NSW Telco Authority

Response to Supplementary Questions

LEGISLATIVE ASSEMBLY
Public Accounts Committee
Hearing date: 25 March 2024

Accountability measures for decision-making for the delivery of major infrastructure, contracting of public services and/or the privatisation of public assets in NSW (Critical Communications Enhancement Program).

Agency contacts

[redacted]

Kylie De Courteney
Managing Director
NSW Telco Authority
[redacted]

Kirsty McKinnon
Executive Director, Program Delivery
NSW Telco Authority
[redacted]

The following supplementary questions were received by the Public Accounts Committee via email on Tuesday 9 April 2024. They include references to the recommendations contained in the NSW Auditor-General's report to Parliament titled 'Management of the Critical Communications Enhancement Program'.

Recommendation 1: The NSW Telco Authority should (in consultation with the Emergency Services Organisations) by October 2023, finalise its Public Safety Network (PSN) Traffic Mitigation Plan (TMP) and determine a schedule and method by which that plan will be tested.

1. When was the Public Safety Network Traffic Management Plan finalised by the NSW Telco Authority and signed off on by all five emergency service organisations?

Answer:
The Traffic Mitigation Plan was finalised in October 2023 with all five Emergency Services Organisations signing off the document by April 2024.

The Traffic Mitigation Plan defines the controls and protocols used to manage potential congestion on the Public Safety Network by modifying the priority, or restricting the permissions, of some customers at selected sites when the automated system for traffic prioritisation is unable to meet demand or a dynamic shift in traffic priorities occurs.

2. What is the schedule and method by which the PSN TMP will be tested?

Answer:
The Traffic Mitigation Plan is subject to a full review every three years by the Service Delivery Governance Forum. The recently signed off Traffic Mitigation Plan will be embedded in the network operations annual exercise schedule currently under review.

Recommendation 2: The NSW Telco Authority should (in consultation with the Emergency Services Organisations) 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. What work has the NSW Telco Authority done to review whether current or planned governance arrangements for the enhanced PSN are adequate for the evolving relationship between agencies, including to support ongoing collaboration and communication?

Answer
A new Service Delivery Governance forum was established in December 2022 to facilitate direct engagement and consultation with Emergency Services Organisations at an operational level through a governed platform.

The Forum's purpose is to ensure sustainable and scalable critical communications operations in a shared environment are delivered, maintained and continually improved to meet the service needs of Public Safety Network Customers.

The Forum's service delivery charter (Terms of Reference) was developed in collaboration with Emergency Services Organisations (including executive endorsement).

Additional strategic engagement forums (separate to the Service Delivery Governance Forum) are in place including:

- Customer Account Management meetings (monthly)
- Executive Customer Forum (quarterly)
- Stay Safe Keep Operational Business Development Forum (bi-annually)

4. As noted in 'Appendix one – Response from agency' in 'Management of the Critical Communications Enhancement Program', what is the status of the NSW Telco Authority's review of current engagements, particularly on operational forums? Please outline:

a. the scope of the review
b. who performed the review
c. how the results were reported
d. when the review was completed
e. the results of the review, and
f. how the NSW Telco Authority has applied these results.

Answer:
A Department of Customer Service audit of client relationships and customer management for NSW Telco Authority was completed in May 2023. Although the Critical Communications Enhancement Program performance audit was not released until 23 June 2023, the timing of the customer audit was used to satisfy the recommendation

The audit was undertaken by the Department's cluster-wide Internal Audit Unit and its objective was to assess whether adequate agreements were in place specifying client relationship management, communication strategies, service delivery expectations, performance standards, Key Performance Indicators, client reporting, confidentiality, intellectual property and feedback.

The review scope covered the following areas:

- Policies, procedures, roles and responsibilities – Reviewed relevant strategies, including policies and procedures, being applied by the Authority to ensure they were adequate and properly implemented, maintained and updated.

- Customer Engagement – Assessed the controls and processes surrounding the administration of agreements and contracts, including customer management plans, ongoing communication protocols, customer governance (including meeting cadence) and monitoring of Service Level Agreements.

- Performance Reporting – Reviewed the effectiveness of performance and measurement mechanisms including performance monitoring, such as KPIs and individual customer and aggregated reporting against the key elements of customer agreements.

