The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Multicultural Affairs
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: GR24-000017

The Hon Milton Dick MP
Speaker of the House of Representatives
Parliament House
CANBERRA ACT 2600

Dear Speaker

I am writing to advise you that the Government provided its response to the Parliamentary Joint Committee on Intelligence and Security's *Advisory Report on the Review of the Cyber Security Legislative Package 2024* during debate in the Senate on 25 November 2024.

I have enclosed the Hansard extract containing the Government response. On page 17 of the Hansard extract, the Government agreed or agreed in principle to all 13 recommendations

Yours sincerely

[redacted]

TONY BURKE

6 / 12 / 2024

Encl. *Hansard extract – Senate – 25 November 2024*

The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Multicultural Affairs
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: GR24-000017

Senator the Hon Sue Lines
President of the Senate
Parliament House
CANBERRA ACT 2600

Dear ~~President~~ Sue

I am writing to advise you that the Government provided its response to the Parliamentary Joint Committee on Intelligence and Security's *Advisory Report on the Review of the Cyber Security Legislative Package 2024* during debate in the Senate on 25 November 2024.

I have enclosed the Hansard extract containing the Government response. On page 17 of the Hansard extract, the Government agreed or agreed in principle to all 13 recommendations.

Yours sincerely

[redacted]

TONY BURKE

6 / 12 / 2024

Encl. *Hansard extract – Senate – 25 November 2024*

1.9 One Nation agrees with this concern. The bill misconstrues human rights as relative, indeed as subordinate to the need of government to suppress opinions they don't like.

That's what you tried to do.

1.10 The Human Rights Law Centre recommended Clause 11(e) should be amended to reflect a broader commitment to human rights in the bill's objectives. It also recommended the Australian Human Rights Commission should be consulted on the development of codes.

'Consultation'—that'd be nice.

1.11 Several submissions related to the specific areas of misinformation. The Australian Medical Professional Society submitted:

By centralising control over what constitutes medical 'truth' in the hands of government regulators, we risk creating an even more Orwellian twist in a system that is already subject to manipulation by powerful interests, to further suppress inconvenient facts and legitimate debate. This would be disastrous not only for free speech and democracy, but for public health as well.

People's lives depend on this. And you wanted to stop it.

1.12 The report failed to address a critical failing in the debate around COVID. Namely that information presented as medical truth at the time has been proven to be wrong—

not only wrong but completely contradicting the truth—

and information banned as misinformation has now been proven to be true.

Repeatedly, repeatedly and repeatedly.

1.13 On the issue of COVID messaging, One Nation has maintained a contrary position to the Government of the day since 2020. This followed expert testimony from multiple specialists, research doctors and whistle blowers which contradicted the official narrative.

1.14 The implication is simple—what is misinformation one day is truth the next. This is the danger in the Government deciding what is and is not misinformation. The bias will always be in favour of the government's 'truth'.

I asked every witness a fundamental question on the last day of the hearing: who is the arbiter of truth? No-one could say who is specified as the arbiter of truth in the bill. They all said that it would default to ACMA. Other provisions in my additional comments included: religious freedom, inauthentic behaviour and media literacy. But the fundamental thing is this was an attempt by the Labor Party to build on the Liberal Party's previous attempts at censorship by corralling misinformation under their definition, and then driving the social media organisations, the big tech companies, to ram it down people's throats. That was what you were doing. I'm pleased to see that the people of Australia have put the brake on you. Now I appeal to the people of Australia to keep a foot on their throat because we must stop the banning of under-16-year-old people from social media.

The ACTING DEPUTY PRESIDENT (Senator O'Sullivan): Senator McKenzie, you have 10 seconds.

Senator McKENZIE (Victoria—Leader of the Nationals in the Senate) (11:34): Ten seconds! How embarrassing it is for the Labor government to have to withdraw the misinformation and disinformation bill on the first day of the last sitting week. You've silenced the Senate this week, and you're trying to silence Australians.

The ACTING DEPUTY PRESIDENT: Thank you, Senator McKenzie. Unfortunately, the time has expired for this debate. The question is that the motion moved by Senator Grogan be agreed to.

Question agreed to.

BILLS

Cyber Security Bill 2024

Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024

First Reading

Bills received from the House of Representatives.

