Australian Government

# 2025 Review

# Transition from Horizon 1 to Horizon 2

## 2023–2030 Australian Cyber Security Strategy

**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

Australian Government

# 2025 Review

## Transition from Horizon 1 to Horizon 2

2023–2030 Australian Cyber Security Strategy

# Table of contents

# Executive Summary

The 2025 Review provides a whole-of-strategy assessment of how the 60 initiatives delivered under Horizon 1 of the 2023-2030 Australian Cyber Security Strategy (the Strategy) have strengthened Australia's cyber resilience since 2023. Across government, business, civil society and international partners, the Review finds strong early progress, clear evidence of impact and a solid foundation as we shift to Horizon 2.

## Shield 1—Strong Businesses and Citizens

*Helping Australians and small businesses protect themselves, respond effectively, and reduce the impact of cyber incidents.*

- **Building cyber awareness:** Millions of Australians have heard our cyber safety messages under the '*Act Now. Stay Secure.*' campaign and are now taking simple, effective protective actions that reduce their chance of falling victim to cybercrime. These behaviour shifts materially reduce the national attack surface by helping Australians adopt practical steps—like multi-factor authentication—that stop cyber incidents before they occur.
- **Scaling support for small entities:** Over 3,300 businesses engaged with the Cyber Health Check Tool in the first month alone following its launch. This early engagement empowered thousands of small businesses and not-for-profits to recognise where they were vulnerable and understand the practical steps they could take to strengthen their cyber defences. By providing accessible, tailored maturity assessments, we are helping close the resource and expertise gap for the small entities that account for nearly 80% of business losses from cyber incidents.
- **Localized resilience for vulnerable groups:** The Government provided $7 million in grants to over 200 community organisations to deliver tailored cyber security advice to priority groups, including First Nations and regional communities. This enabled more than 200 trusted community-led organisations to translate cyber-security guidance into culturally relevant, accessible support that met people where they are. By leveraging these trusted voices, we are closing the resilience gap for Australians most at risk but often hardest to reach.
- **Protecting identity and reducing social harm:** 120,000 victims received tailored recovery support through IDCARE, and more than 15 million Digital IDs, provided via myID, were used to securely access government services. This support and increased use of Digital ID have helped people quickly regain control of compromised identities while dramatically reducing how often people need to share sensitive information—preventing millions from ever facing that risk in the first place. Together, these measures reduce the social and financial harms of identity theft and ensure Australians can 'bounce back' quickly when incidents occur, maintaining confidence in the digital economy.

- **Neutralising high-impact criminality:** Operation Aquila conducted 38 disruptions against major ransomware groups like LockBit, contributing to international takedowns and sanctions. These disruptions undermined the infrastructure, finances and anonymity that cybercriminals rely on, helping entities avert imminent attacks and recover without capitulating to extortion. By increasing the operational costs and risks for ransomware syndicates, Australia is making itself—and its partners—a harder and less profitable target for organised cybercrime.

## Shield 2—Safe Technology

*Ensuring Australians can trust the technology they use through secure-by-design products, better standards, and reduced systemic risk.*

- **Securing technology Australian's use every day:** Australia's Cyber Security Act 2024 and the *Cyber Security (Security Standards for Smart Devices) Rules 2025* mandate a secure-by-default baseline for consumer smart devices. This moves responsibility from individual users to the companies best placed to manage risk, ensuring millions of connected products entering Australian homes and businesses are no longer a weak link. As a result, Australians can trust their devices to be safer out-of-the-box, lifting national resilience without relying on users to be security experts.
- **Helping consumers make cyber secure purchases:** Home Affairs is partnering with industry to develop a voluntary Labelling Scheme for Smart Devices. The scheme will harness consumer transparency to reward manufacturers that invest in stronger security. By letting buyers easily compare security, Australians will be able to make more informed purchasing decisions. We are already seeing strong industry support for the scheme, which will give reputable manufacturers a competitive edge beyond price. This market signal aims to lift the baseline security of the entire smart device ecosystem, improving security for households and small businesses at scale.
- **Hardening digital gatekeepers through global alignment:** Australia's new App Store Code of Practice lifts security standards for the platforms Australians rely on every day. This means apps that Australians download for banking, healthcare and communication are safer before they ever reach their devices. This added protection reduces the risk of malicious or unsafe apps compromising personal data, giving Australians greater confidence that the digital services they depend on are secure-by-default. The new Code of Practice has been modelled closely on the Code developed by the UK Government, ensuring alignment with key jurisdictions.
- **Proactive supply chain risk management:** The Technology Vendor Review Framework gives government a coordinated, whole-of-system way to assess and mitigate vendor-related security risks across hardware and software. By identifying systemic vulnerabilities before high-risk technology is embedded in critical systems, it shifts Australia from reactive fixes to proactive risk control. That foresight helps keep essential services and sensitive data safer, while supporting timely, consistent, and proportionate procurement decisions across the economy.

## Shield 3—World-Class Threat Sharing and Blocking

*Creating a national network that shares and blocks threats at scale, in real time.*

- **Disrupting cyber threats upstream:** The Australian Signals Directorate's sharing platform has distributed nearly 3 million indicators of compromise to 450 partner organisations. This machine-to-machine exchange allows partners to block malicious infrastructure in near real time, stopping threats before they can reach end users. By shifting Australia from reactive response to a proactive posture, this uplift will materially reduce the volume of attacks able to impact businesses and households.
- **Partnering with industry and cyber experts:** Since its inception in September 2023, the National Cyber Intel Partnership has convened industry leaders and cyber experts to promote the exchange of technical indicators and best practices, leading to the development of a threat blocking capability scheme. The Partnership's achievements in Horizon 1 include optimising processes for intelligence sharing, scaling threat blocking activities, and integrating government and industry capabilities to protect end users.
- **Encouraging industry-sectors to establish threat sharing centres:** The establishment of the Health Cyber Security Network, now with 60 members, covering over 600 health facilities, has created a dedicated threat-sharing hub for a sector holding Australia's most sensitive personal data. Members report that high-quality, Australian-specific intelligence—including timely advisories developed through sovereign capability as geographical shifts place global cyber infrastructure under increasing uncertainty—has enabled them to patch vulnerabilities faster and identify systemic gaps previously invisible at an individual-entity level. This marks a critical shift from isolated defences to a collective resilience model.

## Shield 4—Protected Critical Infrastructure

*Ensuring essential systems can withstand and recover from cyber attacks.*

- **Hardening essential services:** Major *Security of Critical Infrastructure Act 2018* reforms and enhanced obligations for Systems of National Significance now require owners and operators of critical infrastructure to identify, mitigate and manage cyber risks that could disrupt services Australians rely on every day. That means the essential systems Australians need to keep the lights on, water running and phones connected, are tougher targets and more likely to stay up when trouble hits.
- **National preparedness:** With 97% of exercise participants reporting meaningful preparedness insights, the National Cyber Exercise Program has strengthened whole-of-nation readiness by identifying critical gaps. The delivery of 12 sector-specific incident response playbooks has made it clear who does what in a cyber crisis. When an attack comes, this rehearsal and clarity will help Australia bounce back faster, so people get the services they need sooner.
- **Protecting Systems of Government Significance:** The Government requires greater visibility of its critical digital functions and systems to prioritise their protection and defence, to prevent catastrophic impacts to the nation. The Systems of Government Significance Regime launched in July 2025, with 4 tranches to be finalised by mid-2026.
- **Mitigating aviation and maritime cyber risks:** The ability for Government to set minimum cyber security requirements for the aviation and maritime sectors will help to ensure these sectors appropriately mitigate cyber risks posed by state-sponsored actors, cyber-criminal threat actors and human error. The first step in achieving this objective was the Royal Assent in March 2025 of the *Transport Security Amendment (Security of Australia's Transport Sector)*

*Act 2025* (TSA Act). The TSA Act introduced an all-hazards security framework which through regulations will set minimum standards for Industry Participants to meet all hazard security obligations, including cyber security.

## Shield 5—Sovereign Capabilities

*Growing and professionalising the national cyber workforce and industry.*

- **Securing a skilled workforce:** CyberPath: Paving the Way Forward for Cyber Professionals, within the Growing & Professionalising Cyber Security Industry Pilot Program, will co-design (with industry) and pilot a Cyber Security Professionalisation Scheme and recommend standards. CyberPath will help provide clear career, skills and education pathways for workers in, and those seeking to enter, the cyber security workforce; and provide industry with guidance regarding skills expectations. Targeted migration reforms will help Australia bring in international talent.
- **Accelerating local innovation:** The Cyber Security Strategy Challenge Grant drew 59 submissions from Australian start-ups and small businesses, with over $400,000 awarded for feasibility projects. This funding lets local firms design and test real solutions to national security needs, building home-grown tools we can trust.
- **Strengthening industry-led workforce leadership:** The Executive Cyber Council's working group ran a Cyber Workforce Summit and created a Cyber Workforce Playbook so employers have practical steps to hire, keep and grow cyber talent. This industry push is helping build a ready, sustainable workforce that can keep pace with emerging threats.
- **Embedding diversity and inclusion in the cyber profession:** Home Affairs and the Government's behavioural insights team released Inclusive Cyber Security Recruitment Guidance to help support organisations of all sizes to attract and recruit women, First Nations people and neurodiverse candidates. The Guidance provides simple, low cost, evidence-based actions recruiters and employers can take to attract and recruit more inclusively.

## Shield 6—Resilient Region and Global Leadership

*Strengthening regional resilience and shaping global norms and standards.*

- **Reinforcing regional stability**: The Cyber Rapid Assistance for Pacific Incidents and Disasters (RAPID) capability under the Southeast Asia and pacific (SEA-PAC) Cyber Program delivered 12 RAPID deployments with a 4.6/5 impact rating by cyber incident response recipients in 2023. These deployments gave Pacific partners timely, hands-on support to restore critical systems during major cyber incidents and identify and mitigate vulnerabilities for long-term resilience. As the partner of choice in the Indo-Pacific, Australia is lifting the collective resilience of our region, supporting shared security, and countering the influence of non-trusted actors who seek to exploit cyber vulnerabilities for financial and geostrategic gain.

  DFAT's SEA-PAC Cyber Exercising Program has also delivered 16 cyber incident preparedness and response table-top exercises with Southeast Asian partners. By supporting partners to prepare themselves for responding to cyber incidents, countries are better able to get their systems back online following disruption, minimising the impacts on their governments, economy, people, and the region.

- **Upholding a rules-based global cyberspace:** Australia's leadership at the United Nations was pivotal in securing the continuation of multi-stakeholder internet governance and the establishment of a new permanent UN Global Mechanism on cyber. Australia helped hold the line against competing state-centric models of digital control, ensuring that norms, standards and internet governance structures remain open, inclusive and grounded in international law. By reinforcing these global rules and governance frameworks, Australia is preserving a free, secure and interoperable digital environment that underpins regional stability and protects the global operating space for Australian businesses.

## Shaping Horizon 2

Horizon 1 laid strong foundations for Australia's strengthened cyber resilience, giving us the national frameworks, partnerships and protections needed to confront a rapidly evolving threat environment. Building on that base, we developed the Horizon 2 initiatives through an evidence-driven assessment of how Australia's cyber risks are changing as our digital footprint expands and frontier technologies like artificial intelligence increase the speed and scale of attacks.

Our analysis of the digital environment where Australians increasingly spend much of their lives has highlighted how critical vulnerabilities have expanded over Horizon 1 with technological and social change.

- The estimated cost of cyber incidents to the Australian economy is $25 billion per year.
- The average self-reported cost of cybercrime for Australian businesses increased 50% year on year in 2024-25 to $80,000.[1]
- A single 4-week catastrophic cyber incident could wipe out $35 billion from the Australian economy, approximately 1.3% of GDP.[2]
- Human error contributes to 60% of breaches, reinforcing the need to strengthen the human firewall with practical, workplace-centred capability.[3]

To focus Horizon 2 initiatives on what matters most, we sought to co-design policy initiatives with industry through a series of public engagements involving more than 170 written submissions, 3 public town halls, 12 co-design roundtables, live impact polls and formal evaluation data. This process clarified where current settings are effective, where capability gaps persist and where government-industry collaboration must deepen.

The Government has now released an Action Plan for Horizon 2, outlining how it is scaling-up cyber maturity through further investments across the broader cyber ecosystem.

1. Australian Signals Directorate Australian Cyber Security Centre (2025), Annual Cyber Threat Report 2024-2025 (p. 3)
2. Australian Institute of Criminology (2025), The cost of espionage (p. 37).
3. Verizon (2025), 2025 Data Breach Investigations Report (p. 11).

# Introduction

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

The Strategy called for a new era of collaboration between industry and Government to keep Australia's digital frontier safe, secure and prosperous. 2 years into this journey, we are seeing significant momentum across a range of cyber reforms, programs and initiatives.


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

**Figure 1. Cyber shields**

The Strategy is structured around 6 'cyber shields' to help defend our citizens and businesses from cyber threats and to take economic and productivity opportunities that cyber security offers Australia.

## Commitment to ongoing review and adaptation

Acknowledging the fast-evolving nature of cyber security and the changing threat landscape, the Strategy established a phased approach to delivery through Action Plans across 3 time-horizons. The points between each Horizon provide the opportunity to reflect on what has been achieved and inform policy development for subsequent Horizons.


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

**Figure 2. Action Plan horizons**

This *2025 Review* report (Review Report) fulfills the commitments in the Strategy and the Horizon 1 Action Plan to ongoing review and the robust evaluation of the progress of initiatives and the overall strategy. Government publicly committed via the Strategy to actively monitor progress to 'ensure we remain on track' and can 'adjust our plan in response to new threats or emerging technologies'. This included reviews of the Action Plan 'with actions being updated, added, or removed as required'. These review and monitoring activities are to be informed by feedback from industry and community leaders, threat intelligence, and the lessons learnt from cyber incidents.

## Review goals

This Review Report achieves the following goals.

1. Detail how all 60 initiatives in the Horizon 1 Action Plan have delivered on intent, on time and on budget.
2. Highlight the impact of those initiatives that are sufficiently mature.
3. Outline what has been learnt during Horizon 1 to inform policy development for Horizon 2, including via feedback from stakeholders during extensive consultation.

# Approach

This Review Report has focused on the following types of evaluation as per the Commonwealth Evaluation Toolkit (Figure 3).

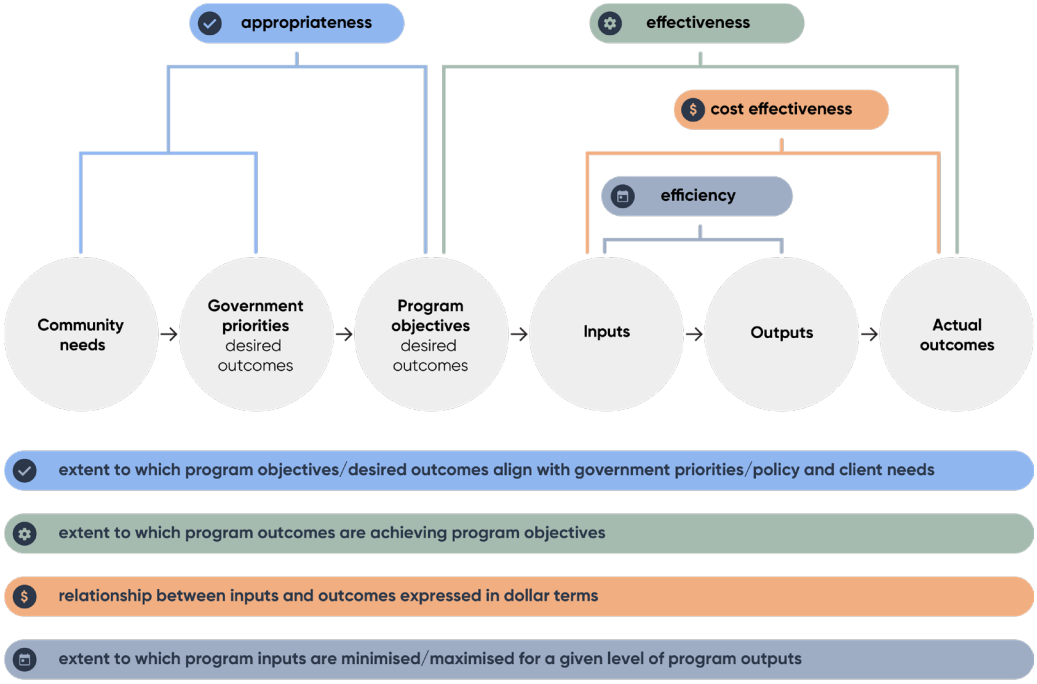


**Figure 3. Commonwealth Evaluation Toolkit: Evaluation Objectives**

## 1. Performance and efficiency

Across all 60 initiatives under Horizon 1, the focus has been on delivering on intent, on time and on budget. This is a key performance metric of government and key to efficiency.

By using internal expertise for the 2025 Review, the cost of this review and any subsequent reviews will be minimised. We have focused our efforts on developing a world-leading, and Australian Public Service-leading, governance and monitoring approach.

## 2. Effectiveness

Implementation of initiatives over Horizon 1 has been staggered, with many in early stages of maturity or undergoing additional execution and co-design. However, a handful of initiatives are sufficiently mature to have started formal evaluations or review processes during Horizon 1 (see 'Review activities'). Additionally, many initiatives have been collecting a range of qualitative and quantitative data to monitor effectiveness during implementation.

As a result, they have been able to assess and report on effectiveness—that is, whether the desired outcomes have been or are likely to be achieved—in the initiative-level analyses in the later part of this report.

This information has been supplemented by polls undertaken with industry stakeholders during the Horizon 2 co-design workshops and roundtables (see 'Review activities'). Stakeholders were asked to provide their perspectives on which activities in Horizon 1 had the biggest positive impact on Australia's cyber security and which are yet to realise the expected impact.

The challenge for reviews of strategies is that, at any given point in time, different initiatives will be at different stages of maturity. There is no one point in time when they are all 'finished' and simultaneously ready to be evaluated.

In line with the components of the Commonwealth Evaluation Toolkit evaluation objectives (Figure 3), this Review articulates for each shield:

- the desired outcomes (as set out in the Strategy)
- inputs and outputs (i.e. resources, actions and interventions expected to achieve the outcomes as set out in the Horizon 1 Action Plan), and
- the outcomes achieved or expected to be achieved and what has been learnt, both during implementation so far, and consultation feedback from stakeholders.

As per the intent of these regular reviews as set out in the Horizon 1 Action Plan, this information has then been used to inform policy development for Horizon 2. The relationship between the actions and outcomes and the 2 types of Strategy documents are set out in Figure 4 below.

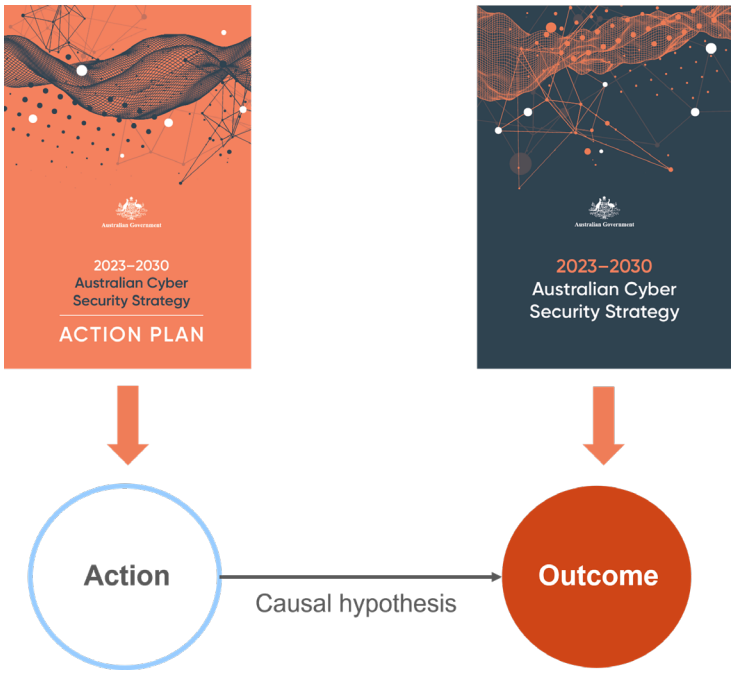


**Figure 4. Relationship between the Action Plan, Strategy, and program monitoring**

### 3. Appropriateness

During Horizon 1 the Department of Home Affairs tested the Strategy's intended outcomes with stakeholders, as articulated in a Strategic Outcomes Model (discussed further on page 16). This consultation included the Horizon 2 discussion paper and public submission process, a dedicated public town hall, and a small co-design roundtable. The high levels of support obtained from stakeholders confirmed the appropriateness of the desired outcomes (i.e. that community needs have been translated into government priorities and program objectives (as per Figure 3)).

