AFC and WISP Compliance

Adrian Robertson – WISPAU President

WISPAU | Wireless Internet Service Provider Association of Australia

About WISPAU

WISPAU Wireless Internet Service Provider Association of Australia

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 ISPs in Australia

Provides support and assistance to WISP 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 WISPs in delivering broadband services and improving connectivity to persons in Australia

WISPAU continues to grow its member base and vendor relationships -> **www.wispau.au**

Agenda

WISPAU | Wireless Internet Service Provider Association of Australia

1

AFC update

Automatic Frequency Coordination in the 6 GHz band, the Australian trials and the path to a class licence

2

SOCI Act

Asset registration, annual reporting and the WISPAU CIRMP / TSRMP template

3

TCP Standard and compliance

The ACMA draft Standard, key concerns for WISPs, new obligations and other compliance support

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 licensed services.

How AFC works

Device reports its location → AFC system checks the licensed incumbents nearby → Permitted channels and power levels returned → Device transmits at standard power

AFC Update

WISPAU | Wireless Internet Service Provider Association of Australia

- AFC trials are underway in Australia. Some have been running since last year with others (and a presentation after this one) progressing now, with other vendor radios planned for later this year
- AFC trials are using various radio equipment and are not locked into any particular radio equipment vendor
- WISPAU has been providing details and updates of the trials to the ACMA, along with other radio vendors
- The trials are to provide ACMA with data on how AFC can move to a permanent, class licence solution to provide WISPs the opportunity to access more spectrum in areas to deliver faster and improved broadband in areas.



AFC Update

WISPAU Wireless Internet Service Provider Association of Australia

- WISPAU attended the RadComms 2026 with further discussions on AFC
- Progress is being made with ACMA and soon a publication on AFC and potential class licence standard power use in Australia will be released
- Discussion was mostly positive on lower 6 GHz band – with some discussion and further work on potentially upper 6 GHz band using AFC
- WISPAU to respond once ACMA publishes



AFC Update

WISPAU | Wireless Internet Service Provider Association of Australia

- WISPAU continues to work towards an AFC class licence in Australia
- Having AFC will dramatically improve WISPs' ability to deliver improved services using existing vendor radio equipment – and such equipment is likely to improve quickly
- WISPs will be able to be competitive with speeds as fast as LEO with the advantage of local support
- AFC is proven to work effectively delivering real results whilst still protecting incumbent licence holders in the spectrum

The 6 GHz band

Lower 6 GHz 5.925–6.425 GHz

Class licensed for low-power use today; AFC trials are testing standard-power outdoor use

Upper 6 GHz 6.425–7.125 GHz

Further work on possible AFC use is under discussion. A trial in this band is currently being discussed and looked at to provide data and details to ACMA

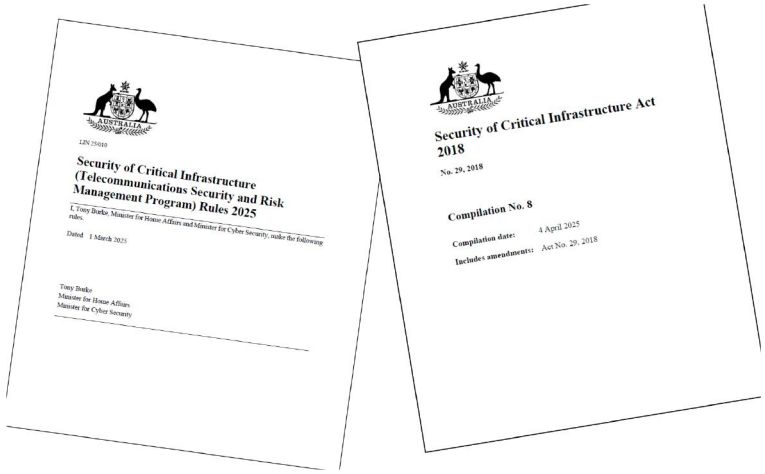
SOCI Act

WISPAU | Wireless Internet Service Provider Association of Australia

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 at least 20,000 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 and be in control of their assets



