

# World class networks



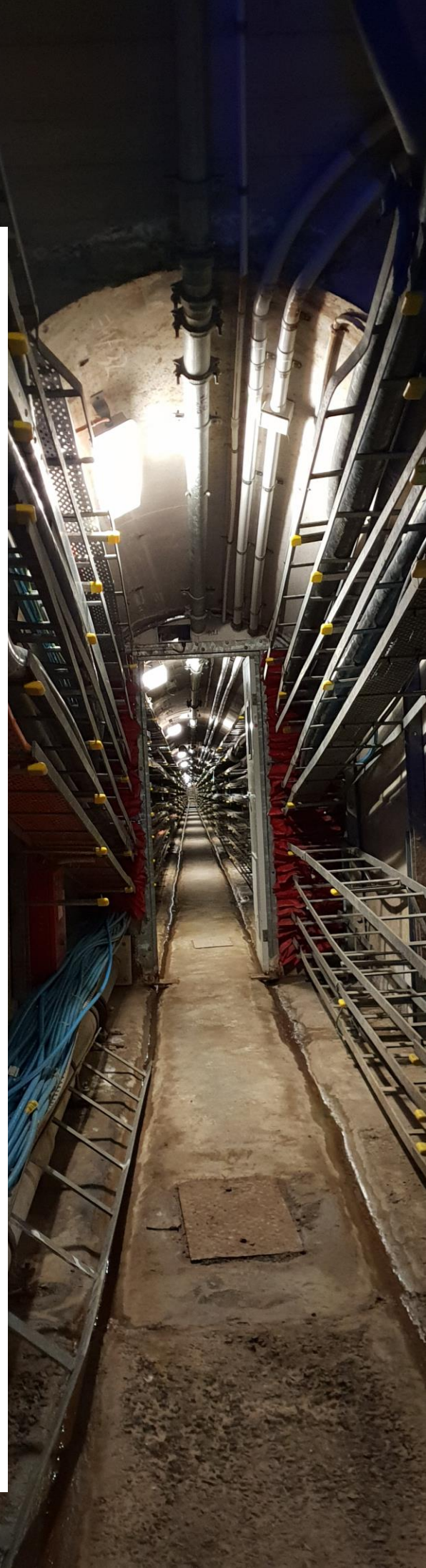
## Telstra LPWAN network whitepaper

June 2020



# Table of contents

	Page
1. Introduction	03
2. The basics	04
3. Shared vs. dedicated spectrum	05
4. Telstra IoT network vs. competitor technologies	08
5. Coverage	09
6. Penetration	13
7. Scalability	14
8. Security	17
9. IoT and 5G	21
10. Summary	22



# Introduction

## By Gerhard Loots

Global IoT Solutions Executive

At Telstra we believe in the potential of IoT to transform your business and home.

Good, timely data empowers businesses of all kinds to do better – to make smarter decisions, to improve efficiency, to lower costs and grow revenues and, most importantly, to improve the customer experience. The Internet of Things (IoT) is your ticket to getting that data and the insights that it unlocks.

There is more to the decision than just 'we need IoT', however. You need to figure out the use cases for how it can benefit your business, such as sensors in pipes that identify leaks or tracking assets through the supply chain, and you need to choose a network to deliver that critical data.

Our IoT network coverage is the largest in Australia, around 4M sq km<sup>2</sup> NB-IoT and around 3M km<sup>2</sup> LTE-M networks' reach. Our low power wide area networks (LPWAN) are built specifically for scaled IoT deployments to give you better, cost efficient coverage even in challenging locations that high bandwidth technologies may not reach. We've redefined the art of possible with our implementation of our LTE LPWAN standards, being the first operator globally to implement a 120km radius on NB-IoT and leading in our approach to security as recognised by the GSMA.

We are helping Australian industries from Utilities, Transport, Agriculture, Mining and

Manufacturing design and deploy secure networks of connected devices that allow you to use scarce resources more effectively, track assets, drive operations improvements, improve your customer's experience and deliver faster return on investment.

But how do you know what features to consider when making your IoT network decisions?

How do you evaluate the strengths and weaknesses of coverage when looking at the alternatives and the specific needs of your business?

How do you decide whether cellular or non-cellular networks are the best fit for you?

That is where this whitepaper comes in. Not all IoT networks are created equally, and it can be hard to get good information about the strengths and weaknesses of different IoT connectivity technologies. We break it down for you, to explain some of the finer details of LPWAN network technologies and the ways the benefits of our Telstra's LTE-M and NB-IoT networks can help you overcome common challenges in deploying IoT solutions in the real world.

We want to make it simpler and easier for you to make your network choice and leverage the power of our LPWAN networks to build a better future for all Australians.



## The basics

Wireless IoT technologies come in two forms. That is, those using dedicated or shared spectrum.

We will explain the difference shortly, but typically it comes down to cellular versus non-cellular. Telstra's LPWAN or low powered wide area network includes two different cellular technologies, both based on global standards: Narrowband IoT (NB-IoT) and LTE-M (which you may have also seen referred to as Cat-M1). Each of these is suited to different applications and each use the same cellular towers as your smartphone.

NB-IoT is intended for use cases that require low amounts of data (in the order of 20 MB a month or less per device), transmitted at low speed and benefiting from greatly extended range and battery life. Telstra has configured it to use a guard band of our frequency spectrum. A guard band is the small space between radio signals to prevent them interfering with each other.

LTE-M supports higher-bandwidth, higher-speed use cases than NB-IoT, while still offering optimisations that provide greater range and battery life than standard LTE devices.

NB-IoT is ideal for stationary applications like sensors, whilst supporting full mobility, LTE-M is better suited to things like a connected car or digital signage requiring higher throughput. LTE-M's mobility capability makes it well-suited to asset tracking, such as in Telstra's Track and Monitor solution – which uses a combination of LTE-M and Bluetooth devices.

