Appendix B - Status of Horizon 1 Initiatives (as at 30 June 2025)

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
1. Support small and medium businesses to strengthen their cyber security			
1a. Create cyber 'health checks' for small and medium businesses to access free cyber maturity assessments, supported by tailored guidance on how to improve their cyber security.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs ASD Treasury
1b. Establish a Small Business Cyber Security Resilience Service to provide a free tailored advice and victim support, accessible through cyber.gov.au.	Delivered/In sustainment	The Small Business Cyber Security Resilience Service was launched by the Minister for Small Business in October 2024, see: Launch of Albanese Labor Government's Small Business Cyber Resilience Service | Treasury Ministers IDCARE Official Website | Identity Theft & Cyber Support	Treasury ASD AGD Home Affairs
2. Help Australians defend themselves from cyber threats			
2a. Expand the national cyber security awareness campaign to uplift cyber security outreach and literacy among the Australian community.	Delivered/In sustainment	The the Act Now Stay Secure Campaign was released in March 2024, see: What are you risking online? | Act Now. Stay Secure.	Home Affairs
2b. Fund grants to community organisations to deliver tailored cyber awareness programs to support diverse cohorts – such as remote and regional communities, culturally and linguistically diverse groups, First Nations communities, young people, seniors, people with disability and neuro-diverse people.	Delivered/In sustainment	Funding was awarded in December 2024. See: Vulnerable Australians receive Cyber Security Awareness Support with close to $7 million grant funding.	Home Affairs DSS (Grants Hub)
3. Disrupt and deter cyber threat actors from attacking Australia			
3a. Amplify current cybercrime disruption activities under Operation Aquila to target the highest priority cybercrime threats impacting Australia, both nationally and internationally.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	AFP AGD ASD Home Affairs
3b. Drive global cooperation to effectively prevent, deter and respond to cybercrime by working with partners to combat cybercrime. Actions include supporting global legal frameworks, making public attributions and imposing sanctions when we have sufficient evidence and it is appropriate to do so.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	AGD DFAT ASD AFP Home Affairs

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
3c. Build regional capabilities to fight cybercrime in the Pacific and Southeast Asia, including through forums such as the Pacific Islands Law Officers' Network and ASEAN Senior Officials Meeting on Transnational Crime. Government will continue to support our region to shape the development of international legal frameworks on cybercrime.	Delivered/In sustainment	Continued involvement in Pacific and Southeast Asian forums, see Pacific law and justice program | Attorney-General's Department ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) - ASEAN Main Portal	AGD DFAT DITRDCSA eSafety
4. Work with industry to break the ransomware business model			
4a. Work with industry to co-design options for a mandatory no fault, no liability ransomware reporting obligation for businesses to report ransomware incidents and payments.	Delivered/In sustainment	Included in the *Cyber Security Act 2024* which received Royal Assent in November 2024, see: Cyber Security Act 2024 - Federal Register of Legislation	Home Affairs AFP AGD ASD
4b. Create a ransomware playbook to provide further guidance to businesses on how to prepare for, deal with and bounce back from a ransomware or cyber extortion attack.	Delivered/In sustainment	Publication of the playbook in October 2024, see: Ransomware Playbook | Cyber.gov.au	Home Affairs AFP AGD ASD DFAT Treasury
4c. Leverage Australia's role in the Counter Ransomware Initiative to strengthen global resilience to ransomware and enable effective member action in countering ransomware, including through the International Counter Ransomware Task Force (ICRTF).	Delivered/In sustainment	The CRI website launched in November 2023, see: Home | International Counter Ransomware Initiative Sept – Oct 2024, Australia participated in the global CRI Summit hosted by US Government. Sept 2024, Australia hosted the regional CRI Summit with indo-pacific partners as part of the 2024 Cyber Champions Summit. Sept 24, CRI members' portal launched, allowing sharing of resources and assistance for incidents Counter Ransomware portal goes live!	Home Affairs DFAT

