



PERFORMANCE AUDIT

20 FEBRUARY 2024

Driver vehicle system

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

We conduct financial or 'attest' audits of state public sector and local government entities' financial statements. We also audit the Consolidated State Financial Statements, a consolidation of all state public sector agencies' financial statements.

Financial audits are designed to give reasonable assurance that financial statements are true and fair, enhancing their value to end users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to Parliament. In combination, these reports give opinions on the truth and fairness of financial statements, and comment on entity internal controls and governance, and compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These assess whether the activities of government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities. Our performance audits may also extend to activities of non-government entities that receive money or resources, whether directly or indirectly, from or on behalf of government entities for a particular purpose.

As well as financial and performance audits, the Auditor-General carries out special reviews, compliance engagements and audits requested under section 27B(3) of the *Government Sector Audit Act 1983*, and section 421E of the *Local Government Act 1993*.

© Copyright reserved by the Audit Office of New South Wales. All rights reserved. No part of this publication may be reproduced without prior consent of the Audit Office of New South Wales. The Audit Office does not accept responsibility for loss or damage suffered by any person acting on or refraining from action as a result of any of this material.



GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38EC of the *Government Sector Audit Act 1983*, I present a report titled '**Driver vehicle system**'.

A handwritten signature in black ink, appearing to read 'Margaret Crawford'.

Margaret Crawford PSM
Auditor-General for New South Wales
20 February 2024



RECONCILIATION COMMITMENT STATEMENT

The Audit Office of New South Wales pay our respect and recognise Aboriginal people as the traditional custodians of the land in NSW.

We recognise that Aboriginal people, as custodians, have a spiritual, social and cultural connection with their lands and waters, and have made and continue to make a rich, unique and lasting contribution to the State. We are committed to continue learning about Aboriginal and Torres Strait Islander peoples' history and culture.

We honour and thank the traditional owners of the land on which our office is located, the Gadigal people of the Eora nation, and the traditional owners of the lands on which our staff live and work. We pay our respects to their Elders past and present, and to the next generation of leaders.

contents

Driver vehicle system

Section one – Driver vehicle system

Executive summary	1
Introduction	8
Management of DRIVES	11
Planning for DRIVES replacement	19

Section two – Appendices

Appendix one – Response from entity	25
Appendix two – Statutory and regulatory framework related to DRIVES	28
Appendix three – About the audit	30
Appendix four – Performance auditing	33

Section one

Driver vehicle system

Executive summary

The **DRIVER VEHICLE System**¹ (often known as DRIVES) is the Transport for NSW (TfNSW) system which is used to manage over 6.2 million driver licences and over seven million vehicle registrations in New South Wales.

DRIVES first went live in 1991 and has been significantly extended and enhanced over the past 33 years. DRIVES is a significant NSW Government information system — containing personal information such as home addresses for most of the NSW adult population, sensitive health information such as medical conditions, and biometric data in photographs.

Service NSW, part of the Department of Customer Service, is the NSW Government's 'one stop shop' for services to NSW citizens and businesses. It uses DRIVES when it delivers many transport-related services to NSW citizens such as licence renewals and checks the identity information stored in DRIVES as part of other services delivered to NSW citizens, such as a 'working with children check'.

DRIVES supports TfNSW's regulatory functions and the collection of more than \$5 billion in revenue annually for the NSW Government. The system is also used by many organisations outside of the NSW Government including commercial insurers and national regulators, as well as individual citizens who access DRIVES for services such as 'Renew my registration' or 'Book a driver knowledge test'.

TfNSW owns and manages DRIVES. It intends to replace DRIVES with a modernised system to improve its cost, performance, and security.

The objective of this performance audit was to assess whether TfNSW is effectively:

- managing the current system, and
- planning to transition DRIVES to a modernised system.

The auditee is TfNSW. We have consulted with the Department of Customer Service as a key stakeholder during the audit process.

¹ DRIVES is also referred to as the 'Driver and Vehicle System' in some documentation and on some websites.

Conclusion

TfNSW has not effectively planned the replacement of DRIVES. It has failed to learn lessons from multiple planning attempts over the last five years.

Since 2019, TfNSW has allocated over \$60 million in funding, spent at least \$36 million, and tried multiple times to prepare a robust business case to underpin a replacement program. It is now on its third iteration but has failed to learn lessons from its past attempts. TfNSW cannot clearly state why its previous attempts have failed or when DRIVES will be replaced. As a result, too much of its planning effort has been wasted and the agency continues to operate a system which should have been replaced in the 2010s.

TfNSW's current attempt to replace DRIVES is taking place at the same time as the NSW Government progresses its plans to produce state digital assets that can be used by multiple government agencies. One of these assets is the Licence NSW platform, developed by the Department of Customer Service for the management of customer and business licences, permits and registrations.

TfNSW originally viewed the Department of Customer Service as an arms-length potential service provider rather than another part of government which could deliver a common service. In mid-2023, TfNSW changed this positioning and now views the platform and its operator (the NSW Department of Customer Service) as central to its efforts to replace DRIVES.

TfNSW and the Department of Customer Service are now working together to determine how the Licence NSW platform and the DRIVES replacement will support the administration of a range of transport regulatory activities. How effective they are in defining and then implementing their respective services will significantly determine whether DRIVES is replaced or modernised this decade.

TfNSW has been slow to reduce the risk of misuse of personal information held in DRIVES.

TfNSW has a clear framework to control access to DRIVES. However, in conjunction with its delivery partner, Service NSW, TfNSW has been slow to develop and implement automatic monitoring of access to DRIVES. This is necessary to reduce the risk of misuse of personal information held within the system. Automatic monitoring was a key recommendation by the NSW Independent Commission Against Corruption as part of its May 2021 investigation of criminal misuse of DRIVES data.

TfNSW has not taken a strategic approach to managing the growth of the system over its long lifespan.

DRIVES first went live in 1991 and has been significantly extended and updated over the past 33 years. Outside of DRIVES, TfNSW has built web-based applications such as 'Renew my registration' which allow the public and users such as Service NSW, NSW Police, insurers, and others to update or view some of the information in DRIVES. The system has grown to become an increasingly important service for the NSW Government but DRIVES' growth has not been well-planned by TfNSW which has lacked a strategy to guide its development. The lack of a strategy to underpin the purpose and development of DRIVES has resulted in it including some services which have little or no connection to transport.

TfNSW uses recognised system management processes for managing most other aspects of the existing DRIVES, but it has not kept the system consistently available for users.

TfNSW manages DRIVES using recognised management processes such as those set out in ISO27001 and the Information Technology Infrastructure Library (ITIL). It reports that it has protected the system from a leak of data or any other intrusive cyber-attack. However, it has failed to consistently keep DRIVES and many DRIVES-linked services available for users. DRIVES-linked services include web-based services which make DRIVES information available to the public and industry. In particular, these services were unavailable in early 2020 due to a distributed denial-of-service attack which impacted TfNSW more generally. Services were unavailable again during 2022 following TfNSW's migration of technology support from a legacy datacentre to a hybrid public-private cloud service. The amount of service downtime is unknown because the agency lacks accurate, consolidated information on DRIVES availability since June 2022 when TfNSW changed to a new technology support provider.

TfNSW needs to prioritise improvements to DRIVES against the NSW Cyber Security Policy.

DRIVES is a significant government information system and is therefore subject to inherent cyber security risks which are exacerbated by its age, evolution, and large number of users. Based on the information provided to this audit, TfNSW has not demonstrated it has a cohesive and prioritised strategy to address these risks proportionately. TfNSW has advised that it is seeking to lift DRIVES' cyber defences, but will not achieve its stated target safeguard level until December 2025. However, even then, one of the target safeguards will not be achieved in full until DRIVES is modernised, and that is part of the RegStar program, which itself does not have a target implementation date. In the interim, TfNSW must increase its focus and prioritise efforts to ensure effective cyber security and resilience measures are in place for DRIVES as a matter of urgency.

1. Key findings

DRIVES has grown to be a core system for the NSW Government, but its growth has not been planned strategically and its role in whole-of-government service delivery is neither fully defined, nor is it supported by an effective and comprehensive service management framework

TfNSW has lacked a strategy that provides guardrails or an overarching logic to guide the development and expansion of DRIVES. As a result, DRIVES includes some services which have minimal or no links to transport. For example, people licenced to own a firearm are recorded in DRIVES while most other non-transport licences (and the remaining details of the firearms registry) are recorded in the Government Licensing Service run by the Department of Customer Service. DRIVES also plays an important role in identity management, as Service NSW uses DRIVES to check identity information during many citizen services such as the 'working with children check'.

Many of the additions to DRIVES may have reflected reasonable decisions at the time they were made. However, DRIVES has moved from a database that was wholly focused on managing transport regulatory activities to a service that is increasingly important across government. DRIVES now supports the collection of revenue of more than \$5 billion annually and has 141 user organisations including commercial insurers, national, state and local government agencies, Revenue NSW, National Heavy Vehicle Regulator, Austroads and the NSW Police Force.

TfNSW has responded to DRIVES becoming a critical part of the NSW Government's overall service delivery architecture by implementing management practices, such as memoranda of understanding and access and use agreements with partners such as Service NSW, law enforcement agencies and regulatory bodies. However, TfNSW has not supported DRIVES' expansion with a clear statement of its role in whole-of-government service delivery, nor has it implemented a comprehensive service framework that ensures users views are heard and can influence the service.

DRIVES is not an easy system to use and is expensive to maintain

The DRIVES user interface retains the look and feel of a system built 33 years ago. The interface is not intuitive for contemporary users, being wholly text-based with green font on a black background. This results in lengthy lead times, increased errors, and a sub-optimal staff experience.

DRIVES is complex, not easy to adapt or scale and includes components which have reached the end of their life. TfNSW has estimated that it has spent \$146.6 million to support DRIVES over the past five years. TfNSW is also finding it difficult to source software specialists to manage DRIVES and has estimated that it incurs more costs to support DRIVES than it would if it replaced DRIVES with a contemporary system. In May 2023, TfNSW estimated that it would save \$31 million over ten years in technology support costs if it implemented a modern system. This was a net saving which considered access costs such as licencing costs and resourcing costs to maintain and change the system.

