



Telstra Response: ACMA compliance and enforcement priorities 2026–27

Public submission

20 March 2026



1. Executive summary

Telstra welcomes the opportunity to respond to the Australian Communications and Media Authority (ACMA) consultation on compliance and enforcement priorities for 2026–27.¹ Telstra recognises the importance of regulatory compliance and enforcement for protecting consumers and driving industry performance. It also supports the ACMA’s graduated, risk based and proportionate approach to compliance and enforcement,² including clear escalation pathways for serious, systemic or repeated non-compliance.

This submission sets out Telstra’s views on the approach in the consultation paper and the priorities that need to be pursued in 2026-27. We recommend the priority areas for 2026–27 be grounded in current and emerging telecommunications risks, implementation experience from recent reforms, and evidence of consumer and community harm.

In 2026–27, the most significant harms that the ACMA’s compliance and enforcement work can help reduce are:

- public safety and continuity risks, including where outages, disasters or device failures prevent emergency calls or timely access to assistance; and
- financial and personal safety harms where telecommunications services are misused to facilitate scams such as through unauthorised porting or SIM swaps, and account takeover.

As outlined below, Telstra encourages the ACMA to set and pursue its compliance and enforcement priorities for 2026–27 in a manner that is consistent with, and gives practical effect to, the ACMA’s Compliance and Enforcement Policy (Policy) particularly where obligations are new, recently strengthened or operationally complex. This includes clear guidance and education, risk-based supervisory assurance, and graduated, proportionate escalation where harm is material, remediation is inadequate, or non-compliance is systemic.

1.1 Telstra’s recommended priority areas for 2026–27

- **Public safety and network resilience** (Triple Zero access, outage safeguards and customer communications)
- **Emergency calling integrity and device compliance** (supplier compliance with the *Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling Instrument 2015* (TLN) and relevant standards; targeted market assurance)
- **EME assurance and transparency** (audits plus publication of outcomes to support informed public confidence)

¹ Australian Communications and Media Authority (ACMA), ‘Compliance and enforcement priorities 2026–27’ (Consultation page, 20 Feb 2026) <https://www.acma.gov.au/consultations/2026-02/compliance-and-enforcement-priorities-2026-27>.

² ACMA, ‘Compliance and enforcement policy’ (webpage) <https://www.acma.gov.au/compliance-and-enforcement-policy>.



- **Tackling the supply of dodgy devices** (expand and operationalise the Equipment Safety Pledge; disrupt repeat offenders; focus on high-risk categories such as jammers and unauthorised boosters)
- **Scam education, compliance and awareness** (scam resilience, identity security and domestic and family violence (DFV) consumer protections), including mobile number fraud disruption and scam/spam mitigation

1.2 Alignment with the ACMA Compliance and Enforcement Policy

As noted in section 1 above, Telstra's recommendations are grounded in, and intended to give practical effect to, the ACMA's Policy.

Telstra broadly supports the Policy's core settings, including (a) promoting a strong compliance culture through education and guidance, particularly where new or amended regulatory requirements are introduced; (b) applying graduated enforcement tools in accordance with the compliance pyramid, with regulatory responses proportionate to the seriousness of the conduct and the level of consumer or community harm; and (c) taking into account systemic issues, compliance history, cooperation and remediation efforts when determining appropriate regulatory action.

These principles are critical to maintaining regulatory certainty, supporting effective compliance outcomes, and ensuring that enforcement action is targeted to areas of greatest risk and harm. For 2026–27, Telstra submits that the ACMA's priority settings, supervisory activity and enforcement decisions should continue to be anchored in these principles and applied consistently across the identified priority areas.

1.3 Implementation approach for the 2026–27 priority areas

Consistent with the Policy outlined above, Telstra encourages the ACMA to pair priority settings for 2026–27 with a practical, risk-based and staged implementation approach - particularly where obligations are new, evolving or operationally complex.

