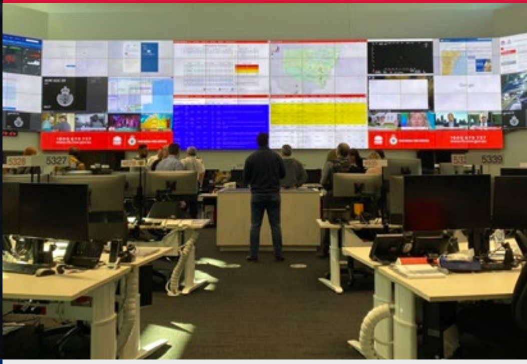
Cyber Security NSW

2026–2028 NSW Government Cyber Security Strategy



Document number: 1

Version number: 0.1

1

Minister's Foreword

Trust is at the heart of every interaction between government and the communities we serve. As our services become increasingly digital, it is essential that people feel confident that their data is secure, their privacy respected, and their experience valued.

The 2026–2028 NSW Government Cyber Security Strategy reflects our commitment to building a secure and inclusive digital future, one that puts people first and ensures that digital transformation is always driven by purpose.

Cyber threats are evolving rapidly, and the responsibility to protect our systems, services and data is shared across government. This strategy provides a clear direction for how we can work together to embed security from the outset, respond swiftly to incidents, and foster a culture of cyber awareness across all agencies.

Cyber Security NSW leads this work in partnership with agencies across the state. But it is through the collective efforts of every department and every team that we will earn and maintain the trust of our communities.

By embracing this strategy, we are not only protecting the services we deliver – we are reinforcing the public's confidence in government and demonstrating the value of secure, ethical, and inclusive digital services.

Together, we can ensure NSW remains a place where innovation is matched by integrity, and where every person can engage with government in a safe and trusted digital environment.

The Hon Jihad Dib MP

Minister for Customer Service and Digital Government

Minister for Emergency Services

Minister for Youth Justice

Member for Bankstown

NSW Chief Cyber Security Officer's Foreword

Marie Patane
NSW Chief Cyber Security Officer
Cyber Security NSW

Cyber security is a core operational requirement for government, underpinning the confidentiality, integrity and availability of the digital services the people of NSW rely on every day.

As the NSW Chief Cyber Security Officer, I lead a coordinated, risk-based approach to protecting government systems, information and critical services in an increasingly complex threat environment.

This strategy provides a clear and practical roadmap for strengthening cyber resilience across the NSW public sector. It recognises that cyber security is not solely a technical challenge, but a leadership and organisational responsibility that requires strong governance, informed decision-making and consistent, shared standards across government.

Through this strategy, Cyber Security NSW will continue to provide strategic leadership, all-of-government coordination and targeted guidance to support agencies in prioritising investment where risk is greatest. We will further strengthen our incident response, intelligence and recovery capabilities, while expanding our focus on identity resilience and the protection of digital services used by the community.

Cyber security is a shared responsibility. By working collectively, we can safeguard public trust, protect essential services and ensure NSW remains secure, resilient and prepared for the future.

Executive summary

Cyber threats are escalating in speed, sophistication and scale, driven by advanced adversaries and a growing attack surface. Generative artificial intelligence (AI) is amplifying phishing, social engineering and malware creation, while the commoditisation of cybercrime makes these tools widely accessible. These trends expose vulnerabilities across digital and physical infrastructure and pose risks to data, service continuity and public trust.

Cyber security is foundational to a trusted digital society. It enables secure digital transformation, protects essential services and builds public confidence. The NSW Government is committed to strengthening cyber and privacy resilience across all departments and agencies to reduce the impact of cyber incidents across our systems, services, and most importantly, our communities. By embedding cyber security into the core of digital initiatives, NSW aims to underpin public trust, minimise disruption and safeguard the state's digital future.

This strategy builds on the foundations of the 2021 strategy, which supported the State in responding to over 500 cyber threat notifications across government and training more than 190,000 employees in cyber awareness. In February 2023, the NSW Government put in place an updated NSW Cyber Security Policy, supported by new best practice guidance and a standardised assurance approach. It also reflects a renewed focus not just on cyber resilience but also protecting and educating communities about how to prevent and recover from cyber or identity related incidents. The NSW Government is also leading the way with innovative pilots like the Digital Photo Card pilot in the NSW Digital Wallet – demonstrating the state's leadership in secure, community-focused digital identity.

