Australian Government

Australian Government response to the Senate Select Committee on Foreign Interference through Social Media:

First Interim and Final Reports

June 2024

Final Report Recommendations

Final Recommendation 1: ***The committee recommends the Australian Government require all large social media platforms operating in Australia to meet a minimum set of transparency requirements, enforceable with fines. Any platform which repeatedly fails to meet the transparency requirements could, as a last resort, be banned by the Minister for Home Affairs via a disallowable instrument, which must be reviewed by the Parliamentary Joint Committee on Intelligence and Security.***

Requirements should include, at minimum, that all large social media platforms:

- ***must have an Australian presence;***
- ***must proactively label state affiliated media;***
- ***must be transparent about any content they censor or account takedown on their platform;***
- ***must disclose any government directions they receive about content on their platform, subject to national security considerations;***
- ***must disclose cyber-enabled foreign interference activity, including transnational repression and surveillance originating from foreign authoritarian governments;***
- ***must disclose any takedowns of coordinated inauthentic behaviour (CIB) networks, and report how and when the platform identified those CIB networks;***
- ***must disclose any instances where a platform removes or takes adverse action against an elected official's account;***
- ***must disclose any changes to their platform's data collection practices or security protection policies as soon as reasonably practicable;***
- ***must make their platform open to independent cyber analysts and researchers to examine cyber-enabled foreign interference activities;***
- ***must disclose which countries they have employees operating in who could access Australian data and keeps auditable logs of any instance of Australian data being transmitted, stored or accessed offshore; and***
- ***must maintain a public library of advertisements on their platform.***

Response: Support in principle

The Government supports the principle of increased transparency requirements for platforms, where appropriate, to address specific harms such as harmful misinformation and disinformation online.

On 25 June 2023, the Government released an Exposure Draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 to provide the Australian Communications and Media Authority (ACMA) with new powers to combat online misinformation and disinformation.

These proposed powers will bring greater transparency on the efforts by digital platforms to respond to misinformation and disinformation on their services including foreign interference, while balancing freedom of expression and speech which is at the heart of democracy and Australia’s way of life.

The Bill will represent a significant step forward in addressing foreign interference in Australia through digital platforms, enhancing the powers and the obligations to ensure Australians have protections against malign messaging that promotes harmful and false narratives.

The ACMA would have reserve code registration and standard making powers that would place obligations on the platforms to have systems and processes that address disinformation and misinformation on their services. This could include a range of measures to tackle foreign interference, and work in collaboration with national security agencies’ advice and existing powers.

The Government will consider feedback from the public consultation process which closed on 20 August 2023, before the Bill is introduced in Parliament.

Final Recommendation 2: ***The committee recommends that, should the United States Government force ByteDance to divest its stake in TikTok, the Australian Government review this arrangement and consider the appropriateness of ensuring TikTok Australia is also separated from its ByteDance parent company.***

Response: Noted

Any decision by the United States Government relating to the forced divestiture of a company or companies is a matter for the United States Government.

The Australian Government continues to assess Australia's technology security policy settings to ensure they remain fit-for-purpose. Policy settings are based on Australia's assessments and implications for Australia's interests, informed by advice from relevant Australian government agencies. We also consult closely with international counterparts on risk assessments. The National Intelligence Community monitors the threat environment, and the Australian Government carefully and wholly considers their advice to ensure our security settings remain proportionate and contemporary. The Australian Government is actively pursuing measures to strengthen the protection of Australia's data under the 2023-2030 Australian Cyber Security Strategy. Measures currently being implemented relevant to social media platforms include:

- the development of a framework for assessing the national security risks presented by technology vendor products and services entering and operating within the Australian economy;
- working with industry and our international partners to co-design a voluntary code of practice for app stores and app developers; and
- conducting a review of the data brokerage ecosystem and explore options to restrict unwanted transfer of data to malicious actors via data markets.

Final Recommendation 3:

(a) ***The committee recommends the Australian Government extend, via policy or appropriate legislation, directives issued under the Protective Security Policy Framework regarding the banning of specific applications (e.g. TikTok) on all government contractors' devices who have access to Australian government data; and***

(b) The Minister for Home Affairs should review the application of the Security of Critical Infrastructure Act 2018, to allow applications banned under the Protective Security Policy Framework to be banned on work-issued devices of entities designated of Systems of National Significance.