## Review activities

The Review was undertaken via the following activities.

### Public discussion paper and submission process

On 29 July 2025, the Department of Home Affairs publicly released the Horizon 2 discussion paper titled *Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (Horizon 2 Discussion Paper).[4]

Over 170 submissions were received from individuals, industry, academia and the not-for-profit sector.

The submissions informed the third town hall summarising 'what we heard' (see below), the focus of co-design workshops and roundtables (also below), and policy development for Horizon 2.

### Three public online town halls

The Department hosted 3 public online town halls:

- 5 August 2025: Overview of the consultation process and discussion paper
- 21 August 2025: Cyber Security Strategic Outcomes Model
- 6 November 2025: Outcomes from the discussion paper and co-design process (i.e. what we heard)

There were over 100 participants at each town hall. As an indication of participant representation, the 21 August town hall included participants from small and medium businesses (18%), large businesses (36%), peak bodies (9%), academia (6%), and government (27%).

Video recordings of the town halls were shared on the Department's consultation website.

### 12 online co-design workshops or roundtables

A dozen co-design workshops and roundtables were hosted during the main consultation period (July-December 2025).

These events were generally 1.5 hours long and included around 30-40 participants from a range of sectors, depending on the topic. What we heard in these sessions was summarised and shared publicly during the 6 November town hall and is incorporated into this report, including in the Stakeholder Insights pop-out boxes.

4. Department of Home Affairs (2025), Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy.

### Ad hoc and bilateral consultation

Alongside the discussion paper, town halls, workshops and roundtables, a range of additional consultation activities were undertaken through ad hoc and bilateral meetings with stakeholders. These included regular meetings and presentations at conferences and events.

### Horizon 1 impact polls in co-design workshops

Live polls were conducted during the co-design workshops and roundtables to ascertain participant perspectives on the impact of Horizon 1.

The results are summarised in the Appendix and incorporated into the report analysis.

### Initiative-level formal evaluations or reviews

The initiatives listed below have undertaken or are planning formal evaluations or reviews. The details are provided within the analysis for each initiative or within an Evidence Use Showcase pop-out box.

- *Act Now. Stay Secure.* campaign ongoing evaluation (initiative 2a, p.23)
- Executive Cyber Council review (11a, p. 44)
- *SOCI Act* compliance monitoring and evaluation plan (14b, p. 54)
- Inclusive Cyber Security Recruitment Guidance (17b, page 62)
- SEA-PAC Monitoring, Evaluation, and Learning system (19a, p. 66)

### Capturing feedback, data and evidence during implementation

As well as these broad and formal feedback and evaluation processes, feedback, data and evidence were captured during initiative implementation. This included, for example, ongoing routine and ad hoc meetings, administrative data collection, surveys, research activities, and public reports (e.g. by the Australian Signals Directorate, the Australian Institute of Criminology, industry and think tanks).

## Report Structure

The remainder of the report sets out the review findings at the whole-of-strategy level, followed by the initiative-level grouped by shield.

Each section is structured to follow the pattern set by the Commonwealth Evaluation Toolkit strategic objectives framework (Figure 3). That is, they set out the links between desired outcomes → inputs → outputs → realised outcomes.

# Whole-of-strategy achievements: Building strong foundations

**Desired Outcomes: From the Strategy (p. 6)**

**By 2030, Australia will be a world leader in cyber security.**

We envisage a future where stronger cyber defences enable our citizens and businesses to prosper, and to bounce back quickly following a cyber attack.

**Key inputs**: During Horizon 1, over 30 Australian Government agencies worked together to achieve the outcomes set out in the Strategy across 60 initiatives through an initial commitment of $586.9 million.

**Outputs and realised outcomes**: The key deliverables in Horizon 1 at a whole-of-strategy level and their outcomes are outlined in the next 4 sections, including:

1. a strong foundation of program governance and assurance was established to ensure that all 60 initiatives delivered on intent, on time and on budget
2. strong collaboration between government and industry drove positive impact
3. early indications that Australia is well positioned to reach the overarching strategy goal of becoming a world leader in cyber security by 2030, and
4. the positive feedback received on the Strategic Outcomes Model that provides the base for strategy level, outcomes-orientated monitoring into Horizon 2 and beyond.

**Strong foundations of program governance and assurance**

In line with the three-tiered horizon approach (Figure 2), Horizon 1 focused on creating strong foundations of sound governance and program assurance.

The Executive Cyber Council provided a forum for ongoing collaboration with industry and other major stakeholders. The National Cyber Security Coordinator directed responses to significant cyber incidents, anticipation and mitigation activities, and whole-of-government cyber security uplift. The Government collaborated with its state and territory counterparts through the National Cyber Security Committee. Australian Government interdepartmental committees were established at the Senior Executive Service Band 1 and Band 3 levels to ensure cross-portfolio collaboration and coordination. Coordinated governance was also supported by a Cyber Security Strategy Program Management Office hosted by the Department of Home Affairs.

This ensured ongoing delivery (Figure 5) on the intent of all 60 initiatives, on time and budget, as set out in this Review Report.

**Strong collaboration between government and industry drove positive impact**

Several co-design and roundtable participants reported that the collaboration between industry and government had one of the biggest positive impacts on improving Australia's cyber security during Horizon 1.[5] This view was also shared in many submissions to the Horizon 2 discussion paper.

5. See the Impact Poll results in the Appendix.

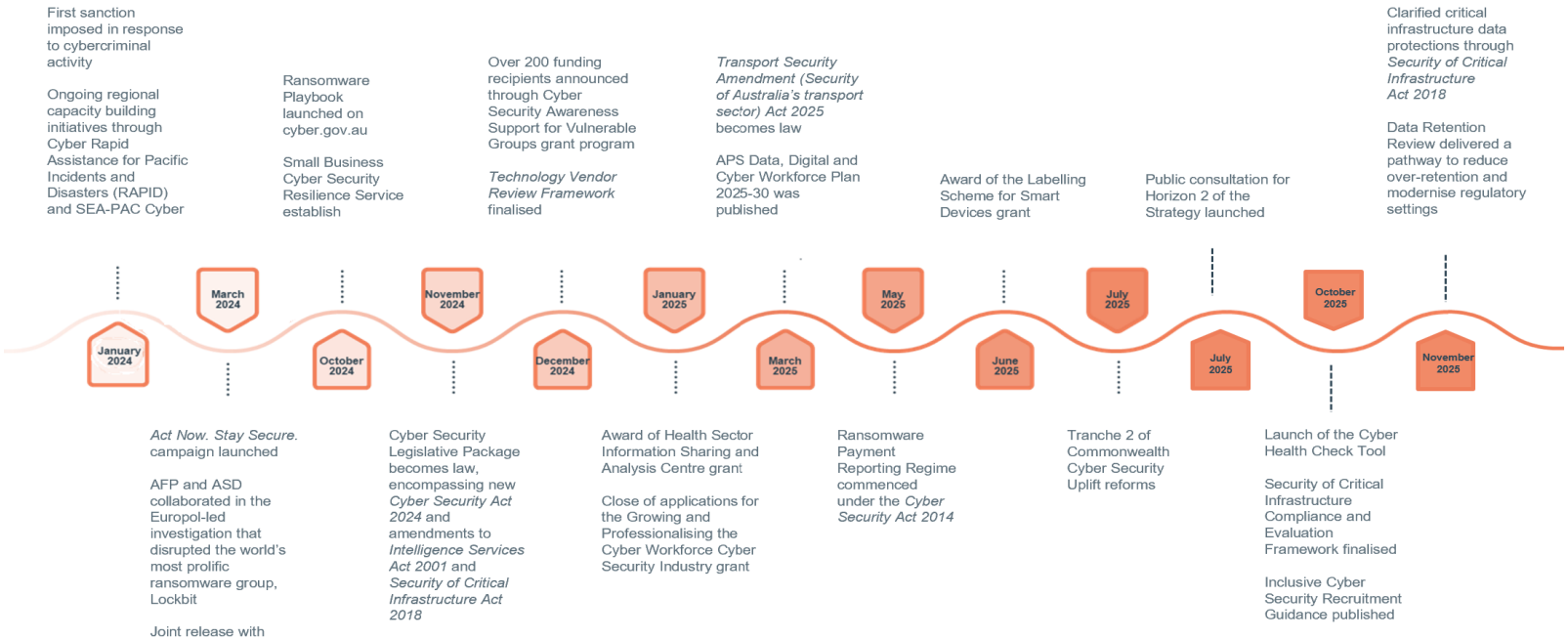


Figure 5. Ongoing delivery of intent, on time and on budget

For instance, the Business Council of Australia noted that 'The collaborative approach established in Horizon 1, particularly through the Executive Cyber Council, has been a positive step'.[6] However, stakeholders also expressed a desire for collaboration to be increased, deepened and expanded to a broader set of stakeholder groups.[7] In its submission, Crowdstrike sought 'more collaboration' with Government recognizing that 'industry expertise' is vital and that 'genuine partnerships' are needed for 'enduring solutions'.[8]

That said, a number of co-design and roundtable participants also reported they expected more reporting from government on strategy implementation progress. This was also raised in submissions. CISO Lens, for example, noted that amongst its members there was 'currently limited understanding of the progress to implement Horizon 1 action items', and that the 'detailed view of progress' provided with the Horizon 2 discussion paper was a 'welcome development'.[9]

**Australia's position as a world leader**

Regarding the overarching strategy goal of Australia becoming a world leader in cyber security by 2030, Harvard Kennedy School's *Cyber Security Strategy Scorecard*[10] and the International Telecommunication Union's *Global Cybersecurity Index 2024*[11] rate Australia highly.

In the Harvard Scorecard, Australia's Strategy leads in 8 of the 18 subcategories studied—equal with Singapore but outdone by the US which leads in 13 subcategories. Australia leads all countries in the category of protecting people and critical infrastructure. It also leads in skill development, codifying government roles and procedural responsibilities, and the clear presentation of its policies. The one area in which Australia is highlighted as lagging is building domestic government partnerships with civil society or state—and local—level bodies.

The Scorecard notes that 'the Australian strategy's weaknesses are minor compared to those of most other strategy documents...The relatively small number of lagging scores indicates that the Australian strategy performs well across most aspects of national cyber strategy'. The report goes on to state that 'the Australian strategy should be treated as a model for upper-middle tier powers seeking to develop incident response and reporting procedures, public-private partnerships, critical infrastructure resilience, and a strong global cybersecurity presence'.

In the ITU Index, Australia is in the top global performance tier as a cyber security role-modelling nation.

Australia's leadership was further recognised in September 2025, with the National Cyber Security Coordinator, Lieutenant-General Michelle McGuinness CSC, awarded the annual Billington International Cybersecurity Award. The award criteria include 'sustained leadership of a cyber effort having recognised international or multi-country impact' and being 'recognised by international peers as a thought leader in the cyber business'.[12]

6. Business Council of Australia (2025), Horizon 2 of the 2023-2030 Australian Cyber Security Strategy: BCA Submission.
7. See the Impact Poll results in the Appendix.
8. CrowdStrike (2025), Request for Comment Response: Horizon 2 Discussion Paper on Australia's National Cyber Security Strategy.
9. CISO Lens (2025), Submission: Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy.
10. Heiding F, O'Neill A, Price L (2025) Cyber Security Strategy Scorecard.
11. International Telecommunications Union (2024), Global Cybersecurity Index 2024.
12. Department of Home Affairs (2025) International cyber award presented to National Cyber Security Coordinator. Media Release.

### Strategic Outcomes Model

In Horizon 1, the Australian Government created a world-first framework for conceptualising the impact of the Strategy. The goal was to support government and its partners to work together to deliver long-term outcomes for Australians. The first step was to develop a clear shared picture of the goals for the Strategy. In the Horizon 2 Discussion Paper we translated the high-level outcomes expressed in the Strategy into a Cyber Security Strategic Outcomes Model (Figure 6). The Model enables us to illustrate how those outcomes link to the initiatives set out in the Action Plan. The goal was to develop a map that is long lasting and drives shared action and investments beyond the current Strategy.

#### From Measuring to Delivering What Matters

The Strategic Outcomes Model sits within a broader framework of a Delivering What Matters Framework (Figure 7). Traditional initiative-level program logics tend to take a 'bottom-up' linear approach by working from interventions (i.e. inputs → outputs → outcomes) to the outcomes that can be solely ***attributed*** to those interventions (intervention → outcome). In contrast, the Strategic Outcomes Model takes a 'top-down' approach. It starts from the high-level outcomes the Strategy aims to achieve and works backwards from there to the interventions that ***contribute*** to achieve them (outcome → intervention).

The Model informs both policy development (e.g. visualising all the initiatives working towards the outcome), and the creation and sharing of data and evidence required for achieving outcomes, not just delivering interventions.

The Strategic Outcomes Model fills the 'missing middle' between traditional evaluation approaches and the Government's Measuring What Matters outcomes. [13,14] It clearly links action (e.g. policy initiatives, programs, and services across portfolios and sectors) to the high-level whole-of-society and economy outcomes expressed in the Measuring What Matters framework. Specifically, it shows the links between the Strategy and its Action Plan, and the Measuring What Matters outcomes of prosperity, security and social cohesion (see Figure 6). This enables us to shift from purely measuring what matters to delivering what matters.

13. Australian Government (2023), Measuring What Matters: Australia's First Wellbeing Framework.
14. The Measuring What Matters framework is a national wellbeing framework intended to track Australia's progress that extends beyond purely economic measures. The framework identified the 5 outcome themes that matter most to Australians: healthy, secure, sustainable, cohesive, and prosperous. It established 50 key indicators to track Australia's progress in achieving these outcomes.

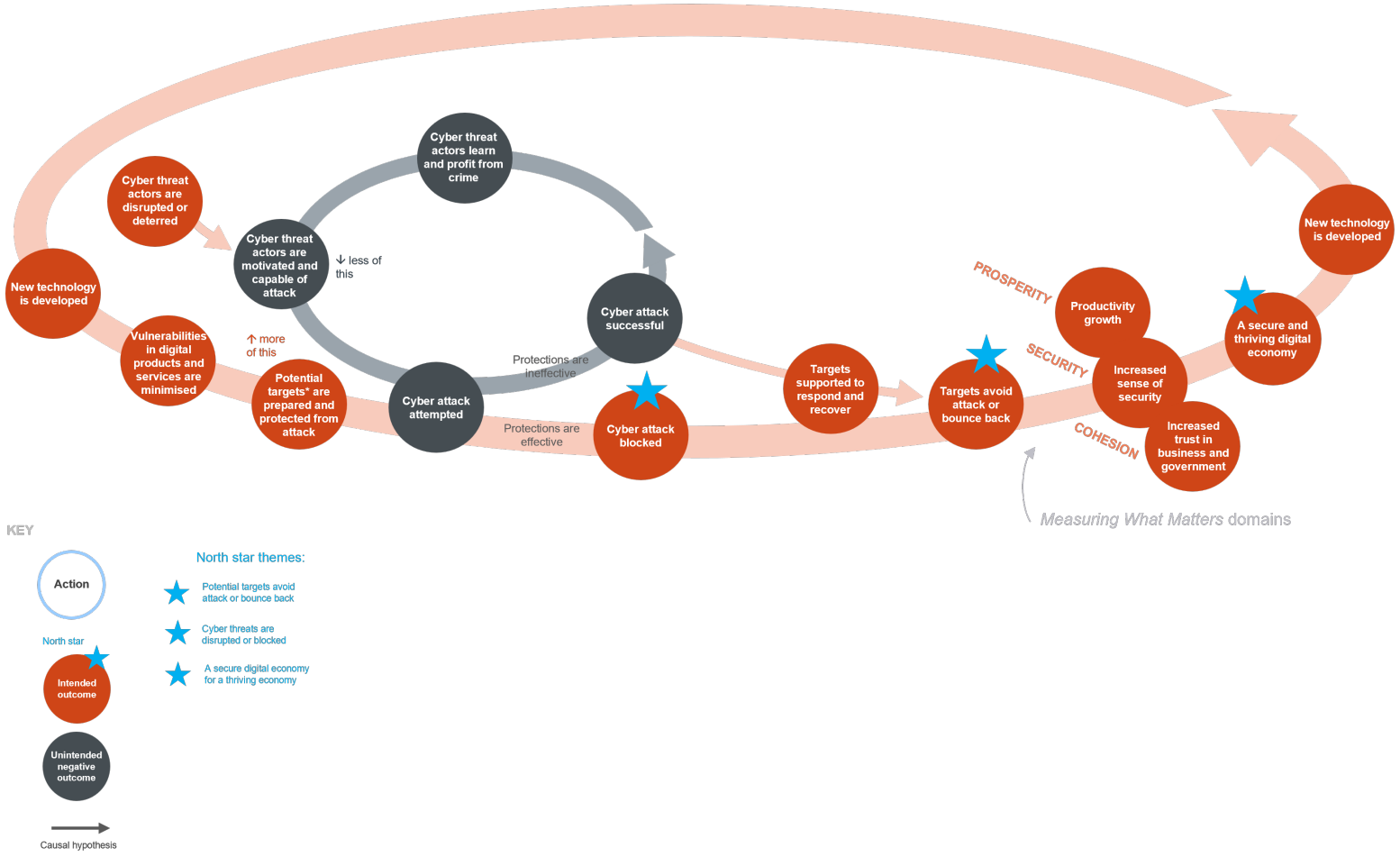


Figure 6. Cyber Security Strategic Outcomes Model

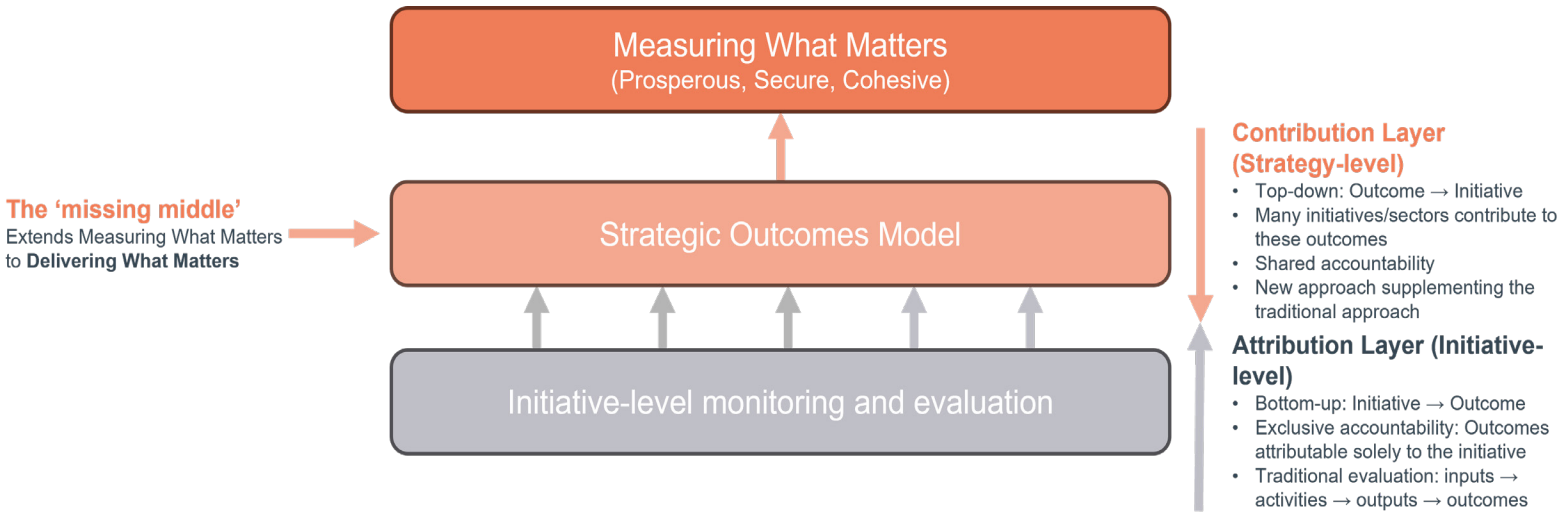


Figure 7. Top-down and bottom-down up approach, and Delivering What Matters as the 'missing middle'

**Feedback from stakeholders on the Strategic Outcomes Model**

The Harvard Kennedy School found that 'developing outcome-oriented goals' was 'the only element…for which there were zero leading ratings' amongst the countries studied (p. 58). The authors 'strongly encourage policymakers to make measurable outcomes a focus of their ongoing efforts to build robust national cybersecurity strategies' (p. 58).