The 2026–2028 NSW Government Cyber Security Strategy will reinforce all-of-government coordination to protect against key risks, with a strengthened focus on securing critical infrastructure and third-party supply chains.

Under this strategy, Cyber Security NSW will take a proactive leadership role in strengthening cyber risk management across NSW Government. Cyber Security NSW will continue to work closely with agencies to improve the consistency and transparency of compliance reporting, ensuring greater accountability and assurance.

> By leveraging these insights, Cyber Security NSW will enable intelligence-led and data-driven decision-making that not only enhances cyber resilience but also informs strategic investment prioritisation.

The strategy includes five strategic objectives to underpin a resilient public sector cyber security posture that is capable of protecting the NSW Government and NSW communities, supporting the growth of public digital services and navigating and mitigating the threats of the complex cyber security landscape. This Strategy supports the NSW Digital Strategy by strengthening the security and resilience of the digital systems that people and services rely on, ultimately helping to make NSW a safer, fairer, easier and more productive place to live and work.

Our objectives

Objective 1

Strengthen risk management, governance and compliance.

Objective 2

Improve incident response and cyber intelligence capability.

Objective 3

Uplift cyber resilience.

Objective 4

Drive continuous development of cyber security tools, processes and methodology.

Objective 5

Support NSW communities to be cyber safe.

Given the ever-changing nature of the cyber threat landscape, robust cyber security cannot be achieved with a one-off project. The NSW Government is committed to continuous progress, driven by forward-looking strategies, and sustained through dedicated effort and investment.

3

Purpose

The 2026–2028 NSW Government Cyber Security Strategy sets a focused two-year agenda to strengthen cyber resilience across the NSW public sector. It aims to uplift capability, reinforce leadership in managing and mitigating cyber risks, and ensure that the services we deliver, and the data entrusted to us, remains secure, trusted and valuable to the communities we serve.

This Strategy guides NSW Government departments, public service agencies and statutory authorities. It does not formally extend to state-owned corporations, non-government organisations, local government or universities.

Through strengthened governance, improved effectiveness of cyber investments, and a commitment to secure-by-design principles, the Strategy keeps community benefit at the heart of all cyber security efforts.

It provides a framework for agencies to guide investment, capability development, coordinated action and accountability – ensuring the secure and reliable delivery of government services.

The Strategy is underpinned by three overarching goals:

01 **a connected NSW, enabled by secure digital systems and supported by strong cyber security capability to create a digitally confident public sector**

02 **a protected NSW, safeguarded by coordinated plans, processes and networks that defend against evolving cyber threats**

03 **a trusted NSW, where communities have confidence in the security and privacy of the digital services they rely on.**

By aligning with national and global best practices, fostering collaboration across government, and building public trust in NSW Government digital systems, this Strategy supports a secure, resilient and purpose-driven digital future for NSW.

3.1 Alignment to other strategies

The 2026–2028 NSW Government Cyber Security Strategy aligns with the NSW Digital Strategy to ensure NSW is maintaining a consistent approach to digital and cyber security issues. It also aligns with relevant pillars from the 2023-2030 Australian Cyber Security Strategy strategic outcomes and initiatives. The NSW Government is committed to supporting the implementation of the Australian Government Cyber Security Strategy. Other relevant NSW strategies have also been considered, including the NSW Data Strategy and the NSW State Infrastructure Strategy.

3.1.1 NSW Digital Strategy

The NSW Digital Strategy reflects the state's public sector priorities to harness the power of digital to make it easier for people to engage and transact with government.

The NSW Digital Strategy is underpinned by five missions for digital transformation across the NSW Government, each dedicated to delivering accessible, inclusive, secure and integrated digital services that every person in NSW can access and benefit from.

Mission 1: Make digital services accessible, inclusive and connected for everyone in NSW.

Mission 2: Use digital to improve service delivery, support the local economy and drive productivity.

Mission 3: Underpin trust in government through reliable, stable digital services and sustainable digital infrastructure.

