NSW Government's Smart Infrastructure Policy

Document number:	Version number: 1.1
Date: Wednesday, July 22, 2020	

Contact details

Name: Office of the Secretary, Department of Customer Service
Email: iotproject@customerservice.nsw.gov.au

July 2020

Table of Contents

1. Policy Statement

1.1 Overview

Whilst the digital age is well established, technologies that will power our future infrastructure are still emerging and there is a need for NSW Government, communities and cities to become smarter and more innovative with existing resources. Fast-growing cities and towns with highly valued, ageing or overused infrastructure are one of the major challenges we face as our population continues to grow. Existing and future infrastructure developments must adapt to meet growing demand and minimise service failure.

In response, the NSW Government has prepared Beyond Digital and a Smart Places Strategy that will guide the government agencies and their partners to deliver an efficient NSW that uses technology and data to drive economic success, social inclusion and sustainable outcomes for NSW citizens and businesses.

New or existing infrastructure can use technology and data to continuously monitor, measure, analyse, communicate and act. It can drive productivity, improve sustainability and optimise planning and design, as well as provide improved customer outcomes and experiences. It can also support us to learn and improve so that insights are shared across infrastructure assets. Turning data into insights creates value - reduced operational costs, additional capacity, more efficient service delivery and a better return on Government investment.

NSW Government is committed to smart infrastructure that produces, analyses and helps to securely share data to improves the liveability, productivity and sustainability of towns and cities in NSW. This underpins the NSW Government's smart places vision. The Smart Places strategy aims to improve physical and digital access for the people of NSW in their everyday participation in society.

The Smart Infrastructure Policy will not only make sure we plan, design, build and operate connected communities, it will also make sure we use these assets to their full potential, ensuring we get the best return on the Government's $97.3 billion infrastructure commitment.[1]

1.2 Purpose of this Policy

This policy sets the minimum requirements for smart technology to be embedded in all new and upgraded infrastructure from 2020 (recommendation 32 of the State Infrastructure Strategy 2018-2038).

It is part of a suite of policies, strategies and frameworks developed by the NSW Government to enable 'Smart Places'.

[1] https://www.budget.nsw.gov.au/sites/default/files/budget-2019-06/Budget_Paper_2-Infrastructure%20Statement-Budget_201920.pdf

The Smart Places Strategy describes the 'building blocks' necessary to realise smart places and informs the decisions and actions by the NSW Government and place owners across the State to implement 'smart' solutions for problems in their cities, towns, suburbs and communities.

This Smart Infrastructure Policy is one of the foundational elements of the Smart Places Strategy.

1.3 Scope of this Policy

This policy applies to infrastructure projects subject to the Infrastructure Investor Assurance Framework (IIAF) and ICT Assurance Framework from late 2020.

It outlines generic smart technology requirements that are applicable to all infrastructure (i.e. not requirements that are specific to a type of infrastructure, such as hospitals).

The Asset Management Policy for the NSW Public Sector (TPP 19-07) mandates NSW Government agencies to adopt a whole-of-government and whole-of-asset lifecycle approach to their assets. One of the objectives of this approach is the utilisation of innovative, contemporary technologies to improve the operation and maintenance of assets. As such, compliance with this Smart Infrastructure Policy may be considered as part of the Asset Management Policy's assurance process in future.

1.4 Smart infrastructure defined

For the purpose of this Policy:

- infrastructure means a system of physical and digital assets that enable the delivery of the services that are the foundation for a successful economy and society'[2] (e.g. transport modes, street furniture, bridges, hospitals, schools, parks, waterways, green spaces, prisons etc).
- smart infrastructure is infrastructure that uses technology and data to optimise performance, increase capacity and achieve a greater return on investment. It uses smart technology (e.g. sensors, computing algorithms) to generate meaningful insights for service and infrastructure providers (including Government, businesses, partners and consumers) who can make better informed decisions about service outcomes for their customers, places (or communities) and the asset(s).
- Smart technology is comprised of devices that can be connected or interconnected. It is comprised of hardware and other physical assets that are embedded with processors, sensors, data storage, software and connectivity that allow data to be

[2] State Infrastructure Strategy 2018-2018 p 19.

exchanged between the product and its environment, manufacturer, operator/user, and other products and systems.