We also strongly encourage the ACMA to adopt an approach aligned with the ACMA's July 2025 letter to the Treasurer and Minister for Finance outlining the actions, within the ACMA's power, that it can take to support productivity, investment and growth.³ In that correspondence, the ACMA observed that, within legislative parameters, it can streamline processes, improve transparency and exercise pragmatic forbearance where appropriate, while maintaining important protections for consumers and business. The ACMA also committed to actions to improve industry understanding of obligations and transparency of its priorities and work program, and to support industry innovation through fit-for-purpose and contemporary technical and regulatory

³ Australian Communications and Media Authority (ACMA), 'ACMA actions to bolster productivity growth' (letter, July 2025) (PDF) https://www.finance.gov.au/sites/default/files/2025-08/ITRDCSA%20-%20ACMA%20-%20Response%20letter%20-%20Nerida%20O'Loughlin_Redacted_0.pdf



frameworks. These commitments align closely with the staged, guidance-led and risk-based implementation approach advocated in this submission.

In practice, this should include (a) clear guidance and worked examples to support consistent interpretation and implementation of regulatory requirements; (b) early engagement with industry and targeted supervisory check-ins to identify and address emerging risks; (c) data-driven, risk-based monitoring, focused on areas of demonstrable consumer or community harm; and (d) escalated enforcement action where there are systemic weaknesses, repeated breaches, inadequate remediation, or conduct that undermines public safety or enables significant financial harm.

This approach combines education, targeted monitoring and proportionate escalation to encourage compliance, detect higher risk issues, and deter serious or repeated non-compliance, while supporting effective and timely implementation of the ACMA's priorities.

2. Proposed compliance and enforcement priorities for 2026–27

2.1 Priority A – Compliance with Triple Zero and public safety requirements

We support the ACMA continuing to treat public safety and network resilience, including Triple Zero access and outage-related safeguards, as an ongoing priority in 2026–27. This priority should be considered within the context of the significant package of recent reforms and new obligations now applying to carriers and carriage service providers (CSPs), which are intended to improve outage notification, customer communications and emergency call continuity outcomes.⁴ These reforms have strengthened obligations in areas such as customer communications during unplanned outages, enhanced complaint handling for outage-related issues, and measures to support emergency call continuity. Given the breadth and recency of these changes, the ACMA's compliance posture in 2026–27 needs to recognise that the sector is still embedding these new requirements into operational practice, systems, processes, training and third-party arrangements. We also note that the Minister has recently announced the review of all Triple Zero legislation and regulation,⁵ which is likely to further change Triple Zero compliance requirements and expectations.

We recommend ACMA prioritise a targeted, risk-based and outcomes-focused approach to embedding recent reforms and new obligations, supported by preventative compliance activities that address known emergency calling risks. This should include progressing the device compliance and market assurance work, together with advancing consultation and design of

⁴ Telecommunications (Customer Communications for Outages) Industry Standard 2024 (Cth) <https://www.legislation.gov.au/F2024L01447/asmade/2024-11-14/text/original/pdf> ; Telecommunications (Emergency Call Service) Determination 2019 (Cth) <https://www.legislation.gov.au/F2019L01509/latest>.

⁵ Media Release - Review into the Triple Zero System. 18 March 2026. Available at: <https://minister.infrastructure.gov.au/wells/media-release/review-beginning-triple-zero-system>



supplier transparency measures under the TLN, including the opportunity for a Supplier's Declaration of Conformity (SDoC) register, as outlined in section 2.2.

2.2 Priority B – Emergency calling integrity and device compliance

Telstra supports an ACMA priority on safeguarding access to emergency call services, including ensuring that end-users can reliably make emergency calls. A key contributor to emergency calling outcomes is whether devices supplied into the market meet applicable Australian requirements (including relevant standards and labelling obligations).⁶

In this context, Telstra recommends that ACMA's 2026–27 program places targeted focus on supplier compliance and market assurance activities that can reduce the risk of non-compliant devices undermining emergency call access.

Recommended focus areas (2026–27):

- Targeted supplier assurance and auditing of compliance with the Telecommunications Labelling Notice and associated standards relevant to emergency calling (e.g., AS/CA S042.1:2025).⁷
- A risk-based market monitoring program prioritising device cohorts most likely to present emergency calling risks (e.g., where labelling/standard conformance is unclear).
- Clear guidance to suppliers on evidence expectations (test artefacts, declarations, labelling practices) to support consistent compliance outcomes.

