SPECIAL REPORT 18 DECEMBER 2020

Service NSW's handling of personal information

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

audit office
OF NEW SOUTH WALES

THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the *Public Finance and 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 Total State Sector Accounts, a consolidation of all agencies' accounts.

Financial audits are designed to add credibility to financial statements, 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 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 examine whether an entity is carrying out its activities effectively and doing so economically and 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.

As well as financial and performance audits, the Auditor-General carries out special reviews and compliance engagements.

Performance audits are reported separately, with all other audits included in one of the regular volumes of the Auditor-General's Reports to Parliament – Financial Audits.

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 *52B of the Public Finance and Audit Act 1983,* I present a report titled **'Service NSW's handling of personal information'.**

Margaret Crawford
Auditor-General
18 December 2020

auditoffice
OF NEW SOUTH WALES

contents

Service NSW's handling of personal information

Section one

Service NSW's handling of personal information

Executive summary

Service NSW was established in 2013 with the intention that it would, over time, 'become the primary interaction point for customers accessing New South Wales Government transaction services'.

Service NSW's functions are set out in the *Service NSW (One-stop Access to Government Services) Act 2013*. This legislation allows for other NSW Government agencies to delegate to and enter into agreements with the Chief Executive Officer of Service NSW in order for Service NSW to undertake service functions for the agency.

Service NSW now has agreements with 36 NSW Government client agencies to facilitate over 1,200 types of interactions and transactions for the community.

The nature of each agreement between Service NSW and its client agencies varies. Some client agencies have delegated authority to allow Service NSW staff to conduct transactions on their behalf in the agencies' systems. Other arrangements do not include the same degree of delegation. In these cases, Service NSW provides services such as responding to enquiries and validating documents.

In addition, Service NSW conducts transactions for its own programs, such as the Seniors Card. Personal information for these programs, as well as information for customers' MyServiceNSW accounts, are stored by Service NSW on its Salesforce Customer Relationship Management (CRM) system.

In March 2020, Service NSW suffered two cyber security attacks in short succession. Technical analysis undertaken by the Department of Customer Service (DCS) concluded that these attacks resulted from a phishing exercise through which external threat actors gained access to the email accounts of 47 staff members. These attacks resulted in the breach of a large amount of personal customer information that was contained in these email accounts. See Section 1.1 for further details.

This audit is being conducted in response to a request from the Hon. Victor Dominello, Minister for Customer Service, under section 27B(3)(c) of the *Public Finance and Audit Act 1983*. Minister Dominello requested that the Auditor-General conduct a performance audit in relation to Service NSW's handling of sensitive customer and business information.

This audit assessed how effectively Service NSW handles personal customer and business information to ensure its privacy.

It addressed the following:

- Does Service NSW have processes and governance in place to identify and manage risks to the privacy of personal customer and business information?
- Does Service NSW have policies, processes and systems in place that support the effective handling of personal customer and business information to ensure its privacy?
- Has Service NSW effectively implemented its policies, processes and systems for managing personal customer and business information?

Conclusion

Service NSW is not effectively handling personal customer and business information to ensure its privacy. It continues to use business processes that pose a risk to the privacy of personal information. These include routinely emailing personal customer information to client agencies, which is one of the processes that contributed to the March 2020 data breach. Previously identified risks and recommended solutions had not been implemented on a timely basis.

Service NSW identifies privacy as a strategic risk in both its Risk Management Guideline and enterprise risk register and sets out a zero-level appetite for privacy risk in its risk appetite statement. That said, the governance, policies, and processes established by Service NSW to mitigate privacy risk are not effective in ensuring the privacy of personal customer and business information. While Service NSW had risk identification and management processes in place at the time of the March 2020 data breach, these did not prevent the breach occurring.

Some of the practices that contributed to the data breach are still being followed by Service NSW staff. For example, business processes still require Service NSW staff to scan and email personal information to some client agencies.

The lack of multi-factor authentication has been identified as another key contributing factor to the March 2020 data breach as this enabled the external threat actors to gain access to staff email accounts once they had obtained the user account details through a phishing exercise. Service NSW had identified the lack of multi-factor authentication on its webmail platform as a risk more than a year prior to the breach and had committed to addressing this by June 2019. It was not implemented until after the breach occurred.

There are weaknesses in the general IT and security controls implemented by Service NSW over its Salesforce Customer Relationship Management (CRM) system, which holds the personal information of over four million NSW residents.

Internal audits carried out by Service NSW, including one completed in August 2020, have identified significant weaknesses in the general IT and security controls implemented by Service NSW over its Salesforce CRM system. These include deficiencies in the management of role-based access, monitoring and audit of user access, and partitioning of program specific transaction information. These deficiencies create an increased risk of unauthorised access to the personal information of over four million customers held in the system.

Lines of responsibility for meeting privacy obligations are not clearly drawn between Service NSW and its client agencies.

Service NSW has agreements in place with client agencies. However, the agreements lack detail and clarity about the roles and responsibilities of the agencies in relation to the collection, storage and security of customer's personal information. This lack of clarity raises the risk that privacy obligations will become confused and missed between the agencies.

Service NSW carries out privacy impact assessments for major new projects but does not routinely review existing processes and systems.

Service NSW carries out privacy impact assessments as part of its routine processes for implementing major new projects, ensuring that privacy management is considered as part of project design. Service NSW does not regularly undertake privacy impact assessments or reviews of existing or legacy processes and systems, which has resulted in some processes continuing despite posing significant risks to the privacy of personal information, such as the scanning, emailing, and storing of identification documents.

1. Key findings

Service NSW identifies privacy risks, but the controls and processes it put in place to mitigate these privacy risks were not adequate to prevent or limit the extent of the data breach that occurred in March 2020

Service NSW's approach to risk management is framed by its Risk Management Guideline, which defines 'privacy and compliance' as one of the key types of risk for the agency. Service NSW's enterprise risk register identifies four strategic privacy-related risks. Service NSW has set out a zero-level appetite for privacy risk in its risk appetite statement.

Service NSW has assessed the adequacy of its controls for privacy risks as needing improvement. To be fully effective, the Risk Management Guideline says that these controls should have a focus that is 'largely preventative and address the root causes'.

> One of the business processes that was a key contributing factor to the data breach was the emailing of personal information by Service NSW staff to client agencies.

This process had been identified as a risk prior to the breach and some steps had been put in place to mitigate the risk. In particular, staff were required to manually delete emails that contained personal information. However, these measures were ineffective in preventing the breach, as the external threat actors still gained access to 47 staff email accounts that contained a large amount of personal information.

It is unclear why Service NSW did not effectively mitigate this risk prior to the breaches. However, Service NSW has advised that it implemented measures in June and October 2020 to automatically archive emails likely to contain personal information. This is expected to limit the quantity of information retained in email accounts for extended periods.

Service NSW has not put in place any technical or other solutions to avoid Service NSW staff having to scan and email personal information to some client agencies. Urgent action is needed to remove the requirement for staff to email personal information to client agencies, thereby mitigating the risk inherent in sending and storing this information using email.

There are weaknesses in the general IT and security controls implemented by Service NSW over its Salesforce CRM system, which holds the personal information of over four million customers

There are weaknesses in the general IT and security controls implemented by Service NSW over its Salesforce CRM system. These weaknesses include deficiencies in governance of role-based access, monitoring and audit of staff access, and partitioning of program specific transaction information. These deficiencies create an increased risk of unauthorised access to the personal information of over four million customers which is stored in this system.

In addition, there is an absence of important controls to safeguard customers' privacy, such as multi-factor authentication and reviewable logs of access history to their information. Such controls, when properly implemented, would enhance the control that customers are able to exercise over their personal information.

A privacy impact assessment conducted on Service NSW's Salesforce CRM system in 2015 recommended that the system include the ability for customers to review access history to their personal information, as well as the option for customers to apply multi-factor authentication to their accounts. While both these recommendations appeared positively received by Service NSW, neither have been implemented.

Since its inception, Service NSW's use of Salesforce has extended to storing transaction data, particularly for transactions for which Service NSW is responsible, such as the Seniors Card. It also holds details of over four million MyServiceNSW account holders, including name, email address and phone number, and optional address details. It was not originally intended for the system to hold this volume and nature of customer information.