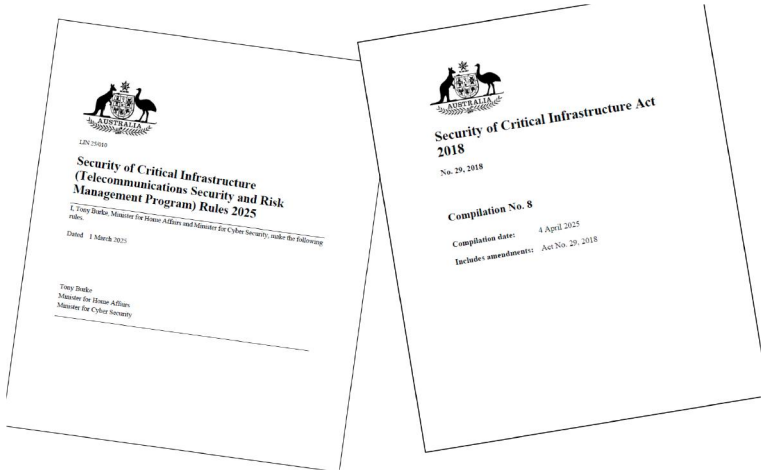
SOCI Act

WISPAU | Wireless Internet Service Provider Association of Australia

WISPs, along with other telecommunication carriers and CSPs that are required to comply should have now registered their asset.

The annual report for CIRMP/TSRMP is also now due via the CISC online submission

Telecommunication carriers and required CSPs have a legal obligation to review and attest to their CIRMP plans being up to date and reviewed by management



SOCI Act

WISPAU Wireless Internet Service Provider Association of Australia

Critical Infrastructure Risk Management Plan (CIRMP)

Carriers and CSPs must identify the ***material risk*** in regard to the likelihood of hazard occurring and the ***relevant impact*** on the asset

What needs to be included in the plan?

1. Outline the process or system in place
2. Minimise risks to prevent incidents
3. Mitigate the impact of incidents
4. Describe the interdependencies between the entity's asset and other critical infrastructure assets
5. Identify personnel in the entity
6. Outline the risk management methodology
7. Describe the circumstances for the review

SOCI Act

WISPAU | Wireless Internet Service Provider Association of Australia

Where to start?

WISPAU has created a template CIRMP / TSRMP document that will assist WISP businesses to fast track the work required to become compliant with the act

CIRMP Template provides guidance on risk methodology and assessments as well as meeting the prescribed material risks required by the TSRMP / SOCI

Contains guidance and examples of risks and controls common in WISP industry, including cybersecurity guidance to meet required maturity levels

WISPAU also has provided a mapping document outlining where in the CIRMP template compliance obligations are met under SOCI and TSRMP legislation.

TCP Standard Update

WISPAU | Wireless Internet Service Provider Association of Australia

Telecommunications (Consumer Protections) Industry Standard 2026

- ACMA has released a draft TCP Standard after rejecting the industry TCP code of conduct
- The new Standard will be enforceable by ACMA.
- Telecommunication providers that are not compliant may receive breach notices and enforceable action from the ACMA

Consultation submissions to the ACMA close 10 November 2026

So what has changed?

New Obligations

WISPAU | Wireless Internet Service Provider Association of Australia

Governance, training and reporting (1 of 3)

Source: ACMA consultation draft, September 2026. Section numbers may change.

Mis-selling reports to the ACMA

s 41

Quarterly written report to the ACMA of all known mis-selling, due 30 business days after quarter end.

No word yet on whether nil reports are needed.

Senior executive accountability

s 9

A senior executive approves, and is responsible for, all policies, procedures and training.

Usually the owner. Keep signed approvals.

Assessed training

s 11, 12

Tested training on the Standard, vulnerability, First Nations and diverse consumers, refreshed yearly.

Includes contract installers and outsourced support.

Quarterly staff monitoring

s 13

A documented check each quarter that staff follow policies and procedures.

A signed quarterly checklist is the simplest evidence.

Sales incentive policy

s 40

If incentives are paid: sales up to 30% of bonus, feedback at least 70%, bonus up to 20% of salary, clawback.

Not needed if no incentives are paid.

What a small WISP needs to set up

- A named accountable person and dated sign-off on each policy
- A policy register reviewed at least yearly (s 8)
- Training modules with a short assessment and a record of results
- A quarterly checklist covering monitoring and the mis-selling register

New Obligations

WISPAU | Wireless Internet Service Provider Association of Australia

Supporting customers and remedies (2 of 3)

Source: ACMA consultation draft, September 2026. Section numbers may change.

