Australian Government

# 2023–2030 Australian Cyber Security Strategy

## HORIZON 2 ACTION PLAN

**Contact us**

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

P - 26-02629

# 2023–2030 Australian Cyber Security Strategy

## HORIZON 2 ACTION PLAN

# Contents

# Executive summary

The Australian Government remains committed to its vision of positioning Australia as a world leader in cyber security by 2030, as outlined in the *2023-2030 Australian Cyber Security Strategy* (the Cyber Security Strategy).

Achieving our vision under the Cyber Security Strategy remains grounded in the actions that the Australian Government will take, and the outcomes that these will achieve, across three horizons:


- **In Horizon 1**, we strengthened our foundations by addressing critical gaps in our cyber shields, building better protections for our most vulnerable citizens and businesses, and supporting initial cyber maturity uplift across our region.
- **In Horizon 2**, we aim to strengthen cyber maturity across the Australian economy, society and digital infrastructure. As outlined in this new *2023-2030 Australian Cyber Security Strategy: Horizon 2 Action Plan* (the Horizon 2 Action Plan), we are making the further investments required across the broader cyber ecosystem.
- **In Horizon 3**, we will advance the global frontier of cyber security. We will lead the development of emerging cyber technologies to adapt to new risks and opportunities across the cyber landscape.

## Our foundations have been strengthened under Horizon 1

Under Horizon 1 of the Cyber Security Strategy in 2023 to 2025, we strengthened our cyber security foundations by delivering on 20 actions supported by 60 initiatives listed in the *2023-2030 Australian Cyber Security Strategy: Action Plan* (the Horizon 1 Action Plan).

Further details about the delivery of actions and outcomes achieved under Horizon 1 are available on the Department of Home Affairs website.

## Responding to our stakeholders and the current cyber threat environment

Since the launch of the Cyber Security Strategy in 2023, the cyber threat environment has continued to evolve, with threats both increasing and changing. There are more malicious cyber actors and our systems are increasingly connected and automated, meaning more potential vulnerabilities to exploit.

We are also seeing artificial intelligence tools that can help automate and supercharge criminal capabilities. The costs of cyber incidents are increasing, particularly for small and medium businesses and individuals. In preparing for Horizon 2 from 2026 to 2028, we have considered the changes in technological, economic and geopolitical trends.

Key threats we are responding to through Horizon 2 include the following:

- The **cost of cybercrime is increasing**. It costs the economy an estimated $25 billion per year, with the average cost of a cybercrime reported to the Australian Signals Directorate increasing 50% between 2023-24 and 2024-25 to $80,000.[1]
- A **single catastrophic cyber incident could wipe out $35 billion** from the Australian economy —approximately 1.3% of GDP.[2]
- Rapid adoption of artificial intelligence is providing an important productivity boost, but **artificial intelligence is an expanding cyber threat vector**—with 97% of organisations that reported an artificial intelligence-related security incident lacking proper artificial intelligence access controls. [3]
- **Malicious cyber actors are adapting**, including by using artificial intelligence and automation tools, with attackers using artificial intelligence in 16% of data breaches in 2024.[4] They are also increasingly targeting vulnerabilities in edge devices (routers and modems) and virtual private networks—up from 3% in 2023 to 22% in 2024.[5]
- **Human error is a factor in 60% of data breaches.**[6]
- Small entities continue to be disproportionately impacted by cyber risks, and this **cyber inequity is increasing** as malicious actors adapt and become more difficult to detect.[7]
- **Government and critical infrastructure are being targeted by sophisticated state-based actors** for espionage, disruption and destruction, potentially pre-positioned for future cyber incidents.[8]

## Scaling-up cyber maturity under Horizon 2

In response to the worsening threat environment, for Horizon 2 of the Cyber Security Strategy, the Australian Government will reduce cyber harm by focusing effort where it matters most and moving fast when it counts.

1. Australian Signals Directorate (2025), Annual Cyber Threat Report 2024-25.
2. Australian Institute of Criminology (2025), The cost of espionage.
3. IBM (2025), Cost of a Data Breach Report 2025.
4. IBM (2025), Cost of a Data Breach Report 2025.
5. Verizon (2025), 2025 Data Breach Investigations Report.
6. Verizon (2025), 2025 Data Breach Investigations Report.
7. World Economic Forum (2025), Global Cybersecurity Outlook 2025.
8. Australian Signals Directorate (2025), Annual Cyber Threat Report 2024–25.

We will focus resources and reform effort on a layered approach, which aims to stop malicious activity at our border, work with industry to secure our most sensitive digital systems in critical infrastructure and government, and uplift the cyber security baseline for small and medium business.

This puts the Australian Government's resources where they will have maximum impact and leverages the strong foundations and new regulatory and relationship levers we have developed through Horizon 1. Partnerships with industry remain at the heart of the Cyber Security Strategy as the challenges we face over the next Horizon cannot be met by government or industry alone.