Lines of responsibility for meeting privacy obligations are unclear between Service NSW and its client agencies

Service NSW's privacy management plan does not clearly set out the privacy obligations of Service NSW and its client agencies. It sets out that 'compliance with the privacy principles will primarily be the responsibility of that [client] agency'. However, Service NSW has its own obligations under the security principles of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) to take reasonable steps to prevent unauthorised access to personal information, which is not made clear in the privacy management plan.

The agreements between Service NSW and client agencies reviewed for this audit only include general and high-level references to privacy. Most do not include details of each parties' privacy responsibilities such as: which agency will provide the customer with a privacy notice explaining how their personal information will be handled, how personal information will be kept secure, how long Service NSW will retain information, what processes will be followed for internal reviews, and what specific planning is in place to respond to data breaches.

Service NSW's privacy management plan has not been updated to include new programs and governance changes

Service NSW's privacy management plan includes most of the matters required by law or good practice, with some exceptions. It does not explain any exemptions that the agency commonly relies on under the PPIP Act and does not address any health information that Service NSW may handle. It had also not been updated to reflect governance changes and the fact that, at the time this audit commenced, Service NSW was disclosing the content of internal review applications (the formal expression for 'complaints') to the Department of Customer Service (DCS). These governance changes were part of the centralisation of Service NSW's corporate support functions into DCS in late 2019, though internal review staff were seconded back into Service NSW during the course of this audit.

The current July 2019 privacy management plan has also not been updated since the rollout of a number of major new initiatives in 2020. These include 2019–20 bushfire emergency recovery initiatives (such as small business grants) and COVID-19 pandemic response initiatives (such as small business grants, border permits and the COVID safe check-in app).

Service NSW routinely conducts privacy impact assessments for new initiatives, though privacy risks remain in legacy systems and processes

Service NSW routinely conducts privacy impact assessments for major new initiatives and the assessments reviewed for this audit largely accorded with good practice guidance.

Service NSW does not routinely review existing processes and systems to ensure that they are effective in ensuring the privacy of customer personal information. Business processes that create the highest risk to privacy, such as emailing of personal information, are more common in these longstanding legacy systems.

Service NSW's significant and rapid growth has outpaced the establishment of a robust control environment which has exacerbated privacy risks

Since it was established in 2013, Service NSW has experienced significant growth in the number and diversity of the types of transactions it provides, as well as the number of client agencies with which it works. The pace and extent of this growth has contributed to important controls not being properly implemented on a timely basis, which has heightened privacy risks, particularly in regard to existing, legacy systems and processes.

The pace of change and increasing demand for new program implementation has limited the opportunity for Service NSW, in collaboration with its client agencies, to revisit and redesign legacy business practices which pose a greater privacy risk. This includes the scanning and emailing of personal information.

While 2019–20 has seen additional demands placed on Service NSW in responding to the 2019–20 bushfire emergency and COVID-19 pandemic, it is the nature of the agency's work that it operates in a fast-paced and complex environment, where it is required to respond to multiple client agencies and stakeholders. Ensuring customer privacy should be integral to Service NSW's business as usual operations.

2. Recommendations

Service NSW commissioned a number of external reviews and investigations stemming from the data breaches. The Auditor-General's recommendations below have taken these other reviews into account. In order to offer assurance that it is appropriately protecting the privacy of its customers, Service NSW should address the full breadth of findings and recommendations made across all relevant reviews.

As a matter of urgency, Service NSW should:

1. in consultation with relevant client agencies and the Department of Customer Service, implement a solution for a secure method of transferring personal information between Service NSW and client agencies
2. review the need to store scanned copies of personal information and, if still required, implement a more secure method of storing this information and regular deletion of material.

By March 2021, Service NSW should:

3. ensure that all new agreements entered into with client agencies from 1 April 2021 address the deficiencies identified in this audit, including that they provide clarity on:
    - the content and provision of privacy collection notices
    - the terms by which personal information will be retained, stored, archived, and disposed of when no longer required
    - steps that will be taken by each agency to ensure that personal information is kept secure
    - the circumstances in which, and processes by which, applications for internal review will be referred by one agency to the other
    - how identified breaches of privacy will be handled between agencies
4. in collaboration with the Department of Customer Service, review its privacy management plan to address the deficiencies raised in this audit, including:
    - to clarify Service NSW's understanding of how responsibility for meeting privacy obligations are delineated between Service NSW and client agencies
    - to better reflect the full scope and complexity of personal information handled by Service NSW
    - to better explain how applications for internal review are handled between Service NSW and the Department of Customer Service
    - to ensure regular ongoing review, either according to a schedule or when Service NSW experiences substantial change to its programs and handling of personal information
5. in consultation with the Department of Customer Service, review its policies and processes for the management of privacy risks, including to:
    - ensure that there are appropriate mechanisms to escalate identified privacy risks from business units to the Executive Leadership Team
    - ensure that there are action plans to address strategic privacy risks that are assessed as having ineffective controls.

By June 2021, Service NSW should:

6. address deficiencies in the controls over, and security for, its Salesforce customer relationship management and related systems that hold customer personal information, including:
    - establish policies and processes for regular access reviews and monitoring of user activity in these systems, including for privileged users
    - enable partitioning and role-based access restrictions to personal information collected for different programs
    - provide customers the choice to use multi-factor authentication to further secure their MyServiceNSW accounts
    - enable customers to view the transaction history of their personal information to detect possible mishandling.

By December 2021, Service NSW should:

7. ensure that all existing agreements with client agencies address the deficiencies identified in this audit, including that they provide clarity on:
    - the content and provision of privacy collection notices
    - the terms by which personal information will be retained, stored, archived, and disposed of when no longer required
    - steps that will be taken by each agency to ensure that personal information is kept secure
    - the circumstances in which, and processes by which, applications for internal review will be referred by one agency to the other
    - how identified breaches of privacy will be handled between agencies
8. carry out a risk assessment of all processes, systems and transactions that involve the handling of personal information and undertake a privacy impact assessment for those that:
    - are identified as high risk and have not previously had a privacy impact assessment
    - have had major changes or updates since the privacy impact assessment was completed.

1. Introduction

1.1 March 2020 Cyber security breach

Details of the breach

In late March to early April 2020, Service NSW suffered two cyber security attacks in relatively short succession. In mid-April 2020, Service NSW engaged a cyber security consultant after concerns were raised that an employee's email account was used to send an email to 2,725 Service NSW users, including content indicative of phishing attempts.

Analysis found that there were likely to have been two separate business email compromise instances, in which an external threat actor sent phishing emails targeting Service NSW employees from a spoofed domain (using a false domain name to make the sender appear legitimate).

The malicious phishing campaign mimicked an Office 365 warning email, prompting Service NSW employees to visit a fake Office 365 login page which solicited the user's Service NSW credentials. As a consequence, 47 staff members had their email accounts accessed without authorisation.

Service NSW originally reported that this cyber attack had resulted in the breach of around five million documents, of which around 500,000 were likely to contain personal information. Service NSW also reported that around 186,000 NSW residents had been affected by the cyber attack. On 16 December 2020, Service NSW issued a statement that, while analysis is still ongoing, it now estimates that fewer customers may be affected by the breach. The data supporting that statement has not been provided to the Audit Office and is not verified by this audit. It remains important to note that even if the estimate of affected customers is revised, the impact of the breach has nevertheless been serious, and the processes in Service NSW need significant improvement.

Response to the breach

On 14 April 2020, Service NSW escalated internally an apparent breach of its cyber security protections. The next day, Service NSW engaged an external consultant to conduct investigative analysis of how staff members' email accounts had been compromised and whether Service NSW's IT system had been more widely compromised.

On 1 May 2020, the consultant reported that the contents of 47 Service NSW email boxes had been compromised.

On 14 May 2020, Service NSW announced the breach to the public. In response to the breach, the Minister for Customer Service wrote to the Auditor-General to request her to undertake a performance audit of Service NSW's handling of 'sensitive customer and business information'. This report presents the findings from this audit.

In response to the breach, the Secretary of the Department of Customer Service (DCS) convened a Cyber and Privacy Resilience Governance Group, which first met in late May 2020. The purpose of this group included providing executive-level leadership and oversight of the response, recovery and resilience activities related to the cyber security breach.

Customers deemed at the highest risk from the breach were notified in May and June 2020, with the balance scheduled to be notified between September and December 2020, following extensive data cleaning to ensure contact details were accurate.

