the enhanced PSN could ultimately be over $2 billion. We derived this estimate by considering:

- the costs incurred by ESOs
- planned costs for the refresh of the paging network
- planned costs of decommissioning existing networks
- capital and operating costs incurred by the NSW Telco Authority, including any infrastructure required to provide in-building coverage.

The full cost of the CCEP project to government has not been tracked by agencies in a consistent manner that allows for comparison over time and was not made transparent to government through any process.

The NSW Telco Authority is not fully compliant with its policy on reserving infrastructure capacity in new radio sites for potential future events, such as expanding the PSN or adopting new communication technologies

In 2021, the NSW Telco Authority introduced the Infrastructure Capacity Reservation Policy, which aimed to make PSN infrastructure readily available to support the possible future introduction of new communication capabilities or technologies. The policy recognises that there are potential efficiencies to be derived by providing additional capacity when PSN infrastructure is first built, rather than having to retrofit or build new infrastructure in the future.

Provisions in the policy include such things as ensuring excess power capacity, reserving physical space in built infrastructure for future equipment, prescribing the height and types of towers that should be built, and the configuration and height of antennae.

The policy requires that planned reservations would be recorded by the NSW Telco Authority in a centralised database that was to be launched by 2021. This has yet to occur. Accordingly, it is unclear how effective this policy will be in delivering its intent and when it will be implemented.

2. Recommendations

The NSW Telco Authority should (in consultation with the Emergency Services Organisations):

1. by October 2023, finalise its PSN Traffic Mitigation Plan and determine a schedule and method by which that plan will be tested
2. by December 2023, review whether current or planned governance arrangements for the enhanced PSN are adequate and appropriate for the evolving relationship between agencies, including to support ongoing collaboration and communication
3. by January 2024, work with other relevant NSW government agencies to provide advice to the NSW Government on the options, benefits and costs of addressing the regulatory gap for in-building public safety communications coverage in new and existing buildings
4. by March 2024, consider what, if any, technical and governance arrangements are required for circumstances where operational communications requires both encryption and interoperability

The NSW Telco Authority should:

5. ensure that it complies with its Infrastructure Capacity Reservation Policy
6. expedite the mitigation of the risk of cloning of unauthenticated terminals by taking the following steps:
    a) by October 2023, implement interim strategies to identify and address the risk of cloned terminals
    b) by June 2024, require that authentication-capable terminals be authenticated
    c) by June 2025, require that all terminals using the enhanced PSN be authenticated.

1. Introduction

1.1 Background

NSW Government Public Safety Network and the Critical Communications Enhancement Program

The NSW Government Public Safety Network (PSN) – previously called the Government Radio Network (GRN) – was established in 1993 with the intention of providing a common mobile radio platform for the five primary Emergency Services Organisations (ESOs):

- NSW Ambulance
- Fire and Rescue NSW
- NSW Police Force
- NSW Rural Fire Service
- NSW State Emergency Service.[3]

This network is also used by other NSW and Commonwealth government agencies, local councils, community organisations, and utility service providers.

However, the PSN has historically only supplemented the radio communication capabilities of these entities, with the ESOs and other entities maintaining their own radio networks and capabilities. In total, there have been up to 70 different radio networks of varying scope and scale, maintained by these entities. The five ESOs are overwhelmingly the main users of the PSN. While the NSW Police Force has only used the PSN for limited operational purposes, it is expected to fully migrate to the enhanced PSN in the future, when the network's coverage and capability is further progressed.

The Critical Communications Enhancement Program (CCEP) was established in 2016 to enhance the PSN's capacity, coverage and performance, enabling NSW government agencies to close their own radio networks and rely on the PSN for mobile radio communications. When completed, the CCEP will expand the coverage of the PSN from approximately 26% to 85% of the geography of New South Wales and extend population coverage from approximately 80% to 99.7%. This level of communications coverage is considered critical to protect people, places, and frontline responders. The expanded network is intended to allow the five ESOs (and other existing users of the PSN) to fully migrate from their separate radio networks onto a single, integrated network, thereby reducing duplication and its inherent costs, and delivering interoperability between ESOs.

The day-to-day management of the PSN is conducted by a private company, BAI Communications ('BAI'), as the managing network partner under contract with the NSW Telco Authority. The re-appointment of BAI was announced in December 2020 under a five-year contract valued at $80 million. BAI has held the contract for the operation and maintenance of the PSN since August 2013.

The PSN is a 'trunked' radio network. While conventional radio networks have defined channels for different groups of users, trunked radio networks have defined groups of users (or 'talkgroups') that are automatically allocated by a computerised network controller to any available channel at the time a user wants to transmit a call. This is discussed further in Appendix two.

[3] The definition of 'emergency services organisation' is set out in the *State Emergency and Rescue Management Act 1989* (NSW).

The PSN does not include the Triple Zero (000) and 112 Emergency-call taking service. Pursuant to the Telecommunications (Emergency Call Service) Determination 2019 and contractual arrangements, when a person calls 000 or 112, they speak to a Telstra emergency call service operator first. Telstra transfers the call to the required individual ESO in each jurisdiction. The emergency response is provided by the requested ESO.

Intended benefits of CCEP

The CCEP emerged from the NSW Telco Authority's 2015 Infrastructure Rationalisation Program (IRP) and the then NSW government's 2015 Operational Communications Strategy (updated in 2020).

The IRP objective was to:

> …rationalise more than 70 radio networks currently being used by NSW government agencies for public safety and other purposes. These multiple networks currently cause significant duplication of capacity, coverage and cost across New South Wales.

The IRP noted that:

> ...many of these networks are at or near end of life and will require major reinvestment in the short term, which would perpetuate this duplication, continue to limit opportunities for standardisation and increased contestability, as well as potentially jeopardise service delivery by Government and community safety.

Network enhancements expected from the IRP included:

- increased coverage
- network interoperability
- increased reliability.

The IRP also intended that rationalisation would enable centralisation of network ownership and management, delivering reduced duplication of support costs and increased innovation. This recognised that, at the time the IRP was prepared, more than 80% of sites maintained across individual agency radio networks were within five kilometres of another NSW government radio site.

The Operational Communications Strategy committed to 'deliver a resilient and secure communications capability for the sector that supports mission critical services for voice, video and data'. The strategy complemented the IRP and introduced a new operating model where public safety agencies would no longer own and operate their radio networks. Instead, the NSW Telco Authority focussing on planning and governance of the integrated portfolio of assets and services on behalf of the NSW Government.

In December 2015, the then Department of Finance, Services and Innovation advised all NSW government agencies that the NSW Telco Authority had commenced the CCEP in order to create a single shared radio network. Agencies were required to provide the NSW Telco Authority access to their radio sites, and information to allow rationalisation planning and works to be carried out.

The expected operational and economic benefits described in the IRP and Operational Communications Strategy were subsequently reflected in the business cases for the CCEP.

Program history

The CCEP commenced in 2016, following the then NSW Government's approval of the program scope outlined in a business case submitted by the NSW Telco Authority in March 2016. However, due to the NSW Government's staged-funding approach, the program progressed in four stages:

- Stage 1 – 2016 pilot in north-west New South Wales
- Stage 2 – 2018 to 2022 roll out into the North Coast of New South Wales as well as selected priority sites
- Stage 3 – 2019 to 2022 greater Sydney metro and priority sites
- Stage 4 – 2020 to 2026 rest of New South Wales.

In October 2022, the completion date for the full state-wide PSN was 're-baselined' again from 2026 to 2027.

As shown in Exhibit 1 below, between 2016 and 2020, the NSW Government approved three business cases to design and deliver the enhanced PSN.

Exhibit 1: Evolution of business cases for the CCEP

Key components of business cases	March 2016	March 2020	October 2020
Stage nominally included	1 to 4	1, 2 and 3	4
Number of PSN sites in business case	732	357	318
Total number of PSN sites expected	732	675	675
Estimated program completion date	2020	2025#	2026
Expected capital cost of business case ($ million)	$400	$617.9	$645.2
Expected full capital cost of CCEP ($ million)	$400	$950 to $1,050	$1,263.1
Expected population coverage of PSN	96%	98%	99.7%
Expected geographic coverage of PSN	77.1%	85%	90%^
Paging network refresh	Included	Not included	Not included

The 2025 program completion date in the March 2020 business case included the future Stage 4.

^ The 90% expected geographic coverage in the October 2020 business case was subsequently revised down to 85%.

Delays and cost increases

The estimated capital cost for the CCEP increased from $400 million in the March 2016 business case, to $1,263.1 million in the October 2020 business case. In the 2022–23 NSW Budget, the capital cost estimate for the program was $1,292.8 million (below the $1,325 million estimated in the 2021–22 NSW Budget).

In addition to cost increases, the time expected to complete the enhanced PSN has increased. Under the 2016 business case, it was expected to be completed in 2020, though this has been revised several times and is currently 2027, seven years later than originally anticipated.

Infrastructure NSW examined the reasons for these delays as part of its project monitoring and assurance role. This audit has not re-examined these reasons, which include:

- significant optimism bias in the mobilisation phase, particularly in site acquisition and design, including government owned property, which required legislative amendments made by the *Government Telecommunications Amendment Act 2022*
- performance and resourcing by the NSW Telco Authority's initial Program Management Office provider
- poor quality of site information
- poor quality engagement and delivery by vendors
- extended time taken to recruit the required project leadership
- adequacy of project costings and contingency allocation.

These assessments were made prior to the 2019–20 east coast bushfire season, the COVID-19 pandemic, and the 2021 and 2022 flood events, each of which were likely to have contributed to further delays and cost increases.

ESO involvement and migration to the enhanced PSN

The migration of ESOs from their own radio networks to the enhanced PSN is incremental and ongoing. As the NSW Telco Authority enhances the PSN in defined geographic areas, ESOs migrate to the network in that area and decommission their own networks. All ESOs except for NSW Police Force have now migrated substantial parts of their radio capability to the enhanced PSN.

Some NSW Police Force specialist commands have migrated to the PSN, though these represent only a small proportion of total NSW Police Force staff. Over the duration of the CCEP, it had been the intent of NSW Police Force to migrate fully to the enhanced PSN once the network was fully available across the state. NSW Police Force and the NSW Telco Authority reached agreement in late-2022 on an implementation model to expedite this migration, especially in the Greater Sydney Area.

Uses of the PSN

NSW Telco Authority media releases have referenced the potential value of the PSN in improving how ESOs respond during major disasters, particularly in the context of the bushfires and flood emergencies that impacted New South Wales between 2019 and 2022. However, as ESOs migrate to the PSN, the radio network will be their primary tool for all radio communications, not just during major incidents. As well as during major emergencies, such as natural disasters, the network is intended to be used for '…special events, training, and other exercises'.

Currently, NSW Ambulance (44%) and NSW Police Force (six per cent) account for around half of all calls made on the PSN even though only a relatively small proportion of NSW Police Force commands are currently using the network. When both agencies fully migrate to the enhanced PSN, they will account for a substantial majority of PSN calls.

While both NSW Ambulance and NSW Police Force respond to major emergencies, a large proportion of their ongoing use of the PSN is likely to be on a regular basis during their day-to-day public safety operations, including for operations inside or near buildings.

The requirements of day-to-day operations are different to those of major emergency operations. This raises different implications for the PSN. For example, during major emergencies, the call capacity (or availability) of the PSN is more likely to be stressed than during day-to-day operations. For day-to-day operations, reliable geographical coverage is likely to be the critical performance issue, rather than the unlikely risk of network congestion.