Amidst the COVID-19 pandemic, for example, a medical supplies company used Track and Monitor to locate iPads used in pre-screening patients in pop-up triage clinics along the east coast of Australia.

A leading geo-civil contracting business, meanwhile, is now moving to use LTE-M tracking devices on 470 of their large non-powered assets.

1. Shared spectrum is predominantly accessed in Australia via a 'class' licence, which has limitations similar to 'unlicensed' spectrum in the US and other jurisdictions .

# Dedicated spectrum vs. shared spectrum

In choosing a communication technology for your IoT use case, you will need to consider whether that technology is deployed on dedicated or shared spectrum. So what's the difference?

Governments around the world have set aside frequency bands that, with some limitations, are available for everyone and anyone to use at no cost.

We call this shared spectrum. Wi-Fi is a great example, as is Bluetooth and even your kitchen microwave. By contrast, dedicated spectrum technologies – like cellular IoT – use frequency bands that a mobile operator has paid to have the exclusive rights to use, control and manage as they see fit.

## Shared spectrum

Proponents of technologies using shared spectrum often point out that mobile operators will need to recover the large amounts of money spent to obtain dedicated spectrum, and therefore cellular IoT will be more expensive. Make no mistake, however – nothing comes free, and shared spectrum is no exception.

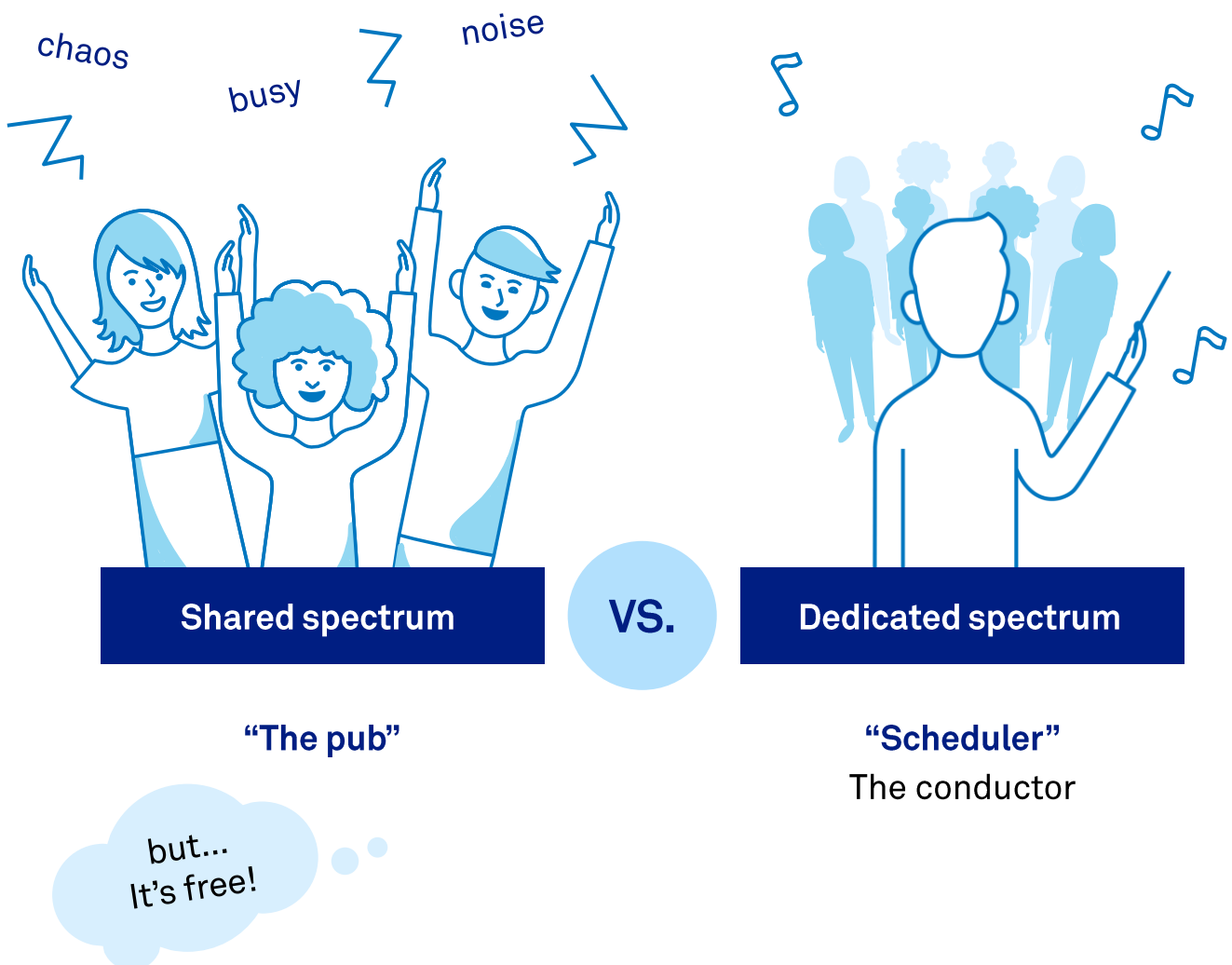
The price you pay for using shared spectrum may come in the form of reduced reliability, decreased quality of service and potential reductions in coverage availability.



One way to think about shared spectrum, and the issues you may face in using that spectrum, is to think of a pub on a Friday night after work. If you are one of the first to arrive, you may find that initially the venue is quiet, and you can communicate with your friends easily. As the night progresses and more people enter the venue, it becomes increasingly difficult to talk to your friends. You may find yourself having to shout or repeat yourself as the noise levels in the room increase.