Accordingly, smart technology encompasses everything from connecting a device to the internet so that it can be controlled and/or monitored remotely, to electronic devices that can collect data and communicate with other devices or systems, to using artificial intelligence and computing algorithms to make systems 'intelligent' so that they can make decisions without human intervention.

1.5 Benefits of smart infrastructure

Smart infrastructure will help the NSW Government to realise benefits including:

- Improved customer outcomes – agencies will be able to use data insights derived from smart infrastructure to improve customer engagement, personalise services to individual needs, and better understand how customers interact with infrastructure and the built environment.
- Productivity improvements – data and technology facilitate transparency and accountability for asset performance and capacity. This information can optimise asset performance, whilst also enabling agencies to apply these learnings to other existing and future infrastructure.
- Information driven decision making – agencies can use the data generated from smart technology to optimise the use of current and future infrastructure and its surrounds (i.e. comparing performance to scale efficiency gains across similar infrastructure, demand driven service delivery, more efficient design and construction of new infrastructure).
- Whole-of-lifecycle asset management – agencies can use this data to deliver user-centric infrastructure and proactively identify and predict maintenance and operational needs based on real-time infrastructure conditions. This can facilitate planned and preventative approaches to asset management that will result in a range of benefits – for example, reduced costs and service disruptions as maintenance is delivered as needed (rather than periodically).

Service delivery that has incorporated smart infrastructure is already a feature of some government agencies' work. The appendix at the end of this document highlights a couple of examples of Smart Infrastructure in NSW. The examples highlight success stories of smart infrastructure in the areas of transport and health.

1.6 Security challenges of smart infrastructure

The security of smart infrastructure (i.e. confidentiality, integrity and availability of devices and data) must be considered throughout the lifecycle, from design, implementation through to operation. In order to ensure these issues are addressed, the following key principles need to be adhered to:

- Security by design – this means using a risk-based approach and thinking about the security of devices and data in all design and ongoing activities.
- Network segmentation – this means separating the smart infrastructure networks from ICT networks, as well as separating high-risk systems within the smart infrastructure network (as appropriate).
- Standards approach – agencies must comply with NSW Government cyber security standards and policies, considering any local or international best practices. This needs to be baked into the design and ongoing management process to enable the systems to be updated as the standards evolve over time.

1.7 Privacy challenges of Smart Infrastructure

In addition to security challenges, privacy is also an important issue that needs to be managed. In order to ensure these issues and challenges are addressed the following need to be adhered to:

- Privacy by design – involves assessing privacy risks early, so you can ensure your project anticipates and addresses these risks. Follow the seven (7) foundational principles of privacy by design.
- Complete a privacy impact assessment – Review all of the privacy risks and mitigate against them. The PIA should evolve as the project evolves.
- Comply with the Information Protection Principles (IPPs), the Health Privacy Principles (HPPs) as well as any other applicable privacy legislation.
- Minimise the collection of personal information.

1.8 Design principles

The following principles will govern the design and deployment of smart infrastructure:

- Customer-centred and inclusive infrastructure - smart infrastructure design and development need to follow a user-centric approach that responds to the sustainable development needs of communities rather than being technology focused.

- Open and accessible – smart infrastructure relies on data to generate insights and inform decision-making resulting in better service outcomes. Data should be open by default and protected as required in accordance with the NSW Open Data Policy. Open data should be accessible on Data.NSW. It should be machine-readable, with open formats and have metadata to ensure it can be discovered and understood.
- Interoperability and flexibility - smart infrastructure technologies are rapidly evolving. Design and development of smart infrastructure components needs to be interoperable by adopting relevant open standards. Smart infrastructure needs to be designed to be flexible to future modifications and enhancements.
- Resilience and sustainability - the convergence of climate change, urbanisation and globalisation presents unprecedented challenges to society, including extreme events. Access to infrastructure is critical and smart infrastructure needs to be sustainable and resilient.
- Managing risks and ensuring safety - smart components raise new risks and safety concerns, as smart infrastructure could be prone to hacking and illegal access with an important consideration being the privacy of citizens. Smart infrastructure development must be supported by appropriate risk management and risk mitigation strategies to ensure it supports privacy, information management and cyber security by design.

1.9 Exemptions

This policy does not apply to infrastructure projects registered under the IIAF or the ICT Assurance Framework before 1 July 2020.