The performance of the PSN is also assessed differently in each context. For example, day-to-day operations do not generally undergo the sort of structured and focused assessment that is applied to major emergencies as part of the 'After Action Review' process conducted by the NSW Telco Authority.

As both contexts are important, we have assessed whether the enhanced PSN (as delivered by the CCEP) is meeting the requirements of ESOs in both their day-to-day operations, as well as in major emergencies, such as the natural disasters that affected New South Wales between late 2019 and 2022.

Mission critical communications

Throughout this audit, numerous stakeholders highlighted the importance of public safety radio communications satisfying 'mission critical' criteria. Accordingly, this term is used throughout this report. Despite its wide use in the field, mission critical '...has meant different things to different groups within the first responder community'.

The European-based TETRA and Critical Communications Association (TCCA) defines the term ‘mission critical’ in public safety radio communications as:

> A function whose failure leads to catastrophic degradation of service that places public order or public safety and security at immediate risk.

The TCCA further holds that a mission critical standard requires '… adequate inbuilt functionality, availability, security and interoperability'.

The October 2020 CCEP business case outlined an understanding of the key characteristics of 'Mission critical voice communication'. These characteristics were:

> …communication can occur instantaneously, on a single network with a high standard for redundancy, channels can be accessed immediately with the capability for group discussions and with state-wide inter-regional coverage.

Project 25 technology

The PSN primarily relies on established land mobile radio technology, rather than new or alternative technologies such as satellite or 4G and 5G mobile telecommunications technology.

Land mobile radio technology is considered the only technology that can reliably deliver 'mission critical' capability and as such will be required over the long term to support ESO operational communications. Radio is often the only form of reliable communications in situations such as bushfires, floods and remote locations. The varied topography across New South Wales and its remote areas with a sparse population is not reliably serviced by commercial telecommunications providers.

The technology specification selected for the PSN is called Project 25 (or P25). P25 refers to a collection of standards (and other measures) for radio networks that evolved in the United States (US) in the late-1980s. This was in response to concerns about the lack of interoperability among first responders in dealing with emergencies. Consequently, the development and ongoing evolution of the standards relies heavily on the input of peak professional bodies in public safety communications.

The primary intent of these standards is to encourage interoperability in land mobile radio systems for mission critical communications. This interoperability is achieved through a series of defined standards, protocols, procedures, formats, methods, and tests codified by the US Telecommunications Industry Association (TIA) under industry-standard TIA-102.

The inability of emergency service workers to communicate with those in other services has also previously been identified as a concern in New South Wales and elsewhere in Australia.

Experience in other jurisdictions

There are over 2,800 P25 public safety radio networks throughout the US, Canada, Australia (including government radio networks in New South Wales, Victoria, Queensland, South Australia, Tasmania, the Northern Territory), and New Zealand.

While other Australia states and territories have built mission critical emergency service radio networks using the P25 technical specification, they are not of the same scale as the enhanced PSN in New South Wales. The closest comparable P25 networks appear to be those summarised below.

- Victoria – The Victorian government retains separate networks for Melbourne/Geelong and for regional areas. The two separate networks cover approximately 100% of the state.
- Queensland – the Government Wireless Network that was initially rolled out to coincide with Brisbane's hosting of the G20 Leaders' Summit in 2014 for the Greater Brisbane area and expanded in 2016 to the south-eastern corner of the state, where it provides around 99% population coverage over 30,000 square kilometres from 179 radio sites and has around 17,000 users.
- South Australia – the South Australian government Radio Network comprises around 200 radio sites linked together to form a voice, data and paging network that covers approximately 96% of the population of South Australia and around 20% of the geography of the state.
- Ontario, Canada – the provincial government announced a modernisation program in 2018 of its public safety network, last replaced in 1998 and described as 'one of the largest and most complex' in North America. This project aims to renew the P25 network, including to ensure interoperability between agencies and other networks, as well as to provide better protection of personal information by enabling encrypted communications. The program will provide coverage over 750,000 square kilometres (around 75% of the province), through 475 sites at a cost of $C765 million.
- New Zealand – the New Zealand government announced in 2022 an investment in that country's national public safety network, include both a P25 radio component, though also work to improve mobile broadband for emergency purposes. The program is forecast to cost $NZ1.4 billion over ten years, including the mobile network component, and will incorporate around 450 sites.

2. Performance of the enhanced Public Safety Network

2.1 Regular monitoring of the enhanced PSN's performance

The NSW Telco Authority regularly measures and reports on the performance of the enhanced PSN

The NSW Telco Authority has processes to regularly monitor the performance of the PSN. These include:

- annual and quarterly service reviews
- monthly performance reports provided by the managing network partner
- monthly Service Improvement Forums
- weekly Change Advisory Board meetings.

For example, the managing network partner submits detailed weekly status update reports. These reports include incidents and outages at individual sites in the previous week, including a short description, resolution notes, and the level of priority attached to the incident. The reports also identify upcoming planned maintenance and outages for individual sites.

The managing network partner also submits detailed monthly performance reports on the network as a whole, as well as any individual sites that experience incidents or outages during a period. These performance reports include:

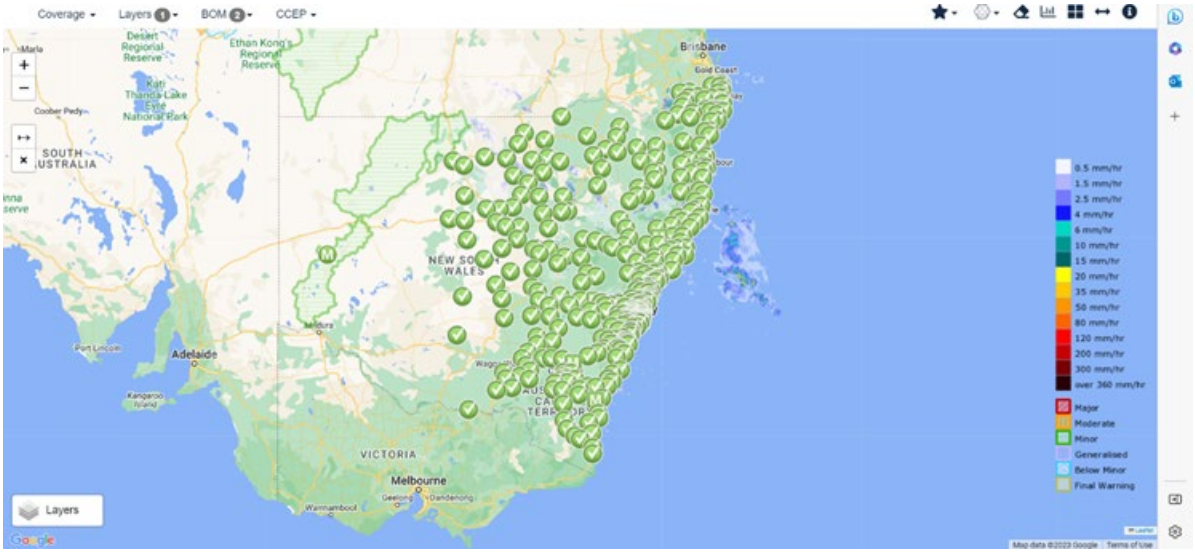
- key learnings and achievements during the month
- availability and reliability of the network and individual sites
- security summary, including cyber and physical
- service level achievement
- network usage data
- 3rd party vendor performance.

In addition, the PSN is subject to real-time monitoring through an online ‘dashboard’ that is available to all ESOs. This application allows all ESOs to view and interrogate the status of individual sites and mobile radio assets, by viewing an interactive map of New South Wales. Flood information and other Bureau of Meteorology data can be overlayed on the same map. This creates greater transparency about the performance of the network by allowing ESOs to view it at any time. ESOs can interrogate the performance of individual PSN sites in regard to:

- site availability
- channel capacity
- grade of service
- utilisation
- power status.

A screen capture of the PSN dashboard is provided below in Exhibit 2.

Exhibit 2: Public Safety Network online performance dashboard



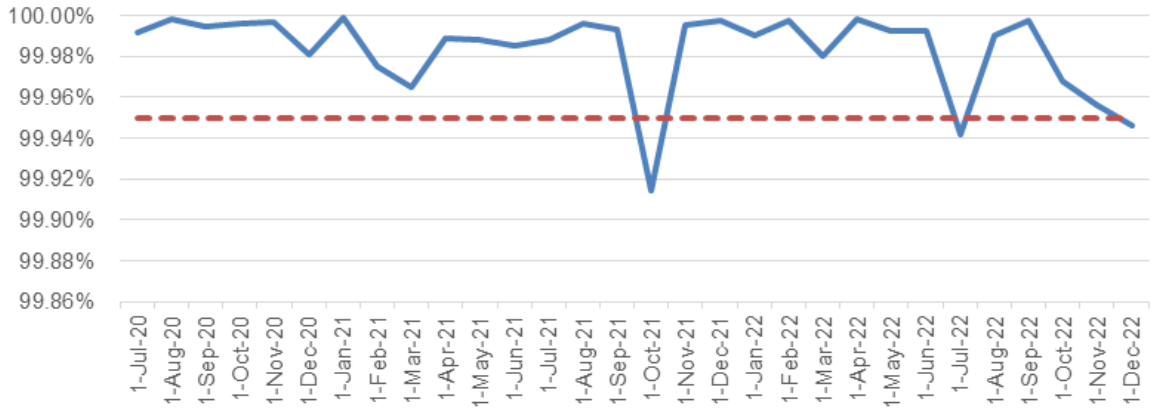
Source: NSW Telco Authority.

The enhanced PSN mostly meets its targets for availability and avoidance of delay in making calls

As a principle, the ESOs require the enhanced PSN to provide mission critical radio communications 'when and where' they need it – these are, respectively, matters of availability (when) and coverage (where). It is a user requirement agreed between the NSW Telco Authority and ESOs that all the sites on the network be available 99.95% of the time. An availability rate of 99.95% is considered a high-level of performance for a mission critical network. It is higher than the 99.91% estimated to have been achieved under the pre-CCEP Government Radio Network.

Exhibit 3 below shows that the 99.95% availability benchmark was met or exceeded in all but three months between July 2020 and December 2022.

Exhibit 3: Average monthly Public Service Network availability, 1 July 2020 to 31 December 2022



Source: Data supplied by NSW Telco Authority.

Small differences in availability can be material. For example, for an individual site, the difference between 99.99% availability and 99.95% is the difference between that site being unavailable for, respectively, four minutes per month or 22 minutes per month.

This can be of particular importance in 'duress' situations, which occur when first responders themselves call for urgent assistance – ensuring the reliability of duress signals is an important user requirement of ESOs and it is a stated intention of the CCEP to ensure first responders are able to raise a duress signal. The NSW Parliament's 2017 inquiry into violence against emergency service personnel made a number of recommendations that highlighted the importance of this functionality, including that the NSW Ambulance should ensure that '…every on duty paramedic has a portable radio capable of duress'. This functionality is important to all ESOs.

The PSN is also assessed for its 'grade of service', which measures whether users are made to wait before they can transmit their communication. This is considered an indicator of 'busy sites', and is based on the number of calls per 1,000 calls in a month that are delayed by more than 1 second (that is, fewer than 0.1% of calls are 'queued'). The NSW Telco Authority proposes that this is a more demanding benchmark than is recommended in the US (one per cent or one in 100 calls). However, we were unable to independently confirm this US-benchmark.

Exhibit 4 below shows performance against this grade of service (or 'busy sites') benchmark at approximately six-month intervals (subject to data availability) from January 2021 to July 2022. In two of the four months selected, all sites achieved the performance target of fewer than 1 in 1,000 busy sites, with the 'worst' performing site in January 2021 having a rate of only 0.23 delayed calls per 1,000 calls.