Using shared spectrum is not much different to the pub analogy. Initially the first users at a location might enjoy good, clear communication. Then as more and more users come into the area, radio noise levels will increase. Since it is open to public use, you have no control over who else can use this public spectrum alongside you. You may find that over time the reliability of your communications deteriorates.

For mission-critical applications, the consequences are stark: you cannot guarantee that your message will get through when you need it to. Unlike the pub where you can almost shout to make yourself heard, there are finite limits to how much power a device can transmit within a shared frequency band. This means that, whilst your initial deployment of access points may have been sufficient to provide coverage, over time you may have to augment that deployment with additional access points to bolster reliability. Additional access points require not only additional capital – to acquire more sites and equipment – but also additional ongoing expenses to maintain and power that equipment. Deterioration of your service quality may be gradual over time or it could happen almost overnight. You have no control over if or when this may happen. You can manage your own devices, but you cannot manage the devices used by others or stop them from setting up camp right next to you.



# Dedicated spectrum

In contrast, frequency bands used by cellular IoT devices are tightly controlled by the mobile operator. Within a mobile base station, a software function called a scheduler controls when a connected device communicates. The operation of the scheduler is akin to a conductor in an orchestra. It coordinates and controls the operation of all devices connected to that base station. Through the use of smarter access techniques, instead of the noise and chaos associated with unlicensed spectrum usage, cellular IoT devices operate in quieter conditions. This provides potentially higher reliability, thereby leading to an improved quality of service and likely increased coverage.

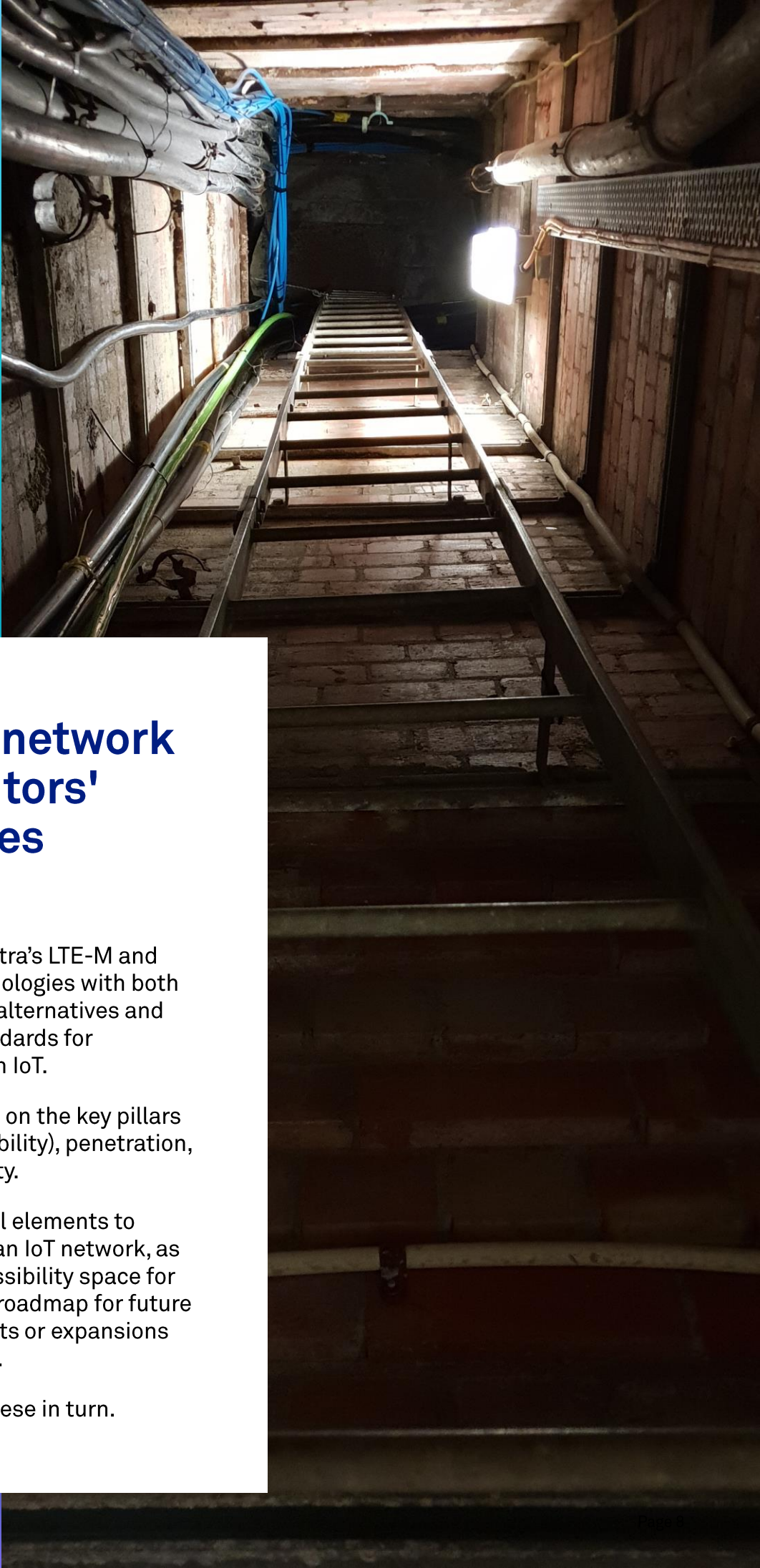
To return to the noisy pub analogy, you can think of dedicated spectrum as the mobile operator having their own private dining room.

