Appendix one – Response from agencies

Response from Department of Customer Service

McKell Building – 2-24 Rawson Place, Sydney NSW 2000
Tel 02 9372 8877 | TTY 1300 301 181
www.nsw.gov.au

Office of the Secretary

Our reference: COR-03592-2021

Ms Margaret Crawford
Auditor-General
Audit Office of NSW
By email: mail@audit.nsw.gov.au

Dear Ms Crawford

Thank you for your letter dated 4 June 2021 and for the opportunity to respond to your audit report *Managing Cyber Risks*. The work of the Audit Office of New South Wales (NSW Audit Office) is an invaluable and key part of improving both the cyber security resilience and accountability of NSW Government entities.

Managing Cyber Risks is a thorough report that has raised important issues regarding the cyber security of NSW Government entities. The Department of Customer Service (the Department) notes the recommendation to "clarify the requirement for the Cyber Security Policy reporting to apply to all systems." The Cyber Security Policy covers the security of Information Technology (IT), Operational Technology (OT), the Internet of Things (IoT) and other connected systems and devices.

To keep pace with a rapidly evolving cyber threat environment, Cyber Security NSW is undertaking a review of the Cyber Security Policy for its 2022 iteration. With the intention to reduce ambiguity, this review will include clearer wording and instructions on the various sections of reporting maturity levels.

The Department also notes the recommendation to "require agencies to report the level of maturity for each mandatory requirement they have determined appropriate for their agency." The Cyber Security Policy is a risk-based Policy whereby agencies determine the appropriate level of maturity based on their risk appetite. Agencies are encouraged to strive for a level across the board collectively, rather than set a benchmark of level 3 for all Mandatory Requirements. However, as part of the current review of the Cyber Security Policy, the Department will explore the option of implementing formalised processes for agency-determined target maturity levels. Likewise, the Department will also consider implementation of the evolving advice from the Australian Cyber Security Centre (ACSC) on risk-based approaches to cyber resilience. This includes consideration of new guidance on the ACSC Essential Eight. Any such changes will be made in close consultation with the reporting entities.

Consistent with the position of the Australian National Audit Office (ANAO) and based on the advice of Australian Signals Directorate (ASD), the Department believes that the interests of accountability and transparency must be balanced with the need to manage risks. This includes risks identified by the ASD in disclosure of information which may be used by adversaries to target their malicious activities. Whilst the Department recognises that the NSW Audit Office is considering this level of balance, we trust that the Audit Office will continue to assess risks associated with the level of disclosure of confidential and sensitive information and seek advice from the ASD, to keep in line with the changing threat environment.

The Department continues to have some concerns regarding the commissioning of external providers to undertake penetration and red team testing. Effective collaboration between all parties on the scope and approach for red team testing would provide a vehicle to identify and address any vulnerabilities whilst safeguarding the very systems and services NSW Government entities, such as Transport for NSW in this instance, are working to protect. The cyber security of NSW Government entities is a collective responsibility and all entities must work together to make NSW Government systems and services more secure, trusted and resilient.

The Department seeks to continually improve the Cyber Security Policy and other processes used to assist these entities, including supporting documentation and the provision of advice. This report is a timely reminder that there is still much work to be done. With the assistance of agencies like the NSW Audit Office, the Department will continue to engage with Transport for NSW, Sydney Trains and all NSW Government entities to assist in uplifting their cyber security posture.

Yours sincerely

Emma Hogan
Secretary

Date: 02/07/21

Response from Transport for NSW

Transport for NSW

Your ref: D2110328
Our Ref: OTS20/07456

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

Dear Ms Crawford

Thank you for the opportunity to respond to the Performance Audit Report (the Report) on managing cyber risks. Transport for NSW (TfNSW) and Sydney Trains welcome the findings of the Report and are committed to further strengthening our organisational and operational cyber security to protect our customers, our staff and our critical infrastructure. Cyber security risk management remains, and has always been, an important part of TfNSW and Sydney Trains executive oversight and decision-making and we are committed to continuing to focus and invest in uplifting our cyber security capabilities.

In the current cyber security environment of constantly evolving threats and high-profile cyberattacks on all types of organisations in Australia and overseas, TfNSW and Sydney Trains recognise the need to continuously improve our cyber defence capabilities to protect our staff, the NSW Government, and the people of NSW.

