INTELLIGENT ACCESS PROGRAM

tca®
Transport Certification Australia

OVERVIEW OF THE IAP FUNCTIONAL AND TECHNICAL SPECIFICATION

© Transport Certification Australia Limited 2016.

This document has been published by
Transport Certification Australia Limited.

This document is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any person or process without the prior written permission of Transport Certification Australia Limited.

Transport Certification Australia Ltd
T +61 3 8601 4600
F +61 3 8601 4611
E tca@tca.gov.au
W www.tca.gov.au

ABN 83 113 379 936

Document Details

Title	Intelligent Access Program: Overview of the IAP Functional and Technical Specification
Document Number	TCA-G24
Version	1.0
Version Date	July 2016
Printing Instructions	Double sided, colour

Document History

Version	Date	Description
1.0	July 2016	Final

Transport Certification Australia Limited believes this publication to be correct at time of printing and does not accept responsibility for any consequences arising from the use of information herein. Readers should rely on their own skills and judgment to apply information to particular issues.

TCA™, Transport Certification Australia™, TCA National Telematics Framework™, TCA Certified™, TCA Type-Approved™, Intelligent Access Program™, IAP®, IAP Service Provider™, IAP-SP™, In-Vehicle Unit™, IVU™, Electronic Work Diary™, EWD™, On-Board Mass™ and OBM™ are trade marks of Transport Certification Australia Limited.

EXECUTIVE SUMMARY

The Intelligent Access Program (IAP) is a ‘world first’ – an initiative that represents a strategic means of utilising existing and new technologies in dealing with Australia’s growing freight task. The IAP meets industry demands for greater productivity, more efficient use of infrastructure, and addresses issues of community, government and industry confidence.

The IAP ensures that the right truck is on the right road at the right time. With the right technology and government and commercial arrangements, operators of heavy vehicles can be granted access, or improved access, to the road network, whilst governments can better manage the network itself, and better manage infrastructure assets.

Although the IAP has been operational in Australia since 2009 – and has been deployed as an operational pilot in Sweden – it is not widely understood by the public. There are a number of reasons for this.

Most road users have a right to access the entire road network – that is, they have *general access*. Other vehicles, such as large trucks or those carrying heavy pieces of equipment, may have *restricted access* – that is, they may be unable to cross a certain bridge, or travel on a certain road at a certain time. The community relies on heavy vehicles to transport all manner of things, but is unlikely to be aware of the complex policy decisions that affect the day-to-day use of heavy vehicles on the road.

Intelligent access is the name given to these complex policy decisions that make the road network safer, smarter, more productive, efficient and environmentally friendly through the use of telematics. It does so by making possible improved access for heavy vehicles. The IAP strikes a balance between industry demands and government responsibilities by creating new ways of using the road network, and new ways of doing business.

The IAP is now an important part of Australia’s heavy vehicle landscape, and an important part of the road network in general.

Another reason why the IAP is not widely understood by the general public is because it is technically complex, and involves a number of unique, ‘back office’ roles and responsibilities.

The operation of the IAP is enabled by the *Intelligent Access Program (IAP) Functional and Technical Specification* (TCA 2006), which sets out the requirements of the technical elements and the entities that are involved in the IAP environment.

Transport Certification Australia (TCA) is the national government body responsible for administering the IAP and the *National Telematics Framework*, of which the IAP is the inaugural application.

TCA has published this public overview of the IAP Specification to increase public understanding of the IAP, by translating the contents of a technically complex document into one that is understandable and useful to a general audience.

Contents

1 ABOUT TRANSPORT CERTIFICATION AUSTRALIA

Transport Certification Australia (TCA) is a national government body responsible for providing assurance in the use of telematics and related intelligent technologies, to support the current and emerging needs of Australian Governments and stakeholders.

TCA provides independent Advice, Accreditation and Administration services for a suite of transport-based policy reforms, and national and international initiatives that use telematics and intelligent technologies and transport systems.

TCA administers the *National Telematics Framework*, which provides a nationally-agreed, sustainable environment to support the current and emerging needs of government, industry sectors and end-users.

The Framework has been recognised by the International Standards Organisation, and its principles were endorsed by Australian Transport Ministers in 2008. The Framework aligns with the principles of the *Policy Framework for Intelligent Transport Systems in Australia*, approved in 2011.

TCA's work in deploying operational applications through the Framework, and management of the complex intersection of technical, policy, operational and commercial elements, is considered a world's best practice to facilitate public purpose outcomes through the use of telematics and related intelligent technologies.

2 WHAT IS TELEMATICS?

The term 'telematics' refers to integrated systems of information, communications and sensors to exchange data and information between vehicles and other locations, including:

- Vehicle to infrastructure (V2I) applications
- Vehicle to vehicle (V2V) applications
- Vehicle to elsewhere (V2X) applications.

The application of telematics and related intelligent technologies is increasingly being used across surface-based transport to improve the mobility of people and freight by improving safety, productivity and efficiency outcomes. This includes those outcomes that facilitate:

- Monitoring and reporting of vehicles and infrastructure
- Providing information to and from vehicles
- Connected and cooperative vehicles
- Automated and autonomous vehicles.

3 THE NATIONAL TELEMATICS FRAMEWORK

3.1 The need for a telematics framework

The Intelligent Access Program (IAP) is a sophisticated tool used to achieve a number outcomes, and is one application of a broader 'toolbox' that combines technical, policy, commercial and operational elements to deliver public purpose outcomes – the *National Telematics Framework*.

Over the last decade, governments have become increasingly interested in using telematics for regulatory purposes and to realise public purpose outcomes through policy. Simultaneously, telematics devices have come to perform multiple functions, and industry is realising the benefits of adopting intelligent transport technologies.

The *National Telematics Framework* allows governments to overcome the need to develop bottom-up technical solutions, and provides an effective nexus between the public and the private sectors. Technology-based operational programs with public-purpose outcomes can be delivered – without significant up-front costs to government and/or industry.

3.2 The *National Telematics Framework*

TCA administers the *National Telematics Framework* on behalf of Australian Governments.

The foundations of the *National Telematics Framework* were established by Australian Governments between 2005 and 2008, when decisions were made about the IAP – and future applications of telematics driven by the policy needs of government – to enable a sustainable approach to the use of telematics and related intelligent technologies in Australia.

The principles of the *National Telematics Framework* include:

- A multi-application, multi-provider operating model
- Performance-based functional and technical specifications
- An independent, national certifier and auditor of telematics systems and services
- A deliberate separation between technology and policy
- A framework that defines roles and responsibilities of participants and stakeholders.

These principles are widely recognised as a world's best practice approach to facilitate the sustainable use of telematics and related technology applications.

The Framework provides a nationally-agreed, sustainable environment to support the current and emerging needs of government, industry sectors and end-users, and supports the principles of the *Policy Framework for Intelligent Transport Systems in Australia*.