The breach also led to the creation of Project TRUST, a series of work programs designed to respond to the breach and build resilience to reduce the risk of future cyber security and privacy breach incidents across the DCS cluster.

As Service NSW's response to the breach was ongoing at the time of this audit, the full cost of its response was not known. However the agency advised that it is expected to be in excess of $30 million. This amount includes postage, legal and investigative resources, as well as external consultants, vendors, and staff costs. The amount does not include any costs for remediation or compensation that may be required to be paid to affected individuals, including any costs of replacing documents such as the licences or passports of affected individuals.

1.2 Overview of Service NSW

Service NSW background

In 2011, the NSW Government envisaged the creation of a government agency that would help to increase customer satisfaction with government services. The government's ten-year strategic plan announced that the new agency, to be called Service NSW, would provide a single NSW Government phone number, a customer-friendly web portal, and one-stop shops for multiple customer transactions.

In 2013, Service NSW was formally created with the intention to provide people with simpler and easier access to services that the NSW Government offers. The then Premier envisaged that the agency would, over time, 'become the primary interaction point for customers accessing New South Wales Government transaction services'.

Service NSW functions

Service NSW's functions are set out in the *Service NSW (One-stop Access to Government Services) Act 2013*. This legislation allows for other NSW Government agencies to delegate to and enter into agreements with the Chief Executive Officer of Service NSW in order for Service NSW to undertake service functions for the agency.

Although far less common, the Commonwealth Government, any State or Territory Government, and non-government entities may also delegate customer service functions to the Chief Executive Officer of Service NSW.

Service NSW processes and systems

Service NSW has agreements with 36 NSW Government client agencies to facilitate over 1,200 interactions and transactions for the community. It also has one agreement with the Commonwealth Government (Services Australia) and with a non-government organisation (the NRMA for the purpose of processing international driver licences).

The agency adopts a multi-channel model of service delivery entailing 'digital, over the counter and over the phone' services, including 109 service centres and five contact (call) centres. In implementing this multi-channel model, Service NSW uses a range of different IT systems.

The nature of the services provided by Service NSW vary across agencies and transactions. Some services are provided wholly by Service NSW, such as the NSW Seniors Card and, more recently, various initiatives responding to the COVID-19 pandemic and 2019–20 bushfire emergency.

For other transactions, Service NSW staff access the systems of client agencies to conduct transactions on behalf of those agencies. For example, Service NSW staff in both the service and contact centres may access the DRIVES system owned by Transport for NSW (TfNSW) to enter data for a range of licence and registration transactions.

Service NSW staff may also access client agency systems to provide information in response to enquiries. For example, contact centre staff have read-only access to the Lifelink system owned by the Registry of Births Deaths and Marriages to answer enquiries over the phone.

In addition to the client agency systems, staff in contact centres and other head office staff have access to a Salesforce CRM system. This CRM is a commercial cloud-based software application. Service NSW uses its Salesforce CRM for retaining customer account details, to record customer interactions, and to make bookings for matters that require an appointment.

Customer information for some individual programs is also stored on the Salesforce CRM system, as well as the MyServiceNSW account information for over 4.3 million Service NSW customers. In addition, the Service NSW website and MyServiceNSW account feature are also partly hosted on the Salesforce CRM system.

1.3 Machinery of Government and governance changes

From time to time, governments may make changes to the administrative and governance arrangements of agencies, including by creating or abolishing departments and transferring responsibilities or agencies from one department to another. In NSW, these Machinery of Government changes are done by an Administrative Arrangements Order made by the Governor on the advice of the government.

Following Machinery of Government changes announced on 2 April 2019, Service NSW was made part of the cluster for the newly formed Department of Customer Service (DCS).

While the Administrative Order for this change is silent on any transfer of functions between Service NSW and DCS, some support functions were subsequently centralised into DCS. This included the transfer of the Governance and Risk team, which had previously performed internal audit and governance services for Service NSW.

The Governance and Risk team had also provided Service NSW with privacy risk, compliance, and advice functions. This arrangement was formalised by a memorandum of understanding made on 31 October 2019, under which DCS agreed to provide this capability to ensure that Service NSW is meeting its privacy obligations. The assistance provided by DCS includes:

- assisting Service NSW to conduct internal reviews under section 53 of the *Privacy and Personal Information Protection Act 1998* (the PPIP Act)
- assisting Service NSW to comply with privacy legislation, including:
  - investigating possible breaches and making findings and recommendations
  - undertaking privacy training
  - drafting documents, including collection notices and privacy statements.

1.4 Privacy legislation in NSW

Regulation of 'personal information'

Most NSW Government agencies are required to comply with the *Privacy and Personal Information Protection Act 1998* (PPIP Act). The PPIP Act regulates how agencies collect, use, disclose, secure and provide access to 'personal information', which is defined as:

> information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Regulation of 'business information'

The definition of personal information is not limited to people acting in a private capacity. If an individual's identity can be determined from business information, the information is personal information for the purpose of privacy legislation. For example, Service NSW's Active Kids program can involve sole traders registering to be eligible as providers of health and fitness services under the program. To the extent that the sole trader's identity is 'apparent or reasonably ascertainable' then their registration information would be personal information and covered by the PPIP Act.

Service NSW conducts privacy impact assessments on programs that are business-focused if they involve the collection of personal information. For example, during 2020, Service NSW conducted a number of privacy impact assessments for small business support grants and tax relief relating to the 2019–20 bushfire emergency and COVID-19 pandemic responses.

The application of the privacy principles will often be different for an individual's business information than for other types of personal information. For example, what is 'reasonable' for an agency to do to secure an individual's health information will generally be much more than what is reasonable to keep publicly available information about the same individual's company directorships.

Regulation of 'health information'

In addition, the *Health Records and Information Privacy Act 2002* (HRIP Act) applies to how agencies handle health information, which is broadly defined to include personal information that is

a) information or an opinion about:
   i) the physical or mental health or a disability (at any time) of an individual,
   ii) an individual's express wishes about the future provision of health services to him or her
   iii) a health service provided, or to be provided, to an individual
b) other personal information collected to provide, or in providing, a health service
c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances
d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual
e) healthcare identifier.

Information privacy principles

Both of these Acts set out a range of 'privacy principles' that regulate how personal information, including health information, must be handled. These principles are intended to afford protection to personal information throughout the 'information lifecycle' by setting out obligations and rights around:

- the collection, use and disclosure of personal information
- an agency's openness, transparency and accountability in how it handles personal information
- the accuracy, quality, and correction of personal information
- the rights of individuals to access their personal information.

The PPIP Act gives effect to these protections through 12 principles, while the HRIP Act has three additional principles dealing with the use of identification numbers and data linkage.

Information and Privacy Commission

The NSW Information and Privacy Commission (IPC) has responsibility for administering the PPIP Act, including by:

- providing assistance to public sector agencies in adopting and complying with the information protection principles
- publishing guidelines relating to the protection of personal information
- conducting education programs promoting the protection of the privacy of individuals
- receiving, investigating, and conciliating complaints about privacy.

Data breach notification

Unlike the Commonwealth *Privacy Act 1988*, the PPIP Act does not require NSW Government agencies to notify individuals whose personal information has been compromised by a data breach.

However, in its Data Breach Guidance, the IPC suggests that agencies consider notification as good practice to assist in mitigating any damage to affected individuals and to reflect positively on an agency's reputation.

1.5 Privacy good practice

Privacy by Design

'Privacy by Design' (PbD) is a contemporary approach for promoting privacy compliance and good practice that seeks to go beyond a reliance solely on technological solutions. Instead, PbD advocates building privacy into decision-making, design and structure of information systems, business processes, products and services.

The IPC has set out the seven internationally recognised principles for PbD as:

1. Proactive not reactive, preventative not remedial
2. Privacy as a default setting
3. Privacy embedded into design
4. Full functionality: positive-sum not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user centric.

The Office of the Australian Information Commissioner (OAIC) also supports the PbD approach, arguing that it is:

> more effective and efficient to manage privacy risks proactively, rather than to retrospectively alter a product or service to address privacy issues that come to light.

Service NSW has adopted the PbD approach to its privacy management and decision making, and the seven principles above are included in its privacy management framework.

Privacy impact assessment

An important part of the PbD approach is the privacy impact assessment process. This has been defined as:

> a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

It is not mandatory for NSW Government agencies to conduct privacy impact assessments, however, the IPC encourages this as good practice.