Through our work to prepare for Horizon 2 of the Cyber Security Strategy, including collaboration with our stakeholders and key industry partners, we have identified three key objectives to achieve our Horizon 2 goals.

**Objective 1: Enabling our workers to be our strongest defence, our 'human firewall'**

We need to challenge the perception that cyber security is a technical issue, to be solely dealt with by IT professionals and software. We need to reinforce our 'human firewall' as our first line of cyber defence. We will focus on small and medium businesses as the highest area of risk, particularly within supply chains, and as the employer of 8.5 million Australians.

Key actions to achieve Objective 1 include:

- **Establishing a fit-for-purpose cyber security standard framework for small and medium businesses** through our new CyberSmart Program—empowering business owners and operators to make risk-based decisions within their operating contexts. (Action 1.2)
- **Safeguarding critical infrastructure and government** by using the *Security of Critical Infrastructure Act 2018* and government procurement levers to promote uptake of the CyberSmart standard to ensure the cyber security of their supply chains. (Action 1.2)
- **Building on the successful *Act Now. Stay Secure.* public awareness campaign** delivered under Horizon 1 to translate awareness into action and ensure Australians develop consistent cyber secure habits and are equipped to **deal with emerging cyber threats, including artificial intelligence-enabled cyber attacks**. (Action 1.3)
- **Baselining strong cyber worker engagement and learning practices for Australian businesses and government**, working with our larger businesses, the Executive Cyber Council and representative bodies to build a package of resources to assist others. (Action 1.1)
- **Launching a single cyber regulatory reporting interface to give businesses** a 'tell us once' experience when they go to cyber.gov.au to report and align cyber regulation across government to support the new interface. (Action 1.6)
- **Delivering an international ransomware standards framework** to set global benchmarks for preparation, prevention, response and recovery from a ransomware attack. (Action 6.2)

**Objective 2: Protecting our critical infrastructure and government systems**

As digital technologies increasingly underpin essential services across government and industry, cyber incidents affecting these systems carry the potential for rapid, cascading impacts with national consequences. The Australian Government's ability to deliver critical services and uphold national resilience depends on the security, reliability and preparedness of its own digital systems and infrastructure.

Horizon 2 will focus on uplifting cyber maturity by strengthening the security, reliability and resilience of government systems and critical infrastructure, shifting beyond baseline assurance and reactive response to a proactive, investment-led approach that enhances preparedness and systemic resilience across critical assets and their supply chains.

Key actions to achieve Objective 2 include:

- **Protecting the Australian Government's most critical services through a robust governance model** that drives prioritised security protections, elevates risk management practices, reduces legacy technology risk, and ensures readiness and resilience **across our Systems of Government Significance.** (Action 4.2)
- **Strengthening Australia's supply chain resilience through the National Office of Cyber Security** by delivering scalable exercises and targeted readiness activities to address cyber risks and economic impacts across critical infrastructure and major businesses. (Action 5.1)
- **Strengthening procurement arrangements** to uplift cyber security across the Australian Government by **embedding minimum cyber security standards and requirements** for information and technology goods and services. (Action 4.2)
- **Elevating information sharing and partnership** with critical infrastructure owners, operators and their supply chains to improve cyber security outcomes, including through enhancements to the Trusted Information Sharing Network. (Action 4.1)
- **Strengthening logging and monitoring standards** across government and critical infrastructure to improve visibility, early detection and coordinated response to cyber threats. (Action 4.1 and 4.2)
- **Exploring options to amend the Directions powers** in the *Security of Critical Infrastructure Act 2018* to better protect critical infrastructure against contemporary threats. (Action 4.1)
- **Addressing the security risks posed by drones** to government and critical infrastructure through whole-of-government security policy to prevent, investigate and penalise drone misuse. (Action 4.1)
- **Undertaking a preliminary assessment of our subsea cable security posture** to prioritise future actions that will strengthen the security and resilience of Australia's subsea cable infrastructure. (Action 4.1)
- **Deepening collaboration and coordination with states, territories and local government** through a National Cyber Security Compact (Action 4.3).

**Objective 3: Shaping, securing and embracing digital technology**

Australia's future economic productivity depends on the safe and confident adoption of increasingly connected and automated technologies across government, business and households. As digital systems, data and emerging technologies such as artificial intelligence become more deeply embedded in everyday services and critical functions, the scale and complexity of cyber risk is increasing.

Malicious cyber actors are exploiting insecure technologies, weak data practices and systemic dependencies. They are using artificial intelligence to increase the speed, scale and sophistication of cyber attacks. Left unaddressed, these risks threaten trust in the digital economy, undermine innovation and expose Australians to harm.

In Horizon 2, we will complement the 'human firewall' by reducing cyber risk at its source. We will shape the technology environment Australians rely on so that safe adoption becomes the default, such as embedding security into the design, deployment and operation of connected technologies, strengthening protections for data that matters most, and anticipating emerging technology risks.

