COMMS CONNECT

AFC, SOCI and WISP Compliance in 2025

Adrian Robertson – WISPAU President

About WISPAU

- **WISPAU** (Wireless Internet Service Providers Association of Australia) is a not-for-profit organisation
- Main focus is on ensuring its objectives promote and support the wireless ISP's in Australia
- Provides support and assistance to WISP's members of Australia
- Improving relationships with vendors that have an association with services and products related to the wireless internet services provided by members
- Advocating on matters of relevance to members and the wireless internet service provider industry
- Establishing links with organisations of similar interests in improving the delivery of services to Australia via wireless internet
- Educating on the importance of WISP's in delivering broadband services and improving connectivity to persons in Australia
- WISPAU continues to grow – Over 85+ members & 45+ vendors. **www.wispau.au**

AFC Update

WISPAU Wireless Internet Service Provider Association of Australia

- **AFC** (Automatic Frequency Coordination) in the 6 GHz frequency band is used to manage and prevent interference between unlicensed devices and licensed incumbents (such as fixed microwave links) operating in the same band.
- AFC automatically determines which 6 GHz frequencies an unlicensed device can use, based on its location and a database of licensed users, to avoid interference.
- This is particularly important in the **5.925–6.585 GHz** range, where **standard-power** unlicensed devices must use AFC before transmitting outdoors or at higher power levels.
- AFC is a key enabler of providing wider channels, faster fixed wireless broadband while protecting existing PTP licenced services.

AFC Update

WISPAU Wireless Internet Service Provider Association of Australia

- AFC is established and successfully in use in America and Canada.
- ACMA has mentioned considerations for AFC in Appendix A of the Future use of the upper 6Ghz band options paper in June 2024.
- Cambium Networks, Qualcomm and WISPAU have been working on and discussing scientific trial requirements with the ACMA
- Trial of AFC under Scientific Licence has now been approved with conditions and will begin with reports to ACMA on any issues.
- Trial to last 12 months

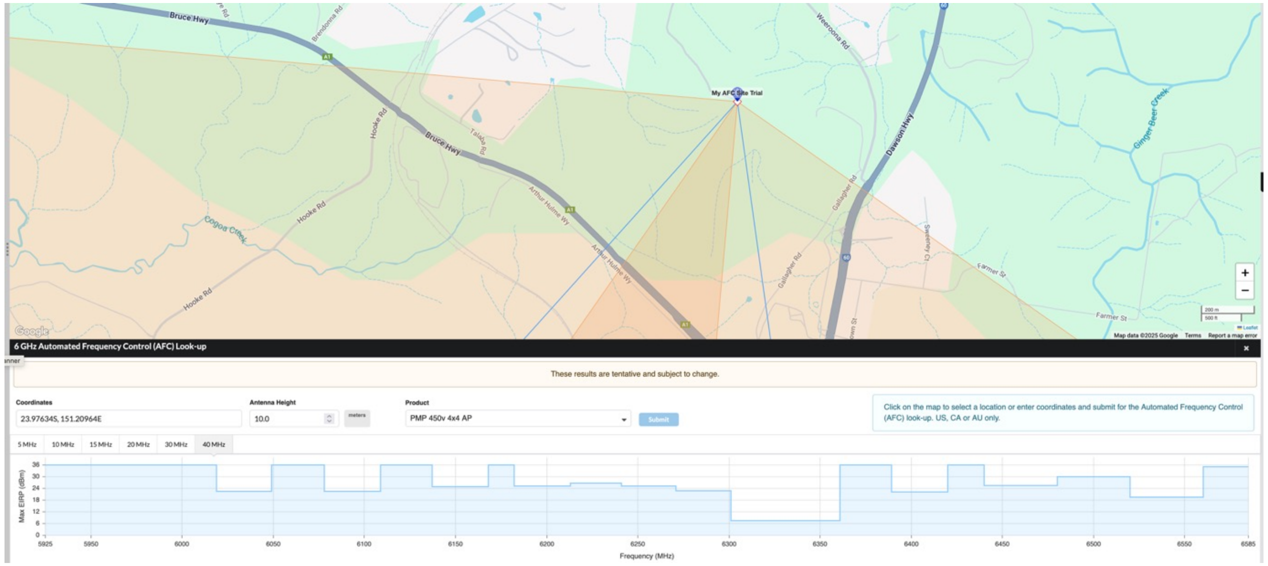
AFC Update

WISPAU Wireless Internet Service Provider Association of Australia

- Qualcomm are importing data from ACMA database every 24hrs for 6Ghz licence link references
- This data is used to determine available channels and power limitations
- Both Access points and CPE require GPS to determine location for calculation of channels and power
- Cambium Networks radio equipment used in the trial – 450V and ePMP 4600

AFC Update

- Cambium Networks have a free online tool that can show available 6Ghz channels and power
- LinkPlanner - https://lp.cambiumnetworks.com/login



6 GHz Automated Frequency Control (AFC) Look-up

These results are tentative and subject to change.