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
5. Provide clear cyber guidance for businesses			
5a. Provide industry with additional information on cyber governance obligations under current regulation. Government will assist businesses to navigate important obligations and requirements that should be considered when developing cyber security frameworks.	Delivered/In sustainment	Cyber Security Governance Principles Cyber Security Handbook for Small Business and Not-for-Profit Directors Cyber Security Governance Principles Checklist for SME and NFP Directors Cyber Wardens Overview of Cyber Security Obligations for Corporate Leaders General Guidance for Critical Infrastructure Assets Mandatory Cyber Incident Reporting - Initial guidance for Critical Infrastructure Sectors Cyber Security Threats: How to Protect Your Small Business COSBOA's Cyber Security Management Solution for SME's Cyber Security: It's Not Just about Technology Report REP 429 Cyber resilience: Health check Cyber resilience good practices | ASIC Key questions for an organisation's board of directors | ASIC Improving cyber resilience: the role boards have to play | APRA Cyber security stocktake exposes gaps | APRA Information Security | APRA Questions for the board of directors to ask about cybersecurity | Cyber.gov.au Small business cybersecurity guide | Cyber.gov.au Essential Eight | Cyber.gov.au Information security manual | Cyber.gov.au Governance Toolkit: Cyber security | ACNC Cybersecurity Standards - Standards Australia	Home Affairs Treasury AGD ASIC Other Departments and Regulators

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
5b. Co-design with industry options to establish a Cyber Incident Review Board to conduct no-fault incident reviews to improve our cyber security. Lessons learned from these reviews will be shared with the public to strengthen our national cyber resilience and help prevent similar incidents from occurring.	Delivered/In sustainment	Included in the *Cyber Security Act 2024* which received Royal Assent in November 2024, see: Cyber Security Act 2024 - Federal Register of Legislation	Home Affairs AFP AGD ASD Defence PM&C Other agencies as appropriate
6. Make it easier for Australian businesses to access advice and support after a cyber incident			
6a. Consider options to develop a single reporting portal for cyber incidents to make it easier for entities affected by a cyber incident to meet their regulatory reporting obligations.	Delivered/In sustainment	Single Reporting Portal launched 22 November 2023, see: Single Reporting Portal | Cyber.gov.au Consultation with industry and regulators continues in 2025 to explore options to enhance the portal.	Home Affairs ACCC ACMA AFP AGD APRA ASD ASIC Defence DITRDCSA DTA OAIC ONDC Treasury Other agencies as required

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
6b. Consult industry on options to establish a legislated limited use obligation for ASD and the National Cyber Security Coordinator to encourage industry engagement with Government following a cyber incident by providing clarity and assurance of how information reported to ASD and the National Cyber Security Coordinator is used.	Delivered/In sustainment	Included in the *Cyber Security Act 2024* and *Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024* which both received Royal Assent in November 2024. Cyber Security Act 2024 - Federal Register of Legislation Limited use obligation is now law | Cyber.gov.au	ASD Home Affairs AFP AGD APRA ASIC OAIC ONDC PM&C Other Departments and Regulators
6c. Co-design a code of practice for cyber incident response providers to clearly communicate the service quality and professional standards expected, and ensure they are delivering fit-for-purpose services consistently across the industry.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	ASD Home Affairs AFP AGD Defence ONDC PM&C Other agencies as required
7. Secure our identities and provide better support to victims of identity theft			
7a. Expand the Digital ID program to reduce the need for people to share sensitive personal information with government and businesses to access services online.	Delivered/In sustainment	Digital ID Bill 2024 received Royal Assent in May 2024, see: Digital ID Bill 2024 – Parliament of Australia	Finance AGD ATO Services Australia ACCC
7b. Continue support for victims of identity crime. This support will identify and guide individuals on recovering identity, how to mitigate damage, review and where necessary advise on how to replace identity credentials. The support will also educate on identifying danger signs that the compromised identity is continuing to be misused.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	AGD

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
8. Ensure Australians can trust their digital products and software			
8a. Adopt international security standards for consumer grade smart devices by working with industry to co-design a mandatory cyber security standard.	Delivered/In sustainment	Included in the *Cyber Security Act 2024* which received Royal Assent in November 2024, see: Cyber Security Act 2024 - Federal Register of Legislation	Home Affairs ACMA AGD DISR DITRDCSA Health Treasury Law enforcement agencies
8b. Co-design a voluntary labelling scheme to measure the cyber security of smart devices, developed through consultation with industry and aligned to international exemplars.	Delivered/In sustainment	Grant was awarded to IoT Alliance Australia on 27 June 2025.	Home Affairs ACMA AGD DISR DITRDCSA Treasury
8c. Co-design a voluntary cyber security code of practice for app stores and app developers to clearly communicate expectations of cyber security in software development and incentivise enhanced cyber security in consumer apps.	In progress	Consultation undertaken on discussion paper in June 2025. Delivery under the Horizon 1 intent is expected by the end of 2025. Australian Code of Practice for App Store Operators and App Developers Discussion Paper	Home Affairs ACMA AGD DISR DITRDCSA Health
8d. Work with Quad partners to harmonise software standards for government procurement and leverage our collective buying power to set strong IT security standards across global markets.	Delivered/In sustainment	Consultation undertaken with Australian industry stakeholders in August 2024. Australia has worked with Quad partners on drafting a public Joint Statement on the Implementation of Quad Secure Software Principles.	Home Affairs AGD DFAT DTA PM&C