Preferred communication method

s 21

Agree, record and use each customer's preferred contact method and time.

Needs a field in the billing or CRM system.

Evidence of vulnerability

s 23, 102

Ask only for minimum evidence, never refuse help for lack of it, and keep the type, not a copy.

A customer's own statement is acceptable evidence.

Remedy for impaired decision-making

s 48

Claim within 6 months; decision in 10 business days; fee-free exit and refund on returned equipment.

Covers installed equipment such as roof antennas.

Remedy for provider technology change

s 47

If a network change leaves the service unsuitable: equivalent service free, or fee-free exit and refund.

Relevant to radio platform and spectrum changes.

Human-operated contact channel

s 59(3), (4)

Customers must be able to reach a person. A chatbot alone does not comply.

Publish contact details and hours of operation.

Mobile coverage check and remedy

s 44, 46

Mobile only: coverage check before sale and a 20 business day exit right.

Not relevant unless mobile services are sold.

New Obligations

WISPAU | Wireless Internet Service Provider Association of Australia

Contracts and accounts (3 of 3)

Source: ACMA consultation draft, September 2026. Section numbers may change.

Deceased customer policy

s 62

Published policy for estate representatives to notify a death and close or transfer the account.

Requests must be handled in a timely, sensitive way.

Cancellation process

s 63

Published process: explain consequences, then change or cancel within 2 business days.

Charge only amounts already incurred or disclosed.

Provider-initiated contract change

s 64

20 business days' written notice before the provider changes a contract.

Covers price and inclusion changes.

Discount expiry notice

s 83

20 business days' notice before a discount or credit ends.

Needs an automated reminder in billing.

Restoration after wrongful disconnection

s 96

Restore within 2 business days if cut off in error or without notice, or agree an equivalent.

Hard for remote sites that need a technician visit.

What a small WISP needs to set up

- Website pages for the deceased account policy and the cancellation process
- Notice templates for contract changes and discount expiry
- A restoration procedure, including what to offer if a site visit is needed
- Billing reminders keyed to 20 business days

Key Concerns

WISPAU | Wireless Internet Service Provider Association of Australia

Six areas where rules built for large mobile retailers land hardest on small and medium regional WISPs

Source: ACMA consultation draft, September 2026. Section numbers may change.

Credit checks at $300

$300 was $1,000

External credit check for every new residential customer. About $22 a check plus staff time, and telcos cannot see repayment history. (s 50 to 54)

Longer road to disconnection

20 business days (was 5 working days)

Three reminder notices before disconnection, no collection fees, and restoration within 2 business days, even for remote sites. (s 91 to 96)

No small-provider tier

30,000 services before any relief

The 2019 concessions for suppliers under 3,000 services are gone. A 900-service WISP carries the same duties as one with 29,000. (s 5)

Governance and reporting

4 a year quarterly reports and checks

Written policies, senior executive sign-off, quarterly monitoring and quarterly mis-selling reports to the ACMA. (s 8, 9, 13, 41)

Assessed training

3 new training topics

Tested before first customer contact and yearly. Adds First Nations, cultural diversity and authorised representative topics. (s 11, 12)

Billing, payments and website

15+ new or changed web items

Two fee-free payment methods, notice before every direct debit, machine-readable CIS and a WCAG 2.2 website. (s 19, 31, 86 to 88)

WISPAU is reviewing the changes and discussing with members and the ACMA on paths forward to assist in a TCP Industry Standard that protects consumers but also recognises the concerns of WISPS with achievable compliance by the WISP industry.

Compliance

WISPAU Wireless Internet Service Provider Association of Australia

And even more compliance ….

WISPAU is also assisting WISPs with compliance including:

- 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 WISPs not only in accessing new opportunities for improving services via AFC and radio vendors but also in improving compliance and business standards.

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.

Find out more or become a member at **www.wispau.au**

COMMS CONNECT

www.comms-connect.com.au

ASSOCIATION PARTNER

ARCIA

MEDIA PARTNER

comms critical

PUBLIC SAFETY | SECURITY | MINING | TRANSPORT | DEFENCE

ORGANISED BY

wfevents

connecting industry

SLIDE 1 – AFC and WISP Compliance (title slide)

Hello everyone.