Progress has been slow on the implementation of automatic monitoring to reduce the risk of misuse of DRIVES data

DRIVES includes important personal information such as home addresses for most of the NSW adult population and other information which should only be accessed in accordance with the *Privacy and Personal Information Act 1998*. TfNSW has policies and procedures to control access to and use of DRIVES which aim to reduce the likelihood of misuse of DRIVES data. However, people with access to DRIVES can still misuse personal information held in the system in ways similar to those investigated by the NSW Independent Commission Against Corruption in May 2021 (Operation Mistral). The ICAC recommended that Service NSW should implement a risk-based system to improve the detection of unauthorised access of personal information.

TfNSW and its delivery partner, Service NSW, are targeting March 2024 for the implementation of a capability to automatically detect unusual or anomalous patterns of access to DRIVES. This is nearly three years after the ICAC recommendation was made. This is a slow response particularly considering the detection capability was estimated to cost only \$200,000 to \$300,000, and require approximately six months to implement.

TfNSW has not kept DRIVES consistently available for users, and since mid-2022, TfNSW cannot demonstrate that it has been accurately monitoring DRIVES service availability

TfNSW has not kept DRIVES, and many closely linked systems, consistently available. Services were unavailable for significant periods of time in late 2019 and early 2020 due to network instability and a distributed denial-of-service attack which impacted TfNSW more generally and caused the unavailability of some internet-connected services that are closely linked to DRIVES. TfNSW advised that they have subsequently implemented software designed to automatically protect against denial-of-service and other cyber-attacks.

TfNSW has set a target for DRIVES to be available to users for 99.99% of the agreed service hours. As DRIVES is intended to be available 24 hours a day for 365 days a year, the target can only be met if unplanned downtime each month is less than 4 minutes 32 seconds. However, TfNSW cannot accurately and quickly report its performance against this target since June 2022. This is because its management information:

- incorrectly records the service as experiencing unplanned downtime during periods of planned downtime
- incorrectly records the service as being unavailable when the service switches to a different datacentre, and the service to users continues to be uninterrupted.

For this audit, TfNSW manually calculated the unplanned downtime for October to December 2022 and found that DRIVES was unavailable for 157 minutes and DRIVES-linked systems were unavailable for 2,847 minutes. The Audit Office of New South Wales asked TfNSW to manually recalculate all unplanned downtime for DRIVES since mid-2022. However, TfNSW did not do this, stating it would require 14 working days to complete the calculation.

TfNSW stated that the poor availability from October to December 2022 was significantly caused by temporary transition issues associated with its adoption of a cloud computing service. TfNSW advised us that it has put in place a service improvement plan to improve its reporting of DRIVES downtime.

TfNSW manages DRIVES using recognised management practices and follows a clear process when it upgrades or changes DRIVES

Over the life of DRIVES, TfNSW has upgraded or changed the system many times to respond to changes in technology and legislative and policy developments, as well as to address customer needs or to fix faults or weaknesses in the system. TfNSW has a clear process to manage risks associated with upgrading or changing DRIVES. This includes forward work plans, business and customer impact evaluation, communication, testing and decision gates.

TfNSW has implemented management practices that are designed to protect information held in DRIVES and ensure technology services are aligned with business needs and meet service standards. TfNSW holds current certification against the ISO27001:2022 standard (the international standard for the protection of information) and has implemented practices set out in the information technology infrastructure library (known as ITIL).

TfNSW needs to do more now to ensure that it is effectively managing DRIVES' cyber security and resilience

DRIVES is registered with Cyber Security NSW as one of TfNSW's 'crown jewels'. TfNSW recognises that the age, evolution, and the number of system users of DRIVES, means that its defence against cyber threats needs to be strengthened.

TfNSW has advised that it is seeking to lift DRIVES' cyber defences, but will not achieve its stated target safeguard level until December 2025. However, even then, one of the target safeguards will not be achieved in full until DRIVES is modernised, and that is part of the RegStar program, which itself does not have a target implementation date.

In the meantime, there is limited evidence provided to the audit that there are sufficient cyber security and resilience safeguards in place for DRIVES, nor a cohesive strategy to lift defences going forward on a sufficiently timely basis. Our observations here are consistent with those made in our 2021 report on [Managing Cyber Risks](#) in TfNSW.

TfNSW's leadership must increase its focus and prioritise efforts to ensure effective cyber security and resilience measures are in place for DRIVES as a matter of priority.

Despite five years of effort, more than \$60 million in funding, and spending at least \$36 million—including over \$14 million with three separate consulting companies—TfNSW does not have an approved business case for the replacement of DRIVES

TfNSW has dedicated a significant amount of time, allocated over \$60 million in funding, spent at least \$36 million and tried multiple times to prepare a robust business case to underpin a replacement program.

In 2018 and 2019, TfNSW first attempted to define a program to replace DRIVES when it started but did not complete a strategic business case. In 2021, TfNSW completed a further strategic business case for a DRIVES replacement program. It then completed preparatory work for the program while, in parallel, it worked on a more complete business case. In 2022, TfNSW completed a 'bronze' full business case (so described because TfNSW considered it was complete but not yet a 'gold' document ready for submission to NSW Treasury). Total program costs under the bronze business case were estimated to be \$498.8 million. In 2023, TfNSW paused work on this business case and developed a new strategic business case for its DRIVES replacement program. This new business case included \$114 million of financial benefits from an expected improvement in cyber security (which had previously been modelled as a non-financial benefit only) but removed \$536 million of financial benefits that TfNSW had previously forecast due to an expected increase in safety on NSW roads.

TfNSW has used three major consulting firms to support its planning to transition DRIVES to a modernised system, spending over \$14 million. It used competitive tender processes to appoint each of the three firms but then varied the underpinning contracts on four occasions, adding a total of \$11.1 million to the agreements. The audit team has seen no evidence of market assessments for any of the contract extensions reviewed for this audit.

TfNSW does not have reliable information on its spending for the DRIVES replacement programs over the full five-year period covered by this audit, but it reports that it has spent at least \$36.44 million to plan the transition of DRIVES to a modernised system. This understates the true amount of expenditure by an unknown amount as TfNSW did not record the cost of employees who were working on DRIVES replacement programs until the RegStar program was formed in 2021.

TfNSW has failed to learn lessons from multiple attempts to plan the transition of DRIVES to a modernised system

TfNSW is now on its third iteration of a DRIVES replacement program but cannot clearly state why its previous attempts have failed or when DRIVES will be replaced. TfNSW's bronze full business case presented an opportunity for TfNSW to set out the program's history and learn lessons from previous delays or changes to the program's strategic direction. However, TfNSW did not take this opportunity and executives currently responsible for the program could not clearly articulate why previous iterations of the program (which took place before their appointments) were not progressed.

TfNSW's positioning of the Department of Customer Service as an arms-length potential provider rather than a partner has been one of the causes of delays to the program

TfNSW's current attempt to replace DRIVES is taking place at the same time as the NSW Government progresses its plans to produce state digital assets that can be used by multiple government agencies. One of these assets is the Licence NSW platform, which was developed by the Department of Customer Service for the management of customer and business licences, permits and registrations.

In August 2021, the Department of Customer Service required agencies to consider the use of the Licence NSW platform as a condition of receiving relevant funding from a whole-of-government digital fund. However, TfNSW evaluated the Department of Customer Service as a potential provider as if it was an external supplier to government rather than another part of government which could effectively deliver a common service.

In mid-2023, TfNSW redirected the DRIVES replacement program towards much closer cooperation with the Department of Customer Service. TfNSW and the Department of Customer Service are now working together to determine how the Licence NSW platform and the DRIVES replacement will support administration of a range of transport regulatory activities.

TfNSW needs to resolve several key issues, including DRIVES' role in whole-of-government service delivery and the potential cost to replace it, before it can progress the DRIVES replacement program

TfNSW has an established program team, prepared extensive program documentation, and completed considerable preparation for the replacement of DRIVES. However, to progress further, TfNSW must urgently resolve several key issues including:

- how the replaced DRIVES supports the NSW Government identity strategy and what role it might have in issuing or verifying digital identities
- how the replaced DRIVES works with the Licence NSW platform including which licensing and regulatory administration activities should be carried out by TfNSW, and which should be carried out by the Department of Customer Service
- what should be the detailed technical design of the replaced DRIVES considering its relationship with the Licence NSW platform and its role in managing digital identities
- how to lower the cost of the DRIVES replacement program.

2. Recommendations

By June 2024, TfNSW should:

1. implement a service management framework which ensures it has insight into the views of DRIVES users (internal and external to government) and which ensures DRIVES users can influence the service
2. ensure it can accurately and cost-effectively calculate when DRIVES is unavailable due to unplanned downtime
3. ensure the implementation of a capability to automatically detect unusual or anomalous patterns of access to DRIVES
4. ensure that it has appropriate cyber security and resilience safeguards in place for DRIVES as a matter of priority
5. develop a clear statement of the future role in whole-of-government service delivery for the DRIVES replacement, in consultation with the Department of Customer Service.

By December 2024, TfNSW should:

6. resolve key issues currently faced by the DRIVES replacement program including by:
 - a) clearly setting out a strategy and detailed technical design for a replacement system that considers its interrelationship with other systems—including Licence NSW—in whole-of-government service delivery and in managing digital identities
 - b) using lessons from previous attempts, preparing a specific business case for system replacement, including a robust assessment of costs, benefits and risks.

1. Introduction

1.1 DRIVES

DRIVES is the Transport for NSW (TfNSW) system for recording and managing NSW driver licences and vehicle registrations. DRIVES was created to meet TfNSW's statutory obligations to maintain road registers and, as a road regulatory authority, TfNSW uses the information in DRIVES to support its regulatory functions and objectives.

DRIVES supports TfNSW's administration of a range of other functions related to owning and operating vehicles on NSW roads such as the issue of mobility parking permits and number plates.

DRIVES stands for the **DR**iver **VE**hicle **S**ystem. The system first went live in 1991 for the management of driver licensing and has been significantly extended and updated over the past 33 years. TfNSW now uses DRIVES to either directly manage, or provide information for:

- driver licences and vehicle registrations
- mobility parking permits and vehicle number plates
- other transport functions such as the mandatory alcohol interlock program
- traffic offences, court conviction and enforcement actions
- customer names and addresses
- NSW Photo cards and proof of identity
- firearms licences.