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
8e. Develop a framework for assessing the national security risks presented by vendor products and services entering and operating within the Australian economy.	Delivered/In sustainment	The Technology Vendor Review Framework was announced in December 2024, see: Technology Vendor Review Framework Factsheet - Technology Vendor Review Framework.	Home Affairs ASD ASIO Defence DFAT DISR DITRDCSA Treasury
9. Ensure Australians can trust their digital products and software			
9a. Conduct a review to identify and develop options to protect Australia's most sensitive and critical data sets, with a focus on datasets that are crucial to national interests yet are not appropriately protected under existing regulations.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs AGD ASIO Defence DISR Finance Health Treasury
9b. Review Commonwealth legislative data retention requirements, including through implementation of the Government's response to the Privacy Act Review, reforms to enable use of Digital ID, and the National Strategy for Identity Resilience.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	AGD Home Affairs Finance OAIC Treasury
9c. Review the data brokerage ecosystem and explore options to restrict unwanted transfer of data to malicious actors via data markets, complementing proposed Privacy Act reforms.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs AGD ASIO Defence DISR Treasury
9d. Work with industry to design a voluntary data classification model to help industry assess and communicate the relative value of their data holdings in a consistent way.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs AGD DISR Finance Treasury

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
10. Promote the safe use of emerging technology			
10a. Embed cyber security into our work on responsible AI to help ensure that AI is developed and used safely and responsibly in Australia, our region and across global markets.	Delivered/In sustainment	Contribution and collaboration with commonwealth agencies and industry to develop guidance materials, frameworks and legislation to support the responsible use of AI through 2023-2025, see: Artificial intelligence | Department of Industry Science and Resources	Home Affairs (through the National Security Node) DISR ASD
10b. Set standards for post-quantum cryptography by updating guidance within the Information Security Manual. Organisations will also be encouraged to prepare for the post-quantum future by conducting a review of their data holdings, and developing a plan to prioritise and protect sensitive and critical data.	Delivered/In sustainment	Information Security Manual updated March 2025, see: Information security manual | Cyber.gov.au Planning for post-quantum cryptography | Cyber.gov.au NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST Compliance FAQs: Federal Information Processing Standards (FIPS) | NIST	ASD CSIRO DISR
11. Create a whole-of-economy threat intelligence network			
11a. Establish the Executive Cyber Council as a coalition of government and industry leaders to improve sharing of threat information across the whole economy, and drive public-private collaboration on other priority initiatives under the Strategy.	Delivered/In sustainment	Inaugural Executive Cyber Council (ECC) meeting held November 2023, see: Opening remarks - Executive Cyber Council | Prime Minister of Australia	Home Affairs ASD
11b. Continue to enhance ASD's existing threat sharing platforms to enable machine-to-machine exchange of cyber threat intelligence at increased volumes and speeds. These platforms will enable a framework within which industry-to-industry and government-to-industry cyber threat intelligence can be exchanged.	Delivered/In sustainment	ASD-Microsoft initiative announced in March 2023 connected ASD's Cyber Threat Intelligence Sharing (CTIS) platform with Microsoft's Sentinel platform, see: ASD-Microsoft initiative bolsters Australia's cyber defence | Defence Ministers	ASD ACMA AGD DITRDCSA
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. This program will start with an initial pilot in the health sector to enable the sharing of actionable threat intelligence and cyber best-practice.	Delivered/In sustainment	Grant awarded to CI-ISAC in January 2025 to establish the Health Cyber Sharing Network (HCSN) Pilot, see: Australia's health sector receives $6.4million cyber security boost with the creation of a new threat information-sharing network | CI-ISAC Australia	Home Affairs ACMA ADHA AGD ASD DITRDCSA Health
11d. Encourage and incentivise industry to participate in threat sharing platforms, with a focus on organisations that are most capable of collecting and sharing threat intelligence at scale across the economy.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs ACMA AGD ASD DITRDCSA

