

IT and the emergency cycle



Introduction

Information technology (IT) is not just a tool, but a lifeline in every stage of the emergency cycle. It is a fundamental pillar of our national resilience, without which the very fabric of our emergency response system would crumble.

For first responders rushing toward danger, having the right information, people and resources can have life-changing consequences. Individual emergency services such as police, firefighters and paramedics have made legacy investments in networking, applications and communications infrastructure to coordinate an efficient and effective response. This infrastructure itself becomes a vector for attack, with potential to impact the entire chain of coordinated services on the ground in an emergency situation if the National Emergency Management Agency's (NEMA) Situation Room in Canberra is compromised. This hub coordinates nationwide emergency responses. Without it, communication breaks down, hindering information sharing, resource deployment and swift emergency responses.¹

Consider a network failure during a flood that compromises real-time software updates on levee conditions. A break goes unnoticed, causing more flooding in low-lying homes and areas, limiting emergency teams of real-time data to coordinate and action responses; and increasing risk.²

Another hypothetical scenario is a category four cyclone damaging critical communications at a hospital and a bushfire causing a hazardous chemical release, requiring network restoration in a danger zone.³

Emergency response plans are therefore a collective sum of public and private IT backup and disaster recovery plans across critical assets:



IT infrastructure: Covering servers, data centres and communication networks essential for emergency operations.

- **Spectrum:** Radio frequencies used for communication are critical for emergency services, including future public safety mobile broadband (PSMB).
- **Power:** Power plants, electrical grids and backup generators must stay operational for the national electricity supply.
- **Water:** Water treatment plants, distribution networks and reservoirs ensure the availability of clean water.
- Transportation: Road and rail networks remain crucial for moving people and goods during emergencies.

Without these plans, first responders and emergency management agencies lack reliable communication channels to coordinate quickly and effectively. Hospitals, power utilities and other critical infrastructures are left isolated – complicating rescue and recovery operations.

First responders can be put under immense mental, physical and emotional distress – often not seeing their families for days or only under the most trying circumstances.⁴

Further, it becomes a matter of national defence, with potentially severe consequences. Armed forces are dispatched to save lives during fires and floods, limiting their availability to respond to other critical threats, such as physical and cyberattacks from nation-states in a volatile geopolitical environment.¹

This white paper urges leaders to reshape emergency management toward IT network transformation. Nearly 200 interconnected critical assets highlight the growing importance and complexity, with Australia investing \$11.4 billion toward becoming the most cyber-physical secure nation by 2030.²

Planning is bringing the future into the present to transform interagency emergency response.

Preparing for the worst brings out our best

When the worst happens, frontline responders require secure, connected and deployable IT frameworks with resilient and rapidly recoverable infrastructure.

At a national level, the federal government is already reengineering its capabilities, teaming with IT to enable more harm mitigation earlier. Over the next decade, public sector investments aim to harden critical infrastructure, making Australia the most cyber-secure nation by 2030.³

A flagship technology in this strategy is renewed leadership and collective action around Public Safety Mobile Broadband (PSMB), with the potential for a 5G rollout to deliver advanced capabilities.

This tech promises secure communication for emergency services while linking ground crews, aerial assets and control centres across various national and local agencies.

Fire, ambulance and police, just to name a few, will be able to access maps, weather data, videos and more. Surpassing current radio network limits will aim to boost coordination, safety and efficiency across Australia.⁴

Chasing extreme situational awareness

Reliable, high-performance network connectivity supports extreme situational awareness for brave responders on the frontlines. Automated devices and software are turning data into public safety intelligence from space to air to ground.

🗞, Satellites

Fire agencies need updates every two minutes for remote incidents. During the Gospers Mountain Fire in NSW in 2019, lightning strikes escalated the number of wildfires from 40 to over 100 in hours, highlighting the criticality of real-time data sharing. Calls are being made for sovereign capability to achieve this, including a global network of satellites equipped with sensors to detect fires as small as a few metres in diameter every 15 minutes.⁵

活 Drones

Closer to Earth, firefighting drones drop combustible fireballs to enhance bushfire preparedness and live stream thermal images to incident command.⁶ During floods, drones⁷ are used for aerial reconnaissance, assessing hazards and safely guiding rescue teams to stranded residents.



