Australian Government
Department of Home Affairs

Submission

For decision
PDMS Ref. Number: MS25-000267
Date of Clearance: 13/02/2025

To **Minister for Home Affairs, Minister for Immigration and Multicultural Affairs, Minister for Cyber Security**

Subject **2023-2030 Australian Cyber Security Strategy - The Road to Horizon 2**

Timing *Not time critical. Consideration by 28 February 2025 is desirable*

Recommendations

That you:

1. s. 47C(1) — agreed / not agreed

2. **note** the proposed consultation pathway and early initiatives for Horizon 2 of the Strategy. — noted / please discuss

Minister for Home Affairs, Minister for Immigration and Multicultural Affairs, Minister for Cyber Security

Signature…… **Date**:……/……./2025

Minister's Comments

Key Issues

1. You, through your office, requested a briefing outlining the proposed approach to development of the next tranche of cyber security policy reforms under the Government's *2023-2030 Australian Cyber Security Strategy* (the Cyber Strategy) as part of 'Horizon 2'.

Looking back at Horizon 1: foundations for change and achievements to date

2. The Cyber Strategy is being delivered across three horizons through to 2030. We are currently over halfway through Horizon 1 with delivery of 60 initiatives across Government, overseen by the National Cyber Security Coordinator.
   - Horizon 1 (2023-25) focuses on strengthening our foundations by addressing the critical gaps in our cyber shields to build strong businesses and citizens through deep partnerships across industry and government.
   - In Horizon 2 (2026–28) we will scale cyber maturity across the whole economy and make further investments in the broader cyber ecosystem, continuing to scale up our cyber industry and grow a diverse cyber workforce.
   - In Horizon 3 (2029–30) we will advance the global frontier of cyber security and lead the development of emerging cyber technologies capable of adapting to new risks and opportunities across the cyber landscape.

3. s. 34(3) All initiatives have commenced, with a significant proportion of these completed or moved to a sustainment model. s. 47C(1)
   - The Action Plan will need to evolve as the Cyber Strategy matures through each of the Horizons.

4. The Horizon 1 program has established a strong foundation for future cyber security initiatives and critical structural reforms. Through the introduction of new legislative frameworks, expansion of our National Cyber Exercise Program, enhanced public-private partnerships dedicated to information sharing and threat blocking, and work to further develop cyber vocational training and workforce retention, Australia is well-positioned to pivot to a proactive program of cyber security innovation and take advantage of opportunities in the cyber domain.
   - For the most recent achievements under Horizon 1, refer **Attachment A**.
   - For a status update on the delivery of Horizon 1 initiatives, refer **Attachment B**.

The Road to Horizon 2: development and conceptualisation

5. Development of Horizon 2 is under way. This tranche of the Cyber Strategy will consider the capability enablers, programs and partnerships required to support continuity of the foundations laid under Horizon 1, and to further embed cyber maturity across the Australian economy.
6. The strategic frame and proposed policy initiatives for Horizon 2 are still in the early stages of development; however, we expect the program will be constituted with policy ideas and initiatives under the following groups:

Sustainment and expansion of Horizon 1 initiatives

- Horizon 2 will seek to expand on successful initiatives that have been, or will be, implemented from Horizon 1. For example, developing the **next tranche of 'secure technology' proposals** to explore the most appropriate solutions for emerging cyber threats in devices used by Australians every day. This would include **complex consumer smart devices (including edge devices like modems and routers**), **industrial and enterprise-grade smart devices (operational technology**), **connected communities and software** to ensure Australians are protected while they use these products.
- Horizon 2 will also include initiatives that build on work completed under Horizon 1 and lay out policy or program options for implementation. For example, following the mapping work for a single reporting portal, we would seek to outline a series of **cyber legislative reforms to simplify, streamline and harmonise regulation across the Government**.
- Horizon 2 initiatives will also seek to refocus some Horizon 1 measures to ensure they remain consistent with the original policy intent. For example **Commonwealth cyber uplift** will build on the substantial progress in Horizon 1 by addressing the major core thematic systemic drivers currently impacting Commonwealth cyber uplift *1.Investment, 2. Prioritisation, 3. Powers, 4. Interventions*, and *5. Whole-of-Government risk management*.
- Finally, the National Office of Cyber Security's **cyber security preparedness and response activities** have moved into sustainment and would be highlighted as an ongoing initiative. However, the Department will still consider potential options for new initiatives under the Cyber Strategy for Horizon 2.

