CISCO PARTNER

Public Safety Reimagined

Powering Australia's Essential Public Safety Services through the Telstra and Cisco Strategic Alliance

Executive Summary

Australia's public safety and critical infrastructure sectors are operating under unprecedented pressure. Emergency services are managing higher incident volumes, more complex threat landscapes, and exponentially greater data demands all while legacy voice centric systems strain under the weight of modern expectations.

Citizens contacting Triple Zero (000) now expect to share live video, location data, and real time telemetry. Operators of essential services face expanding regulatory obligations under the Security of Critical Infrastructure (SOCI) Act. And across energy, transport, and water networks, the convergence of cyber threats, extreme weather, and ageing infrastructure is no longer a future risk it is today's operational reality.

The question facing public safety and critical infrastructure leaders is no longer whether to modernise, it is how to do so securely, at scale, and with proven outcomes.

Through a strategic alliance, Telstra and Cisco deliver a sovereign, industrial grade digital backbone purpose built for Australia's most demanding environments. Telstra's national carrier infrastructure and cellular leadership including 4G 5G, LANES prioritisation, and QPP frameworks, combined with Cisco's industrial networking, edge compute, and security technologies, creates a resilient, compliant, and intelligent foundation for mission critical operations across voice, data, and video.

This paper explores why that foundation matters, what it delivers, and how your organisation can act on it today.

> ***"90% of organisations say their privacy programs have expanded because of AI, and 43% report that privacy spending has increased over the past year to manage growing complexity."***
>
> *Cisco 2026 Data and Privacy Benchmark Study*

1. The Operational Reality: When Hazards Converge, Systems Must Not Fail

Australia has entered an era of hazard convergence where natural disasters, cyber incidents, and national security threats no longer occur in isolation but overlap in ways that compound risk and overwhelm siloed systems.

Bushfires coincide with network outages. Floods simultaneously disrupt transport, energy, and telecommunications. Cyber actors are increasingly targeting operational technology (OT) systems during periods of crisis, a trend accelerated by the rise of AI powered attack tools. Recent global geopolitical tensions illustrate this reality starkly, with critical infrastructure including energy and water treatment systems increasingly targeted as strategic assets beyond conventional military engagements.

Domestically, the scale of events like Cyclone Alfred (February 2025, SEQ NSW), recent east coast flood emergencies, and recurring bushfire seasons has reinforced a critical lesson: communications resilience is not a technical nicety it is a life safety imperative.

Clean energy transformation adds further complexity. The proliferation of distributed assets from renewable generation sites and battery storage to EV charging infrastructure is placing new demands on secure, always on connectivity across networks never designed for this scale or diversity of endpoints.

Meanwhile, community expectations have shifted decisively. The community expects emergency services to receive, process, and act on rich data video, geolocation, sensor telemetry not just a voice call. This drives exponential growth in data volumes across networks built for an earlier era.

The operational imperative is clear: Australia's public safety and critical infrastructure sectors require industrial grade, cyber resilient connectivity that can withstand environmental extremes, defend against sophisticated threats, and support modern, data rich mission critical operations all at the same time.

> ***"Industry estimates indicate that globally, across business network infrastructure, almost half (48%) of assets are ageing or obsolete, representing a massive 'technical debt' that leaves critical infrastructure vulnerable to known exploits."***
>
> *WPI Strategy, Update Critical (2025)*

2. A Sovereign Industrial Connectivity Model Built for Australia

Connecting people and assets in remote environments particularly during emergencies demands more than standard commercial connectivity. Cellular dead zones, absent fibre infrastructure, spectrum regulatory constraints, and physical vulnerability to environmental disruption create a complex deployment environment that no single technology can solve alone.

Meeting this challenge requires a hybrid RF architecture that seamlessly integrates public 5G, private wireless networks, push to talk (PTT) radio, and satellite (non-terrestrial) communications. Deploying this infrastructure rapidly, securely, and at scale requires both specialist capability and genuine operational experience.

The Telstra and Cisco alliance is purpose built to deliver exactly this. Cisco's modular industrial routers and SD WAN capabilities enable seamless integration of multiple wireless bearers including Telstra's 4G/5G network and satellite services under a unified, policy driven architecture. This ensures mission critical traffic is always prioritised, security is maintained throughout, and operational continuity is preserved regardless of what the environment demands.

