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

For workers and small and medium businesses

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 Australian workers and small and medium businesses 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 **Ransomware Playbook** is a **free** online resource that provides easy-to-understand guidance to individuals about how to detect and prepare for a ransomware attack, how to respond and report in the event of an attack and what resources are available to support you to recover. The playbook includes guidance specifically targeting individuals and small to medium businesses.

To ensure the smart devices that businesses use are secure by design and secure by default, we **established new cyber security requirements for smart devices sold or manufactured in Australia** under the *Cyber Security Act 2024* and *Cyber Security (Security Standards for Smart Devices) Rules 2025*.

Further information on these security standards is available on the Home Affairs website.

The **Cyber Health Check Tool** is now available and is another **free** online resource that provides a basic cyber security assessment for small businesses. This will let you know practical steps you can take for your business to improve your cyber resilience.

A **Small Business Cyber Resilience Service**, funded by the Australian Government and delivered through IDCARE, provides free supports to small businesses, including incident support and cyber ‘first aid’, wellbeing support following an incident, and a private, independent review of a business’s privacy and cyber security posture.

Further information about the services IDCARE provides is available on their website.

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 focuses on Australian workers and small and medium businesses

There are a number of initiatives and reforms that will support small and medium business over Horizon 2. Here are just a few examples:

Uplifting small and medium businesses is key to Australia's overall cyber security

Small and medium sized businesses are the cornerstone of Australia's economy, employing two-thirds of the workforce and providing critical inputs into the supply chains of larger organisations.[1] This means that working with small and medium businesses to uplift their cyber security is critical to our national security and key to uplifting Australia's overall cyber resilience.

Improving the cyber security of small and medium businesses was the top issue raised by stakeholders in developing our actions and initiatives for Horizon 2. The clear message was that small and medium businesses need more tailored support that they can easily and affordably adopt in their business, and that they want to go to one place for plain-English resources.

We will establish a new **CyberSmart Program** to drive cyber security improvements for small and medium businesses. Under CyberSmart we will:

- adopt a new **cyber security standard** and **accreditation scheme** tailored specifically to the needs and capabilities of small and medium sized businesses.
  - This will cover the cyber basics and then using a tiered approach, it will grow in maturity as your business grows and your cyber resilience improves.
  - We will engage extensively with industry and other stakeholders on the development of the program, working to ensure that costs remain low and simplicity is at the core of the design.
- create a **CyberSmart Trust Mark** to demonstrate that an organisation has been certified under the CyberSmart scheme.
- establish a **CyberSmart Hub as a centralised location** for program advice and support. The Hub will grow and evolve, and we will work with business to develop new features and functionality.
- **encourage uptake of the new CyberSmart Program through regulatory and policy levers available to government**. This will include risk-based application of CyberSmart in Commonwealth procurement and supply chain management.

In addition to the CyberSmart Program, small and medium businesses will be supported under Horizon 2 through a range of other new and existing programs, including:

- improving the cyber security of modems and routers used in small office settings, and creating a **voluntary Code of Practice for edge devices** provided by internet service providers, reducing exposure to cyber security risk for smaller entities.
- **enhancing the Cyber Health Check Tool** to ensure it remains up-to-date and easily accessible, providing a basic cyber security assessment and action plan for small organisations and individuals.
- **expanding the Digital ID program**, including by making it available to the private sector, reducing the need for individuals to share identity documents and for government agencies and businesses to store them.
- **investing in domestic cyber industry growth**, sustaining our support for cyber start-ups and small and medium sized businesses to develop innovative solutions to cyber security challenges.

---

[1] Australian Small Business and Family Enterprise Ombudsman, Contribution to Australian Employment, https://www.asbfeo.gov.au/small-business-data-portal/contribution-australian-employment

Workers in our small and medium businesses are our ‘human firewall’

Human error contributes to around 60% of all cyber incidents.[2] This means, despite improving cyber security products and technology, improving our collective cyber security needs to include changes to human behaviour. Our digital firewall needs to be supplemented with a ‘human firewall’—with workers in Australia’s 2.5 million small and medium businesses having a key role in improving and defending the cyber security of the organisations they work in.

Relevant Horizon 2 initiatives to strengthen our ‘human firewall’ include:

- collaborating with our industry partners to **baseline strong cyber security awareness and education practices for workers and supply chain entities**, including members of the Executive Cyber Council, and making outcomes publicly available for organisations of all sizes to adopt in their business operations.
- enhancing public awareness and messaging through a **dedicated stream of the *Act Now. Stay Secure.* campaign** focusing on empowering our workforce to act as the ‘human firewall’ for the businesses they work in and protect themselves from AI-enabled cyber threats.

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.

[2] Verizon (2025), *2025 Data Breach Investigations Report* (p. 11).