Australian Government

2023–2030 Australian Cyber Security Strategy

ACTION PLAN

Use of the Coat of Arms

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 - 23-02503-b

2023–2030

Australian Cyber Security Strategy

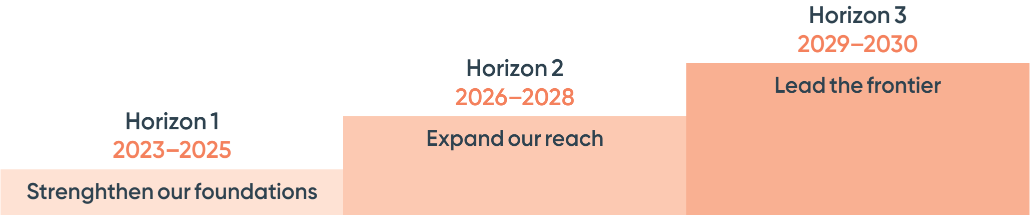
ACTION PLAN

Contents

Executive summary

The Australian Government is committed to its vision of positioning Australia as a world leader in cyber security by 2030. The strength of the *2023–2030 Australian Cyber Security Strategy* (the Strategy) can only be measured by the success of its actions. To achieve success, the Australian Government has developed this Horizon 1 Action Plan, which supplements the Strategy and details the key initiatives that will commence over the next two years to put us on a path to achieving our vision.

In order to become a world leader in cyber security by 2030, the Australian Government will foster genuine partnerships to generate enduring solutions through ongoing collaboration with industry. We will deliver our Strategy across three horizons:



- **In Horizon 1:** we will strengthen our foundations. We will address critical gaps in our cyber shields, build better protections for our most vulnerable citizens and businesses, and support initial cyber maturity uplift across our region.
- **In Horizon 2:** we will scale cyber maturity across the whole economy. We will make further investments in the broader cyber ecosystem, continuing to scale up our cyber industry and grow a diverse cyber workforce.
- **In Horizon 3:** we will advance the global frontier of cyber security. We will lead the development of emerging cyber technologies adapt to new risks and opportunities across the cyber landscape.

This approach has been crafted with careful consideration to minimise regulatory burden, promote innovation and maximise participation. The Government recognises the importance of periodic reviews of the Action Plan to ensure that it remains current.

The Government's new Executive Cyber Council will play an important role in facilitating genuine and transparent co-leadership on key cyber security issues. The Council will support the delivery of national cyber security priorities, including initiatives under this Action Plan.

A flexible approach to achieving the Strategy's vision will enable us to remain adaptive to emerging technological, economic and geopolitical trends. Some actions will commence immediately with the release of the Strategy, while some will be implemented over a longer period. To remain current and relevant through to 2030, the Action Plan will be reviewed every two years, with actions being updated, added and removed as required.

Action plan

Shield 1

Strong businesses and citizens

Action		Accountable agency
1. Support small and medium businesses to strengthen their cyber security		
Offer advice and guidance to support small and medium businesses	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ASD • Treasury
Build cyber resilience and provide support when an incident occurs	**Establish a Small Business Cyber Security Resilience Service** to provide free tailored advice and victim support, accessible through cyber.gov.au.	**Lead agency:** • Treasury **Contributing agencies:** • ASD • AGD • Home Affairs
2. Help Australians defend themselves from cyber threats		
Extend the reach and accessibility of cyber awareness programs	**Expand the national cyber security awareness campaign** to uplift cyber security outreach and literacy among the Australian community.	**Lead agency:** • Home Affairs
Empower diverse communities to grow their cyber awareness	**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.	**Lead agency:** • Home Affairs **Contributing agency:** • DSS (Grants Hub)

Action		Accountable agency
3. Disrupt and deter cyber threat actors from attacking Australia		
Build our law enforcement and offensive capabilities	**Amplify current cybercrime disruption activities** under Operation Aquila to target the highest priority cybercrime threats impacting Australia, both nationally and internationally.	**Lead agency:** • AFP **Contributing agencies:** • AGD • ASD • Home Affairs
Shape international legal frameworks and cooperation on cybercrime	**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.	**Lead agencies:** • AGD • DFAT **Contributing agencies:** • ASD • AFP • Home Affairs
	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.	**Lead agencies:** • AGD • DFAT **Contributing agencies:** • DITRDCA • eSafety
4. Work with industry to break the ransomware business model		
Enhance our visibility of the ransomware threat	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AFP • AGD • ASD
Provide clear guidance on how to respond to ransomware	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AFP • AGD • ASD • DFAT • Treasury