Response: (a) Supported and (b) Support in principle

(a) Under current policy, directions issued by the Secretary of the Department of Home Affairs under the Protective Security Policy Framework (PSPF) are mandatory for all non-corporate Commonwealth entities to apply, unless otherwise specified. Directions relating to the use of specific applications or technology apply to all personnel who access Australian Government information and data. The PSPF defines 'personnel' as employees and contractors, including secondees and any service providers that an entity engages. It also includes anyone who is given access to Australian government resources held by the entity as part of entity sharing initiatives.

(b) The Government supports the principle of working closely with Systems of National Significance (SoNS)—Australia's most vital critical infrastructure—to ensure they are well prepared to respond to and prevent cyber attacks. The Government will continue to provide advice to SoNS to ensure they have broad awareness of security risks.

Final Recommendation 4: ***The committee recommends the Australian Government consider extending the Protective Security Policy Framework directive banning TikTok on federal government devices to WeChat, given it poses similar data security and foreign interference risks.***

Response: Noted

The Australian Government continues to assess technologies that may pose a security risk and will take further action if required. This action could include issuing further directions under the PSPF or amendments to the protective security settings.

Any measures taken will be proportionate and appropriate to protect sensitive government information and Australia's national interests, and will be informed by advice from relevant entities, including through the Protective Security Board, Government Security Committee and its subcommittees.

Final Recommendation 5: ***The committee recommends the Australian Government continues to audit the security risks posed by the use of all other social media platforms on government-issued devices within the Australian Public Service, and issue general guidance regarding device security, and if necessary, further directions under the Protective Security Policy Framework.***

Response: Supported

The Government notes that all social media applications carry risks associated with their use and these risks are particularly acute for Commonwealth entities and Australian Government officials.

The Government will continue to provide guidance to Commonwealth entities on managing cyber security risks arising from mobile applications outlined in the Australian Signals Directorate's (ASD) *Information Security Manual* (ISM), the Australian Cyber Security Centre's *Security Tips for Social Media and Messaging Apps*, and the PSPF. Where there are significant risks identified of national security concern, the PSPF enables directions to be made to non-corporate Commonwealth entities.

Protective security settings remain under constant review and the Government takes the advice of agencies on emerging risks and appropriate mitigations. Any measures taken will be proportionate and appropriate to protect sensitive government information and Australia's national interests and will be informed by advice from relevant entities, including through the Protective Security Board, Government Security Committee and its subcommittees.

Final Recommendation 6: ***The committee recommends the Australian Government establish a national security technology office within the Department of Home Affairs to map existing exposure to high-risk vendors such as TikTok, WeChat and any similar apps that might emerge in the future. It should recommend mitigations to address the risks of installing these applications, and where necessary, ban them from being installed on government devices.***

Response: Noted

Following the 3 August 2023 machinery of government change, the Department of Home Affairs assumed responsibility for protective security for the Australian Government, including the PSPF. The PSPF enables the Secretary of the Department of Home Affairs to issue mandatory directions to government entities when considered necessary to address protective security risks to the Commonwealth.

Protective security settings remain under constant review and the Government takes the advice of agencies on emerging risks and appropriate mitigations. Any measures taken will be proportionate and appropriate to protect sensitive government information and Australia's national interests and will be informed by advice from relevant entities, including through the Protective Security Board, Government Security Committee and its subcommittees.

As a part of the *2023–2030 Australian Cyber Security Strategy* the Government has announced the development of a framework for assessing and managing the national security risks presented by various technology products and services entering and operating within the Australian market.

The Government notes that all social media applications carry risks associated with their use and these risks are particularly acute for Commonwealth entities and Australian Government officials. The PSPF direction to restrict the presence of TikTok on Government devices builds resilience against the threats that social media applications pose to the security of Australians' data.

Final Recommendation 7: ***The committee recommends the Australian Government designate an entity with lead responsibility for whole-of-government efforts to counter cyber-enabled foreign interference, with appropriate interdepartmental support and collaboration, resources, authorities and a strong public outreach mandate.***

Response: Noted

"Cyber-enabled foreign interference" is a broad concept that could encompass efforts to compromise Australian ICT networks or computers, as well as the use of cyber-enabled techniques to create social division and influence public opinion.

Cyber is a vector for foreign interference, not a threat in and of itself. Foreign interference is defined in the *Australian Security Intelligence Organisation* (ASIO) *Act 1979* as "activities relating to Australia that are carried on by or on behalf of, are directed or subsidised by or are undertaken in active collaboration with, a foreign power, being activities that: (a) are clandestine or deceptive and: (i) are carried on for intelligence purposes; (ii) are carried on for the purpose of affecting political or governmental processes; or (iii) are otherwise detrimental to the interests of Australia; or (b) involve a threat to any person."