1.6 About this audit

This audit assessed how effectively Service NSW handles personal customer and business information to ensure its privacy.

It addressed the following:

- Does Service NSW have processes and governance in place to identify and manage risks to the privacy of personal customer and business information?
- Does Service NSW have policies, processes and systems in place that support the effective handling of personal customer and business information to ensure its privacy?
- Has Service NSW effectively implemented its policies, processes and systems for managing personal customer and business information?

2. Identifying and managing privacy risk

2.1 Identifying and monitoring privacy risk

Privacy is identified as a category of risk in Service NSW's Risk Management Guideline

Service NSW's approach to risk management is framed by its Risk Management Guideline of July 2019. This document sets out an overall enterprise risk profile comprised of strategic risks that are owned and managed by the Executive Leadership Team (ELT) and operational risks that are owned and managed by senior leaders within each business unit with oversight from the ELT. In addition, project risks are identified and managed on project risk registers, maintained by the Project Managers with oversight from the Project Director and relevant ELT member.

The Risk Management Guideline also explains that Service NSW's risk management activities incorporate risk assessments and registers structured around key functions. One of these functions is 'privacy and compliance', which aims to identify and manage risks:

> related to data and information governance and management, personal information of citizens and non-compliance with legislative, contractual and government policy obligations.

Service NSW also has a risk appetite statement (dated July 2019), which defines a zero-level appetite for risks relating to privacy. The statement provides examples of ten privacy-related outcomes that should be avoided, including:

- privacy breaches and privacy complaints from customers
- wilful or accidental misuse of personally identifying information by Service NSW staff
- poor product or program design that fails to consider consent or personal data protection requirements and which places personal information or public trust at risk
- loss of customer trust in government services as a result of poor personal information management.

Service NSW's overall risk profile has been assessed internally as high and it has been determined that it needs improvement to align with the agency's risk appetite. This means that the current level of risk for Service NSW is higher than what the agency thinks is appropriate.

Service NSW's enterprise risk register identifies key privacy risks but the effectiveness of controls to mitigate these risks has been assessed as requiring improvement

The enterprise risk register for Service NSW is maintained by DCS. This register currently contains two privacy risks:

- unauthorised access, exposure of or release of personal information
- confidentiality, integrity and availability of our digital systems and products is compromised by cyber incidents.

In addition, two risks directly related to privacy are identified:

- fraudulent entitlements issued to customers — including through the potential misuse of valuable identity information and other data accessible by Service NSW
- information management or handling practices do not support lean agile rapid product and program delivery — including where caused by poor product or program design that fails to consider consent or personal data protection requirements and which places personal information or public trust at risk.

The enterprise risk register includes an assessment of the adequacy of the controls for these risks. In each case, the effectiveness of controls is assessed as 'needs improvement'. According to Service NSW's own definition, this means that there are adequate controls in some areas, however, there are also significant control weaknesses in a number of areas. Service NSW's Risk Management Guideline states that to be fully effective, controls should be 'well designed for the risk, are largely preventative and address the root causes'.

In addition to the enterprise risk register, business units within Service NSW also maintain operational risk registers, a practice that is consistent with the Risk Management Guideline.

The Executive Leadership Team's monitoring and review of privacy risks is inadequate

We were told that risks identified in the Enterprise Risk Register are discussed fortnightly by the ELT at the 'Cybersecurity, Audit and Risk' meeting. We were provided with papers for some of these meetings, though no minutes or other records were available. This creates uncertainty regarding what is discussed at these meetings, whether any formal decisions are made, or actions agreed, at these meetings.

The Service NSW Risk Management Guideline sets out an important role for the ELT, with key responsibilities including:

- monitoring and reviewing risks and compliance obligations for completeness, continued relevance and effectiveness of controls and risk treatment plans
- ensuring appropriate monitoring of performance and reporting on risk, compliance and business continuity
- providing adequate risk and compliance resourcing to manage and maintain a stable work environment including funding for risk mitigation activities (where appropriate) and budgeting provisions for resourcing.

The ELT has previously participated in an annual risk workshop led by the Service NSW Chief Executive Officer and attended by senior leaders and subject matter experts from across the agency and the Department of Customer Service. The last workshop was held in September 2019.

While there is some evidence that the ELT monitors and reviews privacy risk, it is inadequate when measured against the responsibilities described in the Risk Management Guideline, particularly regarding the effectiveness of controls.

At the time of the audit, Service NSW's governance, risk and privacy function was being provided by DCS

Following centralisation of Service NSW's corporate support functions into DCS in late 2019, Service NSW's Governance and Risk team were moved to DCS. This team, among other things, provided Service NSW with risk, privacy, as well as compliance advice and support, including managing internal reviews (complaints). These functions were transitioned to DCS.

As a result, at the time of this audit and at the time of the breach, Service NSW received these services from DCS and did not have an internal team providing this function.

Service NSW and DCS have since recognised that Service NSW needs a governance, risk and compliance team dedicated to providing operational support within Service NSW and reporting to its Chief Executive. This team is expected to include Service NSW Privacy Officer and Risk Officer roles. Service NSW and DCS advised that they have committed to implementing a risk operating model for Service NSW by the first half of 2021.

Service NSW's privacy management plan understates the full nature and extent of the personal customer information that Service NSW holds

Under section 33 of the PPIP Act, every agency must prepare and implement a privacy management plan. Service NSW's privacy management plan states that, except for its Salesforce CRM system, all other systems available to agency staff and holding customer personal information are managed by its client agencies. The plan also states that Service NSW 'holds no personal information in its own systems, but accesses and performs customer transactions directly in the client agency's information systems'.

Part B of Service NSW's privacy management plan purports to set out an 'inventory of significant information systems' and states that its Salesforce CRM system is the main information source for customers' personal information. This understates the extent of operationally vital personal information managed by Service NSW, as well as ignoring other systems where customer information is stored, including in its email system and on shared drives.

Service NSW has identified a large number of NSW residents affected by the cyber attack. Their personal information was held in the email accounts of staff that were affected by the cyber-attack and did not involve information held in the agency's Salesforce CRM system. This demonstrates that the privacy management plan is inaccurate in stating that personal information is not held on Service NSW's other systems.

2.2 Mitigating privacy risks

Service NSW has processes and governance in place to monitor and manage risks but these did not mitigate the key risks that led to the data breach

While Service NSW has processes and governance in place to monitor and report on the management of privacy risks (see above), these were not able to prevent the data breach that occurred in March 2020. Business processes around the emailing of personal information had been identified as a risk at least going back to February 2019 and strategies had been put in place to mitigate this, including a requirement for staff to manually delete emails containing personal information.

However, these processes were not always being followed and so personal information was still held in the staff email accounts that were breached in March 2020. Other contributing factors related to the breach, including the cyber security awareness of staff and the lack of multi-factor authentication on its webmail system, had also been identified as risks prior to the breach occurring but had not been effectively mitigated.

Service NSW advised that from June–October 2020, it implemented an email management initiative to mitigate the risk of similar, future breaches. It advised that this involves automatically archiving emails likely to contain personal information after a specific number of days has passed in order to limit the amount of personal information stored in email accounts.

Operational risks to customer's personal information are not effectively mitigated and business processes that contributed to the recent data breach are continuing

While processes are in place to identify and record risks, the controls in place to mitigate risk need improvement. This is especially the case for controls that seek to mitigate risks of human error by adding additional human interventions, such as:

- manually double-deleting emails with scanned attachments — from both the 'sent' and 'deleted' folders — without any assurance that this is being done
- manually deleting from service centre shared drives, the saved scanned copies of personal identification documents relating to the Registry of Births, Deaths and Marriages (BDM).

Service NSW staff have access to systems containing personal customer and business information. Effective controls are needed to reduce the risk of unauthorised access. Under the PPIP Act, agencies have an obligation to ensure that personal information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse.

