Question on notice no. 18

Portfolio question number: BE24-0018

2024-25 Budget estimates

Legal and Constitutional Affairs Committee, Home Affairs Portfolio

Senator James Paterson: asked the Department of Home Affairs on 28 May 2024—

Senator PATERSON: I'll see how I go. How many of the actions from the cybersecurity action plan have been implemented so far?
Lt Gen. McGuinness: I can take that. At first blush, four have been implemented largely in full, 29 have been substantially progressed, 11 we consider to be ongoing and 16 are yet to be commenced or are in limited progress. That's the plan for the two years.
Senator PATERSON: How far are we into that?
Mr Hansford: Eight months.
Senator PATERSON: Eight months. So we're not yet halfway, but only four of-how many total items?
Lt Gen. McGuinness: Of 60 in total, 33 are considered substantially or largely complete.
Senator PATERSON: What's the difference between something delivered in full and something being substantially progressed?
Lt Gen. McGuinness: Some of them are ongoing and continue throughout the period. But I can pass to Mr Hansford
Mr Hansford: A good example is that the 'Act now. Stay secure' campaign is largely completed. It's being rolled out as we speak, between now and 30 June, and then that will be completed, from our perspective, for the first phase.
Senator PATERSON: Perhaps on notice you could provide the information for the four, 24, 11 and 16.
Mr Hansford: We certainly can, Senator
Answer —
Please see the attached answer.

SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS
BUDGET ESTIMATES
MAY 2024

Home Affairs Portfolio
Department of Home Affairs

Program 1.3: Cyber Security

BE24-0018 - Cybersecurity Action Plan

Senator James Paterson asked:

Senator PATERSON: I'll see how I go. How many of the actions from the cybersecurity action plan have been implemented so far?
Lt Gen. McGuinness: I can take that. At first blush, four have been implemented largely in full, 29 have been substantially progressed, 11 we consider to be ongoing and 16 are yet to be commenced or are in limited progress. That's the plan for the two years.
Senator PATERSON: How far are we into that?
Mr Hansford: Eight months.
Senator PATERSON: Eight months. So we're not yet halfway, but only four of—how many total items?
Lt Gen. McGuinness: Of 60 in total, 33 are considered substantially or largely complete.
Senator PATERSON: What's the difference between something delivered in full and something being substantially progressed?
Lt Gen. McGuinness: Some of them are ongoing and continue throughout the period. But I can pass to Mr Hansford
Mr Hansford: A good example is that the 'Act now. Stay secure' campaign is largely completed. It's being rolled out as we speak, between now and 30 June, and then that will be completed, from our perspective, for the first phase.
Senator PATERSON: Perhaps on notice you could provide the information for the four, 24, 11 and 16.
Mr Hansford: We certainly can, Senator

Answer:

The status of each initiative within the *2023-2030 Australian Cyber Security Strategy Action Plan* as at 30 June 2024 is as follows:

Action		**Delivery Status at 30 June 2024**
Shield 1: Strong businesses and citizens		
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.	Limited progress/yet to be commenced (Working to agreed timeframes)
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.	Substantially progressed
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.	Substantially progressed
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.	Substantially progressed
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.	Ongoing
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.	Ongoing
	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.	Substantially progressed
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.	Substantially progressed
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.	Substantially progressed
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).	Ongoing
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.	Limited progress/yet to be commenced (Subject to further consideration by Government)
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.	Substantially progressed
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.	Substantially progressed
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.	Substantially progressed

	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.	Substantially progressed
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.	Substantially progressed
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.	Ongoing
Shield 2: Safe technology		
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.	Substantially progressed
	Co-design a voluntary labelling scheme to measure the cyber security of smart devices, developed through consultation with industry and aligned to international exemplars.	Limited progress/yet to be commenced (Sequenced after the legislative process for the cyber security standard)
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.	Limited progress/yet to be commenced (Working to agreed timeframes)
	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.	Limited progress/yet to be commenced (Subject to scheduling complexities arising within this multilateral initiative)
Manage the national security risks of digital technology	Develop a framework for assessing the national security risks presented by vendor products and services entering and operating within the Australian economy.	Substantially progressed (Subject to further Government consideration)
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.	Limited progress/yet to be commenced (Working to agreed timeframes)
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.	Substantially progressed
	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.	Limited progress/yet to be commenced (Working to agreed timeframes)

	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.	Limited progress/yet to be commenced (Working to agreed timeframes)
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.	Substantially progressed
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.	Limited progress/yet to be commenced (Consistent with outputs and timeframes of key international partners)
Shield 3: World-class threat sharing and blocking		
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.	Implemented in full
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.	Ongoing
	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.	Substantially progressed
	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.	Limited progress/yet to be commenced (Working to agreed timeframes)
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.	Ongoing
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.	Limited progress/yet to be commenced (Working to agreed timeframes)
Shield 4: Protected critical infrastructure		
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.	Substantially progressed

	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.	Limited progress/yet to be commenced (Working to agreed timeframes)
	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.	Substantially progressed
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.	Substantially progressed
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.	Substantially progressed
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.	Substantially progressed
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.	Substantially progressed
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.	Implemented in full
	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.	Limited progress/yet to be commenced (Working to agreed timeframes)

	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.	Ongoing
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.	Limited progress/yet to be commenced (Working to agreed timeframes)
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.	Limited progress/yet to be commenced (Working to agreed timeframes)
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.	Ongoing
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.	Substantially progressed
Shield 5: Sovereign capabilities		
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.	Limited progress/yet to be commenced (Working to agreed timeframes)
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.	Limited progress/yet to be commenced (Working to agreed timeframes)
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.	Limited progress/yet to be commenced (Working to agreed timerames)
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.	Limited progress/yet to be commenced (Working to agreed timeframes)

Shield 6: Resilient region and global leadership		
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.	Ongoing
	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.	Substantially progressed
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.	Substantially progressed
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.	Ongoing
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.	Ongoing
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.	Ongoing
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.	Ongoing
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.	Substantially progressed

Delivery status as at 30 June 2024 has been included to provide the most current information available. The Department notes the limitations of the delivery status categories currently used in this reporting. The Department is working to assess the

suitability of the methodology used to measure the implementation of the 2023-2030 Australian Cyber Security Strategy, and will seek to optimise the approach toward best practice.