The Framework recognises the relationships between four interconnected elements essential to advance the use of telematics and related intelligent technologies, shown in Figure 1.

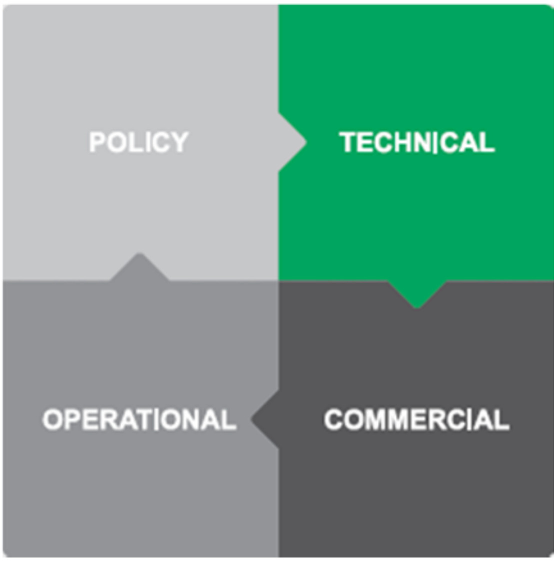

Figure 1: Elements of the *National Telematics Framework*

The Framework provides a critical intersection between public and private interests by:

- Providing a central point of reference for the deployment of telematics and related intelligent technologies in Australia
- Enabling the market to develop and deliver innovative technical, commercial and operational outcomes
- Ensuring public purpose outcomes are delivered through the use of telematics and related intelligent technologies by aligning policy and end-user intent
- Being technology agnostic and capable of being extended as needed to new applications as necessary.

This means that 'bottom-up' solutions are not needed to respond to policy challenges and/or opportunities, allowing policy makers to focus on outcomes, rather than technology inputs.

3.3 An international standard (ISO)

In 2012, the core elements of the Framework were recognised and adopted into *ISO 15638 – Framework for Cooperative Telematics Applications for Regulated commercial freight Vehicles* (TARV).

TARV currently consists of 22 elements to support a breadth – and the continued growth – of Intelligent Transport System (ITS) and Cooperative ITS applications, including access monitoring, driver fatigue management, speed monitoring, on-board mass monitoring, road use charging, emergency messaging and additional commercial services. The TARV series sits within ISO/TC 204 – Intelligent Transport Systems.

Adopting and aligning with TARV means that telematics and ITS can meet any number of commercial and regulatory outcomes.

4 POLICY CONTEXT

The roads on which we travel are not stand-alone stretches of bitumen or concrete, but part of an economic network that spans our suburbs, states, territories and the nation as a whole. This network also includes different types of vehicles, different driving conditions and responsibilities, rural and metropolitan roads and highways, small and large bridges, and any number of pieces of infrastructure.

To manage, optimise productivity, and ensure the safety of the roads and its users, there is a corresponding network of policies, laws and regulations that govern how the road network is managed, designating who and what uses it, and how they use it.

This network includes the institutions that contribute to and make these policies, and these policies affect both the transport industry and everyday drivers.

None of these policies exist in isolation. In fact, each is specifically designed to complement one or more existing policies by bolstering a particular policy aspect, addressing a unique need, or enabling a specific outcome that could otherwise not be achieved.

The *National Telematics Framework* aligns with and upholds the principles, strategies and long term outcomes of existing frameworks and strategies. By interfacing with nationally and internationally focussed initiatives, the Framework facilitates whole-of-government approaches and linkages with Australia's policy landscape.

The suite of policies with which the Framework aligns and upholds can be found at www.tca.gov.au.

As an application of the *National Telematics Framework*, the *IAP Functional and Technical Specification* – and the operational environment that it enables – aligns and interfaces with a wide variety of national, state and territory laws, regulations, policies, frameworks and strategic plans.

As a tool that provides heavy vehicles with access, or improved access, to the road network, the IAP both reflects the intentions, and enables the intended outcomes, of a number of national laws, regulations and policy frameworks, and a number of state and territory policies concerning the day-to-day operation of heavy vehicles. Chief among these are:

- *Heavy Vehicle National Law* – establishes a national scheme for facilitating and regulating the use of heavy vehicles on roads in a way that promotes public safety, manages the impact of heavy vehicles on the environment, road infrastructure and public amenity, promotes industry productivity and efficiency in the road transport of goods and passengers by heavy vehicles, and encourages and promotes productive, efficient, innovative and safe business practices. Chapter 7 deals explicitly with the IAP.
- *Heavy Vehicle (Mass, Dimension and Loading) National Regulation* – refines elements of the *Heavy Vehicle National Law*, and uses of the IAP.
- *Policy Framework for Intelligent Transport Systems (ITS) in Australia* – builds ITS into a shared vision of safe, sustainable, efficient, reliable and integrated transport. Telematics applications, TCA and the IAP are cited as examples of current and prospective uses of ITS for public purpose outcomes.
- State and Territory policies containing IAP Applications – An IAP Application is the generic term for road access schemes, permits, concessions, exemptions, gazettals or notices (the terminology depends on the Road Agency) that specify IAP as a requirement. These policies are set by Road Agencies – the road policy-making authority or authorities in a

given State or Territory. By specifying the IAP as a requirement, a Road Agency may be realising the outcomes of a single local policy, or aligning with any number of national or state policies, frameworks or strategies.

By remaining agnostic and adopting a performance based philosophy, the *National Telematics Framework* in general and the IAP in particular can align with or 'plug into' national and international policy environments. For example, the IAP has been used to assess the potential outcomes of Sweden's High Capacity Transports (HCT) reform.

5 PURPOSE OF THIS DOCUMENT

The *IAP Functional and Technical Specification* (IAP Specification) is the key document used by parties to become participants in the IAP, and informs the day-to-day operation of the IAP environment. Participants or aspiring participants and technology providers use the IAP Specification to identify whether the IAP is the right regulatory or commercial decision for their policy intent or operations, to ensure they can meet the standards required for the certification of their organisation, and for type-approval of their equipment.

Beyond those participants who must comply with it, the IAP Specification is largely of interest to the telematics industry, software manufacturers, and those in the ITS sector. Whether they are interested in submitting their existing devices for type-approval and endorsement for IAP, or embarking on developing a new device with the potential for use within the IAP, these entities need to know that their proposed device can meet the requirements of the IAP Specification.

Nonetheless, the IAP Specification remains a document with a limited audience, because much of its content articulates in technical terms the requirements of a complex operational environment. Administrative, cryptographic[1] and back office systems and protocols are essential to the IAP environment, yet have limited relevance for members of the public, and for drivers and Transport Operators with vehicles enrolled in, or interested in enrolling in, the IAP.

This public overview of the IAP Specification is intended to translate the functional and technical requirements of the IAP Specification into a document that is *understandable* and *useful* for members of the public, the transport industry, and other stakeholders.

The intention is to use conversational language to capture and convey to a general audience the requirements of the IAP Specification, while giving the reader an appreciation of these requirements, and of the IAP itself.