New policy initiatives under Horizon 2

- From consultation and industry feedback, we are aware of a number of areas in cyber policy that are a priority for business to explore within Horizon 2. We will seek to develop initiatives and policy ideas that meet these expectations and address areas of concern. For example, development of **targeted cyber policy package for small and medium businesses and not-for-profits**. These entities are the cornerstone of the Australian economy and need a tailored approach for cyber protection with scalable and affordable options at a low or no cost.
- Under Horizon 2, we are exploring the **role of cyber insurance in supporting Australia's economic resilience** to cyber security incidents across business types and industry sectors. Key to this will be considering what policy intervention from Government would be necessary to ensure we balance incentivising more businesses seek adequate cyber insurance coverage, without distorting the market or driving up costs.

- Workforce, resilience and diversity initiatives developed under Horizon 1 have shown the need to deepen cyber knowledge among Australians, including young Australians. Under Horizon 2, we will seek to develop policy initiatives to **target younger cohorts through school and entry-level education curriculum** to infuse awareness and preventative measures into the fabric of Australian society for future generations.
- Under Horizon 2, we will explore policy options to enhance **regulatory alignment for cyber security in both a domestic and international context**. Domestically this will consider a holistic analysis of cyber security frameworks, legislation and regulation, including across Commonwealth, State and Territory Governments. As well as, establishment of best practice legislation and regulatory frameworks for cyber security to address the "flow" of new regulation. In the international context, this will include initiatives to seek to boost Australia's role as a global leader in cyber by leveraging our global cyber partnerships to consider 'regulatory diplomacy' and harmonisation with key partners in the region and across Five Eyes countries and Europe.
- We will also explore opportunities through Horizon 2 to uplift Australia's technology security settings, with a particular focus on efforts to address **unwanted critical technology transfer**, and mitigate **security risks associated with the convergence of technologies** such as artificial intelligence (AI) and synthetic biology.

Process for development of Horizon 2

7. Initial policy development and consultation across Government has commenced for Horizon 2 with a series of cyber security-focused policy seminars between the Department, partner agencies and close industry stakeholders. These seminars are scheduled to conclude by mid-March 2025 and have supported current thinking on the Horizon 2 program of work and identified areas of focus.

8. s. 47C(1)

9. s. 47C(1)

- This framework will provide clear signals to adapt implementation when policies and programs are not having their intended effect, or the environment has shifted. It will maximise impact and more efficient allocation of resources to proven solutions.
- s. 47C(1)

- Horizon 2 will run for three years (commencing in 2026 and finishing end-2028), for that reason, it will be necessary to revalidate the effectiveness of the current program with government and ensure initiatives remain contemporary and appropriate for the security and regulatory policy environment.

10. The next step will be to continue policy development for Horizon 2 initiatives, and undertake consultation across Commonwealth agencies before, during and following the caretaker period. The Department will ensure that caretaker conventions are adhered to.

11. s. 47C(1)

- The Department will utilise existing stakeholder forums, networks and relationships developed during the Strategy and its current Action Plan to streamline and support continuity of engagement to ensure that the Horizon 2 Action Plan remains linked to the established program and gains made under Horizon 1.

Background

12. On 22 November 2023, the Cyber Strategy was launched by the former Minister for Home Affairs and Cyber Security, the Hon Clare O'Neil MP. The Cyber Strategy sets out six cyber shields that will support Australia to be a world leader in cyber security by 2030.

13. The Cyber Strategy is supplemented by an Action Plan, which details 20 actions and 60 supporting initiatives to be delivered between 2023 and 2025.