We are pleased to advise that there has been measurable uplift in TfNSW and Sydney Trains' cyber maturity in line with our unprecedented investment in Transport's Cyber Defence Portfolio. This Report and its recommendations will serve as constructive input to underpin our ongoing efforts as we continue to focus on improving cyber security as a key priority in our journey towards Future Transport 2056.

TfNSW and Sydney Trains have come a long way over recent years and have invested diligently in planning and delivering measures to address cyber security using a prioritised, risk-based approach. Over the 2019/20 and 2020/21 financial years, our $26 million investment has delivered an uplift in cyber security maturity across the Transport cluster, evidenced by the increase in maturity of essential cyber controls in annual reporting to the Department of Customer Service (Cyber Security NSW) for the last two years.

As a clear demonstration of the continued importance and value placed on cyber security, from July 2020 through to June 2023, Transport will have invested an additional $60 million to support the ongoing uplift of our Cyber Defence Portfolio. In addition, $20 million will be allocated to the Cyber Defence Program from the Digital Restart Fund to further uplift Cyber security.

This journey of continuous improvement and maturity uplift across one of Australia's largest and most complex government entities demonstrates our focus on and commitment to cyber security resilience. Our current and future investments will continuously reduce our cyber security risks in the coming years.

TfNSW and Sydney Trains were among the first NSW Government agencies to recognise the need for robust cyber risk management. Accordingly:

Transport for NSW
231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | **F** 02 8202 2209 | **W** transport.nsw.gov.au | ABN 18 804 239 602

- In 2017, TfNSW initiated the Transport IT risk management program. This program has implemented tools and processes to cover, among other things, cyber security risk management as well as cross cluster critical IT assets.

- In 2018, TfNSW initiated the Cyber Uplift Program followed by Sydney Trains in 2019. The mandate was to develop tools and processes to uplift cyber risk management. This program continues to deliver on the mandate.

- Since 2019, TfNSW and Sydney Trains have invested diligently in planning and delivering measures to address cyber security risks using a prioritised, risk-based approach.

Both TfNSW and Sydney Trains have robust and detailed governance forums where reporting and discussions on cyber security are undertaken by executives with the appropriate specialised expertise.

TfNSW and Sydney Trains' evidenced multi-layered 'defence-in-depth' approach to protecting assets (data, systems and identities) supports a proactive approach to stopping cyberattacks before they occur, protecting our transportation services and safeguarding customer data.

While the Report identifies specific instances for further uplift, TfNSW and Sydney Trains' cyber security controls already effectively prevent a significant number of intrusion attempts and our teams continuously monitor our cyber security environment and respond quickly to cyber security threats.

From July 2021, cyber security training will become mandatory for all staff. In addition to formal training, we frequently communicate with staff across the Transport cluster about cyber security risks through the intranet, emails, communities of practice, and other awareness raising activities to highlight the importance for staff to be aware of the seriousness of cyber risks.

TfNSW and Sydney Trains will continue driving a culture of improved cyber security risk identification, management and reporting. Since 2019, regular reporting to all levels of management has been delivered through the Cyber Defence Portfolio. Transport's independent Audit and Risk Committees also receive detailed quarterly cyber security updates from Transport's Chief Information Security Officer. Further, cyber security risks are embedded in agency enterprise risk reporting to ensure the detailed management and remediation of cyber risks at an operational level and support strategic and investment decisions.

As a demonstration of our commitment to continuously improve cyber security culture and governance, enhanced and more detailed monthly cyber reporting has been introduced to the Transport Executive; based on Cybersecurity NSW reporting requirements, with further refinements being developed across the NSW Government. A new Technology Steering Committee, comprising members of the Transport Executive and key subject matter experts, has been designed to provide a greater consolidation of executive direction and oversight of Transport's customer technology, information technology and operational technology functions.

Cyber security management is a journey of continual improvement against threat actors whose tactics regularly change, and we will continue to respond to this challenge across our systems,

Transport for NSW
231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | **F** 02 8202 2209 | **W** transport.nsw.gov.au | ABN 18 804 239 602

our information and the critical operational and customer services we deliver across all modes of transport in NSW.

If you have any further questions, Fiona Trussell, Deputy Secretary Corporate Services would be pleased to take your call. I hope this has been of assistance.

Yours sincerely

Rob Sharp
Secretary

24/06/2021

Transport for NSW
231 Elizabeth Street, Sydney NSW 2000 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | **F** 02 8202 2209 | **W** transport.nsw.gov.au | ABN 18 804 239 602