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
12. Scale threat blocking capabilities to stop cyber attacks			
12a. Work with industry to pilot next-generation threat blocking capabilities across Australian networks by establishing a National Cyber Intel Partnership with industry partners and cyber experts from academia and civil society. This partnership will pilot an automated, near-real-time threat blocking capability, building on – and integrated with – existing government and industry platforms.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs AFP AGD
12b. Encourage and incentivise threat blocking across the economy, focusing on the entities that are most capable of blocking threats – including telecommunication providers, ISPs and financial services.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs ACMA AGD ASD DITRDCSA
13. Clarify the scope of critical infrastructure regulation			
13a. Align telecommunication providers to the same standards as other critical infrastructure entities, commensurate with the criticality and risk profile of the sector by moving security regulation of the telecommunications sector from the Telecommunications Sector Security Reforms (TSSR) in the *Telecommunications Act 1997* to the SOCI Act.	Delivered/In sustainment	Included in the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* which received Royal Assent in November 2024, see: Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 - Federal Register of Legislation	Home Affairs ACMA AGD DITRDCSA
13b. Clarify the regulation of managed service providers under the SOCI Act and delegated legislation. The proposed clarification of obligations through industry consultation will contribute to a wider security uplift within the data storage and processing sector and provide certainty to affected entities regarding their obligations under the Act.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs DTA

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
13c. Explore options to incorporate cyber security regulation as part of expanded 'all hazards' requirements for the aviation and maritime sectors. Government will consider the development of a reform agenda to strengthen Australia's aviation, maritime and offshore facility security settings, including positive obligations to proactively manage cyber-related risks under existing legislation.	Delivered/In sustainment	The *Transport Security Amendment (Security of Australia's Transport Sector) Act 2025* received Royal Assent in March 2025, see: Transport Security Amendment (Security of Australia's Transport Sector) Act 2025 - Federal Register of Legislation	Home Affairs ACIC AFP AGD AMSA ASD CASA DCCEEW Defence DEWR DFAT DITRDCSA PM&C
13d. Protect the critical data held, used and processed by critical infrastructure in 'business-critical' data storage systems. Government, in consultation with industry, will consider clarifying 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.	Delivered/In sustainment	Included in the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* which received Royal Assent in November 2024, see: Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 - Federal Register of Legislation	Home Affairs AGD OAIC
14. Strengthen cyber security obligations and compliance for critical infrastructure			
14a. 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 develop and maintain a near real-time threat picture.	Delivered/In sustainment	The activation of enhanced cyber security obligations. have been applied for assets declared up to and including August 2023 (except where the entity has existing obligations under other regulatory frameworks), see: ECSO Guidance - Incident Response Planning ECSO Guidance - Cyber Security Exercises Enhanced Cyber Security Obligations Guidance – Vulnerability Assessments CISC Factsheet - Systems of National Significance and Enhanced Cyber Security Obligations	Home Affairs Commonwealth Agencies and Regulators, State and Territory Agencies and Regulators, as appropriate
14b. Finalise a compliance monitoring and evaluation framework for critical infrastructure entities. This framework will have an initial focus on tracking obligations designated sectors to develop, maintain and comply with a critical infrastructure risk management program. This will include consultation with industry on options for enhanced review and remedy powers to address deficient risk management plans.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs Commonwealth, State and Territory Agencies and Regulators, as appropriate