Key actions to achieve Objective 3 include:

- **Enhancing legislative and policy levers to support telecommunication providers and others 'upstream' from our digital interfaces** to block at scale and speed. (Action 3.2)
- **Supporting industry to harden and defend Australia's cyber networks against threats**, with a focus on defining permissible cyber defence activities and vulnerability disclosure. (Actions 3.1 and 3.2)
- **Embedding security into connected technologies used in homes and businesses** through new secure-by-design standards and requirements. This includes focusing on the most common and highest risk devices and services used in Australia like routers, connected operational technology and consumer energy resources. (Action 2.1)
- **Making secure technology the easy choice**, by providing consumers with the right information through continued co-design of a voluntary labelling scheme for smart devices. (Action 2.1)
- **Preparing government and critical infrastructure to manage emerging technology risks, including artificial intelligence and quantum computing**, by mandating quantum readiness and staying ahead of future threats from AI through the Australian AI Safety Institute. (Actions 2.3 and 5.3)
- **Protecting data that matters most** by classifying and securing datasets of national significance through a risk-based framework, reducing national security risk. (Action 2.2)


# Strong businesses, communities and citizens

## Six key actions under Horizon 2:

**1.1 Empower our workers as our first line of cyber defence, our 'human firewall'**

a. Build cyber awareness within Australia's workforce and supply chains.

**1.2 Make it easier for small and medium businesses, and the not-for-profit sector, to strengthen their cyber security**

a. Simplify cyber security for small and medium businesses and provide targeted and actionable support through a new CyberSmart program.
b. Drive cyber uplift and maturity for the not-for-profit sector.
c. Offer tailored advice to support small and medium businesses, not-for-profits and individuals

**1.3 Strengthen community cyber resilience**

a. Extend the reach and accessibility of our public cyber awareness messaging.
b. Empower diverse communities to grow their cyber awareness and build cyber confidence.
c. Uplift cyber security of our day-to-day digital activities by testing ways to make online security behaviours easier.

**1.4 Disrupt and deter cyber threat actors to protect Australians from cybercrime**

a. Build our law enforcement and offensive capabilities.
b. Shape international frameworks and cooperation on cybercrime.
c. Strengthen national ransomware information sharing and preparedness.

**1.5 Secure our identities and provide better support to victims of cybercrime**

a. Expand the adoption of Digital ID across government (the Australian Government, states and territories) and private sector services.

**1.6 Drive productivity for Australian businesses**

a. Harmonise and align cyber security regulation to reduce the compliance burden.

| Action | | Accountable agency |
|---|---|---|
| **1.1 Empower our workers as our first line of cyber defence, our 'human firewall'** | | |
| **Build cyber awareness within Australia's workforce and supply chains** | **Baseline strong cyber awareness practices for the Australian workforce and through supply chains** leveraging the public-private partnerships already in place, including the Executive Cyber Council established under Horizon 1.<br><br>Public resources will be developed through this process, including guidance about common terminology and concepts to be used when developing in-house cyber training resources, to provide a simple, coherent message on cyber awareness and hygiene for our workforce. | **Lead agency:**<br>• Home Affairs<br><br>**Contributing agencies:**<br>• AGD<br>• ASD<br>• DEWR<br>• Education<br>• Treasury |
| | **Introduce a minimum standard of cyber security training in ASD standards.** ASD will develop standards that require and guide the training of an organisation's people through the proposed ASD Essential Series for Enterprise IT. The standards will ensure an appropriate level of governance awareness and training for all staff that access an organisation's systems. | **Lead agency:**<br>• ASD<br><br>**Contributing agency:**<br>• Home Affairs |

| Action | Accountable agency |
|---|---|
| **1.2 Make it easier for small and medium businesses, and the not-for-profit sector, to strengthen their cyber security** | |
| **Simplify cyber security for small and medium businesses and provide targeted and actionable support through a new CyberSmart program** | **Develop a tailored cyber security standard and certification regime for small and medium businesses —CyberSmart—**that supports a simple, adaptable standard to help them increase their cyber resilience.<br><br>This initiative will be delivered through a Conformity Assessment Scheme, developed with the Joint Accreditation System of Australia and New Zealand, to provide a structured governance mechanism to verify whether an entity meets the standard required to be certified. Once certified, entities will be able to display a 'trust mark' in their communications with customers and suppliers.<br><br>**Safeguard critical infrastructure and government** by using the *Security of Critical Infrastructure Act 2018* and government procurement levers to promote uptake of the CyberSmart standard to ensure the cyber security of their supply chains. | **Lead agency:**<br>• Home Affairs<br><br>**Contributing agencies:**<br>• ASD<br>• Treasury |
| | **Create a dedicated, centralised CyberSmart Hub as a repository of resources for smaller entities,** including:<br><br>• resources about CyberSmart certification<br>• consolidated guidance from government<br>• service-specific and product-specific guidance to assist small businesses to choose the most suitable cyber products and services for their needs and skill profile.<br><br>Specific guidance on products and services for small businesses will be developed in close collaboration with technology vendors and service providers. This will enable ready comparison between products and services so that businesses can make informed decisions relevant to their operations. | **Lead agency:**<br>• Home Affairs<br><br>**Contributing agencies:**<br>• ASD<br>• Treasury |