DRIVES purpose, usage, data protection, retention and data access are governed by a number of pieces of legislation including the *Road Transport Act 2013* which requires TfNSW to maintain a register of driver licences and a register of registrable vehicles. In 2022, TfNSW used DRIVES to manage over 6.2 million driver licences and over seven million registered vehicles. DRIVES also records the customer addresses for close to 540,000 maritime licences and 240,000 registered vessels.

The system includes personal information such as home addresses for most of the NSW adult population, sensitive health information such as medical conditions, and biometric data in photographs. This information must be controlled in line with the NSW *Privacy and Personal Information Act 2018*. It is vital that the system is held secure from cyber-related threats. [Appendix two](#) provides further detail on the statutory and regulatory framework related to DRIVES.

1.2 Key users of DRIVES

In June 2023, DRIVES was used by 141 organisations. Exhibit 1 outlines the number of main users by type of entity. Outside of DRIVES, TfNSW has built web-based applications such as 'Renew my registration'. These 'DRIVES-linked applications' allow the public and users such as Service NSW, NSW Police Force, insurers, and others to update or view some of the information in DRIVES.

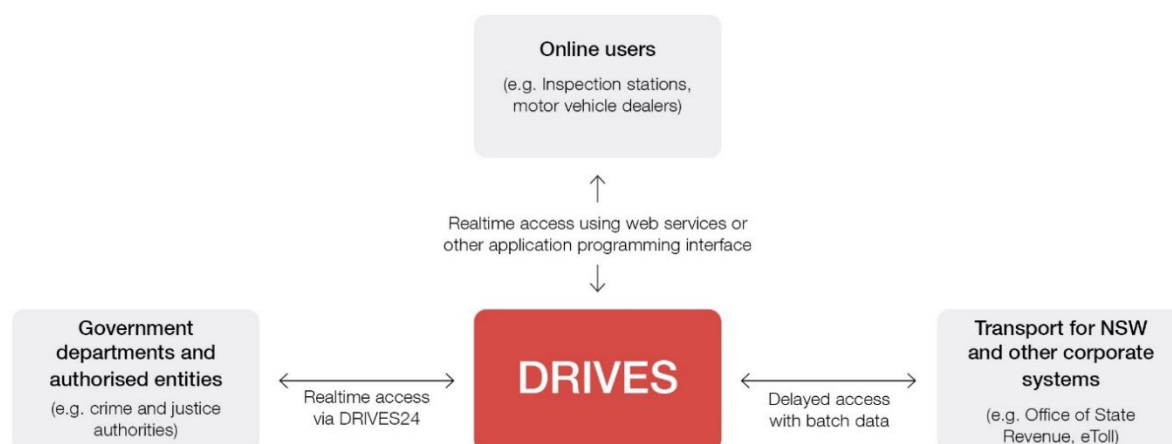
Exhibit 1: DRIVES users by type

Entity type	Number
NSW government agencies	29
Local councils	90
Commonwealth government agencies	11
ACT government agencies	1
Private sector	10
Total	141

Source: Audit Office of New South Wales analysis of TfNSW data.

Most organisations access DRIVES using API (application programming interface) access and online read access. Ten organisations interact with DRIVES through business-to-business e-commerce, including six insurers, Revenue NSW, NSW Police Force, National Heavy Vehicle Regulator, and Austroads. Exhibit 2 is a simplified model of DRIVES main organisational connections.

Exhibit 2: How DRIVES users access the system



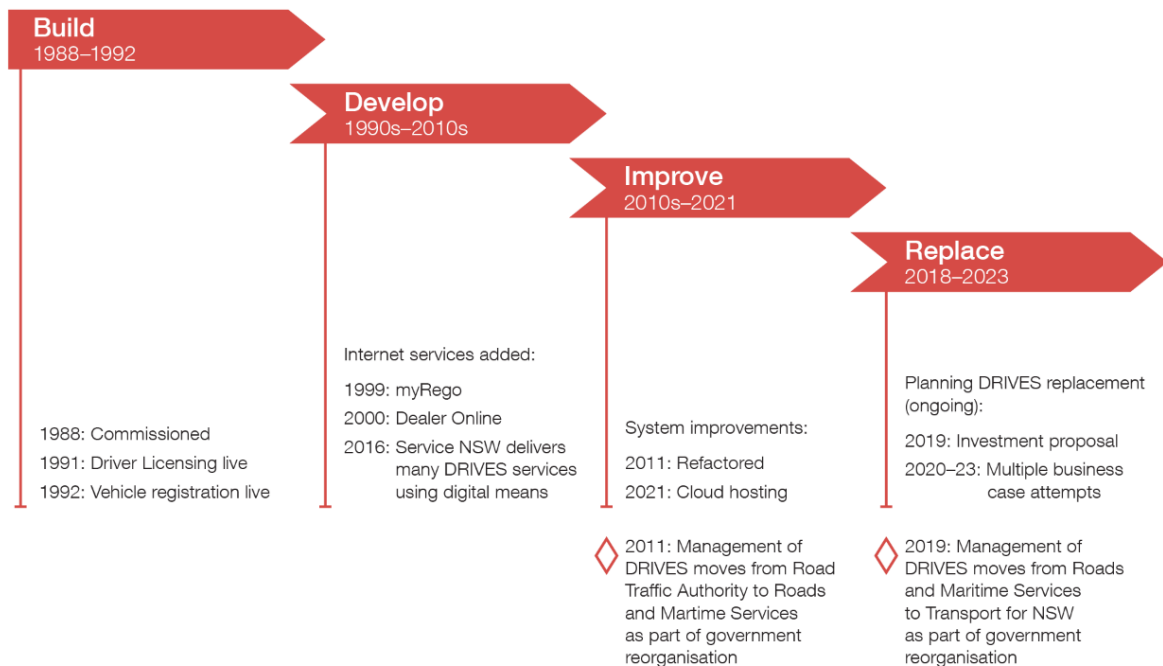
Source: Audit Office of New South Wales analysis of TfNSW documentation.

1.3 The evolution of DRIVES

DRIVES was commissioned in 1988 using CA-Gen Technology² and first went live in 1991 for the management of driver licensing. In June 1992, vehicle registration services were added and internet-based services for external users started in December 1999 with the 'myRego' service.

Key dates in the evolution of DRIVES and TfNSW's recent efforts to replace³ DRIVES are set out in Exhibit 3 below.

Exhibit 3: The evolution of DRIVES



Source: Audit Office of New South Wales analysis of TfNSW documentation.

1.4 About the audit

This audit assessed how effectively TfNSW is managing the **DRIVER VEHICLE System (DRIVES)**. The audit investigated whether:

- TfNSW is effectively managing the current system
- TfNSW is effectively planning to transition DRIVES to a modernised system

[Appendix three](#) provides further information about this audit.

² CA-Gen is software intended for the creation and maintenance of large-scale business applications.

³ DRIVES may be replaced with a new business application or may be retained but very substantially upgraded. For ease, we refer to the replacement or modernisation of DRIVES interchangeably in this report.

2. Management of DRIVES

This part of the report considers whether Transport for NSW (TfNSW) is effectively managing the current system. It considers DRIVES’:

- role in NSW Government service delivery
- ease of use and appropriateness for a modern system
- mechanisms to ensure the service is available for users.

2.1 DRIVES’ role in NSW Government service delivery

DRIVES has grown to become a core system for the NSW Government, but its growth has not been planned strategically, and its role in whole-of-government service delivery is not fully defined, nor is it supported by an effective and comprehensive service management framework

DRIVES growth has not been clearly planned and TfNSW has lacked a strategy that provides guardrails or an overarching logic to guide the development of the system. As a result, the rationale for some DRIVES services is not readily evident and includes services which have minimal or no links to transport. For example, people licenced to own a firearm are recorded in DRIVES but most other non-transport licences (including all other details of the firearms registry) are recorded in the Government Licensing Service run by the Department of Customer Service. DRIVES also plays an important role in identity management, allowing Service NSW to check the identity information stored in DRIVES during many citizen services such as the ‘working with children check’.

Many of the developments to DRIVES may have reflected reasonable decisions at the time they were made. However, as DRIVES has expanded and taken on more functions, it has moved from a database that was wholly focused on managing transport regulatory activities to a service that is increasingly important across government. DRIVES now supports the collection of more than \$5 billion in revenue annually and has 141 user organisations including many outside of TfNSW such as commercial insurers, national, state and local government agencies, Revenue NSW, the National Heavy Vehicle Regulator, Austroads and the NSW Police Force.

TfNSW has responded to DRIVES becoming a critical part of the NSW Government’s overall service delivery architecture by implementing a range of management practices. For example, it has formed memoranda of understanding with key partners such as Service NSW (part of the Department of Customer Service) and has access and use agreements with a wide range of partners such as:

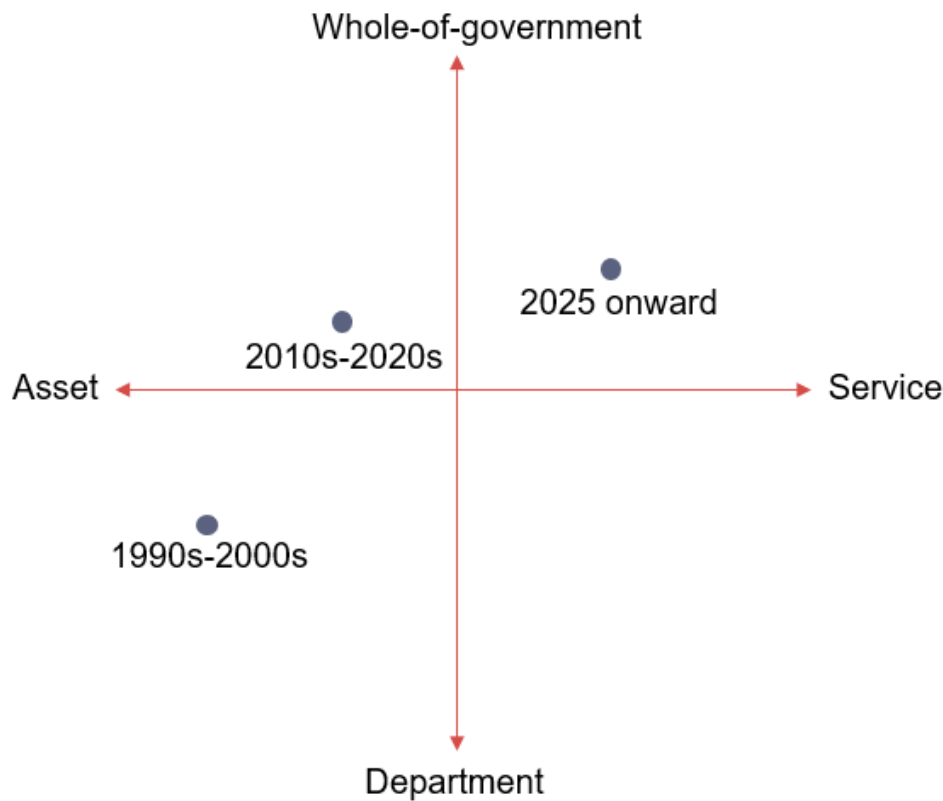
- state and national government agencies
- law enforcement agencies
 - including the NSW Police Force, the NSW Sheriff’s Office, the Australian Criminal Intelligence Commission and the Australian Federal Police.
- regulatory bodies
 - including the State Insurance Regulatory Body (SIRA) and the National Heavy Vehicle Regulator (NHVR).
- commercial insurance companies
- local councils.