Staff in contact centres consistently described a number of controls in place that aim to mitigate the risk of staff accessing information without proper authority. These include:

- role-based access to client agency systems, subject to the completion of mandatory technical training, some of which includes a reminder on the importance of using the system appropriately and the consequences of misuse
- an onscreen reminder when logging on to DRIVES, which states that unauthorised access to DRIVES is prohibited and may breach privacy law, and requires the staff member to agree to certain conditions, including that misuse may lead to termination and civil action
- managers 'walking the floor' to monitor staff conduct, though this is neither a formal practice nor consistently done across centres
- the potential deterrent effect of audit logging by TfNSW, though it was noted that this information is not routinely available to Service NSW and has to be specifically requested from the client agency, and is not available for other systems
- storing papers in locked draws during workhours and in either locked cabinets or secure storerooms outside of workhours.

Overall, much reliance is placed on the value of training, threat of detection, and the occasional physical monitoring by management to set behavioural norms for using client agency systems.

Once trained in how to conduct transactions on client agency systems, staff are provided with access logins. There are no further technical restrictions on a staff member accessing customer information without authority. There is also no way for Service NSW to routinely monitor access. We were told of examples of unauthorised access to customer information, though these were only detected by methods such as another team member reporting suspicious behaviour or following a complaint from a customer who suspected that their privacy had been breached.

Good practice guidance issued by the IPC suggests that agencies should introduce privacy by design methods to their systems and processes by:

> Taking a proactive approach, anticipating risks and preventing privacy-invasive events before they occur.

Service NSW has included this principle in its own Privacy Management Framework, and it is also consistent with the agency's Risk Management Guidelines, which explains that to be fully effective, controls for risks should be 'largely preventative and address the root causes'.

Service NSW relies on client agency systems and business processes to deliver most of its services

Service NSW is bound by agreements to use client agency systems and business processes to deliver most of its services. This limits the control Service NSW has over the handling of personal information, in some cases requiring business practices that might not accord with good privacy practice. This is notwithstanding that Service NSW has its own obligations under the security principles of the PPIP Act to take reasonable steps to prevent unauthorised access to personal information.

For example, Service NSW scans and emails documents to client agencies where those agencies have not delegated transaction authority to Service NSW and where more secure forms of electronic exchange have not been agreed or implemented. This includes transactions on behalf of Fair Trading and BDM.

Service NSW has limited ability to review audit logs of how its own staff use client agency systems, a measure that could allow it to practice more active oversight of how its staff access customer personal information. In relation to DRIVES, for example, Service NSW must complete and submit a form to TfNSW requesting access to transactional information to investigate 'suspected corruption, fraud, breach of privacy or other misconduct or negligence by SNSW staff'.

Service NSW has not adequately addressed weaknesses in its implementation of general IT and security controls for its Salesforce CRM system

Internal audits carried out by Service NSW, including one completed in August 2020, have confirmed significant weaknesses in the general IT and security controls implemented by Service NSW over its Salesforce CRM system. These weaknesses include deficiencies in the management of role-based access, monitoring and audit of user access, and partitioning of program specific transaction information, as well as the absence of privacy-enhancing mechanisms for customers.

The weaknesses in the security controls increase the risk of unauthorised access to and misuse of the personal customer information held in the CRM system. Service NSW advised that it is implementing a major update of the CRM system including to address high priority issues identified in the recent security audit.

A privacy impact assessment conducted on the CRM system in 2015 recommended that the system, particularly the MyServiceNSW account function, include the ability for the customer to monitor their own account history to detect potentially inappropriate access. This assessment asserted proactive audit and monitoring to be 'one of the most fundamental privacy protections' to manage the privacy risks of the CRM system.

The same privacy impact assessment also recommended that customers be given the option to enable multi-factor authentication for when they use processes embedded in the CRM system, including MyServiceNSW. While both these recommendations appeared positively received by Service NSW, neither have been implemented.

The Service NSW CRM system is a cloud-based application that is hosted and managed by its vendor. The CRM was primarily intended to be used for recording customer service interactions in relation to transactions that Service NSW performs on behalf of other agencies, without storing the personal information collected through those transactions. Transaction information is generally stored on client agency systems.

Since its inception, Service NSW's use of its CRM system has extended to storing transaction data, particularly for services for which it has responsibility, such as the Seniors Card. It also holds basic account details for over four million MyServiceNSW account holders, including at a minimum, name, email address and phone number, and optional address details.

Among a sample of transactions examined for this audit, the CRM system also holds de-identified data (such as health, disability, and Indigenous status) about children who have received Active Kids vouchers, and program information for the Affordable IVF program. It also retains transaction information about firearms licence applications for a short period of around two or three days. Some staff interviewed for this audit were concerned that this evolution in the way the CRM system is used to store transaction information, along with the greater volume of data that is stored, has changed the risk profile from that which applied when the system was designed.

Service NSW had identified the lack of multi-factor authentication as a risk but had not implemented it prior to the breach

Under the NSW Cyber Security Policy, agencies are required to annually assess their maturity against eight strategies developed by the Australian Cyber Security Centre (ACSC) to mitigate the risk of cyber security breaches. These strategies are termed the 'Essential Eight'.

A 2018 audit of Service NSW's implementation of the 'Essential Eight' observed low levels of maturity for many of the eight strategies and identified a number of extreme and high risks requiring mitigation. Among a number of control weaknesses, the audit found that multi-factor authentication was not enabled for high-risk areas, including webmail. It was agreed that management would finalise a strategy to address weaknesses by 30 June 2019.

Service NSW advised that it has agreed a cybersecurity remediation and uplift program, which includes addressing weaknesses identified against the 'Essential Eight' strategies.

DCS' internal review of the causes of the March 2020 data breach identified the lack of multi-factor authentication for Service NSW's email system as one of the key contributing factors.

Service NSW's significant and rapid growth has exacerbated privacy risks

Service NSW has experienced significant growth in the number and diversity of transactions it provides and the number of client agencies with which it works. From 2013 to 2020, Service NSW experienced growth in:

- the number of client agencies from three to 36
- staff from 24 to 3,981
- service centres from one to 109, with a further four mobile service centres and 36 council agencies
- types of transactions and interactions from around 800 to over 1,200.

A number of interviewees raised the pace and scale of this growth as posing risks for how effectively Service NSW continues to ensure customer's personal information privacy. It was suggested that the pace of change and increasing demand for new program implementation has limited the opportunity for it, in collaboration with its client agencies, to revisit and redesign poor business practices.

Systems and processes designed according to previously existing parameters have been retained, notwithstanding that the expectations on Service NSW have increased. This includes the need to store sensitive personal information including health, disability or Indigenous status, on a system such as the agency's CRM system that was not initially intended to be used to store such information.

The challenges posed by the pace of work have been compounded by the extra-ordinary circumstances of 2020. Service NSW has had to be agile and to quickly expand (including by doubling its contact centre staffing) to deliver government services relating to both the bushfire and COVID-19 pandemic response.

For example, during 2020, Service NSW had to design and implement processes to:

- receive and administer applications for small business support grants for businesses affected by the 2019–20 bushfire emergency or COVID-19 pandemic restrictions
- receive and administer applications for export assistance to NSW businesses affected by the bushfire emergency or COVID-19 pandemic restrictions
- manage applications for NSW border entry permits for a range of different types of individuals, including critical service and agricultural workers
- working with NSW Pathology, distribute COVID-19 test results via the MyServiceNSW app
- administer the southern border small business support grant
- process applications and allocate accommodation under the NSW Government COVID-19 pandemic crisis accommodation program for international students
- for Revenue NSW, receive and process applications for land tax relief for business affected by COVID-19 pandemic restrictions.

While some interviewees reported that these pressures have affected the focus that the agency can give to project privacy risks, the ongoing pace of work may also hinder the capacity of Service NSW to devote resources to review legacy systems and processes.

Notwithstanding the bushfire and pandemic crises, the risk of short delivery timeframes creating pressure on staff had already been identified by Service NSW as an emerging risk in 2019, before either crisis emerged.

While 2019–20 has seen additional pressures placed on Service NSW, it is the nature of the agency's functional environment that it operates in a relatively fast-paced and complex environment, where it is required to respond to multiple client agencies and stakeholders. Ensuring customer privacy should be integral to Service NSW's business as usual operations.

3. Policies, processes and systems to ensure privacy

3.1 Privacy management plan

Service NSW's privacy management plan does not reflect all programs and governance changes

Section 33(2) of the PPIP Act requires agencies to develop and publish privacy management plans that address certain specified matters.

The IPC has published guidance for agencies on preparing privacy management plans. The audit found that Service NSW's privacy management plan aligned with most elements of the IPC's guidance, although it did not reflect recent governance changes and the fact that, at the time of the audit, internal review processes had been transferred to DCS.