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

For those that don't know me, my name is Adrian Robertson and I am the Director of Dreamtilt, a regional WISP in Central Queensland. Our WISP services around 1,700 customers, primarily on fixed wireless internet connections, and we service residential, business and large industry customers.

I have been in the telecommunications industry for over 20 years and have seen amazing changes and developments in the industry during this time.

Since the start of 2024 I have been the President of the Wireless Internet Service Providers Association of Australia, or WISPAU.

And for those in the room who don't run a wireless network — a WISP, or wireless internet service provider, is a business that builds and runs its own fixed wireless network. That's towers and radio links delivering broadband to homes, farms and businesses, in cities, regional, rural and remote areas all over Australia.

Today I'll cover three things: what's happening with AFC in the 6 GHz band, where providers stand with the SOCI Act, and the ACMA's new draft consumer protections Standard — which will affect every retail telco in this room, not just WISPs.

SLIDE 2 – About WISPAU

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 WISPs are supported, recognised and empowered to deliver reliable, high-performance broadband to Australians everywhere.

We provide support and assistance to our members, help them navigate the regulatory and commercial landscape of telecommunications, and advocate on the issues that matter to them — with government, with regulators and with the wider industry.

We strengthen relationships between WISPs and the vendors who supply them, we build links with organisations that share our interest in better connectivity, and we educate on the role WISPs play in delivering broadband across Australia.

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 3 – Agenda

So, we will go through three topics today.

First, an update on **AFC** — Automatic Frequency Coordination in the 6 GHz band — where the Australian trials are up to, and the path we see to a class licence.

Second, the **SOCI Act** — where carriers and providers stand on asset registration, annual reporting and their risk management programs, and the template WISPAU has built to help.

And third, the ACMA's draft **TCP Standard** — what has changed and the new obligations, then our key concerns for small and medium providers, and the other compliance support WISPAU provides.

Innovation on one hand, and governance on the other. As you'll see, the two go together.

SLIDE 4 – AFC Update: what AFC is and how it works

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

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 them interference.

The diagram at the bottom of the slide shows how it works, in basic four steps.

First, the device reports its location using GPS. Second, the AFC system checks the database of licensed users nearby — in our trials that data comes from the ACMA's Register of Radiocommunications Licences and is refreshed every 24 hours. Third, the system returns the channels and maximum power levels the device is

permitted to use at that location. And fourth, the device transmits at standard power within those limits.

The radio must check in with the AFC system before it can operate, and keep checking in regularly. If a new licensed link appears nearby, the radio will either reduce its power or move to a different channel depending on the radio vendor parameters.

The outcome is both protection and efficiency: incumbents are protected from interference, and new operators gain access to much-needed spectrum capacity.

For fixed wireless providers, the significance of this 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 5 – AFC Update: the Australian trials

In countries like the United States and Canada, AFC systems are already in operation and proving effective. Here in Australia, AFC trials are now underway.

Some have been running since last year — including the trial WISPAU worked on with Cambium Networks and Qualcomm under an ACMA scientific licence — and others are progressing now.

In fact, you'll hear more about one of them in the presentation after this one from Mimosa. Other vendors' radios are planned to join the AFC trials later this year.

An important point is that the trials are not locked into any particular radio vendor. They are using a range of radio equipment, which is exactly what we want — an AFC framework that works across the market, not one tied to a single manufacturer.

WISPAU has been providing details and updates of the trials to the ACMA, along with other radio vendors.

And the purpose of all of this is clear: to give the ACMA the data it needs to see how AFC can move from trials to a permanent, class licence solution — giving WISPs the opportunity to access more spectrum, and to deliver faster and improved broadband in their areas.

I'd also like to quickly thank everyone involved from radio equipment vendors, to those at the ACMA. There has been a great deal of work behind the scenes to get the trials to this stage.

Further details on the trials are available on the WISPAU website at wispau.au.

SLIDE 6 – AFC Update: RadComms 2026

WISPAU also attended RadComms 2026, where there were further discussions on AFC.

Progress is being made with the ACMA, and we expect a publication on AFC and potential class-licensed, standard-power use in Australia to be released soon.

The discussion was mostly positive on the lower 6 GHz band. There was also some discussion, and further work still to do, on potentially using AFC in the upper 6 GHz band.

Once the ACMA publishes, WISPAU will respond on behalf of our members — and I'd encourage anyone here with an interest in this band to do the same.