However, TfNSW has not supported DRIVES’ expansion with a clear statement of its role in whole-of-government service delivery, nor has it matched this expansion with a comprehensive service management framework that ensures users are able to influence the service. For example, TfNSW does not have well-developed insight into the views of DRIVES’ customers or a clear view on whether and how DRIVES’ costs should be recovered through fees.

Organisations using DRIVES have also been unable to satisfactorily resolve some weaknesses with DRIVES, or understand why the weaknesses cannot be addressed, despite repeated engagement through existing channels for customer feedback.

Exhibit 4 shows the indicative positioning of DRIVES as a whole-of-government service over time.

Exhibit 4: DRIVES has increasingly become a whole-of-government service



Note: Representation of DRIVES positioning is indicative only.

Source: Audit Office of New South Wales analysis of documentation provided by TfNSW.

2.2 Appropriateness and ease of use

DRIVES uses a programming language which is inappropriate for a modern system

DRIVES was built using a programming language originally called CA-Gen, now known as Gen. The system went live in 1991 with the capability to manage driver licences. In the following year, TfNSW added the capability to manage vehicle registration. Since then, DRIVES has been significantly extended and now manages a wide range of transport functions associated with owning or operating vehicles on NSW roads, including licences, registrations, mobility parking permits and number plates, as well as the management of traffic offences and enforcement actions.

DRIVES also connects to businesses and government to facilitate functions such as roadworthy inspections and vehicle insurance. It also provides the processing for many transport-related functions that directly serve the public, such as booking a driver licence test or renewing a vehicle registration.

DRIVES programming language was an appropriate choice when DRIVES was created but it is now outdated, relatively inflexible, and requires more time and effort to integrate with other systems than other more modern languages. It is now inappropriate for a modern system.

DRIVES is no longer an easy system to use and is expensive to maintain

The user interface for DRIVES retains the look and feel of a system designed and built over 30 years ago. The interface is not intuitive, being wholly text-based with green font on a black background. This results in lengthy lead times, increased errors, and a sub-optimal staff experience.

DRIVES is complex, not easy to adapt or scale and includes components which have reached the end of their life. Due to the age of the system, TfNSW is also finding it difficult to source software specialists to manage DRIVES which means they may be forced to pay more to attract these specialists to the public sector, or they may be forced to reduce future development of the system.

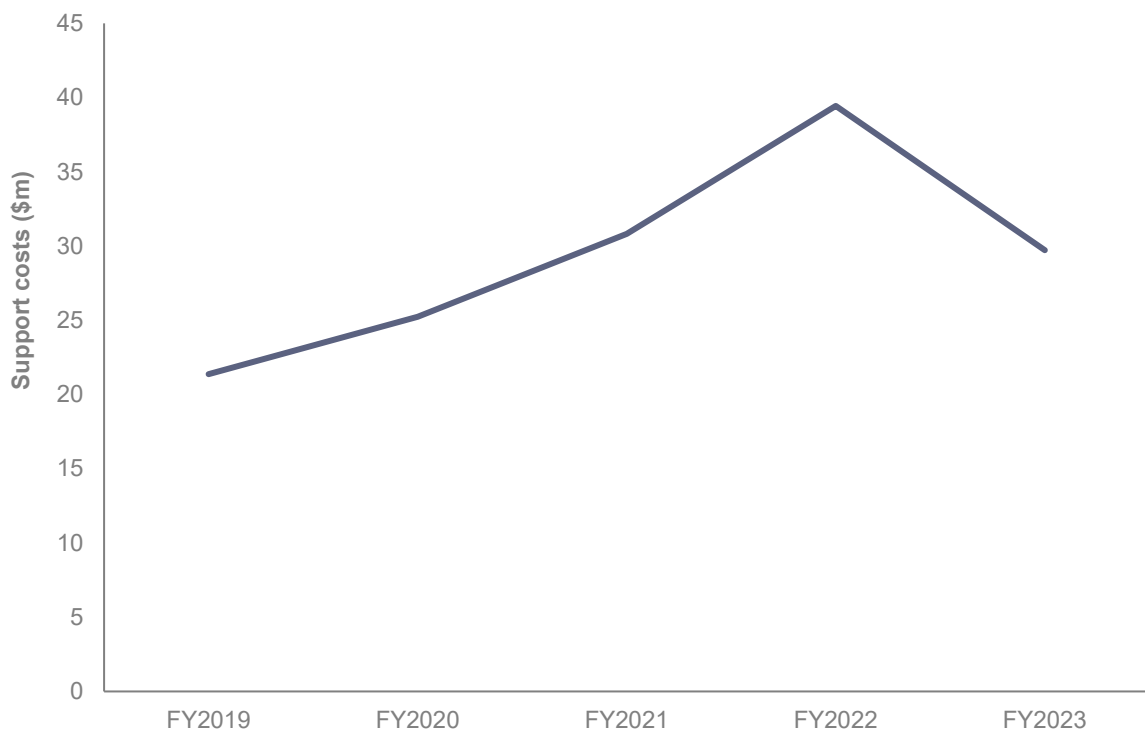
As of August 2023, TfNSW supported and managed changes to DRIVES with a workforce consisting of 130 employees and 52 contractors.

Most of these contractors have been engaged by TfNSW for more than 12 months, with an average tenure of 29 months. Two contractors had been continuously engaged for nine years — which may indicate a risk to the economy of government spending. One of TfNSW's major technology suppliers also provided specialist support for DRIVES and its supporting infrastructure.

TfNSW recognises that the age of DRIVES means that it incurs more costs to support the system than it would if DRIVES was replaced by a modern system. In May 2023, TfNSW estimated that it would save \$31 million over ten years in technology support costs if it implemented a modern system. This was a net saving which considered access costs such as licencing costs and resourcing costs to maintain and change the system.

TfNSW has estimated that it has spent \$146.6 million to support DRIVES over the past five years. Support costs peaked in 2021–22 when the agency migrated support services to a new supplier and incurred duplicate costs for a period of time. Exhibit 5 sets out the approximate annual support costs for DRIVES since 2018–19.

Exhibit 5: Costs to support DRIVES (\$m)



Note: TfNSW does not separately record the cost to support DRIVES and has estimated these costs based upon actual external costs and an attribution of 61.5% of costs incurred across its technology operations for items such as service management, servers, storage and network costs.

Source: Audit Office of New South Wales analysis of data provided by TfNSW (unaudited figures).

TfNSW has a clear framework to control access to DRIVES but, together with its delivery partner Service NSW, it has been slow to implement automatic monitoring to reduce the risk of misuse of DRIVES data

DRIVES includes personal information such as home addresses for most of the NSW adult population, sensitive health information such as medical conditions and biometric data in photographs. Personal information held in DRIVES should only be accessed in accordance with the *Privacy and Personal Information Act 1998*.

DRIVES data is accessed and used by a wide range of organisations through multiple channels including direct access, batch transfer and Application Programming Interface (API) connections.

To manage the challenges of data sharing and appropriate data use, TfNSW has policies and procedures which aim to control access to and use of DRIVES including:

- An agreement for Service NSW to act on behalf of TfNSW.
- Agreements governing access by third party organisations.
- Privacy plans and procedures.
- Internal employee access frameworks.
- Physical access controls such as proximity cards and workplace monitoring.
- Monthly reviews of the need for people to maintain access, and suspension of people's access after 30 days without active use of the system. This includes people within third party organisations.
- Obligations for organisations accessing DRIVES data to maintain records of system access, ensure access is from identified premises and carry out an annual security audit.

While these controls aim to reduce the likelihood of misuse of DRIVES data, people with access to DRIVES can still misuse personal information held in the system in ways similar to those investigated by the NSW Independent Commission Against Corruption in May 2021 (Operation Mistral; ICAC May 2021).

The ICAC found that a Service NSW officer had engaged in serious corrupt conduct and made a series of recommendations including that:

Service NSW should implement a risk-based system designed to improve detection of unauthorised access of personal information, including using analytics of access logs across the system to help detect anomalous or other patterns of access that might indicate unauthorised access.

TfNSW and its delivery partner, Service NSW, are targeting March 2024 for the implementation of a capability to automatically detect unusual or anomalous patterns of access to DRIVES. If this capability is delivered on time, it will go live nearly three years after the ICAC report was published in May 2021. This is a slow response to one of the key recommendations made in the ICAC report, particularly considering the relatively low cost and time that the system is estimated to require (\$200,000 to \$300,000 and approximately six months).

From October 2022 to March 2023, TfNSW recorded four instances of misuse of personal data held in DRIVES. As three of these four instances were reported to TfNSW by either the Australian Federal Police or the NSW Police Force following investigations, the risk remains that further instances of misuse of personal data may have occurred but have not yet been discovered.