📩 Mobile connectivity trucks

On the ground, trucks equipped with radio, 4G/5G and satellite connectivity help ensure uninterrupted communication during network outages.⁸

Power restoration vehicles & mesh networks

Power restoration vehicles restore access to electricity, while advanced mesh networks extend radio communications in typically impaired areas like tunnels or inside buildings. These networks integrate with mobile networks, satellite and other radio frequencies, helping to ensure robust and resilient local connectivity.⁹

Portable communication networks

Quickly establishing a communication network when existing networks are down is critical for conducting an effective emergency response. In the US, the Verizon Rapid Response Connectivity Unit (RRCU) deploys in under 15 minutes, providing satellite and wireless links to establish a private 5G network spanning kilometres. It also offers a Wi-Fi network for nearby personnel, ensuring reliable communication in dynamic environments.¹⁰

The message is clear: Connected frontline responders are safer and more effective when data and information flow more freely before, during and after an emergency cycle.



The frontline edge of safety

The examples above illustrate the shift from centralised IT and cloud architecture to edge and mesh architecture in the emergency cycle, unlocking a further slew of next-generation applications.¹¹

Sensors

This shift integrates IoT (IoT) sensors, like those on levees, that detect water levels and structural integrity.¹² Low-cost flood sensors can also detect changes in water levels, providing real-time data through edge and mesh architecture.¹³ Unmanaged vegetation near power lines causes forest fires, alerting sensors and real-time image analytics to send data back to responders, enabling them to quickly monitor areas remotely and address issues.¹⁴

Digital twins

Floodwaters pouring into a hospital can also activate IoT sensors and inform AI-powered digital twins, which create virtual models of the building. They can assess damage and plan evacuations in real time. Patients are safer as first responders receive instant updates, allowing them to move quickly and provide faster triage.¹⁶

The defence sector uses digital twins for strategic planning, such as simulating an entire city's infrastructure, including plumbing, information and communication technology (ICT) and public amenities. This approach allows for modelling different scenarios and their impacts, such as floods, fires or other black swan events, including a terrorist attack.¹⁷

Immersive training

Stress levels surge in emergencies, demanding well-trained frontline workers. Yet, providing this essential training is often costly and challenging.

If digital twins replicate hospital environments, augmented reality (AR) and virtual reality (VR) can immerse users in these virtual replicas for training.

With the combined power of 5G and multi-access edge computing (MEC), public safety agencies can create virtual environments that simulate real-world situations.¹⁸

Inside these virtual worlds, responders build confidence for high-stress situations, like rescuing people from rooftops during floods or entering smoke-filled hospitals during fires.

Take a human-centred approach

When an emergency agency can successfully assign a low-cost task to volunteers in small boats (tinnies) to rescue a family during a flood rather than deploying a highcost asset such as a helicopter, it demonstrates optimal resource allocation.

This example reflects efforts to build a multi-agency, multihazard¹⁹ approach to emergency management that is always connected and interoperable among emergency services, including community agencies like Lions Clubs, Rotary Clubs²⁰, Apex Clubs, volunteers, RSL clubs, and individuals responding to floods and fires.

IT systems provide real-time data and analytics, giving emergency leaders the tools and systems to direct volunteers and bring us closer to this outcome. Every neighbour, emergency responder and state official is committed to staying connected and applying the right solution at the right time during planning, response, and recovery.

Not only are costs lowered, but agencies operate more efficiently and effectively at lower stress levels while improving mental health outcomes.

This approach is reaching a high degree of maturity in certain states like Victoria as community members become more integrated into emergency response efforts.²¹

When Danielle Eyssens, a community volunteer, receives Level 3 incident management certification, it highlights how far we have come. Using the VicEmergency app, she can coordinate real-time updates, allocate resources efficiently, and communicate seamlessly with other responders.²²

These certifications build leadership and help volunteers like Eyssens stay mentally strong and ready. This means she has the skills to handle challenging situations, like rescuing families during floods.²³

The unpredictable nature of these events takes a toll on all joint responders, including relief volunteers.