While the July 2022 period had four sites that exceeded the benchmark, these were affected by the extended major flooding in New South Wales during this period. The two 'sites' with the worst performance were both mobile radio assets.

Exhibit 4: Performance against grade of service target – calls per 1,000 that are delayed from being made for more than one second, selected months 2021 to 2022

Month	Number of sites failing benchmark	Sites with highest number of busy calls in the month	Busy calls per 1,000 calls in the month
January 2021	--	WestConnex East Tunnel	0.23
July 2021	--	Mt Arthur	0.40
December 2021	2	Mobile unit	1.54
		NorthConnex Tunnel	1.07
July 2022[#]	4	Mobile unit	19.7
		Mobile unit	6.78
		Simpsons Hill	1.72
		Bimmil Hill	1.17

Sites in July 2022 were responding to the significant flood event that affected NSW during this period.

Source: Audit Office analysis of NSW Telco Authority data.

2.2 Coverage provided by the enhanced PSN

ESOs will have greater overall geographic coverage from the enhanced PSN than they had previously from their individual networks

Ensuring that the coverage of the PSN, when the CCEP is completed, meets operational needs is a crucial – possibly the most crucial – requirement of the ESOs. A 2016 realisation plan prepared for the CCEP identified that improved coverage for the 'new shared network' (as it was then called) over the then existing 'Government Radio Network' would be the '…biggest driver of benefits for the NSN (New Shared Network), accounting for 75% of total benefits'. The benefits realisation plan noted that, among other benefits, improved coverage would:

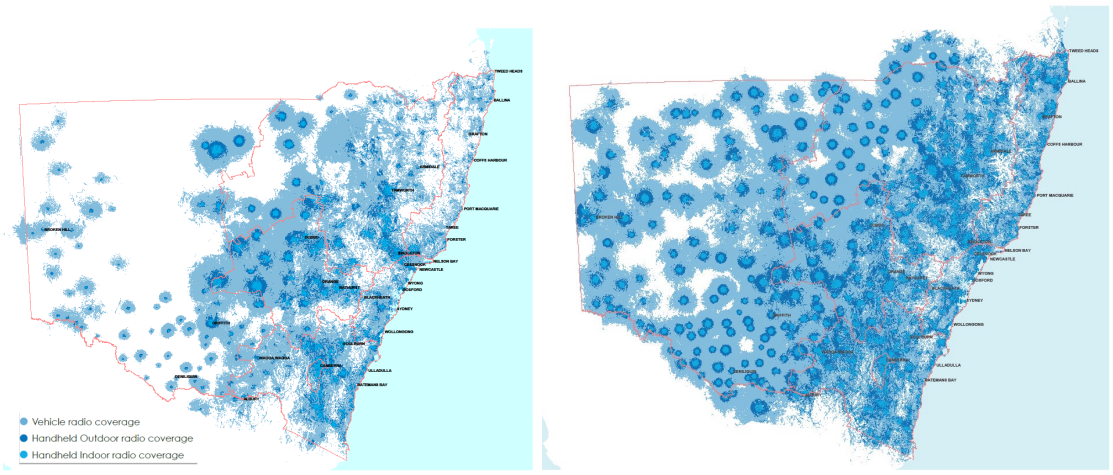
- reduce cardiac mortality by allowing NSW Ambulance to respond to calls when they are in areas not previously covered by existing radio
- reduce regional road accident deaths by allowing first responders, particularly Fire and Rescue NSW and NSW Ambulance, to respond to calls when they are in areas not previously covered by existing radio
- reduce the cost of building fires by enabling firefighters to better prepare and fight building fires due to increased access to portable indoor radio coverage
- reduce the economic cost of serious crime by increasing the productivity of NSW Police Force through increased operational utilisation.

When completed, the enhanced PSN will be required to provide coverage that is, overall, as 'good as or better' than what ESOs had previously. The pre-CCEP coverage available to each ESO is (approximately) the coverage provided by the combination of:

- the pre-existing Government Radio Network (now PSN)
- their own individual radio network.

The NSW Telco Authority prepared detailed mapping of the level of coverage previously available to each ESO, as well as the estimated coverage available to all ESOs when the PSN is completed. The mapping shows that each ESO is expected to have greater overall coverage under the completed PSN than they did before the CCEP commenced. By way of illustration, the pre- and post-CCEP coverage maps (left and right images, respectively) for the NSW Ambulance are shown below in Exhibit 5.

Exhibit 5: Operational radio coverage available to the NSW Ambulance, before (2017) and after (predicted 2027) the CCEP



Source: NSW Telco Authority.

The NSW Telco Authority is working with ESOs to identify and resolve coverage gaps

The process of enhancing overall coverage resulted in some ESOs losing specific pockets of coverage that they previously had under their own networks. Evidence provided by the NSW Telco Authority suggests that these gaps were generally small and localised. One ESO described that, although receiving better coverage overall, its migration from its own network to the PSN had resulted in 'dozens' of gaps in rural and remote areas. Another ESO explained that while it used the PSN where available, it still needed to supplement its radio communications with its own network, particularly outside of the Greater Sydney Area.

The NSW Telco Authority is addressing these coverage gaps through an 'augmentation' module under the CCEP to augment coverage through either additional macro radio sites (such as towers and antennae) or additional in-building coverage sites. Under this work, ESOs may submit claims where they can establish that the enhanced PSN results in a coverage gap compared to their pre-existing radio coverage. Where a coverage gap is confirmed, the NSW Telco Authority works with the ESO to find solutions, which can include repeaters, low power sites, mobile radio assets, or full macro sites with towers and antennae. At December 2022, around 30 additional macro sites were under consideration, while decisions on sites for in-building coverage were held-over until the coverage provided by macro sites (such as external towers and antennae) can be assessed.

The NSW Telco Authority reprioritised sites to accelerate full coverage in identified priority areas

To address coverage gaps, following its final stage funding in June 2021, the NSW Telco Authority revisited its site prioritisation. This was done with a view to identifying sites that could be accelerated so that, when completed, ESOs would be able to migrate fully to the PSN in a defined geographic area. The updated priority list enables all CCEP workstreams (for example, site acquisition and design, build, and operational acceptance) to consider the site migration priority when working on batches of sites. This process saw the number of sites classified as the highest priority increase from 15 to 40, including critical sites in the Greater Sydney Area for the NSW Police Force, and priority sites for NSW Ambulance, NSW Rural Fire Service, and NSW State Emergency Service.

ESOs are also trialling the use of Vehicle-as-a-Node technology to enhance coverage in remote areas or where coverage is otherwise poor. The technology entails a vehicle with multiple communications means, potentially including P25-based PSN, satellite communications, and 4G or 5G-enabled communications.

2.3 In-building coverage

The NSW Telco Authority and ESOs have agreed on sites for in-building coverage

The extent to which the PSN works within buildings and other structures is of crucial importance to ESOs, especially the NSW Police Force, NSW Ambulance, and Fire and Rescue NSW, because a large proportion of their operational communications occurs within buildings.

Decisions about in-building sites and coverage were among the most important outstanding matters for the CCEP. The NSW Telco Authority noted that:

> All NSW ESOs have provided feedback to the [Authority] emphatically in support of improved indoor coverage, particularly in large shopping centres, apartment buildings, tunnels and stadiums.

As at December 2022, the NSW Telco Authority was delaying building new in-building sites until external radio sites are completed. Once these external sites are operational, and their full coverage measured, then the need for in-building sites can be determined.

While final decisions about in-building coverage are dependent on the rollout of the external sites, the NSW Telco Authority has commenced the process of identifying and prioritising possible in-building sites with ESOs.

In March 2023, the NSW Telco Authority and all five ESOs agreed a list of 7,992 sites where in-building coverage could be delivered. Of these sites, 906 were identified as mandatory, of which:

- 412 are NSW Police Force stations that will fall within the coverage of macro sites
- around half of the remaining 494 sites will also be covered by new, existing, or enhanced towers and antennae.

This leaves between 200 and 250 'mandatory' sites that will require their own technical solution to achieve in-building coverage.

In addition to the mandatory sites, there are 7,086 non-mandatory sites identified by the ESOs and the NSW Telco Authority. The NSW Telco Authority has estimated that around 140 (two per cent) of the 7,086 non-mandatory sites would require their own infrastructure to receive adequate coverage, with the balance receiving coverage from nearby external towers and antennae.

Available funding under the CCEP is likely to ensure that in-building coverage is at least equal to that which ESOs had previously

The NSW Telco Authority has estimated that the $25.5 million allocated for in-building coverage under the CCEP will be sufficient to ensure in-building coverage for 49 identified hospitals and between 200 and 250 other sites. If required, additional funding could be sourced from a contingency.

We note advice from the NSW Telco Authority that the $25.5 million funding envelope is unlikely to provide in-building coverage solutions to many (or any) of the identified non-mandatory sites, primarily the 140 that the NSW Telco Authority estimates will not be covered by nearby external towers and antennae.

The overall benchmark for coverage under the enhanced PSN is to provide 'same or better' coverage to each ESO compared to what it previously had. We were advised by the NSW Telco Authority that ensuring adequate in-building coverage for the agreed mandatory sites will meet this benchmark.

There is no regulation setting out circumstances where in-building coverage is required for new and refurbished building infrastructure

The NSW Telco Authority published advisory guidelines for interested parties regarding the requirements for in-building coverage for the enhanced PSN. The guidelines note that:

> In New South Wales and across Australia, there is no building code, regulation or legislation that mandates in-building coverage to support operational communications.

The audit was advised by stakeholders that while some property developers and government departments are mindful of the need to consider public safety communications in their new developments, this is not always the case. We were given an example of a major new (and expensive) place of public gathering and a health care facility that, on opening, either had coverage blackspots or relied on augmented coverage provided by mobile radio assets.

While building codes in Australia are silent on requirements for public safety communications in new buildings or places of mass gathering, we note that, by comparison, section 510.1 of the International Fire Code (2009) adopted by several US states and municipalities requires that:

> All buildings shall have approved radio coverage for emergency responders within the building based upon the existing coverage levels of the public safety communication systems of the jurisdiction at the exterior of the building.

Similar provisions exist in state-based codes in other US jurisdictions.

An alternative model form that exists in a range of US city codes is that:

> …no person shall maintain, own, erect or construct any building or structure or any part thereof or cause the same to be done which fails to support adequate radio coverage for city emergency service workers, including but not limited to firefighters and police officers.

It is unclear how assurance and implementation of in-building coverage in New South Wales, particularly in the private sector, will be provided for new and existing buildings and infrastructure after the CCEP concludes and funding ends.

2.4 Performance of the enhanced PSN during major emergencies

The enhanced PSN performed effectively during the 2021 and 2022 flood emergencies

Evidence regarding the performance of the enhanced PSN during major emergencies since the 2019–20 bushfires indicates that, where it was available, the network performed effectively and met the requirements of ESOs. This evidence includes performance reports, feedback from ESOs, the outcomes of After Action Reviews, and findings made by the independent inquiry commissioned by the NSW Government into the March–April 2022 flood emergency.

The NSW Telco Authority routinely conducts After Action Reviews following major incidents as part of its approach to lessons management. The lessons identified from major events from 2019 to 2022 are focused on operational arrangements, such as information sharing between the NSW Telco Authority and the ESOs, the coordination of resources, and the need to ensure clarity in roles and responsibilities.