2.3 Service availability

TfNSW manages DRIVES using recognised practices, but it has not kept DRIVES consistently available for users

TfNSW has a range of management practices that are designed to protect information held in DRIVES and ensure technology services are aligned with business needs and meet service standards. This includes practices such as those set out in the international standard for the protection of information (ISO27001:2022) and in the information technology infrastructure library (known as ITIL). TfNSW holds current certification against the ISO27001:2022 standard.

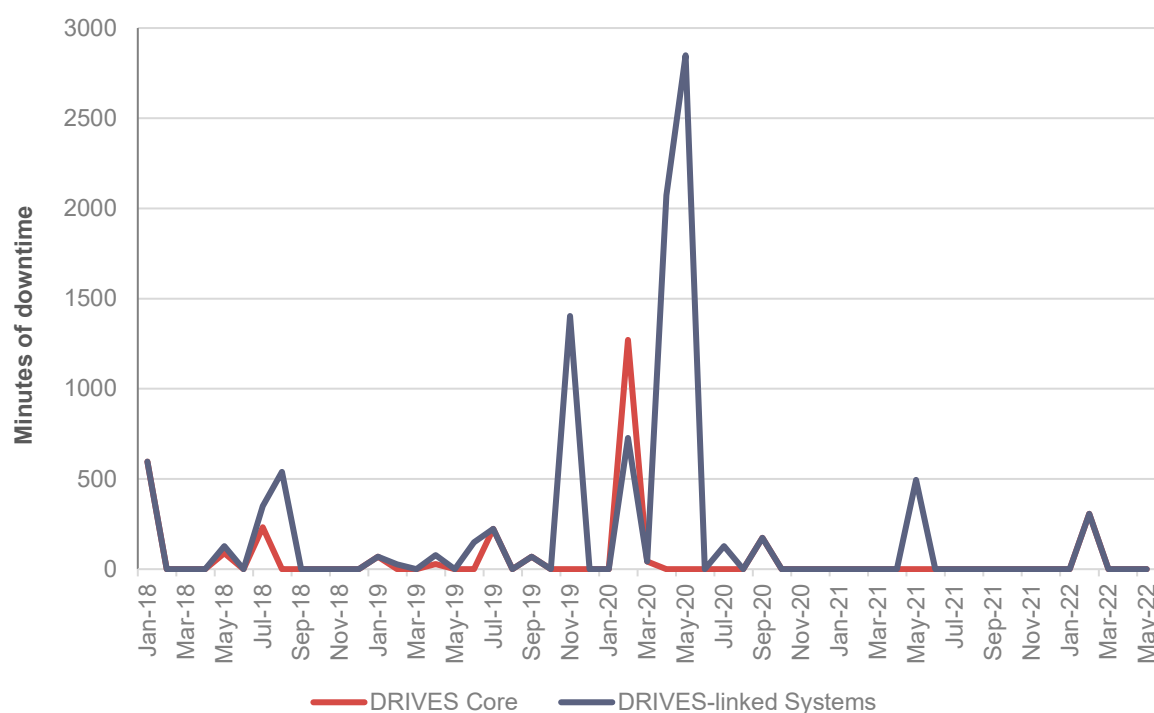
TfNSW has set a target for DRIVES to be available to users for 99.99% of the agreed service hours. For services that are expected to be available 24 hours a day for 365 days a year, the 99.99% target can only be met if unplanned downtime each month is less than 4 minutes 32 seconds.

Over the five-year period examined by this audit, TfNSW contracted with Fujitsu Australia Limited (2018 to May 2022) and Wipro (June 2022 onwards) to provide technology support to TfNSW. This included providing technology support for DRIVES.

Service availability when DRIVES was supported by Fujitsu Australia Limited (2018 to May 2022)

Exhibit 6 shows that DRIVES and many closely linked systems which make DRIVES information available to the public and industry were unavailable for significant periods of time in late 2019 and early 2020. This unplanned downtime meant that Service NSW could not provide many driving-related services to the NSW public for a significant amount of time during November 2019 and February 2020 and then again in April and May 2020. Respectively, these periods of unavailability were caused by network instability (following a planned network change) and a distributed denial-of-service attack which impacted TfNSW more generally and caused the unavailability of some internet-connected services that are closely linked to DRIVES (TfNSW's management of cyber threats related to DRIVES is discussed below).

Exhibit 6: DRIVES and its linked systems were unavailable much more than planned from 2018 to May 2022



Note: DRIVES-linked systems include many services used by the public such as Book a Driver Knowledge Test or by industry such as Dealer Online.
Source: Audit Office of New South Wales analysis of data provided by TfNSW (unaudited figures).

Service availability when DRIVES was supported by Wipro (June 2022 onwards)

TfNSW cannot demonstrate that it has been accurately monitoring system availability since June 2022, and did not provide downtime data requested for this audit

DRIVES and DRIVES-linked systems have suffered unplanned downtime since mid-2022 but the amount of downtime is unknown as TfNSW does not have consolidated, accurate management information on DRIVES service availability.

TfNSW's existing management information on DRIVES service availability since mid-2022 is unreliable due to incorrect coding in the software. As a result, it:

- incorrectly records the service as experiencing unplanned downtime during periods of planned downtime
- incorrectly records the service as being unavailable when the service switches to a different datacentre and the service to users is uninterrupted but not discontinued.

For this audit, TfNSW manually calculated its unplanned downtime for October to December 2022. These calculations showed that DRIVES suffered downtime equivalent to 157 minutes across these three months and DRIVES-linked systems suffered downtime equivalent to 2847 minutes across the same three months.

The Audit Office of New South Wales asked TfNSW to manually recalculate all unplanned downtime for DRIVES since mid-2022. TfNSW did not comply with this request. As such, the audit can provide no assurance over the veracity of downtime data generated within this timeframe, and TfNSW cannot demonstrate that it is accurately monitoring system availability.

TfNSW states that the poor availability during October to December 2022 coincided with, and was significantly caused by, its adoption of a hybrid public-private cloud computing service. In 2022, the agency finalised a four-year program to transfer the support and maintenance of transport systems, including DRIVES, from a legacy datacentre to a hybrid public-private, cloud-based service. TfNSW advised that the transfer reduced risks associated with the performance, cost and security of the legacy service but also led to DRIVES and DRIVES-linked systems being unavailable in late 2022 while transition issues were identified and resolved.

Management information for months when DRIVES and its related systems achieve 100% availability are reliable and TfNSW reported that it had achieved 100% availability on 47 of 61 months examined by this audit. Since January 2023, TfNSW reports that it has achieved very high levels of system availability.

Protection against cyber-attack

TfNSW needs to do more now to ensure that it is effectively managing DRIVES' cyber security and resilience

DRIVES is registered with Cyber Security NSW as one of TfNSW's 'crown jewels' – that is, one of the most valuable or operationally vital systems or information in the organisation.

TfNSW acknowledges that DRIVES remains an attractive target for attack by cyber actors and that the age and evolution of DRIVES means that its defence against cyber threats needs to be strengthened. DRIVES is also accessible to more than 140 organisations.

An example of DRIVES' exposure to the risk of cyber-attack is the successful distributed denial of service attack in early 2020, which impacted TfNSW more generally and caused the unavailability of some internet-connected services that are closely linked to DRIVES.

Following the denial-of-service attack, TfNSW established a set of follow up actions to take after a cyber-attack, including to:

- lift DRIVES' Essential Eight cyber defences to a higher level, which has been assessed as a requirement by TfNSW management⁴
- review, and where appropriate, extend privileged access management for DRIVES users with advanced system access (whilst maintaining controls on this form of access)
- implement multi-factor authentication for internet-linked applications that draw on DRIVES.

TfNSW has advised that it is seeking to lift DRIVES' cyber defences, but will not achieve its stated target safeguard level until December 2025. However, even then, one of the target safeguards will not be achieved in full until DRIVES is modernised, and that is part of the RegStar program, which itself does not have a target implementation date.

In the meantime, there is limited evidence provided to the audit that there are sufficient cyber security and resilience safeguards in place for DRIVES, nor a cohesive strategy to lift defences going forward on a sufficiently timely basis. Our observations here are consistent with those made in our 2021 report on [Managing Cyber Risks](#) in TfNSW.

While TfNSW reports that a range of management practices and governance forums are in place that aim to help to manage cyber risks — including vulnerability reporting, software patching calendars, incident management processes, and regular system penetration testing — the audit team did not receive evidence that these controls are practiced on a consistent and regular basis in a manner responsive to identified risks. TfNSW's leadership must increase its focus and prioritise efforts to ensure effective cyber security and resilience measures are in place for DRIVES as a matter of priority.

Cyber security remains a complex and highly challenging area for TfNSW and all government entities. In July 2021, we assessed how effective TfNSW and Sydney Trains were in identifying and managing cyber security risks. In that audit, we found that neither agency was effectively managing these risks and neither had fostered a culture where cyber security risk management was an important and valued aspect of decision-making. The recommendations we made then remain relevant today.

A key consideration is that, with more than 140 organisations using DRIVES, any vulnerability in individual user's cyber defences could have potentially significant ramifications for DRIVES. Our [2023 Internal Controls and Governance Report](#) concluded that 83% of the 25 largest agencies in the New South Wales public sector (which includes TfNSW) have reported one or more Mandatory Requirements below level three, which is the level at which the requirement is self-assessed and considered to be practiced on a consistent and regular basis.

The information contained in DRIVES, the system's age and evolution, and the high number of users of the system, means that TfNSW must increase its focus and prioritise efforts to ensure effective cyber security and resilience measures are in place for DRIVES as a matter of priority.

Other risks to service availability

The age and design of DRIVES means that TfNSW faces continued risks to the availability and performance of DRIVES. For example, in early 2022, insurers were unable to process applications for compulsory third-party insurance because tables within DRIVES had reached their maximum 'as designed' limit and, as a result, customers were unable to complete vehicle registration transactions. While this issue was resolved and TfNSW now monitors for a potential repeat of it, the risk remains of other issues arising due to the age and design of DRIVES.

⁴ The Essential Eight framework is a suite of cyber controls published by the Australian Cyber Security Centre.

TfNSW follows a clear process when it upgrades or changes DRIVES

Over the life of DRIVES, TfNSW has upgraded or changed the system many times to respond to changes in technology and legislative and policy developments, as well as to address customer needs or to fix faults or weaknesses in the system.