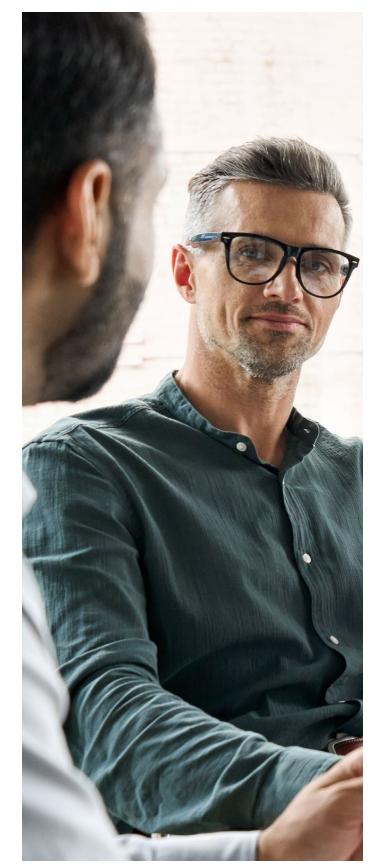
Today, there are more than 370,000 emergency workers in Australia, and around one in 10 develop post-traumatic stress disorder (PTSD), showing us how important the issue of mental health has become.²⁴

When a volunteer or responder cannot save a home or a life, moments of helplessness, guilt, and shame arise.

The Victorian Emergency Management Reform White Paper highlights how technology supports mental health during emergencies. IT systems enable telehealth counselling and online support groups, ensuring people can access mental health help even in remote or disaster-hit areas.²⁵

The paper also stresses the importance of agencies working together. By collaborating, different organisations and community groups provide more vital mental health support for emergency workers and affected communities.

This teamwork ensures comprehensive care and helps reduce stress for everyone involved.



Data-driven interagency coordination

Secure interagency coordination is crucial – for instance, police and fire units decide if a property is safe or ready for re-evaluation after a fire.

Individual agencies are now responsible for independently managing and securing their IT networks and cyber capabilities, including secure internet gateways (SIGs) that protect government systems from the public internet during an emergency.

Pressure mounts to meet interoperability requirements and comply with Australian security standards, such as the Information Security Registered Assessors Program (IRAP) and the Australian Signals Directorate (ASD) Information Security Manual (ISM).

Legacy networks may fail in disasters like floods, cyclones or fires, necessitating deployable assets and secure networks that can integrate without compromising critical services such as police or defence.

For a business like a dairy, minimising damage might require collaboration across various stakeholders—including farmers, veterinarians, truck drivers and milk tanker operators—all needing timely access to resources like power, water and communication for everything from animal welfare to urgent repairs.²⁶

During the Australian bushfires, emergency services like police escorted milk tankers to dairy farms, ensuring milk could be collected despite road closures and fires, preventing significant losses. Emergency supply chains faced considerable strain, with some farmers losing over 50 hours of milking time.

Additionally, the lack of aircraft and limited vehicle capabilities hampered firefighting efforts, highlighting the complex challenges in maintaining public safety and critical agricultural operations during such crises.²⁷

Former Victorian Fire Services Commissioner, Craig Lapsley, emphasises²⁸ the increasing complexity of such operations and the need for federal agencies to optimise coordination, which is only possible through reliable underlying IT systems driving a unified communication fabric.

The approach acknowledges that major utilities, cyber outages or natural disasters do not confine themselves to the borders defined by state organisations like ACT Emergency Services Agency, Northern Territory Emergency Service, NSW Office of Emergency Management and others across Australia.²⁹ The growing hyperconnected nature of the intraagency response also means agencies vary in data maturity.

The Royal Commission into National Natural Disaster Arrangements notes that some IT systems and data analysis tools are cutting-edge, yet neighbouring jurisdictions use different data or platforms during emergencies.

Following the discontinuation of the federal government's cyber hubs pilot in 2023³⁰, the amount of data available for harvesting and analysis siloed in legacy systems, offline spreadsheets, or emerging platforms and apps may also overwhelm cost-sensitive, understaffed agencies.

