27 October 2024

Submission to the Parliamentary Joint Committee on Intelligence and Security on the Cyber Security Legislative Package 2024

We thank the Parliamentary Joint Committee on Intelligence and Security (the Committee) for the opportunity to submit comments on the Cyber Security Legislative Package 2024.

About Access Now

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence and expertise based in over 20 countries across six continents, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now engages with a global community of individuals from over 162 countries in our annual RightsCon summit series, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We have special consultative status at the United Nations.[1]

Access Now actively engages with authorities across the world, including in Australia, on protecting human rights in the digital age. We have previously submitted comments to this Committee regarding the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA).[2] We provided recommendations on the cyber security infrastructure in Australia in our report "Human Rights in the Digital Era: An International Perspective on Australia" and to the Department of Home Affairs on Australia's 2020 Cyber Security Strategy.[3] We have also been engaging consistently with the Privacy Act reform process, including through our recent submission to the Senate Standing Committee on Legal and Constitutional Affairs.[4]

Access Now advocates for stronger, more effective laws and policies around the world to protect people's personal information online. We have been engaged in the process of negotiating the United Nations Convention on Countering the Use of ICTs for Criminal Purposes.[5] We also recently advocated for human rights-respecting cyber security policies and practices at the United Nations

---

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.
[2] Access Now, *Re: Inquiry on Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, https://www.accessnow.org/wp-content/uploads/2019/02/Sub-53-TOLA-Act.pdf.
[3] Access Now, *Human Rights in the Digital Era: An International Perspective on Australia*, https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf; Access Now, *Submission on Australia's 2020 Cyber Security Strategy*, https://www.accessnow.org/cms/assets/uploads/2019/11/Consultation-Australia-2020-cybersecurity-strategy-1-November-2019-.pdf.
[4] Access Now, *Submission to the Legal and Constitutional Affairs Legislation Committee on the Privacy and Other Legislation Amendment Bill 2024*, https://www.accessnow.org/wp-content/uploads/2024/10/Access-Now-Submission-to-the-Legal-and-Constitutional-Affairs-Committee-on-the-Privacy-Amendment-Bill.pdf.
[5] Access Now, *Intervention during 4th meeting of reconvened concluding session (Day 2 Afternoon)*, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP8/Oral_Statement_-_UN_Ad_Hoc_Committee_on_Cybercrime_Reconvened_Concluding_Session_30_July_2024.pdf; Access Now, *Intervention during 18th meeting of reconvened concluding session (Day 10 afternoon)*,https://www.accessnow.org/wp-content/uploads/2024/08/Oral-Statement-UN-AHC-on-Cybercrime-Reconvened-Concluding-Session-9-August-2024.pdf.

General Assembly First Committee on Disarmament and International Security,[6] and have regularly engaged before the first and second United Nations Open Ended Working Groups (OEWG-I and OEWG-II) on developments in the field of information and telecommunications in the context of international security.[7]

Introduction

We welcome the introduction of the Cyber Security Legislative Package to implement key initiatives under the Australian Cyber Security Strategy 2023-2030 (the ACSS) to build rights-respecting cybersecurity policies and practices. Access Now believes in a principle-based, human rights-centric approach to cybersecurity policy and encourages all policy makers to:

- Put vulnerable individuals and communities at the center of cybersecurity policy;
- Apply systemic solutions to systemic problems such as digital security threats; and
- Use open and pluralistic processes to develop cybersecurity policy.[8]

In our 2018 report *Human Rights in the Digital Era: An International Perspective on Australia*[9] we provided the following key recommendations for the Australian government to undertake in the process of updating its cyber security law:

> 1. Commit to building cybersecurity policies and practices around central tenets of human rights, including the right to privacy. This includes compliance with the government's own Cyber Engagement Strategy commitments on human rights and democracy;
> 2. Evaluate government hacking law and practice with the goal of either ending the practice or, at minimum, codifying statutory safeguards to protect human rights;
> 3. Ensure representatives from civil society and the public are meaningfully included in cybersecurity policy-making, including the ability to participate in drafting key documents; and
> 4. Strengthen data breach notification in Australia to ensure full compliance by the public and private sectors.