A majority (90%) of discussion paper submitters who addressed monitoring and evaluation (n=59) also broadly welcomed the Model as a useful framework to guide implementation and monitoring of the Strategy. Only one stakeholder opposed it outright, and a further 5 had significant concerns.

Many individual and business stakeholders praised the ambition expressed in the Model, its whole-of-economy lens, and government's attempt to connect policy actions to real-world outcomes. For example, the Australian Chamber of Commerce and Industry stated that 'The high-level model is a good approach…focused on concrete and outcomes-based actions, and takes the whole of economy into consideration, showing clear roles for government and industry'.[15]

> *The high-level model is a good approach… focused on concrete and outcomes-based actions, and takes the whole of economy into consideration, showing clear roles for government and industry' – Australian Chamber of Commerce and Industry*

Stakeholders consistently emphasised that transparent, regular reporting was a way to demonstrate that government is tracking progress, learning from evidence and adjusting course when needed.

Several submissions observed that openness about both successes and challenges strengthens confidence in government stewardship and encourages industry and citizens to play their part in improving Australia's cyber resilience.

15. Australian Chamber of Commerce (2025), Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy—ACCI submission.


# Strong businesses and citizens

## Desired Outcomes: From the Strategy (p. 16)

**Our citizens and businesses are better protected from cyber threats and can bounce back quickly following a cyber attack.**

In 2030, all Australians will benefit from a **strong digital economy**. We envision a future where every **individual** and **business** has the **skills and resources they need** to be cyber secure.

Australians will have a **clear understanding of cyber risks** and **know how to get help quickly**.

**Small businesses** and **vulnerable groups** will have **dedicated support** from government and industry.

**Diverse communities**—including remote and regional communities, culturally and linguistically diverse groups, First Nations communities, young people, seniors, people with disabilities, and neuro diverse people—will be **empowered to build their cyber resilience**.

Government will help **business leaders understand their cyber maturity** and find ways to embrace digital technology while continuing to **protect their customers**.

**Responsibility** for cyber security is **shared** across the community, with **more cyber risk allocated to those who are most capable** of addressing them.

**Larger businesses** will play a central role in strengthening the security of the economy by **helping to protect those less able to do so**.

By 2030, Australia will be a **hard target** for cyber attacks.

Our objective is to **undermine cybercrime business models** and put Australians in a **strong position to respond effectively**, including if they are asked to pay a ransom.

Businesses will find it **easier to report cyber incidents**, and victims of cybercrimes will **get the support they need to recover**.

**Key inputs**: This shield is the largest in the Strategy. Over 15 agencies worked together towards achieving the desired outcomes across 17 initiatives through an investment of $290.8 million.

The key outputs and their outcomes are outlined over the following pages.

# Action 1: Support small and medium businesses to strengthen their cyber security

**1a. Cyber security 'health checks' for small and medium businesses**

Lead agency: Department of Home Affairs

Contributing agencies: Australian Signals Directorate, The Treasury

The Department of Home Affairs launched the Cyber Health Check Tool in October 2025. The tool supports those with minimal technical experience to self-assess and identify any vulnerabilities, compel users to take action to improve their cyber security, and encourage ongoing proactive cyber security behavioural changes.

In the first month after launch, the tool was completed by over 3,300 users. Feedback received during stakeholder engagement has been overwhelmingly positive. While it is premature to draw conclusions about success in achieving outcomes such as behavioural change, the high levels of early engagement with the tool indicate that it has been effective in reaching the target audience.

***3,000 Cyber Health Check Tool users in the first month and overwhelmingly positive stakeholder feedback.***

**1b. Small Business Cyber Resilience Service**

Lead agency: The Treasury

Contributing agencies: Australian Signals Directorate, Attorney General's Department, Department of Home Affairs

Treasury funded IDCARE in October 2024 to deliver the Small Business Cyber Resilience Service. The service provides free supports, 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.

Evidence from client satisfaction surveys show small businesses value the person-to-person support, tailored to their risk, situation and capability. For example, one client commented

> *'The staff member I spoke with was able to tailor the advice she gave and also to speak in both technical and plain language so I could understand'.*

Clients also value thoroughness and actionable recommendations, noting *'Without this [advice] we would have never covered the detail you have highlighted'* and *'We are coming from a very low base and the advice and ideas are practical and achievable'.*

**Stakeholder and data insights 1: Supports for small entities**

We heard during consultation for Horizon 2 that increased support for small and medium businesses and not-for-profits was at the top of participant's list of areas that need more work.[16] There is a strong consensus that SMBs and not-for-profits are a critical, yet highly vulnerable, part of the Australian economy. They are disproportionately exposed to cyber risks because they often lack the financial resources, dedicated staff and technical expertise to implement robust defences.

Globally, small organisations are reporting decreasing cyber resilience, compared to improving resilience in large organisations. In 2024, 35% of smaller organisations reported to the World Economic Forum that their cyber resilience was insufficient, up from 5% 3 years earlier. In contrast, in large organisations the rate decreased to 7%, down from 13% 3 years earlier.[17] That said, according to the Australian Institute of Criminology's *Australian Cybercrime Survey*, medium business owners in Australia were more likely to seek help from policy or ReportCyber in 2024 than the year before.[18]

Small organisations' vulnerability also presents a systemic risk, as they are integral parts of national supply chains. International analysis by IBM indicates that supply chain breaches are one of the most financially costly cyber incidents for organisations.[19] Just over half (54%) of large organisations participating in the World Economic Forum's 2024 *Global Cybersecurity Outlook* survey identified supply chain challenges as the biggest barrier to achieving cyber resilience.[20]

That said, the Tech Council of Australia highlighted in its submission that, in Horizon 2, supply chain resilience 'should be framed as a source of productivity and competitive advantage—lowering costs, reducing downtime, and positioning Australian firms as trusted providers in global markets'.[21]

Further to this, during Horizon 2 consultation, we also heard that local government organisations could be better supported through a coordinated approach to cyber security frameworks. In line with this, submissions called for more collaboration between Commonwealth, state, territory and local governments. Harvard's Cyber Strategy Scorecard highlighted 'building partnerships with local and state governments and civil society organizations' as an area of weakness for Australia's Strategy.

16. See the Impact Poll results in the Appendix.
17. World Economic Forum (2025), Global Cybersecurity Outlook 2025 (p. 29).
18. Australian Institute of Criminology (2025) Cybercrime in Australia 2024 (p. iii).
19. IBM (2025) Cost of a Data Breach Report 2025: The AI Oversight Gap.
20. World Economic Forum (2025) Global Cybersecurity Outlook 2025.
21. Tech Council of Australia (2025) Submission to the Horizon 2 Discussion Paper.

# Action 2: Help Australians defend themselves from cyber threats

**2a. Expand the *Act Now. Stay Secure.* campaign**

Lead agency: Department of Home Affairs

Phase 3 (March to June 2024) of the *Act Now. Stay Secure.* campaign emphasised why good cyber safe practices are important, and the simple steps people can take to protect themselves online. Phase 4 (May 2025 to March 2026) built on Phase 3 to reinforce the actions Australians should consistently take to protect themselves online (e.g. multi-factor authentication, unique and strong passwords, and installing all software updates).

The Phase 3 and Phase 4 campaign concept, 'What are you risking online', was effective at driving action in those who saw it, with millions of Australians shown to have changed their behaviour and proactively educated themselves on cyber security and added cyber security behaviours into their day-to-day lives.

The Evidence Use Showcase box below highlights the best practice evaluation approach used to monitor the campaign's impact, and the Stakeholder Insights on Awareness Raising (see page 24) outlines the positive feedback the campaign received from stakeholders.

**Evidence Use Showcase 1: *Act Now. Stay Secure.* campaign: building cyber awareness**

**Program overview:**

In Horizon 1, the *Act Now. Stay Secure.* campaign worked to build the baseline cyber security capability of all Australians. The goal was to increase awareness of why cyber security is important, improve the audience's understanding of key cyber security threats and empower them to consistently undertake the actions that will protect them online.

The campaign utilises a mix of targeted advertising, public relations, and stakeholder and community engagement activity. During Horizon 1, 2 phases of the campaign were in market, with Phase 3 running from 17 March 2024–30 June 2024, and Phase 4 launching on 11 May 2025 and continuing in market until 14 March 2026.

**Collecting data and evidence:**

Evidence for the campaign's effectiveness is determined through a comprehensive evaluation framework supported by the whole-of-government evaluation research agency. Key performance indicators are developed to guide measurement across all campaign phases.

Benchmark research is conducted prior to the campaign's launch to establish baseline measures of audience awareness, attitudes and behaviours. While the campaign is live in market, ongoing tracking research is undertaken to monitor performance. These insights inform mid-campaign optimisations based on how the audience is responding.

At the conclusion of the campaign, a final evaluation is conducted, comparing endline results to baseline benchmarks to assess overall impact and effectiveness of the campaign, as well as optimisations for future campaign phases.

**Using evidence to inform program implementation:**

The performance data from ongoing tracking research is used to identify which channels, creative assets and audience segments are performing strongly, and where gaps may exist. Based on these insights, evidence-based optimisations and adjustments can be made if required to enhance campaign performance.

The final evaluation against the objectives at the end of the campaign then further informs future phases by identifying improvements to the media mix, creative approach and audience targeting.

**2b. Fund the Cyber Security Awareness Support for Vulnerable Groups grants program**

Lead agency: Department of Home Affairs

Contributing: Department of Social Services (Community Grants Hub)

Delivered between the Department of Home Affairs and the Department of Social Services Community Grants Hub, this grants program aimed to expand the reach of the national cyber security awareness campaign to priority groups, including culturally and linguistically diverse (CALD) communities, First Nations communities, people with disabilities, young people (up to 18 years of age), and elderly people (over 65 years of age). During consultation on measures to uplift cyber awareness among these cohorts, stakeholders advised that uptake of cyber security advice in vulnerable groups was more likely to be impactful if the messaging was designed by the community groups and leaders who best understand the unique needs of their communities.

Just under $7 million in grants have been provided to over 200 recipients since the Department of Home Affairs launched the program in December 2024.

Participants from this grants program under Horizon 1 reported feeling not only informed and connected through tailored resources but also empowered to support others in building confidence to stay safe online. A grant recipient that provides services to the elderly community around Melbourne shared a powerful example resulting from Horizon 1 awareness programs, where an elderly participant received a threatening text message requesting personal details to prevent digital services being disconnected. Having received tailored guidance aligned with the Act Now. Stay Secure. campaign through trusted community leaders with ongoing support, she felt empowered to resolve the issue by contacting the established help service, not sharing personal details, and confidently report the incident. The participant emphasised that the campaign and activities from this grants program allowed her to finally feel safe and confident online.

**Stakeholder insights 2: Awareness raising**

Stakeholders in Horizon 2 co-design workshops and roundtables reported that public awareness initiatives were amongst those that had the biggest positive impact on Australia's cyber security in Horizon 1 (see Appendix). CISO Lens noted in its Horizon 2 discussion paper submission:

*'There is considerable support for the 'Act Now. Stay Secure.' campaign. This campaign is viewed positively for its messaging about online safety, cybercrime risks and response strategies. Members feel the 'Act Now. Stay Secure.' campaign is doing a good job of raising awareness of key cyber risks across the economy'.*[22]

Surveys by Allianz and the Lowy Institute further confirm that cyber security is at the front of Australians' minds, and that cyber incidents are seen by Australian individuals and businesses as the number one threat.[23,24] As a result of this increased public concern regarding cyber security risks, several stakeholders recommended backing up awareness raising with an increased focus on the 'how'. This included the enhanced cyber security supports for individuals and small entities (e.g. small businesses, not-for-profits) noted earlier in this report.

Some of the conversations emphasised a need to tailor supports to priority groups, such as First Nations communities and the elderly, and the need for trusted supporters and resources. Home Affairs also had productive roundtable discussions about the security of devices, such as routers of which consumers may not have a high level of understanding, and the need for baseline standards and incentives to upgrade insecure devices.

The University of Queensland noted in its Horizon 2 discussion paper submission that:

> 'We acknowledge and celebrate the effectiveness of current federal cyber awareness campaigns (Act Now. Stay Secure). To further build on this effective campaign, we suggest there may be value in incorporating cyber security awareness in the education system'. [25]

See the Stakeholder Insights box on Cyber Security Workforce and Sovereign Capability (page 64) for more on this topic.

## Action 3: Disrupt and deter cyber threat actors from attacking Australia

**3a. Amplify cybercrime disruption activities under Operation Aquila**

Lead agency: Australian Federal Police

Contributing: Australian Signals Directorate, Department of Home Affairs

Operation Aquila continues to disrupt and deter cyber criminals from targeting Australia, including through an established network of international partners, and specialist tactics, techniques and procedures to de-anonymise cyber criminals. Investment in this initiative has allowed the Australian Federal Police and the Australian Signals Directorate to continue to investigate the highest priority cybercrime threats impacting Australia, both nationally and internationally, including LockBit and BlackCat ransomware groups.

22. CISO Lens (2025) Submission: Consultation on development of Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. (p. 8).
23. Lowy Institute (2025), Lowy Institute Poll 2025 (p. 20).
24. Allianz (2025) Allianz Risk Barometer 2025: Cyber top business risk globally as climate change hits record high (see table: The top 10 business risks for 2025 in Australia).
25. University of Queensland (2025) The University of Queensland's submission to the Horizon 2 Public Discussion Paper (p. 8).

In the 2024-25 financial year, 234 ransomware incidents were analysed, 38 disruptions undertaken and 46 intelligence products distributed. This work has increased public awareness and confidence in the Government's ability to respond to cyber threats.

In October 2025, via the Australian Federal Police's international partnerships, Operation Aquila was able to use live intelligence of an imminent ransomware attack to advise an agency to address a serious vulnerability. As a result, the affected agency was able to remediate the vulnerability and prevent the ransomware incident from occurring. Operation Aquila also supported the identification and sanctioning of a Russian cyber criminal involved in the Medibank Private cyber incident and those hosting sites to disseminate stolen personal information. At the conclusion of Horizon 1, Australia, together with international partners, have imposed 5 sets of cyber sanctions on Russian cyber criminals (12 individuals and 3 entities), with discernible impact including cost and reputational effects on the cyber criminal ecosystem.

The cybercrime threat environment is pervasive, persistent and continually evolving. Hence, in Horizon 2, the Government will continue its investment in Operation Aquilla.

**Initiative Deep Dive 1: Operation Aquila—LockBit takedown**

**Program overview:** The Australian Federal Police and Australian Signals Directorate established Operation Aquila in November 2022 to investigate, target and disrupt cybercriminal syndicates and their enablers, with a priority of ransomware threat groups. Under Operation Aquila, the Australian Federal Police and Australian Signals Directorate investigate the highest priority cyber criminals targeting Australia, including the LockBit and BlackCat ransomware groups and the services that enable them.

**What did it achieve:** In February 2024, the Europol-led investigation, Operation Cronos, disrupted critical infrastructure of the ransomware group allegedly responsible for running LockBit. The world's most prolific ransomware group was disrupted as a result of an international investigation involving law enforcement agencies from 10 countries, including the Australian Federal Police. The Australian Federal Police's contribution to the operation included criminal investigations, target development and disruption, and engagement with key international partners. Following Australian Federal Police's participation in Europol's long-run coordinated actions against LockBit ransomware group actors, in May 2024, Australia, the United Kingdom and the United States imposed targeted financial sanctions and a travel ban on Dmitry Khoroshev for his leadership role in the Lockbit group. This was Australia's second tranche of thematic cyber sanctions.

**Impact:** Operation Cronos disrupted LockBit's critical infrastructure. This included its primary platform and 34 servers across Australia, the Netherlands, Germany, Finland, France, Switzerland, the United States and the United Kingdom. France's National Gendarmerie arrested 2 alleged LockBit actors in Poland and Ukraine, and a further 3 arrest warrants and 5 indictments have been issued by French and United States' law enforcement. More than 200 cryptocurrency accounts allegedly owned by the ransomware group have been frozen by law enforcement, stripping the group of significant profits.

**3b. Build regional capabilities to fight cybercrime, including through the Pacific Islands Law Officers' Network's Cybercrime Working Group**

Lead agencies: Attorney General's Department, Department of Foreign Affairs and Trade

Contributing: Australian Signals Directorate, Australian Federal Police, Department of Home Affairs

The Pacific Islands Law Officers' Network (PILON) is a network of senior law officers from 19 Pacific Island countries who work together to contribute to a safe and secure Pacific by advancing key law and justice issues, and collaborating to combat cybercrime.

A central focus of the PILON Cybercrime Working Group is the development of a Cybercrime Legislation Implementation Handbook, which is being co-designed with the Council of Europe and Australia's Attorney-General's Department. The Handbook will provide countries across the Pacific with a comprehensive understanding of how to effectively develop and implement cybercrime laws and will support greater ratification of the 2001 Budapest Convention on Cybercrime and the 2024 United Nations Convention Against Cybercrime.

The Handbook is due for completion at the end of 2026. Anecdotal evidence arising during drafting has shown that participants have already started demonstrating a stronger understanding of cross jurisdictional implementation challenges. Organisational capacity continues to be strengthened though the collaborative drafting model.

**3c. Build regional capabilities to fight cybercrime in the Pacific and Southeast Asia**

Lead agencies: Attorney General's Department, Department of Foreign Affairs and Trade

Contributing: Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, eSafety Commissioner

More broadly, Australia's participation in forums such as the Pacific Islands Law Officers' Network and the Association of Southeast Asian Nations Senior Officials Meeting on Transnational Crime build regional capabilities to fight cybercrime in the Pacific and Southeast Asia.

# Action 4: Work with industry to break the ransomware business model

**Data Snapshot 1: The evolving ransomware threat landscape**

Ransomware and cyber extortion are an escalating domestic and global threat with serious economic, security and social consequences. The threat of this type of cybercrime activity is complex. Our ability to effectively mitigate and respond relies on our ability to understand the threat through data and reporting. It also requires close collaboration both with industry on local initiatives, and the capacity, cooperation and resilience of global partners.

In the 2024–25 financial year, ransomware was the most disruptive cybercrime threat in Australia.[26] The Australian Signals Directorate's Australian Cyber Security Centre responded to 138 ransomware incidents, with 39% detected proactively when ACSC contacted entities about potential threats.[27] Threat actors are continuing to evolve their methods and leverage a global ecosystem of ransomware-as-a-service operators and access brokers.