The National Counter Foreign Interference Coordinator (NCFIC) coordinates whole-of-government efforts to counter foreign interference. The NCFIC works across government and non-government sectors to strengthen arrangements and partnerships to counter foreign interference. The NCFIC is supported by the Counter Foreign Interference Coordination Centre within the Department of Home Affairs, which has a presence in Canberra and most state capitals around Australia.

A comprehensive response to the threats posed by foreign interference via any vector involves action from a range of departments and agencies:

- ASIO established the Counter Foreign Interference (CFI) Taskforce which, discovers, disrupts and investigates foreign interference activity. The taskforce includes the Australian Federal Police (AFP) and other NIC agencies.
- ASD leads well-established incident response mechanisms to help mitigate the compromise of Australian computer networks or systems by malicious cyber actors. ASD is responsible for the provision of expert technical advice and assistance, drawing lessons from its unique intelligence insights and experience in responding to malicious cyber activity, to inform cyber defence and hardening activities across government, industry and the wider economy.
- A number of Commonwealth agencies play a role in dealing with matters of disinformation in Australia.
    - The Department of Home Affairs advises the Government on the national security implications of foreign information manipulation and interference and the impact of digital platform features.
    - The Department of Infrastructure, Transport, Regional Development, Communications and the Arts is responsible for providing policy advice to the Australian Government on disinformation informed by engagement with digital platforms and the Australian Communications and Media Authority.
- The Australian Electoral Commission (AEC) is the Australian Government agency with responsibility for the delivery and integrity of federal electoral events, including elections,

by-elections and referendums. In the event of foreign interference relevant to the integrity of a federal electoral event, members of the Electoral Integrity Assurance Taskforce (EIAT) provide consolidated and coordinated advice and offer assistance to the AEC in the performance of its mandate.

- ASIO's purpose is to protect Australia and Australians from threats to their security, and its functions are set out in section 17 of the *ASIO Act 1979*. Security is defined in section 4 of the *ASIO Act 1979*, which includes the protection of Australia and its people from: espionage; sabotage; politically motivated violence; promotion of communal violence; attacks on Australia's defence system; or acts of foreign interference, whether directed from, or committed within, Australia or not; and the protection of Australia's territorial and border integrity from serious threats.

Separately, a number of agencies play a role in dealing with the technical incident management and consequence management of cyber security incidents. The National Cyber Security Coordinator, supported by the National Office of Cyber Security (NOCS), leads on national cyber security policy, the coordination of the Commonwealth's response to major cyber incidents, whole of Government cyber incident preparedness efforts and the strengthening of Commonwealth cyber security capability. Through the work of the Coordinator and the NOCS, the Government will ensure citizens are better protected and business and critical infrastructure entities are cyber resilient. These arrangements will confirm and preserve the operational independence of the AFP and ASD.

Final Recommendation 8: ***The committee recommends the Australian Government address countering cyber-enabled foreign interference as part of the 2023–2030 Australian Cyber Security Strategy.***

Response: Supported

The Australian Government supports this recommendation and is addressing countering cyber-enabled foreign interference in the *2023–2030 Australian Cyber Security Strategy* (the Strategy).

The Strategy will primarily address countering cyber-enabled foreign interference through initiatives targeted at promoting cyber awareness among the community and actions to enhance the security of our technology.

Awareness raising initiatives will strengthen the collective cyber resilience of Australian communities that may be more vulnerable to cyber-enabled foreign interference. Targeted campaigns will directly support diverse groups, including culturally and linguistically diverse communities, with the tools and information needed to better identify and respond to this threat.

In addition to awareness raising, the Government will provide end-users with confidence that their digital products are safe to use, without hindering industry innovation. Through the Strategy, Government will promote secure-by-design in digital technologies to protect Australian citizens and businesses from cyber incidents, which may include some forms of cyber-enabled foreign interference.

The Government has committed to work with industry to co-design a mandatory cyber security standard for consumer-grade Internet of Things (IoT) devices. To complement the standard, the Government has committed to developing a voluntary, industry-led labelling scheme for consumer-grade smart devices. These initiatives will support consumers embracing the benefits of technology, while uplifting baseline protection against cyber threats. The Government will also work with industry and international partners to shape the development and adoption of secure-by-design and secure-by-default practices in software development, including in applications (apps), by developing a voluntary code of practice for app store operators and developers. Ongoing work, including international efforts in this space, will consider whether further action is required to counter cyber-enabled foreign interference.

The Government will develop a framework for assessing the national security risks presented by vendor products and services operating within and entering the Australian market. Using this framework, the Government will help industry manage supply chain risks and make informed procurement decisions about the security of products and services. We will also consult industry on further options to limit the availability of non-secure products in the domestic market.