14. 38 initiatives are led by the Department, six initiatives are co-led by the Department and other agencies, and 16 initiatives are led by other agencies. As at 31 January 2025:
    - 29 initiatives in the Action Plan have been delivered in full or have transitioned into a sustained work program that will extend beyond the life of Horizon 1. 23 of these are Department-led or co-led initiatives and six are led by other agencies.
    - 31 initiatives in the Action Plan have been progressed. 21 are Department-led or co-led initiatives and are all on track for planned delivery timelines, and 10 are led by other agencies. Refer to **Attachment B** for a detailed initiative status summary.

15. On 2 September 2024, the Department established a Cyber Security Strategy Policy Project Management Office to ensure robust governance of the Cyber Strategy. The Policy Program Management Office model will ensure clear governance and reporting for the delivery of activities under the Cyber Strategy and its Action Plan, supporting ongoing transparency of progress and address potential delays in implementation. The Policy Program Management Office will also coordinate the development of initiatives to be managed under Horizon 2.

Consultation – Internal/External

16. The National Office of Cyber Security was consulted on the content of this brief.

17. Finance Division was consulted on the financial information contained in this brief.

Consultation – Secretary

18. The Secretary was not consulted on this submission.

Client Service Implications

19. There are no client service implications.

Risks and Sensitivities

20. Industry stakeholders are highly invested in the continued program of work under the Cyber Strategy and its Action Plan. A compressed consultation period on the proposed update to the Action Plan under Horizon 2 may be perceived as minimising the opportunity for industry to participate fully in the development of effective policy and program options under this tranche of the Strategy. Other Commonwealth stakeholders may similarly perceive compressed industry consultation as a risk to program development and delivery.
    - The Department will develop a suite of potential policy and program options for consideration under Horizon 2 in full consultation across Commonwealth. The Department will manage communication with industry carefully to support full engagement with any proposed package put forward for consideration by government.
    - The Department will use focused town halls, bilateral meetings with peak bodies and other significant industry partnerships, and standing forums such as the Executive Cyber Council, the Trusted Information Sharing Network and other like-groups to support targeted engagement and alignment with existing public-private policy development and information sharing platforms. This will be supported by routine consultation processes, such as via a public call for submissions in response to a discussion paper.

21. The information contained in this submission is classified and should not be publicly released without the authority of the Department of Home Affairs. In accordance with our long-standing practices, should you wish for unclassified media lines to be prepared in relation to this issue please contact the Home Affairs Media Operations team – media@homeaffairs.gov.au.

Financial/systems/legal/deregulation/media implications

22. There are no financial, systems, legal and deregulation or media implications in this submission.

Attachments

Attachment A Horizon 1: Most Recent Achievements

Attachment B Current status of the Strategy's Horizon 1 Initiatives

Authorising Officer
Cleared by: Hamish Hansford Deputy Secretary Cyber and Infrastructure Security Date: 13/02/2025 Mob: s. 22(1)(a)(ii)

Contact Officer Ashley Bell, Assistant Secretary, Cyber Policy and Programs, s. 22(1)(a)(ii)

CC
Secretary
National Cyber Security Coordinator
DS Executive
FAS Cyber and Technology Security Policy
Deputy National Cyber Security Coordinator
Chief Finance Officer
FAS Executive Coordination
FAS Critical Infrastructure Partnerships and Policy
AS Cyber Security Response Coordination Unit
AS Technology Security Policy
AS Government Cyber and Protective Security
AS External Budgets

Australian Government
Department of Home Affairs

OFFICIAL

Attachment A: Horizon 1 Achievements

Key achievements completed under Horizon 1 One (as at 31 January 2025) include:

1. ***Cyber Security Act (Shield 1, Shield 2 and Shield 4)***
   - On **29 November 2024**, the Cyber Security Legislative Package – encompassing the *Cyber Security Act 2024* and amendments to the *Intelligence Services Act 2001* and *Security of Critical Infrastructure Act 2018* – received Royal Assent and became law. Measures introduced through the Package aim to address existing gaps in legislation and include:
     - powers to mandate minimum cyber security standards for smart devices (***Shield 2, Action 8a***)
     - introduce mandatory ransomware reporting for certain businesses to report ransom payments (***Shield 1, Action 4a***)
     - introduce a 'limited use' obligation for the National Cyber Security Coordinator and the Australian Signals Directorate (ASD) (***Shield 1, Action 6b***)
     - establish a Cyber Incident Review Board (***Shield 1, Action 5b***)
     - align telecommunication providers to the same standards as other critical infrastructure entities (***Shield 4, Action 13a***)
     - protect the critical data held, used and processed by critical infrastructure (***Shield 4, Action 13d***),
     - review and remedy power for Risk Management Program (***partially implements Shield 4, Action 14b***), and
     - expand crisis response arrangements to ensure they capture secondary consequences from significant incidents (***Shield 4, Action 14c***).
2. ***Cyber Security Awareness Campaign (Shield 1 Action 2a)***
   - Phase 3 of the *Act Now, Stay Secure* cyber security awareness raising advertising campaign was in market from 17 March to 30 June 2024. The campaign focused on establishing a baseline cyber security capability for all Australians by empowering them to take control of their cyber security and driving awareness of the simple actions they can take every day to be more secure online.
3. ***Ransomware Playbook (Shield 1 Action 4b)***
   - On **10 October 2024**, the Minister for Home Affairs and the Special Envoy for Cyber Security and Digital Resilience launched the Ransomware Playbook via Ransomware Playbook Cyber.gov.au.
     - The Ransomware Playbook equips industry with clear information on how to prepare for, respond to and recover from a ransomware incident.

- The interactive webpage includes easy-to use guides such as a cyber security checklist for small businesses, a guide to securing devices against a ransomware attack, and guidance for incident response planning.

4. ***Counter Ransomware Initiative (Shield 1, Action 4c)***

- On **14 January 2025**, the United States announced Australia, Germany, the United Kingdom and Singapore will lead a Steering Committee to guide and manage Counter Ransomware Initiative (CRI) activities over the next year. This is in addition to our role as co-Chair of the International Counter Ransomware Task Force (ICRTF).
- The establishment of the Steering Committee reflects our commitment to leverage Australia's role in the CRI and to ensure continued global momentum in response to evolving threats posed by ransomware actors.

5. ***Commonwealth Cyber Security Uplift (Shield 4, Action 15)***

- In December 2024 the Department completed a Systems of Government Significance (SoGS) pilot with the s. 33(a)(i)
  - The pilot assessed an s. 33(a)(i) system against potential SoGS declaration criteria and enhanced **cyber** security obligations. The department is using the pilot results and collaborating across government to inform the development of the policy. As part of this engagement, the department will be undertaking further test cases with a range of entities in the first half of 2025.
- On **8 July 2024**, three Directions were issued under the *Protective Security Policy Framework* to uplift the security and maturity of the Commonwealth's cyber security.

6. ***Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 (Shield 4, Action 13c)***

- On **28 November 2024** the *Transport Security Amendment (Security of Australia's Transport Sector) Bill* was introduced to the House of Representatives. The measures included within the Bill achieve the following four objectives:
  - transport sector that is resilient to current and emerging threats, including cyber security
  - an effective system testing program that is risk-based and responsive to intelligence
  - compliance and enforcement frameworks that are robust and fit-for-purpose
  - regulation that is modern and proportionate.

7. ***Grants***

- In January 2025, the **Health Sector Information Sharing and Analysis Centre** grant was awarded to the Critical Infrastructure Information Sharing and Analysis Centre (**CI-ISAC**) to facilitate ongoing industry-to-industry threat intelligence sharing within the health sector ($6.423m) (Shield 3, Action 11c). The grant opportunity opened to applications from 28 June 2024 – 25 July 2024. The grant agreement between the Commonwealth and CI-ISAC for the Health Sector ISAC was executed on 20 December 2025. The project commenced on 6 January and will run until 31 March 2027.
- On **2 December 2024**, the Australian Government announced that over 200 recipients ($6.9 million) received funding through the Cyber Security Awareness Support for Vulnerable

Groups grants program to uplift cyber awareness amongst vulnerable communities in Australians. (Shield 1, Action 2b).