Mission 4: Keep NSW safe and resilient during emergencies online and in-person.

Mission 5: Uplift digital capability in the public sector workforce.

NSW Digital Strategy

Delivering digital with purpose

3.1.2 2023-2030 Australian Cyber Security Strategy

This strategy outlines the roadmap to realise the Australian Government's vision of becoming a world leader in cyber security by 2030. Through the strategy's six cyber shields, the Australian Government seeks to improve its cyber security, manage cyber risks and better support citizens and Australian businesses to manage the cyber environment around them.

Each shield provides an additional layer of defence against cyber threats and places Australian citizens and businesses at its core.

01 **Strong businesses and citizens**

02 **Safe technology**

03 **World-class threat sharing and blocking**

04 **Protected critical infrastructure**

05 **Sovereign capabilities**

06 **Resilient region and global leadership**

4

Cyber Security NSW: Leading the Strategy

Cyber Security NSW plays a central role in driving the NSW Government's cyber security strategy. Our mission is to support a cyber-secure public sector that safeguards the confidentiality, integrity and availability of systems, services and data for the communities we serve.

As the lead authority on cyber security, Cyber Security NSW sets the strategic direction for agencies, providing tailored products, services and best practice guidance to departments and agencies. We lead and coordinate all-of-government cyber security strategies and responses to significant cyber incidents, crises and data breaches in partnership with operational teams from impacted agencies.

Through ID Support NSW, we provide targeted support to individuals, public sector agencies and organisations affected by data compromises, helping NSW residents and businesses build identity resilience, and recover from identity theft, data breaches or scams.

Our integrated, risk-based approach encompasses technology, people and process – supporting a holistic uplift in cyber risk management across NSW Government.

We work in close partnership with cyber security teams across NSW Government, law enforcement and national counterparts, as well as industry and academia, to address emerging threats, uplift security practices and foster innovation.

Cyber Security NSW works with agencies across government to ensure cyber security investments are informed, targeted and focused on managing the highest risks – protecting systems, data and public trust.

Cyber Security NSW's functions

- Awareness, training and resilience services
- Security assessments, remediation and uplift
- Cyber Audit readiness and quality assurance
- Incident response and emergency management
- AoG leadership and inter-jurisdictional coordination
- Best practice advice and guidance
- AoG insights and reporting to Cabinet & ERC
- Threat intelligence
- NSW Cyber Security Policy
- Investment prioritisation guidance
- ID Support NSW

Objectives

5.1 Strengthen risk management, governance and compliance

5.1.1 Goal – embed mature, resilient and consistent cyber governance and risk practices

What success looks like:

- NSW Government agencies operate with greater confidence and consistency in managing cyber risks.
- Supported by Cyber Security NSW's strategic leadership and strengthened governance and assurance, agencies have clearly defined roles and decision-making pathways to enable faster, more coordinated responses to incidents.
- Operational Technology (OT), Internet of Things (IoT), and critical infrastructure is secured through consistent, risk-based practices aligned with all-of-government standards. Third-party and supply chain risks are proactively managed through improved coordination and shared threat intelligence.
- Compliance with the NSW Cyber Security Policy is robust and transparent, enabling insights that support continuous improvement and informed investment.
- Agencies actively embed the NSW Artificial Intelligence Ethics Policy and comply with the AI Assurance Framework to manage AI safely and adapt to emerging risks in a dynamic digital environment.

5.1.2 How we achieve success

Strong risk management and governance are essential to effective cyber security. They establish clear expectations, promote consistent practices, and enable NSW Government agencies to prepare for and respond to emerging threats with confidence. To achieve this outcome, NSW Government agencies will:

✓ **strengthen governance by clearly defining roles and responsibilities for cyber security across government to support accountability and coordinated incident response**

✓ **enhance assurance under the NSW Cyber Security Policy, increasing the depth of analysis, identifying systemic risk and supporting targeted remediation**

✓ **improve OT and IoT risk management to protect critical government infrastructure, systems and community-facing services**

✓ **strengthen protections and coordination across government to manage cyber supply chain risk and safeguard essential assets and services.**

5.1.3 Work in progress – building foundational capability in cyber risk management

NSW Government agencies are continuously strengthening their cyber resilience. Departments and agencies are focused on proactively identifying and mitigating potential threats before they escalate into confirmed incidents. Cyber Security NSW is driving a whole-of-government uplift in risk management, governance, and compliance to strengthen cyber resilience.