Final Recommendation 9: ***The committee recommends the Australian Government clarify that Magnitsky-style cyber sanctions in the Autonomous Sanctions Act 2011 can be used to target cyber-enabled foreign interference actors, via legislative amendment if necessary, and ensure it has appropriate, trusted frameworks for public attribution.***

Response: Noted

The cyber sanctions framework (under *the Autonomous Sanctions Regulations 2011*) targets individuals and entities involved in causing 'significant cyber incidents'. Australia has recently used cyber sanctions powers on a Russian individual for his role in the breach of the Medibank Private network. Depending on the specific circumstances regarding a particular cyber-enabled foreign interference incident, the cyber sanctions framework may be applicable.

Other geographic or thematic sanctions frameworks under the Autonomous Sanctions Regulations could potentially apply to these circumstances if relevant criteria under these frameworks are met.

The Government has established a range of resilience mechanisms to protect Australia against foreign interference. The Government will continue to assess this recommendation against existing mechanisms and through opportunities within the *2023–2030 Australian Cyber Security Strategy*.

Final Recommendation 10: ***The committee recommends the Australian Government refer the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 to the Parliamentary Joint Committee on Intelligence and Security for review, with particular reference to the Act's effectiveness in addressing cyber-enabled foreign interference.***

Response: Noted

Subsection 6(1B) of the *Independent National Security Legislation Monitor Act 2010* provides that the Independent National Security Legislation Monitor (INSLM) must, as soon as practicable after the third anniversary of the day the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (the Act) receives the Royal Assent, begin a public review under paragraph (1)(a) of the following provisions of Chapter 5 of the Criminal Code:

- Division 82 (sabotage)
- Part 5.2 (espionage and related offences)
- Part 5.6 (secrecy of information).

The Act received Royal Assent on 29 June 2018. The Government will consider any recommendations of the INSLM following receipt of the INSLM's report.

Final Recommendation 11: ***The committee recommends the Australian Government investigate options to identify, prevent and disrupt artificial intelligence (AI)-generated disinformation and foreign interference campaigns, in addition to the Government's Safe and Responsible AI in Australia consultation process.***

Response: Supported

Artificial Intelligence (AI) refers to an engineered system that generates predictive outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are one subset of emerging technologies. AI systems are designed to operate to varying degrees of automation, and include:

- machine learning – patterns derived from training data using machine learning algorithms, which can be applied to new data for prediction or decision-making purposes; and
- generative AI – generation of novel content such as text, images, video, audio and code in response to prompts.

AI is already improving many aspects of Australians' lives. But the speed of innovation in AI amplifies existing and could pose new national security risks, including from foreign interference.

In June 2023, the Department of Industry, Science and Resources (DISR) released the 'Safe and responsible AI in Australia' discussion paper, seeking views on how government can mitigate potential risks of AI and support safe and responsible practice. Feedback will inform policy responses, building on the Government's investment in responsible AI, through the 2023–24 Budget.

The Department of Home Affairs continues to assess the national security threats, risks and vulnerabilities arising from AI, including applications of AI as a tool for misinformation, disinformation and foreign interference. The Department of Home Affairs will continue to work with relevant agencies to address national security risks presented by AI.

The Department of Home Affairs will work closely with DISR and other relevant agencies to undertake further analysis of the options to identify, prevent and disrupt AI generated disinformation and foreign interference campaigns.

The Digital Transformation Agency, working with the DISR has developed interim guidance on government use of generative AI platforms for staff within Commonwealth government agencies. The guidance was developed through broad consultation with Commonwealth agencies and builds on existing agency and inter-jurisdictional guidance.

DTA and NSW Government are co-leading work under the oversight of the Data and Digital Ministers Meeting (DDMM) to develop national framework for the assurance of AI used by governments. An initial framework was agreed by DDMM in February 2024, this initial framework aligns with the Australian AI Ethics Principles and includes common assurance processes. Work is continuing via a cross-jurisdictional working group to develop and release the National Framework for AI Assurance.

Final Recommendation 12: ***The committee recommends the Australian Government establish a program of vetting appropriate personnel in trusted social media platforms with relevant clearances to ensure there is a point of contact who can receive threat intelligence briefings.***

Response: Support in principle

The Government supports the principle that information sharing with trusted social media platforms, including threat intelligence, is a key enabler for collaboration between industry partners and Government. However, the Government does not consider there is a need to establish a program of vetting appropriate personnel, to achieve this outcome, outside of already established avenues.