Coordinates: 23.97634S, 151.20964E

Antenna Height: 10.0 meters

Product: PMP 450v 4x4 AP

Click on the map to select a location or enter coordinates and submit for the Automated Frequency Control (AFC) look-up. US, CA or AU only.

AFC Update

WISPAU Wireless Internet Service Provider Association of Australia

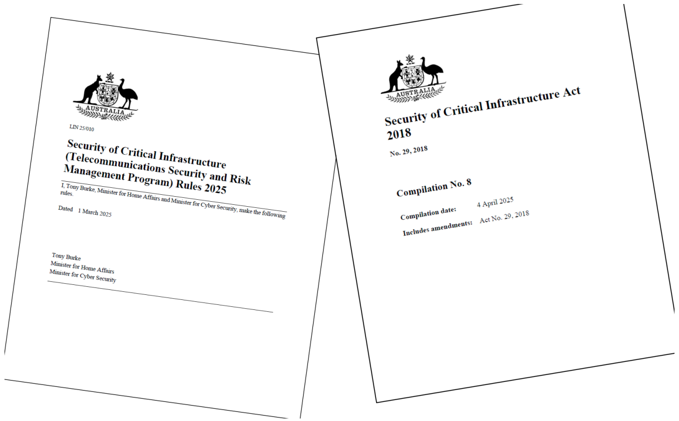
- WISP’s in Australia can participate in the trial
- WISPs must be member of WISPAU
- **Trial limited to 12 months** - no guarantee from ACMA on future decision or direction of AFC
- Trial is run through WISPAU as primary contact point
- Limited to Cambium Networks 6Ghz – PMP450v and ePMP4600
- Interested WISPs / Organisations to contact WISPAU for detailed document on participation and requirements in the trial

SOCI Act

Security of Critical Infrastructure (SOCI) Act

Security of Critical Infrastructure (Telecommunications Risk Management Program) Rules 2025

- Obligations on Telecommunication Carriers and carriage service providers with over 20k services or supply Commonwealth Govt
- Purpose is to protect critical infrastructure from cybersecurity threats, security risks and sabotage
- Legislative requirement with timelines in place
- Entities have a responsibility and obligation to protect their assets



AUSTRALIA

LIN 25/010

Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, make the following rules.

Dated 1 March 2025

Tony Burke
Minister for Home Affairs
Minister for Cyber Security

AUSTRALIA

Security of Critical Infrastructure Act 2018

No. 29, 2018

Compilation No. 8

Compilation date: 4 April 2025
Includes amendments: Act No. 29, 2018

SOCI Act

WISPAU Wireless Internet Service Provider Association of Australia

<table>
<tr><th colspan="2">Obligation</th><th>Timeframe</th></tr>
<tr><td colspan="2">Mandatory Cyber Incident Reporting</td><td>As of 4th April 2025</td></tr>
<tr><td colspan="2">Protect your asset obligation</td><td>As of 4th April 2025</td></tr>
<tr><td colspan="2">Asset Registration</td><td>As of 4th April 2025</td></tr>
<tr><td colspan="2">Notification Obligation</td><td>As of 4th April 2025</td></tr>
<tr><td colspan="2">Critical Infrastructure Risk Management Program</td><td>As of 4th October 2025</td></tr>
<tr><td colspan="2">Cybersecurity Framework Compliance -</td><td rowspan="4">Level 1 Maturity by 4th Oct 2026
Level 2 Maturity by 4th Oct 2027</td></tr>
<tr><td>ISO/IEC 27001:2023</td><td>Essential Eight</td></tr>
<tr><td>NIST Framework</td><td>AESCSF</td></tr>
<tr><td colspan="2">Cybersecurity Capability Maturity Model</td></tr>
<tr><td colspan="2">Obligation to notify data service providers</td><td>Since 2022</td></tr>
<tr><td colspan="2">Responding to serious incidents</td><td>Since 2022</td></tr>
</table>

SOCI Act

Why a *Critical Infrastructure Risk Management Plan* (CIRMP)?