Action		Accountable agency
Drive global counter-ransomware operations	**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).	**Lead agency:** • Home Affairs **Contributing agency:** • DFAT
5. Provide clear cyber guidance for businesses		
Clarify expectations of corporate cyber governance	**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.	**Lead agencies:** • Home Affairs • Treasury **Contributing agencies:** • AGD • ASIC • Other departments and regulators
Share lessons learned from cyber incidents	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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AFP • AGD • ASD • Defence • PM&C • Other agencies as appropriate

Action		Accountable agency
6. Make it easier for Australian businesses to access advice and support after a cyber incident		
Simplify incident reporting	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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ACCC • ACMA • AFP • AGD • APRA • ASD • ASIC • Defence • DITRDCA • DTA • OAIC • ONDC • Treasury • Other agencies as required
Promote access to trusted support after an incident	**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.	**Lead agency:** • ASD • Home Affairs **Contributing agencies:** • AFP • AGD • APRA • ASIC • OAIC • ONDC • PM&C • Other departments and regulators

Action		Accountable agency
Promote access to trusted support after an incident *continued*	**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.	**Lead agency:** • ASD • Home Affairs **Contributing agencies:** • AFP • AGD • Defence • ONDC • PM&C • Other agencies as required
7. Secure our identities and provide better support to victims of identity theft		
Expand the Digital ID program to help keep Australians' identities safe	**Expand the Digital ID program** to reduce the need for people to share sensitive personal information with government and businesses to access services online.	**Lead agency:** • Finance **Contributing agencies:** • AGD • ATO • Services Australia • ACCC
Expand support services for victims of identity theft	**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.	**Lead agency:** • AGD

Shield 2

Safe technology

Action		Accountable agency
8. Ensure Australians can trust their digital products and software		
Adopt international security standards for digital technologies	**Adopt international security standards for consumer grade smart devices** by working with industry to co-design a mandatory cyber security standard.	**Lead agency:** • Home Affairs **Contributing agencies:** • ACMA • AGD • DISR • DITRDCA • Health • Treasury • Law enforcement agencies
	Co-design a voluntary labelling scheme to measure the cyber security of smart devices, developed through consultation with industry and aligned to international exemplars.	**Lead agency:** • Home Affairs **Contributing agencies:** • ACMA • AGD • DISR • DITRDCA • Treasury
Embed cyber security into software development practices	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ACMA • AGD • DISR • DITRDCA • Health

Action		Accountable agency
Embed cyber security into software development practices *continued*	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AGD • DFAT • DTA • PM&C
Manage the national security risks of digital technology	**Develop a framework for assessing the national security risks** presented by vendor products and services entering ad operating within the Australian economy.	**Lead agency:** • Home Affairs **Contributing agencies:** • ASD • ASIO • Defence • DFAT • DISR • DITRDCA • Treasury
9. Protect our most valuable datasets		
Protect our datasets of national significance	**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.	**Lead agency** • Home Affairs **Contributing agencies:** • AGD • ASIO • Defence • DISR • Finance • Health • Treasury
Support data governance and security uplift across the economy	**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.	**Lead agency:** • AGD • Home Affairs **Contributing agencies:** • Finance • OAIC • Treasury

Action		Accountable agency
Support data governance and security uplift across the economy *continued*	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AGD • ASIO • Defence • DISR • Treasury
	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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AGD • DISR • Finance • Treasury
10. Promote the safe use of emerging technology		
Support safe and responsible use of AI	**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.	**Lead agency:** • Home Affairs (through the National Security Node) • DISR **Contributing agency:** • ASD
Prepare for a post-quantum world	**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.	**Lead agency:** • ASD **Contributing agencies:** • CSIRO • DISR

Shield 3

World-class threat sharing and blocking

Action		Accountable agency
11. Create a whole-of-economy threat intelligence network		
Share strategic threat intelligence with industry	**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.	**Lead agency:** • Home Affairs **Contributing agency:** • ASD
Expand tactical and operational threat intelligence sharing	**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.	**Lead agency:** • ASD **Contributing agencies:** • ACMA • AGD • DITRDCA
	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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ACMA • ADHA • AGD • ASD • DITRDCA • Health
	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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ACMA • AGD • ASD • DITRDCA

Action		Accountable agency
12. Scale threat blocking capabilities to stop cyber attacks		
Develop next-generation threat blocking capabilities	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AFP • AGD
Expand the reach of threat blocking capabilities	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ACMA • AGD • ASD • DITRDCA

Shield 4

Protected critical infrastructure

Action		Accountable agency
13. Clarify the scope of critical infrastructure regulation		
Ensure we are protecting the right entities	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ACMA • AGD • DITRDCA
	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.	**Lead agency:** • Home Affairs **Contributing agency:** • DTA
	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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ACIC • AFP • AGD • AMSA • ASD • CASA • DCCEEW • Defence • DEWR • DFAT • DITRDCA • PM&C
Ensure we are protecting the right assets	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AGD • OAIC