Senator AYRES (New South Wales—Assistant Minister for Trade and Assistant Minister for a Future Made in Australia) (11:35): I move:

That these bills may proceed without formalities, may be taken together and be now read a first time.

Question agreed to.

Bills read a first time.

Second Reading

Senator AYRES (New South Wales—Assistant Minister for Trade and Assistant Minister for a Future Made in Australia) (11:36): I table revised explanatory memoranda relating to the bills, and I move:

That these bills be now read a second time.

I seek leave to have the second reading speeches incorporated in *Hansard*.

Leave granted.

The speeches read as follows—

CYBER SECURITY BILL 2024

This Bill, alongside the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill (ISA Bill) and the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill (ERP Bill), form the Cyber Security Legislative Reforms Package that will collectively strengthen our national cyber defences and build cyber resilience across the Australian economy.

This suite of legislative reforms will implement seven initiatives under the 2023-2030 Australian Cyber Security Strategy, a significant step in achieving the Australian Government's vision of becoming a world leader in cyber security by 2030.

To achieve this goal, we must understand that cyber security is everyone's responsibility.

Our connections online form a significant part of the lives of most Australians—they enhance the way we live, work and play, and as we continue to invest in transformative digital technologies, this will only expand. At the same time, we need to be clear about how we're protecting Australian individuals and businesses. In order to enhance our collective cyber resilience, we need a clear legislative framework that addresses whole-of-economy cyber security issues, and positions us to respond to new and emerging cyber threats.

We need to ensure individuals can trust the products they use every day; we need to enhance our understanding of the threat of ransomware and cyber extortion so we can break the ransomware business model; we need to enhance protections for individuals experiencing a cyber incident to encourage their engagement with government; and we need to learn the lessons from cyber security incidents that have had a significant, detrimental impact on millions of Australians so that we can be better prepared going forward.

The Cyber Security Bill provides this framework, bringing together measures to achieve the Australian Government's vision under one holistic piece of legislation.

The Bill contains four measures:

- The first measure under the Bill will ensure Australians can trust their digital products by enabling the Government to establish mandatory security standards for smart devices. This measure will not only bring us into line with international best practice, but will provide Australians with peace of mind, that the smart devices we have come to rely on also meet our expectations around security.
- The second measure helps to build our understanding of the ransomware threat that continues to cause large-scale harm to the Australian economy and national security. Mandatory reporting of ransomware payments will crystalise the picture of how many businesses in Australia are being extorted into making ransomware payments. With these timely and comprehensive insights the Government will be better able to develop the resources, tools and support that are most useful to industry, and help break the ransomware business model.
- The third measure seeks to support and assure Australian organisations as they respond to a cyber security incident. This measure affirms the role of the National Cyber Security Coordinator to coordinate whole-of-government incident response efforts, and seeks to increase trust and engagement between business and Government during a cyber incident by limiting the circumstances under which the Coordinator can use and share information that has been voluntarily provided by an affected entity. This measure complements the limited use measure put in place for the Australian Signals Directorate through the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill. With these measures, businesses will have greater comfort to report cyber incidents and gain the assistance they need to respond to, and recover from, cyber incidents.
- The fourth measure in the Cyber Security Bill establishes the Cyber Incident Review Board as an independent, advisory body to conduct no-fault, post-incident reviews of significant cyber security incidents in Australia. Reflecting the success of the United States' Cyber Safety Review Board, this new Board will review the circumstances that led to a significant cyber security incident, form findings and provide recommendations for both government and industry to enhance collective cyber resilience.

These four measures form the Cyber Security Bill. Together with the other Bills in this Package, this Bill will equip both Government and industry with the awareness and resilience to better protect Australians from cyber security threats, providing a cohesive legislative toolbox for Australia to move forward with clarity and confidence in the face of an ever-changing cyber security landscape.

On 9 October, the Government referred the package to the Parliamentary Joint Committee on Intelligence and Security. The Committee has now handed down its report and recommended that, subject to implementation of the recommendations in its

report, the Package be passed by the Parliament. The Government agrees or agrees in principle to all thirteen recommendations in the Committee's report.

The Government agrees to recommendations two and three, and will ensure reporting is user friendly, leveraging the existing single reporting portal. The Government will take an education-first approach, informing impacted entities of their new obligations through communications campaigns.

