FRONTIER SI

A TIME AND A PLACE FOR RESILIENCE

BUILDING RESILIENCE INTO POSITIONING, NAVIGATION AND TIMING SERVICES FOR AUSTRALIA

RECOMMENDATIONS FOR GOVERNMENT POLICY TO BETTER SUPPORT THE USE OF PNT SERVICES IN THE AUSTRALIAN ECONOMY

March 2024

Joshua Critchley-Marrows, Eldar Rubinov, Phil Delaney, Jia Lee, Alex Linossier

Introduction

This report provides insight into the perspectives of Positioning, Navigation, and Timing (PNT) services within the government of contemporary Australia. It complements the Resilient PNT roadmap outlined in the white paper and consolidates input from a comprehensive review of various public Australian Government policy documents and interviews with experts.

After careful consideration of the PNT context and definitions of resilient PNT, a review of PNT within critical market sectors of Australian society is made. These include maritime, automotive, meteorology, aviation, agriculture, and telecommunications. It also provides a review of critical infrastructure, critical technologies, defence, and foreign affairs in the Australian context. The report concludes with providing recommendations for the next steps for Australia.

It should be noted that given information restrictions in place regarding topics related to Defence, the discussion of defence insights is restrained and brief.

Australia's PNT Context

Positioning, Navigation, and Timing (PNT) technologies are integral to modern Australian society. The services that the Global Positioning System (GPS) provides, which include not only positioning but also precise time synchronisation, have been adopted and intrinsically interwoven in the fabric of most market sectors, including automotive, financial, telecommunication, maritime, aviation, and energy. However, GPS is an asset provided freely to the world by the US Air Force, with command and control held tightly by the military. Studies from Australia, the UK, Europe, Canada, and the USA, some inspired by this lack of sovereignty, have placed a value on the services that GPS and similar systems provide, supporting economic activity exceeding billions of dollars per day.

However, in recent years, the number of radio frequency (RF) and Global Navigation Satellite Systems (GNSS) signal failures and attacks that have taken place, both on-ground and in-space, has increased. Satellite core subsystems have failed, needing replacement; the European-owned GPS ground facility experienced a week-long outage; and in April 2023, the Inmarsat satellite signal delivering Australia's PNT augmentation service, as well as several commercial GNSS correction services, went down, affecting agriculture and maritime sectors which depend on the signal, with degraded or disrupted services.

Targeted signal attacks against GPS and other GNSS signals have been reported across all regions of the globe, even being detected, and characterised as a daily occurrence. Regions across Europe, America, the Middle East, Africa, and Asia have recorded multiple jamming and spoofing attacks against navigation signals. Qantas pilots have reported frequent navigation signal disruptions across Asia-Pacific Sea routes in recent months, presenting safety of life risks to passengers and crew.

Cyber-attacks have also attempted to disrupt supporting infrastructure on multiple occasions, where US Space Force command have made alarming statements regarding an increasing number and growing sophistication of threats. As geopolitical tensions continue to rise globally, the risk of a breach and disruption to global services increases.

The threats to PNT services are not just taking place on Earth, but also to the space assets themselves. A growing number of examples have raised the issue of space assets being a common target of attack by ground-based lasers and RF jammers. Recent statements by the US Space Force General make this strongly apparent [1]. Additionally, numerous recent missile and anti-satellite weapon tests highlight the vulnerability of GPS and similar system infrastructure. System weaknesses and failures have also been reported by GPS-like space infrastructure, disrupting services for weeks.

A compilation of recent events which directly and indirectly threaten Australia are summarised in Table 1. It should be noted that it only includes attacks and failures that have been publicly disclosed and published. Given security risks and saving of public face, many incidents would be only privately disclosed. Each though highlights the risks of GNSS, not only local to the user, such as jamming and spoofing, but also to the infrastructure.

Table 1 - Recent attacks and failures to GNSS signals and infrastructure published in media.

Target	Impact	Region	Source
Jamming and spoofing across the Middle East and Ukraine confound civilian pilots, including Qantas	Disruption and safety risks to air traffic	Russia, Ukraine, Middle East	*New York Times* (2023)
Russia performs anti-satellite missile test capable of impacting GPS	Heightened risk of GNSS failure, disrupting global economy	Russia	*Inside GNSS* (2021)
Iran jams GPS on ships in Strait of Hormuz	Disruption and safety risks to shipping and maritime	Persian Gulf	*GPS World* (2019)
GPS jamming and spoofing attacks creating circular patterns in the Port of Shanghai	Disruption and safety risks to shipping and maritime	China Sea	*The Maritime Executive* (2019)
Australian Qantas pilots subject to GPS jamming from supposed Chinese warships	Disruption and safety risks to air traffic	China Sea	*Australian Aviation* (2023)
GPS jamming disrupts Australian motocross	Disruption to events and surrounding area, including motorists and critical infrastructure	Melbourne	*CNET* (2013)
SBAS outage significantly affected trust and operations in agriculture and shipping	Disruption and safety risks to shipping and maritime Disruption to farmers and mining	Australia	*ABC* (2023)
Nine Galileo satellite clocks have stopped working	Heightened risk of GNSS failure, disrupting global economy	Europe	*BBC* (2017)
Multiple timing issues have been experienced with GLONASS satellites	Heightened risk of GNSS failure, disrupting global economy	Russia	*ICONCOX* (2013)
Three atomic clocks fail on Indian regional GNSS NAVIC	Heightened risk of GNSS failure, disrupting global economy	India	*GPS World* (2017)
GPS ground infrastructure is hacked every day	Heightened risk of GNSS failure, disrupting global economy	USA	*New York Times* (2023)

An illustration of the key threats and vulnerabilities that can affect GNSS infrastructure is shown in Figure 1. As is highlighted, vulnerabilities of GNSS are present in all elements of the system. An important consideration is that most of these issues are outside of Australia's control, as all GNSS assets are neither owned nor operated in Australia[1]. Only the effects that take place at the user end can be prevented or mitigated by Australia. GNSS can also be subject to service availability, where foreign actors can select certain services based on the present geopolitical environment.

Supporting infrastructure, such as the SouthPAN Space-Based Augmentation System (SBAS), managed by Geoscience Australia (GA) and Land Information New Zealand (LINZ), cannot operate without GNSS availability. In addition, it should be noted that this is a service agreement with Lockheed Martin Australia, using a satellite from UK-based Inmarsat. It is built using infrastructure, such as ground stations and central processing facilities, in Australia and New Zealand.

[1] GNSS assets refer to the systems, and supporting infrastructure, of foreign nations and institutions, i.e. Galileo, GPS, Beidou, GLONASS, Michibiki/QZSS and NavIC/IRNSS.

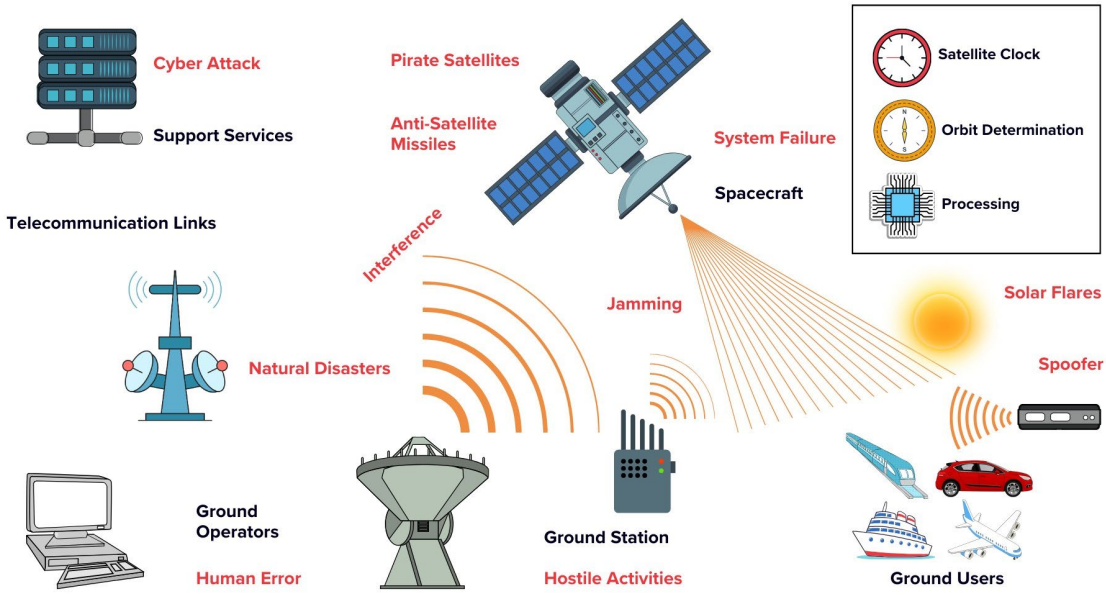

Figure 1 - PNT system architectural components, with threats and vulnerabilities highlighted in red.

International Efforts towards Resilient PNT

Given the highlighted risks and threats to GNSS, many nations have undertaken research and adopted policies that aim to strengthen GNSS and PNT availability. Those that are publicly accessible are summarised in Table 2. They incorporate many facets of ensuring resilient PNT, from detecting and identifying sources of jamming and spoofing to providing alternative PNT services and providing conformance frameworks of the PNT system. Each of these items is unique to each country, but all are necessary to ensure resilient PNT. Australia has not published any policy document explicit on this topic but is motivated by policies in other areas.

Table 2 – International PNT policy and original research.

PNT Policy, Roadmap or Original Research	Country	Year
GNSS Jammer Risk Management	Canada	-
Positioning, Navigation and Timing (PNT) Canadian Risk Assessment and Risk Mitigation Assessment Project	Canada	2021
GNSS PNT Economic Value and Disruptions Cost Study	Canada	2022
GNSS PNT Infrastructure Requirements for Automation in the Transportation Sector	Canada	2023
China's BeiDou Navigation Satellite System	China	2016
China Satellite Navigation and Location Service Industry Development White Paper	China	2022
14th Five-Year Plan for National Informatization	China	2022
European Radio Navigation Plan	European Union	2018
European Union Space Strategy for Security and Defence	European Union	2023
Assessing alternative positioning, navigation, and timing technologies for potential deployment in the EU	European Union	2023

PNT Policy, Roadmap or Original Research	Country	Year
Indian Satellite Navigation Policy	India	2021
Policy on Satellite Positioning	Japan	2021
Main Directions for the Development of Radio Navigation Systems of the CIS Member States for 2019-2024	Russia / CIS	2019
National Space Program Strategy Document	Türkiye	2023
Satellite-derived time and position: a study of critical dependencies	United Kingdom	2017
Economic impact to the UK of a disruption to GNSS	United Kingdom	2017
Government Policy Framework for Greater Position, Navigation and Timing (PNT) Resilience	United Kingdom	2023
Space-based PNT Technical Concepts	United Kingdom	2023
Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services	United States	2020
National Research and Development Plan for Positioning, Navigation and Timing Resilience	United States	2021
A Resilient Architecture for the Realization and Distribution of Coordinated Universal Time to Critical Infrastructure Systems in the United States	United States	2021
Complementary PNT and GPS Backup Technologies Demonstration Report	United States	2021
Resilient PNT Conformance Framework	United States	2022
Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture	United States	2022
Federal Radio Navigation Plan	United States	2022
Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services	United States	2023

What is ‘Resilient PNT’?