| Action | | Accountable agency |
|---|---|---|
| **Drive cyber uplift and maturity for the not-for-profit sector** | **Facilitate greater sharing of cyber knowledge and resources across the not-for-profit sector** through establishing a collaborative not-for-profit community of practice. | **Lead agencies:**<br>• Home Affairs<br>• ACNC<br>**Contributing agencies:**<br>• ASD<br>• DSS |
| | **Deliver a program of services to support not-for-profit cyber uplift**. We will engage with the sector to build a capability assessment of current services and apply these findings to enhance existing cyber resources. | **Lead agencies:**<br>• Home Affairs<br>• ACNC<br>**Contributing agencies:**<br>• ASD<br>• DSS |
| **Offer tailored advice to support small and medium businesses, not for-profits and individuals** | **Enhance the Cyber Health Check Tool** for small and medium businesses and not-for-profits to provide targeted cyber security guidance. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• Treasury |
| **1.3 Strengthen community cyber resilience** | | |
| **Extend the reach and accessibility of our public cyber awareness messaging** | **Enhance the *Act Now. Stay Secure.* public education campaign**, by building on the achievements of this campaign under Horizon 1 to further translate awareness into action and ensure Australians develop consistent cyber secure habits that they use every day. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• AGD<br>• Finance |

| Action | | Accountable agency |
|---|---|---|
| **Empower diverse communities to grow their cyber awareness and build cyber confidence** | **Deliver tailored cyber education programs to support diverse cohorts and further engage priority communities** by continuing the Cyber Awareness Support for Vulnerable Groups grants program under Horizon 1. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• DSS Grants Hub |
| **Uplift cyber security of our day-to-day digital activities by testing ways to make online security behaviours easier** | **Develop new ways to encourage and enable safer online behaviours** through research to understand the real-world barriers that prevent Australians from taking effective security actions online, then design and test solutions that make cyber resilience easier in practice. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• PM&C (BETA) |
| **1.4 Disrupt and deter cyber threat actors to protect Australians from cybercrime** | | |
| **Build our law enforcement and offensive capabilities** | **Uphold our offensive cyber capabilities to investigate and disrupt cybercrime**, and ensure coordination of national responses to cybercrime, through Operation Aquila and the Joint Policing Cybercrime Coordination Centre. | **Lead agency:**<br>• AFP<br>**Contributing agencies:**<br>• ASD<br>• State and territory law enforcement agencies |

| Action | | Accountable agency |
|---|---|---|
| **Shape international frameworks and cooperation on cybercrime** | **Consider ratifying the United Nations Convention against Cybercrime** through prioritising multi-stakeholder participation modalities in the rules of procedure for the Conference of the States Parties and developing likeminded positions to shape the supplementary protocol negotiations. | **Lead agency:**<br>• DFAT<br>**Contributing agencies:**<br>• AGD<br>• Home Affairs<br>• AFP |
| | **Provide practical support to our regional partners to uplift cybercrime prevention capacity and capability in the Pacific,** including through the finalisation of the Cybercrime Legislation Implementation Handbook being developed by the Pacific Islands Law Officers' Network Cybercrime Working Group. | **Lead agency:**<br>• AGD<br>**Contributing agency:**<br>• DFAT |
| **Strengthen national ransomware information sharing and preparedness** | **Deliver public, annual ransomware threat reports and share actionable intelligence** with government and industry to enable the development of tailored tools, services and guidance that enhance our national ransomware response, including to support effective recovery from ransomware and cyber-extortion incidents. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• AFP<br>• AGD<br>• ASD<br>• Treasury |
| **1.5 Secure our identities and provide better support to victims of cybercrime** | | |
| **Expand the adoption of Digital ID across government (the Australian government, states and territories) and private sector services** | **Continue to grow the use of Digital ID to reduce the need for people to share sensitive personal information** when verifying identity, and the risks and impact of identity theft and fraud.<br>The government will continue to enable Digital ID as an option for more government services and efforts to incentivise use of Digital ID in the private sector to increase productivity, security and consumer protection. | **Lead agency:**<br>• Finance |

| Action | | Accountable agency |
|---|---|---|
| **1.6 Drive productivity for Australian businesses** | | |
| **Harmonise and align cyber security regulation to reduce the compliance burden** | **Review the cyber security regulatory environment to establish a clear picture of the regulatory pressure points impacting industry** and work across government, in partnership with industry, to identify opportunities to centralise cyber incident reporting, which may include harmonising and aligning key definitions, timeframes, reporting thresholds, information requirements and other mechanisms to reduce regulatory burden. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• Finance<br>• Treasury |
| | **Create a Single Cyber Incident Reporting Interface** in line with the Department of Finance's 'Tell Us Once' initiative to consolidate cyber incident reporting obligations into one user-friendly webform. This will be informed by the outcomes from the review of regulatory pressure points impacting industry. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• Finance<br>• Treasury<br>• Regulatory portfolios and agencies |

Shield 2

# Secure technology

## Three key actions under Horizon 2:

**2.1 Ensure Australians can trust their digital products and platforms**

a. Adopt a suitable regulatory posture to ensure the security of our digital technology.
b. Support Australians to make informed, secure choices about the technology they use.
c. Manage the national security risks associated with digital technology.