Stems from the obligation in the SOCI Act of ‘***protect your asset***’ obligation

- Protect your asset – ‘maintaining competent supervision of and effective control over the asset, meeting RMP requirements as well as confidentiality of communications, availability and integrity of the asset’
- Carriers and CSP’s must identify the ***material risk*** in regard to the likelihood of hazard occurring and the ***relevant impact*** on the asset
- And ……..…. Annual Reporting in the approved forms to Home Affairs before end of financial year …. easy!

SOCI Act

So ……What hazards to be targeted? Good question….

Hazard	Details
Cyber and information security	Improper access or misuse of information or computer systems or use of a computer system to obtain unauthorized control
Personnel	Where a critical worker either via malice OR negligence compromises critical function or significant damage of the asset
Physical Security	Unauthorised access that could compromise asset
Natural hazards	Fire, flood, cyclone, storm, etc
Supply chain	Malicious exploitation or misuse or disruption of a supply chain and over reliance on suppliers

In each case also define the '***relevant impact***' – where hazard directly or indirectly impacts the asset availability, integrity, reliability and confidentiality

SOCI Act

WISPAU Wireless Internet Service Provider Association of Australia

Developing a Risk Management Plan

- What needs to be included in the plan?
  - ➢ Outline the process or system in place
  - ➢Minimise risks to prevent incidents (as far as reasonably practicable)
  - ➢Mitigate the impact realised of incidents (as far as reasonably practicable)
  - ➢Describe the interdependencies between the entity’s asset and other critical infrastructure assets
  - ➢Identify personnel in the entity
  - ➢Outline the risk management methodology
  - ➢Describe the circumstances for the review

SOCI Act

WISPAU Wireless Internet Service Provider Association of Australia

Easy… Right?

- WISPAU has assisted WISP's with a how-to document on asset registration and guidance on grouping of assets for online registration
- WISPAU and Internet Association of Australia are running group training with Pentagram Advisory for members to develop risk management programs to meet requirements
- WISPAU is also working on assisting WISP members meeting the cyber security maturity levels.

Compliance

WISPAU | Wireless Internet Service Provider Association of Australia

And even more compliance ….

WISPAU is also assisting WISP's with compliance including :

- ➢Telecommunications Consumer Protections Code (TCP)
- ➢Financial Hardship
- ➢Domestic, Family and Sexual Violence
- ➢Communication of Outages and Compensation
- ➢Complaints Handling and TIO membership requirements
- ➢Training of staff requirements

Here to Help

WISPAU Wireless Internet Service Provider Association of Australia

WISPAU has been working to assist WISP's not only in accessing new opportunities for improving services via AFC but also in improving compliance.

WISPAU members have access to templates, training documents, online videos which can assist them meeting their compliance obligations for small to medium WISP businesses who may not have the resources to meet the heavily regulated telecommunications industry

This way WISPs can meet requirements – ***and*** deliver better connectivity and broadband services in Australia.

COMMS CONNECT

www.comms-connect.com.au

ASSOCIATION PARTNER

ARCIA

Australian Radio Communications Industry Association

MEDIA PARTNER

comms critical

PUBLIC SAFETY | SECURITY | MINING | TRANSPORT | DEFENCE

ORGANISED BY

wfevents

connecting industry

Slide 1 – About WISPAU

Hello everyone.

First off, I’d like to say thank you to CommsConnect for having this great event and allowing WISPAU to present.

My name is Adrian Robertson and I am the Director of the regional WISP called Dreamtilt in Central Queensland. Our WISP services just over 1500 customers primarily on fixed wireless internet connections and we service residential, business and large industry.

I have seen many changes in the fixed wireless industry over the last 20 years.

From the start of 2024 I have been the Wireless Internet Service Providers Association of Australia president

For those that are not aware, WISPAU was established in 2016 and is the representative voice of independent and community-driven fixed wireless broadband providers across this country.

We are a not-for-profit organisation formed by the industry, for the industry.

Our mission is simple — to ensure that wireless internet service providers, or WISPs, are supported, recognised, and empowered to deliver reliable, high-performance broadband to Australians everywhere

We help our members navigate the regulatory, and commercial landscape of telecommunications.

We strengthen relationships between WISPs and vendors, foster collaboration with regulators, and provide the resources our members need to stay compliant, competitive, and resilient.