Exhibit 7 shows that TfNSW has spent \$57.5 million to upgrade or change DRIVES over the five-year period examined by this audit (2018–19 to 2022–23).

Exhibit 7: Summary of the costs to upgrade or change DRIVES (\$m)

DRIVES	2018–19	2019–20	2020–21	2021–22	2022–23	Total
Development and enhancement	6.3	8.7	11.8	13.3	17.4	57.5

Source: Audit Office of New South Wales analysis of data provided by TfNSW (unaudited figures).

While changes to DRIVES are necessary, each change introduces risks to system performance and availability. TfNSW advised the audit team that it has a clear process to manage these risks, which includes:

- maintaining a forward work plan which helps TfNSW to plan for, sequence and resource the changes
- evaluating the business and customer impact of each change
- informing relevant business areas of the planned changes including likely system impacts
- using a set of decision gates ('Go' and 'No Go' decisions) which, amongst other things, document and consider the results of testing performed on the planned system change, including system integration, technical, security and business or user testing.

3. Planning for DRIVES replacement

This part of the report considers whether Transport for NSW (TfNSW) is effectively planning to transition DRIVES to a modernised system. It makes findings on the:

- effort to develop a business case to fund the replacement of DRIVES
- issues which have contributed to the slow progress of the replacement program.

3.1 Development of a business case to replace DRIVES

Despite five years of effort and an allocation of more than \$60 million in funding, TfNSW does not have an approved business case for the replacement of DRIVES

TfNSW has dedicated a significant amount of time on its preliminary work to plan the replacement of DRIVES:

- In 2018 and early 2019, TfNSW started, but did not complete, a strategic business case for a DRIVES replacement program.
- In May 2019, TfNSW's Finance and Investment Assurance Committee considered an investment brief for a DRIVES replacement program. This brief envisioned a program which would commence delivery in July 2020 and complete the replacement of DRIVES by June 2026.
- In June 2021, TfNSW completed a further strategic business case for a DRIVES replacement program. Program delivery under this business case was planned to start in the second half of 2021 and complete by the end of 2025. Across 2021–22, TfNSW completed significant preparatory work for the program (referred to as 'tranche 1' activities) as, in parallel, it continued work on the development of a more complete business case.
- In October 2022, TfNSW completed a full business case which it described as a 'bronze' business case because TfNSW considered it was complete but not yet ready for submission to NSW Treasury. At the time, TfNSW intended to refine the document over the following months and present it to NSW Treasury for funding approval in April or May 2023. Program delivery under this business case was planned to start in the second half of 2023 and complete by the end of 2026–27. Total program costs were estimated to be \$498.8 million.
- In 2023, TfNSW paused work on the bronze full business case and developed a new strategic business case for its DRIVES replacement program. This case very significantly changed the treatment of road safety and cyber security benefits - as it included \$114 million of financial benefits from an expected improvement in cyber security (which had previously been a non-financial, or qualitative benefit only) but removed the \$536 million of financial benefits that it had previously forecast due to an expected increase in safety on NSW roads.

None of these documents were provided to NSW Treasury for funding consideration. TfNSW has not briefed either Cabinet or any Cabinet committee on the replacement of DRIVES.

Matching its time commitment, Exhibit 8 shows that TfNSW has allocated significant funding to its efforts to plan the replacement of DRIVES.

Exhibit 8: Summary of the funding allocated to DRIVES replacement programs (\$m)

Program	2018–19	2019–20	2020–21	2021–22	2022–23	Total
RegStar precursor	1.26	4.55				5.81
RegStar				15	40.09	55.09
Overall total						60.90

Note: TfNSW subsequently reallocated \$4.73 million of funding for 2021–22 to the program for 2022–23.

Source: Audit Office of New South Wales analysis of data provided by TfNSW (unaudited figures).

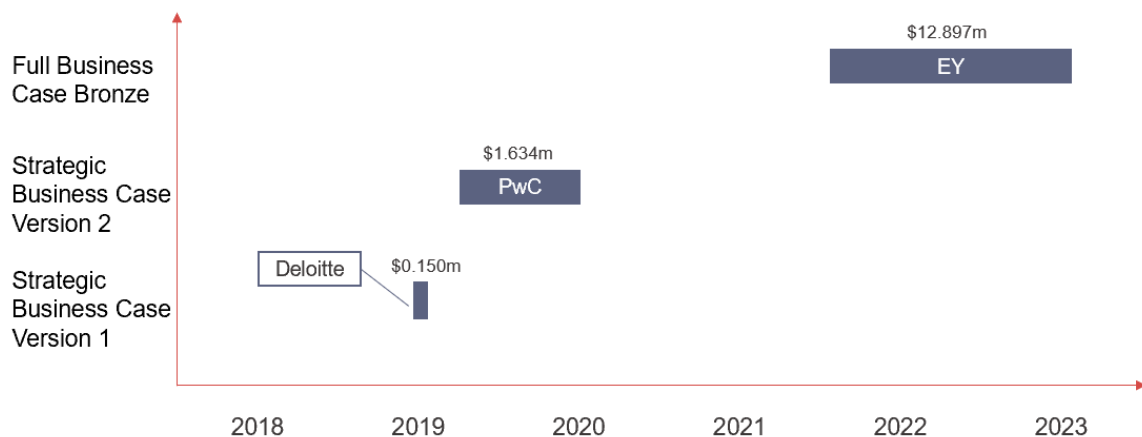
TfNSW does not have reliable information on its spending for the DRIVES replacement programs to date, but reports that it has spent at least \$36 million

TfNSW does not have reliable information on its spending for the DRIVES replacement programs over the full five-year period covered by this audit, but it reports that it has spent at least \$36.44 million to plan the transition of DRIVES to a modernised system. This understates the true amount of expenditure by an unknown amount as TfNSW did not record the cost of employees who were working on DRIVES replacement programs until the RegStar program was formed in 2021.

TfNSW has spent over \$14 million with three consulting companies in its attempts to define the DRIVES replacement program

Exhibit 9 shows that TfNSW has used three major consulting firms to support its planning to transition DRIVES to a modernised system. Spending on EY in 2021–22, 2022–23 and the first four months of 2023–24 totalled \$12.897 million.

Exhibit 9: Spending on major consultancies as part of the DRIVES replacement programs



Source: Audit Office of New South Wales analysis of data provided by TfNSW.

TfNSW used a competitive tender process to appoint each of the three consultancy firms. It subsequently increased its original contract with PwC by \$180,000 and then varied and extended the original contract with EY on three occasions adding a total of \$10,917,522 which includes planned spending up until the end of December 2023 (see Exhibit 10 below).

Exhibit 10: Contract variations under the DRIVES replacement programs (\$m)

Consultancy	Original contract value	Number of extensions or variations	Value of extensions or variations	Revised contract value
Deloitte	0.165	Nil	Nil	0.165
PwC	1.476	1	0.18	1.656
EY	8.113	3	10.918	19.031

Note: Revised contract value for EY includes planned spending up until the end of December 2023.

Source: Audit Office of New South Wales analysis of data provided by TfNSW.

TfNSW advised the audit team that the contracts set out in Exhibits 9 and 10 were not for consulting services but instead were for professional services. However, this is contradicted in part by TfNSW's Annual Report 2021–22 which discloses consultancy spending with EY for the RegStar program (\$1,278,918).

The current version of the NSW Procurement Policy Framework (April 2022) notes that 'routinely exercising extension options or rolling-over contracts reduces competition and limits access to new suppliers, products and services'. Further, the NSW Procurement Policy Framework requires agencies to conduct a 'strategic assessment of the market prior to rolling-over or extending a contract, including how the extension will impact competition'. The audit team has seen no evidence of market assessments for any of the contract extensions reviewed for this audit.

3.2 Issues contributing to current slow progress

TfNSW has failed to learn lessons from multiple attempts to plan the transition of DRIVES to a modernised system

During the five years examined by this audit, TfNSW has prepared multiple business case documents and completed significant program activity but it cannot clearly state why it has paused or redirected the DRIVES replacement program on multiple occasions. Significant changes over this time have included its:

- first strategic business case, which was partly completed in 2019 but then not progressed
- use of three different consultancy companies in four years to support its planning effort
- redevelopment of its bronze full business case into a new strategic business case, rather than a finalised full business case. Amongst other changes, this involved the monetisation of benefits expected from changes in cyber risk profiles and the demotion of road safety from being a central driver for the program, and monetised benefit, to a qualitative benefit only
- movement from an 'arms-length' to a partnership approach to working with the Licence NSW⁵ platform (which is being developed by the Department of Customer Service).

TfNSW's bronze full business case was the most comprehensive set of documents developed during the DRIVES replacement program. As such, it presented an opportunity for TfNSW to:

- set out DRIVES' long history, including its lack of an overall strategy for its development
- set out the program's history, including the multiple attempts to develop a business case
- learn lessons from previous delays or changes to the program's strategic direction.

However, TfNSW did not take this opportunity and executives currently responsible for the program could not clearly articulate why previous iterations of the program (which took place before their appointments) were not progressed.

⁵ Until 2023, Licence NSW was known as Licence.NSW

The most recent change in direction of the DRIVES replacement program was confirmed in June 2023 when the Program Steering Committee discussed closer working and greater collaboration with the Department of Customer Service, along with continued consideration of the Licence NSW platform service.

A gateway review in 2022 failed to highlight the need for closer working with Licence NSW

In November 2022, TfNSW received a 'Gate 2 Review Report' prepared as part of the NSW Government's assurance process for major projects. The report concluded that 'successful delivery of the project to time, cost, quality and anticipated benefits appears feasible but risk and/or issues exist that threaten delivery or overall viability. These appear resolvable if addressed promptly'.

The Gate 2 Review Report was the result of an external independent review undertaken on behalf of the NSW Government and administered by the Department of Customer Service. Amongst other things, the review set out to:

- assess whether the bronze full business case was robust, would deliver value for money, and has outline plans to realise benefits
- confirm that all whole-of-government policies, standards and priorities for digital and technology investments had been considered.

The review also considered a request from TfNSW to assess whether the DRIVES replacement program was significantly impacted by an interaction with the government's digital identity plans and the Licence NSW platform.

