Appendix one – Responses from agencies

Response from Service NSW

Ms Margaret Crawford
Auditor-General for New South Wales
Level 19, 201 Sussex Street
Darling Park Tower 2
SYDNEY NSW 2000

Dear Ms Crawford

Thank you for the opportunity to respond to the Performance Audit *Service NSW's handling of personal information* report, which assessed how effectively Service NSW handles personal customer and business information to ensure its privacy.

Service NSW accepts the recommendations in full. We are committed to significant and enduring changes to the way we do business, to ensure all personal information is secure while in our custody and the trust of our customers and our partner agencies is maintained. A significant amount of work has already occurred since the incident, and our suite of further planned improvements addresses all of the recommendations and commits us to continuously enhancing our cyber and privacy protections as customer needs, technologies and threats evolve. We have outlined this program in a public action plan, which we include with this response.

The data breach of Service NSW's systems earlier this year profoundly affected our customers, our partner agencies' customers, and our staff, in a year when Service NSW has played a leading role in the NSW response to bushfires and the COVID-19 pandemic. We have dedicated teams from Service NSW and the Department of Customer Service to understand, rectify and mitigate this risk into the future. Our primary focus has always been our customers, and our response to this incident is no different. We have put considerable efforts into supporting customers who have been impacted, including hypercare support for all those impacted, and referrals to identity and cyber recovery service IDCare. Feedback on this support from customers and staff has been resoundingly positive. staff has been resoundingly positive.

However, we have much more to do. Service NSW has implemented a risk appetite statement with zero appetite for privacy risk. To give effect to this, we have recently established a comprehensive privacy enhancement program to drive continual improvement in how we manage personal information. We have taken several measures to reduce privacy risks in 2020 including enhanced cybersecurity measures, automated secure archiving of personal information, and mandatory privacy training for all staff. We also have wide-ranging improvements to privacy protection scheduled throughout 2021. These include reducing paper processes and more secure methods of transmitting and storing personal information, better customer access to holdings of their personal information within Service NSW, minimising instances where we need to retain personal information, consistently assessing and mitigating the privacy impact of new products and services and existing products and services as they evolve, and clearer consent and use statements.

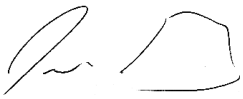
Service NSW is working in partnership with the Department of Customer Service who is leading further cluster-wide improvements in cybersecurity, privacy, information security and governance through its "Project Trust". The significance and the scale of improvements in the pipeline demonstrate how seriously we take our responsibility to rebuilding the trust of our customers and staff.

Service NSW has delivered unprecedented support and relief to citizens in the face of significant crises over the past 12 months. Drought, bushfires and COVID have seen an exponential increase in reliance on Service NSW to deliver for our community, in person, over the phone and online. Responding to these crises so quickly has been challenging, and my leadership team and I have reflected on the insights gained through this experience and this audit. Everything we do is in partnership with other agencies, to deliver services on their behalf, and we are fully committed to working with our partners to embed these lessons across our business and better manage these risks.

Service NSW will address the recommended remediations as a priority, and I look forward to sharing our progress through open and transparent communication, and through independent progress reviews I have requested in 2021.

I would like to again thank you and your team for your work on this audit and the insights it has provided.

Yours sincerely,



Damon Rees
Chief Executive Officer

17/12/2020

Service NSW's Handling of Personal Information – Public Action Plan

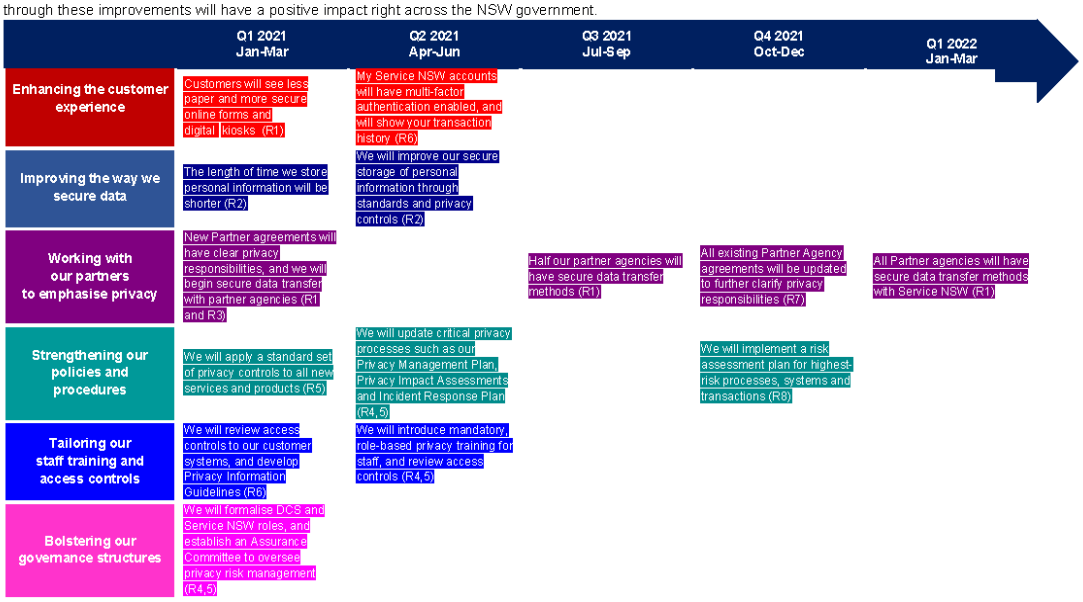
Since the cyber-attack and data breach, Service NSW has completed several interim privacy management improvements and commenced an organisation-wide program of enduring changes and improvements to the way we manage personal information.

