Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Factsheet for Critical Infrastructure

Positioning, Navigation and Timing

November 2024

Australia's critical infrastructure increasingly relies on the delivery of positioning, navigation and timing (PNT) services, which are largely delivered from space. While space-based PNT services are ubiquitous, inexpensive and effective, they are vulnerable to intentional and unintentional interference, which exposes organisations to risks from denial or disruption of, or degradation to service.

A loss of access to, or deliberate or accidental manipulation of PNT systems may constitute a material risk to critical infrastructure under the *Security of Critical Infrastructure Act 2018* Risk Management Program Rules. Responsible entities for critical infrastructure assets should consider how to mitigate this risk as part of their Risk Management Program obligation (RMP).

Why are positioning, navigation and timing systems important?

Positioning, navigation and timing (PNT) systems are vital to the effective and efficient operation of much of Australia's critical infrastructure, and to the broader Australian economy. Many Australian consumers are familiar with the use of positioning and navigation systems, and use them in their day to-day lives. Increasing automation and availability of PNT services means that Australia is becoming more reliant on precise positioning information to improve safety and productivity in sectors like transport and agriculture.

Accurate and reliable timing is essential to sustain digital networks used by critical infrastructure. The precise timing derived from space-based PNT services is essential to the effective and efficient delivery of critical infrastructure, including in the banking and financial, transport, energy, communications and data storage or processing sectors.

What can disrupt or degrade PNT services?

Australians most commonly access PNT services from space (either directly or indirectly), via global navigation satellite system (GNSS) constellations such as the United States' Global Positioning System (GPS).[1]

As these services are extremely reliable, many users – including critical infrastructure owners and operators – are reliant on them. While GNSS provides cost effective PNT solutions, it should be remembered that they are also vulnerable to threats and hazards that may disrupt or degrade the service, and relying on a single source of PNT creates a vulnerability.

The disruption of, or degradation to, a PNT service – locally or on a larger scale – can have significant impacts for critical infrastructure owners and operators.

[1] GPS is the most widely used GNSS in Australia and globally. In addition to GPS, Australia also has high visibility of the additional three GNSS constellations (GLONASS operated by Russia, Galileo operated by the European Union, BeiDou operated by China; and the two Regional Navigation Satellite Systems (RNSS), operated by Japan and India).

CONTACT US | enquiries@CISC.gov.au | CISC.gov.au

Cyber attacks, including spoofing and jamming

PNT services are vulnerable to cyber attacks that can impact the integrity and availability of PNT data.

Much of the equipment required to access both terrestrial and space-based PNT systems (for example, time servers and GNSS receivers) are connected to the internet and are part of the attack surface, which can be exploited by malicious actors.

Jamming devices can also be used to deliberately interfere with GNSS signals. While it is illegal in Australia to own or operate GNSS jamming devices,[2] they are inexpensive to purchase illicitly and can cause serious disruptions to GNSS equipment.

Spoofing is the intentional transmission of fake signals that may cause a user to have incorrect information about time or their position. In a PNT context, this could include deliberately manipulating timestamps.

GNSS systems are also susceptible to system failure in space due to malicious actors.

Natural hazards

Space weather impacts the accuracy, availability, continuity, and integrity of GNSS services. In particular, increased solar activity can impact signal propagation through the ionosphere (ionospheric delays, gradients, and scintillation). Solar radio bursts, which are bursts of broadband radio noise, can also saturate GNSS receivers (amplitude fading and signal-to-noise degradation).[3]

Equipment failures

Equipment such as GNSS receivers and time servers last for many years, but may fail with little or no notice and take time to find a suitable replacement. Time services are usually distributed via the internet, so may not be available in the case of an internet outage.

What can be done to mitigate?

Entities can take actions to mitigate the risk of a disruption to, or degradation of, PNT systems. Ideally, prevention would be the first layer of defence, whereby threats are prevented from entering a system. As it is not always possible to prevent threats from occurring, organisations should identify how failure modes occur, understand how a device or system responds to specific threats, and how the device or system recovers.

1. Understand your PNT requirements

The first step to understanding your exposure to risk from GNSS vulnerability is to know the level of accuracy and integrity for positioning and timing that your critical infrastructure asset requires for effective operation. Depending on your business context, short term disruptions to service and/or a loss of accuracy might be manageable without compromising your operation.