At the outset, we respectfully submit that while the present legislative package implements several measures for better coordination, it will fail in its core objective of improving cyber security for the people of Australia - and indeed risks becoming dead on arrival - unless accompanying steps are taken to implement the recommendations of this Committee and others on urgent reforms of

---

[6] Access Now, *2024 Joint civil society statement on cyber and human security*, https://www.accessnow.org/wp-content/uploads/2024/10/UNGA79-1st-Committee-Joint-civil-society-statement-on-cyber-peace-and-human-security-1.pdf.
[7] Access Now, Statements at OEWG-I and OEWG-II, https://www.accessnow.org/tag/oewg/.
[8] Access Now, *Discussion Paper on International Cybersecurity Norms for the UN Open-ended Working Group*,https://www.accessnow.org/to-keep-us-safe-global-cybersecurity-norms-must-be-human-centered-and-protect-rights/.
[9] Access Now, *Human Rights in the Digital Era: An International Perspective on Australia*, https://www.accessnow.org/wp-content/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf.

electronic surveillance powers, particularly amendments to TOLA.[10] The progress sought to be achieved through the present legislative package is undermined by the actual practice and actions of enforcement agencies and persistent threats to encryption and security, which will continue unabated in the absence of legislative changes.[11]

We reiterate the concerns raised in our submission on Australia's 2023-2030 Cyber Security Strategy where we noted that while many of the goals in the strategy are laudable and seek to establish Australia as a regional and global leader on cyber security, it is crucial recognize how the government's own current actions, including engagement in government hacking and threats to encryption under the Assistance and Access Act (TOLA), actually run counter to these objectives.[12]

Comments on the provisions in the legislative package

1) Objects of the Cyber Security Bill

The objects of the Cyber Security Bill are crucial to guide and shape agencies' actions under the law. We believe it is critical to express a commitment to an "open, free, secure and interoperable internet" as mentioned briefly in the ACSS, and was strongly supported in the Cyber Security Strategy 2016, to ensure that the Bill is responsive to the needs of individuals and communities, rather than solely emphasising the role and authority of the government over cybersecurity products, services, and networks.[13] The Cyber Security Strategy 2016 recognised that an open, free and secure internet is in the best interests of people in Australia, as it "is important for ensuring public and financial accountability and strengthening democratic institutions. It underpins freedom of expression and reinforces safe and vibrant communities.

We recommend that an additional object be added to section 3 of the Cyber Security Bill, to promote a free, open, and secure internet, by advancing cyber security practices and policies across the whole of Government, private sector entities, and other stakeholders which ensures secure communications for all individuals.

2) Security standards for smart devices

The Cyber Security Bill provides that mandatory security standards for devices which can connect to the internet will be prescribed through rules. This is an important provision which can implement preventative measures against cyber attacks and risks to personal data but requires

[10] Parliamentary Joint Committee on Intelligence and Security, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Report.
[11] 404 Media, *Encrypted Chat App 'Session' Leaves Australia After Visit From Police*, https://www.404media.co/encrypted-chat-app-session-leaves-australia-after-visit-from-police-2/.
[12] Access Now, *Submission on Australia's 2020 Cyber Security Strategy*, https://www.accessnow.org/cms/assets/uploads/2019/11/Consultation-Australia-2020-cybersecurity-strategy-1-November-2019-.pdf.
[13] Australia's Cyber Security Strategy 2016, https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf.

consultation and safeguards to ensure that the mandatory standards do not provide the government or its agencies with pathways to access people's personal data.
In this regard, we welcome the Minister's statement in the House of Representatives that the standards devised and implemented under this provision will be designed "not to create backdoors for government agencies."[14] This is a crucial requirement for meaningful protections as any mandate for government access bypassing security standards would endanger the security of all users and undermine the purpose of the security standards. Access Now's report "Why encryption is important: 10 facts to counter the myths" explains why it is essential to prohibit any "backdoor" proposal:[15]

> A backdoor to encrypted content is a security flaw that makes the entire system and the underlying data vulnerable. Targeted or exceptional access, as law enforcement agencies demand, would necessitate the creation of a backdoor in some form. Once such a weakness is created, it can be exploited by a host of malicious actors. There is simply no such thing as a backdoor that only the "good guys" have the keys to. As computer scientists and security experts have explained, implementing exceptional access mechanisms means mandating insecurity. Therefore the assertion that a backdoor can be implemented securely is paradoxical. Bolting the front door is of little avail if the backdoor is unlocked – and a single backdoor indiscriminately puts the security of all users of an encrypted system at risk.

We recommend that the Cyber Security Bill include a prohibition on mandatory government access powers as a limitation on the power to set security standards for smart devices.

3) Interaction with the Privacy Act and coordination with the Office of the Australian Information Commissioner (OAIC)

The security standards to be introduced through the rules under the Cyber Security Act will interact with the rules for security, retention, and destruction of personal data under the Privacy Act, 1988. In the Office of the Australian Information Commissioner's (OAIC) submission on the consultation on the ACSS, the OAIC had recommended that "any minimum standard to mandate for consumer-grade IoT devices sold in Australia is carefully designed so that it is interoperable with existing obligations under the Privacy Act and has regard to the reforms in this area."[16]

The recently introduced amendment to the Privacy Act does not implement proposal 21.2 of the Privacy Act Review Report to include "a set of baseline privacy outcomes under APP (Australian Privacy Principles) 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security

---

[14] Tony Burke MP, *Cyber Security Bill 2024 Second Reading Speech*, https://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/28035/0125/hansard_frag.pdf;fileType=application%2Fpdf.
[15] Access Now, *Why encryption is important: 10 facts to counter the myths*, https://www.accessnow.org/why-encryption-is-important/.
[16] Office of the Australian Information Commissioner, *Consultation on 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Submission by the Office of the Australian Information Commissioner*, https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/oaic-submission.PDF.