This model is architected to align with Australian jurisdictional standards. By ensuring that infrastructure decisions, data management, and operational control remain within Australia, the solution addresses the core requirements for public safety agencies and regulated critical infrastructure operators.

For OT and IT leaders managing complex, distributed environments, this translates to a network foundation that is not only technically robust but regulatorily aligned and operationally trustworthy.

> ***"Critical infrastructure operators must implement a risk management program that identifies and mitigates risks to the security and resilience of critical infrastructure assets, ensuring continuous, reliable operations."***
>
> *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules 2025 (F2025L00325)*

3. Secure by Design: Compliance and Cyber Resilience Are Not Optional

For public safety agencies and critical infrastructure operators, compliance is foundational not aspirational. Obligations under the SOCI Act demand demonstrable security controls across networks, OT systems, and connected assets. RF spectrum compliance with ACMA adds additional layers of regulatory accountability covering licensing and electromagnetic emissions (EME) safety.

The joint Telstra and Cisco solution is architected to support these obligations from the ground up. Key capabilities include:

- Network segmentation between operational zones, limiting lateral movement in the event of a breach
- Controlled and fully audited remote access across field and OT environments
- Continuous monitoring of connected industrial devices with automated anomaly detection
- Comprehensive logging and reporting to support governance, audit, and incident response requirements
- Reduced attack surface across distributed field networks through zero trust security principles

By deploying Cisco industrial networking equipment within Telstra's managed infrastructure, organisations gain a hardened, audit ready foundation that satisfies Australian regulatory obligations while measurably strengthening their operational and cyber resilience posture.

This is not bolt on compliance. It is security embedded at the architecture level from the first mile wireless connection to the operational edge.

> ***"96% of decision-makers say reliable wireless networks are vital for enabling AI, making it foundational to network readiness at scale."***
>
> *Cisco 2026 State of Industrial AI Report*

4. More Than a Vendor: A Partnership Committed to National Resilience

Technology is only part of the story. What distinguishes the Telstra and Cisco alliance is a shared, demonstrated commitment to Australia's national resilience in the field, not just on paper.

Telstra has a proven track record of restoring communications during Australia's most significant disaster events, including Cyclone Alfred in February 2025. Operating as a trusted national partner embedded alongside Premiers, Cabinet Ministers, and Emergency Service Organisations both in crisis command centres and on the ground in affected communities. This is not a vendor relationship. It is a capability that operates at the heart of Australia's emergency response architecture.

Cisco's global Crisis Response (CCR) initiative brings complementary depth. Established in 2005 following Hurricane Katrina, CCR mobilises nearly 1,000 employee volunteers alongside technology, financial resources, and strategic partnerships to restore critical communications for emergency responders and aid organisations worldwide. The program operates across four pillars: Incident Response, Technology Solutions, Strategic Partnerships, and Capacity Building enabling rapid, coordinated deployment wherever it is needed most.

Together, the alliance brings rapidly deployable connectivity infrastructure including mobile network units and satellite enabled field kits that ensures first responders and infrastructure operators maintain communications when traditional systems are damaged, congested, or compromised.

This shared social responsibility is not a corporate narrative. It is a track record, built incident by incident, across Australia and internationally.

5. The Three Pillars of Capability

5.1 Intelligent Industrial Networks

Modern OT and critical infrastructure environments demand networks that do more than connect they must sense, prioritise, protect, and self heal in real time.

The alliance delivers an Intelligent Industrial Network architecture combining Cisco's ruggedised hardware and embedded cybersecurity with Telstra's carrier grade backbone. This architecture ensures:

- Critical OT and control system traffic is prioritised over non-essential data flows
- Mission critical services voice, data, and video are delivered with deterministic, predictable performance
- Continuous health monitoring across distributed environments provides operational teams with real time awareness
- Automated failover and self-healing capabilities maintain continuous operations during degradation events
- Deep observability delivers actionable insight across converged IT/OT environments

Telstra's nationwide 4G/5G network, including regional and remote coverage, provides the reliable first-mile connectivity that underpins the entire architecture. LANES prioritisation for emergency services and QPP traffic pre-emption ensure that essential communications and OT data are never sacrificed during congestion or crisis events.