**2.2 Protect our most valuable assets**

a. Support best-practice data governance and security across the economy.
b. Protect our data sets of national significance.

**2.3 Prepare Australia to harness the benefits of emerging technology**

a. Position Australia as a world-leading manager of cyber security risks associated with emerging technologies.
b. Prepare government to respond to emerging technology risks.
c. Collaborate with industry on securing emerging technology.

| Action | | Accountable agency |
|---|---|---|
| **2.1 Ensure Australians can trust their digital products and platforms** | | |
| **Adopt a suitable regulatory posture to ensure the security of our digital technology** | **Co-design with industry a security standard for consumer-grade edge devices** (routers and modems) used in households and small businesses, in line with international partners and standards, under the *Cyber Security Act 2024*. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• ASD |
| | **Explore options to uplift the cyber security of internet-connected operational technology** used in industrial settings in Australia. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• ASD |
| | **Introduce new national road vehicle cyber security standards** consistent with obligations to harmonise with international vehicle regulations.<br>**Consider cyber security and privacy treatment** of connected vehicles, road infrastructure and associated data storage systems. | **Lead agency:**<br>• DITRDCSA<br>**Contributing agencies:**<br>• Home Affairs<br>• AGD<br>• OAIC<br>• ASD |
| | **Develop a national approach to designing cyber security for consumer energy resources** through the work being undertaken through the Consumer Energy Resources Roadmap. | **Lead agency:**<br>• DCCEEW<br>**Contributing agencies:**<br>• Home Affairs<br>• ASD |
| | **Track actions by international counterparts on security standards for consumer-grade smart devices** to ensure that Australian regulation aligns with international best practice and is fit-for-purpose. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• ASD |
| **Support Australians to make informed, secure choices about the technology they use** | **Continue to develop a national voluntary labelling scheme for the cyber security of smart devices**, aligned with international exemplars through the Global Cybersecurity Labelling Initiative and lessons learned from the pilot program established under Horizon 1. | **Lead agency:**<br>• Home Affairs |
| | **Establish a voluntary Code of Practice for internet service providers about the cyber security of edge devices** they provide or recommend to their customers as an interim measure whilst formal regulation of these devices is being co-designed with industry. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• ASD |

| Action | | Accountable agency |
|---|---|---|
| **Manage the national security risks associated with digital technology** | **Leverage Technology Vendor Risk Framework outcomes to inform regulation and advice** across government, critical infrastructure and industry. | **Lead agency:**<br>• Home Affairs |
| **2.2 Protect our most valuable assets** | | |
| **Support best-practice data governance and security across the economy** | **Uplift data security across the Australian economy** through:<br>• finalising and promoting uptake of the Industry Data Classification Framework, and<br>• developing a Code of Practice for commercial data transactions with industry, as an outcome of the Data Brokerage Review delivered under Horizon 1. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• OAIC<br>• AGD<br>• ASD<br>• DISR<br>• Finance<br>• Treasury |
| | **Drive whole-of-government adoption of the recommendations from the Data Retention Review**, communicating consistent application of data retention principles to legislation and improved industry guidance material. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• Finance<br>• OAIC |
| **Protect our data sets of national significance** | Partner with industry, universities and state and territory governments to **pilot a risk assessment framework for managing human genomic and clinical trial data**. This pilot will shape the production of practical guidance and promote voluntary, best-practice protections. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• AGD<br>• ASIO<br>• Defence<br>• DISR<br>• Finance<br>• Health |

| Action | | Accountable agency |
|---|---|---|
| **2.3 Prepare Australia to harness the benefits of emerging technology** | | |
| **Position Australia as a world-leading manager of cyber security risks associated with emerging technologies** | **Collaborate with trusted public and private partners on artificial intelligence threats** to identify and understand the national security risks of emerging technology. This includes leading the Five Country Ministerial Artificial Intelligence Working Group. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• DISR<br>• DAFF<br>• Health<br>• Defence<br>• DFAT<br>• National Intelligence Community agencies |
| | **Meet the national security challenges posed by quantum computing** by providing actionable guidance for both government and industry. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• National Intelligence Community agencies |