There are relatively few lessons reflecting poorly on the performance of the enhanced PSN itself. However, lessons from the 2019–20 bushfire emergency relate to possible deficiencies in the design and build of the PSN.[4] These lessons were:

- the need to achieve greater resilience in the supply of power to radio sites
- the need to consider whether the NSW Telco Authority had sufficient mobile radio assets
- the need to consider the adequacy of radio communications for cross-border emergency responses.

Each of these issues was subsequently added to the CCEP work program through the October 2020 business case augmentation program for network resilience, or addressed as part of funding to implement an Inter RF Sub-system Interface (ISSI).[5] The response to these recommendations also included $14.5 million for items such as additional longer life batteries, trailer mounted generators, and mobile radio assets. These lessons and their adoption reflected recommendations made in the July 2020 NSW Bushfire Inquiry report initiated by the then NSW Government.

Since the 2019–20 summer bushfire emergency, the independent inquiry commissioned by the then NSW Government into the March–April 2022 flood emergency noted that while commercial telecommunications networks were heavily disrupted:

> On the positive side, the Public Safety Network from February to April [2022] maintained availability at 99.92%, managing around 4.3 million calls.

[4] It should be noted that the PSN at this time was in its early stages of being refreshed and enhanced by the CCEP workplan, and that most of the approximately 100 enhanced PSN sites were in the north-west New South Wales pilot area and on the New South Wales North Coast.
[5] Inter RF Sub-system Interface (ISSI) allows interconnection between two or more P25-compliant trunked systems – such as between the P25 PSN in New South Wales, and any P25 networks in bordering states, particularly Queensland and Victoria.

It further noted that the PSN used '…a combination of technologies to provide power in the event of an outage' including on-site 15-hour batteries and, for remote sites, solar power.

The enhanced PSN generally has substantial call capacity, though additional capacity and congestion management has been required during extreme events

The PSN is designed to have substantial capacity for day-to-day operations. Outside of major emergencies, the PSN averages five per cent utilisation overall, with most sites run at below 15% site capacity utilisation. The NSW Telco Authority documented that, in determining site capacity requirements, it has considered inputs and analysis such as:

- existing PSN site traffic volume
- ESO requirements for presence, including incidents data
- existing footprint coverage provided by the PSN and agency networks
- Australian Census population data
- population per PSN site
- traffic forecasts
- required performance grade of service.

However, notwithstanding this detailed and thorough analysis, capacity issues have occurred during major emergencies, particularly the 2019–20 bushfire emergency (when the enhanced PSN was still in its formative stages). The forecast long-term increased incidence and severity of major natural disasters underscore the importance of adequate PSN capacity for these extended and intensive campaigns.

In its review of PSN performance for the full eight-months of the 2019–20 bushfire season, the managing network partner noted that:

> During times of high usage of the GRN [now PSN], key sites 'maxed out' on channels available, prompting radios to seek affiliation to adjacent sites, consequently creating capacity issues overflowing onto adjacent sites.

There are mechanisms in place to manage capacity during major emergencies. These include:

- temporary capacity expansion kits
- adopting a strategy of bringing forward ‘best efforts’ sites (sites that are technically capable of use, though not yet formally online)
- change embargoes, including embargoes on planned outages during emergencies – for example, there were minimal planned outages during January 2020, which contributed to network availability remaining comparatively high (99.987%).

In addition, through 2022, the PSN has progressively moved from Phase 1 to Phase 2 P25 technology. Phase 2 technology provides more efficient use of radio spectrum, effectively allowing the doubling of channels per 12.5 kilohertz bandwidth by use of Time Division Multiple Access, where two independent conversations share the same channel. This provides a permanent solution to enhance capacity.

The NSW Telco Authority has a draft Traffic Mitigation Plan for prioritising access during network congestion

In addition to the technical and infrastructure solutions outlined above to manage capacity and congestion, a draft PSN Traffic Mitigation Plan has been prepared for managing how access is prioritised if the network is congested or capacity is exceeded. When finalised, this plan is intended to outline the:

> …traffic mitigation principles, levels, procedures, and policies that must be followed by all agencies in the event of network congestion.

This plan has been in draft form since June 2019.

While extreme events are, by definition, infrequent, they should be prepared for, especially given the forecast increase in incident and severity of weather events. This can include capability-development through training, simulations, exercises, or desktop reviews.

The words of the NSW State Coroner in his 2017 report of the 'Inquest into the deaths arising from the Lindt Café siege' are relevant at this point:

> Given the serious communication breakdowns that occurred, it is important that these new technologies are tested to check how well they work at times of high radio traffic and monitored to ensure that they adequately meet the needs of future operations.

This testing and monitoring could also extend to the Traffic Mitigation Plan, when finalised. We note that the NSW Telco Authority's ability to conduct additional training and scenario-based exercises was hampered for three years from late 2019 due restrictions imposed by the COVID-19 pandemic and the heightened demands of operational requirements during successive natural disasters.

2.5 Agreeing user requirements

The user requirements for the enhanced PSN have been agreed through a consultative and evidence-based process

From the time the program was commenced in 2016, there was an exhaustive process of identifying, validating, and refining the user requirements of the enhanced PSN that the CCEP was expected to deliver.

A consultant was engaged by the NSW Telco Authority in late 2016 to conduct desktop research of potential user requirements for an enhanced PSN, as well as to commence engagement with the ESOs on the high-levels categories of uses that they would want included in the PSN.

An iterative process followed, with the user requirements progressively refined up to a nominally final statement of user agreements being agreed in June 2022. The process of developing these agreed user requirements was informed by:

- the acquired knowledge and expertise of ESOs derived from long-term operational experiences
- lessons from significant events that occurred during the process, such as the 2019–20 bushfire season, and major flood events in 2021 and 2022
- a desire to fully exploit the technical capabilities of the P25 radiocommunications standard.

ESOs submitted more than 900 user requirements for enhanced PSN, and most have been agreed

By June 2022, the ESOs had proposed around 920 user requirements of the enhanced PSN (some of these were matters of definitions or asserting assumptions). Around 33 of these requirements were not accepted by the NSW Telco Authority including:

- requirements by some ESOs for the NSW Telco Authority to record voice calls over the radio network: while ESO-owned and operated voice logging was supported, the NSW Telco Authority was not prepared to accept responsibility for evidential recording and archiving. At least two ESOs were actively opposed to the NSW Telco Authority monitoring or recording the content of their radio calls.
- requirements by some ESOs to have network availability greater than the 99.95% site target determined by the NSW Telco Authority (including, in one case, 'at all times' and, in another case, 99.999%).

We also note that the January 2017 version of the business requirements included a service availability target of 99.99% or greater. It is unclear when and why the decision was made to establish a lower 99.95% target.

Many core ESO functional user requirements are based on Project 25, a widely accepted industry standard

Around 12% of all ESO user requirements for the enhanced PSN related to capabilities that were pre-existing for radio networks using the P25 series of standards for radio communications.

There was a general consensus among ESO stakeholders with whom we spoke that P25 is a known, accepted, and fit-for-purpose standard on which to base the PSN, including because it provides a range of features, capabilities and services required in diverse, mission critical public safety contexts. This is consistent with the experience in the other jurisdictions, such as the US, where investment in a national public safety broadband network is not expected to displace the role of P25-based radio networks for mission critical communication.

Compared to its European equivalent (TETRA), and relevant to the New South Wales context, P25 is considered economical and efficient at providing coverage over large geographic areas while using fewer sites. While the proposed UK Emergency Services Network currently under development is a 4G-based network, we note that it will operate in a much geographically smaller and more densely populated jurisdiction. It is also around seven years overdue and, at 2019, was expected to cost over £9.3 billion[6] (50% over budget).[7]

2.6 Technology

The enhanced PSN is intended to provide a platform to support new and alternative technologies to complement the P25 technology

As discussed above, the former NSW Government determined that the enhanced PSN should be based on the P25 standard for the delivery of a shared, trunked digital radio network for mission critical public safety uses. This is the standard on which the original Government Radio Network had been built, and both the NSW Telco Authority and ESOs could articulate reasons why that technology should remain the foundation for the enhanced PSN.

However, the original timeframe for the enhanced PSN anticipated completion by 2020. Given the substantial extension in timeframes to completion to 2027, it is prudent that the NSW Telco Authority retain a 'watching brief' on whether new or alternative technologies, not anticipated when the CCEP commenced in 2016, become available that may:

- expedite the delivery of the expanded PSN
- provide more cost-effective approaches to design and build or
- provide enhanced capability.

The business cases that have supported the CCEP have expressly recognised that the PSN (as the deliverable of the CCEP) will exist in a wider context in which other technologies exist. For example, the benefits realisation plan for the 2016 CCEP business case defines one of the CCEP program goals as being to:

> …provide agencies and the sector with the technology pathway to next-generation services platform to support agencies' future demand and requirements.

Notably, the October 2020 business case retained this theme, explaining that:

> The final stage of the CCEP is a critical part of the future telecommunications and connectivity infrastructure for the State. It will provide the backbone for the best operational communications technology, such as Public Safety Mobile Broadband (PSMB), to enhance the State's response to emergencies.

[6] Around $A16 billion at 2019 exchange rates.
[7] UK National Audit Office, *Progress delivering the emergency services network,* May 2019.

This approach to alternative technology opportunities was reflected in the NSW Telco Authority's own review of the CCEP in November 2017. In this review, the NSW Telco Authority expressed its intention to conduct a satellite (macro layer) proof of concept, in collaboration with some agencies, for the purpose of testing whether user requirements could be better met by satellite services for infill of some coverage gaps in far west New South Wales. This proposal recognised that this coverage was required by ESOs, notwithstanding the high cost required to build the PSN conventionally in this very large, though comparatively sparsely populated region.

We were advised that this proof of concept did not proceed. However, satellite solutions have been and are used as backup infrastructure for the PSN where no terrestrial option exists (including during the 2019–20 bushfires), though call latency means that the technology has not yet been assessed as meeting the mission critical requirements of the PSN.

The CCEP has explored the possible role of new or alternative technologies for the enhanced PSN

While the NSW Telco Authority did not proceed with its 2017 proposal for a satellite proof of concept, a study was commissioned in 2020 on technologies other than land-based radio. One option considered was full deployment of the P25 based enhanced PSN on the eastern seaboard of New South Wales, and an accelerated development of a public safety LTE (4G/5G mobile) network that would not only provide voice, but also data capability for the rest of the state. The study concluded that this option was not yet viable with current technology.

In mid-2022, after receiving funding from the Digital Restart Fund, the NSW Telco Authority initiated a proof-of-concept project on alternative technologies to land based mission critical radio communications. This included the real-life performance of 4G and 5G mobile, satellite, and emerging technologies in geographies and use cases where there is no commercial network coverage, including during major incidents and natural disasters.

In considering the question of whether the CCEP maintains sufficient visibility over new and alternative technologies, we considered the view of some ESO representatives that the CCEP was not providing sufficient leadership in this area. This was also reflected in customer survey responses to the NSW Telco Authority, where it was found that only 41% of ESO respondents agreed that the NSW Telco Authority plays a 'proactive role in identifying new technologies'.

We found that the NSW Telco Authority has maintained an adequate awareness of the wider technological environment of the enhanced PSN. In making this finding, we drew a distinction between the objectives of the CCEP, and the wider objectives of the NSW Government's Operational Communication Strategy, for which the NSW Telco Authority is the lead agency. While the CCEP is an important part of the strategy, the latter also includes work toward a PSMB network, Regional Digital Connectivity Program, and Mobile Black Spots Program. While the NSW Telco Authority has given adequate attention to new or alternative technologies for the purposes of meeting the objectives of the CCEP, we did not audit how effectively it has delivered the Operational Communications Strategy more broadly.