Cisco extends intelligent networking into operational environments through its Industrial IoT portfolio enabling secure, segmented connectivity across substations, transport systems, pipelines, water infrastructure, and renewable energy facilities. SD-WAN, zero-trust security, and OT-native visibility give operators end-to-end control across the full IT/OT convergence stack.

The result is a fully integrated architecture, from first-mile wireless access to the hardened industrial edge, purpose-built for the reliability and performance requirements of mission-critical infrastructure.

5. The Three Pillars of Capability

5.2 Sovereign Rapid Deployable Solutions

In disaster scenarios and remote operations, time is the critical variable. The ability to rapidly establish secure, high bandwidth connectivity in environments with no existing infrastructure can be the difference between coordinated response and operational failure.

The alliance provides rapidly deployable connectivity solutions engineered for exactly this environment. These are not off the shelf products they are operationally proven platforms, field tested across energy, mining, emergency services, and public safety deployments. Key capabilities include:

- Application aware routing and dynamic path selection, automatically prioritising MCX voice and video across all available links
- Policy based segmentation from edge to core, extending secure OT zones across cellular, satellite, and fixed WAN simultaneously
- Centralised orchestration and real time visibility across remote sites, vehicles, and temporary field operations
- Resilient SD WAN overlays across multi bearer networks, aligned with Telstra's 4G 5G and satellite services
- Mobile Internet Connectivity Kits (MICK) combined with Telstra Infrastructure Monitoring (T-IM) and Cisco technology, delivering operational insight and secure connectivity within hours of deployment

This deployable capability enables organisations to establish, scale, and manage secure communications wherever needed. Supporting disaster recovery, emergency response, and critical infrastructure continuity without dependency on permanent terrestrial networks.

5. The Three Pillars of Capability

5.3 The True Edge: Vehicle as a Node (VaaN)

The emergency vehicle has historically been a voice endpoint. The alliance transforms it into something far more powerful: a secure, mobile operational hub extending network intelligence, connectivity, and compute capability to wherever the incident is occurring.

By embedding ruggedised Cisco routing and edge compute technology within Telstra connected vehicles, each unit becomes a dynamic node on the national network. Beyond supporting onboard systems, each vehicle creates a local Wi-Fi and mesh LAN environment enabling frontline personnel and volunteers in proximity to seamlessly access WAN connectivity, command systems, and real time operational data without additional infrastructure.

Vehicle-as-a-Node capabilities include:

- **End-to-end network observability:** full visibility into performance, device health, and application usage across distributed fleets
- **Industrial IoT integration:** real-time monitoring of vehicle systems, environmental sensors, and field assets
- **Edge compute capability:** local data processing for rapid decision-making without central system dependency
- **Secure and resilient networking:** Telstra's carrier backbone combined with Cisco security, maintaining protected communications in remote and challenging environments

Every emergency vehicle becomes not just a transport asset, but a mobile observability, compute, and communications node that extends the operational network to the point of need.

6. Workforce Safety and Sustainability: Technology That Works for People

Workforce fatigue and burnout represent growing risks across emergency services and infrastructure operations. If technology adds cognitive load rather than reducing it, adoption fails and frontline personnel are exposed to greater risk.

The alliance is designed with this reality in mind. Through edge compute, intelligent automation, and purpose-built network design, the joint solution delivers:

- Reduced administrative burden through automated data capture and reporting
- Real time overwatch capabilities that enhance officer and personnel safety in the field
- Simplified situational awareness dashboards that present actionable insight without information overload
- Remote diagnostics that eliminate unnecessary site visits and reduce exposure in hazardous environments

Critically, these capabilities are delivered through a seamless end-user experience where connectivity, applications, and devices work intuitively together. Frontline personnel operate without needing to manage underlying technology in high-pressure environments. The network simply works.

By delivering reliable, secure connectivity that reduces complexity rather than adding it, the alliance directly supports workforce safety, operational efficiency, and long-term capability retention.