Recent business surveys show that ransomware incidents are the most common type of cyber-attack experienced by Australian businesses, comprising 89% of cyber attacks in 2025. International data reflects that ransomware attacks are increasing globally—the presence of ransomware in data breaches grew from 32% to 44% of investigations undertaken by Verizon, and it was the most common technique used by threat actors in cyber breaches 2025.[28] Small and medium enterprises continue to be most targeted, often attributed to perceived vulnerability of being less likely to have backed-up data or dedicated cyber security teams.[29]

However, businesses are maturing in their responses to these threat actors. The estimated average ransom payment amount fell to AUD$711,000, a significant decrease from the AUD$1.35 million average in 2024.[30] The decrease in median payment amount also aligns with a decrease in the proportion of businesses willing to make a ransom payment, dropping to 81% in 2025 compared to 83% in 2024.[31] Consistent with international data, the average global amount paid for a ransom in 2024 declined to USD$115,000 (compared to USD$150,000 in the previous year).[32] Anecdotal evidence suggests this decrease in the amount paid is due to a combination of increasing refusal to pay and 'increased pressure from law enforcement takedowns on these groups…their opening amounts for ransoms have been lower overall'.[33] More robust data is beginning to emerge through Australia's mandatory ransomware payment reporting regime, which commenced on 30 May 2025, and applies to businesses with annual turnover of $3 million or more and all critical infrastructure entities.

26. Australian Signals Directorate (2025), Annual Cyber Threat Report 2024-2025.
27. Australian Signals Directorate (2025), Annual Cyber Threat Report 2024-2025.
28. Verizon (2025), 2025 Data Breach Investigations Report.
29. McGrathNicol (2025), Ransomware: A shift from payment dependent strategies.
30. McGrathNicol (2025), Ransomware: A shift from payment dependent strategies.
31. McGrathNicol (2025), Ransomware: A shift from payment dependent strategies.
32. Verizon (2025), 2025 Data Breach Investigations Report.
33. Verizon (2025), 2025 Data Breach Investigations Report.

**4a. Work with industry to co-design a mandatory ransomware reporting obligation**

Lead agency: Department of Home Affairs

Contributing: Australian Federal Police, Attorney General's Department, Australian Signals Directorate

The ransomware reporting obligation, established under the Cyber Security Act 2024, aimed to strengthen national visibility and responsiveness to ransomware and cyber extortion threats. It mandates that businesses who meet the reporting threshold must disclose and report to the Government any ransom payments made.

The ransomware payment reporting regime commenced on 30 May 2025, with the Department of Home Affairs initially focusing on education and engagement with regulated entities. During this period, the Home Affairs has hosted Town Hall sessions and published fact sheets, frequently asked questions and detailed guidance materials on its website. In 2026, Home Affairs is undertaking a review of the implementation of the regime, looking at opportunities to improve the ease of reporting and engagement and consider when it would be appropriate to take a more active focus on compliance and enforcement.

As the regime matures and the data sets develop, the regime will increase visibility of ransomware and cyber extortion attacks, providing Government and businesses with critical intelligence on threat actors, attack methods and payment trends. This will enable targeted responses and guidance, strengthening the cyber resilience of Australian businesses and individuals.

**4b. Create a Ransomware Playbook**

Lead agency: Department of Home Affairs

Contributing: Australian Federal Police, Attorney General's Department, Australian Signals Directorate, Department of Foreign Affairs and Trade, The Treasury

The Ransomware Playbook was launched by the Department of Home Affairs in October 2024 and hosted by the Australian Signals Directorate on cyber.gov.au. The playbook is an online interactive guide to help Australians prepare for, respond to, and recover from ransomware attacks and cyber extortion incidents. It also provides information on mental health and victim support services.

The playbook includes guidance on reporting obligations and encourages timely reporting to enhance whole-of-economy risk mitigation and preparedness, and help tailor victim support services.

The objective of the Ransomware Playbook was to consolidate the advice from across government. Stakeholder feedback indicated that the previously fragmented nature of government guidance on these issues made it difficult to navigate, particularly for individuals and small businesses with limited technical expertise and resources. The way in which the playbook brought relevant information together and made it accessible for a diverse range of users has been very positively received.

**4c. Leverage Australia's role in the Counter Ransomware Initiative**

Lead agency: Department of Home Affairs

Contributing: Department of Foreign Affairs and Trade

The Department of Home Affairs is strengthening global resilience to ransomware by leveraging its continuing involvement and leadership in the global Counter Ransomware Initiative.

Australia has facilitated a range of Initiative events during Horizon 1, including virtual workshops on information sharing and threat briefings, and a tabletop exercise co-facilitated with the private sector at the 5th Annual Counter Ransomware Initiative Summit in Singapore in October 2025.

Australia administers the Initiative website and members' portal which was launched in November 2023. The members' portal has over 350 registered users and contains over 70 documents. There have been at least 2.2 million hits on the public site and 114,000 hits on the members' portal. Several countries have used the portal to issue specific ransomware alerts seeking assistance from the wider Initiative membership.

The Department presented on the Initiative to a regional audience at Pacific Cyber Week 2025 with industry partners. As a result, a number of Pacific Island countries approached Initiative representatives about joining. Pacific partners noted the value of the Initiative and highlighted the increased coordination across the Pacific on countering ransomware through Initiative engagement. They noted that members were actively supporting each other in cyber incident response and capacity building ideas. This is enhancing regional readiness and fostering stronger operational trust.

Conversations with Initiative members throughout 2025 highlighted that while ransomware continues to be one of the most disruptive cybercrime threats globally, the world lacks a single, universally adopted framework for confronting ransomware.

## Action 5. Provide clear cyber guidance for businesses

**5a. Guidance to company directors on cyber governance obligations**

Lead agencies: Department of Home Affairs, The Treasury

Contributing: Attorney General's Department, Australian Securities and Investments Commission, Other departments and regulators

This initiative aimed to develop guidance for company directors in discharging their duties under the *Corporations Act 2001* to manage cyber security risk.

However, industry consultation ascertained that existing guidance already provides adequate clarity for company directors. Industry considered education, awareness and sharing information on surveillance activity as the most beneficial focus points for the Australian Securities and Investments Commission going forward.

In response, in 2024, the Commission announced the Supervisory Cyber and Operational Resilience Program to focus on education, surveillance and enforcement, and better support directors to comply with their cyber security governance obligations.

The program has supported regulated entities in enhancing cyber resilience, including their use of third-party providers, by reviewing cyber resilience in various industries and sending letters based on findings. The program has also implemented a self-deployed exercise for entities to improve cyber resilience. Moving forward, the program will also work on information-sharing initiatives, design a single reporting portal and partner with the Australian Prudential Regulation Authority for supervisory efforts.

The program has enabled the efficient and targeted delivery of appropriate education to industry to clarify cyber guidance obligations under current regulations. The program complements the Australian Institute of Company Directors' Cyber Security Governance Principles to ensure identified vulnerabilities are not further exploited.

This program is expected to run for a minimum of 3 years, with delivery spanning into Horizon 2.

**5b. Cyber Incident Review Board**

Lead agency: Department of Home Affairs

Contributing: Australian Federal Police, Attorney General's Department, Australian Signals Directorate, Department of Defence, Department of the Prime Minister and Cabinet, other agencies as appropriate.

Recent high-profile and high-impact cyber security incidents, such as the Optus data breaches in 2022 and 2023, the MediSecure data breach in 2024, and the Qantas data breach in 2025, highlight that government and industry need to do more to effectively learn lessons from cyber security incidents and prepare contingencies for future attacks.

In response, Part 5 of the *Cyber Security Act 2024* sets out the legislative framework for the establishment of the Cyber Incident Review Board. The Board would conduct no-fault, post-incident reviews of significant cyber security incidents in Australia.

The Minister for Cyber Security announced the appointment of the Chair and Board Members in May 2026. An expert panel will be established to support the Board. Activities of the Board will be reported in Home Affairs' Annual Report.

# Action 6. Make it easier for Australian businesses to access advice and support after a cyber incident

**6a. Develp a Cyber Incident Single Reporting Portal**

Lead agency: Department of Home Affairs

Contributing: Australian Competition and Consumer Commission, Australian Communications and Media Authority, Australian Federal Police, Attorney General's Department, Australian Prudential Regulation Authority, Australian Signals Directorate, Australian Securities and Investments Commission, Department of Defence, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, Digital Transformation Office, Office of the Australian Information Commissioner, Office of the National Data Commissioner, The Treasury, other agencies as required.

The objective of the Cyber Incident Single Reporting Portal is to make it easier for entities affected by cyber incidents to meet their regulatory reporting obligations. This initiative is being developed across 3 phases.

Phase One was the release of the *Single Reporting Portal* directory on cyber.gov.au in November 2023. The directory links entities to reporting forms for 23 cyber incident regulatory reporting requirements. This 'early win' built a useful foundation for providing a single source for reporting obligations and provided momentum for progressing the next phase of the initiative. Harvard's Cyber Strategy Scorecard highlights 'Australia's single-service incident reporting portal is a great example of an access enabling initiative'.[34]

Phase Two, carried forward over Horizon 1, involved numerous co-design workshops with policy agencies, regulators and industry representatives to discuss legislative and technical barriers, and opportunities for implementing a single reporting interface. This co-design ensured that future iterations of the reporting interface suited the needs of both industry and regulators, and identified 'quick win' enhancements for the existing Directory.

In Horizon 2, the Department of Home Affairs will deliver an incident reporting interface that enables entities to lodge a single online form to meet multiple regulatory reporting obligations.

**Stakeholder Insights 3: Making cyber regulation easier**

The new Cyber Security Act 2024 and amendments to the Security of Critical Infrastructure Act 2018 were highlighted by stakeholders as some of the most positively impactful initiatives undertaken during Horizon 1.[35]

At the same time, submissions affirmed that the complexity of overlapping compliance regimes across the Commonwealth, and across both domestic and international jurisdictions, create a productivity burden on business. The World Economic Forum noted that while 'regulations bolster cyber resilience', their fragmentation across jurisdictions 'is adding a significant compliance burden'.[36]

34. Heiding F, O'Neill A, Price L (2025), Cyber Security Strategy Scorecard (p. 55).
35. See the Impact Poll results in the Appendix.
36. World Economic Forum (2025), Global Cybersecurity Outlook 2025 (p. 4, 7).

This, along with other cyber security challenges, are 'compounded by a widening skills gap'.[37] In our Horizon 2 consultation, we heard that cyber workforce resources are being diverted away from cyber security uplift and incident response and recovery to regulatory compliance reporting.

There was a strong call to review existing regulatory frameworks and identify opportunities to reduce duplication, harmonise definitions and thresholds, and create a clear cyber security regulatory environment to promote best practice.

Stakeholders also noted the need for Australia to be a leader in driving forward regulatory harmonisation across jurisdictions. In November 2025, we met with Organisation for Economic Cooperation and Development countries for a cyber regulatory alignment workshop and held productive bilateral meetings with the United Kingdom and France. Regulatory alignment and cross-jurisdictional recognition remain priority areas of interest for our trusted European partners, who continue to look to Australia for best practice examples through our Strategy programs, including critical infrastructure, ransomware and cyber incident reporting.

**6b. Limited use obligation**

Lead agencies: Australian Signals Directorate, Department of Home Affairs

Contributing: Australian Federal Police, Attorney General's Department, Australian Prudential Regulation Authority, Australian Securities and Investments Commission, Office of the Australian Information Commissioner, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet, other departments and regulators.

The limited use obligation aims to strike a balance between encouraging industry engagement to share cyber security information with government and protecting broader public interests by not impeding an effective regulatory environment.

This initiative was delivered through the introduction of a limited use obligation under the *Cyber Security Act 2024* and Division 1A of Part 6 of the *Intelligence Services Act 2001*. The obligation became law on 29 November 2024. Under the limited use obligation, any information voluntarily provided to, or acquired or prepared by, the Australian Signals Directorate or the National Cyber Security Coordinator about an entity's cyber security incident or potential cyber security incident (including vulnerability information) cannot be used for regulatory purposes.

While it will take time to measure and evaluate the limited use obligation's impact, the Directorate has already observed anecdotal evidence of increased willingness from organisations to engage with the Directorate. Over the last year, the Directorate observed a gradual increase in the response rate from organisations contacted by the Directorate regarding suspicious or malicious activity affecting their organisation. The average response rates for July 2024 to December 2024 was 53%, while January to June 2025 saw a slight rise to 67%.

A change in the response rate is likely influenced by several factors, which may include introducing the limited use obligation. However, operational feedback suggests the obligation is supporting its aims in practice. For example, one organisation that contacted the Directorate regarding an incident was initially hesitant to share.

37. World Economic Forum (2025), Global Cybersecurity Outlook 2025 (p. 9).

However, upon being informed of the limited use provision, the organisation began sharing incident details, including the types of data exfiltration and threat actor information. A similar pattern was observed in the Directorate's engagement with a critical infrastructure entity.

**6c. Code of practice for cyber incident response providers**

Lead agencies: Department of Home Affairs, Australian Signals Directorate

Contributing: Australian Federal Police, Attorney General's Department, Department of Defence, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet, other agencies as required

During a cyber security incident, businesses and individuals rely on cyber security incident response providers to support and guide them through a cyber security incident. However, there were no consistent standards for cyber security incident response providers in Australia, and no frameworks for businesses and individuals to assess whether they were receiving quality service.

The National Office of Cyber Security and the Australian Signals Directorate developed a voluntary Code of Practice to address this issue and undertook a public consultation process on the draft Code from September to October 2025. During the consultation period, submissions were received from 15 organisations. Most submissions supported the publication of the Code and provided appreciation for industry engagement.

The Code was established and published in November 2025 and sets out best practice controls designed to support incident response providers to meet service quality and professional standards, and encourages early collaboration and information sharing with the Directorate's Australian Cyber Security Centre and the National Cyber Security Coordinator.

## Action 7. Secure our identities and provide better support to victims of identity theft

**7a. Expand the Digital ID program**

Lead agency: Department of Finance

Contributing: Attorney General's Department, Australian Taxation Office, Services Australia, Australian Competition and Consumer Commission, Office of the Australian Information Commissioner, the Treasury

The Digital ID program aims to reduce the need for people to share sensitive personal information with government and businesses when verifying their identity. This is critical in uplifting Australia's cyber resilience by reducing the threat surface and ensuring that Australian's sensitive information is secure.

The initiative was delivered through the Digital ID Act 2024 (Digital ID Act), which commenced on 30 November 2024 and governs an accreditation scheme for Digital ID service providers, and the Australian Government Digital ID System. The accreditation scheme is open to private sector and government Digital ID service providers. The Government System is currently based around myID (the Government's Digital ID provider) which can be used to access government services.

From 30 November 2026, private sector entities will be able to apply to participate in the Government System, giving businesses and individuals even greater choice for services using Digital ID.

At December 2025, there were over 15.2 million reusable myIDs that people can use to access around 255 Commonwealth and state and territory government services. The reusability of Digital ID is key to reducing the need for people to share personal information. For example, the 93.6 million transactions in the Government System in 2025 show people are increasingly reusing their Digital ID across different services.

In Horizon 2, supporting increased use of Digital ID will provide further opportunities to reduce sharing of people's personal information. For example, the Department of Finance's consultations with the e-conveyancing industry suggest that if Digital ID was used in half of all property purchase transactions, it would reduce about 6 million instances of sharing identity documents each year. Renters could also be supported to reduce the need to share their identity documents.

**7b. Continue support for victims of identity crime**

Lead agency: Attorney General's Department

In September 2025, the Attorney General's Department published updated and modernised National Identity Proofing Guidelines. The Guidelines provide best practice guidance for identity proofing—establishing a person is who they say they are. The Guidelines align, where possible, with Digital ID Accreditation Rules to increase consistency in identity proofing for both physical and digital ID. They strengthen identity-proofing processes and increase trust through standardised, transparent, national principles and a risk-based approach.

The updated Guidelines are designed to allow organisations the flexibility to address their specific identity related risks.

In 2021, the Government engaged IDCARE to guide individuals on recovering identity, mitigating damage, replacing identity credentials and educating individuals on how to identify danger signs that a compromised identity is continuing to be misused. IDCARE offers direct engagement with a case manager for personalised and confidential response assessment and planning, tailored to the individual's needs. Over 120,000 victims of identity crime have been assisted under the Commonwealth's contracts with IDCARE. IDCARE also provides reporting on private and public sector trends, and emerging threats in cyber and identity crime. These include dark web monitoring and scam alert services.


# Safe technology

## Desired Outcomes: From the Strategy (p. 28)

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

By 2030, all Australians should feel protected by a **secure and resilient digital economy**.

They should feel confident that cyber security will be **enforced by those most capable** of managing it across each layer of the technology supply chain.

Consumers and businesses will benefit from widespread adoption of cyber security standards across our technology and software markets. Australia will adopt a **harmonised approach to cyber security standards** for digital products, consistent with international best-practice.

Our digital products will be **secure by design and default**.

When purchasing digital devices or software, consumers should have peace of mind knowing that **their technology is protected from cyber attacks** and does not have embedded vulnerabilities that will put them or their families at risk.

Our **most valuable datasets** require **adequate protections** that keep pace with the current cyber landscape, without imposing unduly burdensome requirements on industry.

This includes **streamlined data retention requirements** that are appropriate and proportionate.

By 2030, Australians should be able to **safely embrace the opportunities** presented by **critical and emerging technologies**—including quantum, artificial intelligence, and advanced communications systems such as 6G.

**Key inputs:** Over 15 agencies worked together towards achieving these desired outcomes across 11 initiatives through an investment of $4.8 million.

The key outputs and their outcomes are outlined over the following pages.

# Action 8: Ensuring Australians can trust their digital products and software

**8a. Adopting international security standards for consumer-grade smart devices**

Lead agency: Department of Home Affairs

Contributing: Australian Communications and Media Authority, Attorney General's Department, Department of Industry, Science and Resources, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, Department of Health, Disability and Ageing, The Treasury, law enforcement agencies

To deliver this initiative the Department of Home Affairs worked with industry to co-design a mandatory cyber security standard for consumer-grade smart devices.

The passage of the *Cyber Security Act 2024* provided the legislative framework, and the *Cyber Security (Security Standards for Smart Devices) Rules 2025* prescribed requirements, for consumer-grade smart devices. The regime came into effect on and from 4 March 2026, following a 12-month transition period. As requested by industry, guidance materials to support compliance with the Rules have been published on the Home Affairs website. Many stakeholders have acknowledged Australia's international alignment with other key markets as an enabler for their preparation to comply with the Australian security standard.

The Technology Assessment and Regulation Office was established within Home Affairs to be responsible for regulating the cyber security of smart devices. This includes supporting the Secretary to exercise their enforcement and other regulatory powers, relating to the security standards for smart devices, under Part 2 of the *Cyber Security Act 2024*.

**8b. Co-design a Voluntary Labelling Scheme for Smart Devices**

Lead agency: Department of Home Affairs

Contributing: Australian Communications and Media Authority, Attorney General's Department, Department of Industry, Science and Resources, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, The Treasury

When delivered in full, the labelling scheme will enable consumers to make informed decisions about a smart device's level of security when making purchasing decisions. It will align the Australian smart device market with international best practice and encourage greater adoption of security by manufacturers, enabled by confident consumers and secure-by-demand.

The design of the scheme is being informed by behavioural insights research conducted in partnership with the Behavioural Economics Team of the Australian Government, and international collaboration and alignment through the Global Cybersecurity Labelling Initiative.

The Labelling Scheme for Smart Devices Grant Program was launched in January 2025 to provide an Internet of Things peak body with up to $1.7 million in funding to build cyber security protections for consumers and co-design and implement a voluntary labelling scheme. The Connected Technology Alliance (formerly the Internet of Things Alliance Australia) was awarded the grant in June 2025.