This makes dedicated spectrum ideal for mission critical IoT applications. Indeed, one council that Telstra has worked with spoke of using shared spectrum solutions only when dealing with “non-trusted” data – for data deemed useful but not essential to operations – whereas they preferred to use dedicated spectrum, standards-based, carrier-grade technology such as NB-IoT for all of their “trusted” data. That way, they could feel confident that the solution would be supported and maintained over its lifespan and not vulnerable to degradation over time.

For further reading, a joint study by RMIT University and the ACMA <sup>[2]</sup> looked at the utilisation of the 900 MHz Industrial Scientific Medical (ISM) band in Melbourne. This is one of the shared frequency bands. The study provided insight into the utilisation of the band at that time and the potential performance limitations the current crop of non-cellular technologies may experience.

## Notes:

2. [https://www.researchgate.net/profile/Akram\\_AlHourani/publication/326214009\\_Free\\_Spectrum\\_for\\_IoT\\_How\\_Much\\_Can\\_It\\_Take/links/5c9c94f592851cf0ae9c8e17/Free-Spectrum-for-IoT-How-Much-Can-It-Take.pdf](https://www.researchgate.net/profile/Akram_AlHourani/publication/326214009_Free_Spectrum_for_IoT_How_Much_Can_It_Take/links/5c9c94f592851cf0ae9c8e17/Free-Spectrum-for-IoT-How-Much-Can-It-Take.pdf) .



## Telstra IoT network vs competitors' technologies

Now we compare Telstra's LTE-M and NB-IoT network technologies with both the shared spectrum alternatives and the international standards for dedicated spectrum in IoT.

We built our networks on the key pillars of coverage (and reliability), penetration, scalability and security.

These are all essential elements to consider in choosing an IoT network, as they define both a possibility space for your use cases and a roadmap for future updates, improvements or expansions in your IoT operations.

We discuss each of these in turn.



# Telstra's LPWAN networks' pillars



## Coverage

Network coverage is one of the most important factors to consider for any IoT deployment. If you don't have coverage, how is your device going to communicate?

### Cellular and non-cellular downlink/uplink comparison

Shared spectrum IoT technologies operating in the 900 MHz ISM band face regulatory restrictions that limit the amount of power they can radiate from their antennas. Provided a minimum of 20 hopping frequencies are supported, an IoT device operating in the 915-928 MHz ISM band is permitted to radiate a signal not exceeding 1 Watt<sup>[3]</sup>.

In contrast, cellular IoT technologies like LTE-M and NB-IoT do not face the same power restrictions. As a result, if we were to place two transmitters and antennas on a tower – one pair being a typical mobile base station and antenna, and the other being for use on the 900 MHz ISM band – we could expect the cellular IoT signal to reach much further.

In the uplink direction, both the cellular and non-cellular technologies face similar constraints in terms of the battery power available for the device and the physical limitations restricting antenna performance.

On that basis, the signal radiated by each is likely to be much the same.

However, as each technology typically uses the same antenna for uplink and downlink signals, the antenna used for mobile applications could be expected to provide higher gain than the non-cellular equivalent – and hence greater coverage. Additionally, as they share the same infrastructure as regular mobile services, cellular IoT devices in Telstra's network will receive further signal reception (and hence also potential coverage) boosts from the parallel antennas and receivers at base station sites that are used to increase mobile handset speeds.

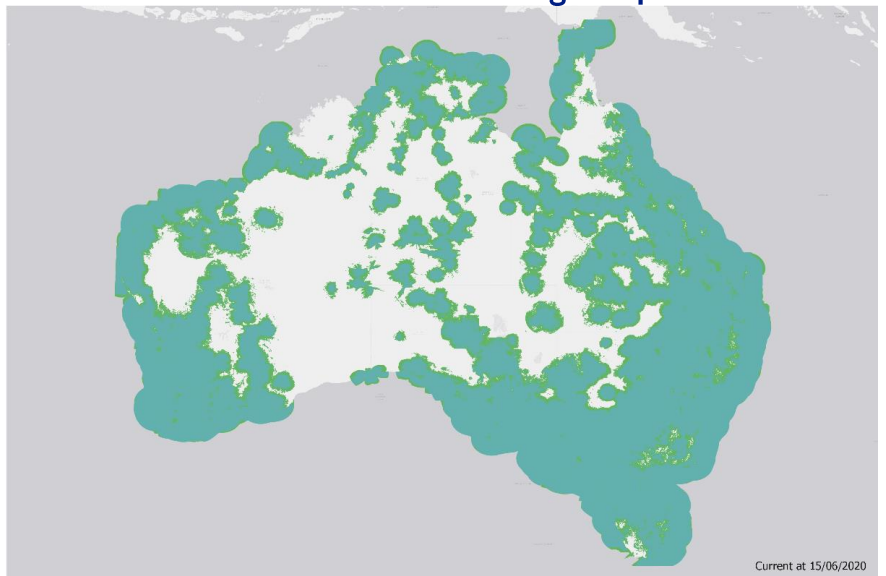
Note that the above also excludes the impact of any noise or interfering sources. If we factor in the higher noise levels often experienced in the 900 MHz ISM band, the coverage differences could be expected to be even greater.

3. <https://www.legislation.gov.au/Details/F2019C00681> Radiocommunications (Low Interference Potential Devices) Class License 2015 Schedule 1 Section 54.

## Ready built coverage

In selecting the cellular IoT technologies of LTE-M and NB-IoT, Telstra was able to leverage the existing mobile facilities we had in place. That is, due to continual investment in our network, we were able to introduce each of these technologies via a software upgrade to existing radio base stations without any site visit or hardware upgrade. This meant that almost overnight we went from having no network IoT coverage to full nationwide coverage. [4]

Telstra NB-IoT coverage map



That, in turn, allows our customers to focus on how they can make use of that coverage rather than waiting for it to be built out or having to pay for it to be built out – as would be required for unlicensed spectrum solutions in many areas.