- **Mandating targeted initiatives**

  Cyber Security NSW has issued Directive DCS-2025-04 – Targeted Initiatives for NSW Government, setting clear expectations for NSW Government agencies to prioritise uplift and achieve compliance with key Mandatory Requirements under the NSW Cyber Security Policy. The directive also introduces additional reporting obligations to Cyber Security NSW.

  - **Strengthening agency responsibilities**

    All NSW Government agencies must:

    - report cyber security incidents within 24 hours
    - maintain inventories and lifecycle management plans for all critical assets
    - document and assess third-party providers to strengthen cyber supply chain risk management.

  - **Expanding leadership roles**

    The directive broadens responsibilities for Secretaries and Chief Information Security Officers (CISOs) to ensure stronger compliance, collaboration, and governance across government.

  - **New posture and asset reporting requirements**

    From 31 October 2025, agencies must assess their posture against defined whole-of-government cyber risks and submit an inventory of crown jewel assets as part of the NSW Cyber Security Policy reporting cycle.

- **Practical support for agencies**

  To enable efficient and consistent compliance, Cyber Security NSW has developed practical tools and templates to support the enhanced reporting requirements for agencies.

5.2 Improve incident response and cyber intelligence capability

5.2.1 Goal – embed an intelligence-led and coordinated cyber response

What success looks like:

- The NSW Government is working towards a more integrated and real-time understanding of the cyber threat landscape. This will enable earlier detection, faster risk minimisation, and more confident incident response.
- Information sharing between agencies, Cyber Security NSW, and the Australian Government will become more streamlined, supporting intelligence-led decisions and reducing duplication.
- Agencies will continue to report real or suspected cyber incidents, enabling Cyber Security NSW to synthesise intelligence, anticipate threats, and coordinate countermeasures that strengthen system-wide resilience and recovery.

5.2.2 How we achieve success

Effective information sharing is critical to reducing the scale, impact and recurrence of cyber attacks. To strengthen threat intelligence capabilities and enable faster, more coordinated responses, NSW Government agencies will:

✓ **ensure timely, accurate and comprehensive agency reporting to Cyber Security NSW to support all-of-government visibility and intelligence-led decision making**

✓ **build agency capability in cyber incident prevention, detection, response and recovery through strategic improvements and continuous refinement of practices**

✓ **streamline cyber intelligence products and threat detection software by reducing duplication across agencies, improving efficiency and maximising return on investment**

✓ **promptly refer or report cybercrime to the NSW Police Force to prevent, disrupt and investigate cyber enabled and dependent crime within NSW.**

5.2.3 Work in progress – strengthening our cyber response and intelligence foundations

The cyber threat landscape has continued to shift in response to global events and evolving threat actor priorities. Cyber Security NSW is advancing the state's cyber resilience through enhanced intelligence and coordinated response capabilities.

- **More frequent threat insights**

  NSW Government agencies report key threats, risks, incidents and mitigation activities to Cyber Security NSW under the NSW Cyber Security Policy. This reporting forms a critical part of the cyber security landscape, enabling Cyber Security NSW to monitor sector-wide activity, identify recurring vulnerabilities, and detect emerging trends.

  To improve timeliness, Cyber Security NSW has shifted from an annual to a tri-annual threat assessment model. This ensures agencies and executive leaders receive relevant intelligence more often, enabling faster, better-informed decisions. These insights support a more informed and coordinated approach to cyber risk management across the NSW Government.

Average cost of cybercrime for businesses rose 50% to

$80,850

with large businesses reporting an average cost of $202,700 (up 219%).

-Australian Signals Directorate Annual Cyber Threat Report 2024-2025

Page 12

- **Strengthening NSW's cyber emergency response capability**

  A major uplift of NSW's cyber emergency response arrangements is underway, including a comprehensive uplift of incident and emergency response frameworks to enable faster, more coordinated action during significant cyber events. These reforms align NSW with national arrangements and address issues identified in a recent review around processes, escalation pathways, and post-incident practices.