We note that ESOs have themselves displayed leadership in introducing technologies to build their broader operational communications. The collaborative approach taken across several ESOs in developing the mobile radio assets and Vehicle-as-a-Node capabilities are good examples.

As discussed below, one area where the NSW Telco Authority could do more is by ensuring there is adequate consideration of potential future requirements and capacity when delivering new or refreshed infrastructure.

The NSW Telco Authority has a policy of reserving infrastructure capacity for future PSN or new technology needs, though it is unclear how effectively it has been followed

As discussed earlier, the three business cases for an enhanced PSN each recognised the potential efficiencies in building a network that could absorb new and alternative technologies, such as a future PSMB, as they become available.

To afford some degree of practical future-proofing, the NSW Telco Authority has a documented policy for the reservation of capacity on PSN infrastructure to economically provide for the possible future introduction of new capacity, capabilities, or technologies. The policy, which was made in February 2021, provides that all NSW Telco Authority designs must '…wherever possible and the cost for doing so is negligible' include provision for:

- future PSN expansions
- paging
- public safety LTE 4G/5G (which could include the PSMB network).

These provisions include such things as ensuring excess power capacity, reserving racks for future equipment, prescribing the height and types of towers that should be built, and the configuration and height of antennae.

The intention of this policy is to recognise that it is essential for the NSW Telco Authority to:

> …identify the future technical requirements and expansions and take steps to provision for the future assets so that when the time comes, infrastructure is readily available.

While this policy is in place, we found that the pressure of delivering the PSN meant that these considerations are not always a priority, with primary attention being given to designing and building, as expeditiously as possible, network infrastructure for P25-based equipment to meet immediate agreed specifications.

Balancing these competing pressures poses a challenge for the NSW Telco Authority, particularly when it is recognised that the requirements for new technology are not always known – as one stakeholder noted, 'we don't know what the PSMB will be yet'.

The reservation policy requires that planned reservations would be recorded in a centralised site database that was required to be launched by 2021, though this did not occur. Accordingly, we were unable to determine whether reservations for future needs have been made, and it is unclear how effective this policy will be in achieving its intent.

2.7 Cyber security

The NSW Telco Authority applies reasonable assurance mechanisms regarding cyber security

The NSW Telco Authority is certified against ISO27001,[8] a recognised information security management standard. The scope of this certification specifically includes the '… information security management system supporting the provision of Public Safety Network (PSN) for the use of government agencies and authorities'.

Additionally, as the PSN is also used by some Commonwealth government agencies, the NSW Telco Authority has been subject to independent Infosec Registered Assessors Program (IRAP)[9] assessment against the Commonwealth government's Information Security Manual (ISM). This assessment found that the '…NSW Telco Authority systems, services, and processes are aligned with the December 2021 version of the Australian Government's ISM'. While IRAP assessors can assess cyber security posture to the Commonwealth government's SECRET level, the NSW Telco Authority was assessed to the lower level of PROTECTED.

[8] 'Information technology – Security techniques – Information security management systems – Requirements'

[9] IRAP is run by the Australian Signals Directorate and is intended to support higher standards for security assessments and training. Endorsed IRAP assessors assist in securing systems and Telco Authority by independently assessing cyber security posture, identifying security risks and suggesting mitigation measure.

The NSW Telco Authority told us that the PSN is covered by the Commonwealth's *Critical Infrastructure Security Act 2018*. This creates certain obligations for the NSW Telco Authority regarding the reporting of incidents, as well as to undertake vulnerability management measures consistent with those required by ISO27001, the ISM, or the NSW Government's Cyber Security Policy.

The NSW Government's Cyber Security Policy applies to the NSW Telco Authority by virtue of the mandatory circular DCS-2020-02 NSW Cyber Security Policy. The Managing Director of the NSW Telco Authority has attested that the agency, in their opinion, has '…managed cyber security risks in a manner consistent with the mandatory requirements of the Cyber Security Policy'. We were provided evidence that the NSW Telco Authority engages third parties to conduct monthly security reporting, cyber security audits, regular software patching reporting, and annual penetration testing of its systems.

The NSW Government's Cyber Security Policy mandates that:

> Agencies are responsible under the cyber security Policy for managing cyber security requirements. This includes contract clauses, monitoring and enforcement for 3rd party ICT providers and the ICT security of non-government organisations holding and/or accessing government systems.

The NSW Telco Authority provided evidence that it has included clauses in its vendor contracts requiring cyber security protections. This is important given the key role played by vendors in supporting the delivery of the PSN, including as the network manager.

The potential cloning of unauthenticated radio terminals poses a risk to the security of communications on the enhanced PSN and needs to be addressed as a matter of urgency

During the process of determining user requirements, all ESOs submitted that the enhanced PSN should provide for the authentication of terminals. Authentication is the process of validating the legitimacy of a terminal seeking access to the network and must be manually set up in both the network and the terminal.

Authentication of terminals (including handsets, consoles, and vehicle mounted radios) provides protection against the risk of being 'cloned', in turn:

- preventing unauthorised radios from accessing PSN services
- providing a system alert when an unauthorised radio is denied access
- protecting the integrity of the system to prevent illegal use of cloned or unsupported radios.

This user requirement was agreed by the NSW Telco Authority broadly on the basis that it is already an optional capability for P25-compliant radios. However, the use of this capability requires authentication-capable terminals. The supply of new terminals is not included within the scope of the CCEP, so ESOs and other PSN user agencies must ensure themselves that they have appropriately capable terminals.

The P25 technology on which the PSN is based provides for authentication of terminals. Almost all (98%) handsets registered for the PSN are already technically capable of being authenticated, though only around 48% are currently authenticated. There are currently around 60,000 radios connected to the enhanced PSN, meaning that around 31,200 radios remain to be authenticated. The NSW Telco Authority estimates that it takes around 30 minutes to authenticate a radio.

In April 2022, the NSW Telco Authority endorsed a project brief for a Radio Authentication and Encryption project. The purpose of this project to is enhance PSN network security with a '…two-pronged approach tackling both authentication and encryption'. The project recognises that the measures require effort from both the NSW Telco Authority and the user agencies. The project is intended to:

- uplift adoption of radio authentication to 100% of terminals on the enhanced PSN by 2025
- change core network settings to only accept authenticated terminals.

In the interim, the NSW Telco Authority is exploring strategies to mitigate the risk of cloning through the examination of usage data. Further work is required to ensure that these strategies are effective.

While 98% of existing handsets are already capable of being authenticated, and notwithstanding the risk posed to the PSN by cloning (exacerbated by the publication by radio enthusiasts of user talkgroup identification codes on the internet), the NSW Telco Authority has not expedited the mandatory authentication of terminals. The NSW Telco Authority has also not implemented effective interim risk mitigation strategies for terminals that are not already authenticated (including the small proportion that are not capable of authentication).

The NSW Telco Authority has not settled with ESOs the governance and planning required to ensure that, where required by operational needs, encrypted radio calls can be made between first responders from different agencies

The ability to encrypt calls is an intended benefit of the CCEP. In addition, the 2016 CCEP business case established that specific supplementary benefits, such as greater crime prevention and increased revenue from fines, were dependent on the encryption of some calls across the PSN. Greater privacy of personal information was also considered a societal benefit of the enhanced PSN. The business case also noted that while digital radio networks (such as the PSN when used without encryption) were difficult to monitor, they '…are not truly secure communications, since they are not encrypted'.

As with authentication, encryption is an optional capability in P25-compliant radios that enables secure voice and data communication. All radios within an assigned group (a 'talkgroup' or 'callgroup') can be issued a unique encryption key that allows users to communicate securely within that group. The encryption key allows communications to be encrypted (locked) when sent, and unencrypted (unlocked) when received. Most contemporary P25 terminals can be issued with multiple encryption keys ('multi-key'), meaning that different keys can be used to manage secure communications with different groups of users. Talkgroups can have different levels of encryption depending on the sensitivity of their communications. Encrypted interoperability requires the sharing of encryption keys, and therefore effective coordination and cooperation is required between agencies.

The capability to provide end-to-end encryption was a requested user requirement of the majority of ESOs, though the importance of encryption is likely to vary between ESOs, and between varying operational scenarios. For at least two of the ESOs, NSW Police Force and NSW Ambulance, routine encryption is likely to have high importance. These two ESOs will also be, by far, the largest users of the PSN.

As it is part of the P25 standards, the enhanced PSN will support encryption, though the provision of encryption-capable terminals, including radio handsets, fall outside the scope of the CCEP.

At the same time, a separate intended benefit of the CCEP is to provide '…opportunity for improved interoperability, allowing agencies to communicate within and between agencies and across state borders'. The 2016 CCEP business case noted the Council of Australian Government's National Framework on Improving Government Radiocommunications Interoperability, which was a response to the concern that:

> …agencies responding to emergencies are often hampered by low levels of radiocommunications interoperability to effectively communicate with other agencies within their jurisdiction or other jurisdictions.

This was reinforced in the October 2020 CCEP business case, which established that:

> The final stage will deliver interoperability allowing ESOs, for example the NSW Police Force and NSW Rural Fire Service, to talk to each other and coordinate efforts. It will also deliver interoperability with Queensland, South Australia and Victoria, allowing coordinated responses to critical incidents across borders.

A complexity emerges in that encryption restricts the sharing of voice and data communications between first responders, whereas interoperability requires it. It is not always appropriate to share communications with other agencies, nor is it always necessary to encrypt communications. The extent to which either is necessary will vary according to the operational requirements of the incident or campaign. As the US Cyber Security and Infrastructure Agency has observed in regard to P25 networks:

> Decision-makers should understand that many public safety channels and talkgroups may not require encryption. By determining in the planning stages which talkgroups, radio channels, and types of information should be encrypted, agency and jurisdictional leaders can implement an effective encryption strategy.

Planning and management are required where operational communications requires both encryption and interoperability. As one subject matter expert has expressed it, the decision to implement encrypted and interoperable communications:

> …must be made with the understanding that encryption can add a significant level of complexity and should be considered only when the operational requirements of the incident outweigh the additional complications.

The Federal Partnership for Interoperable Communications in the US, along with other bodies, has done work in developing guidance and good practice for achieving encrypted interoperability. Its work highlights the importance of collaboration and coordination between agencies in establishing technical, policy, and governance arrangements that support encrypted interoperability where appropriate and necessary.[10]

While the NSW Telco Authority's Radio Authentication and Encryption project does not specifically mention the objective of increased interoperability in operational communications between ESOs, it does contain a number of scope inclusions that may provide a foundation for the governance and technical solutions required. These inclusions are:

- uplifting adoption of radio encryption to all talkgroups that deal with sensitive information or citizen data on the enhanced PSN
- delivering an approach to encryption key management approach
- continuous consultation with agencies about their sentiment, reluctance, concerns and identify any barriers to project success.

2.8 Governance and stakeholder relationships

The NSW Telco Authority has established an effective governance structure for the CCEP that collaboratively involves ESOs in decisions about the CCEP

Successful delivery of the enhanced PSN (through the CCEP) critically relies on the NSW Telco Authority partnering with the ESOs to develop agreed user requirements. This includes matters such as coverage equivalence, and technical requirements such as availability (acceptable congestion), capacity, and voice-call quality, and then ensuring the enhanced PSN performs to these agreed standards.

[10] See, Federal Partnership for Interoperable Communications (2016), 'Considerations for Encryption in Public Safety Radio Systems', (2016) 'Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems', (2020) 'Operational best practices for encryption key management'. Also, US National Council of Statewide Interoperability Coordinators (2019). ' Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials', and US Cyber Security and Infrastructure Security Agency (2022) 'Public safety land mobile communications security'.