- Records Management – Ensured management of customer information, including collecting, securely storing and managing a database of customer information, was adequate to keep this information protected and confidential.

The review covered the period from 1 July 2022 to 15 March 2023.

The review verified that appropriate processes were in place to manage intellectual property rights, such as maintaining agreements, contracts and records.

The review identified that key controls were effective in mitigating key risks affecting the following scope items:

- Policies and Procedures and Roles and Responsibilities
- Customer Engagement (Satisfaction)
- Customer Engagement (Response)
- Performance Reporting (Customer Relationships)
- Performance Reporting (Achievement of Objectives)

- Records Management (Intellectual Property (IP))
- Records Management (Data Management)

In addition, the audit team noted that to mitigate risks Account Management Plans are being finalised for Emergency Services Organisations to ensure customer satisfaction and adequate communication between NSW Telco Authority and its customers.

The review identified the following issues which are being addressed:

- Service Agreements stored in the Customer Relationship Management system are not current (Medium)
- Customer communication is not always passed to the Customer Management Team (Medium)
- Service Agreements and Account Management Plans do not include KPI's

NOTE: This was a confidential internal departmental review and was not published in the public domain.

5. The NSW Telco Authority's submission outlined several governance forums. Of these, which will continue once the Critical Communications Enhancement Program (CCEP) concludes?

Answer:
The following governance forums will continue post the Critical Communications Enhancement Program rollout:

Governance Forums	Responsibility
NSW Department of Customer Service Audit & Risk Committee NSW Audit Office	- Tracks progress against key indicators to ensure the program is being effectively delivered - Assesses performance against time, budget and NSW Government's objectives
Infrastructure NSW (INSW)	- Half yearly "Health Checks" as part of Treasury Assurance Framework - High Profile High Risk – additional governance
NSW Government Telecommunications Authority Advisory Board	- Tracks progress against key indicators to ensure the program is being effectively delivered - Assesses performance against time and budget

Recommendation 3: The NSW Telco Authority should (in consultation with the Emergency Services Organisations) 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.

6. What work has been done to ensure that following the end of the CCEP the NSW Government has sufficient advice on the options, benefits and costs of addressing the regulatory gap for in-building public safety communications coverage in new and significantly refurbished buildings and infrastructure, particularly for private sector construction?

Answer
NSW Telco Authority developed the Digital Connectivity Principles Policy which establishes obligations to ensure that all new NSW Government-funded infrastructure, including major upgrade and renewal projects, include up-front consideration, planning and funding for the appropriate digital connectivity infrastructure to meet customers' needs now and into the future.

The Digital Connectivity Principles became effective on 1 March 2024 and apply to all new NSW Government funded infrastructure worth over $10 million.

The five principles aim to ensure government-funded infrastructure is built with the necessary connectivity infrastructure at the outset. This means major infrastructure projects such as hospitals, schools, office buildings, railway stations and tunnels will be built with supporting digital plumbing as 'pipes and pits', conduit, risers and fibre to support digital connectivity.

Principle two ensures the Public Safety Network is available in critical locations, being areas of mass congregation or critical infrastructure. Public Safety Network In-Building Coverage systems may be necessary where macro coverage is insufficient.

In implementing this principle, NSW Telco Authority has developed guidance materials and tools to help builders of infrastructure in meeting their obligations with respect to in-building coverage for public safety communications.

The implementation of the principles is the first step in addressing in-building coverage via a regulatory response. Further work is underway to explore whether the Principles should be applied more broadly to other sectors, including private sector construction and, if so, whether a regulatory intervention is warranted.

7. As noted in 'Appendix one – Response from agency' in 'Management of the Critical Communications Enhancement Program', NSW Telco Authority is working with relevant NSW government agencies in developing and implementing Minimum Digital Connectivity Principles. What is the status of this work and have these principles been finalised?

Answer
The Digital Connectivity Principles are finalised. Please refer to the response to question 6.

8. If finalised, how and who monitors and enforces government agencies compliance with the Minimum Digital Connectivity Principles?

Answer
A Department of Customer Service circular (DCS-2024-01) establishes the mandatory requirement for all new NSW government-funded infrastructure, major upgrades and renewal projects subject to a Business Case to apply the Digital Connectivity Principles Policy in planning, design and construction.