A number of agencies sponsor clearances in the private sector. The Government engages with a variety of industry partners on a range of thematic issues to inform them of risks, including foreign interference. Engagement includes bilateral agency meetings, topic-dependent agency led forums, and joint-agency engagement.

There are a number of forums for the Government that could be further leveraged to share information, including intelligence, with appropriately cleared individuals in certain industry contexts. For example,

- The Trusted Information Sharing Network (TISN) is an Australian Government engagement mechanism with industry on critical infrastructure and established with the assistance of critical infrastructure owners and operators in 2003. It brings together stakeholders from across the critical infrastructure community, including critical infrastructure owners and operators, supply chain entities, peak bodies, academics, research institutes, and all levels of

government. Through the TISN, member organisations meet regularly within and across sector groups in a secure, non-competitive environment to enhance the security and resilience of critical infrastructure by:

- understanding threat, vulnerability and consequence to better manage risk;
- increasing awareness and understanding of cross-sector dependencies and the impacts of a disruption to any critical infrastructure sector;
- enhancing communication channels and networks between industry and all levels of government;
- identifying gaps and implementing appropriate mitigation strategies within each sector; and
- informing future policies and programs to support critical infrastructure resilience.

Separately, in the electoral context, the Electoral Integrity Assurance Taskforce (EIAT) provides a mechanism for sharing information between relevant agencies on potential threats to electoral integrity such as disinformation campaigns, foreign interference and cyber intrusions. The EIAT is responsible for assessing, understanding and mitigating these risks and, if required, providing advice to the Australian Electoral Commissioner.

- EIAT member agencies engage with online media platforms in the lead up to, and during an electoral event. These engagements seek to continue effective working relationships and confirm escalation points for referring content in breach of Australian electoral legislation.

Should the circumstances arise where current information sharing arrangements on risks, including foreign interference, do not meet requirements, the Government will consider exploring options for sharing appropriate information with the relevant entity.

Final Recommendation 13: ***The committee recommends the Australian Government build capacity to counter social media interference campaigns by supporting independent research.***

Response: Supported

Independent research is a key element of the knowledge base underpinning the Government's addressing of foreign interference through social media, and the Government is currently investing in this capacity

The Department of Home Affairs and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (including the Australian Communications and Media Authority) are investing in independent research on misinformation and disinformation. Recent government-commissioned research projects relating to misinformation and disinformation include research on sources and transmission methods, narratives, engagement behaviours, scale of the issues, and drivers and experiences of reporting misinformation and disinformation online.

Final Recommendation 14: ***The committee recommends the Australian Government ensure that law enforcement agencies, and other relevant bodies such as the eSafety Commissioner, work with social media platforms to increase public awareness of transnational repression.***

Response: Noted

Transnational repression has become a growing focus for non-government organisations and partner countries such as the United States. Australia uses the term *community interference* to describe the broad range of foreign interference activities targeting multicultural communities. Australia considers transnational repression to be one form of community interference. Community interference includes threats, intimidation, surveillance or harassment of community members on behalf of, or in collaboration with, a foreign power. Australia's multicultural communities face unique threats and issues from community interference. Some foreign powers or their proxies seek to silence members of multicultural communities that they see as dissidents; spread false or misleading information and communications; and/or co-opt or coerce multicultural members to advance their national interests at

Australia's expense. These activities prevent individuals from exercising their rights and freedoms in Australia, and risk undermining Australia's open and democratic society.

Social media is one vector for community interference. The Australian Government engages social media companies on a range of issues, and raises concerns where appropriate. The AFP engages closely with social media companies on a variety of law enforcement issues, including child exploitation, in order to detect, deter, prevent and disrupt criminal activity.

Law enforcement agencies engage communities to build public awareness of community interference, strengthen community resilience, and investigate reports of foreign interference within multicultural communities. The AFP has developed a Foreign Interference in the Community Factsheet (the Factsheet), to assist in educating Australian communities on foreign interference (including through online vectors), how to recognise it, and how to report it. The Factsheet is publicly available on the AFP website in over 30 languages.

Australia takes a human rights and democratic values-based approach to online safety regulation, meaning that our approach aims to prevent and address harms so that human rights are protected and promoted. We also recognise that online safety is a complex issue that is a shared responsibility between governments, technology service providers and individuals.

Australia supports global efforts to improve online safety, especially for children. We need to advocate for a safer online environment grounded in democratic values and respect for human rights. Globally, reforms based on these values can deliver considerable benefits for Australians. Australia collaborates with a range of countries and participates in various multilateral forums to address global online safety challenges. We will continue to watch international developments closely.