  Agencies will be required to implement these changes as part of their cyber security obligations. Interim measures are already in place, including a mandatory 24-hour incident reporting requirement, ensuring timely escalation and visibility across government.

  Key activities currently underway include:

  - redesigning the State Cyber Security Emergency Plan and the NSW Cyber Incident Management Arrangements
  - embedding a revised incident categorisation matrix and integrating business continuity planning into these frameworks
  - Cyber Incident and Emergency Management Group, established under the Cyber Security Steering Committee, is driving cross-government collaboration to ensure the new arrangements are coordinated, fit-for-purpose and aligned with agency needs.

5.3 Uplift cyber resilience

5.3.1 Goal – strengthen all-of-government cyber resilience

What success looks like:

- NSW Government agencies will continue to strengthen their resilience to cyber security threats and incidents, consistently meeting and building upon the minimum baseline set by the NSW Cyber Security Policy.
- Agencies will continue to strengthen their OT and IoT controls, with Cyber Security NSW identifying areas for improvement and reinforcing accountability through established governance mechanisms. This includes, but is not limited to, structured oversight and targeted reviews.
- Coordination between emergency management and internal cyber response processes will be further strengthened, enabling more systematic prevention, response and recovery from cyber incidents and related data breaches.
- Agencies responsible for critical infrastructure will maintain a consistent and evolving approach to risk management, supported by strong collaboration across government to identify and manage risks.
- Vendors supplying to the NSW Government will be rigorously vetted and held to high standards of cyber security best practice, with ongoing efforts to reduce third-party risk and strengthen security across the supply chain.

5.3.2 How we achieve success

Strong cyber security and identity resilience practices are essential to defending NSW Government environments, products and services against malicious activity. Through this strategy, the NSW Government will continue to build trust in its digital systems while enhancing its overall cyber resilience. NSW Government agencies will:

✓ **implement targeted uplift programs to secure systems in compliance with the NSW Cyber Security Policy**

✓ **identify and prioritise protection of critical assets, aligning with recognised frameworks to strengthen resilience**

✓ **meet legislative and policy requirements for critical infrastructure in NSW and contribute to coordinated protection efforts across government**

✓ **adopt a modern defensive architecture approach applying secure-by-design and zero trust principles to improve cyber resilience**

✓ **align cyber incident response and business continuity plans with the State Cyber Security Emergency Plan to ensure coordinated and effective recovery.**

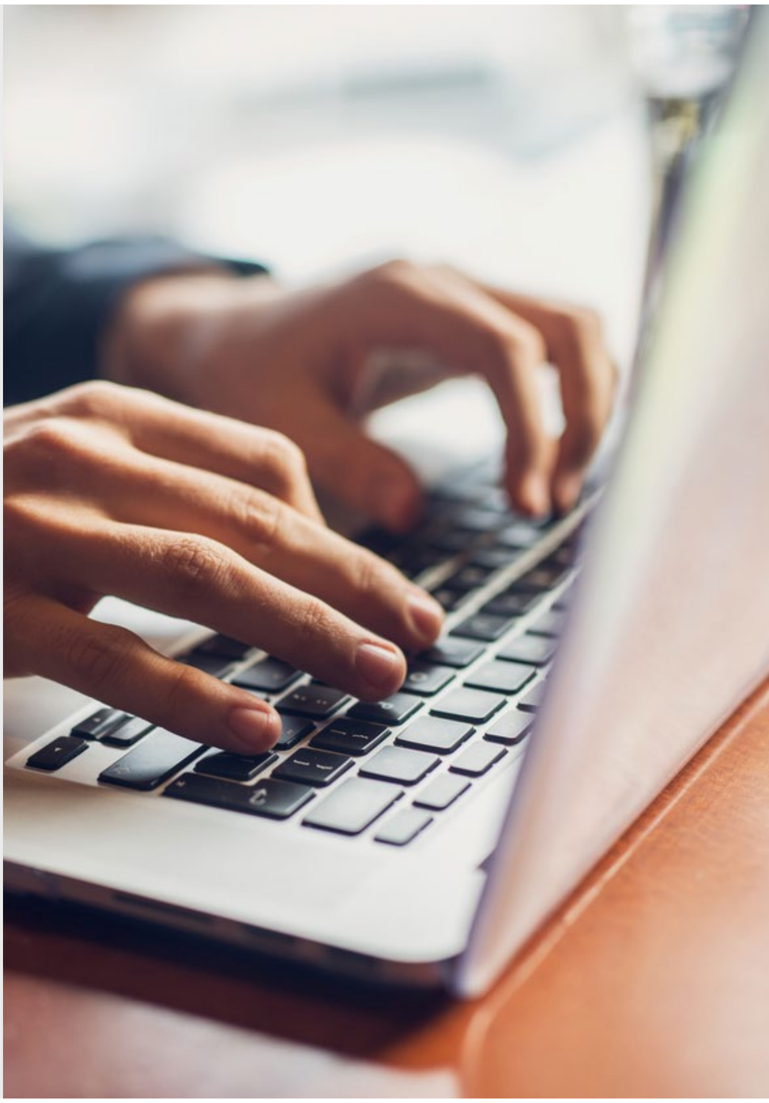
5.3.3 Work in progress – establishing a strategic baseline for cyber risk management