The IPC guidance suggests that privacy management plans be updated every one to two years or after a significant new collection of personal information has commenced. The plan was last reviewed in July 2019, though the version prior is dated 2013. There have been significant new initiatives implemented by Service NSW since July 2019, including in response to the 2019–20 bushfires, and the COVID-19 pandemic. Furthermore, there are some matters that require clarification, particularly the lines of responsibility for satisfying privacy obligations between Service NSW and its client agencies, and the effects of the governance changes from July 2019.

Our audit also found that Service NSW's privacy management plan does not:

- describe any specific exemptions to the PPIP Act that it routinely relies on
- identify the types of health information that Service NSW may collect or otherwise handle
- accurately explain the process for internal reviews, nor the basis on which these are disclosed to DCS
- explain that privacy contact officer functions are provided by DCS.

Awareness of the privacy management plan is low among staff and it has not been submitted to the Privacy Commissioner

While the privacy management plan is intended to 'assist employees to understand and comply with their obligations', awareness of the plan among the staff that we interviewed was low.

Despite being required by the PPIP Act, Service NSW has not provided the plan to the Privacy Commissioner.

Service NSW's core purpose is to manage personal information. Providing personal information to Service NSW is effectively mandatory for almost all adult — and many child — residents of NSW who wish to receive NSW Government services, entitlements, or benefits. This is at a time when the NSW Privacy Commissioner has found that 95 per cent of survey respondents rated the protection of personal information as either 'very' (79 per cent) or 'quite' (16 per cent) important.

Service NSW aspires to be 'recognised as the distinctive leader in the provision of government services'. As such, it should also be a sector-leader in awareness of, and compliance with, its statutory privacy obligations.

3.2 Agreed processes and systems with client agencies

Service agreements with client agencies provide high level acknowledgement of the requirement to comply with legal obligations

Service NSW's relationships with client agencies are governed by service agreements or memoranda of understanding. A sample of agreements reviewed for this audit showed that they varied substantially in length and complexity, however they shared the following common elements:

- a mutual acknowledgement that both parties are bound by applicable privacy law
- a general and high-level commitment to afford security standards to any personal information that is 'consistent with and no less rigorous than those maintained by either party to secure its own data'
- in the event of a data breach, a general obligation to notify the other party and take unspecified steps to avoid further breach.

There is a lack of clarity regarding responsibility for privacy compliance between Service NSW and its client agencies

Service NSW's privacy management plan states:

> Service NSW is somewhat unusual in that the majority of the customer personal information it handles will be for the purpose of fulfilling a transaction on behalf of another government agency or organisation (our 'client agencies'), and compliance with the privacy principles will primarily be the responsibility of that agency.

The privacy management plan cites functions performed by Service NSW on behalf of TfNSW and BDM as among those for which privacy responsibility lies with the client agencies. However, Service NSW collects and stores personal information relating to transactions for these agencies.

This issue is further confused by the explanation of 'holding personal information' on page five of the plan:

> Most of our privacy obligations apply to personal information that we 'hold'. Service NSW will be considered to be 'holding' personal information if it is in our possession or control. 'Control' can include the ability to view or edit information by virtue of our access to client agencies' information systems.

Service NSW staff perform the majority of client agency functions using the systems of those client agencies — for example, DRIVES, LifeLink, and GLS (a system used for a range of transactions, including Fair Trading). The explanation above seems to accept that simply viewing personal information on these systems constitutes 'control' of personal information, in turn invoking privacy obligations for Service NSW as the 'holder' of personal information.

This issue is further complicated by the many different types of relationships and arrangements that Service NSW has with its client agencies. The lines of responsibility for meeting privacy obligations will likely vary between each client agency and the design of each transaction process. It may not be appropriate to attempt to describe each of the client agreements — and how responsibility for privacy obligations varies — in a general document like the privacy management plan. These matters are better clarified in the individual service agreements that exist between Service NSW and its client agencies.

There are privacy gaps in the agreements between Service NSW and client agencies

The lack of clarity in privacy responsibilities in agreements between Service NSW and its client agencies poses two risks. First, that necessary obligations will fall 'between the cracks' of the two agencies, with each assuming the other responsible for meeting an obligation. Second, that it creates uncertainty for individuals about which agency is responsible for their personal information and which agency is accountable should a breach occur — even knowing to which agency the individual should complain.

We reviewed a sample of six agreements, which covered a large proportion of the total volume of Service NSW's transactions. We also took into account the overarching standard terms of engagement that sit over project and service agreements. Of the six agreements we reviewed:

- none clarified the role of Service NSW in ensuring that individuals are provided with a privacy collection notice, including which agency would provide the notice, the content of the notice, or when in the collection process the notice would be provided to the customer
- only two provided any specific information about measures that would be taken to ensure personal information would be kept secure
- none specified the period for which Service NSW would retain data, except for the general obligation that it would be held in accordance with the *State Records Act 1998* and any privacy laws
- none described any principles that might apply in determining whether an application for internal review from a customer would be referred to the other agency, nor did any explain what role the customer would play in this process, including whether their consent would be sought
- none provided any detailed information on data breach response, beyond generally notifying the other party.

Agreements with client agencies do not ensure that privacy collection notices are compliant

Section 10 of the PPIP Act requires agencies to take reasonable steps when collecting personal information to ensure the individual is aware of:

- the purpose for which their personal information is being collected
- the intended recipients to whom the information may be disclosed
- whether the collection is required by law or voluntary
- the existence of any right of access to, and correction of, the information
- the name and address of the agency that is collecting the information and the agency that is to hold the information.

While not mandated by law, the IPC also suggests that an individual should be given notice about how their personal information is stored and for how long, as well as how security will be ensured.

These matters are addressed in a 'privacy collection notice' provided to the individual when their personal information is collected.

The privacy collection notice reflects a crucial point in the information handling lifecycle, by providing the individual clear advice about what will happen to their personal information for that specific transaction, while also establishing parameters for how the agency may handle that personal information.

None of the privacy collection notices that we reviewed for this audit complied with all the criteria established by law or good practice. The closest to full compliance was the privacy notice for the pre-IVF Fertility Testing Rebate — the only criteria it failed to satisfy was Service NSW's own commitment to include privacy notices at the start of the transaction.

3.3 Review of systems and processes to ensure privacy

Service NSW considers the privacy implications of new systems and programs but does not routinely review existing systems and processes

Service NSW was able to provide evidence of having conducted privacy impact assessments for major new projects that involved the handling of personal information. Service NSW has developed a project management framework and tools that demonstrate an organisational commitment to conducting privacy impact assessments, where appropriate. This framework includes:

- defining when the project sponsor should conduct a privacy impact assessment
- requiring a project sponsor to check that a privacy impact assessment has been completed, recommendations addressed and endorsed by the project steering committee
- requiring the project steering committee to confirm that a privacy impact assessment has been conducted, recommendations and responses have been endorsed and any mitigations implemented before the project can proceed.

In addition, Service NSW's Privacy Management Framework states that Service NSW Governance and Risk (now DCS, Governance, Risk and Performance) can assist in completing PIAs and managing privacy gaps.

Service NSW does not routinely review existing and legacy processes and systems to ensure that they are effective in ensuring the privacy of customer personal information. Business processes which create the highest risk to privacy such as emailing of personal information are more common in these longstanding legacy systems and business practices.

Service NSW carries out privacy impact assessments in line with good practice

Of the 11 internally conducted and 11 externally commissioned privacy impact assessments that we reviewed, most were compliant with IPC good practice guidance, including in regard to:

- being an integral part of agency governance and a standard organisational commitment
- being fit for purpose, taking into account the scale of privacy risk that it was responding to, including whether a proposal envisaged the handling of sensitive information or affects the privacy of a large number of individuals
- mapping the flows of information in a project
- being ongoing by allowing updating or revision according to any changes in the project
- considering the nature and size of the project in determining who conducts it and whether specialist knowledge or skills are required.

The audit identified a number of areas where there is scope to better meet the IPC good practice guidelines for conducting privacy impact assessments by:

- engaging early with the people and organisations with an interest in the project, or who will be affected by the project
- ensuring that privacy impact assessments consistently include recommendations that include an action plan and timeline
- ensuring that the privacy impact assessment report sets out all the information gathered throughout the process, including the results of stakeholder consultation, any privacy risks that cannot be mitigated and an assessment of why those risks outweigh the public benefit delivered by the project.