1.10 Compliance

All NSW public sector Secretaries and Chief Executives are responsible for ensuring that this policy is applied within their agencies.

1.11 Audience

This policy applies to all NSW Government Departments and Public Service Agencies in accordance with Schedule 1 of the *Government Sector Employment Act 2013*. Whilst the policy does not apply to State Owned Corporations, it is recommended and encouraged that they use it for new or upgraded infrastructure.

The term “agency” in this policy refers to any or all NSW Government Departments and Public Service agencies.

Alignment and coordination across all levels of government and industry is needed to realise the value of Smart Places and smart infrastructure. Councils, industry and the private sector are encouraged to adopt this policy.

2. Requirements for smart infrastructure

2.1 Needs assessment

All infrastructure projects subject to the IIAF and/or ICT Assurance Framework must complete an options analysis which must detail how the agency will incorporate smart technology as a significant component of the project spend. The analysis will ensure that each project maximises the benefits for customers and taxpayers. It will need to be completed prior to Gate 1 and Gate 2. Workbooks in both frameworks will be updated to include the definition of Smart Infrastructure and the requirement of an options analysis.

The Policy will come into effect from 1 July 2020.

The functional and performance requirements of smart infrastructure will depend on the nature of the infrastructure; the data that is needed to inform business practices, service delivery or asset planning, operations and maintenance; and customer needs (internal, external and end user). This may include network connectivity, sensors, controllers, display and information boards, computing power and computer processing capabilities. The solution should be informed by:

- analysis of existing and future infrastructure management (i.e. maintenance and operation requirements) to understand what is working well and what can be improved
- current and future needs of customers (or users) of the infrastructure
- location of the infrastructure and data that may be useful to improve the efficiency of that place or the services provided to its citizens and businesses
- analysis of the requirements for the infrastructure (i.e. what is the outcome that the agency is seeking? What are the data requirements for the agency? What are the data needs of other partners i.e. local councils, private sector, citizens)
- a clear understanding of how smart technology can optimise the use, management and ownership of the infrastructure, including consideration of the whole of life costs of the infrastructure, as well as impact on the operation and performance of the infrastructure (including safety)
- a national security risk assessment that covers foreign involvement in offshoring, outsourcing and procurement – including consideration of trusted vendors and insider threats – and cyber security threats and vulnerabilities.

2.2 Reference model for smart infrastructure requirements

A level of interoperability and standardisation is needed to achieve the social, economic and environment benefits of a smart place. The following reference model provides the

general building blocks to achieve this. Each layer has associated requirements which are defined at section 2.3. The combination of all layer's results in smart connected systems.

- **Security** – Security is critical and applies to all layers within the reference model. Security by design must be used ensuring the safe and secure operation of smart infrastructure and all associated data, information & privacy.

- **Application & Hosting layer** - applications and hosting services that enable development, operations and use the smart place solution/s. This includes such things as Dev Ops (code, build, test, release), operational systems (identity & access management, device & configuration management), and customer applications (mobile apps, web apps and wearable apps). Hosting services include DNS, cloud, edge computing, on premise etc.

- **Data & Intelligence layer** - solutions that enable data management & analytics. Systems that provide data ingestion, storage and distribution, using data standards and open formats. Smart technologies that enable data analysis, observing behaviour and patterns, learning and predicting, in order to produce insightful outcomes, and to drive smart actions. Smart technologies examples are Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL).

- **Connectivity layer** – networks and related integration services that enable the flow of control messages and data between field sensors (devices) to the data ingestion systems. It includes the network services (Cellular, RFID, WIFI, LoRaWAN etc.), network devices (Gateways, firewalls etc.) and integration (Integration platforms, standards MQTT, CoAP, HTTPS etc.)

- **Sensor layer** – smart assets such as sensors, actuators and devices that measure and monitor different parameters such as such as humidity, water, energy, temperature, occupancy, and state of equipment. This ranges from simple sensors and actuators, to more complex standalone devices such as tracking devices, smart meters, etc. to embedded devices in complex systems such as control systems etc.

Note: At the time of writing this policy, an industry standard for smart cities does not exist. Where relevant, components from IoT Alliance Australia IoT reference framework have been used in combination with language commonly used in smart cities publications.