The NSW Government is actively implementing measures to strengthen cyber resilience. These initiatives are already underway and focus on improving compliance and emergency management, and reducing supply chain risk.

Current initiatives include:

- implementing the DCS-2025-04 Circular: Agencies are reporting cyber incidents within 24 hours and developing and maintaining an asset inventory and a register of third-party providers. As part of the NSW Cyber Security Policy reporting cycle, agencies are also required to assess their posture against defined all-of-government risks and submit an asset inventory of their crown jewels
- implementing interim arrangements pending the redesign of the NSW State Cyber Security Emergency Plan and the NSW Cyber Incident Management Arrangements.

Agencies are working to meet requirements under the NSW Cyber Security Policy to ensure cyber security risks to information and systems are effectively managed. All agencies must **report annually** against the NSW Cyber Security Policy, demonstrating compliance with Mandatory Requirements and applying a **risk-based approach to implementing controls**.



5.4 Drive continuous development of cyber security tools, processes and methodology

5.4.1 Goal – strengthen cyber capability through shared services and continuous learning

What success looks like:

- NSW Government agencies will further mature their cyber resilience by fostering a workforce that is both cyber-aware and confident in responding to evolving common social engineering threats such as phishing. This will be achieved through iterative, targeted training and awareness programs delivered at both an agency and all-of-government level. Community-focused initiatives will also be delivered via ID Support NSW to strengthen privacy and cyber awareness.
- Agencies will reduce duplication of effort by actively leveraging the centralised services, tools and guidance provided by Cyber Security NSW, as well as all-of-government licensing to achieve better value through collective purchasing. This coordinated approach will improve efficiency, ensure consistency in cyber capability uplift, and enable agencies to focus resources on their specific risk environments.

5.4.2 How we achieve success

The continuous development of cyber security awareness among staff is essential for the early identification and mitigation of cyber risks. The NSW Government is committed to advancing cyber security skills across all agencies and fostering a culture of shared responsibility. Recognising the value of collaboration within and across agencies, NSW Government agencies will take the following actions to further strengthen cyber capability and embed cyber security into everyday practice:

✓ **identify and invest in emerging opportunities to uplift talent and cyber workforce capability across the public sector**

✓ **embed a strong security culture through tailored programs and practical guidance that empower all staff to adopt and maintain cyber-safe behaviours**

✓ **strengthen collaboration with industry, academia and government and lead by example for cyber security best practice.**

5.4.3 Work in progress – advancing momentum in cyber vigilance

NSW Government agencies have laid strong foundations for building cyber security capability across the public sector by educating staff on the importance of cyber awareness and promoting early identification of risks. Significant progress has been achieved through targeted awareness programs that help staff understand and respond to evolving threats.

Cyber Security NSW is driving further uplift through key initiatives currently underway.