Here are just five examples of the extensive data sources referenced in the Royal Commission report:³¹

- State emergency apps: Data from apps like NSW's Fires Near Me and VicEmergency
- Navigation apps: Information from Google Maps, Apple Maps and Waze
- Energy providers: Risk assessments using LiDAR and smart metre data
- Air quality monitoring: Real-time data from sensors with one-hour averaging periods
- Infrastructure systems: Data on road closures and damage from systems like Live Traffic NSW³²

The big challenge for multiagency disaster response is making these different applications work together.

Instead of forcing everyone to use the same system, they need to be able to talk to each other.

IT enables this interoperability goal while allowing the best parts of each system to be used, building on the great work already being done in each area.



A fit-for-purpose defence force

Civilian agencies face overwhelming challenges during large-scale crises, a gap the Defence Assistance to the Civil Community (DACC) initiative bridges by uniting military precision with civilian compassion.³³

Yet, recent heavy deployments of the Australian Defence Force (ADF) in domestic disasters involving over 35,000 personnel for tasks like the Lismore floods in 2022 signal a potential imbalance in this pact.

A deployment to Lismore's floods peaked at 8,000 personnel and lasted for months, with a minister warning, "Defence should be the force of last resort for domestic aid to the civil community, except in extreme circumstances."³⁴

Such extensive military involvement raises concerns about compromising the ADF's primary warfighting capabilities, suggesting that the civil sectors might not be fully upholding their end of shared responsibilities.

The current state stresses the ADF and hints at IT gaps in civilian preparedness and response strategies, challenging the integrity of our national resilience framework.

National disaster response for Australia

The government has spent billions on rebuilding key public assets like roads through the Natural Disaster Relief and Recovery Arrangements (NDRRA). This shows a focus on fixing damage rather than preventing it.³⁵

This imbalance is critical; with over 18 million Australians³⁶ hit by natural disasters in a nation experiencing a cyberattack every 6 minutes, public trust is at a premium.³⁷

"Australians expect their political leaders to show up when disaster strikes," says former federal minister for emergency management, Murray Watts.

Watts' centralisation of disaster response under the National Emergency Management Agency (NEMA) shows renewed energy for improving cooperation and preparedness between national, state, local, and civilian agencies.

The agency's nerve centre operates from the National Situation Room (NSR), which functions 24/7 beneath the Australian Federal Police headquarters in Canberra.

This team monitors threats from weather events to cyberattacks, directly connecting with state and territory emergency centres and expanding during crises to include federal, state and private sector representatives.³⁸

NEMA's data strategy, a direct outcome of the Royal Commission report, involves rolling out a hub-and-spoke model to centralise multi-agency data in a secure data warehouse.

The National Joint Common Operating Picture (NJCOP) relies on this centralised data to provide a unified, immediate view of all hazard incidents across Australia. Analysts view a nearreal-time dashboard depicting all hazard incidents on a single display. Critical decisions are made based on the integrated data from sources such as the Bureau of Meteorology (BoM), Australian Public Service agencies, state and territory counterparts, NGOs and the private sector.³⁹

The intent is to provide a single source of truth for data related to warnings, bushfire advisories, cyber incidents, power failures and telecommunications outages.

Other efforts are underway to overhaul the disaster management framework:

- Disaster Ready Fund (DRF): This fund provides access to a \$1 billion fund to enhance disaster readiness over five years.⁴⁰
- National Emergency Management Stockpile (NEMS): Provides crucial emergency supplies.⁴¹
- Fire Danger Rating System⁴², Climate Service Warning System⁴³: These systems improve fire ratings, climate forecasting, and public warnings
- Office of Supply Chain Resilience (OSCR)⁴⁴: Safeguards essential supply chains during emergencies

This strategic shift reflects a more profound, earlier collaboration among various agencies, including the Bureau of Meteorology and the Department of Foreign Affairs, under a cohesive, proactive NEMA framework.

It's a call to action for all sectors to reevaluate and strengthen their roles in national resilience based on data exploding on reliable, secure IT networks.



IT enables it all

Without persistent connectivity, NEMA and these new agencies would face significant challenges in managing intricate response scenarios for a nation spanning over seven million square kilometres.⁴⁵

Secure communication is crucial for efficient coordination, information sharing and resource deployment during emergencies in an arena where natural and man-made disasters are becoming increasingly complex, unpredictable, and challenging to manage.