Telstra supports a graduated, outcomes-focused posture that lifts baseline supplier compliance through clear guidance and targeted assurance, with escalation where ACMA identifies systemic supplier failures, repeated non-compliance, or conduct creating material public safety risk (including where devices materially impede emergency call access).

Telstra considers this priority complementary to ACMA's broader work on non-compliant ('dodgy') devices because emergency calling risks can arise where devices are supplied through online marketplaces or cross-border channels without the required testing, declarations and labelling. A proportionate approach focused on higher-risk cohorts and persistent non-compliance can improve emergency calling outcomes without imposing unnecessary burden on compliant suppliers.

⁶ Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2025 (Cth) <https://www.legislation.gov.au/F2025L00401/asmade/text>.

⁷ Australian Telecommunications Alliance / Communications Alliance, 'AS/CA S042.1:2025' (PDF) https://www.austelco.org.au/wp-content/uploads/2025/06/S042-1_2025.pdf.



Building on the importance of device compliance to emergency calling integrity, Telstra considers supplier transparency under the TLN warrants the ACMA's attention for promoting compliance.

Experience during the 2024 closure of 3G networks highlighted risks posed by non-compliant and grey-import devices, and limited visibility for consumers, carriers and regulators as to whether devices supplied into the market comply with Australian technical standards.

While the TLN requires suppliers to make SDoCs and retain supporting compliance records, those records are not readily accessible and there is currently no central mechanism for consumers or industry participants to verify compliance without inspecting labels or relying on supplier representations.

Telstra and the ATA have proposed that the ACMA establish a public register of SDoCs and supporting compliance records, maintained via supplier uploads and updates, which is accessible to consumers, carriers, CSPs and installers.⁸

This is something that needs to be developed during 2026-27 to improve future compliance and consumer protection outcomes. Such a register would:

- reduce risks of consumer harm and public safety impacts from non-compliant devices;
- improve detectability and enable more targeted enforcement;
- increase consumer confidence through transparency; and
- complement ACMA's broader efforts to tackle non-compliant ('dodgy') devices.

We will also raise this point on the ACMA establishing a public register of SDoCs in our response to the FYSO 2026-31 consultation.

2.3 Priority C – EME assurance and transparency (audits + publication of outcomes)

Telstra supports the ACMA continuing its base station electromagnetic energy (EME) audit program and maintaining tools that provide the public with access to this information. This program functions as an important independent assurance mechanism and helps alleviate community concerns by demonstrating ongoing measurement and compliance verification.

Recommended focus areas (2026–27):

- Maintain the EME audit program as a standing assurance activity and continue updates to public-facing EME information tools.

⁸ Telstra Limited, Submission to ACMA (20 December 2024) (response to ACMA consultation: "Proposal to remake the sunsetting Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015 and 8 telecommunications standards"). Available at: <https://www.acma.gov.au/consultations/2024-10/proposal-remake-tln-and-8-telecommunications-standards>



- Publish an annual summary of audit outcomes, including clear presentation of results and an update on the number and general location of sites checked during the year.
- Use communications products (e.g., infographic-style reporting) to ensure transparency is meaningful and supports community confidence.

Given this priority's assurance role, the focus should remain on measurement, transparency and education, with enforcement tools reserved for instances of verified non-compliance that is material, repeated or inadequately remediated.

Telstra submits that EME assurance remains a strong candidate for priority focus because it responds to persistent community concern and is a confidence-building measure that is well-suited to education, transparency and independent verification, consistent with the Policy's emphasis on using proportionate tools. As networks continue to evolve and increase in deployment density, maintaining audits and accessible publication of outcomes can help sustain informed public confidence, with enforcement reserved for verified non-compliance that is material, repeated or inadequately remediated.

2.4 Priority D – Support for continuing “Tackling the supply of dodgy devices”

Telstra strongly supports the ACMA maintaining “tackling the supply of dodgy devices” as an ongoing compliance and enforcement objective for 2026–27. This priority aligns with the ACMA's focus on matters of significant public interest and consumer harm, elevated risks of non-compliance, and targeted action to encourage compliance, deter non-compliance and strengthen consumer confidence.