This will ensure that the digital connectivity services needed by customers are identified and the relevant digital connectivity infrastructure requirements are funded and delivered.

NSW Telco Authority is engaging across government to build awareness of the Digital Connectivity Principles, so they are nested into infrastructure planning and budgeting processes moving forward.

9. If finalised, has the effectiveness of the Minimum Digital Connectivity Principles been reviewed or when is a review scheduled to occur?

Answer:
An evaluation plan for the Digital Connectivity Principles is in development and is expected to be completed by December 2024.

The evaluation plan will outline a review process which will be informed by further consultation and by factors such as the outcome of Treasury's current Business Case Guidelines Review, for which the consultation paper referred to the potential of digital connectivity being introduced as a mandatory element in business cases.

Although the Digital Connectivity Principles came into effect on 1 March 2024, they only mandatorily apply to infrastructure funded after this date. The effectiveness of the Digital Connectivity Principles may only be assessed once these projects commence.

Recommendation 4: The NSW Telco Authority should (in consultation with the Emergency Services Organisations) by March 2024, consider what, if any, technical and governance arrangements are required for circumstances where operational communications requires both encryption and interoperability.

10. As noted in 'Appendix one - Response from agency' in 'Management of the Critical Communications Enhancement Program' the NSW Telco Authority is leading a 'Radio Authentication and Encryption project'. What technical and governance arrangements has the project identified as required for improved network encryption?

Answer:
Encryption is not mandatory and is the choice of the customer. Encryption is recommended for Public Safety Network users to convey sensitive citizen information.

The Radio Authentication and Encryption Project has raised awareness of the importance and advantages of encryption with Public Safety Network customers, including the associated risks and financial costs so network users can make informed decisions based on their needs.

While the adoption of encryption is measured monthly as part of the Project, no other governance has been put in place for agency compliance as it is not mandatory. However, based on customer feedback, the following actions can be put in place to improve network encryption:

- Configure the NSW Telco Authority Key Management Function to be ready to manage encryption keys and 'Over the Air Re-keying' so we are ready to assist any agency that may request assistance with enabling/managing encryption services of their fleet.

- Uplift the security level of the encryption offered by updating the Public Safety Network common key algorithm. The common key can be used for encrypted communication across multiple agencies.

- Purchase and integrate data encryption modules to meet the NSW Police and other commonwealth agencies requirements for encrypted data.

11. What use cases has the 'Radio Authentication and Encryption project' identified that require both encryption and interoperability?

Answer:
The use cases identified that require both encryption and interoperability include:

- confidentiality of communication on the Public Safety Network between two or more NSW Emergency Services Organisations during a multi-agency incident response.
- confidentiality of communication on the Public Safety Network between Emergency Services Organisations from NSW and another states during a multi-agency incident response that requires two or more jurisdictions to coordinate their response (typically near a state border).

12. Is the NSW Telco Authority confident that it will be able to deliver both encryption and interoperability in the use cases identified?

Answer:
While sharing of encryption keys is a pre-requisite for interoperable encrypted communication between agencies, NSW Telco Authority is not mandating encryption for the use cases.

The network continues to offer encryption to those agencies who choose to adopt it, however NSW Telco Authority has determined it will not mandate encryption on the user-end due to feedback from Emergency Services Organisations, as well as the cost burden and device management overhead it would place on agencies.

During the agency-wide consultation for the Radio Encryption Project in September 2023, Emergency Services Organisations expressed their reluctance towards using encryption in general. Specifically, Emergency Services Organisations expressed their preference to continue with the current Interoperability delivered through the allocation of unencrypted shared talk groups.

Due to security protocols, NSW Police do not wish to share their encryption keys with other agencies or NSW Telco Authority.

13. If not, what is the current and/or future work being done by the NSW Telco Authority to ensure the CCEP will be able to deliver interoperability in operations when and where it is required by the ESOs?

Answer:
The Public Safety Network continues to offer encryption to those agencies who choose to adopt it. NSW Telco Authority will continue to engage with Emergency Services Organisations to ensure their evolving needs continue to be met.