We are likely to see more compounding disasters nationally with far-reaching consequences. These may involve multiple hazards-fires, floods, cyber-attacks, terrorism and storms-occurring simultaneously or sequentially, creating cascading effects that threaten lives, homes, the economy, and critical infrastructure. ⁴⁶

Whether a power disruption prevents healthcare systems from operating, a fundamental grid failure impacts emergency response systems, or traffic systems go down, agencies need to securely share real-time data with each other and with national coordination bodies like NEMA.

Data sharing, however, is only possible when different systems, devices, and organisations work together interoperably within and across organisational boundaries to fulfil this goal.

For instance, NEMA tackles data security with a strong data governance plan, clear data handling policies, secure sharing agreements, automated processes to reduce mistakes and strict privacy and risk management rules to protect data.⁴⁷

Added challenges to this goal include vast geographic coverage gaps, high costs of nationwide cellular expansion, reliance on unreliable two-way radios, atmospheric interference for satellite and rugged terrain blocking signals.⁴⁸

An earlier Infrastructure Australia audit captures the stakes: "Our emergency services infrastructure is not adapting to changes in the nature and rate of emergencies. Without action, emergency services infrastructure that is not fit for purpose for the changing nature of emergencies will reduce access to life-saving services, particularly in rural communities and remote areas." ⁴⁹

Degraded infrastructure invites cyber risk

The recent severe cyberattack on Fire Rescue Victoria (FRV) forced a manual approach to managing the emergencies.

Teams relied on pagers and mobile phones - extending response times and stretching responders to operational limits.

In the three months following the cyberattack, FRV fell short of its goal by more than ten percentage points, failing to reach 90% of structural fires within 7.7 minutes, as reported in the quarterly performance reviews by the independent fire service monitor.⁵⁰

Preparedness strategies must leverage a cybersecurity framework that defends and swiftly restores functionality to essential emergency systems.

This includes adhering to global standards like ISO 27001, NIST, and COBIT and specific Australian standards such as

the ASD Information Security Manual and IRAP certifications for protected data. $^{\rm 51\,52}$

Understanding and following these standards and implementing SIGs takes agencies closer to securing platforms, software and users.

With renewed government action around infrastructure upgrades and security, doors open to transform the IT network toward interoperability and data sharing. Every dollar spent on public infrastructure can significantly increase Gross Domestic Product (GDP), adding up to \$4 of value over the asset's life.⁵³

Public-private partnerships

The 20th Century American humanitarian, author and educator, Helen Keller, once famously stated, 'Alone we can do so little; together, we can do so much.'

During the COVID-19 pandemic, global airports stood empty, with 612 million fewer passengers in the first quarter of 2020 alone.

Australia's Department of Foreign Affairs and Trade (DFAT) partnered with Verizon to help secure Australia's International COVID-19 Vaccination Certificate.

Together, we designed, built and supported digital signing solutions and scaling capabilities to meet the demands of millions of signatures per annum.

This joint initiative has enabled up to around 2,000 certificates to be signed per second, in line with a high level of integrity and security.

To date, over 10 million Australian travellers have activated the certificate using a Medicare account, myGov, or the Medicare Express app. Verizon solutions support real-time digital signatures, which has been important in protecting the integrity of passports and vaccination certificates.

Verizon supports 98 federal agencies in Australia, and we intimately understand the DFAT mandate: Securing data is as crucial as securing physical borders.

Today, over 10 million Australian travellers are protected and activate the certificate using a Medicare account, myGov, or the Medicare Express app. Verizon solutions support real-time digital signatures, which have proven invaluable in protecting the integrity of passports and vaccination certificates.

It sets a new benchmark in securing data at scale as Australia grapples with privacy and data sovereignty issues in an unstable geopolitical climate.⁵⁴

Partnerships also free up public safety agencies to test next-generation private 5G and satellite connectivity technology that mirrors real-world emergencies in the field.