The ACMA's Equipment Safety Pledge campaign has been a very helpful initiative. We welcome the pledge's focus on proactive prevention, action against repeat offenders, preventing re-listing, and rapid removal of illegal listings, supported by annual reporting and KPIs.⁹

Notwithstanding these developments, Telstra remains concerned that illegal mobile jammers and unauthorised mobile repeaters/boosters continue to be marketed to Australian consumers by offshore sellers (including through drop shipping and standalone websites), perpetuating interference and public safety risks, including risks to emergency communications.

To maximise impact in 2026–27, Telstra encourages the ACMA to prioritise the following within this priority area:

- Grow pledge participation and coverage by recruiting additional marketplaces and retailers used by Australians.
- Drive measurable uplift using pledge reporting and KPIs, including monitoring takedown volumes and the percentage of identified listings removed within 2 business days, and targeting engagement where outcomes lag.

⁹ ACMA, 'Equipment Safety Pledge' <https://www.acma.gov.au/equipment-safety-pledge>.



- Increase disruption of repeat offenders and re-listing behaviour, consistent with the pledge commitments to take reasonable action against intentional repeat listers and prevent re-listing of identified illegal devices.
- Maintain targeted consumer education and reporting pathways to reduce consumer harm and improve detection and intelligence flows.
- Apply sharper focus to high-risk categories (including jammers and unauthorised boosters/repeaters) given their interference and public safety impacts, including risks to emergency communications.

Continued ACMA focus on this priority combining platform engagement, targeted disruption of persistent supply pathways, and consumer education will be important to reduce the availability of illegal devices and associated harms.

2.5 Priority E – Scam education, compliance and awareness

Telstra strongly supports the ACMA retaining scams as an enduring compliance and enforcement priority, given the scale of consumer harm and the importance of maintaining public confidence in telecommunications services. Telstra submits that enforcement action, while necessary, is not sufficient on its own to deliver sustained scam reduction outcomes. Where obligations are new, expanding, or still being operationalised, clear and practical guidance supported by education, for both industry and consumers, remain critical to embed consistent compliance and reduce scam harm across the sector.

Consistent with the ACMA's Policy, Telstra supports a graduated, risk-based approach that is calibrated to the maturity of scam obligations and the availability of practical regulatory guidance. In the early stages of new scam-related rules or code obligations, education, supervisory engagement and targeted monitoring are the most effective tools to build capability, resolve interpretive issues and lift baseline performance across industry. Escalated enforcement is best directed to circumstances involving systemic, repeated or egregious non-compliance, or where material consumer harm persists notwithstanding reasonable compliance efforts.

Telstra also notes that the effectiveness of the regulatory framework will depend materially on the design and ongoing administration of the telecommunications scam code that the ACMA will steward. Given the pace at which scam typologies evolve and the reliance on coordination across the broader ecosystem, code development and implementation should be supported by clear regulatory intent, practical consultation and sufficient lead time. Telstra supports the ACMA taking an active, educative role as the code is developed and bedded down, with enforcement expectations appropriately scaled to match the maturing of compliance with the code. This will promote consistent application, maintain regulatory certainty, and support sustained reductions in scam harm.

Within that framework, Telstra recommends the ACMA maintains a targeted 2026-27 focus on high-harm consumer safeguards, particularly where telecommunications services can be misused to facilitate scams, unauthorised porting/SIM swap and account takeover, and where DFV consumer protections are newly strengthened or still bedding in. Priority focus areas include:



- Mobile number fraud disruption: consistent identity verification, clear exception handling and auditability for porting, SIM swap and account changes, supported by targeted assurance activity in higher-risk segments.
- Scam and spam mitigation: risk-based monitoring of control effectiveness (including complaints and consumer outcomes), and transparent thematic learnings to lift baseline performance across the sector.
- DFV consumer protections: practical implementation guidance, monitoring of compliance with new rules, and escalation where failures create material risk to vulnerable customers.

Overall, Telstra supports an education-led posture where requirements are new or interpretation issues remain, complemented by targeted monitoring and proportionate escalation to address systemic weaknesses, repeated breaches, or material consumer harm.