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
14c. Expand crisis response arrangements to ensure they capture secondary consequences from significant incidents. Government will consult with industry on introducing an all-hazards consequence management power that will allow it to direct an entity to take specific actions to manage the consequences of a nationally significant 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.	Delivered/In sustainment	Included in the *Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024* which received Royal Assent in November 2024, see: Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 - Federal Register of Legislation	Home Affairs ASD Commonwealth Agencies and Regulators, State and Territory Agencies and Regulators, as appropriate
15. Uplift cyber security of the Commonwealth Government			
15a. Enable the National Cyber Security Coordinator to oversee the implementation and reporting of cyber security uplift across the whole government. The Coordinator will oversee implementation of the Commonwealth Cyber Security Uplift Plan, assisted by a central cyber program, policy and assurance function within Home Affairs.	Delivered/In sustainment	The National Cyber Security Coordinator has established a section within the National Office of Cyber Security, dedicated to the coordination and outreach of Commonwealth cyber security uplift.	Home Affairs ASD DTA
15b. Develop a whole-of-government zero trust culture to protect government data and digital estate. Government will implement defined controls across our networks that draw from internationally-recognised approaches to zero trust. This builds on the best-practice principles established within ASD's Essential Eight strategies to mitigate cyber security incidents.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs ASD DTA Whole of Government
15c. Conduct regular reviews of the cyber maturity of Commonwealth entities as part of the Investment Oversight Framework, administered by the Digital Transformation Agency. Home Affairs and ASD will provide cyber expertise and advice to support the evaluation of the cyber maturity of Commonwealth entities.	Delivered/In sustainment	Implementation of a regular review cadence and framework review.	Home Affairs ASD DTA
15d. Designate 'Systems of Government Significance' that need to be protected with a higher level of cyber security by identifying and mapping the Australian Government's most important digital infrastructure. This will include an evaluation of the centrality of systems to digital government functions or services, the scale of their interdependencies, and potential for cascading and significant consequences to Australia's national interests, economic prosperity and social cohesion if disrupted.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs ASD Defence DTA
15e. Developing the cyber skills of the APS, harnessing the Digital Profession and APS Academy to provide a whole-of-government approach to addressing cyber skills shortages in the APS, as well as through the establishment of the Defence Cyber College.	Delivered/In sustainment	The APS Data, Digital and Cyber Workforce Plan 2025-30 was published in March 2025, see: The APS Data, Digital and Cyber Workforce Plan 2025-30 has been released | Australian Public Service Commission Home | APS Professions Digital Profession | Australian Public Service Academy	APSC ASD Defence Home Affairs

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
16. Pressure-test our critical infrastructure to identify vulnerabilities			
16a. Expand our National Cyber Exercise Program to proactively evaluate consequence management capabilities, identify gaps in coordination and test the effectiveness of incident response plans. Led by the Cyber Coordinator, these exercises will include participation from states and territories, as well as industry leaders, and will incorporate simulation of systemic cyber incidents.	Delivered/In sustainment	Twenty cyber security exercises have been delivered since the launch of the Strategy in line with ongoing work to expand Australia's National Cyber Security Exercise Program.	Home Affairs AGD Defence NEMA
16b Develop incident response playbooks to help coordinate national incident response across Commonwealth, state, territory and industry stakeholders. Developed by the Cyber Coordinator, these playbooks will be informed by the insights gathered from national exercises.	In progress	Nine sector playbooks have been delivered. Three remaining playbooks are due to be published. Delivery under the Horizon 1 intent is expected by the end of 2025. Communications Sector Playbook (363KB PDF) Data Storage or Processing Sector Playbook (256KB PDF) Energy Sector Playbook (359KB PDF) Financial Sector Playbook (358KB PDF) Food and Grocery Sector Playbook (359KB PDF) Health Sector Playbook (251KB PDF) Professional Services Sector Playbook (360KB PDF) Transport Sector Playbook (260KB PDF) Water and Sewerage Sector Playbook (255KB PDF)	Home Affairs AGD Defence NEMA
17. Grow and professionalise our national cyber workforce			
17a. Attract global cyber talent through reforms to the migration system as part of the government's Migration Strategy. Government will enhance both international and domestic outreach efforts to increase Australia's competitiveness and attract highly skilled migrants to expand the cyber security workforce.	Delivered/In sustainment	Targeted Core Skills Occupation List announced in December 2024, see: Visa reform targets the skills Australia needs | Ministers' Media Centre	Home Affairs
17b. Provide guidance to employers to target and retain diverse cyber talent, with a focus on barriers and biases that dissuade under-represented cohorts – specifically women and First Nations people – from entering and staying in the workforce. Government, through BETA, has conducted an analysis on attracting a diverse cyber security workforce. Building on this, Government will publish guidance for recruiters to attract a wider diversity of applicants, supporting workforce growth and participation.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs DISR PM&C (building on previous BETA work)
17c. Build a framework for the professionalisation of the cyber workforce to provide employers and businesses with the assurance that the cyber workforce is appropriately skilled, and workers that their qualifications and relevant experience are recognised and fit-for-purpose.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs DEWR DISR

