Australian Government

Charting New Horizons

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

Charting New Horizons

In November 2023, the Australian Government released the 2023-2030 Australian Cyber Security Strategy and Horizon 1 Action Plan with a bold vision for Australia to be a world leader in cyber security by 2030.

Six shields each providing an additional layer of protection for businesses and citizens

As Horizon 1 draws to a close and we embark on Horizon 2, it is timely to reflect on what has been achieved under the Strategy and work together to define future possibilities.

The aim of the Horizon 2 Discussion Paper is to continue the conversation and collaboration with businesses, citizens and community groups on the cyber security outcomes we seek to achieve for Australia and how to best achieve them over Horizon 2.

Three horizons to provide review points and enable us to remain adaptive to emerging technological, economic and geopolitical trends

Building on our foundations

The launch of the Strategy in 2023 responded to a call by the Australian public for greater action on cyber security as the rate and severity of cyber attacks has continued to accelerate in Australia and abroad.

In the 18 months since the Strategy's launch, Government has delivered, or is on track to deliver all 60 initiatives under Horizon 1 (see the Discussion Paper for more detail on these achievements and progress).

Our capacity to take-on threats in the cyber domain has been strengthened alongside our ability to forecast lines of effort needed to achieve the ambitions set by the Strategy and support us as we move forward together into Horizon 2.

Key Themes for Horizon 2

Looking towards Horizon 2, the Government is exploring policy ideas and programs that allows Australia to:

Embed

cyber security messaging, standards, capability and efforts across society, from our homes and schools to our businesses and government partners.

Empower

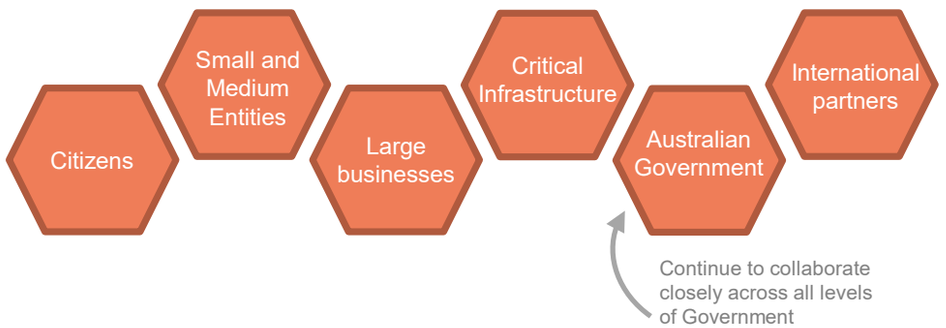
business (particularly small business), not-for-profits and citizens to protect ourselves and each other, reducing the barrier for applying protective frameworks ensuring Australian businesses are more productive and bounce back quicker.

Enhance

our cyber regulatory frameworks through structural reforms to harmonise and simplify regulation, strengthen our cyber workforce and business ecosystem and better coordinate security outcomes for Government cyber uplift.

Cyber Security is a 'team sport'

We want to explore the needs across the economy and cyber ecosystem to better understand opportunities and priorities for reform.



Since the launch of the Strategy the rate and severity of cyberattacks has continued to grow in Australia and abroad

Australian citizens and businesses say cyber security is the #1 threat in 2025

Lowy Institute Poll 2025 and Allianz Risk Barometer 2025

Australia's cyber threat surface is increasing with 109 million more connected devices in Australian homes from 2023 to 2027

Telsyte Australian Smart Home Market Study 2023

Australian businesses and individuals are being targeted with 1 cyber crime reported every 6 minutes

ASD Annual Cyber Threat Report 2023-2024

The costs are increasing

- Investment in IT security and risk management expected to **grow 11% in 2026.**
- Average cost of cyber crime increased by **8% for small businesses** from 2022-23 to 2023-24
- Australian business lost an estimated **$33 billion** in 23-24 due to cyber incidents.