5.1 Note on the language used in this document

The IAP Specification is a technical document written for a technical audience. The language employed, and the words that are chosen, are very precise. For example, there are meaningful distinctions between requirements that shall, may and will be met, and these can relate to functionality of equipment, business capabilities, or the division of responsibilities. These distinctions are important for parties participating, or wishing to participate, in the IAP; less so for a general audience.

The public version of the IAP Specification provides an *active description* of how the IAP works. Where possible, this document avoids legalistic and technical language, omits details that are of

[1] Cryptography– the technique of sharing information that is neither accessible nor understandable to unintended parties. Only intended parties can 'crack the code,' and there are no 'eavesdroppers'.

little or no use to a general audience, and adopts a present-tense account of the requirements of the IAP, and how they give rise to an operational environment.

For example, where the IAP Specification reads:

> *The IVU GPS antenna shall be mounted in an elevated position that meets the manufacturer's specification for the vehicle combination and such that it optimises signal strength from the GPS satellites.*

The public overview reads:

> *When installed in a heavy vehicle, the GPS antenna must be in an elevated position.*

6 STRUCTURE OF THIS DOCUMENT

The structure of the full IAP Specification is technically complex. The public overview of the IAP Specification is divided into three simple sections, with each section capturing the IAP from a different perspective.

Part 1 gives a brief overview of what the IAP is and the entities involved, the philosophy that guides the IAP Specification's approach to leveraging existing industry standards, and its general approach to, and adoption and implementation of, technology.

Part 2 captures the parts of the IAP Specification and the IAP from an 'in-vehicle' perspective – that is, what equipment is installed when a vehicle is enrolled in the IAP and what this equipment does.

The perspective adopted in Part 3 is the opposite of Part 2 – it captures the 'behind the scenes' operation of the IAP, including the roles and responsibilities of entities involved, and the systems, policies and procedures that make the IAP possible.

7 PART 1: OVERVIEW OF THE IAP AND PHILOSOPHY GUIDING THE IAP SPECIFICATION

7.1 What is the IAP?

The Intelligent Access Program (IAP) is the ‘third generation of access’ to the Australian road network, complementing general access and restricted access with *intelligent access*.

The IAP is available to Road Agencies who decide when, where and how they want to use it; and enrolling a vehicle in the IAP is a decision made by a Transport Operator.

The IAP provides heavy vehicles with access, or improved access, to the Australian road network in return for monitoring of compliance with specific access conditions by vehicle telematics solutions.

7.2 How does the IAP work?

The IAP involves a number of roles, responsibilities and interactions, which are elaborated over the course of this document.

There are four distinct entities in the IAP operating model, each with their own responsibilities, as described below, and represented in Figure 2.

Road Agencies

Road Agencies[2] are all the Australian state and territory road transport authorities (e.g. VicRoads in Victoria, Department of Transport and Main Roads in Queensland, Main Roads Western Australia). Road Agencies may establish applications, schemes or permits to improve road access for heavy vehicles and use the IAP as a compliance monitoring tool.[3] The Road Agency examines both the proposed vehicle and the requested access to determine what effect, if any, the proposal may have on safety, infrastructure and the environment.

Transport Operator

A Transport Operator (i.e. a trucking company) enrols in a particular access arrangement – called an IAP Application – offered by a Road Agency, or may approach a Road Agency for a unique IAP Application which better suits its particular needs.

IAP Service Provider (IAP-SP)

An IAP-SP is a third party which provides telematics services, certified by TCA to provide IAP services. A Transport Operator engages an IAP-SP to install and maintain the in-vehicle technology used in the IAP, and to monitor its heavy vehicle from a back office system. The IAP-SP reports instances of non-compliance in the form of a Non-Compliance Report (NCR) to the Road Agency.

Transport Certification Australia (TCA)

TCA is the national government body, responsible for the administration of the IAP, certifying and auditing IAP-SPs, and type-approving the key pieces of equipment used in the IAP.

[2] All Road Agencies have road manager functions under legislation. In their capacity to receive Non-Compliance Reports (NCR – see section 9.5.1) in the IAP, some Road Agencies are regulators, while others act under the delegation from the NHVR.

[3] Since 2013, the National Heavy Vehicle Regulator (NHVR) is also able to instigate IAP Applications..

