Australian Government

Australian Government response to
Chapters 2 and 3 of the Parliamentary Joint Committee on Intelligence and Security's
Report of the inquiry into potential reforms of Australia's national security legislation

Recommendation	Government response

Recommendation 1
 	
The Committee recommends the inclusion of an objectives clause within the *Telecommunications (Interception and Access) Act 1979*, which:
 	
• expresses the dual objectives of the legislation –
  o to protect the privacy of communications;
  o to enable interception and access to communications in order to investigate serious crime and threats to national security; and
 	
• accords with the privacy principles contained in the *Privacy Act 1988*.
	Supported
	
	The Government will work with stakeholders to develop an appropriate clause, noting that the existing privacy protections in the Act extend beyond those contained in the *Privacy Act 1988*.

Recommendation 2 The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Factors to be considered in the proportionality tests include the: • privacy impacts of proposed investigative activity; • public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and • availability and effectiveness of less privacy intrusive investigative techniques.	**Supported** The Attorney-General's Department will examine the proportionality tests within the Act, as amended by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act), as recommended. The question of what proportionality test should apply when agencies seek lawful access to communications is closely linked to matters raised in other recommendations made by the Committee, which the Government also supports, being that: • the Attorney-General's Department examine the standardisation of thresholds for access to the content of live and stored communications

Recommendation	Government response
The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.	(Recommendation 6) • interception be conducted on the basis of specified attributes of communications (Recommendation 7) • interception warrant provisions be revised to develop a single interception warrant regime (Recommendation 10) • the Attorney-General's Department review whether the agencies that may access the content of communications should be standardised, and that the Attorney-General report to the Parliament by 13 April 2017 on the findings of this review (Recommendation 19 of the Committee's *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Advisory Report)), and • the Government review the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* (Recommendation 4 of the Committee's *Advisory Report on the National Security Legislation Amendment Bill (No. 1) 2014*). Given the close interrelationships between these recommendations, it is appropriate that the Government's examination, review and development of detailed responses to these recommendations be progressed in a coordinated fashion. As such, the Government intends to finalise its detailed response to these recommendations

Recommendation	Government response
	following the delivery of the report of the review of access to the content of communications, by no later than 13 April 2017.
Recommendation 3 The Committee recommends that the Attorney-General's Department examine the *Telecommunications (Interception and Access) Act 1979* with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.	**Supported** The Government will continue to examine the reporting requirements contained in the Act, with a view to revising the requirements in the manner recommended by the Committee. The Data Retention Act will substantially enhance the reporting requirements relating to stored communications and telecommunications data, including enhancements recommended by the Committee in its Advisory Report.
Recommendation 4 The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the *Telecommunications (Interception and Access) Act 1979*. Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism. The Committee also recommends the Attorney-General's Department consult with State and Territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.	**Supported** The Attorney-General's Department will review the oversight arrangements for law enforcement agencies under the Act, and will consult with jurisdictions in relation to the appropriate allocation of oversight responsibility for State and Territory agencies. The Data Retention Act will substantially enhance the powers of the Commonwealth Ombudsman to oversight access to stored communications and telecommunications data. Additionally, as recommended by the Committee in its Advisory Report, the Data Retention Act will enable the Committee to inquire, for the first time, into the operational activities of the Australian Security Intelligence Organisation (ASIO) and Australian Federal Police, as they relate to access to retained telecommunications data. ASIO is already subject to oversight across all of its functions and activities by the independent Inspector-General for

Recommendation	Government response
	Intelligence and Security. The Government will also consider the nature and scope of the oversight arrangements as an integral part of each element of the reform process, to ensure that oversight arrangements remain appropriate and adapted to agencies' powers and activities.
Recommendation 5 The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.	**Implemented** The Government has responded to the Committee's recommendation that my Department review the threshold for access to telecommunications data as part of the Data Retention Act, which reduced the number of enforcement agencies able to access telecommunications data, and which strengthened the proportionality test for access to telecommunications data by such agencies.
Recommendation 6 The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the: • privacy impact of the threshold; • proportionality of the investigative need and the privacy intrusion; • gravity of the conduct to be investigated by these investigative means; • scope of the offences included and excluded by a particular threshold; and • impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.	**Supported** The Attorney-General's Department will examine the standardisation of thresholds for accessing the content of communications. As noted above, this recommendation is closely related to recommendations 2, 7 and 10 of the Committee's Report, and recommendation 19 of the Committee's Advisory Report. As such, the Government intends to finalise its detailed response to these recommendations following the delivery of the report of the review of access to the content of communications, by 13 April 2017.