The possibilities are endless, but here are a few examples of hypothetical joint-training scenarios from the United States:

Power grid failure

During a remote power grid failure, the Rapid Response Connectivity Unit (RRCU) swiftly weaves through fallen trees and narrow spaces to restore communication. First responders use its 5G and satellite links to locate and rescue a trapped resident, ensuring swift coordination despite the blackout.⁵⁵

Cyclone damage drones

After a cyclone hits, agencies deploy advanced drones with 4K cameras and real-time data links to capture images of destroyed homes and blocked roads. The data is quickly and securely sent to the weather service, helping to locate survivors and improve future storm warnings.⁵⁶

Nuclear zone rescue

Response teams work alongside the armed forces in a nuclear zone caused by a tornado, using portable cell sites and drones to restore network communication. WiFi hotspots aid safe communication and evacuation in hazardous areas.⁵⁷

These scenarios illustrate how a modernised IT network can ensure uninterrupted communication during outages, supporting emergency and critical operations.

Protecting these expanded attack surfaces requires collaborating with accredited Gatekeeper service providers

for the Australian government and supporting Public Key Infrastructure deployments in government, property, and healthcare industries.

As NEMA rolls out its data-sharing vision towards 2030, it will require the highest-calibre technology partners with deep expertise in global standards like ISO 27001, NIST, and COBIT, as well as specific Australian standards such as the ASD Information Security Manual and IRAP certifications for protected data. ^{58 59}

These measures collectively reinforce Australia's sovereign capability by ensuring that essential services and IT infrastructures remain secure, resilient, and under national control.

Learn more

Discover why 98 federal agencies trust Verizon for digital preparedness and empowerment. Contact your Verizon Agency Account Representative or email apaccontactus@verizon.com to learn more.