Strategy." Dissonance between the standards under the Cyber Security law and the Privacy Act will result in uneven application of privacy protections and potential risks to people's personal data.

We recommend that the development of security standards under the Cyber Security law be undertaken in coordination with the Office of the Australian Information Commissioner and with reference to obligations and protections under the Privacy Act.

4) The office of the National Cyber Security Coordinator

The Cyber Security Bill appears to explain the role and functions of the National Cyber Security Coordinator but the creation and full scope of powers of the office are not specified in the Bill. It is not clear as to whether the government can alter the terms of appointment and powers of the Coordinator or whether such an action would require Parliamentary oversight. It is important for cyber coordination across government agencies — including under the Privacy Act, the present legislative package, and intelligence and enforcement laws — to be run by a dedicated point of contact or agency which is separate from the Australian Signals Directorate (ASD) and protected against arbitrary action on their appointment or term.

In our submission on the ACSS, we noted that the security space would be well served by a clearer separation of powers between bodies responsible for signals intelligence, and those responsible for information assurance (the latter being those trusted with cybersecurity). Such a conflation is not a unique challenge to Australia, but it often results in a more stressful, higher stakes environment for the entire agency. A clear definition of critical infrastructure assets from a cybersecurity priority perspective would also facilitate this clarity.

While there is an apparent separation between the ASD and the Coordinator, there appears to be a gap in the legislation, failing to provide certainty as to the independence and terms of the office of the Coordinator. Statutory recognition of independence would fill this gap and would bring clarity for all agencies, entities and individuals regarding their obligations.

We respectfully submit that the terms of appointment and independence of the office of the National Cyber Security Coordinator should be recognised in the legislation and should not be subject to change without Parliamentary oversight and/ or approval.

5) The role of the National Cyber Security Coordinator

In continuation of our recommendation that the office of the Coordinator be statutorily independent, the Coordinator's role, which is sought to be defined in Section 37 (though not exhaustively) should be broadened to go beyond responsibility to the government, to ensuring responsibility of the government, for the people. In our submission on the ACSS, we noted that a healthy cybersecurity framework should seek to create a well resourced government office to make sure that individuals and industry have continuous access to an accessible, trusted and well integrated government entity, focused on information assurance as a part of a diverse digital security ecosystem, an entity which can support them in time of their need and at their own

behest.

We recommend that the role of the National Cyber Security Coordinator be expanded to include upholding the objects and spirit of the Cyber Security Act and ensuring that entities across the government respect and accept them.

6) Vulnerability disclosure processes

The cyber security legislative package must create a supportive framework for vulnerability disclosures and encourage the growth of the vulnerability reporting ecosystem. In our submission on the ACSS, we pointed out that vulnerabilities in ICT systems are common and will always exist; the important thing is how we respond when we discover them. Several large-scale attacks over the past few years were conducted by leveraging vulnerabilities that governments already knew about but kept secret, to stockpile for use against strategic targets. Attacks can be prevented but only if governments make a stronger commitment to a vulnerability disclosure process that appropriately prioritises defence of digital security, vital systems, and infrastructure.

At Access Now, we advocate for governments to adopt a vulnerability disclosure process for when they find or become aware of technology flaws, and for governments to facilitate coordinated vulnerability disclosure (CVD) for industry.[17] The latter approach is systemic, responding to the issues that create a less secure environment for everyone. It includes making changes that support disclosure and patching of vulnerabilities, such as avoiding criminalising security research and instead giving leeway to prosecutors in related cases or other forms of legal certainty.

The present cyber security legislative package is silent as to creation of a vulnerability disclosure process. The Australian government should implement a vulnerabilities equities process for its own operations as well as mandating a vulnerability reporting policy for government provided services and its own institutions. The latter should be supported by clear language protecting the rights of security researchers (as opposed to treating them as a malicious actor), tempered with a clear delineation of the reporting process and responsibilities. In order to achieve its cybersecurity objectives, we further recommend that the government promote and support the development of coordinated vulnerability policies for all entities operating in its jurisdictions, making sure that it promotes and protects a culture of cybersecurity research and community cooperation.[18]

We recommend that the law include clear vulnerabilities disclosure processes, with protections for security researchers, and enable development of Coordinated Vulnerability Policies.