SLIDE 7 – AFC Update: the path to a class licence

So, WISPAU continues to work towards an AFC class licence in Australia.

Why does that matter? Having AFC will dramatically improve WISPs' ability to deliver better services using existing vendor radio equipment — and that equipment is likely to improve quickly once the market opens up.

It means WISPs will be able to compete with speeds as fast as low earth orbit satellite, with the advantage of local support from a provider just down the road.

And AFC is proven to work — delivering real results while still protecting incumbent licence holders in the spectrum.

The diagram on the slide shows the two halves of the 6 GHz band. The lower 6 GHz band, from 5.925 to 6.425 GHz, is class licensed for low-power use today, and the AFC trials are testing standard-power outdoor use. The upper 6 GHz band, from 6.425 to 7.125 GHz, is where further work on possible AFC use is still under discussion — and a trial in the upper band is currently being discussed, to provide further data and details to the ACMA.

There is no guarantee that AFC will be implemented, but we are hopeful the results of these trials will show that AFC can run successfully in Australia — benefiting WISPs and their customers, and protecting incumbent licensed operators.

It’s an exciting opportunity to be part of developing new ways to deliver better connectivity and fixed wireless broadband to Australians.

SLIDE 8 – SOCI Act

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 these is the Security of Critical Infrastructure Act, or **SOCI Act**, together with the Telecommunications Risk Management Program Rules 2025.

The purpose is to protect Australia's critical infrastructure from cybersecurity threats, security risks and sabotage.

The obligations apply to telecommunications carriers — regardless of how many services they have — and to carriage service providers with at least 20,000 services, or that supply Commonwealth Government agencies.

That first point is worth repeating for this audience. Many WISPs hold a carrier licence because they own their network. So a WISP with just a few hundred customers can have the same SOCI obligations as a major carrier.

These are legislative requirements with timelines in place. Entities have a responsibility, and an obligation, to protect and be in control of their assets.

SLIDE 9 – SOCI Act: where things stand

So where are we up to?

WISPs, along with other carriers and the carriage service providers that are required to comply, should have now registered their assets with the Department of Home Affairs.

Cyber incident reporting also applies — within 12 hours for a critical incident with a significant impact, or 72 hours where there is a relevant impact on your assets.

The annual report for your risk management program is also now due, through the Cyber and Infrastructure Security Centre's online submission portal.

And this isn't set and forget. Carriers and required CSPs have a legal obligation to review their plan, and for management to attest that it is up to date and has been reviewed.

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

Hopefully we are all on top of it!

SLIDE 10 – SOCI Act: the CIRMP

So, what is a Critical Infrastructure Risk Management Program, or CIRMP, and why have one?

It reflects the fundamental obligation set out in the legislation: to "protect your asset." That means maintaining competent supervision and effective control over it, and ensuring its confidentiality, availability and integrity.

Carriers and CSPs must identify the material risks — understanding both the likelihood of a hazard occurring and the relevant impact it could have on the asset, and on your customers. Those hazards cover cyber and information security, personnel, physical security, natural hazards such as fire, flood and cyclones, and the supply chain.

So what needs to be included in the plan? There are seven elements on the slide:

- outline the process or system in place
- how you minimise risks to prevent incidents
- how you mitigate the impact of incidents
- the interdependencies between your asset and other critical infrastructure assets — for example backhaul fibre or connections to other providers
- the personnel in the entity who are critical to the asset
- your risk management methodology
- and the circumstances in which the plan will be reviewed.

The important term in the legislation is “as reasonably practicable”.

Individual WISPs operate in very different contexts. A smaller WISP may not have the budget to address some risks; others face geographic constraints. There may be risks that simply cannot be reduced, and the business decides to operate with that known risk.

The CIRMP needs to be a living document — not a tick and flick, but a way to help WISPs recognise hazards and work towards reducing risk.

And yes, it may be called upon by Home Affairs should a desktop audit occur.

SLIDE 11 – SOCI Act: where to start

All sounds pretty easy — right?

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

That’s where WISPAU has been proactive in helping our members.

We have created a template CIRMP and TSRMP document that helps WISP businesses fast-track the work required to become compliant with the Act.

The template provides guidance on risk methodology and assessments, and on meeting the material risks prescribed under the TSRMP Rules and the SOCI Act.

