Horizon 2 of the *2023-2030 Australian Cyber Security Strategy*

For large organisations and critical infrastructure

The *2023-2030 Australian Cyber Security Strategy* provides a roadmap for Australia to become a world-leader in cyber security by 2030. It sets out the actions that will be taken by the Australian Government to achieve this over three time-based horizons.

The *Action Plan for Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (Horizon 2 Action Plan) sets out 19 actions to be delivered through 64 initiatives, led by 12 different agencies across the Australian Government. These actions and initiatives will enable us to scale-up cyber maturity across the economy in 2026-2028, leveraging the legal and policy frameworks established through our work under Horizon 1 (2023-2025).

This fact sheet provides large organisations and critical infrastructure with information about what has been delivered under Horizon 1, and how the Horizon 2 Action Plan supports them.

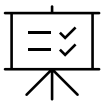
Initiatives delivered under Horizon 1

The **Executive Cyber Council**, chaired by the Minister for Cyber Security, was established bringing together C-suite representatives from Australia's top companies and industry representative groups to strengthen our private/public partnership on cyber security.

Amendments to the *Security of Critical Infrastructure Act 2018* were passed to address risks concerning the cyber security of business critical data held by a critical infrastructure asset, bringing security requirements for telecommunications providers into line with other critical infrastructure entities, and the management of secondary consequences of a cyber security incident.

Significant **aviation and maritime security legislation reforms** were also progressed to expand the scope of relevant legislation to include cyber security risks and mitigation.

The **National Cyber Intel Partnership** was established to encourage larger organisations to **share cyber threat intelligence and block cyber threats at scale**, and ran a series of pilots, transitioning outcomes to enhance the Australian Signals Directorate's threat sharing platform. We also established the **Health Cyber Share Network**, incentivising broader threat sharing and blocking across the economy.



The National Office of Cyber Security delivered **12 industry sector-based cyber incident response playbooks** to guide how the Australian Government and industry will work together in the event of a cyber security incident, available on the Home Affairs website.

We legislated the limited use obligation under the *Cyber Security Act 2024* and the *Intelligence Services Act 2001* to encourage industry to share cyber security information with government while maintaining an effective regulatory environment.

Further detail about the delivery of the full suite of 20 actions and 60 initiatives under Horizon 1 is available on the Home Affairs website.

Horizon 2 initiatives supporting large organisations and critical infrastructure

There are a number of initiatives and reforms that will support large business and critical infrastructure over Horizon 2. Here are some examples:

Cyber security exercises will increase in size and sophistication

- The **National Office of Cyber Security Exercise Program will be strengthened and expanded**, supporting Systems of National Significance and government supply chains. This will include targeted engagement with supply chain dependencies and delivery of scalable readiness activities across the Australian economy.

Our efforts on sharing and blocking will continue

- We will consult with industry stakeholders and government agencies **to enhance legislative and policy levers to ensure 'upstream entities' (such as telecommunication providers) can block threats at scale and speed** to better defend those who cannot defend themselves.
- We will publish **clear advice on the permissible cyber defence activities Australian organisations can take to defend themselves**, providing industry with a framework to harden systems as part of their day-to-day activities and confidence to react and defend their own networks from cyber attack.
- We will develop and publish a **Vulnerability Disclosure Policy Toolkit** that will support large businesses to develop policies to support identification of vulnerabilities in their organisations.

We will harness the benefits of emerging technology while protecting our most valuable assets

- The **Industry Data Classification Framework** and **Code of Practice for commercial data transactions** will help lift industry data and digital governance, strengthening data security practices across Australia.
- We will **implement recommendations from the Data Retention Review** to introduce a consistent, whole-of-government approach to data retention, simplifying obligations and guidance for industry.
- We will protect our data sets of national significance, through a **pilot risk assessment framework for genomic and clinical trial data** supporting practical guidance and best-practice protections.
- Australia will secure the computing power needed to take advantage of emerging technology by **establishing expectations of data centres and AI infrastructure developers** in partnership with states and territories.
- We will strengthen **public, private and international collaboration** on AI and quantum security threats, including leadership of the Five Country Ministerial AI Working Group and improved **crisis management frameworks for major AI incidents**.
- **We will prepare government for post-quantum cryptography** through mandatory transition planning, updated security policies, and stronger protections under the Protective Security Policy Framework.
- We will build national cyber resilience by requiring all Commonwealth agencies to embed **cyber security planning in Digital Investment Plans**.

We will continue to uplift the cyber security of the Australian Government

- The cyber security baseline will be lifted across government by **improving cyber fluency for Australian Public Servants** and **updating cyber security policy and risk management frameworks**.
- We will prioritise the protection of our most critical government services by **establishing the legacy technology baseline for critical systems** and prioritising remediation, as well as developing **incident playbooks and tabletop simulations** to strengthen preparedness and capability for Systems of Government Significance.
- **Investment will be targeted to address the highest risks** by reviewing technology purchasing arrangements and refining investment indicators to prioritise the most critical cyber security uplift areas.

We will enhance the security and resilience of Australia's critical infrastructure

- We will **explore further amendments to the *Security of Critical Infrastructure Act 2018***, including amendments to Ministerial Directions powers and enhancements to Critical Infrastructure Risk Management Program requirements for high-risk asset classes.

- The **Trusted Information Sharing Network** will continue to encourage greater collaboration and information sharing between critical infrastructure entities and all levels of government.
- We will support Systems of National Significance to be compliant with their **Enhanced Cyber Security Obligations** and provide targeted insights on incident response planning.
- We will develop a **whole-of-government drones security policy** to prevent, investigate and penalise drone misuse where it presents a security threat.
- We will continue to **protect Australia's foundational cyber infrastructure**, **subsea cables**, by assessing our current subsea cable infrastructure protections to ensure they are fit-for-purpose.

We will streamline cyber security regulation and reporting for business

- We will boost business productivity by cutting duplicated cyber security rules and streamlining how industry meets its obligations. We will deliver a **Single Cyber Incident Reporting Interface** aligned with the Tell Us Once agenda, replacing fragmented processes with one clear, efficient pathway.
- A focused **review of the regulatory landscape** will identify pressure points and opportunities to centralise reporting, driving consistent definitions, timeframes, and thresholds—reducing compliance costs, improving regulatory efficiency, and strengthening Australia's overall cyber resilience.

We will continue to support the development of a professional, diverse and dynamic cyber security workforce

- Following a pilot program commenced under Horizon 1, we will **explore the feasibility of a national rollout of a framework for the professionalisation of the cyber workforce**.

Further detail about the 19 actions and 64 initiatives that will be delivered under Horizon 2 is available on the Home Affairs website.

How you can stay informed about Horizon 2

We will provide regular updates about the progress of Horizon 2, including opportunities for consultation and co-design processes and upcoming events and Town Halls. To stay up to date, check our website.

For further enquiries, please contact CSSH2@homeaffairs.gov.au.