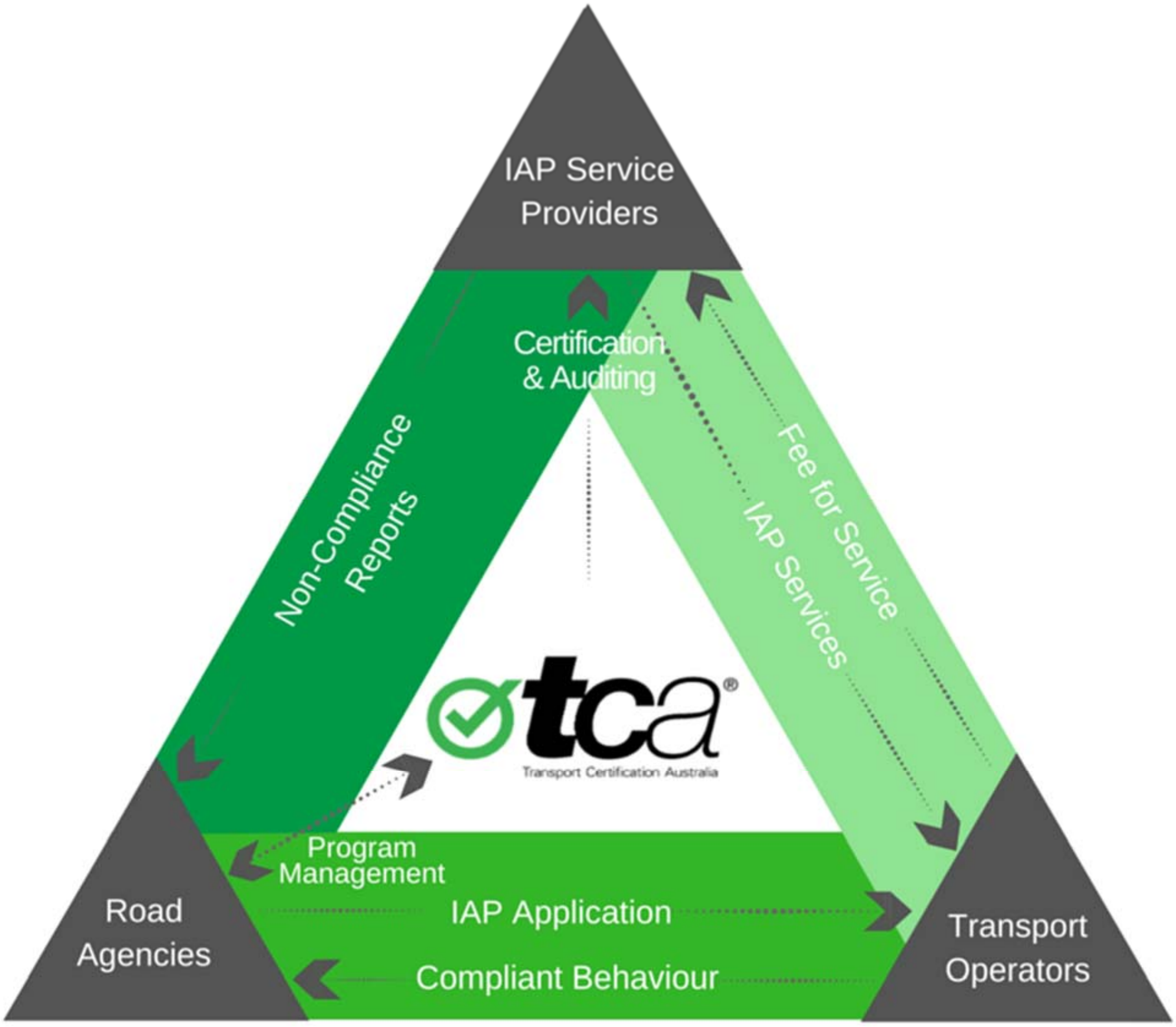

Figure 2: IAP Participants and Interactions

7.3 References and requirements

7.3.1 References

Inherent to the IAP approach is the leveraging of existing industry standards and best practices. This ensures that any implementation of the IAP does not 'reinvent the wheel' – rather, it incorporates and builds upon already existing and widely received standards, codes of practice and directives.

These standards can relate to safety requirements, technical capabilities, physical and information security management, administrative and business practices, and so on.

Standards can be international or national, depending on the policy objectives of the implementation – the goal is to leverage what is already available and what already works in order to achieve a 'fit for purpose' IAP.

As an application of the *National Telematics Framework*, the IAP itself has been acknowledged and adopted as an element within an International Standard (*ISO I5638 – Framework for Cooperative Telematics Applications for Regulated commercial freight Vehicles*). This means that the IAP and the *National Telematics Framework* have been received as world's 'best practices', and are internationally available to those wishing to implement or leverage them.

The specific standards leveraged by the Australian implementation of the IAP can be found in the full version of the IAP Specification, while more information about ISO 15638, the international adoption of the *National Telematics Framework* inclusive of the IAP, can be found at www.iso.org.

7.3.2 Requirements

The requirements of the IAP Specification are, as much as possible, performance based. In plain terms, this means that the requirements articulate outcomes that must be met, but do not articulate *how* they must be met.

Following a performance-based philosophy means that no matter where or how the IAP is implemented, as long as these requirements are met, a high quality government program is achievable.

This philosophy sets the IAP Specification apart from the majority of specifications, which prescribe both the 'what' and the 'how' – potentially resulting in inflexible, non-scalable implementations and proprietary environments, which are unable to keep pace with technological developments, and the evolving needs of government and industry.

The performance-based approach means that technology manufacturers and organisations are encouraged to develop innovative ways of meeting the various functional and technical requirements – both in terms of the technology they propose to use, and differing business practices.

This will enable the IAP to draw upon the best in available technology and practices as the environment develops from time to time and, indeed, to encourage its development, rather than simply availing itself of the technology which was available at a particular point in time.

7.3.3 Purpose and benefits of type-approval of In-Vehicle Units (IVUs)

The equipment used in the IAP is required to be of a high standard. The IVUs[4] – the telematics 'black boxes' installed in heavy vehicles – used in the IAP are required to undergo a process called type-approval.

Type-approval is a process that assesses a 'type' of equipment against a set of criteria to ensure that it can deliver specific, desired outcomes. These criteria commonly take the form of requirements set out in a specification that has been produced in consultation with policy makers and industry stakeholders, including original equipment manufacturers and potential consumers of the piece of equipment.

Manufacturers submit a piece of equipment, along with the necessary documentation, for type-approval so that it can be made available for a particular use. An IVU can be built into or distributed within a vehicle, or can be a separate piece of equipment.

The assessments performed by TCA involve the type-approval of IVUs, and IVUs that are both Type-approved and endorsed for the IAP.

[4] In-Vehicle Unit (IVU) is the term employed in this Specification. However, similar devices are known internationally as On-Board Units and On-Board Equipment.

Type-approval processes are commonly carried out by an independent, impartial entity, usually a government body. In the ISO adoption of the *National Telematics Framework*, for example, the entity responsible for conducting the type-approval process (among other responsibilities) is generically termed the Approval Authority. In the Australian implementation of the IAP, TCA performs this role.

The primary purpose of type-approval is to provide assurance that a *type* of a piece of equipment – a specific configuration or model, including hardware, firmware, software and physical characteristics etc. – meet the minimum functional and technical requirements for a particular purpose. If any of these characteristics are altered, the type-approval of that type of equipment is no longer valid.

It is equally important that type-approval provides a means for consumers to make informed choices when making procurement decisions. When there are multiple options available on the market, each claiming to deliver the same as or more than competing models, the type-approval process provides consumers with a selection of products that have been proven to deliver on their claims.

Type-approval is also beneficial for governments and regulatory uses of technology. It is not uncommon for governments, when using technology to achieve policy outcomes, to become inadvertently ‘trapped’ or ‘locked in’ by a single manufacturer or provider. This means that while a given piece of technology may satisfy present requirements, it may not be able to evolve with policy decisions. An equally undesirable outcome is when an effective policy becomes hostage to advancements in technology.

The type-approval process allows policy makers to establish their needs, encourages multiple providers and manufacturers to come forward with different technology solutions that satisfy these needs, whilst also leaving room for additional functionality for commercial purposes.

Type-approval also caters for governmental and regulatory uses of technology that may require higher standards than the commercial sphere for the purposes of law enforcement. However, a type-approval process that ensures reliability, accuracy, integrity and security is obviously beneficial for commercial operators, and puts them at a competitive advantage by distinguishing their business and procurement practices from others.

For the IAP, only type-approved IVUs, which are endorsed for the IAP, can be installed in heavy vehicles. This provides the foundations for collecting, storing and transferring data. Getting the hardware and software right before operations commence ensures that end-use objectives can be reliably managed.

8 PART 2: IAP SPECIFICATION – IN-VEHICLE OPERATIONS

8.1 Overview

Part 2 of this public overview of the IAP Specification captures the requirements and operation of the IAP from an in-vehicle perspective – that is, what is required and what occurs when a vehicle enrolled in the IAP is operating.

This part of the document focuses primarily on the equipment that is used in the IAP. While the IAP uses a number of advanced technologies, it is important to note that the IAP is first and foremost a tool to realise policy intent. This means that the equipment detailed in this part of the document *does not drive* policy, but *enables* its objectives.