- On **30 January 2025**, the **Labelling Scheme for Smart Devices** grant was launched to co-design and implement an industry-led and internationally aligned voluntary labelling scheme for consumer-grade smart devices in Australia ($1.7 million) (Shield 2, Action 8b).

8. Cyber Incident Management

- **Ten sectoral cyber incident playbooks** are currently being finalised to help coordinate national cyber incident responses between all tiers of government and industry (Action 16). One playbook has been completed for professional services (***Shield 4, Action 16b***).
- As at 31 December 2024, the National Office of Cyber Security has **led twelve, participated in six and observed four exercises.** (***Shield 4, Action 16a***)
  - Refer to Back Pocket Brief Number NCS-03 - *National Cyber Exercise Program* for further detail.

9. Systems of National Significance (SoNS) (Shield 2, Action 8c)

- The incident response planning and cyber security exercise Enhanced Cyber Security Obligations have been applied to almost all SoNS:
  - Exceptions include: a small number of SoNS in the financial services and markets sector due to existing obligations under other regulations (eg: APRA regulations), and a small number of SoNS that were decleared in December 2024.
- The Vulnerability Assessment and System Information Enhanced Cyber Security Obligations have not yet been applied to any SoNS. These will only be used on a targeted, as needs basis – where a regulatory response is required.
- Guidance material regarding incident response planning, exercising and undertaking vulnerability assessments is available on the Department's website.

10. Technology Vendor Review Framework (Shield 2, Action 8e)

- On **20 December 2024**, the Minister for Home Affairs announced the finalisation of the Technology Vendor Review Framework (the Framework).
- The Framework provides Government with a dedicated and proactive process to consider foreign ownership, control or influence risks associated with technology vendors.

11. International Cooperation on Cyber Response (Shield 6, Action 20e)

- In 2024, Australia participated in **nine technical advisories with attribution, four Statements of Support and three sanctions with Five Eyes and other international counterparts**, to respond to malicious cyber activity.
  - This included Australia's first cyber sanction (Aleksandr Ermakov; 23 January 2024) and Australia's first ASD-led technical advisory attributing malicious cyber activity to a state-sponsored actor (APT40, China's Ministry of State Security; 9 July 2024).
- On 29 January 2025, Australia participated in its first international response activity for the year. Through the Department of Foreign Affairs and Trade, the Australian Government made a statement of support for the EU's imposition of sanctions on three individuals linked to the Russian Armed Forces for their role in malicious cyber activity targeting Estonia.

2023–2030 Australian Cyber Security Strategy

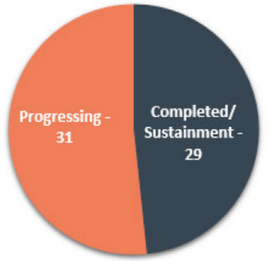
Horizon One Delivery Snapshot

(31 January 2025)

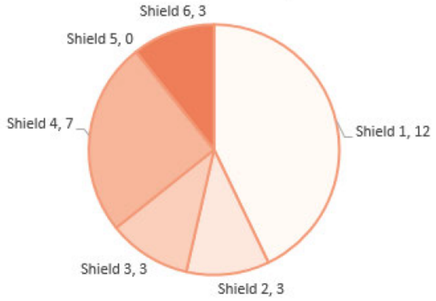
Overview

The Department of Home Affairs has substantially progressed many of the initiatives in the Australian Cyber Security Strategy Action Plan, with a focus on the building blocks to enable enduring policy and private-public partnerships and to establish frameworks to achieve the Australian Government's vision of positioning Australia as a world leader in cyber security by 2030

Horizon 1 Initiatives as at 31 Jan 2025



Initiatives Complete by Shield



The Cyber Security Strategy's Horizon 1 Action Plan contains 20 Actions, made up of 60 Initiatives.