To further enhance existing network encryption, the Radio Encryption Project will update the encryption key implemented in late 2024.

Three interoperability projects are also underway to enable improved communication between NSW and interstate agencies for operations:

- Talkgroup Sharing Project - this project facilitates reciprocal talkgroup sharing arrangements between interstate agencies and NSW agencies.

  It allows Emergency Services Organisations from Victoria, South Australia and Queensland to share their talkgroups. (It should be noted that talkgroup sharing cannot replace a full interoperability solution in its entirety as there are technical limitations such as pairing with interstate agencies that have compatible dual frequency band devices.

- South Australia/NSW Interstate Interoperability Solution - This project will deliver a seamless experience for users of the network as they move from our coverage footprint to that of South Australia.

- Victoria/NSW Interstate Interoperability Solution - This project will deliver a seamless experience for users of the network as they move from our coverage footprint to that of Victoria.

14. If ESO requirements like interoperability can't be maximised, is the business case still reflective of its expected benefits?

Answer:
Yes. Business case benefits are realised through geographic and population coverage.
The program is delivering against these benefits, which are not dependent on interoperability.

Recommendation 5: The NSW Telco Authority should ensure that it complies with its Infrastructure Capacity Reservation Policy.

15. As noted in 'Appendix one - Response from agency' in 'Management of the Critical Communications Enhancement Program' through the delivery of the CCEP the NSW Telco Authority will address the infrastructure capacity reservation policy, including improved capture of information relating to reservations. What work has been done to improve the capture of information relating to reservations?

Answer:
The Infrastructure Reservation Policy is periodically reviewed and updated (last updated September 2023.)

To further improve the capture of reservation information and enhance enforcement of the Policy new procedures have been put in place around co-location requests and site design drawings. A project is also underway to develop a Site Data Hub (internal database) for immediate capture of reservations data.

All Critical Communications Enhancement Program sites have now been acquired to complete the delivery the program including lease terms. All sites have complied with the Policy.

16. What work is being done to monitor and ensure that the NSW Telco Authority complies with its Infrastructure Capacity Reservation Policy?

Answer:
All Critical Communications Enhancement Program sites have now been acquired to complete the delivery the program including lease terms. All sites have complied with the Policy.

17. If any further non-compliance with the Infrastructure Capacity Reservation Policy been identified, provide an overview of the non-compliance and what action the NSW Telco Authority has taken to address the further non-compliance.

Answer:
No further non-compliance has been identified.

Recommendation 6: The NSW Telco Authority should 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.***

18. As noted in 'Appendix one - Response from agency' in 'Management of the Critical Communications Enhancement Program' these recommendations are being addressed through either operational process or as part of the 'Radio Authentication and Encryption project'. For each of these steps (a, b and c):

1. provide an update on what action/s has been taken and when
2. outline the progress and outcome of the actions
3. specify how the actions sufficiently mitigate the risk of cloning of unauthenticated terminals

Answer:
A - By October 2023, implement interim strategies to identify and address the risk of cloned terminals:

- The CloneWatch monitoring application was implemented in August 2023 to detect and reduce potential issues of unauthorised radio cloning within the Public Safety Network.
- NSW Telco Authority monitors the application's reporting monthly and reports suspicious or unusual radio data to relevant agencies for action.
- The increase of authenticated terminals on the Public Safety Network combined with the CloneWatch monitoring application detects suspicions radio activity and mitigates the risk of cloning by pro-actively identifying, reviewing and blocking cloned radios.

B - By June 2024, require that authentication-capable terminals be authenticated:

- A Radio Authentication project was commenced in 2021 to assess, measure and uplift the adoption of authentication across the Public Safety Network. The terminal guidelines for Public Safety Network have mandated authentication-capable terminals since 2017.
- In July 2021, the Terminal Guidelines for the Public Safety Network were updated to reflect that all terminals using the network would need to be both authentication-capable and authentication-enabled from 1 July 2024. These guidelines were shared with Public Safety Network customers and terminal manufacturers.

- In February 2024, NSW Telco Authority rolled out a new Remote Radio Authentication solution to support the rapid authentication to Public Safety Network customers' radios. This solution makes it easier, faster and less costly for customers to implement authentication because it means they can enable authentication remotely without having to physically recall all the devices back to a central location for programming.