The Department of Home Affairs and the Alliance will continue to work together through Horizon 2 to develop a voluntary labelling scheme, aligned with international exemplars. They will launch a pilot of the scheme in late 2026 to early 2027.

We are already seeing enthusiasm among industry to adopt the label. Industry representatives have reached out expressing their interest in the label as they would be able to use it as a product differentiator in a saturated market, competing on security, not just price. While still in design phase, the label is also helping industry to consider implementing more secure-by-design features to be able to apply for a higher-tier label.

**Evidence Use Showcase 2: Using evidence for labelling scheme design**

Prior to the launch of the Labelling Scheme for Smart Devices Grant Program, the Department of Home Affairs engaged the behavioural economics research team within the Department of the Prime Minister and Cabinet to evaluate the effectiveness of cyber security labelling and different label features on Australians' smart device purchasing decisions. Outcomes of this work were used to support the design of the grant and evidenced the need for a label in the Australian context.

Furthermore, the Department of Home Affairs and the Alliance will continue to leverage the Behavioural Economics Team of the Australian Government's research to inform the labelling scheme design process and stakeholder engagement approach, and to ensure the messaging is fit-for-purpose for Australian consumers. Consumer insights research will assess consumer understanding of prototype label designs for the Australian scheme in 2026.

**8c. Voluntary Code of Practice for App Store Operators and App Developers**

Lead agency: Department of Home Affairs

Contributing: Australian Communications and Media Authority, Attorney General's Department, Department of Industry, Science and Resources, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, Department of Health, Disability and Ageing

During Horizon 1, the Department of Home Affairs set out to improve the cyber security of apps as a first step to enhancing software security. It committed to providing guidance on actions that app stores and developers can take to protect consumers and businesses from cyber attacks.

Home Affairs conducted targeted consultation with a significant portion of app store market and development stakeholders with equities in Australia to inform the development of the code of practice. Ninety-one percent of consulted stakeholders were supportive of international alignment and Australia's adoption of global best practice where possible. As a small technology market, both in terms of app users and app developers, Government understood industry's preference for identifying and aligning with an existing approach.

Following the release of a discussion paper and industry feedback, the Australian Voluntary Code of Practice for App Store Operators and App Developers was published in October 2025.

**8d. Harmonising software security standards**

Lead agency: Department of Home Affairs

Contributing: Attorney General's Department, Department of Foreign Affairs and Trade, Digital Transformation Agency, Department of the Prime Minister and Cabinet

Led by the United States, this Quad[38] initiative sought to harmonise software standards for government procurement across Quad partners and to leverage their collective buying power to set strong IT security standards across global markets. By leveraging the voice of the Quad, the 4 countries sought to promote and strengthen a culture where software security is by design and default.

In the Quad Leaders' Statement released on 21 September 2024, Australia joined Quad partners in identifying joint efforts on pursuing secure software development standards and certification, and the ongoing work to harmonise those standards.

**8e. Technology Vendor Review Framework**

Lead agency: Department of Home Affairs

Contributing: Australian Signals Directorate, Australian Security Intelligence Organisation, Department of Defence, Office of National Intelligence, Department of Foreign Affairs and Trade, Department of Industry, Science and Resources, Department of the Prime Minister and Cabinet, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, The Treasury, Department of Finance, Department of Climate Change, Energy, the Environment and Water, Attorney-General's Department.

The Technology Vendor Review Framework, announced in December 2024, established a dedicated and proactive process for assessing risks related to foreign ownership, control or influence associated with technology vendors. The framework enables Government to analyse vendor related security risks and provide guidance practical mitigations to support informed procurement decisions across both the public and private sectors.

By identifying systemic vulnerabilities before high risk technology is embedded in critical systems, Australia is able to move from reactive fixes to proactive risk control. The decisions that flow from the Technology Vendor Review Framework will help to keep essential services and sensitive data safer, while supporting timely, consistent, and proportionate procurement strategies across the economy.

The framework is country agnostic and risk based, ensuring that security outcomes are balanced and do not unnecessarily discourage technology adoption or innovation.

To protect the integrity of its processes and safeguard information relevant to national security, the framework will not be publicly released.

38. A diplomatic partnership between Australia, India, Japan, and the United States.

**Stakeholder Insights 4: Secure technology**

Looking forward to Horizon 2, stakeholders have expressed that the expanding attack surface of smart devices, including edge devices and operational technology, opens Australians up to more targeted and frequent attacks. Between 2023 and 2024, there was a surge in threat actors exploiting vulnerabilities in edge devices and virtual private networks, up to 22% of vulnerabilities exploited from 3%.[39]

Stakeholders noted a need to focus on uplifting smart device cyber security in areas where those most affected by a cyber incident also have limited control over device security. They suggested we should prioritise a human-centred approach to smart device security. This includes ensuring the devices are manufactured to be secure-by-design and default, and that we look to innovations in the market to balance security and regulatory friction.

They also emphasised the importance of proportionate, risk-based and internationally aligned measures to uplift the cyber security of a broader range of technologies across their lifecycle. In discussions, stakeholders called for Australia to be a fast follower and contribute to international discussions shaping consumer-grade edge device security.

Additionally, stakeholders indicated a need to invest more in consumer education and awareness raising, to increase information and knowledge about smart device cyber security and contribute to a secure-by-demand market expectation.

In discussion paper submissions, artificial intelligence and post-quantum cryptography were firmly in industry's line of sight. The clear rapid advancement of these emerging technologies was recognised as a transformative trend that will shape the future threat landscape.

## Action 9: Protect our most valuable data sets

**9a. Review of Australia's most sensitive and critical data sets**

Lead agency: Department of Home Affairs

Contributing: Attorney General's Department, Australian Security Intelligence Organisation, Department of Defence, Department of Industry, Science and Resources, Department of Finance, Department of Health, Disability and Ageing, The Treasury

In 2025, the Department of Home Affairs undertook a review of Australia's most sensitive and critical data sets. The final review report was finalised in November 2025, following a threat landscape assessment, regulatory landscape analysis and targeted industry engagement.

The review found that the data lifecycle of sensitive and critical data is opaque and difficult to track, especially across borders and systems. Current regulatory frameworks do not provide comprehensive protection, leaving gaps for de-identified data and data stored or processed offshore, further compounding the risk. The review also identified a need for a robust, repeatable process to systematically identify and assess risks to sensitive and critical data, which will underpin effective policy and regulatory interventions.

39. Verizon (2025), 2025 Data Breach Investigations Report (p. 21).

The Data Sets of National Significance initiative will subsequently progress the review recommendations, with:

- a pilot of the Risk Assessment Framework;
- the development of voluntary guidelines informed by engagement with Commonwealth agencies, state and territory governments and industry stakeholders; and
- the operationalisation of the Risk Assessment Framework across Commonwealth portfolios.

**9b. Review of Commonwealth legislative data retention requirements**

Lead agencies: Attorney General's Department, Department of Home Affairs

Contributing: Department of Finance, Office of Australian Information Commissioner, The Treasury

This review responds to recent large-scale data breaches that have impacted millions of Australians and highlight the risks of entities retaining large volumes of data. A key focus was on the over-retention of data and whether ambiguous or complex data retention obligations in Commonwealth legislation could be simplified to reduce this practice.

Following targeted consultation with industry stakeholders between February and April 2025, the Data Retention Review was finalised in November 2025. The review found that the current regulatory landscape is complex, with overlapping, inconsistent and ambiguous retention periods. It concluded that it is the cumulative effect, rather than any particular piece of legislation, that presents the primary challenge for industry. It heard strong calls for clearer industry guidance and support for Digital ID to reduce personal information holdings.

Work is underway to implement the 6 review recommendations to modernise Commonwealth legislation, provide greater clarity for industry and Commonwealth agencies, and to address related cyber and privacy risks. This has included the development of the 'Data retention principles to guide Commonwealth policy development'. Delivering on these recommendations will promote a culture of data minimisation and reduce regulatory burden for industry.

**9c. Review of the data brokerage ecosystem**

Lead agency: Department of Home Affairs

Contributing: Office of the Australian Information Commissioner, Attorney General's Department, Australian Security Intelligence Organisation, Department of Defence, Department of Industry, Science and Resources, The Treasury

Stakeholder consultations and analysis have confirmed that the data brokerage ecosystem's increasing scale, complexity and opacity, combined with the sensitive nature of traded data, present serious and growing risks to Australia's security. Malicious actors exploit commercial data markets as a low-cost, low-risk method to access Australians' data, including personal and sensitive information. Recent incidents, such as the exposure of the Prime Minister's mobile number, highlight tangible vulnerabilities in existing data brokerage safeguards.

The Data Brokerage Review evaluated the threat posed by malicious actors accessing Australians' data via legal markets, assessed the adequacy of existing laws and policies in regulating such access, and considered international responses. This review complements work underway to reform Australia's *Privacy Act 1988* and the Australian Competition and Consumer Commission's Digital Services Inquiry.

A final report was delivered in November 2025 following consultation with key government and academic stakeholders. The Review found that strengthening privacy protections and enforcement will deliver positive national security outcomes, but additional government intervention is required to encourage the proactive management of security risks within the ecosystem. Implementing these findings will be a focus in Horizon 2.

**9d. Voluntary data classification model**

Lead agency: Department of Home Affairs

Contributing: Attorney General's Department, Department of Industry, Science and Resources, Department of Finance, The Treasury

The voluntary data classification model was developed to help Australian industry assess and communicate the value of their data holdings in a consistent way. This will improve data security practices and enable trusted data sharing.

The model was designed by data scientists from the Commonwealth Scientific and Industrial Research Organisation's Data61 in partnership with the Department of Home Affairs. Industry representatives were involved in the design and testing phases, and their feedback informed development of the final product, now called the Industry Data Classification Framework.

The Framework is due to be released in 2026. Feedback indicated strong support for the model and its potential to provide a common language, and positive views on its practicality and alignment with existing standards.

Under Horizon 2, the Department of Home Affairs will enhance the Framework and expand resources to support industry adoption, in particular small-medium enterprises. Engagement with Commonwealth agencies will continue to ensure the Framework aligns to other frameworks and standards.

# Action 10: Promote the safe use of emerging technology

**10a. Embed cyber security into responsible artificial intelligence**

Lead agencies: Department of Home Affairs (through the National Security Node), Department of Industry, Science and Resources

Contributing: Australian Signals Directorate

The objective of this initiative was to ensure cyber security was embedded into the Department of Home Affairs' work on responsible artificial intelligence policy. On 4 June 2024, the Department established a team to provide national security policy advice to support whole-of-government artificial intelligence policy development.

One tangible example of cyber security being embedded into the Department of Home Affairs' policy development on AI was the February 2025 Direction issued under the Protective Security Policy Framework (Direction 001 2025). This Direction requires Australian Government entities to prevent the access, use or installation of DeepSeek products, applications and web services, and removal where found. This was based on threat and risk analysis that considered, amongst other factors, cyber security issues.

Additionally, under the Government's National Artificial Intelligence Plan, Home Affairs, the National Intelligence Community and law enforcement agencies will continue efforts to proactively mitigate the most serious risks posed by artificial intelligence.

**10b. Post-quantum cryptography standards**

Lead agency: Australian Signals Directorate

Contributing: Commonwealth Scientific and Industrial Research Organisation, Department of Industry, Science and Resources

Advances in quantum computing could leave contemporary cryptography insecure, meaning that the technology we have become reliant on to protect our data will no longer keep our information safe. To prepare for these risks, we must anticipate future requirements of encrypted systems as we transition to post-quantum cryptography.

The Australian Signals Directorate has published initial standards for post-quantum cryptography by updating guidance within the Information Security Manual. This has included adding 2 post-quantum cryptography algorithms to the list of the Directorate Approved Cryptographic Algorithms, as well as identifying traditional cryptographic algorithms that are not quantum-resistant and are not approved by the Directorate beyond 2030. The Directorate has also provided advice on the implementation of post-quantum cryptography by 2030.

Setting a 2030 timeline for implementing post-quantum cryptography brings Australia in line with its Five Eyes peers who have set similar trajectories for post-quantum cryptography transition. The Directorate is monitoring international post-quantum cryptography standardisation efforts and will continue to update its public guidance accordingly.

Shield 3

# World-class threat sharing and blocking

## Desired Outcomes: From the Strategy (p. 34)

**Australians should feel confident that the Government and industry are working together to identify and block cyber threats before they cause significant harm.**

The **Government** draws on its access to expertise and information from classified sources to **help businesses anticipate and respond to sophisticated cyber threats.**

Meanwhile, **industry** provides **real-time data on emerging threats and vulnerabilities,** helping the Government to **enhance preparedness and response options**.

By 2030, we will have a **thriving whole-of-economy threat sharing and blocking network** that will build on the Australian Signals Directorate's existing intelligence threat sharing platforms to enhance our ability to share cyber threat intelligence at machine speed across the nation.

This network will include enhanced **industry-to-industry information sharing**, providing a multi-directional 'hub and spoke' model feeding data back into government threat intelligence systems and **enabling information to be effectively distributed to industry**.

**Real-time threat sharing** will facilitate **automated threat-blocking capabilities**, enabling industry and the Government to **block cyber threats before they reach end users**.

**Key inputs**: 8 agencies worked together in partnership with industry and others towards achieving these desired outcomes across 6 initiatives through an investment of $9.4 million.

The key outputs and their outcomes are outlined over the following pages.

## Action 11: Create a whole-of-economy threat intelligence network

**11a. Executive Cyber Council**

Lead agency: Department of Home Affairs

Contributing: Australian Signals Directorate

The Executive Cyber Council (the Council) was established in November 2023 as a key initiative under Horizon 1 of the Strategy. Chaired by the Minister for Cyber Security, the Council brings together senior representatives from government, civil society, peak bodies, and private sector companies across critical sectors such as banking, retail, telecommunications, transport and technology.

Its achievements include the creation of 4 working groups focused on priority areas: cyber workforce development, sovereign cyber capability, emerging technology, and small and medium business resilience.

Notably, the Council facilitated the Cyber Workforce Summit, which informed the development of the Australian Cyber Workforce Playbook, and launched the Stop the Hack campaign to empower small businesses.

Through regular meetings and collaborative activities, the Council has fostered strategic insights, coordinated national cyber shields and advanced public-private partnerships, ensuring diverse perspectives inform Australia's cyber resilience efforts.

In accordance with the Council's Terms of Reference, the National Cyber Security Coordinator undertook a review to assess the Council's effectiveness and impact on uplifting national cyber security in the context of Horizon 1 of the Strategy. The review was conducted between August and October 2025 and was informed by survey responses received from 19 of the 31 Council members. Responses noted that the Council is effective, having a positive impact on the uplift of national cyber security and supporting strategic objectives in line with the Strategy. The Review identified 4 recommendations which seek to ensure the Council remains fit-for-purpose and well-positioned to progress national cyber security priorities. All recommendations were endorsed by the Minister for Cyber Security as Chair of the Council.

This Council is ongoing under Horizon 2. An expression of interest process was conducted in early 2026 which determined membership for the second two-year term of the Council. By end Q2 2026, a program of work will be agreed to ensure that the current industry-led working groups are aligned with the objectives of Horizon 2, with the possibility that new industry-led working groups are established.

**11b. Continue to enhance Australian Signals Directorate's existing threat sharing platforms**

Lead agency: Australian Signals Directorate

Contributing: Australian Communication and Media Authority, Attorney General's Department, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

The Australian Signals Directorate's enhancements to its Cyber Threat Intelligence Sharing platform have bridged a gap between cyber threat intelligence generation and the disruption of malicious infrastructure.

Collaboration with industry partners, including Microsoft's Sentinel platform (in March 2024) and Splunk (in September 2025), enabled network defenders to efficiently integrate Cyber Threat Intelligence Sharing into their cyber defences. These integrations enable machine-to-machine exchange of cyber threat intelligence at increased speed and scale. They also provided a framework for industry-to-industry and government-to-industry cyber threat intelligence exchange.

In November 2024, the Directorate brought the Cyber Threat Intelligence Sharing platform in-house to enhance government and industry's ability to share cyber threat intelligence and create a cutting-edge global cyber threat intelligence system.

The Directorate created a closed group with trusted entities in the finance and telecommunications sectors under the Threat Sharing and Threat Blocking Scheme. The purpose was to promote sharing intelligence through Cyber Threat Intelligence Sharing to enable the effective and timely blocking of cyber threats at the telecommunications level for the protection of all Australians.

As at October 2025, Cyber Threat Intelligence Sharing has shared over 2,984,000 indicators of compromise with platform partners. In the 2024-25 financial year, the number of partners expanded to 450—a 13% increase from the past year.

In Horizon 2, the Directorate will continue to enhance the Cyber Threat Intelligence Sharing platform, and prioritise the on-boarding of the large volume of government and industry entities seeking to join.

**Data Snapshot 2: Investments in threat sharing and analytics reduce cyber breach impact**

Threat intelligence is one of several factors that have been shown to reduce the cost of a cyber breach, alongside integrating security at every stage of software development, AI and machine learning insights, and security analytics.[40] In 2025, according to IBM, the global average cost impact of a data breach reduced for the first time in 5 years, including in Australia.[41] IBM reported that, 'shorter breach investigations are pushing down detection and escalation costs'.[42]

Harvard's Cyber Strategy Scorecard highlighted 'Australia's robust threat intelligence and blocking program' as an excellent example 'of how governments can improve real-time threat intelligence and knowledge sharing between public and private sectors'.[43]

**11c. Threat sharing acceleration fund**

Lead agency: Department of Home Affairs

Contributing: Australian Media and Communications Authority, Australian Digital Health Agency, Attorney General's Department, Australian Signals Directorate, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, Department of Health, Disability and Ageing

Information Sharing and Analysis Centres provide an intelligence-sharing platform where participants interact and share information regarding cyber threats on their gateways and networks. The focus in Horizon 1 was on establishing a pilot Centre for low maturity sectors in Australia. The health sector and its suppliers hold highly sensitive and personal data about the health and wellbeing of Australians. As the health industry sector continues its digital transformation, the sector must be able to respond to cyber threats as they arise.

In January 2025, CI-ISAC was awarded a $6.423 million seed funding grant over 3 years to establish a Centre to support industry-to-industry threat intelligence sharing in the health sector.

*The health sector holds some of the most highly sensitive and personal data about Australians, but it did not have a mature cyber threat sharing ecosystem.*

*The now-60 members of Australia's Health Cyber Security Network have found the intelligence shared enables them to patch vulnerabilities and understand gaps in their network environment.*

40. IBM (2025), Cost of a Data Breach Report 2025: The AI Oversight Gap (p. 21).
41. IBM (2025), Cost of a Data Breach Report 2025: The AI Oversight Gap (p. 11).
42. IBM (2025), Cost of a Data Breach Report 2025: The AI Oversight Gap (p. 10).
43. Heiding F, O'Neill A, Price L (2025), Cyber Security Strategy Scorecard (p. 55).

The program will ensure compatibility with the national cyber threat intelligence platform, the Australian Signals Directorate's Cyber Threat Intelligence Sharing. This will ensure existing threat intelligence sharing forums can share meaningful threat intelligence with the healthcare ecosystem.

The Health Cyber Security Network established under the program has enabled organisations within the sector to exchange cyber security threat information with greater speed and security. The now-60 members across Australia—covering over 600 health facilities—report that high-quality intelligence advisories enable them to patch vulnerabilities faster, respond to common vulnerabilities and exploitations ahead of public disclosure, and identify systemic gaps across their environments. This bi-directional sharing model provides a measurable shift from reactive to proactive cyber security across the health sector. The program must be self-sustaining within 3 years of commencement; CI-ISAC is on track to achieve this by 2027.

**11d. Incentivise industry to participate in threat sharing platforms**

Lead agency: Department of Home Affairs

Contributing: Australian Communication and Media Authority, Attorney General's Department, Australian Signals Directorate, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

This initiative aimed to identify barriers and challenges to threat sharing and blocking at scale. It focused on organisations that are most capable of collecting and sharing threat intelligence, and threat blocking at scale, and the identification of options to encourage and incentivise industry to participate.