This part of the public overview of the IAP Specification encompasses the following:

- The requirements, functionality and purpose of equipment installed in vehicles, including type-approved IVUs and Self Declaration Input Devices (SDID)
- The types of data collected by the IVU and SDID
- The types of records that are generated from the data collected by the IVU and SDID, and how they are handled and transferred from the IVU to the IAP-Service Provider (IAP-SP).

8.2 In-vehicle equipment used in the IAP

Each vehicle enrolled in the IAP needs to be fitted with a telematics 'black box' called an In-Vehicle Unit (IVU), which is one of two pieces of in-vehicle equipment used in the IAP. The IVU can be a piece of equipment, or built into and distributed in the vehicle. The other piece of in-vehicle equipment is the Self Declaration Input Device (SDID), described below. Together, they collect and generate the data that forms the basis of the monitoring that occurs in the IAP, which is transferred to the IAP-SP from the IVU.

8.2.1 In-Vehicle Unit (IVU)

Description and purpose

A type-approved IVU used for the IAP meets the requirements of, and behaves in accordance with, the descriptions contained in this section.

Although somewhat similar to a 'black box' or flight recorder used in aeroplanes, IVU is a collective term that includes a Global Positioning System (GPS) receiver and antenna, a communications device, and all associated cabling and connections. IVUs must be type-approved, as per section 7.3.3.

The data collected and transmitted by an IVU is detailed below. Broadly, for IAP purposes, the IVU collects, monitors, stores and transmits GPS and other required data. In addition to automatically collecting data, the IVU is also capable of receiving data the driver may be required to enter themselves. This is called a self declaration, for which the driver uses the SDID, a touchpad/keypad/screen with which the driver can interact.

The IVU and its functions follow the 'one box, many uses' approach of the *National Telematics Framework* – that is, it can be used for the IAP, and for other commercial purposes. The components that make up an IVU and its uses must be clearly documented by the IAP-SP. Provided that TCA is notified and approves, and the functioning of the IAP is not compromised, the IVU can be used for any other purpose.

The IAP-SP is responsible for providing the IVU to the Transport Operator, and for its correct installation and ongoing maintenance (this process is described in detail in Part 3 of this document).

Identifiability and security features

Because each vehicle enrolled in the IAP is required to have an IVU, each IVU used in the IAP is unique to a single vehicle, and are themselves uniquely identifiable.

An IVU is installed in the prime mover of the vehicle, and monitors that vehicle alone – it cannot be associated with more than one vehicle.

A vehicle enrolled in the IAP may or may not be allowed to change the type or number of trailers it tows (this is called a vehicle 'combination').[5] Even when the vehicle changes trailers, it is still being monitored under the IAP, because the IVU is installed in the prime mover.

Each IVU has a unique serial number that unambiguously identifies the physical device (by a visible etching or marking) and the data that it collects and transmits. The serial number is called an identifier (IVU ID) and is alphanumeric – a combination of letters and numbers. An IAP-SP can set and alter the IVU ID, but it must otherwise not be able to be modified, removed or tampered with.

In addition to the unique identifier that distinguishes the physical IVU and the data it supplies, an IVU has physical security seals. Security seals are used to deter and provide evidence of unauthorised tampering with the physical device.

If the security seals are broken, they cannot be reinstated, and they need to be designed in such a way that any attempt to break them can be clearly identified. Security seals must meet the requirements of relevant national or international standards.

Even if the IVU's power supply fails or shuts down, the IVU can retain stored data for a period of time, and can continue to monitor the vehicle's connectivity to the IVU.

Suitability for use in vehicles

It is important that other non-IAP equipment installed or used in the day-to-day operation of a vehicle does not interfere with or compromise the IVU, and vice versa.

The performance of an IVU must not be unduly affected by external factors that may be present during its day-to–day use.

An IVU must meet the requirements of relevant national or international standards relating to vibration, impact, cold or hot temperatures and levels of humidity.

An IVU must also meet the requirements of relevant national or international standards to ensure that it is protected from electromagnetic and radio interference, and be physically positioned and robust enough to be protected from the entry of dust and water.

Additionally, an IVU must not negatively affect the performance of other equipment, and must meet the requirements of relevant national or international standards relating to electromagnet emissions.

[5] If required, a separate type-approval process can be undertaken in order for an IVU to automatically identify and record the presence and information of trailers connected to the prime mover. In this scenario, the IVU communicates with a Trailer Identification Device (TID), which must meet requirements similar to those of an IVU. Data from up to ten trailers can be recorded.

An important component of the IVU is its GPS capability. The GPS receiver and GPS antenna of the IVU must meet the requirements of relevant national or international standards and the licence that authorises transmission or reception of radio emissions. When installed in a heavy vehicle, the GPS antenna must be in an elevated position.

8.2.2 Self-Declaration Input Device (SDID)

The second piece of in-vehicle equipment used in the IAP is the Self Declaration Input Device (SDID). Although the SDID interacts with the IVU, there are some important differences between the operation and requirements of these two pieces of equipment.

The SDID is used to input and collect data and facilitate the generation of records that are not automatically generated by the IVU. These are outlined in further detail below.

Unlike an IVU, not all vehicles enrolled in the IAP have a SDID installed– only those that are required to by the Road Agency to satisfy a particular purpose. In cases like this, the driver is obliged to use the SDID to input data at certain times (more on this below).

Furthermore, unlike IVUs, SDIDs are not required to undergo type-approval, but must meet the requirements of the IAP Specification.

Like the IVU, provided that TCA is notified and approves, and the functioning of the IAP is not compromised, the SDID can be used for other, non-IAP purposes.

The SDID may be a touchpad/keypad/screen that the driver uses to make to input data into the IVU, which is called a self-declaration.

The SDID is inclusive of the hardware, software and cabling and connections leading up to, but not including, the IVU. The SDID can only input data into the IVU – it cannot access or modify IVU data or IVU software.

To assist the driver to meet any obligations they may have, when the SDID or the vehicle's ignition is turned on, the SDID immediately prompts the driver to make a self declaration, and prompts are repeated at least once every 24 hours.

8.3 Data collected in the IAP

This section describes the data that is collected in the IAP for regulatory purposes.

Most of the data collected in the IAP is done so automatically by the IVU. Other data is input by the driver into the IVU via the SDID.

There is an important distinction to be made between data and Data Records. The former can be understood simply as 'raw data,' whilst the latter are bundles of data, processed by the IVU to form a record, which are themselves further compiled to form Data Blocks. Data Records and Data Blocks are detailed in the following section of this document.

Altogether, the IVU collects the following types of data, which are individually defined and explained below[6]:

- Date and time data
- GPS quality data
- Vehicle position data
- Vehicle direction of travel data

[6] Trailer identification data can also be collected by the IVU, if the vehicle's combination is being monitored, in which case it will be fitted with one or more Trailer Identification Device.

- Vehicle speed data (if applicable)
- Alarm status data
- Self Declaration (SD) data (if applicable).