Some businesses may be subject to regulations that require a certain level of precision for positioning and/or timing services. For example, the Australian Securities and Investments Commission requires market operators in the financial sector to ensure that their clocks stay within a certain tolerance of the time maintained by the National Measurement Institute.

Businesses should also consider what level of accuracy is required for PNT services. While precise positioning services are available in Australia – offering down to 3 to 5 centimetre accuracy in some geographic areas – not all businesses will require this level of accuracy. It is important to understand your minimum requirements, for short, medium and long-term outages, when designing your risk mitigation plans.

2. Use a trusted source of time

If you need to connect your business online, it is essential to understand where your organisation obtains access to time and frequency standards.

In Australia, the National Measurement Institute (NMI) is the legal authority for time. The NMI uses atomic clocks to maintain UTC (AUS), the Australian realisation of Coordinated Universal Time (UTC), and distributes this time via the internet. The NMI also provides Australia's official time and frequency dissemination service for users who need to know more accurate time of day, traceable to UTC (AUS).

The Cyber and Infrastructure Security Centre (CISC) recommends that critical infrastructure asset operators use the NMI time service as a fall back where possible and ensure that the timing service is traceable to UTC (AUS) and accounts for the difference between GNSS time and UTC/UTC leap-seconds.

[2] The Jamming Equipment Permanent Ban provides the rules for GNSS jammers.
[3] The Bureau of Meteorology's Australian Space Weather Alert System provides further details.

3. Consider hardening your equipment

Depending on your business context, it may be worth considering protecting and hardening your GNSS equipment. Options for protecting GNSS equipment could include:

- Using equipment with anti-jamming and/or anti spoofing measures.
- Implementing physical security measures to protect GNSS equipment.
- Using encryption when data needs to be securely transmitted or stored to ensure the accuracy and security of data.

4. Introduce redundancy

There are numerous ways to introduce redundancy and reduce the risks of relying on a single source of positioning and/or timing. For example:

- Where appropriate, consider using multi constellation GNSS receivers which will enhance accuracy, reliability, and availability for applications and reduce the impacts of an outage of a single constellation.[4]
- Using multiple antennas and/or receivers will protect against equipment failures and may assist in detecting interference.
- Adopting multiple PNT sources. For timing, an example could be to use a time server that has GNSS as its primary time source, configuring a trusted network time protocol (NTP) time source as a secondary source of time. For positioning, traditional terrestrial surveying techniques such as measurements derived using theodolites and total stations provide an alternative to GNSS, especially in environments where satellite signals are compromised or unavailable.
- Using high quality holdover devices (such as inertial positioning systems or holdover clocks) that provide some redundancy in the case of disruption to GNSS services. Organisations must consider their business continuity processes to ensure a seamless recovery and change-over between holdover devices, and ensure that holdover devices are regularly tested and standalone devices calibrated.
- Consider the use of a combination of satellite and terrestrial services.

Any redundancy measures introduced should be regularly tested as part of a PNT resilience testing regime to ensure that they are implemented effectively.

5. Maintain strong cyber security posture

Maintaining a strong cyber security posture should be a priority for all Australian critical infrastructure. Implementing key cyber security measures can assist prevent most (cyber-related) network incidents and make it harder for adversaries to compromise your systems or data. Ensuring employee compliance with cyber security practices will reduce opportunities for low complexity cyber incidents.

The Information Security Manual, produced by the Australian Signals Directorate, outlines a cyber security framework that organisations can apply to protect their systems and data from cyber threats. More specific information can also be found in the US National Institute of Standards and Technology (NIST) *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation and Timing (PNT) Services* (NISTIR 8323).

Further information on what the Australian Government is doing to build Australia's cyber resilience can be found in the 2023-2030 Australian Cyber Security Strategy.

6. Maintain space situational awareness

Space situational awareness can assist entities in understanding the space environment, and distinguishing anomalies caused by natural hazards from those potentially resulting from system failures or malicious actors.

The Australian Space Weather Alert System (ASWAS), operated by the Bureau of Meteorology, communicates space weather conditions and potential effects, aiding operators and decision-makers in taking mitigating actions.

Where can I find out more?

More information can be found on the CISC website. Within the Department of Home Affairs, the CISC drives an all hazards critical infrastructure risk management regime in partnership with government, industry and the broader community. The CISC assists critical infrastructure owners and operators to understand the risk environment and meet their regulatory obligations.

[4] The use of multi-constellation receivers may not be appropriate for certain industries, for example, aviation, where there are constraints on which GNSS systems may be used.