- **29 initiatives in the Action Plan have been delivered in full** or have transitioned into a sustained work program that will extend beyond the life of Horizon One.
- **31 initiatives in the Action Plan have been progressed**.

Home Affairs is leading or co-leading on 44 initiatives - 39 of the 44 initiatives identified key milestones for completion in **Q1 and Q2 FY25**.

- **A total of 47 of the 50 milestones (94%) were completed** with significant progress achieved in the reporting period.

1 Strong Business & citizens

29% (Progressing)

71% (complete/ in sustainment)

17 Initiatives

- ❑ Consultation and implementation of Ransomware reporting and CIRB rules
- ❑ Establishment of the CIRB
- ❑ Consultation on Small Business Cyber Health Check design
- ❑ Operationalisation of 'limited use' provisions

2 Safe technology

73% (Progressing)

27% (complete/ in sustainment)

11 Initiatives

- ❑ Launch grant for smart devices labelling scheme
- ❑ Consultation on and implementation of IoT device rules
- ❑ Consultation with App stores/ Developers on secure app code of practice
- ❑ Consultation on data retention review
- ❑ Continued development of data brokers review and Voluntary Data Classification Framework

3 World-class threat sharing & blocking

50% (Progressing)

50% (complete/ in sustainment)

6 Initiatives

- ❑ Health ISAC grant commenced
- ❑ Consultation with industry on threat sharing and threat blocking incentives.
- ❑ Pilot 2 of NCIP

4 Protected critical infrastructure

50% (Progressing)

50% (complete/ in sustainment)

14 Initiatives

- ❑ Consultation on SOCI Cyber Security rules and implementation of legislation
- ❑ Framework for assessing non-Digital Investment Oversight (DIO) proposals
- ❑ Zero Trust Guiding Principles drafted for PSPF Release 2025

5 Sovereign capabilities

100% (Progressing)

4 Initiatives

- ❑ JSA consultation on 2025 OSL for cyber careers (incl. industry input)
- ❑ Cyber Diversity roundtables with industry and Australian Government
- ❑ Cyber Professionalisation grant assessment process underway
- ❑ BRII grant recipients announced

6 Resilient region& global leadership

62% (Progressing)

38% (complete/ in sustainment)

8 Initiatives

- ❑ Ministerial agreement to the Australian Government Cyber Attributions and Responses Framework