Endnotes

- www.defence.gov.au/news-events/news/2023-12-22/adf-provides-flood-assistance-north-queensland
- 2 www.cisc.gov.au/how-we-support-industry/events-and-outreach/cyber-and-infrastructure-security-conference-2023
- 3 budget.gov.au/content/03-future-made.htm
- 4 nema.gov.au/sites/default/files/inline-files/Public%20Safety%20Mobile%20Broadband%20%28PSMB%29%20-%20Program%20Fact%20Sheet%20-%20December%202023.pdf
- 5 www.innovationaus.com/space-based-earth-observation-brings-extreme-fires-into-focus/
- 6 fire.nsw.gov.au/news.php?news=2431
- 7 www.fire.nsw.gov.au/incident.php?record=1646398800
- 8 fire.nsw.gov.au/news.php?news=2431
- 9 fire.nsw.gov.au/news.php?news=2431
- 10 www.verizon.com/about/news/verizon-frontline-debuts-two-newest-deployable-asset-prototypes
- 11 www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends
- 12 www.digital.nsw.gov.au/sites/default/files/2022-09/iot-policy-guidance.pdf
- 13 www.iothub.com.au/news/when-minutes-save-lives-iot-delivers-earlier-flood-warnings-592626
- 14 www.youtube.com/watch?v=w6EyQMIqsyg
- 15 www.youtube.com/watch?v=w6EyQMIqsyg
- 16 azure.microsoft.com/es-es/blog/using-ai-and-iot-for-disaster-management/
- 17 www.innovationaus.com/bridging-the-physical-and-virtual-worlds-with-digital-twins/
- 18 www.verizon.com/business/resources/5g/5g-business-use-cases/public-sector/immersive-tactical-training/
- 19 files.emv.vic.gov.au/2021-07/Victorian-Emergency-Management-Reform-White-Paper-Dec-2012.pdf
- 20 hilobayrotary.com/stories/community-emergency-response-team
- 21 hilobayrotary.com/stories/community-emergency-response-team
- 22 emergency.vic.gov.au/news-and-media/opening-doors-danielle-eyssens-on-becoming-the-first-vicses-volunteer-to-achieve
- 23 files.igem.vic.gov.au/2021-03/Publication%20Review%20of%20incident%20management%20teams_%20accreditation%20and%20rostering.PDF
- 24 www.smh.com.au/lifestyle/health-and-wellness/one-in-10-emergency-workers-develops-ptsd-finally-help-is-on-its-way-20240326-p5ff86.html
- 25 files.emv.vic.gov.au/2021-07/Victorian-Emergency-Management-Reform-White-Paper-Dec-2012.pdf
- 26 www.youtube.com/watch?v=w6EyQMlqsyg
- 27 www.theguardian.com/australia-news/2020/jan/03/australian-dairy-farmers-shore-up-supplies-as-they-prepare-for-bushfire-flashpoint
- 28 knowledge.aidr.org.au/resources/ajem-apr-2011-opinion-fire-services-commissioner-for-victoria/
- 29 knowledge.aidr.org.au/resources/key-groups-and-organisations/
- 30 www.itnews.com.au/news/home-affairs-to-migrate-austrac-acic-out-of-cyber-hub-596140
- 31 www.royalcommission.gov.au/system/files/2020-12/Royal%20Commission%20into%20National%20Natural%20Disaster%20Arrangements%20-%20Report%20%20&5Baccessible%5D.pdf
- 32 www.livetraffic.com/
- 33 www.defence.gov.au/defence-activities/programs-initiatives/defence-assistance-civil-community-initiative
- 34 www.theguardian.com/australia-news/2023/sep/14/adf-australian-defence-force-natural-disasters-response-could-degrade-fighting-ability
- 35 www.pc.gov.au/inquiries/completed/disaster-funding/report/disaster-funding-volume1.pdf
- 36 www.smh.com.au/politics/federal/disasters-hit-18-million-australians-and-the-number-is-growing-20230915-p5e4z7.html
- 37 www.sbs.com.au/news/podcast-episode/new-cybercrime-reported-in-australia-every-six-minutes-and-its-getting-worse/rm217tkww
- 38 www.smh.com.au/politics/federal/floods-fires-and-more-floods-murray-watt-has-had-a-busy-year-20231212-p5eqyg.html
- 39 www.smh.com.au/politics/federal/floods-fires-and-more-floods-murray-watt-has-had-a-busy-year-20231212-p5eqyg.html
- 40 nema.gov.au/disaster-ready-fund
- 41 nema.gov.au/sites/default/files/inline-files/budget-2024-25-factsheet-national-emergency-management-stockpile.pdf
- 42 afdrs.com.au/
- 43 www.acs.gov.au/
- 44 www.industry.gov.au/trade/office-supply-chain-resilience
- 45 www.ga.gov.au/scientific-topics/national-location-information/dimensions/australias-size-compared#:~:text=Australia%20is%20the%20planet's%20sixth,is%20the%20world's%20largest%20island.
- 46 www.royalcommission.gov.au/system/files/2020-12/Royal%20Commission%20into%20National%20Natural%20Disaster%20Arrangements%20-%20Report%20%25Baccessible%5D.pdf
- 47 nema.gov.au/sites/default/files/inline-files/NEMA%20Data%20Strategy%202023-25.pdf
- 48 www.themandarin.com.au/245670-enabling-a-response-to-disasters-in-remote-australia/
- 49 www.infrastructureaustralia.gov.au/sites/default/files/2019-08/Australian%20Infrastructure%20Audit%202019%20-%200.%20Executive%20Summary.pdf
- 50 www.theage.com.au/politics/victoria/hack-attack-sparked-months-of-delays-for-firefighters-20240404-p5fhb6.html
- 51 www.verizon.com/business/en-au/solutions/australian-government-solutions/
- 53 www.infrastructureaustralia.gov.au/sites/default/files/2019-08/Australian%20Infrastructure%20Audit%202019%20-%200.%20Executive%20Summary.pdf
- 54 www.verizon.com/business/resources/casestudies/beyond-borders-how-dfat-and-verizon-keep-travellers-safe-in-a-connected-world.pdf
- 55 www.verizon.com/about/news/verizon-frontline-connects-utah-first-responders
- 56 www.verizon.com/about/news/verizon-frontline-noaa-partner-advanced-disaster-response-research
- 57 www.verizon.com/about/news/verizon-partners-us-military-extreme-training-prepare-natural-disaster-response
- 58 www.verizon.com/business/en-au/solutions/australian-government-solutions/
- 59 www.verizon.com/business/resources/reports/securing-critical-infrastructure.pdf

52 www.verizon.com/business/resources/reports/securing-critical-infrastructure.pdf



© 2025 Verizon. All rights reserved. The Verizon name and logo and all other names, logos and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners. 03/24