The *Online Safety Act 2021 (Cth)* (the Act) gives the eSafety Commissioner powers to tackle illegal and harmful content online – these are some of the strongest powers in the world. The Act enhanced content removal powers and takedown schemes, while also moving Australia towards a more systems-based and preventative approach that is underpinned by transparency and accountability of online service providers.

Final Recommendation 15: ***The committee recommends the Australian Government empower citizens and organisations to make informed, risk-based decisions about their own social media use by publishing plain-language education and guidance material and regular reports and risk advisories on commonly used social media platforms, ensuring this material is accessible for non-English speaking citizens. Specific focus should be on protecting communities and local groups which are common targets of foreign interference and provide pre-emptive information and resources.***

Response: Support in principle

Empowering individuals to make informed decisions about their use of digital technologies can build resilience not only to foreign interference through social media, but also to other online harms perpetuated by malign actors. The Department of Home Affairs engages with communities to build awareness of foreign interference vectors and techniques. The Counter Foreign Interference Coordination Centre (CFICC) within the Department of Home Affairs works with the Departments Community Liaison Officer (CLO) Network to conduct targeted engagement on foreign interference where the community identifies a concern. CFICC engagement teams located in most states and territories support the Department's CLO network, and provide information on Australia's approach to counter foreign interference and other measures to counter foreign interference.

Providing resources and programs in collaboration with trusted stakeholders can assist in building an informed population that is able to assess the risks of their social media use. Partnerships across government and non-government stakeholders that have sound relationships with the community, particularly vulnerable groups, supports effective messaging.

The ASD publication *Security Tips for Social Media and Messaging Apps,* first published on 1 August 2011, and last updated on 14 July 2022 provides cyber security guidance highlighting the risks of social media and messaging applications, including the exploitation of personal information, data collection, identity theft, fraud, and reputation damage. The guide also provides recommendations for businesses and individuals to assist in securing their social media accounts and messaging applications.

To help support multicultural audiences secure their devices, ASD has expanded its most popular personal cyber security guides on www.cyber.gov.au into more than 20 languages, increasing accessibility of information to more people from non-English speaking backgrounds.

Australia's eSafety Commissioner undertakes research, consultation and community engagement to understand online risks and identify the needs of people from different multicultural backgrounds. ESafety's regulatory schemes can assist individuals who may be susceptible to foreign interference, such as diaspora groups, those with low digital literacy, and minority groups who may be the target of cyber abuse and illegal activity. These schemes intersect on a range of issues to provide multiple avenues of support for individuals. Its educational resources are also translated into multiple languages and Easy English for people with low literacy, or with intellectual or cognitive disabilities, ensuring its resources are accessible to a range of individuals and communities.

The Australian Government recognises that digital and media literacy provides the foundation for empowering Australians to use social media safely. In October 2022, the Australian Government committed $6 million over three years (2023–24 to 2025–26) to make the Alannah and Madeline Foundation's suite of digital and media literacy tools freely available to all schools nationwide. These products are:

- The eSmart Digital Licence+ for students aged 10 to 14,
- The eSmart Media Literacy Lab for secondary students aged 12 to 16, and
- A new eSmart Junior Digital Licence+ for primary students aged 5 to 9, the development of which will be funded by this election commitment.

These products will help Australian students develop the skills they need to be critical, safe, responsible and empowered citizens online.

The 2023-24 Budget also provided $2.5 million to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts to partner with the Federation of Ethnic Communities' Council of Australia (FECCA) to support media literacy in CALD communities.

Final Recommendation 16: ***The committee recommends the Australian Government support independent and professional foreign-language journalism by supporting journalism training and similar programs, thereby expanding the sources of uncensored news for diaspora communities to learn about issues such as human rights abuses inside their country of origin.***

Response: Support in principle

Protecting Australia's Media and Communications sector is critical to underpinning Australia's commitment to freedom of expression and the value placed on a trusted, free and open media sector.

The Government is currently developing the News Media Assistance Program (News MAP) to guide future policy interventions that support public interest journalism and media diversity. The News MAP will establish a principles-based policy framework and evidence base to inform decisions around when intervention is warranted and where and how it should be targeted. The Government will consider any additional future support for journalism training as part of the News MAP.

The primary purpose of the Special Broadcasting Service (SBS) is set out in its Charter, contained in section 6 of the *Special Broadcasting Service Act 1991*, and requires the SBS to provide multilingual and multicultural broadcasting and digital media services that inform, educate and entertain all Australians, and, in doing so, reflect Australia's multicultural society.