8.3.1 Date and time data

The IVU collects and stores date and time data in Coordinated Universal Time (UTC) format.[7]

The date and time is stored with a resolution of 1 second.[8]

The IVU has an internal clock that can continue to work for a period of time if the IVU is disconnected.

The accuracy of the IVU internal clock is such that it does not deviate by more than 1 second.

8.3.2 GPS quality data

The quality of GPS data is determined by the number satellites that an IVU's GPS receiver can see, and how well placed they are in sky.

TCA uses its software and systems for the purposes of type-approval, and to ensure the GPS quality of the IVU.

8.3.3 Vehicle position data

The IVU GPS receiver determines the position of the vehicle.

If an IVU's communication with GPS satellite signals is interrupted, it must resume recording vehicle position once the signal is reacquired.

8.3.4 Vehicle direction of travel data

The IVU GPS receiver determines the direction in which the vehicle is travelling.

8.3.5 Vehicle speed data

The IVU GPS receiver determines the speed of the vehicle.

8.3.6 Alarm status data

There are a range of alarm conditions that are transmitted and are designed to monitor the proper functions of the IVU and to detect tampering of the device. For example, if an IVU is disconnected or reconnected, this is reflected in alarm status data.

If the IVU is disconnected, it is still possible to detect if a vehicle has moved via two non-GPS based features.

8.3.7 Self declaration (SD) data

There are two types of data that can be input into the SDID that are not automatically generated by the IVU.

The first type of SD data is related to Vehicle Type (e.g. B Double) and Total Combination Mass (the combined mass of the laden or unladen trailer(s) and the prime mover/rigid truck). When the

[7] UTC is the time standard used and coordinated globally.

[8] Resolution is different from accuracy, in that it relates to the smallest unit that can be reliably reported.

driver inputs this data, they select from a list of vehicle types, and also record the number of axles the combination has.

The second type of SD data are comments. A driver selects a generic comment category (e.g. road closure) and can then make any additional comments.

Both the lists of vehicle types and comment categories are able to be expanded, to meet the evolving needs of Road Agencies.

8.4 Data Records generated in the IAP

The data collected in the IAP is combined to generate Data Records which are transferred to the IAP-SP.

This section describes the Data Records that are generated and transferred in the IAP for regulatory purposes.

Records are generated when the IVU processes the types of data in the previous section into Data Records. These are then stored by the IVU and transferred to the IAP-SP.

Altogether, the IVU stores and transmits the following types of Data Records, which are individually defined and explained below:

- Position Records
- Speed Records (if applicable)
- Alarm Records
- SD Records.

8.4.1 Record numbering

All Data Records generated by the IVU are assigned a record number. Data Records are numbered successively, in the order in which they are generated. The cycle of the numbering sequence used is such that no single record can be mistaken for another.

Position, Alarm and SD Records share the same numbering sequence, while Speed Records have their own, separate sequence, and one sequence cannot be mistaken for another.

8.4.2 Record storage in the IVU

Before they are transferred to the IAP-SP, Data Records are stored in the IVU.

The IVU must be able to store a minimum number of Position, Alarm and SD Records (combined).

8.4.3 Handling and transfer of data from the IVU to the IAP-SP

The generation of data by the IVU into Data Records, and their subsequent transmission to the IAP-SP in the form of Data Blocks is the final step in the perspective of in-vehicle operations of the IAP.

Data generated by the IVU is subject to strict requirements relating to security and confidentiality. The IAP-SP has a method of authenticating and proving the integrity and origin of Data Records.

It is not possible for collected or stored data or software memory within the IVU to be accessible or capable of being manipulated by any person, device or system (including the SDID), other than that authorised by the IAP-SP. Security and confidentiality of data stored in the IVU is maintained at all times.

Data stored in the IVU is scheduled to be transferred to the IAP-SP at least once every 24 hours. A transfer can only take place when the vehicles ignition is on. If the ignition is not on when a transfer is scheduled, the transfer takes place within five minutes of next time the vehicle's ignition is on. Only after the transfer is completed and confirmed by the IAP-SP can data be deleted from the IVU.

IVU Data records are transferred to the IAP-SP in the form of Data Blocks. These can be compressed, provided they can be fully reconstructed when decompressed.

Like IVU Data Records, Data Blocks are numbered successively, in the order in which they are generated. The cycle of the numbering sequence used is such that no single Data Block can be mistaken for another.

Position Records

The IVU generates and stores records of the vehicle's position every 30 seconds when the vehicle's ignition is on. These are called Position Records.

A Position Record consists of at least the following data:

- Record number
- Date / time of generation (UTC format)
- Vehicle position (latitude/longitude)
- Direction of travel
- GPS quality
- Non-GPS based features.

Speed Records

If applicable, the IVU generates and stores records of the vehicle's speed every 3 seconds.

The IAP-SP processes Speed Records either in the IVU, the IAP-SP System or a combination of both.

A Speed Record consists of at least the following data:

- Record number
- Date / time of generation (UTC format)
- Vehicle position (latitude/longitude)
- Vehicle speed
- GPS quality.

Alarm Records

Whether the IVU is connected or disconnected, it generates Alarm Records when it detects possible instances of tampering, unauthorised access, and when parts of the IVU are disconnected and reconnected.

An Alarm Record consists of at least the following data:

- Record number
- Date / time of generation (UTC format)
- The event that triggered the generation of the Alarm Record.

Self Declaration (SD) Records

Data entered into the IVU via the SDID contains information about vehicle type and/or comments. The IVU processes this data into two separate SD Records.

An SD Record consists of at least the following data:

- Record number
- Date / time of generation (UTC format)
- Vehicle category
- Number of axles
- Total Combination Mass
- Comments (if applicable).

9 PART 3: IAP SPECIFICATION – SYSTEMS, POLICIES AND PROCEDURES

9.1 Overview

While Part 2 of this public overview of the IAP Specification captured the requirements and operation of the IAP from an in-vehicle perspective, Part 3 captures the requirements and operation of the IAP from the opposite perspective, relating to IAP-SP systems, policies and procedures.

As highlighted at the start of Part 2, the in-vehicle equipment used in the IAP does not drive policy, but enable its objectives. The requirements and operations relating to systems and procedures outlined in this part of the document are further enablers of policy intent and detail those decisions that are implemented as a result of policy decisions.

This part of the public overview of the IAP Specification encompasses the following:

- Roles and responsibilities of IAP Service Providers (IAP-SP)
- What the IAP monitors and how it is monitored
- The Intelligent Access Map (IAM)
- Identification of non-compliance and issuing of Non-Compliance Reports (NCRs).

9.2 Roles and responsibilities of IAP Service Providers (IAP-SP)

9.2.1 Importance of certification of IAP-SPs

An IAP-SP is a third party which provides telematics services (such as fleet management systems and services) to the transport industry.