## So what?



Telstra has extensive coverage across Australia available today. Customers don't need to wait for Telstra to build out coverage or to invest in and maintain their own coverage solution. They can simply leverage Telstra's IoT coverage and focus their time and capital on solving their business needs.

Regulatory restrictions have the potential to limit the signal strength and hence coverage available from non-cellular IoT technologies. Cellular IoT devices can leverage infrastructure provided for mobile broadband to experience additional coverage gains.

## Australian coverage

Different IoT use cases place different demands on coverage.

For example, in rural areas, agricultural use cases demand a wide breadth of coverage across the vast distances of the Australian landscape. In contrast, in built-up areas, where smart city use cases are common, a wide breadth of coverage is less important and the depth of coverage tends to dominate. (You will learn more about the depth and breadth of our coverage in the Penetration section later in this paper).

Today Telstra's mobile phone coverage extends to more than 2.5 million square kilometers, covering 99.5 % of the Australian population. Using the very same base stations and towers, our cellular IoT coverage extends to around 3 M sq kms for LTE-M and almost 4 M sq kms for NB-IoT.

With this expanded coverage, businesses with geographically dispersed assets can save tremendous amounts of time on inspections.

## Additional coverage feature

So how can the very same base stations and towers provide such a large amount of additional coverage for these low-powered wide area networks (LPWANs)?

The answer lies in an additional coverage enhancement feature that is available to all mobile devices but today is only used by cellular IoT devices. Coverage enhancement allows a device to send a message multiple times. When a cellular IoT device is in a poor coverage area, it is able to repeat the message to get it through.

This increase in the number of message repetitions is what extends LPWAN coverage in comparison to traditional mobile broadband devices that don't make use of the feature today. The net effect is that, like a battery-powered bunny, cellular IoT devices can keep operating where regular mobile handsets have stopped working due to lack of signal.

## So what?



A water company in Victoria, for instance, manages a number of very remote bores. It might take as long as hours for two workers – two, not one, because of OH&S requirements – to drive there for a physical inspection. IoT sensors installed at the sites not only save the time and cost of that travel but also they provide a more in-full view of water assets – as now the company can get daily or even hourly measurements instead of once every month or quarter.

## Reliability

Telstra builds its base stations to comply with rigorous standards. Not only do we ensure our sites are physically robust and able to withstand the enormous load of cyclonic winds, we also ensure sufficient battery capacity to allow the site to operate for a reasonable period under normal conditions until external power can be restored.

In considering our base station deployment, we comply with industry codes like the Australian Communications Alliance's C564:2018. Commonly referred to as the "Deployment Code", C564:2018 outlines the steps telecommunications carriers must take when designing new mobile phone base stations. Only mobile network carriers must comply with the requirements of the Code, however.

### So what?



From a customer perspective, you can feel safe in the knowledge that the mobile base station sites from which our IoT technologies radiate are deployed according to strict standards codes and built to last. Your mission-critical application needs this sort of rigour.

## Critical infrastructure services

Both in normal circumstances and in times of natural disaster, such as during a bushfire crisis, telecommunications services are considered vital for the social and economic well-being of the country.

For example, base stations during natural disasters may lose power. Emergency services may then take control over who can get access to generators and decide how to allocate those limited resources. In such times, Telstra will be actively engaged with emergency service organisations and jointly with those authorities take steps to ensure that the vital telecommunications services we deliver are restored or maintained. To expedite this activity, our Telstra technicians may even be escorted into critical areas by the relevant emergency service. It's these same facilities that deliver our IoT service. A knock-on consequence of that is that your mission critical IoT deployments could also stay online.

### So what?



From a customer perspective, you can feel safe in the knowledge that the mobile base station sites from which our IoT technologies radiate are considered significant to the social or economic well-being of the nation and will be kept operational as a priority. This means your mission critical application could also remain operational.





# Penetration

Great coverage is all well and good, but Australia is a huge country and many IoT use cases involve putting devices in extremely remote or hard-to-reach places. That is why we invested in building out both the breadth and depth of our base station range beyond the typical experience of a mobile network.

## Breadth of coverage

Telstra runs modified base station software to grant its cellular IoT networks world-leading coverage. This base station software allows off-the-shelf cellular NB-IoT devices with enough radio signal strength to communicate at a range of up to 120 kms. Other NB-IoT networks around the globe, by contrast, are limited to approximately 35 kms in range. Telstra has been recognised internationally – including an award honour at Mobile World Congress – for this world's first approach to extend the breadth of coverage available to our customers.

## Depth of coverage

It's not uncommon to want devices to operate at or below ground level, especially in built-up areas where smart-city applications are prevalent. A water utility company, for instance, may have many below-ground assets that they wish to monitor with sensors that can trigger alerts when a blockage occurs or a wastewater level approaches potential overflow.

Whilst Telstra's expanded 120km range capability is of minimal value in these situations, the same coverage enhancement feature makes it possible to extend the reach of coverage below ground. This may avoid the need for a business to deploy expensive infrastructure, such as signal repeaters, to push the measurement or condition report to ground level.

Telstra has showcased this ability by placing NB-IoT devices approximately 5m below ground in the city of Melbourne, where they continue to operate at a location where mobile phones will not. This does not guarantee that cellular IoT devices will operate at this depth at every location throughout our vast network, but it illustrates the potential for cellular IoT devices and applications to penetrate deeper than ordinary mobile solutions.

## So what?



For customers considering competitive network technologies, this means they can build their business case using cellular IoT with greater confidence that their devices will work in more places more often.

## So what?



With NB-IoT, Telstra-powered cellular IoT devices may continue to operate far deeper below ground than typical mobile connections, so you can make large-scale IoT deployments underground without spending big on additional infrastructure.