Today, WISPAU represents more than eighty-five members and over forty-five vendor partners across Australia — a community that continues to grow.

WISPAU believes that wireless connectivity isn’t just a technical service — it’s an enabler of opportunity, economic growth, and digital equity. Every WISP plays a role in bridging the digital divide, ensuring that small towns, remote communities, and regional businesses have the same access to modern connectivity as our major cities.

SLIDE 2 AFC in the 6 GHz Band

One of the most exciting developments for the WISP sector is the progress of **Automatic Frequency Coordination**, or **AFC**, in the 6 GHz spectrum band.

AFC in 6Ghz represents a major leap forward in how we manage radio frequencies in shared spectrum environments.

In simple terms, AFC is the system that allows outdoor standard power unlicensed radio devices to operate in the same 6 GHz band as licensed incumbents — such as point-to-point microwave links — without causing interference.

It achieves this by using geolocation and database coordination to automatically determine which specific channels and power levels a device can use at a given location.

The outcome is both protection and efficiency: incumbents are not interfered, and new operators can access much-needed spectrum capacity.

The significance of AFC for fixed wireless broadband providers cannot be overstated.

It opens the door to wider channels, faster throughput, and improved reliability — all while maintaining the integrity of existing services that rely on this band. For WISPs, AFC can mean the difference between incremental improvement and transformative performance.

SLIDE 3

In countries like the United States and Canada, AFC systems are already in operation and proving effective.

They have shown that the combination of coordination and spectrum management can enable both innovation and protection.

The ACMA has mentioned the potential of AFC in an appendix in its *Future Use of the Upper 6 GHz Band* options paper published in June last year.

And whilst this paper discussed some policy issues and on going work required on what government and industry roles play in introducing AFC into Australia, it also provided an opportunity to discuss a potential trial of AFC in Australia under certain set conditions in the 6Ghz spectrum.

As such, WISPAU, Cambium Networks and Qualcomm have been working for over a year discussing what a potential trial would look like in Australia with the ACMA.

And I am pleased to state that we now have had an AFC trial approved by the ACMA under a Scientific Licence with the trial to last 12 months. During this time reports will be provided to the ACMA on the AFC trial.

Further details on the trial including locations are available on the WISPAU website at wispau.au

I’d also like to quickly thank all those involved from Cambium Networks and Qualcomm in getting the trial to this stage. There has been quite a bit of work behind the scenes to get to a point where a trial can be approved by the ACMA.

SLIDE 4

The AFC system in the trial requires Qualcomm to import data from the ACMA Register of Radiocommunications Licences database every 24hrs.

It completes this via an API to the data and can determine every licenced 6ghz link located in Australia using this data.

This, along with GPS location details on both the radio access points and the customer radio unit allow the AFC system to determine available frequencies and the required maximum power levels that can be used by the radio’s.

The trial is currently utilising Cambium Networks PMP450v and ePMP4600 and is limited to this equipment for this trial.

Before the Cambium Network radios can operate it must establish contact with the AFC system to determine the available spectrum and power levels.

It must also check the AFC system every 24hrs to allow the radios to operate.

It is unlikely that spectrum availability will change frequently over time, as the AFC is only protecting licenced links, which are typically not added or removed frequently, however any changes will be detected by the regular checking and the radio will either decrease power or a new channel will need to be located.

Knowing what spectrum and power levels are available in an area is then obviously important to a WISP before deploying any 6Ghz AFC enabled radio equipment.

SLIDE 5

Fortunately for WISPs, Cambium Networks has also provided a free online tool to check areas in Australia prior to any equipment deployment or scientific licence applications for available spectrum channels in 6Ghz and the maximum power levels possible.

Cambium Networks LinkPlanner can guide WISPs as to availability using same data from ACMA as the AFC and is a very handy tool to determine if 6Ghz would be viable for WISPs to deliver improved broadband services to a specified area.

For further information – hit up the Cambium Networks team that are here at CommsConnect and they can discuss in detail further!

SLIDE 6

The great thing AFC does is give WISPs a path to use that spectrum responsibly — balancing innovation with protection.

It ensures that WISPs can expand access to bandwidth without compromising the systems already in place.

It can (and hopefully will be), a model of how technology and regulation can work hand-in-hand to create better outcomes for everyone.

At WISPAU, we see AFC not as a distant possibility but as an immediate opportunity.