Following extensive consultation in 2024 and 2025, including workshops and a consultation paper, final findings have been shared with industry via National Cyber Intel Partnership. Under Horizon 2, options to address the consultation findings and amplify current initiatives will be taken forward.

## Action 12: Scale threat blocking capabilities to stop cyber attacks

**12a. Pilot next-generation threat blocking capabilities**

Lead agency: Department of Home Affairs

Contributing: Australian Signals Directorate

The National Cyber Intel Partnership was established with the inaugural meeting held on 8 September 2023 (then known as the Threat Blocking Steering Group) and is chaired by the National Cyber Security Coordinator. It has been instrumental in enhancing threat intelligence sharing and piloting new threat blocking capabilities across Australian networks.

Since its inception in September 2023, the National Cyber Intel Partnership has convened industry leaders and cyber experts to promote the exchange of technical indicators and best practices, leading to the development of a threat blocking capability scheme.

This scheme, initially focused on banking-related phishing threats, has expanded to include major corporations and telecommunications providers, such as Westpac, Telstra, Woolworths, ANZ, NAB, CBA, Optus, and TPG.

The Partnership's achievements in Horizon 1 include optimising processes for intelligence sharing, scaling threat blocking activities, and integrating government and industry capabilities to protect end users.

This work will continue under Horizon 2.

**12b. Incentivise threat blocking across the economy**

Lead agency: Department of Home Affairs

Contributing: Australian Communication and Media Authority, Attorney General's Department, Australian Signals Directorate, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

This initiative is covered under 11d.

**Stakeholder Insights 5: Threat sharing and blocking**

During Horizon 2 submissions and co-design workshops, participants called for expanded involvement in threat sharing and a more coordinated whole-of-system approach to threat blocking. More support and guidance from government on threat blocking was requested, as well as the establishment of more trusted groups that can block threats at scale.

There was also a clear desire expressed across sectors to move towards a more proactive cyber posture. This involves improving the speed and utility of threat intelligence sharing, blocking threats upstream before they reach end-users and clarifying permissible active cyber defence activities organisations can undertake in Australia.

There was a shared view that vulnerability disclosure should remain voluntary, except perhaps for critical infrastructure. It was suggested that a best practice voluntary disclosure policy toolkit could be a good next step.

Legislative protections for security researchers were expressed by stakeholders as desirable so researchers can safely report vulnerabilities. However, it was emphasised that protections should not provide a mechanism for malicious actors to skirt the law. Industry suggested that government could lead the way to implementing bug bounties.

Shield 4

# Protected critical infrastructure

## Desired Outcomes: From the Strategy (p. 38)

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

In 2030, every Australian should have peace of mind, knowing that **essential services**—such as our electricity grid, water supply and banking systems—are **able to withstand and bounce back** from hazards that might disrupt their functions.

The array of **critical infrastructure** we rely on every day must be able to **better prevent, respond, and be resilient to cyber attacks**.

**Owners and operators** of critical infrastructure and designated Systems of National Significance need to have **clear visibility of the risks they face**—including cyber threats, personnel risks, physical hazards, supply chain disruptions, and natural disasters.

Under the SOCI Act, they must **put appropriate risk mitigation plans** in place to protect against these threats.

Through regulation and proactive collaboration, the Government will work with industry to provide a high level of assurance that **owners and operators** are **complying with their security obligations**.

The **Australian Government** will also **lead by example**. Government needs to hold itself to the same standard as it imposes on industry.

As we increasingly adopt new and enhanced technology to support a range of **government services**, we will strive for a **high level of cyber maturity**, fostering public trust that we meet world-class cyber security standards.

In doing so, we will **work with state, territory and local governments** to build a **nationally consistent and robust** culture of cyber resilience.

**Key inputs**: Over 15 agencies worked together towards achieving these desired outcomes across 14 initiatives through an investment of $143.6 million.

The key outputs and their outcomes are outlined over the following pages.

# Action 13: Clarify the scope of critical infrastructure regulation

**13a. Aligning telecommunication providers to the same standards as other critical infrastructure entities**

Lead agency: Department of Home Affairs

Contributing: Australian Communications and Media Authority, Attorney General's Department, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

This initiative aligned telecommunication providers to the same standards as other critical infrastructure entities. This was achieved by moving security regulation of the carriers and carriage service providers from the *Telecommunications Act 1997* to the *Security of Critical Infrastructure Act 2018* (SOCI Act) via the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* which received Royal Assent in November 2024. The *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025*, registered on 4 March 2025, set out a telecommunications-specific risk management program to address all hazards, with a focus on unique risks to critical telecommunications assets.

On 4 April 2025, both primary and subordinate legislation effecting the transition of telecommunications security regulation to the SOCI Act framework commenced and policy guidance was published on the Critical Infrastructure Security Centre's website.

Stakeholders in Horizon 2 co-design workshops and roundtables reported that the SOCI Act and critical infrastructure reforms were amongst those that had the biggest positive impact on Australia's cyber security in Horizon 1 (see Appendix).

**13b. Clarifying the regulation of managed service providers**

Lead agency: Department of Home Affairs

Contributing: Digital Transformation Agency

Industry stakeholders raised concerns that the definition of 'data storage or processing providers' introduced through the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* was overly broad, particularly in its application to managed service providers (MSPs). In response, Home Affairs developed targeted guidance to clarify how the SOCI Act applies to MSPs.

The guidance clarifies which entities are intended to be captured under the Act and the obligations that apply to them, supporting critical infrastructure owners and operators to better manage risks associated with the use of MSPs. It was developed in consultation with industry through the Trusted Information Sharing Network in September 2025 and has been published on the Cyber and Infrastructure Security Centre website in November 2025. This initiative provides greater regulatory certainty for affected entities, and contributes to a broader security uplift across the data storage and processing sector through improved transparency and industry collaboration.

As noted for 13a, the SOCI Act and critical infrastructure reforms were among those initiatives that co design workshop and roundtable participants thought had the biggest positive impact on Australia's cyber security in Horizon 1 (see Appendix).

**13c. Explore options to incorporate cyber security regulation as part of expanded 'all hazards' requirements for the aviation and maritime sectors**

Lead agency: Department of Home Affairs

Contributing: Australian Criminal Intelligence Commission, Australian Federal Police, Attorney General's Department, Australia Maritime Safety Authority, Australian Signals Directorate, Civil Aviation Safety Authority, Department of Climate Change, Energy, the Environment and Water, Department of Defence, Department of Employment and Workforce Relations, Department of Foreign Affairs and Trade, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, Department of Prime Minister and Cabinet

The ability for Government to set minimum cyber security requirements for the aviation and maritime sectors will help to ensure these sectors appropriately mitigate cyber risks posed by state-sponsored actors, cyber-criminal threat actors and human error. The first step in achieving this objective was the passage of, and Royal Assent for, the *Transport Security Amendment (Security of Australia's Transport Sector) Act 2025* (TSA Act) in March 2025.

The TSA Act introduced an all-hazards security framework in the *Aviation Transport Security Act 2004* and the *Maritime Transport and Offshore Facilities Security Act 2003* which will, through amendments to subordinate legislation, set minimum standards for regulated industry participants to meet all hazard security obligations, including cyber security. Under the all-hazards security framework, aviation and maritime industry participants will be required to mitigate risks specific to their operating and threat environments.

As at January 2026, Home Affairs is progressing regulatory amendments, which will include the specific cyber security requirements for the aviation and maritime sectors. The majority of industry participants supported the introduction of an all-hazards security framework, including new cyber security requirements. In response to stakeholder concerns regarding regulatory burden and duplication, Home Affairs has committed to ensuring the amended regulations and associated guidance are clear and accessible, and to addressing legislative duplication, where practicable.

**13d. Protecting critical infrastructure critical data**

Lead agency: Department of Home Affairs

Contributing: Attorney General's Department, Office of the Australian Information Commissioner

This initiative aimed to protect the critical data held, used and processed by critical infrastructure in 'business-critical' data storage systems.

Delivery of this initiative was achieved through its inclusion in the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* which received Royal Assent in November 2024.

The amendment clarified the application of the SOCI Act to ensure critical infrastructure entities are protecting their data storage systems where vulnerabilities to those systems could impact the availability, integrity, reliability or confidentiality of critical infrastructure.

As noted for 13a, the SOCI Act and critical infrastructure reforms were among those initiatives that co design workshop and roundtable participants thought had the biggest positive impact on Australia's cyber security in Horizon 1 (see Appendix).

Stakeholders were broadly supportive of the proposed reforms to data storage systems. Guidance was released in November 2024 to resolve ambiguity around business critical data and secondary systems, which has had a positive impact on clarifying obligations and promoting compliance with stakeholders.

Submissions from the Horizon 2 discussion paper outline support for this initiative and its approach to establish security standards whilst strengthening and standardising obligations across critical infrastructure assets.

**Stakeholder Insights 6: Positive Feedback on Critical Infrastructure Reforms**

Australia's critical infrastructure cyber security reforms were commonly cited by participants in Horizon 2 co-design workshops and roundtables as one of Horizon 1's most positively impactful actions.[44]

In their Horizon 2 submission, CISO Lens noted that the critical infrastructure shield is 'popular among both critical infrastructure and non-critical infrastructure organisations…likely an indication these organisations recognise the benefits of improved critical infrastructure to their broader supply chains'.[45]

Harvard's Cyber Security Scorecard cited Australia's critical infrastructure reforms as a key strength. The 'critical infrastructure defense concept, underpinned by the landmark SOCI Act, sets the standard worthy of emulation' and one of the bases upon which the 'Australian strategy should be treated as a model for upper-middle tier powers'.[46]

44. See the Impact Poll results in the Appendix.
45. CISO Lens (2025), Submission: Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy (p. 7).
46. Heiding F, O'Neill A and Price L (2025), Cyber Security Strategy Scorecard (p. 29).

# Action 14: Strengthen cyber security obligations and compliance for critical infrastructure

**14a. Enhanced Cyber Security Obligations**

Lead agency: Department of Home Affairs

Contributing: Commonwealth agencies and regulators, state and territory agencies and regulators, as appropriate

This initiative undertook to activate Enhanced Cyber Security Obligations for Systems of National Significance, including requirements to develop cyber incident response plans, undertake cyber security exercises, conduct vulnerability assessments, and provide system information to ASD to develop and maintain a near real-time threat picture.

These Enhanced Cyber Security Obligations seek to uplift the preparedness and resilience of Australia's most significant critical infrastructure assets to effectively prepare for and respond to a major cyber security incident.

The Incident Response Planning and Cyber Security Exercise Enhanced Cyber Security Obligations have been applied to all responsible entities, except for a small number of entities in the financial sector where alternate regulatory frameworks are in place. The Vulnerability Assessment and System Information Enhanced Cyber Security Obligations are available to be used on a targeted basis, where a regulatory response is required.

See the Evidence Use Showcase box below for further information on how the Enhanced Cyber Security Obligations program has been uplifting the cyber security of Australia's most vital critical infrastructure assets through continuous feedback and actionable insights.

Future compliance and assurance activities aim to uplift security and resilience of Systems of National Significance entities by encouraging them to aspire toward higher standards of incident preparedness, cyber security and resilience. Rather than expanding security obligations or enforcement, the Horizon 2 proposal builds on Home Affairs' partnership with industry through a mix of both regulatory and non-regulatory engagement initiatives. These initiatives will provide a greater understanding of the cyber preparedness of our most interdependent critical infrastructure, enabling more effective and timely responses to cyber threats.

**Evidence Use Showcase 3: Enhanced Cyber Security Obligations**

The Enhanced Cyber Security Obligations regime has been designed to support Systems of National Significance entities to prepare for and respond to a major cyber security incident.

To accompany the regulatory regime, Home Affairs provides clear Enhanced Cyber Security Obligations guidance, a framework outlining 'what good looks like', and structured assessments to support compliance and uplift of cyber security maturity. Synthesising findings from regulated entity assessments and sharing actionable insights across critical infrastructure owners and operators has ensured continuous improvement and preparation for evolving threats, while reinforcing transparency and trust between government and industry.

This has been achieved by synthesising evidence into actionable feedback.

Home Affairs has assessed organisations' incident response plans and cyber security exercise reports against published guidance. The synthesis of findings identified sector-wide trends, common gaps and leading practices.

Assessment findings informed targeted interventions, including tailored bilateral briefings with organisations to deliver specific and actionable feedback. These findings have also been developed into reports outlining key insights and recommendations for entities to improve cyber preparedness.

These reports have been shared with all Systems of National Significance entities and other critical infrastructure organisations via the Trusted Information Sharing Network.

This analysis and engagement function will remain a priority and expand over time. Continued assessments will provide quantitative trends of cyber preparedness uplift across time.

As a result, Australia's Systems of National Significance are more secure and resilient

Regulated entities report greater clarity on expectations and improved capability to respond to cyber security incidents, demonstrating how evidence-driven evaluation translates regulatory obligations into meaningful security outcomes.

CISO Lens reported in its submission to the Horizon 2 consultation process that its members were mostly positive in their assessment of the SOCI Act, 'with members understanding their obligations and the role…of the regulator.'[47] Furthermore, CISO Lens noted the:

> *'requirements of the SOCI Act are generally considered beneficial to improving the security posture of regulated organisations, Moreover, the regulatory burden is considered proportionate to the risk and outcomes being sought, and the department's emphasis on education before enforcement is appreciated'.*

**14b. Security of Critical Infrastructure Compliance Monitoring and Evaluation Framework**

Lead agency: Department of Home Affairs

Contributing: Commonwealth, state and territory agencies and regulators, as appropriate

The Security of Critical Infrastructure Compliance Monitoring and Evaluation Framework was finalised in October 2025. It outlines how the Department of Home Affairs will evaluate its performance in providing assurance that industry is complying with obligations set out in the SOCI Act. Home Affairs will establish annual compliance plans, which will be evaluated at the end of each financial year. Routine evaluation of compliance activities will drive continuous business improvement and enable Home Affairs to assess the effectiveness of its regulatory posture under the SOCI Act. Key outcomes from the annual evaluations will be reported through Home Affairs' Annual Report as required.

47. CISO Lens (2025) Submission: Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy (p. 14).

**14c. Expand crisis response arrangements to capture secondary consequences from significant incidents**

Lead agency: Department of Home Affairs

Contributing: Australian Signals Directorate, Commonwealth agencies and regulators, state and territory agencies and regulators, as appropriate

Initiative 14c was delivered through the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* receiving Royal Assent in November 2024. This initiative expanded crisis response arrangements to ensure they capture secondary consequences from significant incidents. Government consulted industry on introducing an all-hazards consequence management power that allows it to direct an entity to take specific actions to manage the consequences of any incident. This is a last-resort power, used where no other powers are available and where it does not interfere with or impede a law enforcement action or regulatory action.

As noted for 13a, the SOCI Act and critical infrastructure reforms were among those initiatives that co design workshop and roundtable participants thought had the biggest positive impact on Australia's cyber security in Horizon 1 (see Appendix).

## Action 15: Uplift cyber security of the Commonwealth Government

**15a. Government Cyber Security Uplift**

Lead agency: Department of Home Affairs

Contributing: Australian Signals Directorate, Digital Transformation Agency

Throughout Horizon 1, the National Office of Cyber Security, working closely with counterparts across Home Affairs, has supported the National Cyber Security Coordinator in promoting and implementing Commonwealth Cyber Security Uplift and the Strategy.

As a key component of Commonwealth Cyber Security Uplift efforts, the Government released the 5 Guiding Principles to Embed a Zero Trust Culture in July 2025, strengthened the Digital Transformation Agency's Investment Oversight Framework process with the inclusion of cyber security assessments, and established a Systems of Government Significance regime.

In addition, the Government is maintaining a robust governance structure that allows effective management of Commonwealth Cyber Security Uplift, through the Commonwealth Cyber Security Uplift Committee and the Cyber Security Private Sector Forum.

**15b. Whole-of-government zero trust culture**

Lead agency: Department of Home Affairs

Contributing: Australian Signals Directorate, Digital Transformation Agency, whole of government

Embedding a zero-trust culture allows opportunities to better combat the current and emergent risks stemming from a rapidly evolving threat landscape. It represents a shift from a traditional strong perimeter protection to a zero-trust architecture, rooted in the core principle of 'never trust, always verify'.

Following government and industry consultation from November 2024 to February 2025, Home Affairs has developed and released 5 Guiding Principles to Embed a Zero Trust Culture in July 2025, to help entities plan for the organisational transformations needed to adopt a Zero Trust approach. These are:

- Identify and manage cyber security risk at an enterprise level
- Understand accountabilities and responsibilities at all levels
- Know and understand your most critical and sensitive technology assets
- Maintain resiliency through a comprehensive cyber strategy and uplift plans
- Go Beyond Incident Planning

In parallel, the Australian Signals Directorate's Australian Cyber Security Centre released the *Foundations for a Modern Defensible Architecture* in February 2025. These Foundations provide a baseline of secure design and architectural activities to help organisations prepare and plan for adopting technologies based on Zero Trust principles. Together, these foundations and the Guiding Principles offer Commonwealth entities the governance and technical guidance needed to begin their Zero Trust architecture journey.

***Using evidence for continuous improvement:***

***The next step is to design and implement the Protective Security Policy Framework Zero Trust Culture Maturity Survey, enabling entities to accurately assess their current cyber security posture and identify priority areas for improvement.***

*Protective Security Policy Framework—Release 2025* mandates Zero Trust Guiding Principles through Requirement 0098[48]. The next step is to build on this baseline by designing and implementing the Protective Security Policy Framework Zero Trust Culture Maturity Survey, enabling entities to accurately assess their current cyber security posture and identify priority areas for improvement.

48. Australian Government Department of Home Affairs (2025) Australian Government Protective Security Policy Framework —Release 2025 (p. 73).

**15c. Commonwealth entities cyber maturity reviews**

Lead agency: Department of Home Affairs

Contributing: Australian Signals Directorate, Digital Transformation Agency

Since July 2024, Home Affairs has been providing specialist cyber policy advice to assist with the strategic prioritisation of digital investments. Home Affairs leads the assessment of the cyber security-specific aspects of proposals submitted through federal budgetary processes via the Digital Transformation Agency's Investment Oversight Framework. This ensures alignment with policy requirements to manage Commonwealth cyber security risk. By embedding cyber security requirements within the broader digital investment assessment process, the Department influences cultural change from the outset, reinforcing the 'secure-by-design' principle. This outcome is demonstrated by integrating cyber risk management into digital investment proposals.

Home Affairs has further matured the Commonwealth cyber security assessment process to reflect critical risk indicators, such as the Systems of Government Significance declaration. Next steps include continuing to reflect Commonwealth Cyber Security Uplift activities in assessment criteria and a deep dive analysis of Commonwealth digital estate areas of concern, such as legacy technology.

**15d. Systems of Government Significance**

Lead agency: Department of Home Affairs

Contributing: Australian Signals Directorate, Department of Defence, Digital Transformation Agency

The Government requires greater visibility of its critical digital functions and systems to prioritise their protection and defence to prevent catastrophic impacts to the nation. To address this need, Home Affairs has developed the Systems of Government Significance regime to identify and prioritise the Government's most critical digital infrastructure for investment and cyber security uplift. This includes an evaluation of the centrality of systems to digital government functions or services and potential for significant consequences to Australia's national interests, economic prosperity and social cohesion if disrupted

The Systems of Government Significance Working Group commenced in December 2024, and Home Affairs carried out 4 test assessments of potential Systems of Government Significance from October 2024 to May 2025. The Systems of Government Significance Regime launched in July 2025, and the first tranche was declared on 3 November 2025, with a second tranche declared on 16 December 2025. A third tranche is expected to be declared in Q2 2026, with a fourth tranche tiering of Systems of Governance Significance finalised in 2026. Home Affairs' process for identifying Systems of Government Significance has been comprehensive, including engagement with 104 entities, and the support of central and implementation agencies.