- In the discovery phase of the Radio Authentication project in 2021, analysis showed that 37.7% of terminals on Public Safety Network were authenticated and 62.3% of terminals were authentication capable. As of April 2024, after extensive engagement with customers, 45.5% are authenticated and 99.5% of terminals are authentication capable.

- To drive this adoption up to 100%, would require 35,900 radios owned by 49 agencies to enable authentication on their devices.

- NSW Telco Authority is continuing to work with its customers (prioritising Emergency Services Organisations customers who carry the largest fleet of radios) however the June deadline may not be met because of technical or financial barriers.

- However, following the adoption of authentication by NSW Ambulance and NSW Police Force, it is expected that the total of authenticated devices will be at 78.5% across the network and expected to increase over coming months.

C By June 2025, require that all terminals using the enhanced Public Safety Network be authenticated:

Please refer to response to Question 18, B.

- NSW Telco Authority continues to work towards the June 2025 delivery date and has advised its customers of requirements.

- It must be noted that enabling authentication is ultimately customer funded and implemented and it is expected the last 5% of unauthenticated terminals may be subject to technical and financial barriers faced by smaller Public Safety Network customers.

- Authenticated terminals across the Public Safety Network would eliminate any risk of cloned unauthenticated terminals.

19. Given the improvements in coverage and reliability that the CCEP is expected to deliver to the enhanced PSN, does the NSW Telco Authority expect more non-ESO terminals to use the network?

Answer:
Yes. Under the *Government Telecommunications Act 2018 No 67* NSW Government agencies are required to use the Public Safety Network (previously Government Radio Network) for operational communications requiring the use of a telecommunications network.

20. If more non-ESO terminals are expected to use the PSN once the CCEP is completed, what work has the NSW Telco Authority done to evaluate how this may impact the risk of cloning of unauthenticated terminals?

Answer:
All new terminals provisioned for the Public Safety Network must comply with the *Radio Terminal Configuration Policy – NSW Public Safety Network.*

NSW Telco Authority has a radio terminal testing scheme where radio terminal features and functionality (including radio authentication) of radio models are tested on the Public Safety Network.

TRANSPARENCY

21. Page 4 of the Auditor-General's report to Parliament, *Management of the Critical Communications Enhancement Program*, noted that the increasing capital cost of the Critical Communications Enhancement Program was not communicated to Parliament or the community until the 2021-22 NSW Budget. Can you explain why this occurred?

Answer:
NSW Telco Authority noted in its response to the Auditor-General's report that this finding was not entirely correct. The total investment in the Critical Communications Enhancement Program was disclosed to Parliament and the community as phased funding was approved.

For example, media releases between 2018-2020 refer to the total investment of the Critical Communication Enhancement Program. The full cost of the program ($1.3bn) was disclosed once the total investment in the Critical Communications Enhancement Program was known (2021-22 NSW Budget papers).

NSW Telco Authority was unable to disclose investment to the community until the NSW Government at the time had approved the investment.

22. What has the NSW Telco Authority done to improve the transparency of the CCEP's capital costs to Parliament, to the public, and to other relevant stakeholders?

Answer:
NSW Telco Authority cannot issue a media release or parliamentary update on budget announcements on behalf of the Minister or NSW Treasury.

NSW Telco Authority has and continues to provide regular reports on the Critical Communication Enhancement Program's capital cost to NSW Treasury, NSW State Emergency Service Organisations, the Ministerial Office and the NSW Board of Commissioners.

WHOLE-OF-GOVERNMENT COST

23. What steps has the NSW Telco Authority done to improve the tracking and reporting of whole-of-government cost of the CCEP, including with reference to Infrastructure NSW's 2019 recommendation?

Answer:
This was included in NSW Telco Authority's response to the NSW Auditor General.

NSW Telco Authority tracks and reports monthly on the cost to deliver the Critical Communication Enhancement Program. NSW Government agencies who run their own networks/infrastructure are not obligated to report their expenditure to NSW Telco Authority.

Whole-of-Government budgeted and forecasted costs are captured as part of the NSW Treasury processes for Parameter Technical Adjustments and New Policy Proposals.