2.3 Requirements

The table below sets out the requirements for smart infrastructure. Requirements that include:

- 'must' are mandatory

- 'should' are recommended (note: if these requirements are not followed, agencies may be at risk of not meeting the Government's commitment to smart places.

2.3.1 General requirements – applicable to all layers

Requirements	Why is it important
Agencies must select: • open technology and/or vendor agnostic platforms where available and suited to agency needs • open and recognised standards within and between the horizontal common layers of smart infrastructure.	Using open standards and platforms can: • improve an agency's ability to change the vendors it has paid to build, and support the solutions • reduce the cost of scaling to large numbers of devices and users of the solution. • increase the amount of alternate solution options available now or for future replacements/upgrades.
Smart infrastructure should be deployed for the following infrastructure types: • Power • Water • Waste • Ground & Air quality • Public spaces (safety & capacity) • Building management • Transport • Agriculture Any infrastructure that can obtain data to meet the local community smart place objectives	This requirement sets out a non-exhaustive list of infrastructure types where smart infrastructure should be deployed. Smart infrastructure creates smart places that can be used to reduce cost of living, increase quality of life, stimulate local economic activity, improve public safety, spaces and government services.
Smart infrastructure must adopt privacy by design. This includes minimising the collection of personal information and de-identifying identified data (where possible).	Privacy by design is the process of proactively identifying privacy risks during the design of smart infrastructure, so that risks can be mitigated as part of the design of the project. It allows privacy to be 'baked-in' from the beginning so that the smart technology solution is privacy-protective by default. Once personal or health information is collected, there are obligations under NSW legislation (and Commonwealth legislation in some cases) about how the data is held and accessed. Personal or health information should not be collected unless it is necessary. A privacy impact assessment will help identify privacy impacts on individuals and set out recommendations for managing, minimising or eliminating that impact.

	More information on privacy by design for smart technology be found in the Internet of Things Policy.

2.3.2 Security layer

Requirement	Why is it important?
Smart infrastructure must be secure by design and comply with the NSW Cyber Security Policy and Internet of Things Policy. Any local or international best practices also need to be considered. As a part of the NSW Cyber Security Policy: • high and extreme cyber security risks relating to smart infrastructure must be reported to Cyber Security NSW • any cyber security incidents detected against smart infrastructure must be reported to your agency or cluster cyber security team and subsequently Cyber Security NSW.	A consistent government wide approach on cyber security creates an environment that: • enables government to effectively focus on areas of improvement • can be more effectively managed in the event of serious cyber security incidents.
Procurement of smart infrastructure should use relevant State and/or Federal Government-approved panels or purchasing lists where possible. In instances where a panel or list does not exist or is not fit-for-purpose, State Government procurement processes must be followed including (but not limited to), an assessment of cyber security risks. This process must also consider capability to deliver compliance with State (and where applicable, Federal) government cybersecurity policy and legislative requirements.	It is important to ensure the products/services from the Vendor can meet the policy requirements to ensure the quality and functionality of vendor products and services. Vendors also need to have appropriate quality control measures and risk management in place to ensure their product is secure.
A comprehensive change management process must be developed which will document all network, device, credential, process, configuration changes with detailed information about at least what the change is, who requested and approved. The process must include a provision for retrospective and emergency changes.	Understanding the who, what, when, where and why of any changes to the smart infrastructure will help avoid accidently introducing vulnerabilities or data loss.

Requirement	Why is it important?
Agencies must ensure that common vulnerabilities are not present in smart infrastructure. This includes: • weak, guessable or hardcoded passwords • unneeded or insecure network services left running on devices • insecure update mechanisms • insecure ecosystem interfaces • use of outdated and unsupported components • lack of encryption for sensitive data at rest or in transit • lack of physical hardening The smart infrastructure should be assessed against the ACSC Essential 8 to ensure the appropriate controls are in place for each device. Not all elements of the essential 8 will be relevant for all devices. More information on the top cyber security vulnerabilities can be found in the Internet of Things Policy.	Smart infrastructure should be secure by design, meaning that it has been designed to be secure and built in such a way as to minimise flaws that can compromise security. This will help mitigate the risk of a significant incident impacting confidentiality, integrity, availability and safety. More information on the top cyber security vulnerabilities for smart technology can be found in the Internet of Things Policy.
Within the smart infrastructure you must centrally log alerts and alarms. Where possible, this will include change actions taken on all devices.	It is difficult for security teams to detect, respond or recover from cyber security incidents without logging and alerting in place
Any Smart infrastructure component (including devices and controllers) that use updatable software or firmware must be remotely and securely accessible	Agencies can minimise vulnerabilities and damage in the case of a cyber attack or security breach by making sure systems are up-to-date with all software release updates or patches regularly.
Software that is partially or entirely based on open source projects should include a statement of the benefits provided, how the software will be maintained and the process for ensuring no new vulnerabilities are introduced. **A risk assessment of the software must be conducted so that the potential impacts to maintenance, security and quality throughout the supply chain are understood and appropriately managed.**	Vulnerabilities in software can be minimised by ensuring that open source software is managed in a controlled, transparent manner. Open source software can lack the commercial assurances that help ensure the management of security issues throughout the product lifecycle. Where used, stakeholders should understand the potential risks and limited recourse available. The potential risks and impacts of using open source software should be considered so they can be managed and/or mitigated through a risk framework,