The technology is proven, the policy groundwork is being laid, and our industry is keen to demonstrate that fixed wireless providers can use this spectrum safely, efficiently, and for the public good.

Whilst there is no guarantee that AFC will be implemented by the ACMA in the future, we are hopeful that the results of this AFC trial will show that an AFC can be successfully run in Australia benefiting WISPs and protecting incumbent licenced operators.

Its an exciting opportunity to be involved in developing new ways to deliver better connectivity and fixed wireless broadband services to Australians

SLIDE 7

Of course, as they say, with great power comes great responsibility.

The Australian telecommunications environment is not only advancing technically — it’s also becoming more tightly governed under a growing number of legislative frameworks.

One of the most recent of these is the Security of Critical Infrastructure Act, or SOCI Act.

The purpose of the SOCI Act and the associated Telecommunications Risk Management Program Rules 2025 is to strengthen the resilience of Australia’s critical infrastructure against cybersecurity threats, espionage, and sabotage.

The SOCI Act introduces obligations for all carriers (regardless of number of services) and carriage service providers with over 20,000 services or supplying Commonwealth Government agencies.

SLIDE 8

These obligations and timeframes are listed in the table on the slide seen here.

Obligations to Carriers and CSP’s include

- mandatory cyber incident reporting within 12 hours if deemed a critical incident with significant impact or 72 hours if it has a relevant impact on your assets ,
- telecommunications asset registration with Department of Home Affairs,
- notification of telecommunication asset changes to the Department,
- Cybersecurity compliance to level 1 by October 2026 and level 2 maturity by end of 2027 as per the suggested frameworks
- obligation to notify any 3rd party data storage providers that they are holding business critical data and information
- as well as a Critical Infrastructure Risk Management Program otherwise known as a CIRMP.

Is there anybody here that is not aware of these obligations and dates?

Hopefully we are all on top of it !

SLIDE 9

So, what and why have Critical Infrastructure Risk Management Plan, or CIRMP?

This CIRMP reflects the fundamental obligation set out in the legislation: to “protect your asset.”

Protecting an asset means maintaining competent supervision and effective control over it.

It means ensuring confidentiality, availability, and integrity. It also means identifying material risks — understanding both the likelihood of a hazard occurring and the potential impact it could have on your infrastructure and your customers.

Each year, entities are required to report to the Department of Home Affairs on how they are meeting these obligations — a process that may sound straightforward but, can be in practice, more complex and time consuming for smaller organisations without the resources of larger organisations.

Whilst most WISP businesses are no doubt familiar with what are hazards and risks, they may not be familiar in identifying all the hazards and risks required to meet CIRMP obligations and documenting them.

SLIDE 10

So what hazards need to be targeted in a businesses CIRMP?

There are 5 main categories detailed that need to be assessed which are

- Cyber and information security, where you need to consider improper access or misuse of information or systems or unauthorised control of the asset

- critical workers and personnel, where these persons through either malice or negligence could compromise the function or damage the asset,
- physical security of the asset, where issues in access could result in damage of the asset
- natural hazards impact , with issues of fire, flood, cyclones or storms
- and supply chain hazards. where issues such as exploitation or disruption of the supply chain, or even an over reliance on a supplier could result in issues to the asset.

Hazards in each category need to be identified and then assessed as to the relevant impact it may have on the asset.

SLIDE 11

The Risk Management plan for the business needs to address how, “as reasonably practicable”, the business is minimising risks to prevent incidents and the impact of such incidents to the asset.

The importance of the term reasonably practicable in the legislation is important – as individual WISPs may have different operating contexts.

For example, smaller WISPs may not have the income and budget to address some risks, while others may have geographical constraints or business size.

There may be some risks that simply cannot be reduced and the business has made a decision to operate with that known risk and risk level.

Interdependent risks between other critical assets must also be considered (for example backhaul fibre connections or connections to other providers)

Critical personnel to the business and those that have access to business critical data or operations need to assessed, recognised and documented.

The CIRMP essentially needs to be a living document – and is not designed to be simply a tick and flick, but a means to assist WISPs to understand and recognise hazards and work towards risk mitigation.

And yes, this document may be called upon by Home Affairs should a desk top audit occur by the Department.

SLIDE 12

All sounds pretty easy – right?

Especially for a WISP with a carrier licence with a few hundred customers in a regional or remote area and say 2 or 3 employees? No problem!

That's where WISPAU has been proactive in helping our members navigate these requirements.