Only suppliers certified by TCA can deliver IAP services. If a supplier is certified, this means that TCA has been satisfied that the IAP-SP's operations conform with the requirements of the IAP Specification. When certifying an IAP-SP, TCA assesses the capabilities and conformance of:

- IAP-SP System – the IAP-SP's hardware and software (excluding IVUs and SDIDs) used in the collection, processing, testing, storage and reporting of IAP data
- IAP-SP Quality System – the IAP-SP's other back office systems and processes, including a Quality Monitoring Station, which is used to monitor the performance of IVUs.

9.2.2 Provision, installation and ongoing maintenance of IAP in-vehicle equipment

In addition to monitoring enrolled vehicles, the IAP-SP is responsible for providing, installing and monitoring the ongoing performance of equipment used in the IAP – namely, the IVU and SDID.[9]

To receive and maintain certification, IAP-SPs must provide only TCA type-approved IVUs for vehicles enrolled in the IAP. This does not preclude the IVU's use for other commercial or regulatory purposes, and it ensures that the requirements of the IAP can be met.

The IAP-SP is responsible for the correct installation of all IVU hardware and software, and installation of the IVU itself in the vehicle.

[9] If required, these responsibilities can also extend to Trailer Identification Devices.

The IAP-SP is also responsible for undertaking and documenting the IVU's ongoing operation and maintenance. This includes scheduled checks for physical signs of tampering and wear and tear, replacing batteries, checking the integrity of connections, and resolving malfunctions.

If the IVU malfunctions, or does not function in accordance with the requirements of the IAP, the IAP-SP and the Transport Operator work together to resolve the issue. The IAP-SP must also report the issue to the relevant Road Agencies, and ensure transfer of IVU Data Records to their system for processing.

The IAP-SP must also report any evidence of tampering, attempted tampering, and of malfunction which appears to be the result of tampering.

IAP-SP responsibilities for installation and maintenance of IVUs also extend to SDIDs (both hardware and software), with one important difference. First, installation of the IVU should not interfere with the vehicle's normal operation, and is therefore performed in consultation with the vehicle manufacturer; installation of the SDID is consistent with relevant national or international guidelines on installation of in-vehicle technologies/devices. The IAP-SP must also document the communications protocols for data transfers from the SDID.

9.2.3 Systems, capabilities and data handling requirements

The IAP-SP's Quality System, and approaches to information security and human resources (policy, staff changes, access to information, physical and environmental security, etc.) – must meet the requirements of the relevant international or national standards.

A high level of transparency in these matters is required of IAP-SPs for auditing purposes to maintain their certification.

To receive and maintain certification, IAP-SP Systems must be able to support the number of IVUs for which they are responsible to monitor. This includes having sufficient transfer capability and processing capacity.

The IAP-SP operates a Quality Monitoring Station (QMS), which is used to monitor the performance of IVUs and their compliance with the requirements of this IAP Specification. The QMS includes one of each type of IVU monitored by the IAP-SP.

The IAP-SP receives data from an operational vehicle's IVU as least once every 24 hours. Data is backed up daily, and appropriately archived.[10]

The IAP-SP tests data for its completeness and consistency, and for any errors. The GPS quality of Position Records, and possible IVU malfunctions, are also tested.

If the IAP-SP System malfunctions, or does not function in accordance with the requirements of the IAP Specification, the IAP-SP reports the issue, and the time expected to take to resolve it, to TCA. TCA needs to be satisfied with any resolution to a malfunction or issue, and also be alerted to any evidence of tampering, attempted tampering, and of malfunction which appears to be the result of tampering.

The IAP-SP documents and records all installation, programmed maintenance and resolution of malfunctions for the IAP-SP System, and keeps these documents on record for a minimum of four years.

[10] As an alternative to providing and using a SDID – and providing TCA approves – the IAP-SP can arrange to have the Transport Operator's self-declared data entered directly into the IAP-SP System.

The IAP-SP's information security management practices must comply with relevant international or national standards, and the security and confidentiality requirements of their certification agreement with TCA.

Their data storage and processing facilities are required to be electronically and physically secure, and access is restricted to approved personnel on a need-to-know basis – users only have access to what is required for them to perform the responsibilities of their job. Records are kept of what data is accessed, and of who accessed it.

9.2.4 Auditing

To achieve and maintain certification, the ability of IAP-SPs to meet the requirements of the IAP Specification is reviewed and audited by TCA.

This process includes providing TCA access to all IAP data and documentation, and supplying type-approved IVUs and one SDID.

Any changes to the IAP-SP System, QMS or Quality Systems need to be approved by TCA before they are made, and require the IAP-SP to undergo re-certification.

9.3 What the IAP monitors, and how it is monitored

9.3.1 Intelligent Access Conditions (IAC)

This section defines and describes the purpose of four important elements of the IAP: IAP Applications, Intelligent Access Conditions (IAC), IAP Conditions, and Interim IACs. The first three are part of the day-to-day operation of the IAP, whilst Interim IACs are part of a process that occurs when a Transport Operator applies to commence with, or utilise a new application of, the IAP.

When a Transport Operator wishes to utilise the IAP, they apply through a Road Agency to join an IAP Application. An IAP Application is the generic term for road access schemes, permits, concessions, exemptions, gazettals or notices that specify IAP as a requirement.

To make use of that IAP Application, the Transport Operator must comply with an Intelligent Access Condition (IAC). A vehicle may operate with any number of IACs, depending on the tasks it performs, and the requirements established by the Road Agency.

IAP Conditions are contained within an IAC, and include the conditions the Transport Operator needs to comply with. IAP Conditions can either be 'off-the-shelf' (standard and made developed for widespread use) or unique (a condition tailored to specific requirement).

This section will cover off-the-shelf IAP Conditions, because they are the most commonly used.

Vehicle position (spatial compliance) is an IAP Condition that is used to determine if a vehicle strays off an allowed route, or enters a prescribed zone. Other IAP Conditions may require that a vehicle does not exceed a certain speed (speed compliance), or that it does not to use a part of the road or piece of infrastructure at a certain time (temporal compliance). These three conditions – spatial, temporal and speed – can be monitored automatically through the IVU.

There are other conditions that a Road Agency may require that are collected by self-declarations, where the driver inputs the information through their SDID. These Self Declaration (SD) Conditions can relate to the type of vehicle and number of axles, or Total Combination Mass (the combined mass of the laden or unladen trailer(s) and the prime mover/rigid truck).

An IAC may have multiple IAP Conditions of the same type – for example, multiple Spatial Conditions relating to a number of allowed or disallowed routes or zones.

Road Agencies supply the IAC and its IAP Conditions to the IAP-SP. The IAP-SP tests them with their systems, and ensures that the IVU collects the data necessary for the Transport Operator to demonstrate compliance with the IAP Condition.

An IAP-SP or Transport Operator can request cancellation of an IAC, although only a Road Agency can make the decision to cancel it. Any changes to an IAC cause the IAC to be cancelled, and a new one to be issued.