Vulnerabilities and security regarding PNT have been discussed since the inception of the GPS and the release of a public service by the US Air Force. Vulnerabilities most under discussion were signal disruption or manipulation by other communication sources, taking advantage of widely distributed technical information and the low power of the transmitter. Since then, GPS, as well as other GNSS systems, have been integrated into every sector of modern society, with a strong dependence on the services now offered. The increasing adoption however has seen a rise of many other threats and risks to these services.

This topic has seen growing attention from the international community. A report published by the University of Sydney and the University of Tokyo reviewed the approach of eleven spacefaring / space-dependent countries: United States, Canada, the European Union, Russia, the United Kingdom, India, Japan, Australia, Türkiye, China and South Korea [2]. A central theme of the report is defining the challenge that PNT faces, and what terminology is associated. Numerous terms were identified, including assured, robust, augmented, and alternative, but the most common and all-encompassing term was resilience. The definitions concluded in the report are illustrated below.

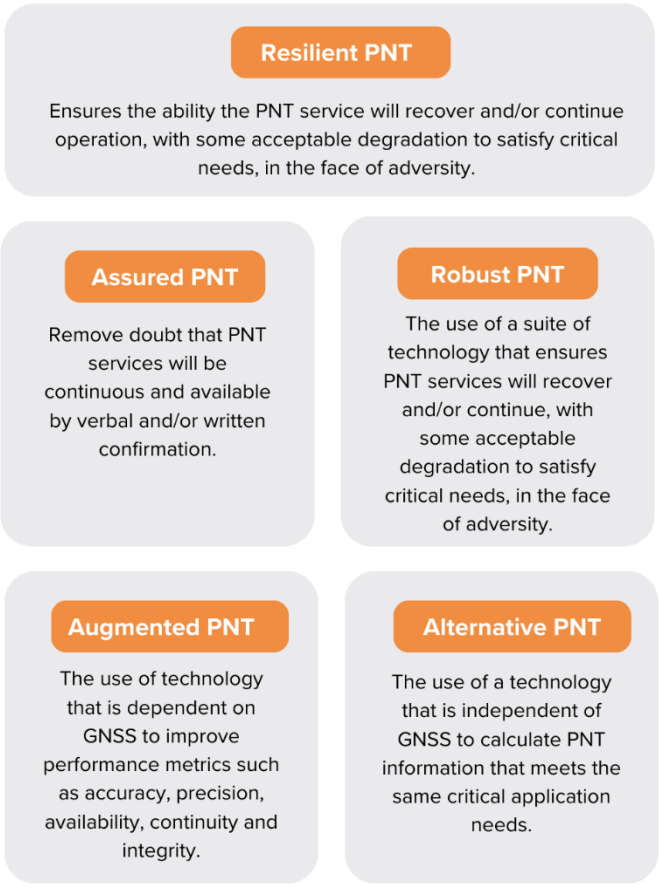

Figure 2 - Various themes and definitions of Resilient PNT [2].

As mentioned, the present report encompasses various interviews and perspectives from experts. Resilience is a common topic for critical sectors and systems beyond PNT. The authors understood the following consolidated definition of 'resilient PNT' by experts, from an Australian perspective, based on their own experience within each of their domains:

Ensure the ability of PNT services to withstand and recover from disruption, both natural and man-made, to provide availability and continuity, and encourage trust.

Components to 'Ensuring' Resilient PNT

The Tokyo-Sydney report [2] also consolidated methodologies from global perspectives on PNT resilience into nineteen core components, that would each form part of any resilient PNT programme. As resilient PNT is a universal challenge, where the technology and use cases are common to each nation, it is seen that the roadmap for Australia would also include these elements. Having said that, the solution delivered would be unique, given Australia's remote location on the globe, sparse population, and resource-dependent economy. Each of the components is illustrated in

Figure 3. These components are analysed in the context of Australia later in this report.

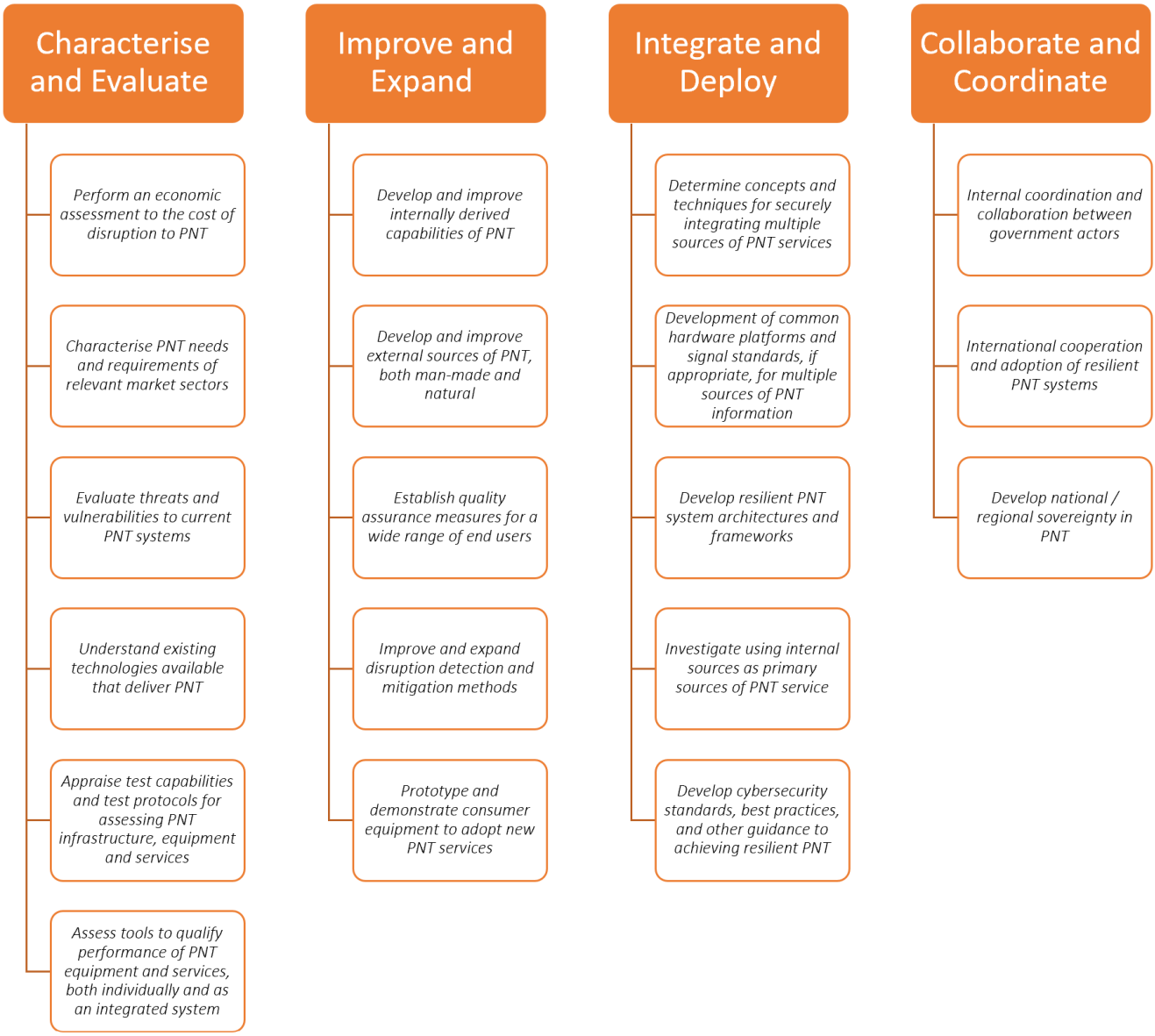

Figure 3 - Activities to ensure a nation's or region's PNT services are resilient [2].

PNT for Australia

This section explores perspectives of PNT across critical sectors in the governance of Australia, and how the resilience of PNT intersects with policy. Policy recommendations are made where appropriate, as well as a general highlight of why the sector needs resilient PNT. References are made to policy documents and the literature for all statements unless an opinion from experts is referred to.

PNT and Critical Infrastructure

Australia's Security of Critical Infrastructure (SOCI) Act 2018 was established to create a framework for the regulation and protection of critical infrastructure sectors [3]. Recent reforms in response to growing cybersecurity threats place an obligation on critical infrastructure owners and operators to be responsive to and protect against threats. The Act currently includes eleven critical infrastructure sectors and twenty-two asset classes.

The only reference to PNT in the SOCI Act is as an example of a space-related service in the Space Technology sector of the Australian economy, where it is written as a 'position, navigation and timing services in relation to space objects.' However, for Australia, space object-based PNT is foreign-owned and operated, and even then, it is viewed that the SOCI Act cannot ever explicitly include satellites, being seen as outside of Australia's borders and hence jurisdiction. Currently, the SOCI Act Space Technology sector contains no underlying assets, and according to experts, the sector is introduced so the Act can 'be ready' as the technology matures.

Another note is that according to the Telecommunications Act 1997 – Sect 360Q, 'if the carriage service is supplied using a satellite', then the following does not apply: 'The eligible service must enable the carriage service provider to supply, to end-users at premises in the service area, carriage services that can be used by those end-users to make and receive voice calls' [4]. In its current form, since PNT cannot make and receive voice calls, the assured delivery of PNT satellite signals is also not required under the Telecommunications Act, despite PNT signals meeting the definition in the Act of a carriage service. PNT could also be included in the Communications Sector of the SOCI Act as a critical broadcasting asset, and this may be related to both PNT data or PNT augmentation data, where augmentation refers to data that improves PNT performance.

The role of the Cyber and Infrastructure Security Centre (CISC), within the Department of Home Affairs, is to enhance the security and resilience of Australia's critical infrastructure and systems of national significance through coordination. Under legislation, industry is required to complete risk assessments by a process of self-assessment. Many hazards are reviewed, including those relevant to space such as cyber threats, supply chain disruptions, PNT vulnerabilities and space weather phenomena. They are also obligated to provide operational information and risk management plans. The CISC seeks to support industry in fulfilling their obligations under the Act. Responsible entities of asset classes under the SOCI Act are required to establish, maintain, and comply with a written risk management program. These expectations are managed under the Critical Infrastructure Risk Management Program (CIRMP) [5].

PNT is treated as a critical component to Critical Infrastructure (CI) assets by the CISC. The Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023 explicitly uses PNT as an example of material risk, where a PNT system may be at 'a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the CI asset' [6]. The intersection of CI sectors with PNT is highlighted below, with those in bold containing an explicit dependence. However, all sectors would be affected by any disruption of GNSS services. Some of these sectors are discussed in further detail in the next subsection, alongside their intersections with the current policies of the Commonwealth of Australia.