There are a number of CCEP governance committees (both internal to NSW Telco Authority and those involving the ESOs). At the apex of this governance framework is the CCEP Program Steering Committee, chaired by a Deputy Secretary from the Department of Customer Service, a senior member from each of the five ESOs, and the CCEP Program Director from the NSW Telco Authority. The stated purposes of this committee are to:

- act as the highest decision-making body for the Program (both CCEP and Operation and Maintenance Transformation)
- promote the Program's vision and ensure Program alignment with business and customer objectives
- advise on action required to resolve escalations impacting the Program and its ability to deliver to the agreed scope, schedule and benefits.

The governance mechanisms for the ongoing operation of the enhanced PSN are unclear in how they ensure that ESOs participate in future operational decisions about the network

Once the CCEP is complete, the ESOs will decommission their own radio communication networks and migrate entirely to the PSN, which is operated, managed, and maintained by the NSW Telco Authority. The PSN will transform from being a supplementary source of radio communications, to being the only source of mission critical radio communications for ESOs. The ESOs will depend entirely on the NSW Telco Authority to provide their primary mission critical communications. This greater degree of dependency also heightens the need for transparency, trust, and collaboration between parties for the ongoing operation of the enhanced PSN.

The comprehensive governance arrangements the NSW Telco Authority has put in place for implementation of the CCEP provides a collaborative approach that includes ESO's in making key decisions about the CCEP, as facilitated primarily through the Program Steering Committee.

It will be important that a similar governance mechanism is available to allow ESOs to participate in key operational and service delivery decisions for the enhanced PSN on a permanent basis after the CCEP concludes.

While the NSW Telco Authority demonstrated that it has invested in improving how it collaborates with ESOs for the routine management of the PSN, its own customer survey results indicated that there is scope for improvement.

One option that could satisfy this need is the Operations Service Delivery Governance forum, one purpose of which is to '…facilitate collective governance of the PSN for operational matters, supporting a common purpose in representation of all PSN users'. The intent of this forum appears to be to foster formal engagement with the ESOs on the operation of the enhanced PSN. However, the audit was provided with incomplete terms of reference for this forum, which did not clarify:

- those matters on which ESOs could make decisions
- how decisions would be made, including decisions rules
- what escalation processes are available in the event of dispute
- the standing of any decisions made, including whether decisions of the forum could be overruled.

2.9 Lessons management and record keeping

Lessons from operational experience have informed user requirements

A range of experiences and lessons, including those codified in external inquiries, have informed user requirements, and in turn the design and build of the PSN.

These include:

- the 2016 CCEP business case identified consultation with international and other state governments about their experience on similar projects
- the NSW Telco Authority conducted lessons learned exercises during the formative phases of the CCEP, including the north-west New South Wales pilot and North Coast rollout
- the findings of the Coronial Inquiry into the Lindt Siege (2017), particularly that there had been breakdowns in radio communications in the final stages of the siege
- the NSW Parliament's Legislative Assembly's Inquiry into Violence Against Emergency Services Personnel' (2017), which highlighted the need to provide ambulance paramedics with duress devices, as well as the need to address communications blackspots across New South Wales
- the Bega Valley Fires Independent Review (2018), which recommended using the PSN for the priority roll out of automatic vehicle location tracking for the NSW Rural Fire Service fleet
- lessons workshops were convened by the NSW Telco Authority's Telecommunication Emergency Management Unit following the 2019–22 bushfires.

While the NSW Telco Authority appears to recognise the value of lessons management and applies sound methods consistent with good practice guidance in the field, it is unclear whether this function is formalised, including how lessons derived from operational staff in the PSN are fed back into the design and build function in the CCEP. The governance plan for the CCEP does not reference a lessons management function, allocate responsibly for it, or explain how it links to the elsewhere in the NSW Telco Authority. Similarly, the NSW Telecommunications Services Functional Area Supporting Plan (a supporting plan to the NSW Emergency Management Plan) does not include lessons management process or responsibility.

The NSW Telco Authority has not maintained adequate record keeping for the CCEP

The NSW Telco Authority was unable to provide documents in two instances where key evidence was sought by the audit team. The first related to documents evidencing, how and why paging was excluded from the CCEP scope, and the second was details of a proof of concept for use of satellite communication in western New South Wales alluded to in the NSW Telco Authority's March 2017 program review.

In discussions with NSW Telco Authority personnel, we were advised that there were issues on compliance with the *State Records Act 1998*, and that a program to address these had been put in place. Following from a 2022 Records Management Assessment Tool (RMAT) ratings, the NSW Telco Authority compliance team has been leading a work program around Information Security and Records Management to increase maturity across the business.

3. Costing the enhanced Public Safety Network

The NSW Telco Authority established and tracked its own costs for the CCEP

Over the course of the program from 2016, the NSW Telco Authority prepared a series of business cases and program reviews that estimated its cost of implementing the program in full, including those shown in Exhibit 6 below.

Exhibit 6: Estimated costs to fully implement the CCEP

Source	Capital cost ($ million)	Operating cost ($ million)	Completion date
March 2016 business case	400	37.3	2020
November 2017 internal review	476.7	41.7	2022
March 2020 business case	950–1,050	--	2025
October 2020 business case	1,263.1	56.1	2026

Source: CCEP business cases as identified.

In response to the 2016 CCEP business case, the then NSW Government approved the NSW Telco Authority implementing the CCEP in full, with funding provided in stages. The NSW Telco Authority tracked its costs against approved funding, with monthly reports provided to the multi-agency Program Steering Committee

Throughout the program, the NSW Government was informed of increasing costs being incurred by the NSW Telco Authority for the CCEP

The various business cases, program updates, and program reviews prepared by the NSW Telco Authority were provided to the NSW Government through the required Cabinet process when seeking approval for the program proceeding and requests for both capital and operational funding. These provided clear indication of the changing overall cost of the CCEP to the NSW Telco Authority, as well as the delays that were being experienced.

There was no transparency to the Parliament and community about changes in the capital cost of the CCEP until the 2021–22 NSW Budget

As the business cases for the CCEP were not publicly available, the only sources of information about capital cost were NSW Budget papers and media releases. The information provided in the annual Budget papers prior to the 2021–22 NSW Budget provided no visibility of the estimated full capital cost to complete all stages of the CCEP. As shown in Exhibit 7 below, this information was fragmented and complex.

Media releases about the progress of the CCEP did not provide the estimated total cost to the NSW Telco Authority of $1.325 billion to complete all stages of the CCEP until June 2021. Prior to this date, media releases only provided funding for the initial stages of the program or for the stages subject to a funding announcement.

Even during the September 2019 and March 2020 Parliamentary Estimate Committee hearings where the costings and delays to the CCEP were raised, the estimated full cost of the CCEP was not revealed.

Exhibit 7: CCEP funding in NSW Budget papers from 2015–16 to 2022–23

Financial year	Type of major work	Description of expenditure	Forecast estimate to complete ($ million)	Estimated duration
2015–16	New work	Infrastructure Rationalisation Program: Planning and Pilot	18.3	2015–16
2016–17	Work in progress	CCEP Planning and Pilot	18.3	2015–17
	New work	CCEP	45	2016–17
2017–18	New work	CCEP	190.75	2017–21
2018–19	Work in progress	CCEP North Coast and State-wide Detailed Design	190.75	2017–21
	New work	CCEP Greater Metropolitan Area	236	2018–22
2019–20	Work in progress	CCEP	426.9	2018–22
2020–21	Work in progress	CCEP	664.8	2018–22
2021–22	Work in progress	CCEP	1,325	2018–26
2022–23	Work in progress	CCEP	1,292.8	2018–26

Source: NSW Treasury, Annual State Budget Papers.

The original business case for the CCEP included estimated ESO costs, though these costs were not tracked throughout the program

Estimates for ESO costs for operating and maintaining their own radio networks over the four years from 2016–17 were included in the original March 2016 business case. They included $75.2 million for capital expenditure and $95 million for one-off operating costs. These costs, as well as costs incurred by ESOs due to the delay in the program, were not subsequently tracked by the NSW Telco Authority.

In January 2017, Infrastructure NSW reviewed the CCEP business case of March 2016. In this review, Infrastructure NSW recommended that the NSW Telco Authority identify combined and apportioned costs and cashflow for all ESOs over the CCEP funding period reflecting all associated costs to deliver the CCEP. These to include additional incidental capital costs accruing to ESOs, transition and migration to the new network and the cost (capital and operational) of maintaining existing networks. This recommendation was implemented in the November 2017 program review, with ESO capital costs estimated as $183 million.

In 2019, Infrastructure NSW conducted a Deep Dive Review on the progress of the CCEP. In this review, Infrastructure NSW made what it described as a 'critical recommendation' that the NSW Telco Authority:

> …coordinate a stocktake of the costs of operational bridging solutions implemented by PSAs [ESOs] as a result of the 18-month delay, so that a whole-of-government cost impact is available to the NSW Government.

It should be noted that the delay to CCEP completion now is seven years and that further ‘operational bridging solutions’ have been needed by the ESOs.

'Stay Safe and Keep Operational' costs incurred by ESOs will be significantly higher than originally estimated

Stay Safe and Keep Operational (SSKO) funding was established to provide funding to ESOs to maintain their legacy networks while the CCEP was refreshing and enhancing the PSN. This recognised that much of the network infrastructure relied on by ESOs had reached – or was reaching – obsolescence and would either require extensive maintenance or replacement before the PSN was available for ESOs to migrate to it. ESOs may apply to NSW Treasury for SSKO funding, with their specific proposals being reviewed (and endorsed, where appropriate) by the NSW Telco Authority. Accordingly, SSKO expenditure does not fall within the CCEP budget allocation.

As shown in the table below, extracted from the March 2016 CCEP business case, the total expected cost for SSKO purposes over the course of the CCEP was originally $40 million, assuming the enhanced PSN would be fully available by 2020.

Exhibit 8: Stay Safe and Keep Operational forecast costs, 2017 to 2020

Year	2017	2018	2019	2020	Total
SSKO forecast ($ million)	12.5	15	10	2.5	40

Source: March 2016 CCEP business case.

In October 2022, the expected completion date for the CCEP was re-baselined to August 2027. Accordingly, ESOs will be required to continue to maintain their radio networks using legacy equipment for seven years longer than the original 2020 forecast. This will likely become progressively more expensive and require additional SSKO funding. For example, NSW Telco Authority endorsed SSKO bids for 2022–23 exceeded $35 million for that year alone.

Compared to the original forecast made in the March 2016 CCEP business case of $40 million, we found ESOs had estimated SSKO spending to 2027 will be $292.5 million.

A refresh of paging network used by ESOs and the decommissioning of redundant sites were both removed from the original 2016 scope of the CCEP

Paging

A paging network is considered an important user requirement by the Fire and Rescue NSW, NSW Rural Fire Service, and NSW State Emergency Service. The 2016 CCEP business case included a paging network refresh within the program scope of works. This was reiterated in the November 2017 internal review of the program. These documents did not estimate a cost for this refresh. The March 2020 and October 2020 business cases excluded paging from the program scope. The audit is unable to identify when, why or by whom the decision was made to remove paging from the program scope, something that was also not well communicated to the affected ESOs.

In 2021, after representations from the affected ESOs, the NSW Telco Authority prepared a separate business case for a refresh of the paging network at an estimated capital cost of $60.31 million. This program was subsequently approved by the NSW Government and included in the 2022–23 NSW Budget.

In determining an estimated full whole-of-government cost of delivering the enhanced PSN, we have included the budgeted cost of the paging network refresh on the basis that:

- it was expressly included in the original approved March 2016 business case
- the capability is deemed essential to the needs of three ESOs.