When a Transport Operator commences the application process, the Road Agency issues them with an Interim IAC. The Interim IAC contains information about the period for which the IAC is applicable, the IAC Conditions, and the Transport Operator's details and the specific vehicle and, if applicable, the vehicle combination to be used.

By issuing an Interim IAC, the Road Agency indicates their intention to grant the IAC, provided the Transport Operator engages an IAP-SP (if they are not already IAP participants, and have no existing Agreement with one).

If the Transport Operator does not have an existing Agreement with an IAP-SP, they need to enter into one. The IAP-SP reviews the Interim IAC, verifies that the Transport Operator's vehicle matches the one proposed in the IAC, and then installs the relevant IAP equipment (IVU, SDID etc.) and ensures that it is working. This information is then sent back to the Road Agency for approval of the IAC. The IAP-SP commences monitoring of the IVU, and the Transport Operator can commence using the IAP Application.

9.3.2 IAP Conditions: Spatial, Temporal, Speed and Self-Declared

The IAP-SP monitors vehicles for compliance with the IAP Conditions as specified by the Road Agency in the IAC. These can be a single condition, or a combination of Spatial, Temporal, Speed and SD conditions.

Spatial Conditions have additional layers of complexity, and are outlined here.

When a vehicle's use of a certain route or access to a particular zone is monitored for compliance, this type of IAP Condition is called a Spatial Condition, and is specified in an IAC.

An IAC can contain multiple Spatial Conditions, and a vehicle may have a number of IACs, each with different Spatial Conditions.

A Spatial Condition details where access is allowed, or where access is not allowed.

If there are multiple Spatial Conditions in an IAC, the set of conditions operates in a hierarchy: Absolute-inclusion, Exclusion, Inclusion, in that order.

Absolute-inclusion means that the route or zone is allowed and this access takes precedence over any other Spatial Condition which may apply to any access point in the Absolute-inclusion route or zone.

Exclusion is where access is not allowed. Exclusion takes precedence over other Inclusion conditions which may apply to any access point in the Exclusion route or zone.

Inclusion is where access is allowed. If there is an Exclusion condition it would normally be spatially set within an Inclusion condition.

For instance, a vehicle can be granted access to all of the metropolitan areas of a capital city (Inclusion) but denied access to the streets of the CBD (Exclusion). When considering points within the CBD they have two conflicting conditions applying to them (one Inclusion and the other Exclusion). The Exclusion takes precedence over the Inclusion and the vehicle must not access the CBD but can access areas outside of that zone within the broader metro area.

9.4 Intelligent Access Map (IAM)

The compliance of vehicles with access conditions is monitored with reference to an electronic map.

To convert the vehicle's position as captured by the IVU into an actual location, the IAP uses spatial mapping data. The Intelligent Access Map (IAM) is the approved and issued electronic road network map providing the 'reference' from which heavy vehicles' compliance with their IAC is determined.

TCA issues the IAM, and updated versions on a scheduled, quarterly basis, to IAP-SPs and Road Agencies.

The IAM is provided by a mapping data entity that can meet the requirements of the IAP Specification.[11]The use of this single map ensures a 'one route, one map' policy, and that the data is the latest available, appropriately checked and reviewed, and consistent across jurisdictional boundaries.

9.5 Identification of non-compliance and issuing of Non-Compliance Reports (NCRs)

9.5.1 What is an NCR and what behaviour is reported?

An IAP-SP System receives Position, Speed, Alarm and Self Declaration Records from monitored IVUs at least once every 24 hours. The IAP-SP then assesses the data sent by the IVU to determine if the vehicle has not been compliant with an IAC.

If the assessment detects an instance of non-compliance with an IAC – or of possible tampering – the IAP-SP generates and issues to the Road Agency a Non-Compliance Report (NCR), itemising each instance of non-compliant behaviour against the relevant IAP Conditions in the IAC.

This section deals with the kind of NCRs that can be issued if an IAP-SP assessment of those records against the relevant IACs determines incidents of non-compliance.

The NCR may include, as relevant, the vehicle's position, speed, the day and time at which the incident occurred, and any self-declared records, which might justify the non-compliant behaviour, e.g. a road closure resulted in the vehicle taking an alternative, non-approved route.

It is important to note that, in the IAP, *only instances of non-compliant behaviour are reported* – the Road Agency has neither full nor immediate access to data generated by IVUs, and only NCRs relate to their Road Agency alone.

It is equally important to note that the IAP Specification *does not* contain any information about, and makes no provision for, the kind of enforcement action that may result from an NCR – it is entirely the role of the Road Agency to determine the specific behaviour they want to be monitored for non-compliance, and the appropriate response to an NCR.

Spatial and Temporal compliance

To assess if a vehicle has been compliant with the Spatial and Temporal conditions in an IAC, the IAP-SP uses the IAM in tandem with Position Records generated by the IVU. Position Records are generated every 30 seconds when the vehicle is in operation, and tell the IAP-SP where the vehicle was at a particular point in time, and the direction it was travelling.

Speed compliance

[11] The Public Sector Mapping Agencies of Australia (PSMA) provides TCA with the IAM.

To assess if a vehicle has been compliant with the Speed Conditions in an IAC, the IAP-SP uses Speed Records generated by the IVU. Speed Records are generated every 3 seconds when the vehicle is in operation, and tell the IAP-SP where the vehicle was at a particular point in time, and how fast it was travelling.

If a vehicle exceeds the maximum speed specified in an IAC, a Speed Event is triggered. A Speed Event is the set of Speed Records that cover the period in which the vehicle exceed the maximum allowable speed, and are included in a Speed NCR.

SD Data in Spatial, Temporal and Speed NCRs

If a spatial, temporal or speed NCR is generated, and the IAC requires the driver to make self-declarations, all SD Records, including any comments made by the driver, for the period 24 hours before, and 12 hours after the incident are included in the NCR.

Alarm NCRs

The IAP-SP can also generate and issue an NCR in response to an alarm. Alarms can be generated by the IVU, or by the IAP-SP System.

An NCR based on alarms generated by the IVU may relate to possible instances of tampering, unauthorised access, and when parts of the IVU are disconnected and reconnected.

An NCR based on alarms generated by the IAP-SP System can relate to irregularities and inconsistencies in the collection, presentation, quality or plausibility of data and vehicle behaviour.

Participants Reports

In addition to NCRs, the IAP-SP provides the Road Agency with monthly reports called Participant Reports, relating to each vehicle that is monitored and a summary of NCRs that have been generated.

10 REFERENCES

Commonwealth of Australia. Standing Council on Transport and Infrastructure. (2012). *Policy Framework for Intelligent Transport Systems in Australia*. Canberra, Australia.

Heavy Vehicle National Law (Queensland). 2016 [2012].

Heavy Vehicle (Mass, Dimension and Loading) National Regulation (Queensland). 2016 [2012].

Transport Certification Australia (TCA). (2006). *Intelligent Access Program: Functional and Technical Specification*, inclusive of addenda 1-8. Transport Certification Australia Limited. Melbourne, Australia.