Figure 4 - Critical infrastructure sectors under the SOCI Act 2018, where those with a strong dependence on PNT are highlighted in orange.

A risk assessment advisory has been established for the Space Technology sector by the CISC, with GNSS referred to frequently throughout the text, alongside the augmentation system SouthPAN [7]. GNSS positioning data, which may also include timing data, is emphasised to be relied upon by other critical infrastructure assets. Foreign interference may also disrupt or cause a cessation of general PNT services from space.

Generally, all Space Technology sector threats or hazards can be applied to PNT services delivered by GNSS. Specific vectors of each with the influence this may have on GNSS data include:

1. Cyber-espionage, delivering fake forms of GNSS-related service data or internal infrastructure data.
2. Cyber sabotage, disrupting or impairing GNSS infrastructure.
3. Severe weather events, causing degradation or denial of GNSS-related services.
4. Space weather events, impairing or destroying GNSS infrastructure in space.
5. Space debris and pollution, preventing GNSS infrastructure from being developed or continuing services.
6. Anti-satellite weapons, impairing or destroying GNSS infrastructure in space.
7. Supply chain issues, disrupting development and maintenance to GNSS supporting Australian ground-based infrastructure.
8. Global security environment changes, leading to selective availability or disruption of GNSS services delivered by foreign actors.

Under the CIRMP, the obligations of these risks should be managed by the responsible entity of the CI asset. However, for PNT by GNSS, which is treated as part of the Space Technology sector, there is no obligation to a responsible entity, as there is no asset. Where the responsibility lies must be further explored and established, including through approaches outside of the SOCI Act.

Of note, the risk assessment advisory of the Communications Sector highlights natural hazards such as space weather that can disable communications infrastructure ‘through damage caused to […] GPS satellites in orbit’ [8]. This would indicate that GPS satellites are part of the Communications Sector, forming part of the infrastructure, that is impacted by the hazard of ‘Space Weather’. In addition, in the risk assessment advisory of the Data Storage or Processing sector, GPS-stored data is mentioned as something that might be disrupted by the environment, causing an impact on the Transport Sector [9].

In November 2023, the first edition of the Critical Infrastructure Annual Risk Review was published [10]. In this document, PNT has been treated according to the CIRMP hazard vectors. ‘Significant disruption to positioning, navigation and timing services relied on by Australia’ is illustrated in a cross-sector risk prioritisation considering plausibility and impact. PNT in particular is presented to be the most damaging, but the least plausible. This is contrasted alongside data breaches, staff shortages, and supply chain issues. Cyber-related threats to space-based critical services are described as ‘yielding value for malicious targeting of infrastructure to create the widest impact’, alongside the natural hazard of solar flares/radio blackout storms in space that could disrupt GNSS. Thus, the responsible entity should be aware of these hazards to PNT services and act appropriately according to the CIRMP.

In the SOCI Act, as mentioned, the Space Technology sector contains no underlying assets [3], and this is where the stressed challenge arises. Hazards and threats to the Space Technology sector, where PNT services are treated to fall under, are a raised interdependency to other sectors. PNT and GPS services are explicitly a raised risk to multiple sectors, which according to the SOCI Act, will flow from the Space Technology sector. Asset owners from other sectors will need to mitigate this risk flowing from the Space Technology sector, as the Space Technology sector is not responsible under the SOCI Act. It is important to note that foreign GNSS asset owners do invest heavily in risk mitigations, however, whether these mitigations are suitable or adequate for Australian users of signals is completely out of Australian control. If PNT is owned or operated by the Australian Government, as might be the case for the National Positioning Infrastructure of Geoscience Australia, which includes SouthPAN SBAS and the Continuously Operating Reference Station (CORS) network, this would be governed by the Protective Security Policy Framework and is not covered by the SOCI Act.

Given the CISC's mandate, is to enhance the security and resilience of Australia's critical infrastructure and systems of national significance, and to support the industry in their obligations, PNT should be considered more carefully. The ambiguity to which PNT lies, as a non-existent but essential asset to Australia's critical infrastructure, should motivate support for clearer characterisation of PNT to CI. Given that GNSS is an asset outside of Australia's control, it should be treated as a hazard or threat to CI, with a complementary mitigation pathway available that other asset owners/operators can use. It should not be given as an example of a Space Technology sector, as this implies for an asset owner that the responsibility of mitigation may lie in the Space Technology sector. In addition, CISC should support the mitigation of the risk of PNT failure, given that this is important for other sectors and asset owners, but cannot arise by enforcement of the SOCI Act.

Recommendation 1: Building resilient PNT services should not be treated as an outcome of enforcement of legislation, e.g. SOCI Act. Other methods should be considered to achieve the same level of resilience as other Australian Critical Infrastructure assets.

Recommendation 2: The Department of Home Affairs' Cyber and Infrastructure Security Centre should provide mitigation pathways that asset owners/operators can use to mitigate risks to disruption or degradation of GNSS.

PNT for Critical Applications

PNT for Agriculture

The Australian agriculture sector accounts for more than 10% of the country's goods and services exports. However, there are concerns that with a slowing in the sector's productivity growth, the export value is at risk. Recent policy releases have made innovation at the centre of improving productivity, directed through the National Agricultural Innovation Policy Statement from the previously named Department of Agriculture, Water and the Environment [11]. This policy statement, released in 2022, uses research and development roadmaps and directions outlined in previous years, led by the Cotton Research and Development Corporation (CRDC).

One principal report, titled Accelerating Precision Agriculture to Decision Agriculture [12], highlights the benefits of digitisation internationally in agriculture, alongside stressing the need for Australia to 'step-up' to maintain competitiveness. To achieve this, it emphasises the adoption of innovative technologies that allow machinery to operate precisely with minimal intervention by a human operator. When it comes to navigating, GNSS fused with vision cameras are highlighted as one fundamental to be adopted.

Another report from the CRDC presents a review of on-farm telecommunications challenges and opportunities in supporting a digital agriculture future for Australia [13]. A precision of 2 cm is required for spraying, seeding and harvesting agricultural fields, driven by an ability to autosteer the vehicle. This level of accuracy is also used in the development of yield and elevation maps, as well as provide an ability to automatically turn-off the vehicle when it leaves a geo-tagged area. GNSS, as well as supporting local infrastructure to provide augmentation and correction, is solely used to deliver these services.

However, recent challenges with satellite delivered services have raised the importance of resilience in PNT infrastructure. Interruption to the transmission from the Inmarsat I-41F satellite in April 2023, where receiver architectures have become dependent on the corrections delivered from that satellite, led to automated tractor failures across Australia and New Zealand [14]. These sorts of issues lead to not only a loss in productivity, but a distrust of the services that deliver high precision PNT.

Why Agriculture needs Resilient PNT

Empower the sector to increase crop yields and general productivity.

Deliver on an increased adoption of digital infrastructure in rural areas.

Ensure continuity of service and avoid technology distrust by agricultural communities.

PNT for Australian Time

Timing services are essential to most critical industries within Australia, such as energy, telecommunications, and financial. However, amongst both private and public operators, most are dependent on satellite-delivered signals, and especially on GPS and other GNSS. According to experts, most users of timing from GNSS are private operators, and there is little awareness of the dependency they have on this PNT infrastructure. The National Measurement Institute (NMI) is Australia's core government agency related to timing, and there is minimal interaction between them and private users of GNSS timing services. Given arguments presented earlier in the context of the SOCI Act, support to Australian CI operators is necessary for resilience of timing in Australia.

The NMI provides a fee-based time and frequency service for Australia, supporting calibration and testing of instruments. They also provide Australia's official time and frequency dissemination service, traceable to Coordinated Universal Time (UTC) Australia. As mentioned, telecommunication operators and energy companies usually use separate time and frequency dissemination services, which are not managed nor coordinated by the NMI. The Department of Defence may also host a time and frequency laboratory.

The NMI dissemination service operates from a national facility connected through the Internet Protocol (IP) to numerous remote locations across the country. Each site hosts an atomic clock and a GPS receiver. Timing signals broadcast by GPS are used to measure the difference between UTC(AUS) and the remote clock so that the remote clock can be adjusted to UTC(AUS). A diagram of the service is given below, as detailed in the Using NTP for Traceable Time and Frequency [15].

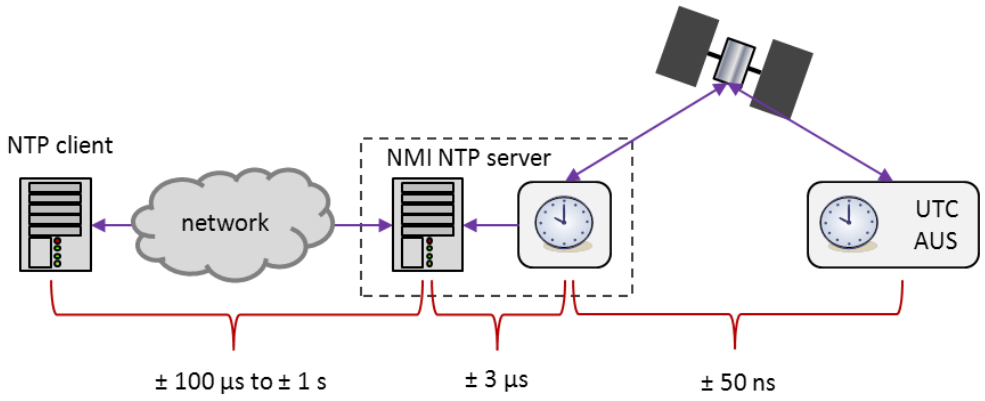

Figure 5 - Concept of Australian UTC dissemination and synchronisation [15].

Time and frequency are distributed to users by the Network Time Protocol (NTP) using IP. As using IP for both transfer to a server or to a user creates error by delay, distributed accuracies range from 100 micro-seconds to seconds. However, this performance satisfies many user groups of the NMI dissemination service. User groups consist of internet service providers, telecommunication operators outside of core infrastructure, banks and financial institutions, education providers including schools and universities, as well as government departments.

If GPS is disrupted, remote calibration services provided by NMI will stop after three months, relying on atomic clocks of the facility but no corrections. NMI could keep operating from Sydney and Melbourne sites at the required level of accuracy (1 ms) until the clocks fail. NTP will no longer be able to provide services after one month. Private companies also operate by a similar approach. A critical need of timing services is supply and access to atomic clocks, currently caesium, which must be physically located at each site. Only a few manufacturers of this technology exist.

Recommendation 3: Australia needs to develop an alternative source of timing, either through space or terrestrial means, that will aid in synchronisation and dissemination across the nation.

Recommendation 4: Australia should review and address its supply chain dependencies on atomic clock technology.

Why Timing needs Resilient PNT

Support the dissemination of Australian UTC across the continent.

Ensure private operators, such as telecommunication and energy providers, can synchronise time across their networks.

Provide critical supply of atomic clock technology for Australian critical infrastructure.