Decommissioning costs

The 2016 CCEP business case included cost estimates for decommissioning surplus sites (whether 'old' GRN sites or sites belonging to ESOs' own networks). These estimates were provided for both the NSW Telco Authority ($38 million) and for the ESOs ($55 million). However, while these estimates were described, they were not included as part of the NSW Telco Authority's estimated capital cost ($400 million) or (more relevantly) operating cost ($37.3 million) for the CCEP. This is despite decommissioning being included as one of eight planned activities for the rollout of the program.

In the October 2020 business case, an estimate of $201 million was included for decommissioning agency networks based on a model whereby:

- funding would be coordinated by the NSW Telco Authority
- scheduling and reporting through an inter-agency working group and
- where appropriate, agencies would be appointed as the most appropriate decommissioning party.

This estimated cost is not included in the CCEP budget.

In determining an estimated full whole-of-government cost of the enhanced PSN, we have included the estimated cost of decommissioning on the basis that:

- decommissioning was included in the 2016 CCEP business case as one of eight 'planned activities for the rollout of the program'
- effective decommissioning of surplus sites and equipment (including as described in the business case as incorporating asset decommissioning, asset re-use, and site make-good) is an inherent part of the program management for an enhanced PSN
- costs incurred in decommissioning are entirely a consequence of the CCEP program.

The estimated minimum cost of building an enhanced PSN consistent with the original proposal is over $2 billion

We have derived two estimated minimum whole-of-government costs for delivering an enhanced PSN. These are:

- $2.04 billion when calculated from NSW Telco Authority data – shown as estimate A in Exhibit 9 below.
- $2.26 billion when calculated from ESO supplied data – shown as estimate B in Exhibit 9.

Both totals include:

- budgeted amounts for both CCEP capital expenditure ($1,292.8 million) and operating expenditure ($139 million)
- the NSW Telco Authority's 2020 estimated cost for decommissioning ($201 million)
- the NSW Telco Authority's approved funding for paging refresh ($60.3 million).

The two estimated totals primarily vary around the capital expenditure of ESOs (particularly SSKO funding). To determine these costs, we used ESO provided actual SSKO costs to date, as well as their estimates for maintaining their legacy radio networks through to 2027.

The equivalent cost estimates from the NSW Telco Authority were sourced from the November 2017 internal review and the October 2020 business case for CCEP. It should be noted that the amounts for both estimates are not audited, or verified, but do provide an indication of how whole-of-government costs have grown over the course of the program.

The increase in and reasons for the increase in total CCEP costs (capital and one-off operating) incurred or forecast by the NSW Telco Authority (from $437.3 million in 2016 to $1,431.8 million in 2022) have been provided to the NSW Government through various business cases and reviews prepared by the NSW Telco Authority, as well as by reviews conducted by Infrastructure NSW as part of its project assurance responsibilities.

However, the growth in ESO costs and other consequential costs, such as paging and decommissioning, from around $263 million in the 2016 CCEP business case to between $600 million and $800 million, has to a large degree remained invisible and unexplained to the NSW Government and other stakeholders.

Exhibit 9: Estimated whole-of-government costs of the enhanced PSN

	Estimated whole-of-government cost, over time				
Cost type	**2016[1]**	**2017[2]**	**2020[3]**	**2023 - Estimate A[4]**	**2023 - Estimate B[5]**
	$ million	**$ million**	**$ million**	**$ million**	**$ million**
CCEP capital expenditure	400[a]	476.7[b]	1,263.1[c]	1,292.8[d]	1,292.8[d]
CCEP operating expenditure	37.3[a]	41.7[b]	41.5[e]	139[d]	139[d]
CCEP total	**437.3**	**518.4**	**1,304.6**	**1,431.8**	**1,431.8**
ESO capital expenditure	75.2[a,f]	183[b,e]	75.4[e]	258.4[g]	292.5
ESO one-off operating expenditure	93[a]	n.a.[l]	86.5[e]	86.5[h]	273
ESO total	**168.2**	**183**	**161.9**	**344.9**	**565.5**
Paging	n.a.[i]	n.a.[i]	n.a.[j]	60.3[k]	60.3[k]
Decommissioning	93	n.a.[l]	201.0	201[h]	201
Paging and decommissioning total	**93**	**n.a.**	**201**	**261.3**	**261.3**
Whole-of-government total	**698.5**	**701.4**	**1,667.5**	**2,038**	**2,258.6**

Notes:

a Financial year 2016 to Financial year 2020.

b Financial year 2016 to Financial year 2021.

c Financial year 2016 to Financial year 2025.

d Financial year 2016 to Financial year 2026.

e Financial year 2022 to Financial year 2025.

f Stay Safe and Keep Operational (SSKO) costs plus terminals costs.

g November 2017 internal review and October 2020 Business case.

h October 2020 Business case.

i Included in CCEP capital expenditure at that time.

j By 2020, a refresh of the paging network had been removed from the CCEP scope.

k A separate business case for a refresh of the paging network was approved by government in 2022.

l Figure not included in the source document.

Sources:

1 March 2016 CCEP business case.

2 November 2017 Internal Review conducted by the NSW Telco Authority.

3 October 2020 CCEP business case.

4 Derived from business cases, with ESO costs drawn from NSW Telco Authority data.

5 Derived from business cases, with ESO costs based on data provided to the Audit Office of New South Wales by each of the five ESOs.

Section two

Appendices

Appendix one – Response from agency

Department of Customer Service
Office of the Secretary

NSW GOVERNMENT

Our reference: COR-01873-2023
Your reference: 02307737

Ms Margaret Crawford
Auditor General of New South Wales
NSW Audit Office

Dear Ms Crawford,

Thank you for your letter conveying the Performance Audit – "Management of the Critical Communications Enhancement Program (CCEP)" report.

The report accurately details that:

(i) The NSW Telco Authority is delivering a radio network that meets the needs of Emergency Service Organisations (ESO's) and will exceed any radio coverage previously available to ESO's, and
(ii) More work is needed to review governance mechanisms, expedite device authentication and address the policy gap for in-building coverage in new and existing buildings post program completion.

NSWTA accepts all recommendations and is pleased to confirm that work has commenced against each. Comments against each recommendation are provided below:

The NSW Telco Authority should (in consultation with the Emergency Service Organisations):

1. **by October 2023, finalise its PSN Traffic Mitigation Plan and determine a schedule and method by which that plan will be tested.**
   The NSW Telco Authority in collaboration with ESOs have drafted the plan. Testing and finalisation of the plan is on track for completion October 2023.

2. **by December 2023, review whether current or planned governance arrangements for the enhanced PSN are adequate and appropriate for the evolving relationship between agencies, include to support ongoing collaboration and communication**
   The NSW Telco Authority maintains strong relationships with customers through a range of forums, including the State Emergency Management Committee and with representation by Emergency Service Organisation on the NSW Telco Authority advisory board. A review of the current engagements will be undertaken, with a particular focus on operational forums. Specifically, the NSW Telco Authority will, in consultation with Emergency Service Organisations, review the terms of reference for the Operational Service Delivery Governance forum by December 2023.

3. **by January 2024, work with other relevant NSW government agencies to provide advice to the NSW Government on the options, benefits and costs of addressing the regulatory gap for in-building public safety communications coverage in new and existing buildings**
   NSWTA is working with relevant NSW government agencies in developing and implementing Minimum Digital Connectivity Principles, which will promote the requirements for in building

McKell Building
2-24 Rawson Place, Sydney NSW 2000

Tel 02 9372 8877
TTY 1300 301 181

ABN 81 913 830 179
nsw.gov.au

coverage in new and significantly refurbished major infrastructure being funded by the NSW government. The principles are planned to be implemented as part of a first phase by January 2024 via an NSW Government Administrative Requirement.

4. **by March 2024, consider what, if any, technical and governance arrangements are required for circumstances where operational communications requires both encryption and interoperability**
   Interoperability is currently delivered through the allocation of unencrypted shared talk groups (which allow ESO's to communicate with each other), and General Liason channels (which allow all PSN users to communicate with each other). Interstate interoperability is also delivered today through connection of two network cores, eg: QLD and NSW networks.
   The 'Radio Authentication and Encryption project' being led by the NSW Telco Authority is looking to overcome the encryption and interoperability challenge. This program will determine the technical and governance arrangements required for improved network encryption and identify those use cases that require both encryption and interoperability.

The NSW Telco Authority should:

5. **ensure that it complies with its Infrastructure Capacity Reservation Policy**
   Through the delivery of the CCEP, NSWTA will address the infrastructure capacity reservation policy. This includes improved capture of information relating to reservations.

6. **expedite the mitigation of the risk of cloning of unauthenticated terminals:**

   a. **by October 2023, implement interim strategies to identify and address the risk of cloned terminals**
      This risk is known to ESOs and currently mitigated through operational process. The NSW Telco Authority has commenced work to address issues relating to cloned terminals and will have a plan in place from October 2023.

   b. **by June 2024, require that authentication-capable terminals be authenticated**
      In progress as part of the current 'Radio Authentication and Encryption project.'

   c. **by June 2025, require all terminals using the enhanced PSN be authenticated.**
      In progress as part of the current 'Radio Authentication and Encryption project.'

I would like to thank your staff for their time and professionalism during the audit.

Sincerely,

Emma Hogan
Secretary

McKell Building
2-24 Rawson Place, Sydney NSW 2000

Tel 02 9372 8877
TTY 1300 301 181

ABN 81 913 830 179
nsw.gov.au

Appendix two – Trunked public safety radio networks

Trunked public safety radio networks

Unlike conventional radio networks, the enhanced Public Safety Network is a 'trunked' radio network. Instead of having defined channels for different users, trunked radio networks have defined groups of users that are automatically allocated to any channel that is available at the time a user wants to transmit a call.

Managing talkgroups

Most radio calls made on a trunked radio network are between the members of a pre-defined group of radio users. These are called talkgroups or callgroups.

Talkgroups typically comprise users who perform certain functions (for example, ‘Operations’, ‘Emergency Response’, ‘Fleet’, ‘Training’ etc), are in the same geographic area (‘Metro East’, ‘Central Coast’ etc). These can also be combined: such as, ‘Metro East – Operations’.

Each time a user in a talkgroup keys their radio (presses a button) to speak, the following process happens:

- the radio will send a data message over a dedicated ‘control channel’ asking the computerised network controller to find and allocate a channel for the call
- the network controller will search for an available channel from the pool of channels
- if the network controller finds an available channel, it allocates that channel to the requesting radio
- the network controller then switches each radio in that talkgroup to that channel
- the talkgroup is then established on a channel for the call to be transmitted by the user who initially keyed their radio.

When the initiating user commences talking, all members of the talkgroup will hear the transmission and that channel cannot be used by another user for the duration of the call.

The process of requesting, allocating, and switching all radios to an allocated channel happens instantaneously to ensure that operational communications achieve mission-critical performance.

When the initiating user releases their talk button, the channel is also released immediately (or within a few seconds)[11] back into the pool of available channels. The process would then repeat if another member of the talkgroup replies, hence the talkgroup can change channels every time a microphone is keyed.

Accordingly, a trunked radio network removes the need for a user to find an available channel, relieving the user of a task that can become complex and confusing if the network is congested.

Managing channels

In addition to removing the burden on the user, a trunked radio network increases how efficiently channels are used.

Under a conventional radio network, channels are usually reserved for specific purposes, and therefore may remain underused during times when other channels are experiencing congestion. In contrast, in a trunked radio network each requested call is allocated to the next available channel and therefore channels are not left idle when other parts of the network are busy.