Requirement	Why is it important?
A comprehensive and secure backup/restore process must be built into the system for the smart device controllers. It needs to cover both data and configuration for all devices as appropriate. The backups should be verified and the restore process should be tested on a regular basis.	Backups will limit losses and recovery time in the event of a significant cyber incident
A comprehensive credential management process must be developed. It should incorporate strong password requirements, RBAC (Role based Access Control), certificate management and logging of any credential change activity.	Keeping passwords secure and of a high quality reduces the likelihood of an attack on the smart technology systems succeeding.
A defence in depth methodology to security is required, including security hardening of nodes and devices, network segregation, protecting sensors with reduced security capabilities, network access control (NAC) and role-based control, protection of data integrity and confidentiality, quarantine and remediation.	Defence in depth is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. These security requirements provide a better chance of stopping adversaries compromising smart infrastructure. If one control does not prevent the attack, another layer of security will.
Budget must be available to fund ongoing cyber security maintenance, vulnerability assessments and penetration testing for ICT.	Whole of life budgeting improves an agency's ability to identify and respond to security incidents.
Agencies must consider: • cost-effective and tamper resistant smart systems or device architectures • evolutionary trust models (i.e. trust is not static but dynamic, and associated values can change along time) for scalable and secure intersystem interaction • abstract and comprehensive security policy languages • self-monitoring and self-protecting systems, as well as development of (formal) methods for designing security and privacy into complex and interdependent systems • overall thread models that allow to take multiple sub-systems into account.	Cyber security resilience can be improved by the implementation of these practices and policies. Agencies can protect a system from a security breach or cyber-attack by adhering to the core security principles of confidentiality, integrity and availability, along with a broad range of clear cyber security policies, plans and systems. While advanced mitigation strategies like evolutionary trust models are recommended, they should not be implemented at the expense of basic cyber security controls and fundamentals.

Requirement	Why is it important?
Smart infrastructure must be segregated from corporate ICT systems. Where there is value in integrating the data with ICT systems ensure that appropriate cyber security protocols are in place between the two networks.	This ensures that if smart infrastructure is compromised it does not enable an attack on government ICT systems, or vice versa.

2.3.3 Application and hosting layer

Requirements	Why is it important?
Solution components that will have an impact to multiple users on failure must have redundancy.	A single smart device may fail in a smart place with minimal impact. If many (i.e. tens/hundreds or thousands) of smart devices fail this will have a significant impact to users. Outages to specific solution components will impact hundreds/thousands of smart devices. For example, device & user authentication, data aggregation, data distribution and event processing.
Any smart infrastructure solution component that should be loosely coupled designed.	Loosely coupled design means the components in a solution can more easily be replaced as opposed to tightly coupled that are hard to replace. Coupled refers to how the component is integrated into the overall solution via use of technology & interfaces (integration). The effort and cost to replace a component that is loosely coupled is typically less than a component that is tightly coupled.
The selected hosting services (onshore or offshore) must be appropriate to the sensitivity and risk of the information contained in the solution	If an agency choses a hosting service that is offshore and someone accesses the agency's solution or data without its consent, the agency needs to be comfortable it has the controls and legal support to contain, resolve and fix the problem in the appropriate time frames. Where data is hosted outside of NSW there are requirements under the Health Records and Information Privacy Act 2002 (NSW) and General Disposal Authority GA35 Transferring records out of NSW for

	storage with and maintenance by service providers based outside of the State. Concerns can be addressed by ensuring hosting of the data is in accordance with the Cloud Guidance and Policy, including a risk assessment of controls for ownership, access, security and privacy, exit clauses and return/destruction of data