PNT for Automotive

In contrast to the sea or the air, land infrastructure for the automotive sector is highly developed and complex. The use of traffic lights, lane markers, reflectors, and delineators, amongst others, form part of an interconnected network to help drivers navigate. New developments in Australia to aid navigation and ensure safety include Cooperative-Intelligent Transport Systems (C-ITS), providing support for communications and decision-making abilities between road infrastructure elements, and autonomous vehicles technology development and legislative pathways.

Given the strict importance of safety in these systems, resilience is a key consideration in their development. The infrastructure in road transportation provides a stronger pathway to achieving this, when compared to other transportation domains and sectors. Many trials by state government agencies managing road infrastructure have been completed. A compiled database is made by Austroads [16], which serves as the association of Australian and New Zealand transport agencies, representing all levels of government.

Nation-wide land transportation technology development is consolidated as part of the National Policy Framework for Land Transportation Technology [17] and the National Land Transportation Technology Action Plan [18], with the most recent version developed for 2020-23 and reviewed in December 2022. The framework operates on a rolling four-year delivery, first proposed and reviewed by industrial consultation. Within the Action Plan, five central themes are composed, Safety, Security and Privacy, Digital and Physical Infrastructure, Data, Standards and Interoperability, and Disruption and Change. Even though resilience is not expressed explicitly, itis implied in these themes. Interviews with key policy makers expressed interest in the topic and future PNT technologies that may ensure this.

Highlighted technologies include ‘Rapid Advances in Vehicle Automation’ and ‘The Potential of Connected Vehicles’ [18], each of which have a critical dependency on GNSS technology. The deployment of future technologies will require assurances to the resilience of such components, with expressed intention in Safety, Security and Privacy to ‘protect such systems from cyber-attacks'. Under the theme of Disruption and Change, there is an expectation to ‘experience more disruptive changes in the future’ and an intention to be ‘preparing for changes that are able to be anticipated, while taking a flexible approach to unexpected issues as they arise’. Specific Items that this may fall under include 1.4, ‘Accelerate the deployment of road safety technologies and innovation’, and 2.1, ‘Develop guidance on how infrastructure can be future ready for CAV technology within an integrated transport and land use planning framework’.

More explicit policy principles towards an Australian C-ITS, which form part of the National Policy Framework, include a set of Draft Principles for a National Approach [19], alongside an external strategic advice report led by engineering consultancy group WSP [20]. Principles include working together to achieve ‘a nationally consistent C-ITS environment’, ‘harmonis[ation] with European approaches’, and ‘security of system and messaging and privacy of data’. The WSP report highlighted findings in the Cooperative Intelligent Transport Initiative, where significant insufficiencies in information quality from GPS solutions, as well as lack of security, is delaying system readiness and preventing a quantitative safety analysis.

Experts highlight that policy within the Australian automotive sector is use-case based. The approach in Australia of future technology such as connected vehicles and autonomation is primarily safety driven. An emerging technologies and trend analysis by the Queensland Department of Transport and Main Roads highlights cybersecurity concerns being a potential inhibitor to progress in improving future transport mobility [21], which would lead to an increase in road-related accidents and reduced efficiencies. Similar mentions of cybersecurity are part of future transport investigations by South Australian [22] and New South Wales [23] state governments.

A significant regulatory element in the automotive sector that critically depends on PNT information is the use of in-vehicle telematics. Transport Certification Australia (TCA), a subsidiary of Austroads, administers the National Telematics Framework, which is leveraged by government transport authorities to enable the position and movement of regulated heavy vehicles to be monitored, and the exchange of assured telematics data that enables productivity, road safety and

infrastructure protection outcomes to be achieved. The TCA have published guiding documents on implementing the vehicle monitoring applications under the National Telematics Framework, where the availability and quality of GNSS data is assessed [24]. TCA specifications consider spatial accuracy and horizontal dilution of precision, as well as the explicit use of GPS, but this might be further refined as new quality checks are put in place, such as authentication.

Further technology developments may also be considered, such as new GNSS frequencies, as well as upcoming services from satellite mega constellations. Their current responsibility does not include any assurances of safety performance, but if C-ITS is implemented in Australia, then it is expected that their responsibilities will increase. Adoption of GNSS is also a potentially more robust approach to securing infrastructure investments such as through equitable road user charging. Current approaches such as using toll road infrastructure, self-reporting, or fuel excise laws have limitations, and are currently considered by some to be socially and politically contentious. GNSS-based monitoring and verification of how far vehicles have travelled, and whether they have complied with location-based regulations may prove to be a more equitable approach for road users, while making vehicle compliance monitoring and assurance easier.

Recommendations 5: Consider leveraging Transport Certification Australia's (TCA's) National Telematics Framework, and its approach to GNSS assurance, under any future nationalised conformance framework for resilient PNT.

Why Automotive needs Resilient PNT

Delivery of safety, security, and privacy concerns for road transport users.

Be prepared for disruptive changes that may occur to PNT technology.

Paving the way for new autonomous automotive technologies to Australia's roads.

PNT for Aviation

The aviation sector was one of the key drivers for a GNSS and the original motivator for SBAS, including in Australia. However, aviation is also a common group affected when GNSS is degraded or denied. Recent news has referred to cases of GNSS being unavailable for users, with incidents reported over 2022-23 in Denver [25], Dallas [26], Finland [27], and Taiwan [28]. Airlines on routes near the Middle East have raised strong concern of the issue, as hostilities continue to rise in the region [29]. Even though there has been no recently reported incidents in Australia, GNSS anomalies have been reported by Qantas pilots over the South China Sea [30].

Reservations within aviation were recently expressed by Airservices Australia in a response to the CISC Protecting Critical Infrastructure and Systems of National Significance Consultation Paper [31]. There is a strong concern of cyber related risks to aviation, encapsulating airports, airlines, air traffic management and airspace management. PNT is explicitly mentioned, and a strong need to protect it to support these important sector functions as well as broader association and collaboration with other PNT intersecting sectors.

The Australian Civil Aviation Safety Authority (CASA) regulates according to guidelines set by the International Civil Aviation Organisation (ICAO). ICAO is especially aware of risks to GNSS, with guidelines in place, or under development, to maintain integrity even if it is degraded or disrupted. However, according to experts, ICAO sometimes creates guidelines that are unsuitable for the Australian operational context, and so CASA participation is important to ensure Australia needs are represented.

Presently, Australian aviation is only authorised to use GPS. There is an expressed concern that dependency on other constellations, which may improve performance and permit pilots' greater freedom to navigate, would present significant risk if that constellation was later denied. There are intended plans to switch to dual-frequency, multi-constellation, supported by SouthPAN [32], [33], but the risk that it may not be available in the future is acknowledged by experts. Another concern is the increase in ionospheric activity and potential for signal disruption due to the solar cycle, which is discussed in the subsection on Meteorology.

Further risks to PNT for aviation caused by 5G telecommunication infrastructure have been raised by CASA, where some operating bands are shared closely by aircraft radar altimeters, which measure the air vehicle's altitude above ground. This led to extensive discussions with the Australian Communication and Media Authority (ACMA), and proposed technical guidelines, to prevent significant disruption of this critical navigation component [34]. Alternative sources of PNT information,

including GPS-derived heights and air traffic control reports, are encouraged to review data outputs from radio altimeter systems. Such studies should also be encouraged for across other sectors, which is highlighted in other sections of this report.

Recommendation 6: Australia needs a comprehensive study and appraisal of all vulnerabilities to a loss of GNSS, with recommended mitigations.

A key area of growth and adoption for the aviation sector is in unmanned aerial vehicles, especially in drone technology. Such systems are critically dependent on navigation systems, where the absence of a human operator means alternative means of autonomous forms must be derived. GNSS is widely adopted in these platforms, providing an absolute navigation reference for maintaining position, return to home or following a series of waypoints.

Use of drones is not without risk however, where drone usage has posed significant danger to airports, populated areas, as well as general public wellbeing. Light shows using drones in Australian capital cities, such as in Melbourne [35] and Perth [36], have experienced technical incidents where drone communication and navigation systems have failed resulting in drones falling to the ground and into rivers.

The Australian Government Department of Infrastructure, Transport, Regional Development and Communications published a policy statement on National Emerging Aviation Technology [37], providing direction to the future of critical technologies in the aviation sector. Even though GNSS and PNT is not explicitly referred to in the statement, indirect policy direction has called for improved management and administration of Australian airspace and adopting a security- and safety-by-design approach toward the cyber resilience of unmanned traffic management and component systems, both of which have a strong dependence on resilient PNT.

Why Aviation needs Resilient PNT

Ensure aviation safety for Australian flagged airships within Australia and overseas.

Enable the safe introduction and sustainable growth of unmanned aerial vehicles in Australia.

Support Australian aviation resilience under an increasingly congested radio communication spectrum.

PNT for Defence

Deterrence and resilience are critical components of the Defence Strategic Review (DSR) [38]. It is described that intelligence and reconnaissance are critical for ensuring our borders are protected and foes are deterred. Given our large geographical separation from key international industrial bases, resilience in our supporting infrastructure, including cyber resilience, is crucial to deterrence. PNT is not explicitly mentioned in the review, but it is arguable that no infrastructure is at greater risk of degradation or denial than PNT, which often relies on a single point of failure for hardware or software, terrestrial or space-based, and alongside the ownership and operation of our satellite infrastructures by foreign nations.

PNT services underpin Defence's capabilities to achieve the strategic posture described in the DSR, and are relied on across all domains of Army, Navy, Air Force, Cyber and Space. As described in other subsections of this report, location and timing services are foundational services for critical civil infrastructure, including power grids, communication networks, and transportation, where degradation can undermine the ability for Defence to operate effectively in Australia or at distance.

Strategic technology pillars, known as Science, Technology and Research Shots (STaR Shots) [39], of the Defence Science and Technology Group (DSTG), as part of the Australian Department of Defence, target fields with cross-over relevance to PNT. The explicitly labelled, 'Quantum-Assured PNT' looks at quantum technology to deliver an alternative PNT technology for defence, while 'Resilient Multi-Mission Space', seeks to support resilience of space-based services, including 'resilient satellite services providing accurate position and timing information to enable precision effects in contested environments.' This is a direct reference to build sovereign capability in alternative space based PNT beyond GNSS. A successor to this programme is seen through the Australian Strategic Capabilities Accelerator, which includes quantum technologies such as sensing as a key priority area.

Resilient PNT delivery is a clear necessity to Australian Defence, and recently published tenders to ensure services has implied this claim. Defence is an important partner to any resilient PNT delivery, especially also considering Defence

relationships such as AUKUS (Australia-UK-US), where collaboration through joint R&D programmes could be pursued. As has been raised as a motivation for this work, resilient PNT is a global problem.

Recommendation 7: Defence is a fundamental stakeholder of PNT services, including those delivered from civilian infrastructure. Any civilian resilient PNT solution should take a dual use approach partnered with Defence.

Why Defence needs Resilient PNT

Support industrial capability in scenarios where our geographical separation leaves Australia at a disadvantage.

Provide operational resilience for Australian defence forces when GNSS is compromised.

Achieve advanced R&D ambitions for Australian defence industry.