Meaningful changes we have made since the breach to reduce the risk of a similar type of data breach occurring in future include:

- implementing Multi-Factor Authentication on the majority of critical applications, to reduce the risk of unauthorised access to staff email accounts and key software
- strengthening information security practices for increased volumes of staff working remotely, including accessible Working Securely advice for staff, increasing the vigilance of our staff on security
- reduced by an estimated 92% the amount of personal information held in email inboxes by automatically archiving emails to a secure location after a specified number of days (where they are no longer available within the email account itself), and auto-archiving emails known to contain personal information in a much shorter time
- migrated email services to a multi-agency, secured "tenancy", to benefit from regular and consistent whole-of-government improvements, patches and security updates
- removed out-of-date system authorisations and accesses
- migrated sensitive Service NSW staff information into secure systems and portals
- upgraded software licensing for increased security features and threat protection
- contributed to Phase 1 (Immediate response and resilience priorities) of the Cluster-wide Project TRUST, led by the Department of Customer Service, designed to uplift privacy, cybersecurity, information security and information governance practices.
- appointed a Chief Risk Officer and Chief Privacy Officer to lead these reforms and to drive continuous improvement in, managing personal information and mitigating privacy risk.

Service NSW has also commenced work on the following significant improvements, which will be implemented by end of March 2022

The following work is underway. These actions will address the Audit Office's recommendations, significantly reduce our risk profile and make our systems even more resilient, while continuing to provide the level and quality of service that we pride ourselves on, and our customers, the people of NSW, expect from Service NSW. Importantly, these improvements are being implemented in partnership with our 63 partners across government. The benefits to be realised through these improvements will have a positive impact right across the NSW government.



Response from Department of Customer Service

McKell Building – 2-24 Rawson Place, Sydney NSW 2000
Tel 02 9372 8877 | TTY 1300 301 181
ABN 81 913 830 179 | www.customerservice.nsw.gov.au

Ms Margaret Crawford
Auditor-General Audit
Office NSW

Via email: margaret.crawford@audit.nsw.gov.au

Dear Ms Crawford,

Report on the Performance Audit into Service NSW's handling of personal information

Thank you for the opportunity to respond to the Performance Audit of Service NSW's handling of personal information.

I acknowledge your findings, which Service NSW has also accepted in full.

As noted in your report, DCS is committed to response, recovery and resilience activities related to the Service NSW cyber security breach. Customer trust underpins our work, and we take that responsibility very seriously.

In May of this year, I established the Cyber and Privacy Resilience Governance Group (CPRGG). The CPRGG, including representatives from DCS, Service NSW, Cyber Security NSW, Digital NSW, Resilience NSW, NSW Police, IDCARE and Information Integrity Solutions, is charged with overseeing our response to the Service NSW data breach and our 'Project Trust' program of work to making the Department of Customer Service, and Service NSW an exemplar in cyber security and privacy management. In our role as a central agency role, we are also committed to sharing these learnings across government.

Project Trust has been established to lead the development of the ongoing recovery framework for the Department, including building and strengthening our resilience to cyber and privacy risks and our overall cyber and privacy incident preparation, prevention, detection, response and recovery for the benefit of all NSW Government customers, our staff and our partner agencies.

Cyber security is a key focus of NSW Government agencies and a critical enabler to digital transformation and the delivery of digital services for NSW citizens. The Digital Restart Fund includes $240 million already allocated to uplift cyber security maturity, a critical part of transformation.

I look forward to delivering on our action plan and updating our customers and stakeholders on our progress throughout 2021.

Yours sincerely

Emma Hogan
Secretary