The next steps include ongoing final tiering and review of the Systems of Government Significance list, embedding systems in Digital Investment Oversight process (see initiative 15c), and analysis of assessment data to identify trends and drive opportunities for prioritised security protections. This will elevate Systems of Government Significance risk management and ensure readiness and resilience across the regime.

**15e. Uplifting the cyber skills of the Australian Public Service**

Lead agency: Department of Home Affairs

Contributing: Australian Signals Directorate, Department of Defence, Digital Transformation Agency, Australian Public Service Commission

This initiative was delivered through the publication of the *Australian Public Service Data, Digital and Cyber Workforce Plan 2025-30* in March 2025.

The Australian Public Service Commission worked with the Skills Framework for the Information Age Foundation and relevant stakeholders on the expansion of the Foundation support development of cyber skills of the APS, harnessing the Digital Profession and Australian Public Service Academy to provide a whole-of-government approach to addressing cyber skills shortages in the Australian Public Service, as well as through the establishment of the Defence Cyber College.

## Action 16: Pressure-test our critical infrastructure to identify vulnerabilities

**16a. National Cyber Exercise Program expansion**

Lead agency: Department of Home Affairs

Contributing: Attorney General's Department, Department of Defence, National Emergency Management Agency

The National Cyber Exercise Program enables the National Cyber Security Coordinator to ensure that Government departments' cyber security exercise programs are integrated. Working with Government agencies, the Program captures planned and undertaken cyber security exercises in which agencies will practice responses to hypothetical cyber incidents and test their level of preparedness. The Program aids the National Cyber Security Coordinator and the National Office of Cyber Security in identifying gaps or sectors that require further focus or should be prioritised.

In November 2024, the National Cyber Security Coordinator launched the program, seeking input from government departments and agencies. By the end of 2025, 117 exercises were registered and conducted in the program.

As a part of its remit, the National Office of Cyber Security Exercise Program delivers national cyber security coordination and consequence management exercises to improve collaboration and coordination between government and industry stakeholders during cyber security incidents. The National Office of Cyber Security-Exercise Program is conducted through tabletop discussion exercises. 28 cyber security exercises have been delivered since the launch of the Strategy in line with ongoing work to expand Australia's National Cyber Exercise Program.

The Evidence Use Showcase below highlights how the National Office of Cyber Security is using exercises as a feedback loop for cyber security preparedness.

To meet the growing threat and complexity of response arrangements in an ever-increasingly connected environment, the National Office of Cyber Security will strengthen its program in Horizon 2 hosting multiple cross-sector exercises with industry and government departments, including Systems of Government Significance, and with sectors of Australian industry and critical infrastructure not previously target. Additionally, the National Office of Cyber Security will strengthen Australia's supply chain resilience by delivering scalable exercises and targeted readiness activities to address cyber risks and mitigate economic impacts through critical infrastructure and major businesses.

**Evidence Use Showcase 4: Exercises as a feedback loop for cyber security preparedness**

Exercises increase government and industry awareness and understanding of the role of the National Cyber Security Coordinator and the National Office of Cyber Security (NOCS), and their capacity to assist government and industry in coordinating whole-of-government consequence management in response to a cyber security incident. The feedback received and lessons identified from exercises are being incorporated into sector-level policies, protocols and plans to assist government and industry stakeholders to coordinate responses to cyber incidents impacting Australia's critical infrastructure.

The National Office of Cyber Security-Exercise Program has expanded its leadership of national exercising and its participation reach over the course of 2025. In 2024, the National Office of Cyber Security led 11 exercises and participated in 11. In 2025, the NOCS led 17 exercises and participated in 40. After each exercise, the National Office of Cyber Security collects exercise participants' feedback via a survey. In the current survey, in use since July 2025, 97% of surveyed participants indicated that the National Office of Cyber Security-led cyber preparedness exercises provided meaningful cyber security preparedness insights. Participants have reported that 'the scenarios were well thought out and relevant to potential issues that can arise' and it was 'good to find out NOCS [National Office of Cyber Security] role in [cyber incident response]'.

Through these processes, the National Office of Cyber Security has found that these exercises:

- build stronger industry awareness of the Government's technical, law enforcement and coordination mechanisms available to an impacted entity during a cyber security incident; and
- provide government agencies and industry stakeholders with the opportunity to establish key connections to use during a crisis, noting cyber incident response arrangements (particularly in a crisis) rely heavily on relationship management.

The National Office of Cyber Security is leading a number of exercises in 2026 with government and critical infrastructure sectors, with a focus on larger, cross-sectional exercises and growing complexity.

**16b. Incident response playbooks**

Lead agency: Department of Home Affairs

Contributing: Attorney General's Department, Department of Defence, National Emergency Management Agency

Incident response playbooks are high level guides that outline how the National Office of Cyber Security will coordinate the national response and consequence management activities for a cyber incident impacting an entity in each sector. The playbooks outline how the National Office of Cyber Security will support the impacted entity, government and broader industry response. The playbooks are a key part of government's furthering of trusted and transparent industry to-government relationships on cyber security incident response arrangements.

12 sector playbooks have been delivered and are available on the Home Affairs website. The suite includes playbooks for each of the critical infrastructure sectors as defined under the SOCI Act. The National Office of Cyber Security provided a briefing on the playbooks to the cross-sector Trusted Information Sharing Network platform on 14 May 2025, with over 320 government stakeholders and critical infrastructure owners and operators in attendance throughout the presentation.

Through the publication of these incident response playbooks, several key elements were identified as essential to effective incident response. Overall public sentiment on the development of the playbooks has been positive, and the National Office of Cyber Security will continue to review based on feedback through an annual review process.

Shield 5

# Sovereign capabilities

## Desired Outcomes: From the Strategy (p. 46)

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

By 2030, Australia will foster a **thriving cyber security ecosystem** that **attracts, grows and retains talent,** houses **strong cyber security companies and capabilities,** and **nurtures innovative new technologies.**

Our nation will be **recognised for pioneering wor**k in cyber technology and applied sciences, with a **large, skilled and diverse cyber workforce**.

**High-quality education and training opportunities** will support **defined pathways** into the cyber security profession.

Our cyber workforce will be **professionalised**, with clear standards to validate cyber skills and experience.

By leveraging our existing commitments to landmark reforms across the immigration, education and training systems, we will assemble a **world-class cyber workforce** that **welcomes people** from a wide range of backgrounds.

Our cyber workforce will be **inclusive**, with **strong career opportunities for diverse cohorts** —especially women, who are significantly underrepresented in the sector.

Australia will have a **thriving and robust cyber security industry** that supports national prosperity, generates high-wage jobs, and creates innovative solutions to current and future cyber security requirements.

Cyber security firms will be supported by a **robust market**, with better opportunities to obtain government contracts and investment to stimulate growth.

Australia's **strong academic and research institutions** will continue to drive world leading cyber research and innovation.

Through **closer, focused collaboration between industry and government**, we can tackle some of the toughest cyber security problems and invest in the secure development of emerging technologies like AI and quantum computing.

**Key inputs**: 4 agencies worked together towards achieving these desired outcomes across 4 initiatives through an investment of $8.6 million.

The key outputs and their outcomes are outlined over the following pages.

# Action 17: Grow and professionalise our national cyber workforce

**17a. Migration system reforms to attract global cyber talent**

Lead agency: Department of Home Affairs

Reforms have been made to the migration system to better attract and facilitate the entry of international cyber talent to Australia. These include new visas such as the Skills in Demand Visa and National Innovation Visa, the creation of new residency pathways that improve transition from temporary to permanent residency, and the streamlining of our visa processes. Labour market testing requirements were reformed to make it easier for business to sponsor critical talent, and the Targeted Core Skills Occupation List which included critical cyber security occupations was announced in December 2024.

These reforms have been promoted through existing outreach visa efforts. However, in the event these are not increasing the intake of cyber security talent through these streams, additional outreach resources have been drafted for finalisation and use in Horizon 2.

**17b. Guidance to employers to target and retain diverse cyber talent**

Lead agency: Department of Home Affairs

Contributing: Department of Industry, Science and Resources, Department of the Prime Minister and Cabinet

The Strategy outlines Australia's vision for a flourishing cyber industry, enabled by a diverse and professional cyber workforce. There is a growing body of literature supporting diversity and inclusion in the cyber and technology sector. For example, feedback received during stakeholder roundtables highlighted the unique strengths that neurodivergent individuals bring to the cyber security sector. This initiative also aims to reduce the attraction and recruitment barriers and biases faced by women and First Nations people—Australian 2021 Census data shows that only 17% of cyber security professionals at the time were women.[49] This drops to 5% for the more highly-paid cyber security architects.[50]

Home Affairs, in collaboration with Behavioural Economics Team of the Australian Government (BETA) at the Department of the Prime Minister and Cabinet, published guidance for recruiters to attract a wider diversity of applicants into the cyber security workforce, supporting workforce growth and participation. The Inclusive Cyber Security Recruitment Guidance was published in October 2025. The Evidence Use Showcase below provides more information on how the guidance was evidence-based and how its impact will be further tested in practice through evaluation.

Additionally, the Executive Cyber Council's Cyber Workforce Working Group Cyber Workforce Playbook (see 17c) provides diversity and inclusion guidance for those already working within organisations. These 2 resources complement each other: the Recruiter Guidance to better attract and recruit diverse talent to the cyber security workforce, and Cyber Workforce Playbook provides diversity and inclusion guidance for those who have joined the workforce.

49. Australian Bureau of Statistics (2021) Census of Population and Housing: TableBuilder.
50. Australian Bureau of Statistics (2021) Census of Population and Housing: TableBuilder.

A focus in Horizon 2 will be promoting these resources within the cyber security industry.

**Evidence Use Showcase 5: Workforce diversity guidance**

**Evidence-based research prospectively informed policy development**

BETA led stakeholder engagements and research to develop the Inclusive Cyber Security Recruitment Guidance (the Guidance) in support of the Department of Home Affairs. This Guidance was informed by consultation with cyber security industry professionals who specialise in inclusive recruitment, industry representatives and government partners. The Guidance is underpinned by evidence-based research and incorporates insights from private and public inclusive recruitment programs, academia, and representative associations. As outlined in the Strategy, this Guidance focuses on practical advice to reduce attraction and recruitment barriers and biases faced by women and First Nations people(s).

**The policy will be subsequently evaluated in practice**

The Department of Home Affairs will undertake an evaluation to assess the impact of the Guidance alongside other key diversity and inclusion-based frameworks and resources launched in Horizon 1 to ensure these are holistically addressing the need for a diversity and inclusion toolkit.

**17c. Professionalisation Framework**

Lead agency: Department of Home Affairs

Contributing: Department of Employment and Workplace Relations, Department of Industry, Science and Resources

This initiative aims to provide employers and businesses with assurance that the cyber security professionals they hire have the necessary skills and training. It will support applicants to enter and progress within the sector through horizontal and vertical avenues. By engaging with existing skills frameworks and professional accreditation streams, interoperability with industry and across jurisdictions will be maximised. Growth of the domestic cyber workforce will be fostered and barriers removed to entry for job seekers, existing professionals, and minority groups. A consultative, industry led approach will inform design.

To achieve these goals, the Growing and Professionalising the Cyber Security Industry Program Grant was awarded to the Australian Computer Society and its consortia in November 2025. The grant provides $1.9 million in funding to design, promote and pilot a professionalisation scheme for Australia's cyber security workforce.

Additionally, the Executive Cyber Council and its Cyber Workforce Working Group has taken a strong leadership role in working across industry to explore options and ideas to grow and expand Australia's skills pipeline, and improve the diversity of the cyber workforce. This culminated in the inaugural Cyber Workforce Summit in 2024, which included over 100 participants from industry, government, industry groups and academia. The output from the Summit was the development of the Cyber Workforce Playbook, which provides a suite of actionable tools and guidance for industry to tackle cyber workforce challenges.

**Stakeholder Insights 7: Cyber Security Workforce and Sovereign Capability**

Key themes emerged during Horizon 2 submissions and co-design roundtables, including that data is currently not capturing the nuance of the workforce challenge, particularly the lack of granular data. Deeper collaboration between industry, academia, employers and government was encouraged to ensure early career entrants were workforce ready and to support diverse and flexible entry pathways.

Some of the suggested ways forward included skills-based learning environments, improved national data on workforce trends, improved accessibly and entry points including practical placements.

Government was also encouraged by roundtable participants to reduce information and communication technology concentration risk through amending procurement practices. Stakeholders also suggested that Australia needs to map its sovereign capabilities if we are to truly understand cyber risks and vulnerabilities, and develop mitigation plans.

## Action 18: Accelerate our local cyber industry, research and innovation

**18a. Australian Cyber Security Strategy Challenge Grant**

Lead agency: Department of Home Affairs

Contributing: Department of Industry, Science and Resources

The goal of this initiative was to invest in the growth of Australia's domestic cyber industry. To achieve this, cyber start-ups and small-to-medium businesses were provided with funding to develop innovative solutions to a cyber security challenge articulated by government. This aimed to provide both funding and credibility to start-ups while increasing government agencies' sourcing of new-to-market solutions.

The Department of Home Affairs is leading the grant program through the Department of Industry, Science and Resources' Business Research Innovation Initiative program. The challenge sought innovative solutions on validating the authenticity of information disseminated by the Government. The proposed solution aims to strengthen public trust in the source of government information and improve cyber security in response to new threats in a generative artificial intelligence environment by validating the authenticity of government information.

Grant applications were opened from 7 November 2024 to 18 December 2024, and 59 submissions were received. On 22 October 2025, Home Affairs and DISR announced the 5 successful grant applicants for the feasibility round of the grant, awarding over $440,000 across the 5 entities. Home Affairs is working with successful grant applicants to finalise the feasibility round.

Shield 6

# Resilient region and global leadership

## Desired Outcomes: From the Strategy (p. 52)

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

By 2030, Australia envisages a **region better able to manage, mitigate and recover** from the impacts of cyber incidents.

Australia will continue to **cooperate and build coalitions** with international partners, industry and civil society to s**hape and advocate for rules, norms and standards** that are consistent with our shared interests and values.

Australia will be the **partner of choice for cyber security**, with the trust and expertise required to manage increasing threats to the region; our regional efforts will deliver sustainable and shared cyber resilience.

With our assistance, **partners will have developed and retained the skills and capacity** to be more cyber resilient.

Though threats proliferate, **few attacks will inflict significant damage**, because protections are strong and recovery is swift.

Increased resilience and strategic stability will ensure a**n open, stable and prosperous region**, where citizens and businesses benefit from access to the global digital economy.

**International standards** for critical technologies **will reflect Australia's interests and expertise**.

**Global technology markets** will be **transparent and competitive**, with a diversity of suppliers of products and services that are secure and safe by design.

Australian citizens and businesses will reap the economic and security benefits of **high-quality standards** and **digital trade rules**.

A **stable cyberspace** will be supported by the agreed United Nations framework for **responsible state behaviour.**

There will be **clear consequences** when states contravene their obligations and commitments.

The **internet will be open, free, secure and interoperable**—with responsible and accountable multi-stakeholder management and governance.

**Key inputs**: Over 9 agencies worked together towards achieving these desired outcomes across 8 initiatives through an investment of $129.7 million.

The key outputs and their outcomes are outlined over the following pages.

# Action 19: Support a cyber-resilient region as the partner of choice

**19a. Southeast Asia and Pacific Cyber Program**

Lead agency: Department of Foreign Affairs and Trade

Contributing: Australian Federal Police, Attorney General's Department, Australian Signals Directorate, Department of Defence, Department of Industry, Science and Resources, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, eSafety Commissioner, Department of Home Affairs

Stability across Southeast Asia and the Pacific is vital to Australia's security, prosperity and national interests—as is being the partner of choice in the region. The Southeast Asia and Pacific Cyber capacity building program (SEA-PAC Cyber Program) builds on Australia's support to date and leverages existing partners and expertise from across the region to provide a coherent response to the cyber and critical technology challenges faced across Southeast Asia and the Pacific.

Under the SEA-PAC Cyber Program, the 2019-2024 Cyber and Critical Technology Cooperation Program has been redesigned and refocused to achieve 3 specific outcomes:

- Cyber security and critical technology capacity and capabilities are enhanced across Southeast Asia and the Pacific, including through increased access to the provision of secure and trusted technologies.
- Cyber resilience across Southeast Asia and the Pacific is enhanced through strengthened, coordinated cyber incident preparedness and response.
- National, regional and international cyber norms, standards, regulations and laws support an open, free and secure cyber ecosystem across Southeast Asia and the Pacific.

Under the SEA-PAC Cyber Program, the following have been delivered or are currently underway:

- 21 ODA-funded projects across the Indo-Pacific region
- 7 cyber incident preparedness and response training activities in Southeast Asia (the Philippines, Laos, Brunei and Singapore)
- 12 RAPID deployments to support Pacific partners to respond to cyber incidents, at their request; and
- 9 Pacific modernisation initiatives focusing on proactively identifying vulnerabilities and modernising systems to build long term resilience.

The Department of Foreign Affairs and Trade (DFAT) has partnered across the Government to deliver cyber capacity-building efforts. Some examples include:

- Coordinated assistance in 2025 between the Department and the Attorney General's Department to Solomon Islands' Ministry of Communications and Aviation to review national cybercrime legislation.
- The Australian Federal Police's Cyber Safety Pasifika program delivering cyber safety and cybercrime investigations skills to all Pacific Islands Chiefs of Police members.
- Through the Pacific Cyber Security Operational Network (PaCSON), the Department and the Cyber Security Centre support a network of Pacific security operations centres and computer emergency response teams.

- In Southeast Asia, the SEA-PAC Cyber Program provided funding to the Australian Strategic Policy Institute which, in collaboration with the University of Indonesia, developed Indonesia's first cyber diplomacy course, with modules covering international law and norms, human rights and internet governance.
- DFAT engaging an industry partner in 2025 to deliver a series of cyber incident preparedness and response tabletop exercises for Southeast Asian partners, including in the Philippines, Laos and Brunei.
- Following a sophisticated ransomware incident targeting the Mekong River Commission Secretariat, the department funded a network assessment to identify potential vulnerabilities and enhance the overall security posture.
- Through the SEA-PAC Cyber Program, the Department of Foreign Affairs and Trade has supported Southeast Asian and Pacific countries, through a regional gap analysis and travel, to sign the UN Cybercrime Convention against Cybercrime (the Convention). The Convention will support regional and global efforts to harmonise cybercrime legislation, strengthen investigation and cooperation, and narrow the operating space for organised crime groups.

**Evidence Use Showcase 6: SEA-PAC Monitoring, Evaluation and Learning system**

**Using data and evidence to ensure accountability, robust decision-making, continuous improvement, adaptation to change, and support stakeholder engagement**

The Monitoring, Evaluation and Learning system for the SEA-PAC Cyber Program has been designed to ensure accountability, provide robust evidence to inform decision-making, and enable continuous improvement throughout program implementation. It will also support adaptive management, allowing the program to respond effectively to evolving policy and contextual changes across Southeast Asia and the Pacific. An additional benefit will be the provision of evidence to inform and influence stakeholders with regards to promoting closer ties between Australia and partner governments in the Pacific and Southeast Asia and strengthening collaboration within the cyber sector.

**Developing indicators and baselines to inform regular review**

An overarching Monitoring, Evaluation and Learning Framework (the Framework) defines the program's intended performance and the indicators against which progress will be measured. While the Framework serves as the overarching template, a detailed Monitoring, Evaluation and Learning Plan will be developed in Q1 2026. This plan will include an early baseline assessment to enable accurate tracking of progress. The formal Monitoring, Evaluation and Learning system will be developed by mid-2026 to operationalise the plan. The Framework will be reviewed annually as part of the program's critical reflection and lesson-learning process to ensure it remains fit-for-purpose and responsive to any necessary program adaptations.