PNT for Foreign Affairs

The Department of Foreign Affairs and Trade (DFAT) promotes and protects Australia's international interests to support our security and prosperity. Their mandate is to work with international partners and other countries to tackle global challenges, increase trade and investment, protect international rules, keep our region stable and help Australians overseas. Within this mandate, they also manage a network of Australian embassies, high commissions, consulates, multilateral missions, and representative offices.

The DFAT plays an essential role in managing and improving relationships with neighbouring countries, allies, and the international community. The Australian Government has released a new international development policy, establishing long-term directions for Australia's development programme [40]. Priorities include ensuring the Blue Pacific remains peaceful, prosperous, and equipped to respond to the challenges of our time, as well as helping the development and future of Southeast Asia. Australia will continue to invest in Pacific partner country needs and priorities, as well as collaborating with Southeastern Asian governments to support development and increasing inclusivity, all to build resilience across the region.

These priorities in Southeast Asia and the Pacific have led to investment in key PNT related areas, including funds to support monitoring of illegal fishing activities in Pacific Island nations by geospatial surveillance satellites [41]. In addition, a project sponsored and supported by Australian Aid with the Pacific Community was established to assist 'countries across the region adopt a modern geodetic reference frame underpinning fundamental geospatial systems and applications.' These services are understood to support 'roads and transport, ports and shipping, water and sewerage, energy and power utilities, telecommunications, construction, agriculture, town planning, climate change adaptation and many more sectors and industries.'

Recommendation 8: To deliver on international development policy, participation in or development of new sovereign PNT systems should consider their multi-layered impact to diplomacy and relations overseas, especially in the Asia-Pacific community.

For DFAT, their mandate also ensures the safety of Australians at home and overseas, as part of its support to Australian consular services. Consular services are provided in accordance with the Consular Services Charter [43]. As part of their charter, they strive to:

- Empower Australians to help themselves overseas.
- Effectively prepare for and manage overseas crises.
- Deliver a consular service focused on Australians most in need.

Special arrangements may also be made to support in cases of international terrorism, civil disturbances and natural disasters.

The development of Emergency Warning Systems as part of GNSS and PNT infrastructure has received interest by Australian civil authorities. The EU and Japan are collaborating on a common alert messaging standard, to be implemented by the European GNSS Galileo and Japan's regional equivalent QZSS. Demonstrations by the EU in the GRALLE project using the Japanese QZSS were made in Melbourne in 2019, and test messages were sent to users via smartphone [44]. DFAT participated in this project through Austrade. Comments from experts mentioned similar capabilities would be of interest overseas to support consular services abroad.

As part of DFAT's priority to delivering a secure and effective overseas Australian Government presence, and to support in deliver of consular service, it 'invest[s] in efficient, cost-effective technologies and infrastructure to fully support the global network and to adapt practices to ensure [staff] are safe and able to operate effectively to deliver for Australia around the world'. As part of this, 'the department will provide a reliable, secure and sustainable Information and Communications Technology (ICT) network that supports flexibility and innovation'. According to the DFAT Corporate Plan 2021-2022, they will achieve this by 'Strengthen[ing] protective security measures commensurate with the evolving global security environment.'

GNSS is used to provide staff tracking for security and safety. It serves part of an emergency positioning radio beacon, similar to the EPIRB. However, unlike EPIRB that communicates location directly to a satellite, the signal is communicated via a terrestrial radio network that does not employ local communication networks such as mobile. The location of the repeated communication is calculated by GNSS [45].

Why Foreign Affairs needs Resilient PNT

To deliver on the consular services charter, that strives to serve Australians overseas.

To provide safety and security for Australian government staff overseas.

To aid in the joint development of Australia's Pacific Island partners.

PNT for Maritime

The Australian Maritime Safety Authority (AMSA) acts as the statutory authority responsible for the regulation and safety oversight of Australia's shipping fleet and management of Australia's international maritime obligations. It commits to these obligations through participation and providing leadership to the International Maritime Organisation, the International Association of Lighthouse Authorities, the International Electrotechnical Commission. AMSA has published clear policy guidance for supporting navigation services, The Navigation Services in Australian waters - Outlook to 2030 [46].

According to experts in the maritime domain, PNT resilience implies the capability to 'withstand and recover from disruptions to PNT systems, which would result in critical and adverse effects on the maritime industry'. These effects are far reaching, impacting onboard safety of navigation, aids-to-navigation, port operations, supply chains, search and rescue operations, maritime assistance operations (pollution, recovery), and the external environment. Accuracies of PNT services are required up to 10 cm for critical port functions.

While AMSA has always regarded PNT resilience as important, policy now treats it as an absolute necessity for the modernisation of maritime vessels and port infrastructure. The maritime industry is presently undergoing a digital and automation transformation, and the integrity of high-accuracy PNT systems is fundamental. According to AMSA's outlook to 2030 [46], motivation is to maintain maritime safety and environmental protection mandates. Agility and innovation are important as the maritime sector becomes more digitised and autonomous. The report considers AMSA to be in a position to coordinate a global approach to resilience, given their representation of the Commonwealth in international forums.

Recommendation 9: Australia's maritime sector is one of the most critical sectors to strongly depend on GNSS and should be treated as a first use case in any future infrastructure developments.

Presently, GNSS remains the primary form of navigation, especially for coastal and oceanic phases of the voyage, which is under AMSA's jurisdiction. The new VHF Data Exchange System (VDES), which is set to replace identification beacons known as the Automatic Identification System, is being considered to support ranging services, known as R-mode. Signals are currently augmented by shore-based transmitters supplying a signal known as Differential GNSS, however these systems are being slowly phased out. Terrestrial, and potentially satellite, components of VDES may be used to deliver an R-mode. In response to PNT concerns in the maritime domain, AMSA will critically appraise emerging PNT technologies for their suitability to provide resilient PNT in Australia, including shore-based and those not reliant on man-made infrastructure, such as celestial and radar.

For Australia, land-based infrastructure is complex and costly due to the size of its geographical landscape. The geometry of Australia's coastline is also challenging for maritime-only navigation solutions in ports, such as terrestrial VDES R-Mode from shore-based infrastructure. It can however provide more robust solutions than that of space-based solutions alone. This is all considered to be under evaluation by AMSA, encouraging a solution that benefit not just maritime but the entire nation.

With regards to timing, accuracy is fundamental to the provision of VDES and related services. Most ports host accurate timing instruments, including atomic clocks, to provide this capability. They are synchronised using GNSS receivers, also assuring affective dissemination throughout port infrastructure and vessels, leading to a strong dependency.

The Department of Home Affairs complements the work of AMSA by providing policy directives and strategy to Civil Maritime Security [47]. 'Civil maritime security advances and protects Australia's interests by actively managing non-military risk to Australia and Australia's maritime domain.' Civil maritime security supports protecting national interest in: people smuggling, terrorism, transnational serious and organised crime, natural resources, critical infrastructure (as those supported by the CISC), amongst many others.

Explicit reference to navigation is in the first objective of the strategy, to 'Uphold Australia's sovereignty, freedom of navigation and maritime trade'. Freedom of navigation is dependent on resilient PNT infrastructure and services to protect Australia from security threats that would tamper with this infrastructure. Other objectives that support achieving resilient PNT for Australia is to 'Protect Australia's maritime infrastructure' and 'Protect users of Australia's maritime domain'. It should be noted that a resilient PNT strategy is not just geared towards developing alternative services, but also to protecting existing infrastructure against threats.

An additional field of significant Australia government activity reliant on PNT comes from delivery of the Australian Antarctic Program and Australian sovereignty over the Australian Antarctic Territory, which is administered by the Australian Antarctic Division, of the Department of Climate Change, Energy, the Environment and Water. Australia is a signatory to the Antarctic Treaty of 1959 and is committed to the international governance of the region through the instruments of the Antarctic Treaty System. Installation and activities related to PNT must be consistent with the requirements of the Treaty and its Protocol on Environmental Protection, including the Treaty's non-militarisation provisions.

The Australian Antarctic Strategy and 20 Year Action Plan [42], released in February 2022, provides a whole-of-government perspective to Australia's national Antarctic interests. Including research and scientific plans for the region, there was a declared delivery of a safe Australian Antarctic Program through 'emergency management, search and rescue', alongside 'develop[ing] a leading-edge maritime capability for unprecedented delivery of Australia's Antarctic activities providing, [...] maritime contingency to better respond to unforeseen developments, such as incidents requiring search and rescue or maritime assistance.' These ambitions have clear link to resilient PNT capabilities, especially that GNSS performance over poles are degraded, where current navigation satellite coverage, such as GPS, is concentrated over mid-latitude regions.

Why Maritime needs Resilient PNT

Ensure the responsible regulation and safety oversight of all vessels, Australian and foreign, located in Australian waters.

Lead the digitisation and autonomation of Australia's port infrastructure.

Provision of precise timing for maritime communication systems.

PNT for Meteorology

The intersections between PNT technology and meteorology are multi-faceted. PNT performance and availability is susceptible to the influence of weather, both within our atmosphere and in space. The Earth's ionosphere and troposphere affect the precision of GNSS for all users. Conditions of these atmospheric layers are monitored, and both terrestrial and space-based services report on their state. Australia's largest space infrastructure investment, the Space-Based Augmentation System (SBAS) SouthPAN, managed by Geoscience Australia, delivers these services across the country [32]. The service delivered allows any errors to be corrected at the user end, enabling a performance to the centimetre. These services depend on the accuracy and reliability of weather monitoring systems, a capability in which the Bureau of Meteorology (BOM) provides through the Automatic Weather Station (AWS) network.

The BOM's AWS uses PNT data for communications, especially in remote areas that require access to Broadband Global Area Network satellite coverage. In order to connect with a satellite signal, location data is required. Recent interruptions in the AWS network, critical services for capturing Australia's climate history as well as supporting essential services for natural disaster relief through prediction and monitoring, have highlighted the risks associated with this station network. After an extensive public inquiry, key hardware limitations were found to be culprit [48]. Even though not directly related to PNT, the

public outcry and implications for the BOM raises a need to ensure that Australia's climate monitoring systems are operating reliably without error.

Another growing area of interest for future Australian meteorological capabilities is in the use of GNSS signals for climate monitoring. GNSS reflectometry, a technique that measures reflected GNSS signals off the Earth's surface by satellites in space, provides insights into the Earth's environment. Applications to altimetry, oceanography, especially regarding wave height and wind speed, cryosphere monitoring and soil moisture monitoring. GNSS data is also being used in analysing atmospheric moisture content, where terrestrial based GNSS stations are used to provide information on the total transfer time of the GNSS signal from space to ground. Even for the profound impacts this may have to geo-informational monitoring, the users of these applications are in consequence becoming more dependent on the supporting GNSS infrastructure that supply these signals.

Space weather can also impact the performance and operational state of PNT services by GNSS. The most influential of these is the Sun, with solar cycles heavily impacting the Earth's ionosphere. At periods of solar maximum, the ionosphere is most unpredictable and PNT performance may degrade accordingly. In addition, large particle emissions from the Sun can seriously disrupt or impair satellite infrastructure, including those that transmit GNSS signals for navigation and timing. A serious event could disrupt GNSS services for many days. The general space environment can also present radiation risks and damaging particle emissions from neighbouring star systems.