SHIELD 1 Strong businesses and citizens	SHIELD 2 Safe technology	SHIELD 3 World-class threat sharing and blocking	SHIELD 4 Protected critical infrastructure	SHIELD 5 Sovereign capabilities	SHIELD 6: Resilient region and global leadership
1a. Create cyber 'health checks' for small and medium businesses	**8a.** Adopt international security standards for consumer grade smart devices	**11a.** Establish the Executive Cyber Council as a coalition of government and industry leaders	**13a**. Align telecommunication providers to the same standards as other critical infrastructure entities	**17a**. Attract global cyber talent through reforms to the migration system	**20e.** Increase costs for malicious cyber actors
2a. Expand the national cyber security awareness campaign	**8b.** Co-design a voluntary labelling scheme to measure the cyber security of smart devices	**11c.** Launch a threat sharing acceleration fund to provide seed funding to establish or scale-up Information Sharing and Analysis Centres (ISACs) in low maturity sectors	**13b.** Clarify the regulation of managed service providers under the SOCI Act	**17b**. Provide guidance to employers to target and retain diverse cyber talent	Document 1.2
2b. Fund grants to community organisations to deliver tailored cyber awareness programs to support diverse cohorts	**8c.** Co-design a voluntary cyber security code of practice for app stores and app developers	**11d.** Encourage and incentivise industry to participate in threat sharing platforms	**13c.** Explore options to incorporate cyber security regulation as part of expanded 'all hazards' requirements for the aviation and maritime sectors	**17c**. Build a framework for the professionalisation of the cyber workforce	
4a. Work with industry to co-design options for a mandatory no fault, no liability ransomware reporting obligation	**8d.** Work with Quad partners to harmonise software standards for government procurement	**12a.** Work with industry to pilot next-generation threat blocking capabilities across Australian networks	**13d**. Protect the critical data held, used and processed by critical infrastructure	**18a.** Provide cyber start-ups and small-to-medium enterprises with funding to develop innovative solutions to cyber security challenges	
4b. Create a ransomware playbook	**8e.** Develop a framework for assessing the national security risks presented by vendor products and services operating within and entering the Australian economy	**12b**. Encourage and incentivise threat blocking across the economy	**14a**. Activate enhanced cyber security obligations for Systems of National Significance		
4c. Leverage Australia's role in the Counter Ransomware Initiative (including ICTRF)	**9a.** Conduct a review to identify and develop options to protect Australia's most sensitive and critical data sets		**14b**. Finalise a compliance monitoring and evaluation framework		
5a. Provide industry with additional information on cyber guidance obligations under current regulation	**9b.** Review Commonwealth legislative data retention requirements		**14c**. Expand crisis response arrangements to ensure they capture secondary consequences from significant incidents		
5b. Co-design with industry options to establish a Cyber Incident Review Board	**9c.** Review the data brokerage ecosystem		**15a**. Enable the National Cyber Security Coordinator to oversee the implementation and reporting of cyber security uplift		
6a. Consider options to develop a single reporting portal for cyber incidents • Sustainment phase 2 and 3	**9d.** Work with industry to design a voluntary data classification framework		**15b**. Develop a whole-of-government zero trust culture		
6b. Consult industry on **options** to establish a legislated limited use obligation (co-lead ASD)	**10a**. Embed cyber security into our work on responsible Artificial Intelligence		**15c**. Conduct regular reviews of the cyber maturity of Commonwealth entities		
			15d. Designate 'Systems of Government Significance' that need to be protected with a higher level of cyber security		

Horizon One: Home Affairs-led Action Initiatives

Progressing on track= 21	21
Delivered = 13	13
Sustained/Enduring = 10	

2023–2030 Australian Cyber Security Strategy

Horizon One: Agency-led Initiatives

Document 1.2

SHIELD 1	SHIELD 2	SHIELD 3	SHIELD 4	SHIELD 5	SHIELD 6
Strong businesses and citizens	**Safe technology**	**World-class threat sharing and blocking**	**Protected critical infrastructure**	**Sovereign capabilities**	**Resilient region and global leadership**
1b. Establish a Small Business Cyber Security Resilience Service • *Treasury*	**10b.** Set standards for post-quantum cryptography by updating guidance within the Information Security Manual. • *ASD*	**11b.** Continue to enhance ASD's existing threat sharing platforms • *ASD*	**15e.** Developing the cyber skills of the APS, harnessing the Digital Profession and APS Academy to provide a WofG approach to addressing cyber skills shortages in the APS. • *APSC*		**19a.** Refocus Australia's cyber cooperation efforts under the Cyber and Critical Technology Cooperation Program • *DFAT*
3a. Amplify current cybercrime disruption activities under Operation Aquila • *AFP*					**19b.** Build a regional cyber crisis response team • *DFAT*
3b. Drive global cooperation to effectively prevent, deter, and respond to cyber crime • *AGD and DFAT*					**19c.** Pilot options to use technology to protect the region at scale • *DFAT*
3c. Build Regional capabilities to fight cybercrime in the Pacific and Southeast Asia • *AGD and DFAT*					**20a.** Collaborate with partners in international standards development forums • *DISR*
7a. Expand the Digital ID Program • *Finance*					**20b.** Advocate for digital trade rules • *DFAT*
7b. Continue support for victims of identity crime • *AGD*					**20c.** Continue to defend an open, free, secure and interoperable internet in international forums • *DITRDCA*
					20d. Continue to uphold and improve the framework of responsible state behaviour in cyberspace • *DFAT*

Horizon One: Agency Led Action Initiatives

Progressing = 10	10
Delivered = 1	6
Sustained/Enduring = 5	