---

[17] Access Now, *The EU needs to get serious about fixing vulnerabilities*, https://www.accessnow.org/the-eu-needs-to-get-serious-about-fixing-vulnerabilities/.
[18] We may note in this regard that we support the submission by HackerOne to this Committee in the present inquiry, suggesting the adoption of vulnerability disclosure programs and coordinated vulnerability policies.

7) Systemic insecurities caused by conflicting laws and practices

As mentioned at the outset, the present legislative package will be ineffective to deal with the underlying threats to privacy and security caused by the Government's own practices regarding data access, sharing, and gathering. The system insecurity caused by these existing legal instruments and practices is in addition to the cost that such instruments and programs bear on the reputation and trust of Australian cybersecurity services and products abroad.

We recommend a full audit of existing legal instruments and programs which may be perpetuating a systemic insecurity to the Australian digital environment.

8) Guidance on the interaction between the SOCI Act and the Privacy Act

The Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (SOCI) proposes to allow the Minister to direct sharing of personal information in certain situations, with authorisation from the Minister administering the Privacy Act 1988.

We recommend that the Office of the Australian Information Commissioner be involved in preparing guidance on the interaction between the SOCI Act and the Privacy Act, including on any and all directions seeking disclosure of personal information.

9) Transparency of information-gathering directions and individual rights

Ministerial authorisations under the SOCI Act will have significant consequences for the individuals impacted by a serious incident, or who may be affected by a serious incident in the future, including with respect to disclosure of their personal information. The government should be required to make a statement as to the exercise of these powers which goes beyond acknowledging that they have been exercised, to the impact of such directions on people's privacy and other rights.

We recommend including a requirement for the Minister to disclose not only the number of authorisations in the periodic reports under Section 60 of the SOCI Act, but a full report of such authorisations including their impact on people's personal information and provisions of the Privacy Act.

Where people's personal information is involved, they should also have a dedicated right to remedy or redressal with the authority collecting such information. For example, the United States's Cybersecurity and Infrastructure Security Agency (CISA) maintains a dedicated Office of Privacy with a clear mandate to ensure compliance with privacy policies within CISA.[19] The Office provides guidance for individuals to be able to submit a redressal request with respect to their personal information.

[19] Cybersecurity and Infrastructure Security Agency Office of Privacy, https://www.cisa.gov/cisa-office-privacy.

We recommend that people have a clear, accessible remedy in case of violations of their privacy or harms arising from the disclosure of personal information under the SOCI Act.

10) Cyber Incident Review Board

We welcome the introduction of the Cyber Incident Review Board to examine specific cyber incidents for the purpose of providing constructive recommendations to the government and to private entities to strengthen cyber security practices. In keeping with the purpose of the Board, we make the following recommendations to improve the Board's ability to work for all people in a transparent manner and increase trust in its reviews and findings.

We recommend that the rules for a review under Section 46(5)(g) enable individuals or communities impacted by a cyber incident to provide information or submissions to the Board to assist with an ongoing review.

We recommend that when the Minister does not approve the terms of reference for review under Section 46(2)(c), such disapproval should be in writing with reasons for the decision, and this should also be reflected in the Minister's annual report at the least, if not made public at the time of the disapproval.

11) Ransomware reporting

We welcome increased sharing of information around cybersecurity incidents and ransomware payments. We urge that in addressing ransomware, the legal framework created by the Cyber Security Package includes impacted individuals and communities within its area of focus. Additionally, given the overlap between ransomware activity and the threat to protecting personal data, the framework should include coordination with the OAIC and its role under the Privacy Act.

We recommend that in the "ransomware payment report" to be made under Section 27, entities be required to report whether there is a risk of disclosure, breach, or loss of personal information, and if so, what potential action can be taken to prevent such occurrence and what remedies are available for impacted persons.

We further recommend that the provision clearly indicate whether such reports, made to the "designated Commonwealth body", will also be shared with the Office of the Australian Information Commissioner (OAIC) and to what extent the OAIC will be involved in the safeguarding of people's personal information to streamline implementation of relevant provisions in the Privacy Act.

Conclusion

Thank you for the opportunity to participate in this consultation in the Cyber Security Legislative package inquiry process. We remain available for any clarification or queries in relation to this feedback, and hope to be of further assistance in this important process.

Yours sincerely,

Shruti Narayan
Asia Pacific Policy Counsel
shruti@accessnow.org

Namrata Maheshwari
Senior Policy Counsel and Encryption Policy Lead
namrata@accessnow.org

Raman Jit Singh Chima
Global Cybersecurity Lead | Senior International Counsel and Asia Pacific Policy Director
raman@accessnow.org

Access Now | https://www.accessnow.org