Cases of major space weather events and its affect to critical infrastructure has been raised since the Carrington event of 1859 [49], a large geomagnetic storm that created wide spreading auroras and fires to electrical equipment. Such an event in today's technologically dependent era would be much further reaching, with serious implications to GNSS infrastructure. One of the more recent space weather events was in Quebec, Canada where a solar sparked storm disrupted power to six million people for days.

The BOM provides a space weather advisory for aviation [50], with a list of implicated technologies including GNSS. The BOM also collaborates with the CSIRO, Australian Bureau of Statistics and Geoscience Australia to publish a significant amount of material for public use on the impact of weather to GNSS and PNT services, alongside other services that may be impaired by weather events. These are all collated on the Australian Climate Service website [51].

Why Meteorology needs Resilient PNT

Ensure the continued operations of essential climate and weather monitoring systems.

Support Earth and climate science research and prediction services.

Protect Australian infrastructure from serious space weather events.

PNT for Telecommunications

PNT is fundamentally a communication technology, at least when it applies to GNSS and other forms of radio-based navigation. A critical risk in radio communications, and a motivation for delivering resilient PNT, is the jamming and spoofing of specific frequencies in the electromagnetic spectrum. Jamming refers specifically to the transmission of radio signals from a specially designed transmitter at the same frequency of some targeted telecommunication service with the intent to disrupt or deny. Spoofing mimics a radio signal from the targeted telecommunication service to provide false information. Both approaches are frequent at targeted GNSS frequencies and are also permanently banned under the Radiocommunications Act 1992 [52].

The Australian Communications and Media Authority (ACMA) role, as an independent Commonwealth statutory authority, is to regulate communication and media services in Australia. This explicitly includes the license to use equipment that transmit or receive messages through certain radio frequencies, as well as the regulation of illegal equipment such as jamming devices that target GNSS frequencies. Exemptions can be awarded by the Act, such as Defence and related entities [53], that critically use jamming equipment to demonstrate resilient PNT in their operations.

ACMA also regulates licenses to set and operate a new satellite network. ACMA will supply technical details of the satellite to the International Telecommunication Union (ITU) on behalf of the Australian entity, given the ITU only deals with administrations. It is treated as a spectrum management function under the Australian Communications and Media Authority Act 2005. In addition, the entity, such as satellite operators, must apply for a radiocommunications licence to use or operate a

satellite network in Australia. ACMA will support coordination with existing and planned networks in Australia. Separate communications are managed by the Australian Space Agency for launching a space object in Australia or an Australian space object overseas. Any new PNT system in Australia which operates by radiocommunications must follow these pathways.

Why Telecommunications needs Resilient PNT

Effectively regulate against jamming and spoofing threats to GNSS.

Regulate without risk new Australian satellite constellations, which would critically depend on GNSS-based services.

Coordination of new frequency bands that would deliver alternative radio-based PNT.

PNT Considerations in Australian R&D

The List of Critical Technologies in the National Interest [54], revised and republished on a regular (approximately annual) basis, consolidates and details the specific technological fields of focus for the government. The most recent publication of the List, and to which this report refers, is of May 2023. The list is developed against criteria which have been identified from what benefits Australia, including well-paid, secure jobs, attract investment, many different applications, revive Australian manufacturing, support emission target reduction, amongst others. There is also a management of risk, similar to guidelines provided by the Australian CISC. It is important to note that the List is to guide government policy as well as industry and academia towards technology related pursuits that are important to Australia, and funding is allocated from other sources and not by the List. The selection of technologies to be included in the List is selected based on where current government funding is prioritised, and not to guide future funding priorities.

The Critical Technologies (CT) Hub, under the Department of Industry, Science and Resources, role is to coordinate, compile and disseminate the List of Critical Technologies in the National Interest. They do not serve as subject matter experts, where they liaise with other government departments to support in providing guidance. They act as the overarching body, integrating scientific, economics and national security content, reacting to and supportive of needs as they arise. They operate to help connect industry and academia with relevant contacts in government.

When it comes to PNT, the List incorporates this under the field of ‘Autonomous systems, robotics, positioning, timing and sensing’ [55]. They explicitly refer to ‘satellites and systems that precisely measure position, navigation or timing data’. It is important to note that it is the only field on the List that refer explicitly to satellites and space, unlike the List of 2021 which directly referred to ‘sensing, timing and navigation’, as well as ‘transportation, robotics and space’. PNT lies across both these fields, as a space-based asset. A publication consultation in 2022 'highlight[ed] the overlapping applications of technologies across multiple sectors’, and it appears this inconsistency has been removed [56].

According to experts, for the Australian Commonwealth Scientific and Industrial Research Organisation (CSIRO), there is uncertainty in what could be fairly contributed in national PNT priorities. CSIRO strengths in communication technologies such as Wi-Fi could support R&D towards resilient PNT for Australia, as well as proposed pulsar-derived PNT and quantum navigation. However, a technical roadmap is necessary for funding prioritisation. Similar perspectives are also realised by the Australian Space Agency, where the contributions of Australia have been studied but not yet published for Australia’s PNT objectives.

Delivering a Solution

This section provides general recommendations for Australian PNT policy, as well as an appraisal of current work and progress in ensuring resilient PNT in Australia. Each is a response to the discussion and analysis of the previsions to this report.

Recommendations for Australian PNT Policy

This report has led to a consolidated list of recommendations for Australian policy directions towards resilient PNT. These are complementary to the other subsections on delivering an Australian solution. An additional recommendation is made to the multi-faceted nature of PNT, and the need for an office to consolidate and govern PNT issues for Australia. Similar offices have been proposed and made in the UK and Canada, funded by small contributions from different agencies across government.

Recommendation 1	Building resilient PNT services should not be treated as an outcome to enforcement of legislation (e.g. SOCI Act). Other methods should be considered to achieve the same level of resilience as other Australian Critical Infrastructure assets.
Recommendation 2	*The Department of* Home Affairs' Cyber and Infrastructure Security Centre should provide mitigation pathways that asset owners / operators can use to mitigate risks to disruption or degradation of GNSS.
Recommendation 3	Australia needs to develop an alternative source of timing, either through space or terrestrial means, that will aid in synchronisation and dissemination across the nation.
Recommendation 4	Australia should review and address its supply chain dependencies on atomic clock technology.
Recommendation 5	Consider leveraging Transport Certification Australia's (TCA's) National Telematics Framework, and its approach to GNSS assurance, under any future nationalised conformance framework for resilient PNT.
Recommendation 6	Australia needs a comprehensive study and appraisal of all vulnerabilities to a loss of GNSS, with recommended mitigations.
Recommendation 7	Defence is a fundamental stakeholder of PNT services, including those delivered from civilian infrastructure. Any civilian resilient PNT solution should take a dual use approach partnered with Defence.
Recommendation 8	To deliver on international development policy, participation in or development of new sovereign PNT systems should consider their multi-layered impact to diplomacy and relations overseas, especially in the Asia-Pacific community.
Recommendation 9	Australia's maritime sector is one of the most critical sectors to strongly depend on GNSS and should be treated as a first use case in any future infrastructure developments.
Recommendation 10	Given the multifaceted intersection of PNT across various Australian Government agencies and departments, an office is necessary to consolidate PNT-related outputs and provide governance of PNT issues for Australia.

Ensuring Resilient PNT in Australia

The core components to all resilient PNT programmes were introduced in Figure 4. Under the umbrella of resilience, administrations seek to characterise, evaluate, improve, expand, integrate, and deploy PNT. The progress towards delivery has been challenged however, especially in terms of financial sponsorship. The response of Australia to each of these components or milestones can be evaluated, based on current work and considerations by various Australian Government departments and organisations. The fields are written alongside comments to their implementation in Australia in Table 3. If such a programme has not been developed nor planned within public documents, it is written as 'No programme'.

Table 3 - Appraisal of resilient PNT progress in Australia across components first defined in [2].

Theme	Component	Response
1. Characterise and Evaluate	*a. Perform an economic assessment to the cost of disruption to PNT*	Australia has already delivered a market assessment of GNSS-related technologies through the SBAS test-bed programme, and the positive benefits high-accuracy positioning services may deliver to the economy. However, this assessment did not include the market benefit of basic or essential PNT services, and so cannot be used to assess what might happen to the Australian economy if PNT was denied from space. This is fundamental to decision makers to inform the economic consequences of PNT degradation or denial.
	b. Characterise PNT needs and requirements of relevant market sectors	PNT needs and requirements have been partially identified with regard to Australian SBAS, as well as general regulatory treatment of PNT, such as in automotive or aviation. However, quantitative, measurable needs and requirements from each Australian market sector should be captured, in the context of being an alternative or back-up source of PNT, especially with regards to accuracy, precision, availability, integrity and continuity.
	c. Evaluate threats and vulnerabilities to current PNT systems	No programme.
	d. Understand existing technologies available that deliver PNT	A technology appraisal within Australia has been completed by the Australian PNT roadmap, which was presented at the IGNSS conference in 2022 by the Australian Space Agency. However, this has not yet been released publicly yet.
	e. Appraise test capabilities and test protocols for assessing PNT infrastructure, equipment and services	No programme.
	f. Assess tools to qualify performance of PNT equipment and services, both individually and as an integrated system	No programme.
2. Improve and Expand	*a. Develop and improve internally-derived capabilities of PNT*	Internally-derived PNT, being PNT technologies that do not rely on external measurements, for example gyroscopes, have been outlined for priority funding under both civil and defence R&D schemes. It is a core component of the DSTG STaR Shots, explicitly under the Quantum Assured PNT pillar. National priorities of the List also include Quantum Sensing and Positioning, Timing and Sensing.
	b. Develop and improve external sources of PNT, both man-made and natural	External sources of PNT have been outlined as priority funding under both civil and defence R&D schemes. It is a partial component to the DSTG STaR Shots. National priorities of the List also include satellite and positioning technologies.
	c. Establish quality assurance measures for a wide range of end users	No programme.

Theme	Component	Response
	d. Improve and expand disruption detection and mitigation methods	This is a priority in the maritime domain, explicitly under the Civil Maritime Security policy of the Department of Home Affairs. ACMA has also regulated GNSS jammer usage. Detection and mitigation should be further improved and prioritised with an all domain and government programme.
	e. Prototype and demonstrate consumer equipment to adopt new PNT services	No programme.
3. Integrate and Deploy	*a. Determine concepts and techniques for securely integrating multiple sources of PNT services*	Internally-derived PNT has been indirectly outlined as priority funding under civil R&D schemes. National priorities of the List include Autonomous Systems.
	b. Development of common hardware platforms and signal standards, if appropriate, for multiple sources of PNT information	Progress in the delivery and adoption of SBAS services in Australia, such as SouthPAN, as well as 5G, has led to new GNSS services.
	c. Develop resilient PNT system architectures and frameworks	Resilient PNT system architectures has been contributed to through SBAS augmentation through SouthPAN.
	d. Investigate using internal sources as primary sources of PNT service	No programme.
	e. Develop cybersecurity standards, best practices, and other guidance to achieving resilient PNT	This has been partly achieved under the SOCI Act 2018 and through the CISC. However, more explicit integration is needed.
4. Collaborate and Coordinate	*a. Internal coordination and collaboration between government actors*	This is realised through the Australian Government PNT Working Group, and an intended objective of this report.
	b. International cooperation and adoption of resilient PNT systems	Australia effectively contributes to international forums, however more visibility is necessary. International approaches have been outlined in this report.
	c. Develop national / regional sovereignty in PNT	Sovereignty for Australian critical infrastructure is a core objective of the SOCI Act 2018. However, it is unclear how this applies to PNT.