Service NSW does not publish privacy impact assessments even though the IPC states that this is good practice and a number of Service NSW’s own privacy impact assessments have recommended publication. Where an assessment includes confidential material, a redacted or summary version can be an appropriate alternative.

Service NSW has a mechanism to seek staff input to continuous improvement

All staff are able to access an intranet portal called the 'Circle of Service', which allows staff to submit suggestions for improvement or changes, report risks, or raise concerns about any matter across Service NSW. Staff interviewed for this audit reported that the Circle of Service was effective in encouraging submissions, including because all submissions are given due consideration, feedback is published, and there are examples where changes have been implemented.

Of the 1,763 suggestions related to customer service functions made in 2019–20:

- 847 were fully or partially implemented — 37 related directly to the handling of customers' personal information, with the most common being a recommendation to improve customer guidance on proof of identity requirements for Working with Children Checks
- 916 were not accepted — 11 were declined expressly due to concerns about privacy, while another eight cited unacceptable information security risks posed by the proposals.

While the Circle of Service cannot be considered a regular formal review, it is a mechanism to encourage staff to reflect on how Service NSW conducts its business and make proposals to improve the handling of customers' personal information.

4. Privacy training, awareness and compliance

4.1 Staff training and awareness of privacy

Service NSW staff undertake privacy training

Service NSW staff undertake training that is designed to meet the needs of individual roles. There are four forms of training, including:

- Mandatory cluster-wide training for all staff in the DCS cluster — this training includes an information security module, as well as training on the Code of Conduct and Ethics.
- Service NSW induction training, delivered by DCS, that includes an online privacy module — in this training, staff are also required to read the Service NSW privacy management plan (though they are not assessed on whether they have done this).
- Advanced privacy training, such as privacy by design, that is delivered to a smaller cohort of staff, particularly those involved in project design and delivery.
- Training on client agency systems and applications, which can include privacy related matters relevant to specific transactions and is provided according to the needs of individual roles (discussed further below).

At the end of September 2020, completion rates for the mandatory privacy and information security training were 88.2 per cent and 86.7 per cent, respectively.

As noted in Section 3.1 of this report, we found low levels of awareness among staff of the privacy management plan, suggesting that this could be afforded greater prominence in the training.

Some staff receive privacy training as part of learning client transactions as well as other ad hoc privacy training and awareness raising activities

Service NSW staff receive technical training as required for their role focused on specific client agency transactions. This training is provided to staff once and must be completed before staff can conduct these specific transactions. Following the technical training, on the job training and mentoring is relied on to establish and maintain competency.

For both service and contact centre staff, curriculum documentation for technical training show that privacy is addressed for key client agencies. For example:

- Stage one of DRIVES training for service centre staff includes the facilitator sharing ‘case studies from the ICAC website to bring the content to life’.
- BDM Lifelink training for contact centre staff includes the facilitator taking ‘learners through a formal confidentiality agreement and discusses the risks associated with transactions’.
- GLS training for Fair Trading transactions for service centre staff includes a ‘deep dive into proof of identity requirements and security risks’.

Service NSW makes a detailed Critical Documents Guide available to Customer Service Representatives, Centre Concierges, and Centre Managers. This guide has the dual stated aims of ensuring understanding of responsibilities while using DRIVES, as well as an understanding of the PPIP Act.

Service NSW also provided Privacy by Design training to some staff in project and system design roles. Training records show that at least 80 staff attended externally facilitated Privacy by Design training through 2019 and 2020. Participants rated this training highly in their feedback.

In addition to training, Service NSW conducts a number of other activities to promote privacy awareness. For example, Service NSW promoted Privacy Awareness week 2020 to staff using webinars, videos, articles and memes via social media, email and Intranet channels. Staff we interviewed also reported that awareness is promoted informally in staff meetings.

Following governance changes in July 2019, there were no privacy awareness or education activities coordinated through DCS in the September quarter of 2019, and only limited activities in the December quarter.

Service NSW has not assessed the privacy awareness of its staff in line with its privacy management framework

The Service NSW privacy management framework (October 2019), an accompanying document to the privacy management plan, states that Service NSW will assess privacy knowledge and awareness annually by a privacy awareness survey. The survey is intended to 'evaluate privacy training effectiveness and privacy maturity,' however the first survey has not yet been run. An internal assessment of staff privacy awareness reported in May 2019 concluded that:

> the maturity of privacy risk in Service NSW is very low, as many staff are not familiar with the legislated privacy principles.

Despite this, we found that Service NSW service centre staff and managers interviewed as part of this audit were able to identify a range of scenarios that they assessed as posing risks to privacy (see Exhibit 1).

Exhibit 1: Operational risks identified during contact centre staff interviews

1. The risks of using email to send scanned documents, especially where there is no read-receipt from the recipient.
2. The specific risks around complex transactions, like overseas licence applications.
3. The risk of using unregistered Australia Post mail to send original hardcopy identity documents.
4. The risk of photocopying or scanning proof of identity documents, rather than certifying them as sighted.
5. The risk posed from not promptly removing system access when staff leave or change roles.
6. In some centres, the risks of physical layouts that do not provide for sufficient privacy during conservations with customers.
7. The risk of retaining scanned documents for extended periods on local systems.
8. The risk of using unsecured courier bags in certain situations.
9. The risk posed by inconsistent POI requirements, and the ensuing complexity and confusion that result, across the sector.

Source: Interviews conducted with Service NSW service centre staff from 10–28 August 2020.

4.2 Reviewing compliance and performance

Staff are subject to quality assurance processes however these have a limited focus on privacy

Service NSW has a Quality Control Framework that aims to increase focus on operational compliance. In service centres, the Quality Control Framework has three components: work-checking, health checks, and quarterly quality attestation by managers that policies have been complied with.

According to the Framework, the work-checking process involves a sample of the previous day's transactions being checked every day, including all high-risk transactions and all transactions for new staff. The intention of the framework is that every Customer Service Representative will have the equivalent of a full day's work checked every quarter. Any errors are discussed with the work-checker, and systemic poor quality can be escalated to a performance issue.

Work-checking has a focus on the accuracy of transactions, including whether personal information is accurately collected. Done effectively, this would help Service NSW to comply with section 18 of the PPIP Act, which requires agencies to take such steps as are reasonable in the circumstances to ensure that personal information is accurate.

In contact centres, the quality framework sets out that staff will have between four and 12 calls reviewed per month by call reviewers and their managers, though this may vary depending on availability and workloads of team leaders and customer experience analysts. However, as each staff member may, on average, take around 70 calls per day, it is a relatively small proportion that is assessed.

The second component of the framework is to conduct 'Health Checks' against three predetermined key responsibility areas: people, customer, and organisation. Customer privacy is one of the 32 specific focus areas that sit under these key responsibility areas.

There are two forms of Health Checks: informal self-assessments of centres and independent assessment conducted by the Service NSW Operational Governance team. Staff reported during interviews that informal self-assessments are done differently in different centres and regions. In some centres, staff do Health Checks on their own centre, or alternatively staff from neighbouring centres or even regions can conduct the assessment. These self-assessed Health Checks are usually done every six months. Independent Health Checks are done by Operational Governance, which aims to do between 50 and 100 each year.

The final component of the Quality Control Framework is managerial quarterly assurance which requires that every centre manager must submit a quarterly quality assurance certification, including certifying that they have ‘managed the delivery of all transactional services in accordance with agencies, and Service NSW policies and procedures’. In addition to certifying compliance with policies and procedures, managers must certify that work-checking has been done in accordance with the framework.

4.3 Achieving compliance with privacy obligations

Not all privacy processes are being followed consistently including processes that contributed to the data breach

Under the Health Check process, service centres are assessed against the following privacy-related criteria:

- personal information secured at all times
- screens locked when left unattended
- storeroom is secured at end of shift
- paperwork not necessary is stored
- scanned documents and emails are reviewed and not retained for longer than six months (and emails containing scanned documents are deleted daily).

This audit reviewed all 24 Health Checks carried out by Operational Governance between April 2019 and July 2020 and found that:

- ten of the 24 assessments found non-compliance with the requirement that service centre G-drives be purged of any customer documents stored for longer than six months — these documents include proof of identity related documents and other scanned personal customer information
- four of the five assessments carried out since the cyber breach in March 2020 found non-compliance with the requirement to purge emails containing personal customer information on the day of sending.