The Gate 2 Review Report made six recommendations, including three recommendations it rated as critical on funding and the appropriate treatment of business case options. The report did not recommend redirecting or otherwise pausing the program and made no specific recommendation on the impacts of digital identity or on working more closely with the Department of Customer Service on the program, despite a government directive that requires departments to consider Licence NSW as part of digital funding applications. It did however comment that the Licence NSW platform should be included in the consideration of options in the business case.

TfNSW's positioning of the Department of Customer Service as an arms-length potential provider rather than a partner has been one of the causes of delays to the program

TfNSW's current attempt to replace DRIVES is taking place at the same time as the NSW Government progresses its plans to produce state digital assets that can be used by multiple government agencies. One of these assets is the Licence NSW platform, which was developed by the Department of Customer Service for the management of customer and business licences, permits and registrations.

In August 2021, the Department of Customer Service issued a whole-of-government circular (DCS-2021-03 Licence NSW) which placed a requirement on agencies to evaluate the use of the new Licence NSW platform when seeking funding from whole-of-government digital funds.

In early 2023, TfNSW responded to the whole-of-government circular by conducting a proof-of-concept evaluation of the Licence NSW platform, evaluating the Department of Customer Service as if it was an external supplier to government rather than another part of government which could effectively deliver a common service.

In mid-2023, TfNSW redirected the program towards much closer cooperation with the Department of Customer Service. TfNSW and the Department of Customer Service are now working together to determine how Licence NSW platform and the DRIVES replacement will support the administration of a range of transport regulatory activities.

TfNSW needs to resolve several key issues, including DRIVES' role in whole-of-government service delivery and the potential cost to replace it, before it can progress the DRIVES replacement program

TfNSW has an established program team, prepared extensive program documentation and completed considerable preparation for the replacement of DRIVES including work to prepare:

- strategic business cases and a bronze full business case
- cost benefit analyses for DRIVES replacement options, including a technical-only upgrade
- market engagement and sourcing strategy
- business process mapping and redesign documents
- program management documents such as stakeholder and change management, risk management and schedule management.

However, to progress further, TfNSW must urgently resolve several key issues including:

- how the replaced DRIVES supports the NSW government identity strategy and what role it might have in issuing or verifying digital identities
- how the replaced DRIVES works with the Licence NSW platform including which licensing and regulatory administration activities should be carried out by TfNSW, and which should be carried out by the Department of Customer Service
- what should be the detailed technical design of the replaced DRIVES considering its relationship with the Licence NSW platform and its role in managing digital identities
- how to lower the cost of the DRIVES replacement program.

Section two

Appendices

Appendix one – Response from entity

Transport for NSW



Ms Margaret Crawford
Auditor General
Audit Office of NSW
GPO Box 12
SYDNEY NSW 2000

RE: Performance Audit Report into DRIVES

Dear Ms Crawford

Thank you for the opportunity to respond to the Performance Audit Report (the Report) into the DRIVER Vehicle System (DRIVES). Transport for NSW (TfNSW) has carefully considered the audit report and accepts its six recommendations in full. It is however important that TfNSW places on the public record our response to the Report's commentary, particularly on cybersecurity and monitoring of access to DRIVES.

The Report recognises that DRIVES is a complex digital environment that has been upgraded and altered over time to respond to changes in technology, legislative and policy developments and to meet customer needs and the challenges of an evolving cybersecurity landscape. We at TfNSW acknowledge the vigilance, effort and cost required to maintain and uplift to contemporary standards this aging infrastructure. It is in this context that we have initiated the RegStar (DRIVES replacement) program to establish a new technology environment; one that will be more resilient, adaptable, and better aligned with the evolving needs and expectations of our stakeholders and customers.

I welcome the Report's acknowledgement that TfNSW has a rigorous process to manage risks associated with upgrading or changing DRIVES, and a clear framework to control access. As the custodians of the personal information of many NSW citizens, we at TfNSW take seriously the need to maintain privacy and security of DRIVES, to protect our digital assets generally and the information of those we serve. In recent years, TfNSW has uplifted and enhanced the security guard-rails and features of DRIVES. The DRIVES modernisation program and the cloud migration have provided significant uplift, including additional cyber security defences. I wish to emphasise that TfNSW complies with NSW Government Cyber Security Policy and works closely with Cyber NSW.

It is important to acknowledge new criteria introduced into the self-assessment standards framework in 2023 altered TfNSW's score as referenced in the Report, but that this change does not represent a

Transport for NSW
231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | W transport.nsw.gov.au | ABN 18 804 239 602

OFFICIAL

deterioration in actual performance or service delivery.

Regarding automatic detection of unusual or anomalous patterns of access to DRIVES, TfNSW acknowledges this is an in-flight recommendation stemming from a Service NSW (SNSW) breach investigated by the Independent Commission Against Corruption. TfNSW can confirm our work to assist SNSW in the implementation of this recommendation has been partly delivered, with full roll out on track by the end of the first quarter of 2024. While this capability has been in development, other detection measures have been in place, and TfNSW has no evidence to support the Report's assertion that further instances of misuse of personal data may have occurred.

TfNSW accepts the need for, per the Report's recommendations, better mechanisms for reporting unplanned downtime. I note though that the core components of the DRIVES platform consistently meet industry benchmarks for performance and availability, which is noteworthy given its complexity, real-time integration with diverse external systems and government agencies, and the volume of transactions managed. The DRIVES core platform consistently maintains an impressive 99.9% availability rate. The Report's remarks pertain primarily to minor outages in the MyRTA service only, which is not a central component of DRIVES. The outages occurred during a defined period and did not impact a majority of customer services.

I also wish to address the Report's characterisation that DRIVES has changed from a database wholly focused on managing transport regulatory activities to a whole-of-government service. TfNSW has various regulatory obligations to maintain driver licensing and vehicle registration data under the *Road Transport Act 2013*. The DRIVES system was created as TfNSW's repository of such registers to discharge the department's legislative obligations, which aligns with a national approach to road safety via driver licensing, vehicle registration and standards. This continues to be the core purpose of DRIVES, and any system changes need to be tested to ensure compliance with TfNSW's statutory obligations can be maintained.

Furthermore, repositioning DRIVES as a whole-of-government service at this stage presents a range of significant challenges as the information it holds is collected for the limited purposes set out in legislation. It is accessed by other NSW agencies under legislative exceptions which allow driver and vehicle information to be used in limited circumstances for purposes unrelated to road safety, or where there is consent from the individual involved. Access to DRIVES (including DRIVES24) and the personal information contained within it is governed by road transport, state records and privacy laws and robust access assurance frameworks.

Regarding the recommendation to implement a service management framework for DRIVES, TfNSW's challenge lies in effectively articulating to stakeholders the intricate and complex nature of the DRIVES environment and the statutory requirements it serves. TfNSW actively manages a robust service

Transport for NSW

231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | W transport.nsw.gov.au | ABN 18 804 239 602

OFFICIAL


management framework. I acknowledge the coordination and integration of support services could be enhanced, and TfNSW is committed to taking a collaborative approach to DRIVES upgrades via stakeholder engagement and governance forums.

I wish to acknowledge the challenges faced in the planning of the RegStar program. Factors such as the COVID-19 pandemic and a constrained fiscal environment have played a role. Our agency is also acutely aware of the significant challenges other state jurisdictions and agencies have encountered in large-scale transformation programs, and TfNSW suggests the Report's findings are not fully reflective of such risks. That being said, Transport has made significant progress to date. Our investment in the RegStar program so far has delivered comprehensive planning and process re-engineering, and detailed service design blueprints that will reduce costs in the detailed design and future stages of the program.

TfNSW is committed to a strategic evaluation of the Lic.NSW platform and determining whether it is fit-for-purpose. We are actively collaborating with key stakeholders to determine the platform's core and common functionalities.

Once again, I appreciate your review of this important digital infrastructure and the opportunity to respond to the findings and recommendations in the Report.

Yours sincerely

A handwritten signature in black ink, appearing to read "Josh Murray".

Josh Murray
Secretary

12 February 2024

Transport for NSW
231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | W transport.nsw.gov.au | ABN 18 804 239 602

OFFICIAL

Appendix two – Statutory and regulatory framework related to DRIVES

The information in this appendix was provided by TfNSW to help set out the context which DRIVES operates within. The Audit Office of New South Wales has made minor adjustments for readability purposes.

Summary

DRIVES was created to meet TfNSW's statutory obligation to create, hold and maintain accurate road registers which align with a uniform national approach to road safety via driver licensing, vehicle registration and standards. As a road regulatory authority, TfNSW uses the information in DRIVES to support its regulatory functions and objectives. The nature of the information kept matches that retained by road agencies in other jurisdictions to support a national approach to driver licensing and competency, road rules, enforcement and vehicle safety.

A range of legislation governs DRIVES purpose, usage, data protection, retention and data access including the:

- *Road Transport Act 2013* ('the Act') and Regulations and statutory rules under the Act
- *Photo Card Act 2005*
- *State Records Act 1998*
- *Privacy and Personal Information Protection Act 1998*.

Because of its nature, DRIVES contains personal information. NSW driver and vehicle information are routinely shared with other state and territory road agencies for road safety purposes (for example, to exchange information about a NSW driver who was penalised for speeding in another jurisdiction). In addition, the information in DRIVES is accessed by other NSW agencies for purposes associated with their own statutory functions including law enforcement and, more recently, digital identity.

Although there are a range of alternative uses for driver and vehicle registration data, the data is only collected for purposes associated with road safety laws. It is accessed by other NSW agencies under legislative exceptions which allow driver and vehicle information to be used in specific circumstances for purposes unrelated to road safety, or where there is consent from the individual who the data relates to. That is, the primary purpose for collection of the information in DRIVES is to meet regulatory requirements arising under road safety laws.

Sharing of driver licensing and vehicle registration information with other government entities is a secondary feature of TfNSW's regulatory role and is not without risk. Provisions in the *Road Transport Act 2013* impose an obligation on TfNSW to ensure that sensitive information is not released except as allowed by law. Expanding the role of DRIVES beyond its core function increases the risk profile of data security and protection of private information, and require an enhanced data management and security posture across the proposed utilisation and lifecycle of the data.