2.3.4 Data and intelligence layer

Requirements	Why is it important?
Agencies must have a documented approach to data governance and management that considers authority, transparency, openness, real-time and usability.	Agencies need to have an agreed approach to data governance and management to ensure that high quality and relevant data is captured, stored, secured and used, and is available in formats and standards that enable its interoperability and use across the agency and beyond. Information on government policies, standards and processes are available via the Data.NSW Program.
The information security classification of the data should be determined and recorded in accordance with the NSW Government Information Classification, Labelling and Handling Guidelines.	The NSW Government Information Classification, Labelling and Handling Guidelines help agencies to identify the confidentiality requirements of their information assets, apply suitable protective markings and handle that information appropriately. It allows information to be shared among State and Commonwealth agencies with confidence that the information will be handled and protected according to its sensitivity.
Where possible, data sets must be open, available for re-use using standard formats and licensing that allow others to reuse the data in original ways. Consider sharing data if it cannot be made open.	Open government data supports transparency of government programs, allows improvement of services and citizen engagement with government, innovation and creation of new products and increased efficiency of government.
Data sets developed for monitoring, analytics and reporting that can be made open must be available on Data.NSW. Data which is spatially enabled would	Data.NSW provides a way to find and use NSW government open data.

benefit by being made available through the Spatial Collaboration Portal.	
Procurement specifications and contracts relating to smart infrastructure must address the following requirements: • NSW Government owns the data • data hosting location is appropriate to data sensitivity • cloud service (As A Service) model is appropriate to data sensitivity • data retention and destruction terms • **Open data standards**	It is recommended that NSW government agencies own data generated or collected by infrastructure. This ensures that agencies have all reasonable control over the data and provides flexibility to use the raw data for other purposes Hosting of the data should be in accordance with the Cloud Guidance and Policy, including a risk assessment of controls for ownership, access, security and privacy, exit clauses and return/destruction of data Use the NSW Government Information Classification, Labelling and Handling Guidelines to determine the sensitivity of the data. All data held by a service provider should be returned to government at the end of a contract, or when a service or relationship with a service provider is discontinued. Alternatively, evidence of data destruction can be provided if the destruction has been authorised. The *State Records Act 1998* (NSW) sets the rules for how government information needs to be stored and retained. More information on data ownership, retention and destruction can be found in Internet of Things Policy.

2.3.5 Connectivity layer

Requirements	Why is it important?
Data that relates to achieving the smart place objectives must be available via Application Programming Interface (API) that is documented and published on api.nsw.gov.au. These APIs must at a minimum be discoverable and self-describe themselves on an API call enabling machine to machine discoverability.	Achieving smart place objectives depends on data that an agency can find and use. APIs enables agencies to discover and share data. Api.nsw.gov.au is the standard repository for publishing APIs that can be used across NSW government.

APIs developed to meet smart place objectives must use the V3 and above OpenAPI specification https://swagger.io/specification/.	The cost or ability to use an API depends on how well it is designed, built & documented. Building to the OpenAPI specification standard increases the useability and should reduce a developer's time to code applications/systems that use the API.
Agencies should provide to smart infrastructure service providers a standard data model for API development specific to a domain (e.g. water, energy)	If the data model needed to realise a smart infrastructure objective is the same across different solutions; • cost to develop applications to access data should reduce • risk of incorrect data used in reports or analytics should reduce
APIs must use standardised tags to describe the infrastructure the data relates to (e.g. Haystack).	This requirement has the same cost & risk benefit as above: • cost to develop applications to access data should reduce • risk of incorrect data, reports or analytics should reduce.
The smart infrastructure network must implement redundancy and diversity at all layers (where economically feasible) to protect from node or link failure and to facilitate in-service maintenance. In the event of a failure, the network must rapidly reconverge (restore to full operation). The network infrastructure must notify when nodes are offline if redundancy is not feasible.	This will enable: • maintenance (planned outages) of the network without outages to users. • increase the likelihood of identifying and restoring network failures quicker reducing the impact of unplanned outages to users.
The network architecture must be scalable to support the current and future forecast bandwidth demands for two way communication, multi-tenancy, containers, devices and users.	A smart place will require multiple connected (integrated) solutions. These will be commissioned at different times. An agency will likely reduce costs if it reuses and scales out existing network services.
The network architecture should support user of hybrid cloud deployments, edge computing, multiple security zones, multi-tenancy and multicast technologies.	A smart place will require multiple connected (integrated) solutions. The network needs to support the likely cloud, security & tenancy requirements of these solutions.