Action		Accountable agency
14. Strengthen cyber security obligations and compliance for critical infrastructure		
Enhance cyber security obligations for Systems of National Significance	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • Commonwealth agencies and regulators, and state and territory agencies and regulators, as appropriate
Ensure critical infrastructure is compliant with cyber security obligations	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • Commonwealth, state and territory agencies and regulators, as appropriate
Help critical infrastructure manage the consequences of cyber incidents	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ASD • Commonwealth agencies and regulators, and state and territory agencies and regulators, as appropriate

Action		Accountable agency
15. Uplift cyber security of the Commonwealth Government		
Strengthen the cyber maturity of government departments and agencies	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ASD • DTA
	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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ASD • DTA • Whole of government
	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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ASD • DTA
Identify and protect critical systems across government	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • ASD • Defence • DTA
Uplift the cyber skills of the Australian Public Service (APS)	**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.	**Lead agency:** • APSC **Contributing agencies:** • ASD • Defence • Home Affairs

Action		Accountable agency
16. Pressure-test our critical infrastructure to identify vulnerabilities		
Conduct national cyber security exercises across the economy	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AGD • Defence • NEMA
Build playbooks for incident response	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • AGD • Defence • NEMA

Shield 5

Sovereign capabilities

Action		Accountable agency
17. Grow and professionalise our national cyber workforce		
Grow and expand Australia's cyber skills pipeline	**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.	**Lead agency:** • Home Affairs
Improve the diversity of the cyber workforce	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • DISR • PM&C • (building on previous BETA work)
Professionalise the domestic cyber workforce	**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.	**Lead agency:** • Home Affairs **Contributing agencies:** • DEWR • DISR
18. Accelerate our local cyber industry, research and innovation		
Invest in domestic cyber industry growth	**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.	**Lead agency:** • Home Affairs **Contributing agency:** • DISR

Shield 6

Resilient region and global leadership

Action		Accountable agency
19. Support a cyber-resilient region as the partner of choice		
Strengthen collective cyber resilience with neighbours in the Pacific and Southeast Asia	**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.	**Lead agency:** • DFAT **Contributing agencies:** • AFP • AGD • ASD • Defence • DISR • DITRDCA • eSafety • Home Affairs
	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.	**Lead agency:** • DFAT **Contributing agencies:** • A range of agencies, including ASD
Harness private sector innovation and expertise in the region	**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.	**Lead agency:** • DFAT **Contributing agency:** • ASD

Action		Accountable agency
20. Shape, uphold and defend international cyber rules, norms and standards		
Support international standards for transparent and secure development of technology	**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.	**Lead agency:** • DISR **Contributing agencies:** • Whole of government
Advocate for high-quality digital trade rules	**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.	**Lead agency:** • DFAT **Contributing agencies:** • Whole of government
Defend an open, free, secure and interoperable internet in international forums	**Continue to defend an open, free, secure and interoperable internet in international forums** by working with international partners, industry, academia, the technical community, civil society and other relevant stakeholders. Government will advocate for continuing, consensus-based improvements to existing mechanisms of multi-stakeholder internet governance.	**Lead agency:** • DITRDCA **Contributing agencies:** • Whole of government
Uphold international law and norms of responsible state behaviour in cyberspace	**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.	**Lead agencies:** • DFAT **Contributing agencies:** • AGD • Defence
Deploy all arms of statecraft to deter and respond to malicious actors	**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.	**Lead agency:** • DFAT • Home Affairs **Contributing agencies:** • AFP • AGD • ASD

Appendix A: Lead and contributing agency abbreviations

ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
ACMA	Australian Communications and Media Authority
ADHA	Australian Digital Health Agency
AFP	Australian Federal Police
AGD	Attorney-General's Department
AMSA	Australian Maritime Safety Authority
APRA	Australian Prudential Regulation Authority
APSC	Australian Public Service Commission
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIC	Australian Securities and Investments Commission
ASX	Australian Securities Exchange
BETA	Behavioural Economics Team of the Australian Government (within PM&C)
CASA	Civil Aviation Safety Authority

CSIRO	Commonwealth Scientific and Industrial Research Organisation
DCCEEW	Department of Climate Change, Energy, the Environment and Water
Defence	Department of Defence
DEWR	Department of Employment and Workplace Relations
DFAT	Department of Foreign Affairs and Trade
DISR	Department of Industry, Science and Resources
DITRDCA	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
DSS	Department of Social Services
DTA	Digital Transformation Agency
eSafety	eSafety Commissioner
Finance	Department of Finance
Health	Department of Health and Aged Care
Home Affairs	Department of Home Affairs
NEMA	National Emergency Management Agency
OAIC	Office of the Australian Information Commissioner
ONDC	Office of the National Data Commissioner
PM&C	Department of the Prime Minister and Cabinet
Treasury	Department of the Treasury