Statutory and Regulatory framework within which DRIVES operates

DRIVES (**DR**iver **VE**hicle **S**ystem) is the name given to the computer system which was introduced to store and house the statutory road registers. It also stores other information managed and collected by TfNSW in the course of its obligations under the road transport and other legislation.

The Statutory Registers

Under the *Road Transport Act 2013*, TfNSW is the road authority and regulator. It administers the driver licensing regime and the vehicle registration regime. The object of the Act is to (relevantly) provide for, in a manner consistent with national reforms a:

- driver licensing system as part of a uniform national approach to driver licensing (including uniform driver licence classes and licence eligibility criteria)
- vehicle registration system as part of a uniform national approach to vehicle registration and standards.

In its role as a road authority, TfNSW is required to maintain statutory registers, including a register of:

- driver licences (section 27 of the Act)
- driver licence photographs (kept notionally separate from the driver licence register because of the different rules that the Act provides for how photographs may be stored, used and disclosed – see section 30 and Part 3.5 of the Act)
- demerit points (section 31 of the Act)
- registrable vehicles (section 64 of the Act)
- written off light vehicles (section 83 of the Act)
- written off heavy vehicles (section 104B of the Act).

These statutory registers are contained in the DRIVES database. The statutory registers are required in each case to be maintained (that is, kept up to date and accurate) and to be kept secured (that is, to only be used, accessed, or disclosed as permitted). The following Regulations also provide for the specific type of data that is required to be recorded in each register:

- Road Transport (Driver Licensing) Regulation 2017
- Road Transport (Vehicle Registration) Regulation 2017
- Road Transport (General) Regulation 2021
- Road Rules 2014.

Privacy and data sharing

The data in each road transport register is personal information and is generally not permitted to be dealt with under the Act other than in compliance with NSW privacy legislation (*Privacy and Personal Information Protection Act 1998*), or as authorised under an Act.

The data in the photograph registers has an elevated privacy regime applied to it, and may only be used and disclosed under the provisions in Part 3.5 of the Act, which is more stringent than the state privacy legislation.

The road transport legislation provides for certain exemptions from the state privacy regime for their respective registers, for instance to enable the conduct of routine business and to allow important functions to occur which require access by third parties to a register or registers (for example, for driver licences see Part 13 Division 1 of the Road Transport (Driver Licence) Regulation 2017, for vehicle registration see Part 8 Division 4 of the Road Transport (Vehicle Registration) Regulation 2017).

Appendix three – About the audit

Audit objective

This audit assessed how effectively TfNSW manages the **DRiver VEHICLE System (DRIVES)**.

Audit criteria

We addressed the audit objective with the following audit criteria:

1. TfNSW is effectively managing the current system
 - a) TfNSW's operation of DRIVES meets its legislative requirements, including the privacy of information and cyber security
 - b) TfNSW has clearly articulated whole-of-government governance arrangements for DRIVES, including the assignment accountabilities
 - c) TfNSW is appropriately managing risks to operating the current system, including threats to the privacy of information and cyber security
 - d) TfNSW has clearly defined operational targets for DRIVES (including for maintenance), and it monitors and reports progress against these targets to key stakeholders.
 - e) Unplanned outages and any other operational incidents are managed within agreed specifications.
2. TfNSW is effectively planning to transition DRIVES to a modernised system
 - a) TfNSW has clearly articulated its business strategy ('future state') to underpin planning work
 - b) TfNSW has clearly stated roles, responsibilities, and governance arrangements for the modernisation project
 - c) TfNSW has an appropriate planning framework in place, to manage any system transition risks and ensure on-going protection of personal information and cyber security against the standards set by government
 - d) TfNSW communicates effectively with key stakeholders and decision-makers, including the Department of Customer Service and NSW Treasury, on project progress (timeliness, cost and budget) and management of key risks

Audit scope and focus

The audit examined the current management of DRIVES, as well as the planned transition to a modernised system. The audit focused on the following aspects:

- policy and legislative requirements
- governance and accountabilities (including risk assessment and mitigation)
- protection of personal information and cyber security
- resources (workforce, cost and funding)

The audit covered the period from 2018 to 30 June 2023.

Audit exclusions

The audit did not seek to:

- examine IT solutions to replace DRIVES
- assess TfNSW's management of other related IT systems
- comment on the merits of government policies.

However, we may comment on these issues where they affect our findings or to provide context.

If warranted, we may change the audit objective, scope or criteria during the course of the audit. If we feel this is necessary, we shall discuss any changes to the plan and the reasons for them with the entity before finalising

Audit approach

The audit team conducted the audit in accordance with ASAE 3500 'Performance Engagements' and ASAE 3000 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information'. The standards require the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance about an activity's performance against identified criteria and express a reasonable assurance conclusion against the audit objective.

Our procedures included:

1. Interviewing:
 - a) relevant staff at TfNSW involved in the management and modernisation of DRIVES
 - b) relevant staff in the Department of Customer Service about the Digital Restart Fund, cyber security, and legacy systems
 - c) relevant staff in Treasury about the funding of the RegStar program and other issues related to DRIVES
 - d) interviewing relevant staff in agencies that use DRIVES to understand:
 - i) accountabilities for the information stored on DRIVES
 - ii) the impact of the operation and modernisation of DRIVES on their service delivery
 - iii) the management of risks associated with the access to DRIVES
 - iv) stakeholders to understand their perspective on the current operation of DRIVES, including issues and shortcomings, and the plans for the updating/replacement of the system
2. examining relevant documents, such as policies and procedures, to assess whether processes required under relevant legislation and government policies were followed
3. analysing data on DRIVES' operation and modernisation.

We also examined:

- cabinet and legal professional privileged information
- documentation from other stakeholders obtained throughout the audit such as research and studies, statistical data and analysis
- information from other jurisdictions for comparison.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Auditing Standard ASAE 3500 Performance Engagements and other professional standards. The standards require the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. Our processes have also been designed to comply with requirements specified in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

Acknowledgements

We gratefully acknowledge the cooperation and assistance provided by Transport for NSW. We would particularly like to thank our liaison officers and staff who participated in interviews and provided evidence for the audit.

We also wish to thank other stakeholders, such as the NSW Police Force and the Department of Customer Service, that spoke to us and provided material during the audit.

Audit cost

The estimated cost of this audit including disbursements is \$427,260.

Appendix four – Performance auditing

What are performance audits?

Performance audits assess whether the activities of State or local government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws.

The activities examined by a performance audit may include a government program, all or part of an audited entity, or more than one entity. They can also consider particular issues which affect the whole public sector and/or the whole local government sector. They cannot question the merits of government policy objectives.

The Auditor-General's mandate to undertake audits is set out in the *Government Sector Audit Act 1983* for state government entities, and in the *Local Government Act 1993* for local government entities. This mandate includes audit of non-government sector entities where these entities have received money or other resources, (whether directly or indirectly) from or on behalf of a government entity for a particular purpose (follow-the-dollar).

Why do we conduct performance audits?

Performance audits provide independent assurance to the NSW Parliament and the public.

Through their recommendations, performance audits seek to improve the value for money the community receives from government services.

Performance audits are selected at the discretion of the Auditor-General who seeks input from parliamentarians, State and local government entities, other interested stakeholders and Audit Office research.

How are performance audits selected?

When selecting and scoping topics, we aim to choose topics that reflect the interests of parliament in holding the government to account. Performance audits are selected at the discretion of the Auditor-General based on our own research, suggestions from the public, and consultation with parliamentarians, agency heads and key government stakeholders. Our three-year performance audit program is published on the website and is reviewed annually to ensure it continues to address significant issues of interest to parliament, aligns with government priorities, and reflects contemporary thinking on public sector management. Our program is sufficiently flexible to allow us to respond readily to any emerging issues.

What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing.

During the planning phase, the audit team develops an understanding of the audit topic and responsible entities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the audited entity, program or activities are assessed. Criteria may be based on relevant legislation, internal policies and procedures, industry standards, best practice, government targets, benchmarks or published guidelines.

During the fieldwork phase, audit teams will require access to books, records, or any documentation that are deemed necessary in the conduct of the audit, including confidential information which is either Cabinet information within the meaning of the *Government Information (Public Access) Act 2009*, or information that could be subject to a claim of privilege by the State or a public official in a court of law. Confidential information will not be disclosed, unless authorised by the Auditor-General.

At the completion of fieldwork, the audit team meets with management representatives to discuss all significant matters arising out of the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with management representatives to check that facts presented in the draft report are accurate and to seek input in developing practical recommendations on areas of improvement.

A final report is then provided to the accountable authority of the audited entity(ies) who will be invited to formally respond to the report. If the audit includes a follow-the-dollar component, the final report will also be provided to the governing body of the relevant entity. The report presented to the NSW Parliament includes any response from the accountable authority of the audited entity. The relevant Minister and the Treasurer are also provided with a copy of the final report for State government entities. For local government entities, the Secretary of the Department of Planning and Environment, the Minister for Local Government and other responsible Ministers will also be provided with a copy of the report. In performance audits that involve multiple entities, there may be responses from more than one audited entity or from a nominated coordinating entity.

Who checks to see if recommendations have been implemented?

After the report is presented to the NSW Parliament, it is usual for the entity's Audit and Risk Committee/Audit Risk and Improvement Committee to monitor progress with the implementation of recommendations.

In addition, it is the practice of NSW Parliament's Public Accounts Committee to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report received by the NSW Parliament. These reports are available on the NSW Parliament website.

Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian standards.

The Public Accounts Committee appoints an independent reviewer to report on compliance with auditing practices and standards every four years. The reviewer's report is presented to the NSW Parliament and available on its website.

Periodic peer reviews by other Audit Offices test our activities against relevant standards and better practice.

Each audit is subject to internal review prior to its release.

Who pays for performance audits?

No fee is charged to entities for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in-progress, please see our website www.audit.nsw.gov.au or contact us on 9275 7100.

OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

OUR PURPOSE

To help Parliament hold government accountable for its use of public resources.

OUR VALUES

Pride in purpose
Curious and open-minded
Valuing people
Contagious integrity
Courage (even when it's uncomfortable)

Level 19, Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000 Australia

PHONE +61 2 9275 7100

mail@audit.nsw.gov.au

Office hours: 8.30am-5.00pm
Monday to Friday.