Notably, at least one Health Check undertaken prior to March 2020 reported breaches of the requirement to delete emails containing personal information on the same day as they were sent. Had this risk control been effectively implemented more broadly, it would likely have mitigated the quantity of personal information affected by the March 2020 cyber breach.

Executives have not self-assessed their business area's privacy compliance

Service NSW's privacy management framework sets out that executive staff will complete an annual privacy compliance self-assessment and attestation. This attestation is intended to assist the agency in discharging responsibilities under TPP15-03 Internal Audit and Risk Management Policy for the NSW Public Sector. The attestations require executives to confirm that:

- the executive's area has adopted the privacy framework and is committed to compliance
- that key controls mitigating privacy risks have been implemented, monitored and tested periodically
- that all privacy matters that have occurred in their area (that they are aware of) have been reported and are being managed.

Service NSW is not complying with its own framework, as no evidence was provided that these self-assessments have been completed.

There have been relatively few complaints and breaches

For the period from 1 July 2019 to 14 July 2020, Service NSW received 31 privacy complaints, of which 15 were determined to constitute breaches. Most of these complaints related to Service NSW disclosing information in error. This included customers receiving emails and mail not intended for them and photo cards being sent to the incorrect address. This was a substantial increase on the numbers of complaints received for 2018–19 (four), 2017–18 (six) and 2016–17 (four).

For 2019–20, DCS identified 16 formal privacy breaches (as opposed to complaints), which appears relatively low compared to the number of transactions processed and personal information handled, though still beyond Service NSW's risk appetite of zero. It is also important to note that Service NSW is not able to routinely monitor staff activity within other agency systems (e.g. DRIVES and LifeLink) and is not routinely monitoring staff activity in the CRM system, which increases the risk that Service NSW is not identifying all privacy breaches.

From 1 July 2017 to 30 June 2020, there were 48 code of conduct and ethics breaches found against Service NSW staff. Five of these related to breaches of customer privacy, and all of these resulted in the termination of the staff member's employment. Of the remaining 43 breaches, only seven resulted in termination.

Regional and centre managers reported that there is no guidance provided on how to assess the relative materiality of different types of privacy breach and that this may result in the inconsistent handling, reporting and escalation of breaches across Service NSW's locations. In contrast, the Call Quality Framework for contact centres includes a formal 'calibration' process to ensure that call reviewers are consistent in their assessments.

Section two

Appendices

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.

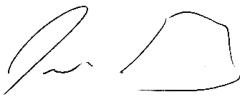
Service NSW is working in partnership with the Department of Customer Service who is leading further cluster-wide improvements in cybersecurity, privacy, information security and governance through its "Project Trust". The significance and the scale of improvements in the pipeline demonstrate how seriously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

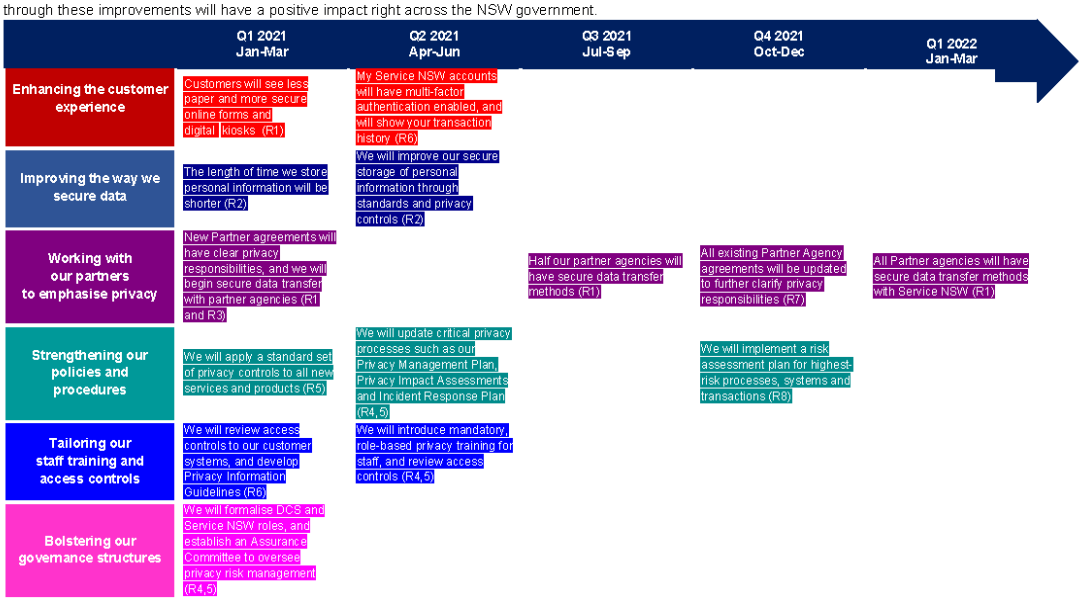
Since the cyber-attack and data breach, Service NSW has completed several interim privacy management improvements and commenced an organisation-wide program of enduring changes and improvements to the way we manage personal information.

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

Appendix two – About the audit

Audit objective

This audit assessed how effectively Service NSW handles personal customer and business information to ensure its privacy.

Audit criteria

We addressed the audit objective with the following audit criteria:

1. Does Service NSW have processes and governance in place to identify and manage risks to the privacy of personal customer and business information?
2. Does Service NSW have policies, processes and systems in place that support the effective handling of personal customer and business information to ensure its privacy?
3. Has Service NSW effectively implemented its policies, processes and systems for managing personal customer and business information?

Audit scope and focus

In assessing the criteria, we checked the following aspects:

1. Does Service NSW have processes and governance in place to identify and manage risks to the privacy of personal customer and business information?

a) Service NSW has a comprehensive inventory of the personal information it holds (including sensitive and high-risk information), where the information is stored and who is responsible for it.

b) Service NSW has identified risks to the personal information it holds, including risks associated with unauthorised access and has designed mitigations for these risks.

c) Service NSW has governance structures in place that monitor and report on the management of these risks.

2. Does Service NSW have policies, processes and systems in place that support the effective handling of personal customer and business information to ensure its privacy?

a) Service NSW has a privacy management plan in place that complies with the relevant legislation and guidance.

b) Service NSW has processes in place with other government agencies to ensure the privacy of information.

c) Service NSW regularly reviews existing processes and systems and designs processes and systems for new programs to ensure their effectiveness and efficiency in maintaining the privacy of personal information.

3. Has Service NSW effectively implemented its policies, processes and systems for managing personal customer and business information?

a) Service NSW conducts awareness raising activities, including training, covering policies, processes and systems relating to the privacy of personal customer and business information.

b) Service NSW staff are handling personal information in line with the relevant policies and processes.

c) Service NSW undertakes regular reviews or audits of staff and third-party compliance with relevant policies and processes, and there is prompt action to investigate and report on potential non-compliances.

This audit focused on:

- storage and handling of personal customer and business information as it relates to the privacy of that information
- effectiveness of policies, processes and systems to ensure the privacy of personal information
- effectiveness of arrangements with other agencies to ensure the privacy of personal information
- electronic and physical personal information
- compliance with privacy legislation.

Audit exclusions

The audit did not question the merits of government policy objectives.

Audit approach

Our procedures included:

1. interviewing Service NSW staff including:
   - senior staff responsible for service delivery
   - staff with responsibility for privacy management, including the Privacy Contact Officer
   - internal audit staff
   - risk management staff
   - a selection of Service Centre and Contact Centre staff
2. consultation with other stakeholders including the Department of Customer Service, Service NSW client agencies and the Information and Privacy Commission
3. examining documentation.

The audit approach was complemented by quality assurance processes within the Audit Office to ensure compliance with professional standards.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit 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 *Public Finance and Audit Act 1983* and the *Local Government Act 1993*.

Acknowledgements

We gratefully acknowledge the co-operation and assistance provided by staff at Service NSW and Department of Customer Service.

Audit cost

The estimated cost of this audit, including staff costs and overheads, was approximately $330,000.

Professional people with purpose

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)

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

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

PHONE +61 2 9275 7100
FAX +61 2 9275 7200

mail@audit.nsw.gov.au

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

audit.nsw.gov.au