| Action | | Accountable agency |
|---|---|---|
| **Prepare government to respond to emerging technology risks** | **Assess the suitability of existing crisis management frameworks in responding to major artificial intelligence incidents**, including the Australian Government Crisis Management Framework and supporting legislation. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• DISR<br>• DTA<br>• NEMA<br>• PM&C<br>• Treasury<br>• Defence<br>• National Intelligence Community agencies |
| | **Prepare critical Australian systems for post-quantum cryptography** by:<br>• mandating transition planning through the Protective Security Policy Framework for Australian Government agencies, and<br>• strengthening critical infrastructure systems, including through regulatory levers under the *Security of Critical Infrastructure Act 2018*. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• DTA<br>• Treasury<br>• Defence<br>• National Intelligence Community agencies |
| | **Require cyber security planning in Digital Investment Plans** to set standards and timeframes for all Commonwealth agencies to build national resilience. | **Lead agency:**<br>• DTA<br>**Contributing agency:**<br>• Home Affairs |
| **Collaborate with industry on securing emerging technology** | **Build the Australian Government's visibility of artificial intelligence incidents in critical infrastructure** by working with regulators and industry to increase information sharing, leveraging existing forums and structures, such as the Trusted Information Sharing Network. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• DISR |

Shield 3

# World-class threat sharing and blocking

## Two key actions under Horizon 2:

**3.1 Create a whole-of-economy threat intelligence network**

a. Expand tactical and operational threat intelligence sharing.

**3.2 Scale threat blocking capabilities to stop cyber attacks**

a. Enable greater uptake of threat blocking activities across the economy.
b. Empower industry to harden and defend networks against threats to better protect end users

| Action | | Accountable agency |
|---|---|---|
| **3.1 Create a whole-of-economy threat intelligence network** | | |
| **Expand tactical and operational threat intelligence sharing** | **Evaluate the Health Cyber Sharing Network launched in Horizon 1** and identify further sectors of the economy that would benefit from Information Sharing and Analysis Centres. | **Lead agency:**<br>• Home Affairs |
| | **Publish a Vulnerability Disclosure Policy Toolkit to support the hardening of systems before vulnerabilities are exploited** and to lessen the burden of large organisations developing a policy from scratch. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• AFP |
| **3.2 Scale threat blocking capabilities to stop cyber attacks** | | |
| **Enable greater uptake of threat blocking activities across the economy** | **Enhance legislative and policy levers to ensure entities, such as telecommunication providers and others 'upstream' from our digital interfaces, can block at scale and speed** to better defend those who cannot defend themselves.<br><br>To increase the update of threat blocking activities across the ecosystem, **identify a national opt in threat blocking pilot,** including whether legislation is required to enact. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• AFP<br>• AGD<br>• ASD<br>• DITRDCSA |

| Action | | Accountable agency |
|---|---|---|
| **Empower industry to harden and defend networks against threats to better protect end users** | **Publish a public statement clarifying the permissible cyber defence activities industry can undertake in Australia.** This will provide a framework for industry to harden systems as business-as-usual, and to react and defend their own networks effectively and with confidence. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• AFP |
| | **Assess legislation and policy to ensure industry and the Australian Government can collaborate at speed on defensive cyber measures** (including threat blocking) and address impediments. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• AFP |

Shield 4

# Protected critical infrastructure

## Three key actions under Horizon 2:

**4.1 Harden Australia's critical infrastructure**

a. Uplift the cyber security of Australia's critical infrastructure.
b. Protect Australia's foundational cyber infrastructure.

**4.2 Uplift cyber security of the Australian Government**

a. Mature the government's cyber security baseline.
b. Prioritise the protection of our most critical digital services.
c. Strengthen cyber resilience through more targeted government investment.

**4.3 Drive greater collaboration and coordination across all levels of government**

a. Promote the expansion of coordination and support across jurisdictions to uplift cyber security policy alignment.

| Action | | Accountable agency |
|---|---|---|
| **4.1 Harden Australia's critical infrastructure** | | |
| **Uplift the cyber security of Australia's critical infrastructure** | **Explore options to reform the *Security of Critical Infrastructure Act 2018***, including amendments to Ministerial Directions powers (Part 3) and enhancements to the Critical Infrastructure Risk Management Program requirements for high-risk asset classes to provide greater agility and precision in responding to emerging threats. | **Lead agency:**<br>• Home Affairs |
| | **Enhance the security and resilience of Australia's most critical infrastructure** through continued engagement, partnership and information sharing between government and industry. | **Lead agency:**<br>• Home Affairs |
| | **Support Systems of National Significance organisations to be compliant with their Enhanced Cyber Security Obligations** and provide targeted insights on incident response planning and cyber security exercising to uplift industry preparedness. | **Lead agency:**<br>• Home Affairs |
| | **Develop a whole-of-government and critical infrastructure drones security policy** to prevent, investigate and penalise drone misuse where it presents a security threat. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• DITRDCSA |