2.3.6 Sensor layer

Requirements	Why is it important?
Deployed network devices must have the appropriate IP ratings for the environment it is being deployed in.	IP rated devices are built to handle environmental conditions such as heat, dust, water etc. Warranty may be void if a device is exposed to environmental conditions that it hasn't been built for. Note this is specific to the supplier.
Sensors must record their location in accordance with the spatial data requirements set out in the Internet of Things Policy (where possible).	The NSW Government is developing a digital twin, or digital copy, of NSW that will provide the visual model upon which government, developers and residents are able to plan, develop and assess infrastructure (such as transport links), new community facilities, public spaces and homes. It is important to record device location correctly in order to meet spatial data requirements. Having the data correctly recorded will lead to better analysis, identification of issues and solutions. More information spatial data requirements and the NSW Digital Twin can be found in the Internet of Things Policy
Smart infrastructure should use appropriate smart sensors and devices that are consistent with the Internet of Things Policy.	The Internet of Things Policy applies to all NSW Government agencies. It provides: • practical guidance to help organisations design, plan and implement internet of things (IoT) solutions • advice on standards and obligations where available and practical • tools and templates to help effectively manage an IoT- enabled project • guidance on where and how to source additional advice if required.

3. Appendix: Case Studies

3.1.1 Smart Infrastructure on the Sydney North West Metro

The Sydney Metro is the biggest urban rail infrastructure project in Australian history. The first stage of the Sydney Metro, the North West Metro, links to the North West suburbs of Sydney and opened on 26 May 2019. Within the first two weeks of operations, more than a million journeys had been taken. The 36-km metro line between Tallawong and Chatswood is the country's first fully automated (driverless) and fully accessible rail service. The line is equipped with all the infrastructure and technology required for the self-driving feature of the trains, directly sent to the train through a 5GHz communications system.

Smart technology, smart infrastructure and automation technologies have enabled the Sydney Metro to transform rail service delivery, providing more opportunities to connect communities and enhancing the experience of Sydney commuters with cost savings, better safety technologies and reduced travel times.

The benefits of Smart Infrastructure on the Sydney North West Metro

- Smart systems with in-built automation to continually control and monitor the health and status of the railway. These signalling and communications systems control trains, doors, tunnels, platforms and tracks to deliver a safe and reliable journey.
- Constant electronic monitoring by expert train controllers that monitor the entire metro system so they can track performance and can prevent and identify issues as they arise.
- Customers connected at all stages of their journey to help get to their final destination.
- 97.4 per cent of services in October 2019 met the required frequency of four minutes in the peak and 10 minutes in the off peak
- 94 per cent of services in October 2019 achieved the travel time of less than 38 minutes between Tallawong and Chatswood.

3.1.2 Smart Infrastructure at John Hunter Hospital

The John Hunter Hospital and John Hunter Children's Hospital is the principal referral centre and a tertiary hospital for Newcastle, and northern New South Wales, Australia. John Hunter hospital engaged private firm Schneider Electric to conduct a $6 million review of its energy management infrastructure and advise on solutions to reduce costs and power usage.

The objective was to incorporate smart infrastructure into the hospital to be able to reduce operational costs. Aging infrastructure was replaced with an Energy Management System for full-scaled utility energy supervision and control. Other improvements included upgraded lighting, solar hot water, boiler optimisation, and window tinting for high traffic areas of the hospital prone to harsh sunlight.

The benefits of Smart Infrastructure at John Hunter Hospital

John Hunter Hospital has been able to save more than $800,000 per year in energy costs as a result of the implementation of smart infrastructure. The implementation of smart infrastructure and technology has resulted in the hospitals:

- Carbon footprint being reduced by 22% per year
- Electricity usage cut by 23% per year
- Gas usage lowered by 14% per year
- Water usage trimmed by 3% per year