# Scalability

Telstra's networks are built to open global standards with dedicated, capacity-managed spectrum and a roadmap for the future. From a manufacturing perspective, sharing a single set of truly open standards enables each manufacturer in the value chain – be they a chipset vendor or infrastructure vendor – to focus their production on a global market. This drives economies of scale and accelerates the technology maturation.

But what of the network perspective? What happens as traffic volumes increase? How will your provider cope?

## Non-cellular capacity

For non-cellular technologies this is a considerable challenge. Many of the non-cellular technologies operating in the unlicensed spectrum use communications protocols based on pure ALOHA. A device based on a pure ALOHA protocol does not listen to the channel before transmitting. This may result in it transmitting over the top of one or more existing services.

Technology based on this very simple ALOHA protocol will have much lower system complexity, and this may consequently reduce device cost. However, a longer-term challenge is scalability.

Simple access protocols based on pure ALOHA reach maximum efficiency at approximately 18% channel utilisation. A joint study by RMIT University and the ACMA identified this challenge and concluded the “need to implement smarter access techniques to allow for higher utilisation of the spectrum”.<sup>[2]</sup> As traffic levels grow and radio channel utilisation increases, non-cellular technologies operating in the ISM band may run into trouble as that 18% channel utilisation level is reached.

In contrast, cellular IoT technologies are not based on pure ALOHA .

## So what?



Non-cellular IoT technologies operating in the shared spectrum mostly use a communications protocol that is cheaper and easier to set up but may struggle to cope with growing demand long-term.

## Cellular capacity

We are often asked how many devices can operate in a single NB-IoT cell? In considering such a question, firstly we must clarify what constitutes a cell. Cellular technologies commonly segment a cell into thirds. In that situation, what most people think of as a single cell can be three separate base stations acting in unison to create the appearance of a single cell. That act of segmenting a cell, taken on its own, has the potential to increase capacity by a factor of three because each radio then needs to handle only a third of the coverage area.

In considering the capacity of an unsegmented cell, the 3GPP standards body looked to the City of London as an example of a densely populated area, and hence one where many NB-IoT devices might be expected. Based on household density figures from census data and an average 40 devices per household, with typical cell radii for densely-populated areas and a traffic model encompassing a mix of periodic and ad-hoc messaging, they were able to determine the needs of greater than 50,000 devices could be handled by a single cell.<sup>[5]</sup>

So what happens when this sort of limit is reached? Today Telstra has a single NB-IoT carrier deployed in the guard band of our 20 MHz-wide spectrum allocation in the 700 MHz band. Without any physical construction activities, we have the potential to turn on additional NB-IoT carrier signals in that band in either the other guard band or potentially alongside our existing NB-IoT signal. If traffic levels increase many times over and those additional NB-IoT radio signals are still insufficient, we could potentially increase capacity through segmenting a cell, if it's not already segmented, to get a further three-fold increase. Neither of these approaches requires Telstra to invest in new sites.

## So what?



Cellular IoT is designed to withstand very high demand in densely-populated areas on current network infrastructure, and its capacity – at least in Telstra's case – has the potential to expand to meet higher future demands without constructing additional network sites.



## Telstra spectrum scalability vs. other cellular providers

With a 20 MHz-wide spectrum allocation, Telstra has the largest spectrum holding in the 700 MHz band of all Australian operators. This investment in a large spectrum holding allows us to deploy our NB-IoT signal in a guard band space that is twice what we would have if we had acquired just 10 MHz of spectrum. The benefit to our customers is that we have a far greater potential to scale our cellular IoT services through this larger holding. We have the potential to introduce additional NB-IoT carriers into our guard band space if that becomes necessary.

## Telstra spectrum quality vs. non-cellular providers

Service providers operating in ISM bands (which are generally used as shared spectrum) have no control over who else operates in that shared spectrum. Even when a specific technology has pre-defined usage plans for the spectrum, other users of that spectrum may overlap and interfere with one another. This has repercussions on scalability. As traffic increases, overall noise levels rise, and so then does the potential for other users to disrupt your service. With no control over who or how the spectrum is used, service providers operating in the ISM band may find themselves competing with one another for limited spectrum, increasingly densifying their coverage to overcome the increase in the base radio noise floor.

## So what?



Telstra can not only control the use of our spectrum but has the potential to scale better than anyone to meet increased demand. In contrast, shared spectrum users face a risk of potential interference, disruption and even shut down, as long-term spectrum use and service-level agreements cannot necessarily be guaranteed.