| Action | | Accountable agency |
|---|---|---|
| **Protect Australia's foundational cyber infrastructure** | **Undertake an assessment of Australia's current subsea cable protections** to support Australian Government decision making and prioritisation of future actions to strengthen the security and resilience of Australia's subsea cable infrastructure. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• DITRDCSA |
| **4.2 Uplift cyber security of the Australian Government** | | |
| **Mature the government's cyber security baseline** | **Strengthen cyber fluency of Australian Public Servants** in non-information technology specialist roles through foundational resources to support cyber security practice across the Australian Government. | **Lead agency:**<br>• APSC<br>**Contributing agencies:**<br>• Home Affairs<br>• ASD<br>• Defence<br>• DTA |
| | **Adapt existing cyber security policy requirements** to better identify emerging and contemporary cyber security risks and improve visibility within government. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• ASD |
| | **Strengthen procurement arrangements for information and technology goods and services** to uplift cyber security across the Australian Government. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• Finance<br>• DTA<br>• ASD |
| **Prioritise the protection of our most critical digital services** | Target legacy technology risk reduction for Systems of Government Significance by **establishing the legacy technology baseline for critical systems and prioritising remediation** to enhance the Commonwealth's cyber security, resilience and continuity of services. | **Lead agencies:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• DTA |
| | **Strengthen preparedness and capability through the development of incident playbooks and tabletop simulations** for Systems of Government Significance to test decision-making, coordination and incident response arrangements in a controlled environment. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency**<br>• ASD |

| Action | | Accountable agency |
|---|---|---|
| **Strengthen cyber resilience through more targeted government investment** | Building on the foundations established through Horizon 1, **strengthen and refine the critical indicators that guide cyber security investment**, ensuring funding is systematically prioritised toward the highest areas of risk and delivers demonstrable, measurable uplift in security posture. | **Lead agencies:**<br>• Home Affairs<br>• DTA |
| **4.3 Drive greater collaboration and coordination across all levels of government** | | |
| **Promote the expansion of coordination and support across jurisdictions to uplift cyber security policy alignment** | **Design a National Cyber Security Compact** to enable all levels of government in Australia to collaborate on cyber security initiatives and escalate key issues at a national level. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• ASD |

Shield 5

# Sovereign capabilities

## Three key actions under Horizon 2:

**5.1 Enhance our proactive cyber security posture at a national level**

a. Conduct national cyber security exercises across the economy.

**5.2 Grow and professionalise our national cyber workforce**

a. Foster cyber security as a national security profession.

**5.3 Accelerate our local industry, research and innovation**

a. Invest in domestic cyber industry growth.
b. Support Australia to have the secure computing power needed to take advantage of emerging technology.

| Action | | Accountable agency |
|---|---|---|
| **5.1 Enhance our proactive cyber security posture at a national level** | | |
| **Conduct national cyber security exercises across the economy** | **Strengthen the National Office of Cyber Security Exercise Program by hosting multiple cross-sector exercises** incorporating industry sectors and government departments, including Systems of Government Significance (see Action 4.2), and sectors of Australian industry and critical infrastructure not previously targeted. Identification of supply chain dependencies and delivery of scalable and targeted readiness activities will support improved preparedness across the Australian economy where it is needed most. | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• ASD<br>• NEMA |
| **5.2 Grow and professionalise our national cyber workforce** | | |
| **Foster cyber security as a national security profession** | **Explore the feasibility of a national rollout of a national framework for the professionalisation of the cyber workforce,** following a review of the pilot program commenced under Horizon 1 (to be finalised in June 2027). | **Lead agency:**<br>• Home Affairs<br>**Contributing agencies:**<br>• DEWR<br>• Education<br>• DISR Business Grants Hub |

| Action | | Accountable agency |
|---|---|---|
| **5.3 Accelerate our local industry, research and innovation** | | |
| **Invest in domestic cyber industry growth** | **Sustain our support for cyber start-ups and small-to-medium enterprises** to develop innovative solutions to cyber security challenges.<br><br>This initiative will build on our work under Horizon 1 through the Cyber Security Industry Challenge program under the Business Research and Innovation Initiative. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• DISR |
| **Support Australia to have the secure computing power needed to take advantage of emerging technology** | Following the National Artificial Intelligence Plan launched in December 2025, **establish expectations of data centres and AI infrastructure developers in partnership with states and territories** to clarify what it looks like for investment in data centres to align with Australia's overall national interests.<br><br>This initiative will be delivered by the Australian AI Safety Institute. | **Lead agency:**<br>• DISR<br>**Contributing agencies:**<br>• ASD<br>• Whole-of-Government<br>• State and territory government agencies |

# Shield 6 Resilient region and global leadership

## Two key actions under Horizon 2:

**6.1 Support a cyber-resilient region as the partner of choice**

a. Strengthen collective cyber resilience with neighbours in the Pacific and Southeast Asia.
b. Harness private sector innovation and expertise in the region.