Gartner Research (2022) and ASD Annual Cyber Threat Report 2023-2024

The cyber professionals skills gap is growing

Estimated global shortage of cyber security professionals is currently **4 million**. This is expected to grow to **85 million** in 2030.

World Economic Forum Strategic Cybersecurity Talent Framework 2024

Across Horizon 2 we want to achieve an end-state in 2028 where:

- **Our citizens**, particularly vulnerable Australians, are educated about cyber security risks and motivated to take action to reduce risks to themselves and their communities. Australians can make informed decisions about the digital tools they bring into their homes, and are confident about the authenticity and reliability of their online activities and the technologies they choose to use.

- **Small and medium-sized businesses and the not-for-profit sector** are increasingly educated and motivated about cyber risks, digital tools and online activities and have access to suitably designed standards that are cost effective to implement and provide a simple and clear pathway to uplift their cyber resilience.

- **Large business** is deploying their best efforts on cyber security in Australia and have access to an abundant and diverse cyber security workforce with the skillsets to start solving tomorrow's problems today. Security-by-design and security-by-default is incorporated appropriately into business practices, supported by harmonised and simplified cyber regulation.

- The cyber security of our **critical infrastructure** has been uplifted to a meaningful standard, supported by a mature regulatory position from Government ensuring any non-compliance is identified and rectified.

- **Federal, state and local governments** are working together to maintain the resilience of online government services and systems. The Australian Government is an exemplar in cyber security leadership and data protection.

- **Australia remains a cyber partner of choice in the region.** We continue to shape, uphold and defend international cyber rules, norms and standards, and effectively impose costs on state and non-state malicious actors.

Focus areas and discussion questions

How can Australia...?

1 Strong businesses and citizens

Our citizens and businesses are better protected from cyber threats, and can recover quickly following a cyber attack.

- Consolidate our cyber awareness messages across the economy?
- Increase cyber literacy in our schools and early learning programs?
- Target resilience uplift to small and medium-sized entities that cannot adequately protect themselves, including through tailored cyber security standards that are cheap to apply?
- Enhance support for citizens and victims of cybercrime to help them bounce back quicker?
- Harmonise and simplify cyber regulation to promote best practice and efficiency?

2 Safe technology

Australians can trust that their digital products and services are safe, secure and fit for purpose.

- Develop appropriate standards for high risk devices?
- Protect our most vulnerable datasets?
- Promote the safe use of emerging technology?

3 World-class threat sharing and blocking

Australia has access to real-time threat data, and we can block threats at scale.

- Encourage and enable the private sector to block threats and take a more proactive posture against cyber threat actors?
- Amplify existing government and industry models for threat blocking and threat sharing?
- Review policy frameworks, as necessary, for resilience to a widespread incident, conflict or crisis situations to protect Australia's national interests?

See the Horizon 2 Discussion Paper for more detailed information and questions on each Shield to help inform your Submissions.

Focus areas and discussion questions

How can Australia...?

4 Protected critical infrastructure

Our critical infrastructure and essential government systems can withstand and bounce back from cyber attacks.

- Mature the regulatory framework for critical infrastructure security?
- Centralise risk management, investment and policy for Commonwealth cyber uplift to drive more coordinated security outcomes?

5 Sovereign capabilities

Australia has a flourishing cyber industry, enabled by a diverse and professional cyber workforce.