The Australian Government moved the SBS (and the Australian Broadcasting Corporation) to 5-year funding terms commencing 1 July 2023 as part of the 2023-24 Budget. These new arrangements extend previous multi-year funding arrangements – funding for the national broadcasters has been agreed in 3-year periods ('triennia') since 1988 and supported by successive governments.

Over the 5-year term to 30 June 2028, SBS will receive $1.8 billion. This funding includes additional funding of $45 million over 4 years for SBS to continue work to increase the availability of news and content to Chinese and Arabic speaking communities in Australia. SBS uses this funding to provide locally produced in-language news bulletins for Chinese and Arabic speaking communities, subtitling in Simplified Chinese and Arabic for its full portfolio of commissioned and locally produced content, and a free English language learning program for migrants.

Final Recommendation 17: ***The committee recommends the Australian Government promote the digital literacy and the infrastructure of developing countries in the Indo-Pacific region that are the targets of malicious information operations by foreign authoritarian states.***

Response: Supported

Malicious information operations have the capacity to undermine the sovereignty and agency of countries in the Indo-Pacific, and our ability to shape an open, stable and prosperous region, operating by agreed rules, standards and laws.

The Australian Government's capacity building programs with Indo-Pacific partners strengthen the region's cyber and critical technology, media development and literacy, infrastructure, and online safety capabilities.

Australia works with the region through bilateral and multilateral investments, including Australia's Cyber and Critical Tech Cooperation Program (supporting cyber, critical tech and online safety literacy) and delivers a range of activities, including strengthening independent media, training for journalists, capacity building for government agencies and fostering civil society advocacy.

First Interim Report Recommendations

First Interim Recommendation 1: ***The Committee recommends that the Australian Government clearly delegate the lead accountability for cyber-enabled foreign interference to a single entity in government.***

Response: Noted

See the government response to Recommendation 7 from the Senate Select Inquiry on Foreign Interference through Social Media *Final Report.*

First Interim Recommendation 2: ***The Committee recommends that the Australian Government take a proactive approach to protecting groups that are common targets of foreign interference but are not classified as government institutions.***

Response: Supported

Government agencies have been proactive in their efforts to safeguard sectors at risk of foreign interference. Initiatives are either specifically designed to counter foreign interference, or counter a broad range of security threats, including foreign interference.

Government agencies have worked in partnership with the higher education sector, and research and grants agencies to mitigate risks and build resilience to foreign interference. On 17 November 2021, updated *Guidelines to Counter Foreign Interference in the Australian University Sector* were launched following extensive consultation with the university sector through the University Foreign Interference Taskforce.

The Australian Signals Directorate, through the ACSC has a dedicated outreach campaign that provides advice to small-to-medium enterprises on cyber threats and improvement of cyber security practices. Individuals and families can access dedicated advice on cyber.gov.au, including translations in 27 languages. The eSafety Commissioner has published resources to help Australians to have safe experiences online in 27 different languages.

The Department of Home Affairs is working to strengthen Australia's social cohesion, with policies and programs aimed at building community resilience, including from foreign interference. The Department's network of Community Liaison Officers support the communication of official information to multicultural communities, and provide a mechanism for community members to share information about their priorities and concerns. The Counter Foreign Interference Coordination Centre state-based engagement officers regularly hold meetings with a range of stakeholders, including community groups, to raise awareness and help build resilience to foreign interference in CALD communities.

The establishment of the Strengthening Democracy Taskforce in the Department of Home Affairs recognises the role of democratic resilience in responding to national security threats. The biggest challenges to our democratic resilience are those affecting three sources of historic democratic strength:

- Trusted institutions – democratic institutions that maintain legitimacy by performing their roles responsively, securely, and with integrity.
- Credible information – the accuracy, relevance, responsibility, accessibility, and civility of information flows within a deliberative public sphere.
- Social inclusion – a society that is connected, cohesive, participatory, engaged and respectful, reinforcing and reflecting a sense of common purpose and shared identity.

Government agencies continue to raise awareness amongst Commonwealth and state and territory parliamentarians and their senior staff of the threats posed to them by foreign interference.

First Interim Recommendation 3: ***The Committee recommends that the Australian Government establish appropriate, transparent, and non-political institutional mechanisms for publicly communicating cyber-enabled foreign interference in our elections and review the processes and protocols for classified briefings for the Opposition during caretaker with respect to cyber-enabled foreign interference.***

Response: Noted

During the caretaker period, EIAT member agencies operate within the framework of the *Guidance on Caretaker Conventions*. While policy advice is generally not provided to Ministers during the caretaker period, situations may arise where an agency head considers that the responsible Minister should be briefed to enable responsible ongoing administration or to protect Australia's interests. The *Guidance on Caretaker Conventions* provides for the responsible Minister to consult the Opposition on significant matters.