**6.2 Shape, uphold and defend international cyber rules, norms and standards**

a. Enhance collaboration on counter-ransomware activities globally.
b. Advocate for high-quality digital trade rules.
c. Defend an open, free, secure and interoperable internet in international forums.
d. Uphold international laws and norms of responsible state behaviour in cyberspace.
e. Deploy all arms of statecraft to deter and respond to malicious actors.

| Action | | Accountable agency |
|---|---|---|
| **6.1 Support a cyber-resilient region as the partner of choice** | | |
| **Strengthen collective cyber resilience with neighbours in the Pacific and Southeast Asia** | **Continue Australia's regional cyber cooperation efforts** under the Southeast Asia and Pacific Cyber Program (SEA-PAC Cyber). | **Lead agency:**<br>• DFAT<br>**Contributing agencies:**<br>• AFP<br>• AGD<br>• ASD<br>• eSafety |
| | **Continue our regional cyber crisis response team in the Pacific**, including supporting regional events, prioritising Pacific-led Security Operations Centres, in line with our framework on when and how to deploy our limited resources across the region. | **Lead agency:**<br>• DFAT<br>**Contributing agencies:**<br>• Various agencies, including ASD |
| **Harness private sector innovation and expertise in the region** | **Maintain our pilots of technology solutions to protect the Indo-Pacific region at scale** by partnering with our regional neighbours and the private sector to leverage industry solutions to protect more people, systems and data from cyber threats. | **Lead agency:**<br>• DFAT<br>**Contributing agency:**<br>• ASD |

| Action | | Accountable agency |
|---|---|---|
| **6.2 Shape, uphold and defend international cyber rules, norms and standards** | | |
| **Enhance collaboration on counter-ransomware activities globally** | **Establish a global ransomware standards framework through the Counter Ransomware Initiative** for members to act on the policy approaches, legislative levers and strategies required to galvanise against ransomware risk. | **Lead agency:**<br>• Home Affairs<br>**Contributing agency:**<br>• DFAT |
| | **Enhance information sharing between Counter Ransomware Initiative members** through improvements to the website and online members portal. | **Lead agency:**<br>• Home Affairs |
| **Advocate for high quality digital trade rules** | **Advocate for digital trade rules** that advance our economic interests, complement international cyber security settings and reinforce the rules-based trading system. | **Lead agency:**<br>• DFAT<br>**Contributing agencies:**<br>• Whole-of-Government |
| **Defend an open, free, secure and interoperable internet in international forums** | **Continue to defend an open, free, secure and interoperable internet in international forums** by working with international partners, industry, academia, the technical community, civil society and other relevant stakeholders. Government will advocate for continuing, consensus-based improvements to existing mechanisms of multi-stakeholder internet governance. | **Lead agency:**<br>• DITRDCSA<br>**Contributing agencies:**<br>• Whole-of-Government |
| **Uphold international laws and norms of responsible state behaviour in cyberspace** | **Uphold and improve the framework for responsible state behaviour in cyberspace**, including how existing international law applies and best practice implementation of norms, through the new permanent United Nations Global Mechanism on Cyber. | **Lead agency:**<br>• DFAT<br>**Contributing agencies:**<br>• AGD<br>• Defence<br>• Home Affairs |
| **Deploy all arms of statecraft to deter and respond to malicious actors** | **Continue increasing costs for malicious cyber actors** by working with international partners to deter and respond to malicious cyber activity. This includes continuing to publicly attribute malicious activity to, and impose sanctions on, those who carry out or facilitate significant cyber incidents, when we have sufficient evidence and it is in our interests to do so. | **Lead agency:**<br>• DFAT<br>• Home Affairs<br>**Contributing agencies:**<br>• AFP<br>• AGD<br>• ASD |

# Appendix A: Lead and contributing agency abbreviations

| | |
|---|---|
| ACNC | Australian Charities and Not-for-profit Commission |
| AFP | Australian Federal Police |
| AGD | Attorney-General's Department |
| APSC | Australian Public Service Commission |
| ASD | Australian Signals Directorate |
| ASIO | Australian Security Intelligence Organisation |
| BETA | Behavioural Economics Team of the Australian Government (within PM&C) |
| DAFF | Department of Agriculture, Fisheries and Forestry |
| DCCEEW | Department of Climate Change, Energy, the Environment and Water |
| Defence | Department of Defence |
| DEWR | Department of Employment and Workplace Relations |
| DFAT | Department of Foreign Affairs and Trade |
| DISR | Department of Industry, Science and Resources |
| DITRDCSA | Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts |

| | |
|---|---|
| DSS | Department of Social Services |
| DTA | Digital Transformation Agency |
| Education | Department of Education |
| eSafety | Office of the eSafety Commissioner |
| Finance | Department of Finance |
| Health | Department of Health, Disability and Ageing |
| Home Affairs | Department of Home Affairs |
| NEMA | National Emergency Management Agency |
| OAIC | Office of the Australian Information Commissioner |
| PM&C | Department of the Prime Minister and Cabinet |
| Treasury | Department of the Treasury |