It contains guidance and examples of the risks and controls common in the WISP industry, including cybersecurity guidance to help members reach the required maturity levels.

We have also provided a mapping document that shows where in the template each compliance obligation under the SOCI Act and the TSRMP Rules is met.

We have also worked with the Department of Home Affairs, the Internet Association of Australia and Pentagram Advisory on information sessions and group training for smaller providers.

Our aim is simple: WISPs, regardless of size, should have the tools and knowledge they need to meet these obligations without losing focus on service delivery and innovation.

SLIDE 12 – TCP Standard Update

Which brings me to the third topic — and the one that will affect every retail telco in this room: consumer protections.

For many years, consumer protections in telecommunications were set mainly through an industry code — the Telecommunications Consumer Protections Code, or TCP Code — developed by industry and registered by the ACMA.

The ACMA has now released a draft Telecommunications (Consumer Protections) Industry Standard 2026, after rejecting the industry's TCP Code.

The big difference is that a Standard is made by the ACMA and is directly enforceable. Providers that are not

compliant may receive breach notices and face enforcement action from the ACMA.

Consultation submissions to the ACMA close on **10 November 2026**. WISPAU will be making a submission, and I'd encourage every provider here to make their own.

So what has changed?

SLIDE 13 – New Obligations: governance, training and reporting (1 of 3)

The next three slides show obligations that have no direct equivalent in the 2019 Code. I won't read every box, but I'll touch on the ones that will make the biggest difference.

First, **mis-selling reports**. Every provider will report all known mis-selling to the ACMA in writing each quarter, within 30 business days of the quarter ending. Mis-selling is defined widely — any breach of a responsible

selling rule — and the draft doesn’t yet say whether a nil report is needed.

A **senior executive** must approve, and be responsible for, all policies, procedures and training. In a small WISP, that’s usually the owner.

Training must be assessed and refreshed every year, and it includes contract installers and outsourced support — not just office staff.

There must be a documented check, **every quarter**, that staff are following the policies and procedures.

And if a provider pays **sales incentives**, there are new rules on how they’re structured, including clawback. If you don’t pay incentives, that one won’t apply.

For a small WISP, the practical work is in the navy panel on the right: a named accountable person and dated sign-off on each policy, a policy register reviewed yearly, training modules with a short assessment, and a quarterly checklist.

SLIDE 14 – New Obligations: supporting customers and remedies (2 of 3)

The second group is about supporting customers.

Providers must agree, record and use each customer's **preferred communication method** — phone, email, SMS or post — and the preferred time where relevant. For most of us, that means a new field in the billing or CRM system.

Where a customer is in **vulnerable circumstances**, providers must ask only for the minimum evidence, accept the customer's own statement where that's enough, and never refuse help just because evidence wasn't provided. They record the type of evidence, not a copy.

There are new **remedies**. If a customer's decision-making was impaired when they signed up, they can claim within six months for a fee-free exit and a refund on returned equipment — and for a WISP, that equipment is an installed roof antenna and cabling.

And if a provider's own network or technology change leaves a service unsuitable, the customer must be offered an equivalent service free, or a fee-free exit. That's very relevant to WISPs as we change radio platforms and spectrum bands — including, hopefully, into 6 GHz.

Customers must also be able to reach a **human**. A chatbot alone does not comply.

And there are mobile coverage checks and remedies — which won't affect most WISPs unless they sell mobile services.

SLIDE 15 – New Obligations: contracts and accounts (3 of 3)

And the third group covers contracts and accounts.

A published policy for managing a **deceased customer's account**, so families and estate representatives know how to close or transfer it.

A published **cancellation process** — explain the consequences, then make the change or cancel within 2 business days.

20 business days' written notice before a provider changes a contract, including price changes, and 20 business days' notice before a discount or credit ends.

And **restoration within 2 business days** if a service was cut off in error or without the right notices.

Many of these are sensible and low cost. The deceased account policy and a simple cancellation process are good practice, and WISPAU supports them. The challenge for small providers is the volume of new website pages, notice templates and billing changes, all arriving at once – all requiring compliance.

SLIDE 16 – Key Concerns

So that's what is changing. Now to what concerns us.

Let me be clear up front: WISPAU supports strong, enforceable consumer protections. Telecommunications

services are essential, and customers deserve to be treated fairly.