We've developed guidance documents that explain how to register assets under the SOCI framework and how to group similar infrastructure components to simplify compliance.

We have also teamed up with Internet Association of Australia and Pentagram Advisory, to deliver group training sessions on risk management programs to smaller WISP organisations.

These sessions are allowing group collaboration and learning on SOCI obligations, hazard and risk identification and determination, documentation of the risks and controls as well as assisting in developing better business resilience and asset management.

We have also organised online meetings with the Department of Home Affairs that allows WISP members to review information in regards to their obligations from these presentations and ask questions directly.

We have further meetings with Home Affairs to provide feedback directly from members on issues they may have and how working together we can achieve the compliance outcomes.

Our aim is to ensure that WISPs, regardless of size, have access to the tools and knowledge they need to meet regulatory obligations without losing focus on service delivery and innovation.

In parallel, we’re helping members align with cybersecurity maturity models, so they can measure and improve their readiness over time and meet the required maturity levels by next year and the following year again in 2027.

Security and resilience are not just static goals — they need to be ongoing disciplines.

SLIDE 13

The SOCI Act is only one part of a wider compliance picture facing today's telecommunications providers. WISPs must also comply with the

- Telecommunications Act

-Telecommunications Consumer Protections Code,

- the Financial Hardship Industry Standard,

-the Domestic, Family and Sexual Violence Standard,

- the Telecommunications Consumer Protection and Service Standards

- the Telecommunications Consumer Complaints Handling Industry Standard

- the Telecommunications Customer Communications for Outages Industry Standard
- the Telecommunications Interception and Access Act

Just to name a few ….

These frameworks are designed to ensure fairness, transparency, and accountability in the way telecommunications services are delivered.

But they can also be daunting for small to medium providers, and even larger players have trouble abiding to all the requirements.

No WISP provider goes out of their way to be a bad provider to the customers – indeed a WISP relies heavily on making sure their customer satisfaction and local service is excellent otherwise they would be out of business in their areas.

But many WISPs need assistance in determining and meeting the requirements in the standards and codes.

This can be anything from having the right policy procedures in place for issues such as –

- Complaints Handling
- Financial Hardship
- Domestic Family and Sexual Violence
- Privacy Protections
- Authorised Representative and Advocates
- Customer Relationship Agreements and Standard Form of Agreements
- Credit Management
- Critical Information Summaries
- Communication of Outages

And training for staff for not just technical issues but also for responsible selling of services, domestic and family violence training, complaints handling, determining vulnerable customers and credit management.

Many WISPs operate as lean, technical businesses with limited administrative capacity.

Sometime, despite the best efforts of WISPs, they may not meet the compliance obligations and requirements as set out in industry legislation, standards and codes.

SLIDE 14

WISPAU recognises this reality.

That’s why our support extends beyond advocacy — we provide templates, training materials, and online resources to help members meet their obligations efficiently.

We have regular online meetings where members can share information and collaborate constructively.

Our goal is not just compliance for compliance’s sake, but a culture of professionalism that builds trust with regulators, customers, and partners alike with the WISP industry.

Taken together, AFC and SOCI and the recent legislation (and likely more to come) highlight the dual nature of our industry’s evolution — innovation on one hand, and governance on the other.

We cannot have sustainable progress without both.

AFC gives us the spectrum agility and efficiency we need to keep delivering faster, more reliable broadband.

SOCI and legislative framework’s ensure that as we expand, we do so responsibly — protecting the integrity of our telecommunication networks and the security of our nation’s digital infrastructure.

WISPAU’s role is to help WISPs navigate this balance — to turn complexity into clarity, and regulation into opportunity.

By working together, we are proving that the fixed wireless industry in Australia is mature, capable, and forward-looking.

We are showing that small and regional operators can innovate at the same level of sophistication as major carriers — and, in many cases, do so with greater agility and community focus.

Every WISP that can improve its compliance posture, strengthens its cybersecurity defences, and invests in next-generation spectrum technologies contributes to a stronger, more connected Australia.

That's the vision we pursue at WISPAU — an industry that isn't defined by its size, but by its capability, integrity, and commitment to serving communities.

Our message is simple:

Australia's digital future depends on diversity, inclusion, and resilience in its telecommunications ecosystem. WISPs are a vital part of that story —

and WISPAU is here to make sure that story continues to grow.

Thank you and thanks again to CommsConnect for allowing WISPAU to present today.

Happy to take any questions on the presentation.