Final Remark

Delivery of more resilient PNT services involves a coordinated response from both a technological and policy perspective, as may be understood by the previous sections. PNT services for the last 60 years have been predominantly a government delivered infrastructure, for public good. However, Governments may also act as a customer to the commercial industry for PNT infrastructure construction, especially given that PNT is generally considered as a public good, presently freely provided to the community.

About FrontierSI

FrontierSI stands at the forefront of Australia's journey towards resilient PNT infrastructure. Leveraging over 20 years of expertise and collaboration, FrontierSI aims to drive innovation towards a more resilient PNT infrastructure and is well-placed to provide leadership in ensuring resilient PNT for the nation.

FrontierSI, formerly the CRC for Spatial Information, has a strong record of delivering spatial information services throughout Australia, New Zealand and around the world. We harness the transformative power of collaboration and robust networks to curate top-tier teams dedicated to effective problem-solving. As a trailblazing social enterprise, FrontierSI focuses its deep spatial expertise on developing and implementing solutions using applied geodesy, spatial infrastructures, analytics, space technologies, and artificial intelligence.

Acknowledgements

FrontierSI would like to acknowledge the Australian Aboriginal and Torres Strait Islander peoples as the traditional custodians of the land across Australia where our services are located. We also pay our respects to Elders past and present.

This report was funded by FrontierSI under the Resilient PNT Transformational Initiative. FrontierSI would like to thank those who participated for their constructive ideas and contributions. While members of the Australian government were consulted in the process of producing this report, the contents of this report do not represent the position of the Australian government.

FrontierSI would like to acknowledge the principal authors and reviews of this report, including:

Joshua Critchley-Marrows, Eldar Rubinov, Graeme Kernich, Phil Delaney, Jia Lee, and Alex Linossier.

Image(s) used are sourced under license from Bozgor/Shutterstock.com.

Acronyms

ACMA	Australian Communications and Media Authority
AMSA	Australian Maritime Safety Authority
AWS	Automatic Weather Station
BOM	Bureau of Meteorology
C-ITS	Cooperative-Intelligent Transport Systems
CI	Critical Infrastructure
CISC	Cyber and Infrastructure Security Centre
CORS	Continuously Operating Reference Station
CRDC	Cotton Research and Development Corporation
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CT	Critical Technologies
DFAT	Department of Foreign Affairs and Trade
DSR	Defence Strategic Review
DSTG	Defence Science and Technology Group
EPIRB	Emergency Position Indicating Radio Beacon
GA	Geoscience Australia
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
IRNSS	Indian Regional Navigation Satellite System
ITU	International Telecommunication Union
LINZ	Land Information New Zealand
NMI	National Measurement Institute
NTP	Network Time Protocol
PNT	Positioning, Navigation and Timing
QZSS	Quasi-Zenith Satellite System
RF	Radio Frequency
SBAS	Space-Based Augmentation System
SOCI	Security of Critical Infrastructure
TCA	Transport Certification Australia
UTC	Coordinated Universal Time
VDES	Very High Frequency Data Exchange System

References

[1] Trevithick, 'U.S. Satellites Are Being Attacked Every Day According To Space Force General', *The Warzone*, Nov. 30, 2021.

[2] J. Critchley-Marrows and Q. Verspieren, 'Ensuring PNT resilience: A global review of navigation policies and roadmaps', Graduate School of Public Policy, The University of Tokyo, Tokyo, Japan, Jul. 2023. Accessed: Aug. 08, 2023. [Online]. Available: https://stig.pp.u-tokyo.ac.jp/stig/wp-content/uploads/2023/07/Resilient_PNT_Policy_Report_FINAL_ONLINE.pdf

[3] *Security of Critical Infrastructure Act 2018*, vol. C2023C00376. 2023.

[4] *Telecommunications Act 1997*, vol. ta1997214. 2008.

[5] 'Critical Infrastructure Risk Management Program - Part 2A Security of Critical Infrastructure (SOCI) Act 2018 Factsheet', Cyber and Infrastructure Security Centre, Feb. 2023. Accessed: Nov. 10, 2023. [Online]. Available: https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-risk-management-program.pdf

[6] *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*, vol. F2023L00112. 2023.

[7] 'Risk Assessment Advisory for Critical Infrastructure - Space Technology Sector', Cyber and Infrastructure Security Centre, 2023. Accessed: Nov. 10, 2023. [Online]. Available: https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/raa-space-technology.pdf

[8] 'Risk Assessment Advisory for Critical Infrastructure - Communications Sector', Cyber and Infrastructure Security Centre, 2023. Accessed: Nov. 10, 2023. [Online]. Available: https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/raa-communications.pdf

[9] 'Risk Assessment Advisory for Critical Infrastructure - Data Storage or Processing Sector', Cyber and Infrastructure Security Centre, 2023. Accessed: Nov. 10, 2023. [Online]. Available: https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/raa-data-storage-or-processing.pdf

[10] 'Critical Infrastructure Annual Risk Review', Cyber and Infrastructure Security Centre, Nov. 2023. Accessed: Nov. 10, 2023. [Online]. Available: https://www.cisc.gov.au/resources-contact-information-subsite/Documents/cism-2023/critical-infrastructure-annual-risk-review-first-edition-2023.pdf

[11] 'National Agricultural Innovation Policy Statement', Department of Agriculture, Water and the Environment, Oct. 2021. Accessed: Oct. 30, 2023. [Online]. Available: https://www.agriculture.gov.au/sites/default/files/documents/dawe-innovation-policy-statement.pdf

[12] 'Accelerating Precision to Decision Agriculture', Cotton Research and Development Corporation. Accessed: Oct. 30, 2023. [Online]. Available: https://www.crdc.com.au/accelerating-precision-decision-agriculture

[13] D. Lamb, 'A Review of On-Farm Telecommunications Challenges and Opportunities in Supporting a Digital Agriculture Future for Australia', Cotton Research and Development Corporation, 2017. Accessed: Oct. 30, 2023. [Online]. Available: https://hdl.handle.net/1959.11/22738

[14] D. Claughton and A. Conn, 'Inmarsat I-4F1 satellite outage disables tractor GPS services for farming operations and some maritime safety', *ABC News*, Apr. 18, 2023. Accessed: May 14, 2023. [Online]. Available: https://www.abc.net.au/news/rural/2023-04-18/inmarsat-i-4f1-satelite-outage-asia-pacific-gps-farms/102234678

[15] M. Wouters, 'How to use NMI Network Time Protocol Servers to Obtain Traceable Time and Frequency', National Measurement Institute, Jul. 2015. Accessed: Jul. 07, 2023. [Online]. Available: https://www.industry.gov.au/sites/default/files/2019-11/nmi-using-ntp-for-traceable-time-and-frequency.pdf

[16] 'Australian and New Zealand Trials', Austroads. Accessed: Oct. 12, 2023. [Online]. Available: https://austroads.com.au/drivers-and-vehicles/future-vehicles-and-technology/trials

[17] 'National Policy Framework for Land Transport Technology', Transport and Infrastructure Council, Aug. 2019. Accessed: Oct. 12, 2023. [Online]. Available: https://www.transportinfrastructurecouncil.gov.au/sites/default/files/documents/National_Policy_Framework_Land_Transport_Technology_and_Action_Plan_2020-2023.pdf

[18] 'Annual Review as at December 2022 – National Land Transport Technology Action Plan 2020–23', National Land Transport Technology Working Group, Dec. 2022. Accessed: Oct. 12, 2023. [Online]. Available: https://www.infrastructure.gov.au/sites/default/files/documents/annual-review-as-at-december2022-national-land-transport-technology-actio-plan-2020-23-june2023.pdf

[19] 'Draft Principles for a National Approach to Co-operative Intelligent Transport Systems (C-ITS) in Australia', Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Feb. 2023. Accessed: Dec. 22, 2023. [Online]. Available: https://www.infrastructure.gov.au/have-your-say/draft-principles-national-approach-cooperative-intelligent-transport-systems

[20] D. Alderson, J. Tong, and S. Polley, 'WSP Report—Advice on Strategies to Support C-ITS in Australia', WSP, Mar. 2022. Accessed: Dec. 22, 2023. [Online]. Available: https://www.infrastructure.gov.au/have-your-say/draft-principles-national-approach-cooperative-intelligent-transport-systems

[21] 'Emerging technologies and trends', The State of Queensland (Department of Transport and Main Roads). Accessed: Oct. 12, 2023. [Online]. Available: https://www.tmr.qld.gov.au/Community-and-environment/Planning-for-the-future/Emerging-technologies-and-trends

[22] 'Future Mobility Lab', Government of South Australia - Department for Infrastructure and Transport. Accessed: Oct. 12, 2023. [Online]. Available: https://www.dit.sa.gov.au/transportinnovation