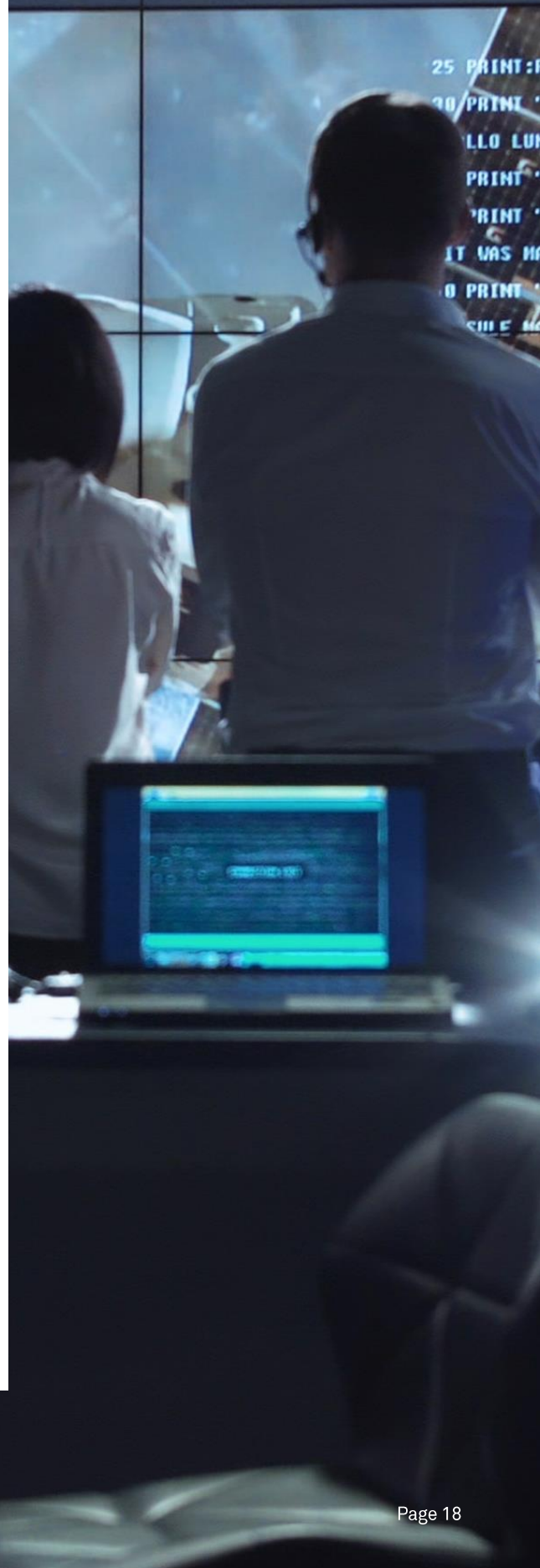


## Security

Many IoT use cases have emerged because of the lowered cost of IoT, which makes it economically viable to deploy such a service. In reducing the cost, however, security is not always deemed a priority. There have been numerous articles in popular and industry press of individuals and organisations deploying an IoT service only to find that, from a security perspective, their solution leaks like a veritable sieve. Too often, security – if it has been considered at all – has been treated as an afterthought.

Recognising the risk that a poorly thought-through IoT solution presents, not only to the owner of the service but also to others around it, a range of reputable organisations and government bodies have published security guidelines or codes of practice for deployment of IoT solutions. Telstra actively engages with a number of these organisations and our contribution to IoT security was formally recognised in an award at the 2019 GSMA Mobile World Congress in Barcelona.

Many businesses fail to realise a high proportion of internet-enabled devices are sold without built-in security. Some devices even lack an operating system that can support the installation of security software. For IoT, or indeed any product or service, security can no longer be an add-on or an afterthought. Security needs to be an integral part of any design.



## Security guidelines

It is no surprise that the security guidelines and codes of practice that have been developed, whilst each worded slightly differently, all have a common theme. The Australian government's Home Affairs draft code of practice identified 13 principles of which "The first three principles are the highest priority to achieve the greatest security benefit."<sup>[5]</sup>

If we consider those first three:

1. No duplicated default or weak passwords
2. Implement a vulnerability disclosure policy
3. Keep software securely updated

## Authentication

Passwords are one way of authenticating a user or a device. From an IoT perspective, authentication is a multifaceted consideration. Mutual authentication makes sure that not only is the device who it says it is but conversely that the network or server is who it claims to be. From a network perspective, cellular IoT devices make use of a UICC (often called a SIM) in either a physical or eUICC form factor. This facilitates a mutual authentication capability. At an application level, users would want to perform an additional level of authentication. Again, the SIM can play a role in this space. Standardised by the GSMA, users can leverage the secure operating environment of the SIM to safely store credentials used for application level authentication.

Telstra is an active member of the GSMA, and we have successfully demonstrated authentication at an application level using credentials that were securely stored on a SIM.

## Vulnerability disclosure

The second principle related to the need to establish a point of contact for security vulnerabilities. For Telstra, this is nothing new.

We have been an active participant in the cyber security sphere for many years, and we have brought various cyber security-related products and services to market for our customers. Behind the scenes, we regularly receive security advisories and information about critical incidents worldwide.

## Software and firmware updates

The third key point related to the need to keep software securely updated. This is critical for IoT applications where devices are typically deployed in the field and potentially left unobserved or untouched for extended periods. With this in mind, the choice of IoT connectivity technology becomes crucial. You need to ask, can this technology support software or firmware upgrades over the air? You may find your business case is crippled by the expense of a truck roll if that is the only way to maintain the software in application end points.

The way devices handle updates is equally important. Is the update distributed as a single monolithic image or is it possible to implement patches through delta or incremental updates? IoT connectivity technologies with only a modest ability to download updates may struggle to handle the demands of large monolithic images when they are distributed to multiple devices. This, in turn, could have a big impact on your ability to deploy IoT devices at scale.

5. <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>  
DRAFT Code of Practice - Securing the Internet of Things for Consumers.

## Further protections

Another important consideration is the need to protect device data when the data is in motion or at rest. Leveraging existing mobile technologies, cellular IoT benefits from the encryption and integrity procedures used by the billions of mobile devices used across the world every day. The ability to individually protect each data session from snooping, together with the ability to identify if the packet contents have been swapped out, is vital for critical applications.

To take matters further, it is common for applications to want to isolate themselves from all others. That is, to create an air gap between their application and the rest of the world. Again, leveraging a heritage in mobile technology, cellular IoT is able to set aside dedicated APNs that can only be accessed by devices with the proper credentials. Devices and data from those devices are then able to operate in their own portion of the network without encountering other user devices or the Internet.



## So what?

Customers need to consider the security requirements of their solution and whether their chosen IoT technology meets those needs. When looking at non-cellular network technologies without over-the-air software/firmware update abilities, you must also consider the potential replacement or lifecycle costs of manually updating software.