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
18. Accelerate our local cyber industry, research and innovation			
18a. Provide cyber start-ups and small-to-medium enterprises with funding to develop innovative solutions to cyber security challenges through the Cyber Security Industry Challenge program, leveraging DISR's Business Research and Innovation Initiative. The program will allow agencies to articulate cyber security challenges, to which start-ups can propose solutions. Successful entities will receive grants to develop their solution, providing both funding and credibility to start-ups while increasing agencies' sourcing of new-to-market solutions.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	Home Affairs DISR
19. Support a cyber-resilient region as the partner of choice			
19a. Refocus Australia's cyber cooperation efforts under the Cyber and Critical Technology Cooperation Program to support enduring cyber resilience and technology security and better position regional governments to prevent cyber incidents. Through the Program's redesign, a new strategy for gender equality, disability and social inclusion will be developed.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	DFAT AFP AGD ASD Defence DISR DITRDCSA eSafety Home Affairs
19b. Build a regional cyber crisis response team, drawing on specialist industry and government expertise. Government will develop a framework to identify when and how to deploy our limited resources across the region.	Delivered/In sustainment	Rapid Assistance for Pacific Incidents and Disasters (RAPID) teams established, see: 2023-2030 Cyber Security Strategy: Resilient Region and Global Leadership | Ministers and Assistant Ministers	DFAT A range of Agencies, including ASD
19c. Pilot options to use technology to protect the region at scale by partnering with our regional neighbours and the private sector to leverage industry solutions to protect more people, systems and data from cyber threats. This includes proactively identifying vulnerabilities – such as end-of-life hardware and software – and providing scalable solutions that are fit-for-purpose, including security features that mitigate avoidable cyber incidents.	In progress	Delivery under the Horizon 1 intent is expected by the end of 2025.	DFAT ASD
20. Shape, uphold and defend international cyber rules, norms and standards			
20a. Collaborate with partners in international standards development forums to shape and defend the development of transparent international standards. The Government will continue to leverage existing programs, such as DISR's Tech Standards Knowledge Program, to bolster the capability of industry technical experts engaged in this work.	Delivered/In sustainment	The World Telecommunication Standardization Assembly held in 2024, see: Proceedings of the World Telecommunication Standardization Assembly, Quantum technology- ISO and IEC standards joint technical committee launch in January 2024, see:	DISR Whole of Government

INITIATIVE	STATUS		ACCOUNTABLE AGENCIES
		ISO - IEC and ISO launch new joint technical committee on quantum technologies JTC3 Australian expert panel establishment in 2024.	
20b. Advocate 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 address personal information protection, encourage digital cooperation, and promote cybersecurity as part of the responsible design, development, deployment, and use of AI.	Delivered/In sustainment	Australia co-convening (with Singapore and Japan) the negotiations and finalisation of WTO Agreement on E-Commerce, see: New trade rules for the digital economy | Australian Government Department of Foreign Affairs and Trade Comprehensive Economic Partnership Agreement with the UAE, see: Australia-UAE Comprehensive Economic Partnership Agreement (CEPA) | Australian Government Department of Foreign Affairs and Trade Upgrade of AANZFTA, see: ASEAN-Australia-New Zealand FTA | Australian Government Department of Foreign Affairs and Trade	DFAT Whole of Government
20c. Continue to defend an open, free, secure and interoperable internet in international forums by working with international partners, industry, academia, the technical community, civil society and other relevant stakeholders. Government will advocate for continuing, consensus-based improvements to existing mechanisms of multi-stakeholder internet governance.	Delivered/In sustainment	Continued collaboration and involvement in international forums, see: International involvement in telecommunication and internet forums | Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts	DITRDCSA Whole of Government
20d. Continue to uphold and improve the framework of responsible state behaviour in cyberspace, including how international law applies and best practice implementation of norms. Government will support the establishment of a permanent UN Programme of Action to advance peace and security in cyberspace.	Delivered/In sustainment	Continued engagement in the UN to shape and implement the framework for responsible state behaviour in cyberspace, including the application of international law, norms, confidence-building measures and capacity-building, see: UN norms of responsible state behaviour in cyberspace	DFAT AGD Defence
20e. Increase costs for malicious cyber actors by working with international partners to deter and respond to malicious cyber activity. This includes publicly attributing and imposing sanctions on those who carry out or facilitate significant cyber incidents – when we have sufficient evidence and it is in our interests to do so. A review of our attribution framework will ensure it continues to be fit for purpose.	Delivered/In sustainment	Implementation of the cyber sanction framework, see: Significant cyber incidents sanctions regime | Australian Government Department of Foreign Affairs and Trade	DFAT Home Affairs AFP AGD ASD