Department cites prolonged contract negotiations, complexity in AusAlert delays

The Department of Communications has cited the protracted contractual negotiations and complexity of the AusAlert project as the reasons why contracts to build the national messaging system were only signed in February and March 2025.

In early 2023 the federal government indicated it expected the NMS to be up and running by the end of 2024. According to briefing notes prepared by the department for a Senate estimates hearing and released under Freedom of Information, the system is now on track to be operational by 1 July 2026 with public facing implementation by 1 October 2026.

The overall value of the contracts with MNOs for the system are valued at $67.64 million, the notes reveal. That includes a $22.27m contract with Telstra to build the cell broadcast entity, which is a key part of the system to create and send messaging. Three separate contracts with the mobile carriers relate to build cell broadcast centres that support the integration of the AusAlert system.

"The breakdown of contract values has never been published due to commercial sensitivities," the briefing stated.

The initial funding for the project was $33 million announced as part of the 2022-23 Federal Budget. Additional funding of $25.3 million was provided as part of the 2023-24 budget with a contingency of $8.23 million.

The build process includes system testing to understand how messages will be delivered across different devices. The department is working with manufacturers including Apple and Google as well as with the Australian Telecommunications Alliance and ACMA to ensure requirements are met.

Samira Sarraf

OneWiFi says automated call testing platform has broader network assurance role

OneWiFi & Infrastructure CEO Mevan Jayatilleke has said the company's automated emergency call verification platform could be deployed beyond its own neutral host footprint, with potential use across conventional mobile networks and for call testing beyond Triple Zero.

Mevan Jayatilleke

The company developed the autonomous emergency call verification agent to reduce reliance on manual field testing of critical voice and emergency call services across remote, regional and multi-operator mobile sites.

The platform uses a rack-mounted device installed at a mobile site to initiate programmed or on-demand test calls, simulate real user behaviour, inject pre-recorded audio and capture radio parameters including RSRP, RSRQ, PCI and frequency layers. OneWiFi said it was designed for geographically dispersed networks and neutral host environments where multiple operators share infrastructure while retaining separate service quality and regulatory obligations.

Jayatilleke told CommsDay the same architecture could be applied more broadly across the mobile sector, including on single-operator networks and for general service assurance, public safety and enterprise resilience testing.

He said the core issue was proving that a customer at a given site could make a call when needed, rather than relying only on alarms or retrospective fault reports.

"You can't afford to have a site dormant or users camping on a site not being able to make calls," he said. "Whether it be Triple Zero is the worst case scenario where it's critical, but even normal calls."

Jayatilleke said traditional validation usually required technicians to visit sites with test equipment, which could be costly and slow when some locations were "around 16 hours from the nearest satellite town."

"Unless you can physically, unless you can mimic the user behaviour at that site, it's impossible to validate that it's working 100%," he said.

A notable feature is support for both Android and Apple devices. Jayatilleke said Android testing was more straightforward because it could be software controlled, while Apple required a mechanical workaround. OneWiFi developed robotic arms to physically interact with iPhones where direct software call initiation was unavailable.

"Apple is challenging. That is why we have to specifically design the AI around Apple because Android is so much easier," he said. "It doesn't let you do a backdoor software call, you have to physically do it externally."

The system can test multiple operators sequentially using multiple SIMs. If a primary network fails, it can also check whether the site has correctly "wilted", allowing devices to move to another available network.

"If the site has not wilted automatically, it will send the agent message saying call fail and the RF parameters showing the site hasn't wilted," Jayatilleke said. "So it's a double insurance policy."

He said this allowed operators to identify both the call failure and the risk that users remained camped on a site unable to complete calls. Results and associated site data could be returned to OneWiFi's network operations centre or to an operator's own NOC, with Jayatilleke saying the end-to-end response time could be less than one minute.

OneWiFi said the agent could be triggered automatically by service-impacting alarms from a network management system, operated manually by NOC staff or used for scheduled validation.

Jayatilleke linked the proposition to requirements for post-maintenance and periodic emergency call validation, saying large operators faced a significant operational burden if they needed to test extensive site portfolios after network changes.

"Operators are now required to do Triple Zero validation after every maintenance or network upgrade and/or every six months," he said. "So imagine trying to do this for 10,000 sites every time you do a software upgrade."

The platform also produces logs and audit trails that can help isolate whether a failure sits in the radio access network, transmission or core network. Jayatilleke said the agent's logs could be analysed with base station data to support faster fault diagnosis and dispatch.

OneWiFi is deploying the capability across its neutral host sites and will provide it at no additional charge on its own network. Jayatilleke said the tool could also be made available commercially to other operators.

"We provide that free of charge, but equally the tool is commercially, we can make it available to other operators if they wish," he said.

Grahame Lynch

AMTA advocates for prompt notification of use of drone jammers

The Australian Mobile Telecommunications Association is calling for requirements to notify any authorised use of mobile signal jamming equipment to counter remote operated drones either in advance or as soon as the notification can be made.

In its submission to the Department of Home Affairs' consultation on proposed approaches to Australia's drone security, AMTA also asserted that any use of jammers should be constrained to the smallest area possible and for a duration no longer than needed to mitigate the risk posed by the operation of a drone.

AMTA said it recognises that one of the tools for countering remote operated drones is the use of jammers to electronic spectrum, and that mobile technology has been used to control drones, so disrupting signals can counter their operation.

But the industry body noted that jamming communications to the drones results in disruption to the mobile signal for legitimate users in the immediate vicinity, and that one of the legitimate uses could be contacting emergency services. For this reason, the use of jammers should be targeted and constrained as much as possible, the submission argues.

The Australian Communications and Media Authority's guidelines require already the operator of devices exempt from the prohibition of the use of signal jammers to keep records of any use of the devices and notify potentially affected parties, AMTA said. But the provisions allow in some instances for notifications to occur after the device has been used.

Mobile operators detect and must investigate interference to their networks as part of their normal operational processes, but the cost can be avoided where the cause of interference is known to have occurred from the use of a device under exemption, AMTA said. Rapid notification can therefore benefit the industry.

The submission also requests that if operation of drone jammers is to be extended to beyond those currently allowed, that the newly authorised entities be made aware of the requirement to notify spectrum licensees when jammers are used.

Dylan Bushell-Embling

IAA warns of risks from overlapping regulations

The Internet Association of Australia has told a Senate inquiry into the government's unfair trading practices bill that telecommunications contracts should be excluded from provisions in the legislation aimed at subscription-style contracts.

The IAA said the measures risk duplicating existing obligations within the telecommunications sector.