## Telecommunications Sector Security Reform (TSSR)

To protect the national economic interests of Australia, the federal government introduced the TSSR in 2015. This action and the legislative bills associated with it are intended to protect critical Australian infrastructure from influence and control by foreign actors. Today critical infrastructure is identified as water, electricity, gas and ports. The scope may or may not change in the future.

As part of the reform, providers of communications services for critical infrastructure must submit documentation to the federal government describing the robustness and reliability of their network against attacks. This includes not only the network architecture, topology, physical and cyber security aspects but also the choice of equipment vendors and people and processes in use.

For example, providers are required to document what security checks are in place for people with access to vital elements of the network and, in the case of outsourced network maintenance, who is providing that, where in the world is it being provided from and what security checks are in place for staff of those third-party organisations.

As a provider of communications services to critical infrastructure, Telstra is required to fulfil these requirements. In considering use cases for critical infrastructure, customers need to ensure that their service provider meets these requirements and, in the event that the scope of critical infrastructure changes, is there a possibility their deployment could fall within that redefined scope?

### So what?



Use cases in support of critical infrastructure – currently, water, electricity, gas or ports – face additional, more rigorous security expectations.

# 5G 5G

## Why Cellular IoT technologies are future proof

As 5G evolves, it is expected to deliver Ultra Reliable Low-Latency Communications, high speeds and massive Machine-Type Communications that enable a range of new high-performance use cases. That does not, however, spell the end for the cellular IoT technologies of today. The 3GPP standards body believe both LTE-M and NB-IoT fulfil all the requirements for 5G mMTC. On this basis, Telstra intends to support LTE-M and NB-IoT until 2035 \*

## Telstra's Cellular IoT meet 5G requirements

In support of this claim, 3GPP have made a formal proposal to the International Telecommunications Union for LTE-M and NB-IoT to be accepted as technologies able to fulfil the requirements of IMT-2020 (commercially known as 5G). This has been accepted.

This means that, at some stage in the distant future, when 4G LTE is retired, LTE-M and NB-IoT as recognised 5G technologies could potentially continue to operate. Your existing IoT devices should therefore be unaffected by the transition to 5G, which will ensure a long service life if you plan to put some in a pipe buried underground for a decade or more.

## Future of Cellular IoT is not directly linked to 4G

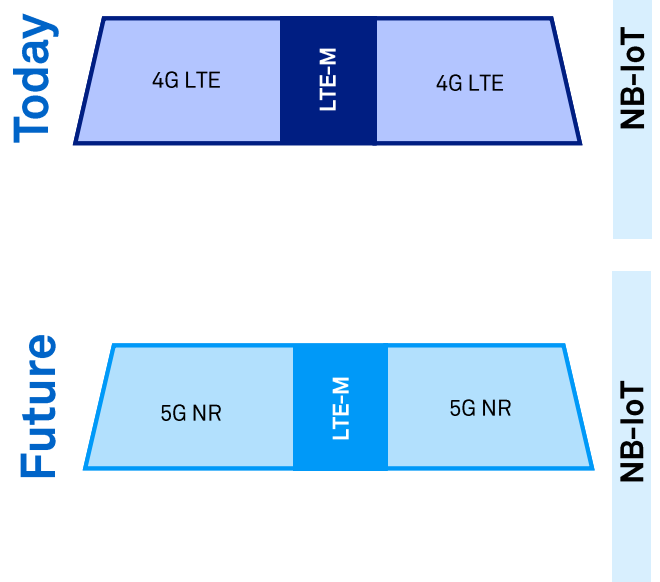
### So what?



What this means is that LTE-M and NB-IoT will coexist with 5G NR technology in a similar manner as they coexist today with 4G LTE technology.

This could potentially increase the service life of devices in the field, enabling some use cases to be economically viable where otherwise they might not.

### IoT in a 5G world



\*Service from 2030 onwards is dependent on the Australian government or the ACMA renewing Telstra's relevant spectrum licences under the Radiocommunications Act

# Summary

As you have now seen, the choice of IoT connectivity network for your business case is not a trivial decision. We hope you now feel much better equipped and confident that you understand the decision-making considerations and the advantages of choosing Telstra's LPWAN network.

## To recap the key takeaways:

- Telstra's IoT network is already built, with a massive coverage range of almost four million square kilometres for NB-IoT devices, at up to 120 kilometres from the nearest cell tower – and around three million square kilometres for LTE-M, you can use it right away.
- Shared spectrum technologies may be perceived as a lower cost option– that is, assuming the shared spectrum network is even built out where you need it – and they may work well right now, but using them comes at the price of long-time reliability and you could end up paying more to maintain it.
- With Telstra, potentially you could apply NB-IoT to below-ground use cases like sensors embedded in pits – with less additional infrastructure spend.
- Cellular IoT is designed to withstand extremely high future demand, and Telstra's network is better equipped than any other in Australia to expand to meet immense increases potentially without requiring any investment in new network sites.
- Cellular IoT adheres to strict standards and codes of practice for security, reliability and maintenance of service, so its performance should not degrade over time.
- Many non-cellular IoT technologies lack support for effective over-the-air software updates, which may necessitate manual updates or replacements and could thus cripple the business case for large-scale deployments.
- Both NB-IoT and LTE-M are able to meet the requirements for 5G massive machine type communications and as such have the potential to serve your goals of future proof communications technologies.

**When thinking about trusted IoT,  
think cellular IoT**



**Contact your Telstra  
account representative  
for more details or go to:**

[www.telstra.com.au/](http://www.telstra.com.au/)

1300 835 787

Contributors:

Technology strategy team

IoT Product and Sales Specialists

IoT Value Creation Team

Richard Moss, Consultant Writer