24. What is the whole-of-government cost, for each financial year, incurred to date for the CCEP?

Answer:
Please refer to response provided in Question 23.

NSW Telco Authority does not have visibility of these costs and the question should be referred to NSW Treasury.

REFRESH OF PAGING NETWORK

25. Page 34 of the report, *Management of the Critical Communications Enhancement Program*, noted that the refresh of the paging network was included in the original scope of the CCEP, then removed from the scope of work during delivery, and later included in a separate business case after representations from the affected ESOs. The Auditor-General reported record-keeping for these decisions was not adequate.

Can you clarify:

a. Whether these records have subsequently been located?
b. If not, why no records are available on this matter?
c. What was the decision-making process to remove the paging network refresh from scope including what accountability measures informed this process?

Answer:
The Critical Communications Enhancement Program is delivering against 828 accepted user requirements. These requirements, which exclude paging, were signed off by each Emergency Service Organisation multiple times including:

- In 2018 following network design
- In 2020 when requirements were updated to include resiliency amendments following the Bushfire Inquiry
- In 2022 following an iNSW recommendation to re-validate requirements

The decision making process on what the Critical Communications Enhancement Program would deliver involved all five Emergency Service Organisations, NSW Treasury and Cabinet. Signed Statement of Requirements from Emergency Services Organisations' commissioners (or assistant commissioners) confirm this.

26. What was the decision-making process to develop a new and separate business case for refresh of the paging network, including what accountability measures informed this process?

Answer:

The steering committee made the decision to progress paging as a distinct program, under its own business case to allow the final Critical Communications Enhancement Program business case to specifically focus on requirements for completing the Public Safety Network, and incorporating lessons learnt from operational experience and recommendations from the NSW bushfire inquiry.

The steering committee approves the scope of the program including release and usage of contingency. Scope changes (and associated costs) are approved by the steering committee, Treasury and Economic Review Committee of NSW Cabinet, including the separation of paging as a distinct program and business case.

27. How and when was the removal of the refresh of the paging network refresh from CCEP scope communicated to the ESOs?

Answer:
Across 2019/2020 a Statement of Requirements was updated for the Critical Communications Enhancement Program following the Black Summer Bushfires.

28. What was the timeframe between the decision to remove the paging network refresh from CCEP scope and communicating this decision to the ESOs?

Answer:
Emergency Services Organisations were involved in the decision making process which occurred throughout 2019-2020.

Each agency signed off the Statement of Requirements for what the final funding phase of the Critical Communications Enhancement Program would or would not include.

29. Noting that the decision to remove the refresh of the paging network appears to have resulted in rework and the development of an additional business case, how has the NSW Telco Authority improved its processes to avoid similar re-work in the future?

Answer:
NSW Telco Authority established a new business case function in 2021-2022. A dedicated business case team now manages business cases end-to-end including engagement with NSW Treasury and all relevant customers and stakeholders.

DECOMMISSIONING

30. What is the status of the decommissioning of redundant sites, including what cost savings the CCEP has achieved to date?

Answer:
NSW Telco Authority tracks costs to deliver the Critical Communication Enhancement Program. NSW Telco Authority does not have visibility of other agencies costs or cost savings which are reported to NSW Treasury.

Site decommissioning is still being worked through. Consultation with the Minister, NSW Treasury, Emergency Services Organisations and other stakeholders on the status of decommissioning will occur throughout 2024 and 2025.

31. How does the NSW Telco Authority track and report on the cost savings realised to date from the rollout of the CCEP?

Answer:
NSW Telco Authority tracks costs to deliver the Critical Communications Enhancement Program. NSW Telco Authority does not have visibility of other agencies costs, which are reported to NSW Treasury.

NSW Treasury is best placed to advise on cost savings from the Critical Communications Enhancement Program rollout on completion of the program following the migration of all emergency services organisations to the Public Safety Network.

BENEFITS REALISATION

32. How does the NSW Telco Authority measure, evaluate and report on the realisation of benefits from the CCEP achieved to date?

Answer:
Public Safety Network coverage benefits are measured and reported monthly against business case targets. The Critical Communications Enhancement Program is delivering against business case benefits. Benefits are measured in terms of coverage provided by the Public Safety Network across NSW population and land mass

ENDS