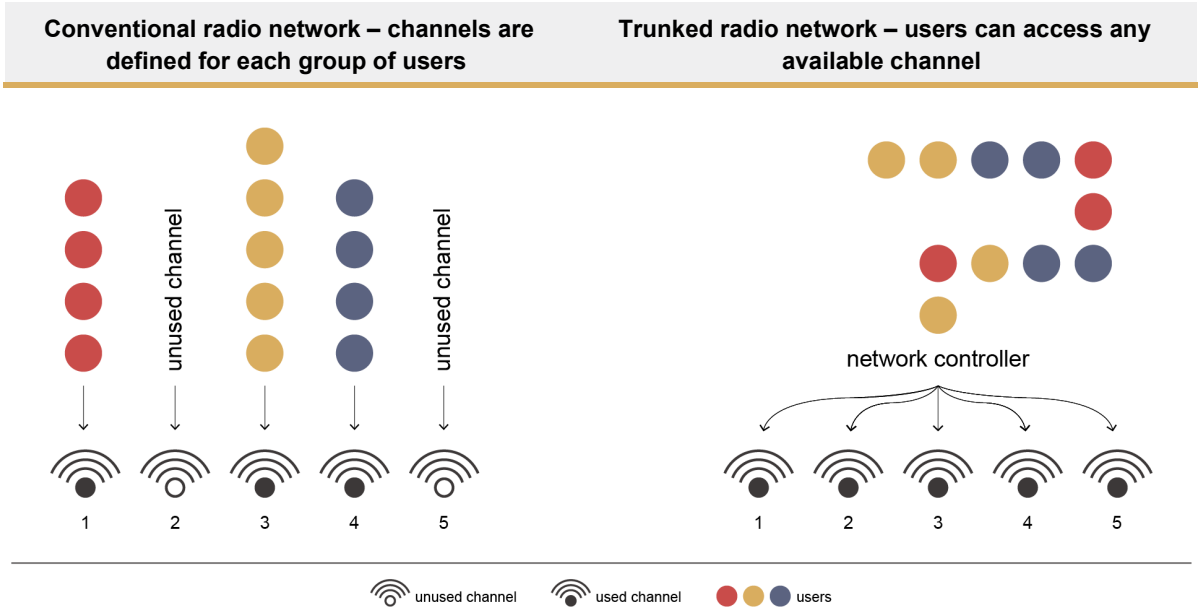
[11] In some circumstances, the channel may be reserved for a few seconds to provide for an immediate reply from another member of the talkgroup.

This benefit of trunked radio networks is usually described with reference to queue theory. Instead of individual users being confined to the pace of an individual queue, users in the queue have access to the next available channel - much like a queuing for an airline check-in.

Exhibit 10 below illustrates how the management of channels differs between conventional and trunked radio networks. In the first illustration, each group of users has a dedicated channel for their communications. At different times, some channels will approach or even exceed their call capacity, while other channels may have unused capacity. This can result in some channels becoming congested, while others are underused. This is an inefficient use of the channels.

In the second illustration below, because calls are allocated to the next available channel, no channels are left underused during busy times. By maximising the use of all channels and allowing for more calls to be made, trunked radio networks are more efficient than conventional radio networks when there are a large number of users.

Exhibit 10: Simple illustration of conventional versus trunked radio network



Reference: Audit Office of New South Wales based on: Cast, C. (2018) 'Radio communications' presentation to Marjory Stoneman Douglas High School Public Safety Commission; Mississippi Emergency Management Agency (2018) 'Unit 5: Frequency Regulations and Usage'; Stephan, K.D. (2006) 'We've got to talk; Emergency communication and engineering ethics' in IEEE Technology and Society Magazine, July.

Other types of calls available on a trunked radio network

While the majority of calls made on a trunked public safety radio network are usually within one or more talkgroups, P25 digital technology, as used for the Public Safety Network, allows for other forms of communication, including (subject to the capabilities of the terminal being used):

- system messages, whereby the system administrator communicates to all users
- duress calls, where a user in distress or in need of urgent assistance can press a button on the radio to allow priority alerts to the network – this can also activate location tracking and open a 'hot mic' whereby the user's microphone is turned on without any action from them
- user-to-user messaging, including where the radios are outside coverage of the network and are effectively communicating directly on a line-of-sight basis as 'walkie talkies'
- roaming voice calls on 4G or satellite when the user is outside of radio network coverage
- calls to mobile phone numbers over the trunked radio network when outside mobile coverage.

Appendix three – About the audit

Audit objective

This audit assessed whether the Critical Communications Enhancement Program (CCEP) to enhance the Public Safety Network (PSN) is being effectively implemented by the NSW Telco Authority.

Audit scope and focus

We addressed the audit objective by answering the following two questions:

1. Have user requirements, as per the agreed Statement of Requirements for the CCEP between NSW Telco Authority and emergency service organisations of NSW Police Force, NSW Ambulance, Fire and Rescue NSW, NSW Rural Fire Service, and the NSW State Emergency Service (ESOs), been met under day-to-day and emergency operational conditions?
2. Has there been adequate transparency to the NSW Government and other stakeholders regarding whole-of-government costs related to the CCEP?

Audit criteria

In answering the above questions, we used the following criteria:

1.
    a) The enhanced PSN has met the agreed requirements of emergency services organisations during their routine operations.
    b) The enhanced PSN has met the agreed requirements of emergency services organisations during emergency operations, including natural disasters.
    c) The agreed user requirements take into account any relevant laws, policies, standards, or operational lessons.
2.
    d) The full cost of the CCEP to the NSW Government has been established and is regularly updated.
    e) There has been adequate transparency to the NSW Government and other stakeholders about the full cost of the CCEP.

Audit exclusions

The audit did not:

- assess the value-for-money of the costs incurred as reported by the NSW Telco Authority or by the ESOs
- assess the NSW Telco Authority response to the findings and recommendations in the Infrastructure NSW assurance reports
- assess the performance of the PSN to standards greater than the agreed Statement of Requirements except where the Statement of Requirements does not take into account relevant laws, policies, standards or operational lessons
- examine the costs incurred by organisations other than ESOs as users of the PSN (such as local councils)
- question the merits of NSW Government policy objectives.

However, we commented on these issues where they affect our findings or to provide context.

Audit approach

Our procedures included:

- interviewing key personnel from the NSW Telco Authority associated with the implementation of the CCEP, particularly in relation to costs, scope and operation of the PSN
- consultation with ESOs particularly in relation to their costs and CCEP scope and performance of the PSN
- fieldwork on site with selected ESOs to better understand how the PSN under CCEP is meant to work and how it is performing
- examining documentation relating to decisions made by the NSW Telco Authority regarding implementation of the CCEP.

We also examined documentation from other stakeholders obtained throughout the audit, such as Infrastructure NSW.

The audit approach minimised overlap and duplication of the assurance work already performed by Infrastructure NSW on the CCEP implementation. It will draw on the experiences of ESOs in using the PSN in actual emergency management and incident response, including whether those experiences have been taken into account in subsequent design and implementation decisions.

The audit approach was complemented by quality assurance processes within the Audit Office to ensure compliance with professional standards.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standard ASAE 3500 Performance Engagements and other professional standards. The standards require the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. Our processes have also been designed to comply with requirements specified in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

Acknowledgements

We gratefully acknowledge the cooperation and assistance provided by staff of the NSW Telco Authority and the Emergency Services Organisations: NSW Police Force, NSW Ambulance, Fire and Rescue NSW, NSW Rural Fire Service, and the NSW State Emergency Service.

Audit cost

The total cost of this audit is estimated at $480,000.

Appendix four – Performance auditing

What are performance audits?

Performance audits assess whether the activities of State or local government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws.

The activities examined by a performance audit may include a government program, all or part of an audited entity, or more than one entity. They can also consider particular issues which affect the whole public sector and/or the whole local government sector. They cannot question the merits of government policy objectives.

The Auditor-General's mandate to undertake audits is set out in the *Government Sector Audit Act 1983* for state government entities, and in the *Local Government Act 1993* for local government entities. This mandate includes audit of non-government sector entities where these entities have received money or other resources, (whether directly or indirectly) from or on behalf of a government entity for a particular purpose (follow-the-dollar).

Why do we conduct performance audits?

Performance audits provide independent assurance to the NSW Parliament and the public.

Through their recommendations, performance audits seek to improve the value for money the community receives from government services.

Performance audits are selected at the discretion of the Auditor-General who seeks input from parliamentarians, State and local government entities, other interested stakeholders and Audit Office research.

How are performance audits selected?

When selecting and scoping topics, we aim to choose topics that reflect the interests of parliament in holding the government to account. Performance audits are selected at the discretion of the Auditor-General based on our own research, suggestions from the public, and consultation with parliamentarians, agency heads and key government stakeholders. Our three-year performance audit program is published on the website and is reviewed annually to ensure it continues to address significant issues of interest to parliament, aligns with government priorities, and reflects contemporary thinking on public sector management. Our program is sufficiently flexible to allow us to respond readily to any emerging issues.

What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing.

During the planning phase, the audit team develops an understanding of the audit topic and responsible entities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the audited entity, program or activities are assessed. Criteria may be based on relevant legislation, internal policies and procedures, industry standards, best practice, government targets, benchmarks or published guidelines.

During the fieldwork phase, audit teams will require access to books, records, or any documentation that are deemed necessary in the conduct of the audit, including confidential information which is either Cabinet information within the meaning of the *Government Information (Public Access) Act 2009*, or information that could be subject to a claim of privilege by the State or a public official in a court of law. Confidential information will not be disclosed, unless authorised by the Auditor-General.

At the completion of fieldwork, the audit team meets with management representatives to discuss all significant matters arising out of the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with management representatives to check that facts presented in the draft report are accurate and to seek input in developing practical recommendations on areas of improvement.

A final report is then provided to the accountable authority of the audited entity(ies) who will be invited to formally respond to the report. If the audit includes a follow-the-dollar component, the final report will also be provided to the governing body of the relevant entity. The report presented to the NSW Parliament includes any response from the accountable authority of the audited entity. The relevant Minister and the Treasurer are also provided with a copy of the final report for State Government entities. For local government entities, the Secretary of the Department of Planning and Environment, the Minister for Local Government and other responsible Ministers will also be provided with a copy of the report. In performance audits that involve multiple entities, there may be responses from more than one audited entity or from a nominated coordinating entity.

Who checks to see if recommendations have been implemented?

After the report is presented to the NSW Parliament, it is usual for the entity's Audit and Risk Committee / Audit Risk and Improvement Committee to monitor progress with the implementation of recommendations.

In addition, it is the practice of NSW Parliament's Public Accounts Committee to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report received by the NSW Parliament. These reports are available on the NSW Parliament website.

Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian standards.

The Public Accounts Committee appoints an independent reviewer to report on compliance with auditing practices and standards every four years. The reviewer's report is presented to the NSW Parliament and available on its website.

Periodic peer reviews by other Audit Offices test our activities against relevant standards and better practice.

Each audit is subject to internal review prior to its release.

Who pays for performance audits?

No fee is charged to entities for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in-progress, please see our website www.audit.nsw.gov.au or contact us on 9275 7100.

Professional people with purpose

OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

OUR PURPOSE

To help Parliament hold government accountable for its use of public resources.

OUR VALUES

Pride in purpose

Curious and open-minded

Valuing people

Contagious integrity

Courage (even when it's uncomfortable)

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

Level 19, Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000 Australia

PHONE +61 2 9275 7100

mail@audit.nsw.gov.au

Office hours: 8.30am-5.00pm
Monday to Friday.

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au