Evaluation will occur at key milestones throughout the program. A Mid-Term Review will be conducted in Q3-Q4 2026 to assess progress and recommend adjustments. A lessons-learned review will take place in Year 4 (October/November 2027) to evaluate effectiveness, efficiency, and progress toward intermediate and end-of-program outcomes, informing the design of a potential second phase. An independent end-of-program evaluation will be conducted approximately 18 months after program completion (anticipated in 2031 if extended) to verify outcomes and guide future programming directions.

**19b. Regional cyber crisis response team**

Lead agency: Department of Foreign Affairs and Trade

Contributing: A range of agencies, including Australian Signals Directorate

Australia has successfully established a deployable Pacific regional cyber crisis response capability, Cyber Rapid Assistance for Pacific Incidents and Disasters (RAPID), which has already been deployed 12 times to Pacific countries to respond to cyber incidents affecting their government and critical infrastructure.

The RAPID capability has been used proactively to support major events (such as Samoa's hosting of the Commonwealth Heads of Government Meeting, Tonga's hosting of the Pacific Islands Forum Leaders' Meeting in 2024 and Solomon Island's hosting of the Pacific Island Forum Leaders' Meeting in 2025).

In a survey conducted of Pacific Island countries 12 months into the commencement of the RAPID program, 93% of respondents were aware of the Cyber RAPID capability, and the ability to call on the Australian Government to support in a cyber incident. The Cyber RAPID team was given an average 4.6/5 rating for the ability to resolve the cyber incident or the mitigate the possibility of an incident occurring. 100% of participants would call on the RAPID team for subsequent cyber incidents.

Following one incident, the Pacific representative shared the following statement of support:

> *'The Cyber RAPID team provided excellent guidance, enabling our system admins and networks admins to significantly enhance their skills in a cyber incident… A fantastic service and a great level of support and assistance… literally a lifesaver.'*

Following 18 months of disruptive cyber attacks worsening and increasing requests for our assistance, including from key partners in Southeast Asia such as the Philippines and Indonesia, Australia is seeking to expand Cyber RAPID to Southeast Asia. Extending this capability would also strengthen regional cyber security and complement existing mechanisms, including the Association of Southeast Asian Nations Regional Computer Emergency Response Team recently established to support regional cyber security incident response coordination.

The Initiative Deep Dive below illustrates how RAPID is providing effective and trusted assistance during the height of a cyber crisis to harden our region's cyber resilience.

**Initiative Deep Dive 2: Cyber RAPID Response to the Tonga Ministry of Health Ransomware Attack**

On 15 June 2025, the Tongan Ministry of Health was impacted by a ransomware attack that made all core services inaccessible and disrupted the national healthcare network. At the request of the Tongan Government, the Australian Government deployed a Cyber RAPID team within 72 hours to assist the Ministry with the investigation and remediation efforts. The ransomware attack was conducted by INC Ransom, a ransomware group that operates a ransomware-as-a service model for criminal groups motivated by financial gain and double extortion.

The attack impacted the entire Tongan Health Network, including 4 major hospitals and 14 remote health clinics. Healthcare workers were unable to retrieve patient data, dispense medicines, undertake laboratory work or provide imaging services. The Cyber RAPID team worked closely with the Tongan Computer Emergency Response Team (Tonga CERT) and Ministry IT staff as a Joint Incident Response Team to successfully restore all core systems and re-engineer applications to achieve a temporary operating environment where hospital staff could perform their primary functions while an appropriate longer-term solution could be planned and developed. After returning to Australia, the Cyber RAPID team provided remote support to ensure the Ministry IT staff were equipped to manage the temporary environment while continuing to harden their systems.

The Cyber RAPID response paved the way for deepening cyber cooperation between Tonga and Australia. Following the incident, in September 2025 Australia and Tonga signing of a Cyber Cooperation Memorandum of Understanding on Cyber Cooperation. The speed and success of the remediation efforts by the Cyber RAPID team was praised at the highest levels in the Tongan government, including the Crown Prince, the Deputy Prime Minister and the Minister for Health.

In February 2026, Tonga CERT, the Australian Cyber Security Centre and New Zealand's National Cyber Security Centre co-sealed an advisory identifying INC Ransom as the cyber actor responsible for the ransomware attack on the Tongan Ministry of Health—Australia's first-ever cyber attribution with a Pacific island country.

**19c. Pilot options to use technology to protect the region at scale**

Lead agency: Department of Foreign Affairs and Trade

Contributing: Australian Signals Directorate

Protecting the region at scale is a priority to advance Pacific Island countries' ambitious digital transformation agenda. The adoption of AI, cloud and data centre solutions will continue to be subject to significant geostrategic competition, as increasing digitisation creates strategic openings that external actors can exploit to embed influence within local institutions and provide enduring access to critical infrastructure. With increasing cyber criminal and state sponsored malicious cyber activity in the Pacific, demand for support on incident response, threat blocking and uplifting digital infrastructure will also increase, providing further opportunities for reinforcing our partner of choice status in the region.

To ensure trusted hardware and software solutions are part of the Pacific's digital ecosystem, Australia is operationalising cloud pilots across the Pacific, as well as a scalable Protective Domain Name System (PDNS) pilot in at least 2 Pacific Island countries (initially Papua New Guinea and Vanuatu, with other Pacific nations under consideration). The Department of Foreign Affairs and Trade is currently delivering Phase 1 pilot of a secure government cloud in Vanuatu. The pilot is delivering a secure cloud platform and enablers (training, policy, process) for Vanuatu's long-term adoption of cloud infrastructure. All Vanuatu government websites are transitioning to the cloud platform as well as 2 high-importance government applications: Vanuatu's trade portal and medical supplies application.

Another example of piloting secure technology deployment is the trial of open source/ low-cost cyber security tooling during the 54th Pacific Islands Forum Leaders' Meeting (54PIFLM) in Honiara. This was part of a RAPID deployment (see 19b) to assist the Solomon Islands Government with their cyber security posture during the week of events. For the 54PIFLM, a low-cost, open-source security incident and event management solution supplemented the existing Solomon Islands network monitoring apparatus. The Cyber Security Operations officers were taught how to implement, use and draw insights from this solution.

This pilot was conducted with future intention for Australia to deploy low-cost, easy-to-use and interoperable tooling to computer emergency response teams across the Pacific. As a result of this pilot, teams across the region will have access to the same products, improving interoperability and enabling the region to share expertise on how to derive the most value from these tools.

## Action 20: Shape, uphold and defend international cyber rules, norms and standards

**20a. Shape and defend the development of transparent international standards**

Lead agency: Department of Industry, Science and Resources

Contributing: Whole of government

Australia is collaborating with international partners to shape and defend the development of transparent international standards, including with Quad partners through the Critical and Emerging Technology Working Group, and in the United Nations International Telecommunication Union's Standardization Sector.

Australia participated in the World Telecommunication Standardization Assembly held in 2024, working to promote robust international standards for critical technologies. Following the launch of the International Electrotechnical Commission and International Organisation for Standardisation's Joint Technical Committee 3 in January 2024, Australia established its mirror committee in 2024, ensuring that Australian interests and expertise were reflected in the early work on Quantum standards. In 2025, Australia sent representatives to the APEC AI Standards Conference, the Global ICT Standards conference and the International AI Standards Summit, helping to strengthen relationships with partner countries to align on strategies and foster transparent international standards.

This initiative includes the successful delivery of a Tech Standards Knowledge Program, which lifts capability and broadens the situational awareness of Australian standards experts through bespoke training and development. This program helps enable industry representatives to protect and promote Australia's interests in standards development for critical technologies. Over 180 experts have registered for training, including experts involved in setting cyber security standards. Participant feedback is consistently positive, with the majority of participants agreeing the training is relevant and applicable to their role in standard setting.

We are working with the International Telecommunication Union and regional fora to help improve standardisation capacity in the Pacific region. We also continue to be seen as a trusted partner through our active cooperation in the Pacific Island Forum, the ICT Ministerial dialogue (and other Senior Officials Meetings progressing work under the 2023 Lagatoi Declaration), and the Asia Pacific Telecommunity. Seeking leadership positions, such as through the Internet Corporation for Assigned Names and Numbers and the Asia Pacific Telecommunity, will help us continue to amplify Pacific Voices.

**20b. Digital trade rules**

Lead agency: Department of Foreign Affairs and Trade

Contributing: Whole of government

Through this initiative, the Government is advocating for digital trade rules that advance our economic interests, complement international cyber security settings, reinforce the rules-based trading system, reduce the risk of rule fragmentation, and address trade restrictive, coercive or distortive behaviours. This includes advocating for rules that facilitate the cross-border flow of data, prohibit forced technology transfer, address personal information protection, encourage digital cooperation, and promote cyber security as part of the responsible design, development, deployment and use of artificial intelligence.

To achieve this, we continue to advocate in bilateral, plurilateral and multilateral settings for a rules based and open global digital trade environment that protects personal information, promotes cyber security and encourages international cooperation. Australia has successfully advocated for the negotiation and implementation of digital trade rules at the World Trade Organization (WTO), with our bilateral free trade agreement partners, and through our plurilateral trade agreements—the Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP), the Regional Comprehensive Economic Partnership (RCEP) and the Agreement Establishing the ASEAN-Australia-New Zealand Free Trade Area (AANZFTA).

Key activities include:

- In March 2026, Australia and the European Union concluded negotiations on a free trade agreement, which includes strong digital trade rules.
- Also in March 2026, Australia (with Singapore and Japan) led 66 WTO members to adopt the WTO Agreement on E-Commerce with Interim Arrangements, which puts in place the first ever baseline set of digital trade rules with global reach. Australia continues to co-convene the 91-member WTO Joint Statement Initiative on E-Commerce.
- In late-November 2025, the CPTPP membership agreed to launch upgrade negotiations in early 2026 to modernise the Partnership's digital trade rules.
- The Australia-United Arab Emirates Comprehensive Economic Partnership Agreement—Australia's first Free Trade Agreement in the Middle East region—entered into force on 1 October 2025, bringing with it ambitious digital trade rules.
- The upgrade of AANZFTA entered into force on 21 April 2025, strengthening rules for digital trade with Southeast Asia.
- Australia is working to conclude its first set of digital trade rules with India as part of the ongoing Comprehensive Economic Cooperation Agreement negotiations.

**20c. Defend an open, free, secure and interoperable internet**

Lead agency: Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts

Contributing: Whole of government

Australia is promoting its policies and vision for an open, free, secure and interoperable Internet under multi-stakeholder governance, and we have bolstered our leadership, presence and reputation in our region and at key international forums to achieve that.

We hold leadership positions in the Internet Corporation for Assigned Names and Numbers and regularly engage at multi-stakeholder events such as the Internet Governance Forum, globally, regionally, sub-regionally and nationally to advance Australia's priorities and policies.

In the Pacific, the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts ran a workshop in July 2025 to build capacity in Internet governance for 40 participants including youth from the multi-stakeholder community. The Department also engaged the Pacific cyber community on domain name system abuse and community connectivity in partnership with key Internet technical community organisations at the inaugural Pacific Cyber Week 2025.

**Initiative Deep Dive 3: World Summit on the Information Society 20-year Review**

**Highlighting the importance of a multi-stakeholder approach for effective internet governance**

The World Summit on Information Society is a United Nations process focused on global digital governance and development. It establishes an important foundation for the multi-stakeholder approach to Internet governance and other digital issues. 20 years after the original, the United Nations General Assembly High-level Meeting on 17 December 2025 reaffirmed this approach.

The Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts led Australia's engagement on the world summit and on the 20-year review in late 2025 with support from the Department of Foreign Affairs and Trade and other agencies, and led an extensive multi-stakeholder preparatory process to amplify our impact. We took a whole-of-community approach towards developing our negotiating positions, which included:

- Working across government to identify policy interests and ways the 20-year review could support objectives.
- Releasing a non-paper early, offering ideas across key digital policy areas, promoting discussion around what the 20-year review could address. This was based on our desktop review, bilateral conversations, and the perspectives of over 30,000 stakeholders.
- Speaking with over 90 governments, and hundreds of stakeholders, to understand their perspectives on current challenges and opportunities.
- Establishing and regularly seeking input from a domestic multi-stakeholder group.

- Inviting public input and initiating events to help us share knowledge and coordinate efforts.
- Regularly providing progress reports to interested parties, sharing progress and inviting further stakeholder views.

The department's 20-year review engagement has advanced Australia's digital priorities, including an open, free, secure and interoperable Internet. The coordination between governments and non-government stakeholders has influenced early drafts of the world summit text, highlighting the strengths of multi stakeholder engagement.

Outcomes will be fed back to Australian Government agencies and the department will continue to lead Australia's world summit implementation with whole-of-government support. Ongoing stakeholder engagement will be essential for this implementation work to ensure the Internet remains aligned to the Government's objectives and priorities, including ensuring regional strategic balance and online safety.

**20d. Uphold and improve the UN framework of responsible state behaviour in cyberspace**

Lead agency: Department of Foreign Affairs and Trade

Contributing: Attorney General's Department, Department of Defence, Department of Home Affairs

On 25 October 2025, Australia, together with 71 other states, signed the United Nations Convention against Cybercrime (the Convention) in Hanoi. The convention is the first ever UN-endorsed instrument addressing cybercrime and the first international crime treaty to be adopted in over 20 years. It aims to harmonise cybercrime legislation across the globe and establish a framework for the collection and sharing of electronic evidence for all serious crimes, creating a stronger basis for international criminal investigation and cooperation, and narrowing the operating space for organised crime groups.

The Convention's expanded investigative powers include safeguards to uphold privacy, due process and fundamental freedoms. Australia is proud of its role in shaping provisions to prevent technology-facilitated abuse, especially of children. Australia, along with its like-minded partners, will continue to engage in the ongoing Ad Hoc Committee on the Convention processes, including in the preparation of draft rules of procedure for the Convention Conference of States Parties, and ensuring multi-stakeholder participation is maintained and international law, human rights, fundamental freedoms and the rule of law are upheld in the preparation of any draft supplementary protocols to the Convention.

Australia has actively engaged in the UN Open-Ended Working Group on Cyber 2021-2025, working with international partners to strengthen and implement the UN framework for responsible state behaviour in cyberspace. The Department of Foreign Affairs and Trade delivered regular national statements on our positions on the framework's pillars including cyber threats, international laws, norms, confidence-building measures, capacity-building and regular institutional dialogue. We provided text proposals for every report and advocated for a permanent mechanism on cyber to consolidate and advance the framework with a focus on practical implementation. We led the drafting of a Joint Working Paper on the Application of International Law in the use of ICTs: Areas of Convergence and a Joint Working Paper on Gender and the Future Permanent Mechanism.

In July 2025, the working group's Final Report was agreed by consensus and the new permanent UN Global Mechanism established. Australia led efforts to ensure references to international law and gender were included in the final report. We will take a proactive approach in shaping an inclusive, practical and action-oriented Global Mechanism with integrated, policy-oriented and cross-cutting dedicated thematic groups on cyber challenges and capacity-building.

We will also continue to support international efforts to prevent the proliferation and irresponsible use of commercial cyber intrusion capabilities, including through the Pall Mall Process.

**20e. Increase costs for malicious cyber actors**

Lead agencies: Department of Foreign Affairs and Trade, Department of Home Affairs

Contributing: Australian Federal Police, Attorney General's Department, Australian Signals Directorate

Malicious cyber actors have continued to expand the scale and complexity of their activities. This has included the escalating use of ransomware by cyber criminals, and compromises of democratic institutions and pre-positioning on critical infrastructure by state-affiliated actors. Advances in AI have helped amplify these threats as well as execute at a larger scale and at a faster rate.

With these evolving cyber threats predicted to increase, Australia can work to deepen collaboration with existing and additional partners on cyber deterrence measures including the attribution of malicious cyber activity, issuing of cyber technical advisories to share information on mitigation of the threats, and the implementation of cyber sanctions. We also need to continue efforts to build a broader coalition of international partners, including from the Pacific and Southeast Asia, willing to join in deterrence activities.

Since the establishment of Australia's thematic autonomous sanctions framework in relation to significant cyber incidents, Australia has stepped up its efforts to raise awareness of malicious cyber threats and impose costs to deter them. Together with international partners, we have imposed 5 sets of cyber sanctions on Russian cybercriminals (12 individuals and 3 entities) since the beginning of 2024. These have had a discernible impact, including cost and reputational effects, on the cybercriminal ecosystem.

In the same period, Australia joined or supported 10 attributions of malicious cyber activity to state based, state-backed or state-affiliated actors, including from China, Russia and Iran. Australia also led a technical advisory co-sealed by Five Eyes partners, Germany, Japan and Republic of Korea which attributed malicious cyber activity to China state-based actor APT40 and issued 4 statements of support for attributions made by international partners

The attributions and advisories both damage the reputations of the states that are called out, and help raise awareness of the tactics, techniques and procedures of the malicious actors to enable community, industry, critical infrastructure and government network defenders to better defend against them.

# Appendix: Horizon 1 Impact Poll

## Goal

To support an assessment of the impact of Horizon 1, live polls were conducted in the online Horizon 2 consultation co-design workshops and roundtables (see page 11).

## Approach

Three questions were asked of participants:

1. What had the biggest positive impact on Australia's cyber security in Horizon 1 (2023-2025)? *Open question*
2. How do you rate Australia's progress in becoming a world leader in cyber security by 2030?
    a. Well progressed
    b. On track
    c. Lagging
3. Is there anything that did not have the expected impact? *Open question*

Participation was voluntary and anonymous. Participants provided their responses live via Slido during the introductory session of the workshop or roundtable. Responses were displayed live during the session. Participants were given the option of emailing responses directly to the team if they chose, though none took this up.

## Limitations

This method had neither the participant population size nor representativeness to be statistically valid. This is supported by the results for question 2 varying widely based on the topic of conversation. Rather than being representative of the Australian population, workshop participants were selected based on their specific interests and expertise relative to the topic. However, the method did have the benefit of targeting those with deep interest in cyber security matters. At the same time, it is likely to have missed the voices of everyday Australians and vulnerable groups.

Live polling has a high risk of skewing the data as participant's answers may be biased by seeing what others have already contributed, though polling over several separate sessions goes some way to mitigating this.

The benefits of live polls is the transparency they provide; unpalatable results cannot be hidden. They also uplifts engagement during a live session, creating an effective way to maximise participation, compared to post-workshop or separate surveys.

This method replaced earlier, less successful, attempts to obtain feedback via online questionnaires shared via peak bodies distribution lists, which received poor response rates. This may have been due to their release alongside other competing stakeholder priorities, including discussion paper submissions and/or organisations' own member surveys.

Potential participants may have experienced survey fatigue, or that they chose to contribute their views through other channels.

### Results

Responses to the poll were received by 98 participants across 8 sessions.

The themes receiving 5 or more responses to the question of 'what had the biggest positive impact' were:

1. Awareness raising (16 responses)
2. Collaboration, particularly industry and government (14)
3. Critical infrastructure reforms (12)
4. Cyber Security Act (8)
5. Threat blocking (5)

The themes receiving 5 or more responses to the question of 'what did not have the expected impact' were:

1. Support for small and medium enterprises and not-for-profits (15)
2. Cyber security workforce including professionalisation, skills uplift, and diversity (15)
3. A need for broader collaboration (9)
4. Transparency and measurement of progress (7)

Percentages will not be provided for question 2 as they are not statistically valid; numbers are likely to be misunderstood as valid statistics.

Broadly speaking, just over half of co-design and roundtable participants thought Australia was currently lagging in its efforts to meet its world leading ambitions by 2030. Of the remaining participants, a majority believed Australia to be on track, while some thought we were progressing well. It is notable that the responses to question 2 varied substantially by workshop topic. For example, those participating in a workshop on awareness raising were mostly positive about progress, whereas those discussing the cyber security workforce were mostly negative.