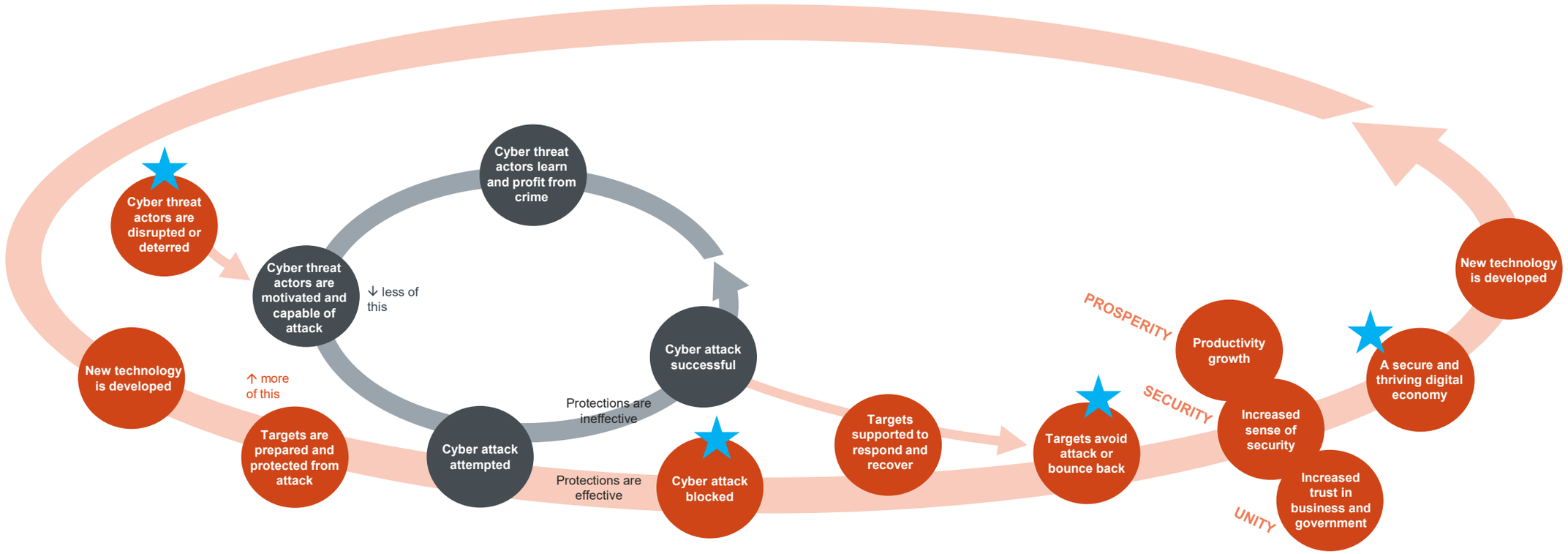
- Boost productivity by promoting a sustainable and diverse cyber workforce and business ecosystem?
- Provide greater support for academic research and strengthen collaboration between academia, industry and government?
- Nurture the growth and development of robust sovereign capabilities?

6 Resilient region and global leadership

Australia's region is more cyber resilient, and will prosper from the digital economy. We will continue to uphold international law and norms and shape global rules and standards in line with our shared interests.

- Continue to use all arms of statecraft to impose costs on state and non-state malicious cyber actors?
- Strengthen cyber resilience and cooperation on critical technologies in the region?
- Continue to shape, uphold and defend international cyber and digital trade rules, norms and standards in our interest?
- Drive a program of international regulatory alignment?

See the Horizon 2 Discussion Paper for more detailed information and questions on each Shield to help inform your Submissions.



Cyber Security Policy Evaluation Model

The Australian Government has embarked upon creation of a world-first framework to support Government and its partners to work together to deliver long-term outcomes for Australians in a changing world.

The first step is to develop a clear shared picture of our long-term goals.

In the Horizon 2 Discussion Paper we have translated the high-level outcomes expressed in the Strategy into a Cyber Security Policy Evaluation Model (see diagram).

Our goal is to develop a map that is long lasting and drives shared action and investments, including in data, beyond the current Strategy.

The model will guide both the selection of interventions and the monitoring and evaluation of their effectiveness.

We seek your views on whether the Model resonates and invite you to collaborate with us on further iteration and data creation.

We want to hear from you

Please send any questions to:

- CSSH2@homeaffairs.gov.au
- Submissions should be made in PDF via the Horizon 2 Discussion Paper webform at: homeaffairs.gov.au
- Submission due date: 29 August 2025

Please see our website homeaffairs.gov.au for a schedule of other ways you can engage such as live online town halls and work shops.