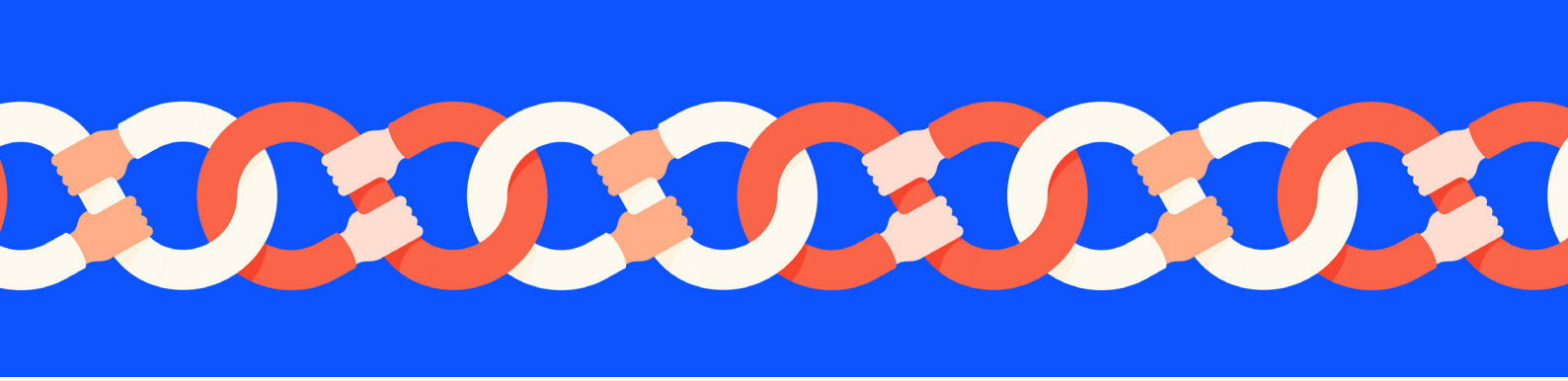
7. A Practical Roadmap: Demonstrate, Deploy, Scale

Public safety and critical infrastructure leaders prioritise mission continuity and operational stability. They require proven outcomes, not theoretical architectures, to guide procurement decisions. The alliance is structured to meet this standard.

Telstra and Cisco operate joint innovation and demonstration facilities across Australia, including the Telstra Muru D innovation centre, which showcases validated architectural blueprints for emergency services, renewable energy zones, mining operations, and remote or complex infrastructure environments.

A centrepiece of this capability is **Telstra Infrastructure Monitoring (T-IM)**, a joint solution combining Cisco industrial connectivity for secure, intelligent routing and switching, Telstra's national network for reliable wide-area coverage, and continuous infrastructure visibility with operational monitoring to support Industrial IoT and public safety use cases.

Cisco's **Country Digital Acceleration (CDA)** program offers a framework for the exploration of structured Proof of Concept engagements. These initiatives evaluate industrial solutions in live environments to gauge potential fit before committing. This "demonstrate, deploy, scale" approach reduces procurement risk, builds internal capability, and creates a pathway to long-term, scalable outcomes.



Conclusion and Call to Action

Australia's public safety and critical infrastructure sectors must move beyond incremental modernisation. Escalating cyber threats, environmental hazards, and strict regulatory obligations demand an immediate step change. These sectors require a sovereign, industrial grade digital foundation that performs reliably under pressure.

The Telstra and Cisco alliance delivers this foundation today. It is a proven, deployable capability backed by two partners committed to Australia's national resilience from the command centre to the field.

Next steps:

Demonstrate. Engage with Telstra and Cisco's innovation facilities to see validated solutions performing in environments that reflect your operational reality.

Deploy. Leverage structured Proof of Concept frameworks to de-risk adoption and build organisational confidence before full-scale rollout.

Scale. Build a sovereign digital backbone that grows with your operational complexity — supporting AI-enabled decision-making, regulatory compliance, and national continuity for the decade ahead.

To arrange a briefing, visit an innovation facility, or initiate a Proof of Concept engagement, contact your Telstra or Cisco account representative today.

Telstra and Cisco

Trusted Partners in Australia's National Resilience.