Our concern is proportionality. The draft has two tiers: large providers with 30,000 or more services, and everyone else. Many of its rules were designed around large mobile and handset retailers — and they now apply in full to small regional providers that sell neither.

The slide shows six areas where that lands hardest.

First, **credit checks**. Under the draft, a new residential customer whose contract could result in a debt of more than $300 needs a credit assessment, including an external credit check. Under the old Code that figure was $1,000.

A typical fixed wireless plan on a 12-month term is caught. That’s time, and imposed cost for small businesses that have never needed a credit bureau account — and a telco’s credit report can’t show repayment history, so it says very little about whether someone can afford the service.

If the customer fails, the provider must refuse the contract — for someone who may have no other terrestrial broadband option.

Second, a **longer road to disconnection**. Three reminder notices are required over at least 20 business days, where the old Code needed one notice and 5 working days. Collection fees can no longer be charged. And if a service is cut off in error, it must be restored within 2 business days — which is very hard when the customer's antenna has been collected and the site is hours from the depot.

Third, there is **no small-provider tier**. The 2019 Code gave some relief to suppliers with fewer than 3,000 services. That's now gone. A WISP with 900 services now carries the same duties as a provider with 29,000.

Fourth, **governance and reporting**. Written policies for every obligation, with senior executive sign-off, documented monitoring every quarter, and quarterly mis-selling reports to the ACMA — four times a year.

Fifth, **assessed training**. Staff must pass an assessment before their first customer contact and at

least yearly, with new topics including First Nations awareness, cultural diversity and dealing with authorised representatives.

And sixth, **billing, payments and the website**. Two fee-free payment methods, a notice before every direct debit, a machine-readable Critical Information Summary — that's the short summary of a plan customers get before they sign up — and a website that meets the WCAG 2.2 accessibility guidelines.

So where to from here? WISPAU is reviewing the changes and discussing paths forward with our members and with the ACMA. Our aim is a TCP Industry Standard that protects consumers, but also recognises the concerns of WISPs — with compliance that the WISP industry can actually achieve.

That's not about seeking an exemption. It's about obligations scaled to the size of the provider, credit checks targeted at real risk, a notice path that fits services paid in advance, and realistic timeframes for remote sites.

To help, WISPAU has released a member briefing on the draft Standard, setting out every new obligation section by section, what needs to be updated, our key concerns, and the options we will be putting to the ACMA.

SLIDE 17 – Compliance: and even more compliance

And the TCP Standard is only one part of a wider compliance picture.

WISPs must also comply with the Telecommunications Act, the Financial Hardship Standard, the Domestic, Family and Sexual Violence Standard, the Complaints Handling Standard, the Customer Communications for Outages Standard and the Telecommunications Interception and Access Act — just to name a few.

WISPAU is assisting WISPs with compliance across the areas on the slide: financial hardship; domestic, family and sexual violence; communication of outages and compensation; complaints handling and membership of

the Telecommunications Industry Ombudsman, or TIO; and the training of staff.

These frameworks are designed to ensure fairness, transparency and accountability. But they can be daunting for small to medium providers — and even the larger players have trouble meeting all of the requirements.

No WISP goes out of its way to be a bad provider to its customers. A WISP relies heavily on customer satisfaction and local service — otherwise it would be out of business in its area. But many WISPs operate as lean, technical businesses with limited administrative capacity, and they need help to meet these requirements.

SLIDE 18 – Here to Help

WISPAU recognises this reality.

We have been working to help WISPs, not only to access new opportunities to improve services through

AFC and our radio vendor partners, but also to improve compliance and business standards.

WISPAU members have access to templates, training documents and online videos, designed for small to medium WISP businesses that may not have the resources to meet the demands of a heavily regulated industry. We also hold regular online meetings where members can share information and collaborate constructively.

That way, WISPs can meet their requirements — and keep delivering better connectivity and broadband services across Australia.

Taken together, AFC, SOCI and the new TCP Standard show 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 and efficiency to keep delivering faster, more reliable broadband. SOCI and the consumer protection framework ensure that as we

grow, we do so responsibly — protecting our networks, our customers and the nation's digital infrastructure.

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.

If you'd like to find out more, or become a member, please visit www.wispau.au.

SLIDE 19 – Thank you (closing slide)

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.