The Government agrees in principle to recommendation four. The Government agrees that ransomware payment reporting obligations will only apply to the extent that the ransomware incident relates to the reporting business entity's operations in Australia. The Cyber Security Bill as drafted gives this effect and this will be clarified in guidance.

The Government agrees to recommendation five and has revised the Explanatory Memorandum. The Explanatory Memorandum as tabled in the Senate gives effect to this intention that Standing Members of the Board will not need to be members of the Australian Public Service. In line with the Committee's report, composition of standing members will be considered further through industry consultation on the rules.

The Government agrees in principle with recommendation six, that the Minister for Cyber Security should consult with the Board before approving the Terms of Reference for each review. Consultation with the Board is built into the legislative framework and the Terms of Reference will be developed by the Board itself, prior to seeking approval from the Minister for Cyber Security.

The Government agrees with recommendation seven of the Committee's report, and has made amendments to the Cyber Security Bill in the House of Representatives to address this recommendation. The Cyber Security Bill, as introduced in the Senate, clarifies that information obtained by the National Cyber Security Coordinator in relation to a cyber security incident, or acquired by a Commonwealth body or State body from a ransomware payment report, is not admissible against the impacted entity in certain criminal or civil proceedings.

Concomitantly, these amendments ensure that information obtained by the Cyber Incident Review Board in the performance of its functions is not admissible in evidence against the entity in certain criminal and civil proceedings. The ISA Bill has also been amended in the House of Representatives to address recommendation seven to further clarify the application of the admissibility protections conferred by the limited use obligation.

Protections afforded to individuals and information under limited use have been further clarified in the Bills, explanatory memorandum and industry guidance, to address recommendation seven.

These actions ensure Government and industry can work together to communicate with clarity and confidence, making our responses more efficient and based on real-time insights. Cooperation on a national scale is one of Australia's greatest advantages against malicious cyber activity.

The Government agrees in principle to recommendation eight. The Government agrees any other right, privilege or immunity that a ransomware payment reporting entity has in respect to any proceedings, including legal professional privilege, will not be impacted. The Cyber Security Bill, as introduced in both chambers, provides this legal effect and the Department will ensure that this is clear to entities affected by the regime.

The Government agrees to recommendation nine, and the Department of Home Affairs will publish additional guidance on the intended interpretation and application of key definitions introduced in the *Security of Critical Infrastructure Act 2018* (SOCI Act). This will be part of the comprehensive guidance being developed on the amendments being made under the ERP Bill to assist regulated entities in understanding their obligations. Consistent with previous reforms to the SOCI Act, the Department will continue to take an education-first approach to compliance, reserving compliance and enforcement action to a last resort.

The Government agrees with recommendation ten of the Committee's report, and has amended the Cyber Security Bill in the House of Representatives. The Cyber Security Bill, as introduced in the Senate, introduces a provision that the Committee may review the operation, effectiveness and implications of the Cyber Security Act as soon as practicable after 1 December 2027.

The Government agrees to recommendation eleven. The Minister for Home Affairs will initiate an independent review under section 60A of the SOCI Act by no later than 1 November 2025.

The Government agrees with recommendation twelve, and has amended the ERP Bill in the House of Representatives to amend section 60B of the SOCI Act to extend the Committee's ability to initiate a review into the operation, effectiveness and implications of the SOCI Act from 3 years to 5 years from Royal Assent of the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act). The Government acknowledges the importance of conducting a holistic review of the SOCI Act, after the amendments being made by the ERP Bill are implemented. Together, the approach to recommendations eleven and twelve will ensure an independent review can fully assess the operation of the SOCI Act in time to inform the Committee's next review.

The Government agrees with recommendation thirteen, and has amended the ERP Bill in the House of Representatives to repeal section 60AAA of the SOCI Act, removing the now redundant six-monthly reporting to the Committee relating to consultation undertaken by the Department on the amendments made by the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* and the SLACI Act. I thank the Parliamentary Joint Committee on Intelligence and Security (Committee) for its work on this Bill through its inquiry and recommendations.

I extend my thanks to staff at the Department of Home Affairs for their incredibly hard work developing this Bill. I commend this Bill to the chamber.