[23] 'Future Transport Technology - Roadmap 2021–2024', Transport for New South Wales, 2022. Accessed: Oct. 12, 2023. [Online]. Available: https://www.transport.nsw.gov.au/system/files/media/documents/2022/NSW_Future_Transport_Technology_Roadmap_2021-2024.pdf
[24] 'Telematics In-Vehicle Unit: Functional and Technical Specification Version 3.0', Transport Certification Australia, Feb. 2019. Accessed: Dec. 22, 2023. [Online]. Available: https://tca.gov.au/specification-telematicsivuftsversion3-0-external-1/
[25] D. Goward, 'What happened to GPS in Denver?', *GPS World*, Sep. 21, 2022. Accessed: Nov. 21, 2023. [Online]. Available: https://www.gpsworld.com/what-happened-to-gps-in-denver/
[26] D. Goodin, 'GPS interference caused the FAA to reroute Texas air traffic. Experts stumped', *Ars Technica*, Oct. 20, 2022. Accessed: Nov. 21, 2023. [Online]. Available: https://arstechnica.com/information-technology/2022/10/cause-is-unknown-for-mysterious-gps-outage-that-rerouted-texas-air-traffic/
[27] 'Security specialist: GPS-jamming of Finnish aircraft likely Russian hybrid attack', *YLE*, Feb. 01, 2023. Accessed: Nov. 21, 2023. [Online]. Available: https://yle.fi/a/74-20015779
[28] K. Everington, 'CAA denies impact of GPS jamming on Taiwan aviation', *Taiwan News*, Apr. 26, 2023. Accessed: Nov. 21, 2023. [Online]. Available: https://www.taiwannews.com.tw/en/news/4873720
[29] S. Gebrekidan, 'Electronic Warfare Confounds Civilian Pilots, Far From Any Battlefield', *The New York Times*, Nov. 21, 2023. Accessed: Dec. 06, 2023. [Online]. Available: https://www.nytimes.com/2023/11/21/world/europe/ukraine-israel-gps-jamming-spoofing.html
[30] B. Rolfe, 'Qantas warns about interference by the "Chinese military" in the South China Sea | — Australia's leading news site', *news.com.au*, Mar. 17, 2023. Accessed: Nov. 21, 2023. [Online]. Available: https://www.news.com.au/travel/travel-updates/incidents/qantas-warns-about-interference-by-the-chinese-military-in-the-south-china-sea/news-story/40ff6a6a66408d666565085c5abf5d86
[31] C. Marrison, 'Protecting Critical Infrastructure and Systems of National Significance - AirServices Australia Response', AirServices Australia, Sep. 2020. Accessed: Oct. 25, 2023. [Online]. Available: https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/Submission-178-Airservices-Australia.PDF
[32] 'Southern Positioning Augmentation Network (SouthPAN)', Geoscience Australia. Accessed: Oct. 20, 2023. [Online]. Available: https://www.ga.gov.au/scientific-topics/positioning-navigation/positioning-australia/about-the-program/southpan
[33] 'Advisory Circular AC 91-05v1.0: Performance-based navigation', Civil Aviation Safety Authority, Oct. 2021. Accessed: Dec. 22, 2023. [Online]. Available: https://www.casa.gov.au/performance-based-navigation
[34] 'Airworthiness Bulletin: Potential 5G Interference of Radio Altimeter Systems', Civil Aviation Safety Authority, AWB 34-020, Sep. 2023. Accessed: Dec. 22, 2023. [Online]. Available: https://www.casa.gov.au/aircraft/airworthiness/airworthiness-bulletins/potential-5g-interference-radio-altimeter-systems
[35] P. Hatch, 'Yarra River battery pollution fears after 350 drones fall into water', *The Age*, Jul. 16, 2023. Accessed: Nov. 21, 2023. [Online]. Available: https://www.theage.com.au/national/victoria/extremely-concerning-yarra-battery-pollution-fears-after-drone-show-fail-20230716-p5dol8.html
[36] H. McNeill, 'Perth City of Light: More than 50 drones plunge into Swan River during light show', *WA Today*, Nov. 21, 2022. Accessed: Nov. 21, 2023. [Online]. Available: https://www.watoday.com.au/national/western-australia/an-expensive-event-50-drones-plunge-into-swan-river-during-sky-show-fail-20221121-p5c037.html
[37] 'National Emerging Aviation Technologies - Policy Statement', Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 2021. Accessed: Oct. 25, 2023. [Online]. Available: https://www.infrastructure.gov.au/sites/default/files/documents/national-emerging-aviation-technologies-policy-statement.pdf
[38] 'National Defence: Defence Strategic Review 2023', Department of Defence, Apr. 2023. Accessed: Nov. 05, 2023. [Online]. Available: https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review
[39] 'Science Technology and Research (STaR) Shots', Defence Science and Technology Group, Aug. 2020. Accessed: Nov. 05, 2023. [Online]. Available: https://www.dst.defence.gov.au/strategy/star-shots
[40] 'Australia's International Development Policy', Department of Foreign Affairs and Trade, Aug. 2023. Accessed: Sep. 08, 2023. [Online]. Available: https://www.dfat.gov.au/publications/development/australias-international-development-policy
[41] S. Erwin, 'HawkEye 360 satellites to monitor illegal fishing in Pacific Islands', *SpaceNews*, Jul. 06, 2023. Accessed: Nov. 21, 2023. [Online]. Available: https://spacenews.com/hawkeye-360-satellites-to-monitor-illegal-fishing-in-pacific-islands/
[42] 'Australian Antarctic Strategy & 20 Year Action Plan', Australian Government, Feb. 2022.
[43] 'Consular Services Charter', Smart Traveller. Accessed: Sep. 08, 2023. [Online]. Available: https://www.smartraveller.gov.au/consular-services/consular-services-charter
[44] 'GNSS-Based Emergency Warning Service Successfully Tested with Japan's QZSS in Australia', *Inside GNSS*, Oct. 17, 2018. Accessed: Nov. 21, 2023. [Online]. Available: https://insidegnss.com/gnss-based-emergency-warning-service-successfully-tested-with-japans-qzss-in-australia/
[45] 'Department of Foreign Affairs and Trade (DFAT) sign 3 year emergency radio network support contract with Simoco Wireless Solutions', Simoco Wireless Solutions. Accessed: Nov. 21, 2023. [Online]. Available: https://simocowirelesssolutions.com/media-and-events/press-releases/department-of-foreign-affairs-and-trade-dfat-sign-3-year-emergency-radio-network-support-contract-with-simoco-wireless-solutions/

[46] ‘Navigation services in Australian waters - outlook to 2030’, Australian Maritime Safety Authority, Jun. 2019. Accessed: Jul. 22, 2023. [Online]. Available: https://www.amsa.gov.au/sites/default/files/navigation-services-aus-waters-2030.pdf
[47] ‘Australian Government Civil Maritime Security Strategy’, Department of Home Affairs, 2021. Accessed: Nov. 15, 2023. [Online]. Available: https://www.homeaffairs.gov.au/nat-security/files/australian-government-civil-maritime-security-strategy.pdf
[48] ‘Review of the Bureau of Meteorology’s automatic weather stations’, Bureau of Meteorology, Sep. 2017. Accessed: Oct. 20, 2023. [Online]. Available: https://apo.org.au/sites/default/files/resource-files/2017-09/apo-nid106276.pdf
[49] ‘When Solar Storms Attack: Space Weather and our Infrastructure’, National Environmental Satellite, Data, and Information Service. Accessed: Oct. 20, 2023. [Online]. Available: https://www.nesdis.noaa.gov/news/when-solar-storms-attack-space-weather-and-our-infrastructure
[50] ‘Space Weather Advisories’, Bureau of Meteorology. Accessed: Oct. 20, 2023. [Online]. Available: http://www.bom.gov.au/aviation/space-weather-advisories/
[51] ‘Australian Climate Service’, Australian Climate Service. Accessed: Oct. 20, 2023. [Online]. Available: https://www.acs.gov.au/
[52] *Radiocommunications (Jamming Equipment) Permanent Ban 2023*, vol. F2023L00214. 2023.
[53] *Radiocommunications (Prohibited Device) (RNSS Jamming Devices) Exemption Determination 2014*, vol. F2023C00365. 2023.
[54] ‘List of Critical Technologies in the National Interest’, Department of Industry, Science and Resources. Accessed: Nov. 16, 2023. [Online]. Available: https://www.industry.gov.au/publications/list-critical-technologies-national-interest
[55] ‘Autonomous systems, robotics, positioning, timing and sensing’, Department of Industry, Science and Resources. Accessed: Nov. 16, 2023. [Online]. Available: https://www.industry.gov.au/publications/list-critical-technologies-national-interest/autonomous-systems-robotics-positioning-timing-and-sensing
[56] ‘List of Critical Technologies in the National Interest: stakeholder consultation report’, Department of Industry, Science and Resources. Accessed: Nov. 16, 2023. [Online]. Available: https://www.industry.gov.au/publications/list-critical-technologies-national-interest-stakeholder-consultation-report

Appendix – A summary of National Documents concerning PNT

Title	Year	Supporting Agency
Protecting Critical Infrastructure and Systems of National Significance - Airservices Australia Response	2020	Airservices Australia
Australia in Space A Decadal Plan for Australian Space Science 2021-2030	2022	Australian Academy of Sciences
Australian Antarctic Strategy & 20 Year Action Plan	2022	Australian Government
Navigation services in Australian waters	2019	Australian Maritime Safety Authority
Australian and New Zealand Trials	2023	Austroads
Review of the Bureau of Meteorology's automatic weather stations	2017	Bureau of Meteorology
Advisory Circular AC 91-05v1.0: Performance-based navigation	2021	Civil Aviation Safety Authority
Accelerating Precision Agriculture to Decision Agriculture	2017	Cotton Research and Development Corporation
A review of on-farm telecommunications challenges and opportunities in supporting a digital agriculture future for Australia	2017	Cotton Research and Development Corporation
Critical Infrastructure Risk Management Program	2023	Cyber and Infrastructure Security Centre
Risk Assessment Advisory for Critical Infrastructure - Space Technology Sector	2023	Cyber and Infrastructure Security Centre
Risk Assessment Advisory for Critical Infrastructure - Communications Sector	2023	Cyber and Infrastructure Security Centre
Risk Assessment Advisory for Critical Infrastructure - Data Storage or Processing Sector	2023	Cyber and Infrastructure Security Centre
Critical Infrastructure Annual Risk Review	2023	Cyber and Infrastructure Security Centre
National Agricultural Innovation Policy Statement	2021	Department of Agriculture, Water and the Environment
National Defence: Defence Strategic Review	2023	Department of Defence
Resilient multi-mission space	2020	Department of Defence - DSTG
Quantum assured position, navigation and timing	2020	Department of Defence - DSTG
Australia's International Development Policy	2023	Department of Foreign Affairs and Trade
Consular Services Charter	2023	Department of Foreign Affairs and Trade
Australia's International Development Policy	2023	Department of Foreign Affairs and Trade
Australian Government Civil Maritime Security Strategy	2021	Department of Home Affairs
Australian Government Civil Maritime Security Strategy	2021	Department of Home Affairs
List of Critical Technologies in the National Interest - Autonomous systems, robotics, positioning, timing and sensing	2023	Department of Industry, Science and Resources
National Emerging Aviation Technologies	2021	Department of Infrastructure, Transport, Regional Development and Communications
Annual Review as at December 2022 – National Land Transport Technology Action Plan 2020–23	2022	Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Title	Year	Supporting Agency
Draft Principles for a National Approach to Co-operative Intelligent Transport Systems (C-ITS) in Australia	2023	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
Advice on Strategies to Support C-ITS Deployment	2022	Department of ITRCA
Annual Review as at December 2022 – National Land Transport Technology Action Plan 2020–23	2022	National Land Transport Technology Working Group
How to use NMI Network Time Protocol Servers to Obtain Traceable Time and Frequency	2015	National Measurement Institute
Inquiry into the Department of Defence Annual Report 2019-20	2021	Parliament of Commonwealth
Space and Spatial Industry Growth Roadmap	2023	SmartSat CRC, SSSI, SIBA-GITA, FrontierSI
National Policy Framework for Land Transport Technology	2019	Transport and Infrastructure Council
Telematics In-Vehicle Unit: Functional and Technical Specification Version 3.0	2019	Transport Certification Australia

contact@frontiersi.com.au

linkedin.com/company/frontiersi

frontiersi.com.au

FRONTIER SI