- Exercise-as-a-Service: Supporting agencies with tailored cyber security exercises to test and refine incident response plans, improving readiness and confidence.
- Collaboration across government: The Cyber Security Community of Practice and Awareness Working Groups connect staff across agencies to share insights, align messaging and foster consistent approaches to cyber risk management.
- Executive-level engagement: Corporate compromise gamification sessions are being delivered to senior leaders, providing interactive experiences that highlight key risks and controls, strengthening leadership decision-making.

5.5 Support NSW communities to be cyber safe

5.5.1 Goal – expand identity resilience across NSW communities

What success looks like:

- NSW will continue to strengthen its role as a trusted provider of a 'one-stop shop' for promoting identity resilience, where individuals feel supported by government in the aftermath of identity misuse and data breaches. This builds on existing confidence and capability, reinforcing NSW's leadership in community-focused support.
- Building on current efforts, ID Support NSW will empower individuals – especially those in at-risk communities – with the knowledge and tools to strengthen their identity resilience and remain safe online. This work will also underpin Pillar 5 of the NSW Digital Inclusion Strategy, ensuring equitable access to cyber safety resources.
- NSW Government agencies will lead by example in promoting cyber safety and protecting the community's data, setting a benchmark for industry and other jurisdictions.
- Agencies will leverage both established internal capabilities and external resources and partnerships to support communities following cyber incidents and data breaches, with ID Support NSW continuing to play a central role in recovery and resilience-building.

5.5.2 How we achieve success

To continue protecting the personal information of NSW communities and supporting victims of cybercrime, the NSW Government, through ID Support NSW, will:

✓ **continue to deliver NSW's leading data breach support and remediation services through a customer-centred approach**

✓ **expand its outreach to vulnerable and culturally and linguistically diverse communities through targeted engagement on identity resilience, scams and identity protection**

✓ **promote the adoption of innovative and practical tools and products that embed privacy-by-design principles, ensuring security is built into everyday digital interactions**

✓ **drive and support programs that assist small businesses across NSW to build cyber security awareness and foster a strong cyber-safe culture within their operations.**

5.5.3 Work in progress – setting the standard for identity resilience services

ID Support NSW delivers a nation-leading identity resilience service that has proven critical in supporting NSW communities through the response to, and recovery from, data breaches and identity compromise. The function assists individuals whose government-issued identity credentials have been stolen or fraudulently misused and supports business owners in safeguarding personal information and recognising data risks.

- **Identity protection legislation**
  - In August 2025, the Identity Protection and Recovery Act 2025 successfully passed NSW Parliament. The Act allows ID Support NSW to:
    - establish a fraud check service and the Compromised Credential Register
    - be formally recognised as the lead provider of identity protection and recovery services
    - support individuals affected by data breaches through document replacement, alerts and personalised assistance.

How we will implement the Strategy

An action plan will be developed to guide delivery against the Strategy's commitments and ensure it remains current and aligned with the NSW Government's digital vision, supports the uplifting of national cyber capabilities and advances departmental priorities.

Structured around horizon-based planning and developed in consultation with cyber security and ICT stakeholders across government, it will set out what actions will be taken, and when, including:

01 **formal reporting, within internal all-of-government Cyber Security and ICT leadership forums**

02 **milestone updates outlining progress to date, and where applicable, changes to incorporate emerging technologies and digital trends.**

This alignment will ensure performance metrics and indicators remain relevant to NSW's strategic objectives and are interoperable with broader state and federal frameworks, enabling consistent benchmarking and transparent reporting.

Cyber Security NSW will oversee the tracking of the defined action plan and will establish the governance and review processes by which agencies will provide reporting.

Conclusion

The NSW Government has made significant progress in strengthening cyber and privacy resilience and embedding security across its operations. This strategy builds on that foundation and will drive continued uplift in capability, governance and collaboration to keep pace with an evolving threat environment.

Through sustained focus and shared responsibility, NSW Government agencies will continue to enhance their cyber maturity, protect critical services and data, and ensure the NSW public sector remains secure, trusted and resilient, delivering safe digital services that communities can rely on.

Cyber Security NSW

2/24 Rawson Place
Haymarket NSW 2000

E: info@cyber.nsw.gov.au
W: https://www.digital.nsw.gov.au/delivery/cyber-security