In the event of a foreign interference incident related to the integrity of a federal election, the Australian Electoral Commissioner would consider the appropriate briefing and actions, in conjunction with other relevant agency heads, depending on the nature and severity of the matter. The EIAT would provide inter-agency coordination and advice to assist the Australian Electoral Commissioner in discharging this obligation. This process would be followed regardless of the nature or source of the foreign interference incident.

The nature and timing of any communication with the public on incidents of foreign interference in Australia's electoral processes and systems would be a matter of discussion between the AEC, other relevant agency heads and the responsible Ministers. Ministers may seek to consult the Opposition on this in accordance with the Caretaker Conventions.

First Interim Recommendation 4: ***The Committee recommends that the Australian Communications and Media Authority's report into the functioning of the Australian Code of Practice on Disinformation and Misinformation be publically released as a matter of priority.***

Response: Supported

On 21 March 2022, the Australian Communications and Media Authority published on its website its *Report to government on the adequacy of digital platforms' disinformation and news quality measures*.

First Interim Recommendation 5: ***The Committee recommends that the Australian Government publically release the Electoral Integrity Assurance Taskforce's terms of reference*****.**

Response: Supported

The purpose of the EIAT is to provide consolidated and coordinated information and advice to the Australian Electoral Commissioner on matters that may compromise the real or perceived integrity of a federal electoral event, which includes elections, by-elections and referendums.

Terms of reference for the EIAT are available on the EIAT webpage (hosted by the AEC).

First Interim Recommendation 6: ***The Committee recommends that the Australian Government establish clear requirements and pathways for social media platforms to report suspected foreign interference, including disinformation and coordinated inauthentic behaviour, and other offensive and harmful content, and formalise agency remits, powers and resourcing arrangements accordingly.***

Response: Support in principle

In the electoral context, EIAT member agencies, including the AEC, have established working relationships with the major social media platforms operating in Australia to enable rapid communication with clear points of contact in the event of suspected foreign interference during a

federal electoral event. It is appropriate that cyber-enabled foreign interference which relates to electoral integrity continues to be reported to the AEC. EIAT member agencies engage with social media companies in the lead up to, and during federal electoral events to enable reporting and response arrangements to be managed efficiently and effectively. In relation to non-electoral contexts, the Government will give further consideration to the co-ordination of reporting by social media platforms of suspected foreign interference and the management of responses.

The eSafety Commissioner has well established relationships with the major social media platforms operating in Australia to respond to harmful online content. The eSafety Commissioner works closely with social media platforms for regulatory activity under the *Online Safety Act 2021 (Cth)* and the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Cth)*. The eSafety Commissioner also engages regularly with the digital industry on policy issues through the eSafety Advisory Committee and ongoing work to progress new industry codes to keep Australians safe from harmful online content.

On 20 January 2023, the Australian Government announced its intent to provide the Australian Communications and Media Authority (ACMA) with new powers to hold digital platforms to account and improve efforts to combat harmful misinformation and disinformation in Australia.

On 25 June 2023, the Government released an Exposure Draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023. The Bill would provide the ACMA with information-gathering and record-keeping powers to provide greater transparency over digital platform activities, and reserve code and standards powers should industry self-regulation prove inadequate.

These proposed powers will bring greater transparency on the efforts by digital platforms to respond to misinformation and disinformation on their services including foreign interference, while balancing freedom of expression which is at the heart of democracy and Australia's way of life.

First Interim Recommendation 7: ***The Committee recommends that the Election Integrity Assurance Taskforce undertake an audit to assess capability relevant to detecting disinformation prior to the coming election and, further, that the Australian Government consider providing information about relevant capabilities and resourcing to this Committee as appropriate to assist in our deliberations.***

Response: Support in part

In relation to the 21 May 2022 Australian federal election, EIAT member agencies exercised their capabilities, as required, to detect and investigate potential instances of election-related foreign-sponsored disinformation. The EIAT will continue to meet through non-election periods to share relevant information and prepare for upcoming electoral events. The EIAT provides a whole-of-government mechanism for collaboration, information sharing and collective action when required. Taskforce member agencies exercise their functions and powers within existing accountabilities to responsible Ministers and within respective legislative frameworks, which include audit, capability review and performance reporting requirements. EIAT member agencies are available to provide a classified briefing on processes, capabilities and resourcing to assist deliberations.