Recommendation	Government response
Recommendation 7 The Committee recommends that interception be conducted on the basis of specific attributes of communications. The Committee further recommends that the Government model 'attribute based interception' on the existing named person interception warrants, which includes: • the ability for the issuing authority to set parameters around the variation of attributes for interception; • the ability for interception agencies to vary the attributes for interception; and • reporting on the attributes added for interception by an authorised officer within an interception agency. In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures: • attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated; • oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and • reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.	**Supported** The Government will consider developing an attribute-based interception regime in consultation with key stakeholders, including members of the telecommunications industry. The Government will also work to develop appropriate safeguards, and oversight and accountability measures. The Government notes that careful consideration will need to be given to aspects of this recommendation, in particular: • reporting on the attributes added for interception will need to balance the interests of transparency and accountability with operational security and the protection of sensitive investigative capabilities and methodologies • the nature of the oversight of attribute based interception by the ombudsmen, for law enforcement agencies, and Inspector-General of Intelligence and Security, for ASIO, will be contingent on the outcome of the Attorney-General's Department's review of oversight arrangements, as recommended by the Committee (Recommendation 4) • reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute-based interception • whether including a specific proportionality test for ASIO warrants would result in duplicative or inconsistent requirements to the proportionality requirements set out in the Attorney-General's Guidelines, which apply across all of ASIO's functions and activities, and

Recommendation	Government response
	• any additional regulatory impact upon the telecommunications industry. As noted above, this recommendation is closely related to recommendations 2, 6 and 10 of the Committee's 2013 Report, and recommendation 19 of the Committee's Advisory Report. As such, the Government intends to finalise its detailed response to these recommendations following the delivery of the report of the review of access to the content of communications, by 13 April 2017.
Recommendation 8 The Committee recommends that the Attorney-General's Department review the information sharing provisions of the *Telecommunications (Interception and Access) Act 1979* to ensure: • protection of the security and privacy of intercepted information; and • sharing of information where necessary to facilitate investigation of serious crime or threats to national security.	**Supported in part** The Attorney-General's Department will review the information sharing provisions of the Act Given the covert and intrusive nature of the powers under the Act, it is appropriate that there be strict limits on the circumstances in which agencies may share information lawfully obtained using those powers. However, the complex and prescriptive nature of the existing information sharing framework represents a significant barrier to the effective use of lawfully obtained information within agencies, and to meaningful cooperation between agencies. Accordingly, the Government intends to develop a simplified regime that appropriately protects the privacy and security of lawfully accessed information, while facilitating the effective use and sharing of such information for legitimate law enforcement and national security purposes. However, the Government does not support limiting the sharing of information to circumstances involving only 'serious crime' or 'serious threats to national security'. At

Recommendation	Government response
	present, the Act appropriately places more stringent restrictions on access to, and the use and disclosure of more sensitive information, such as the content of intercepted communications. Comparatively, access to, and the use and disclosure of less sensitive information, such as subscriber records, is permitted at a lesser threshold. The Government considers this arrangement should continue to apply. Additionally, limiting the ability of law enforcement agencies to use and disclose information to circumstances involving 'serious crime' would remove the existing ability to use less sensitive information in enforcement-related proceedings, such as actions for proceeds of crime, or to enforce civil penalty provisions for corporate wrongdoing. Such an amendment may also be inconsistent with the Committee's recommendation, in its Advisory Report, that corporate regulators be granted the power to access both the content of stored communications and telecommunications data to empower them to investigate serious contraventions of the law.
Recommendation 9 The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to remove legislative duplication.	**Supported** The Government will amend the Act to remove legislative duplication, consistent with the Government's Clearer Commonwealth Law's initiative.
Recommendation 10 The Committee recommends that the telecommunications interception warrant provisions in the *Telecommunications (Interception and Access) Act 1979* be revised to develop a single interception warrant regime. The Committee recommends the single warrant regime include the following	**Supported** The Government will consider legislative amendments to revise the interception and stored communications warrant provisions to develop 'single warrant regimes' for law enforcement agencies and ASIO. The Government notes that careful consideration will need to be given to whether including a specific proportionality

Recommendation	Government response
features: • a single threshold for law enforcement agencies to access communications based on serious criminal offences; • removal of the concept of stored communications to provide uniform protection to the content of communications; and • maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises. The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures: • interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated; • rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security; • reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and • Parliamentary oversight of the use of interception.	test for ASIO warrants would result in duplicative or inconsistent requirements to the proportionality requirements set out in the Attorney-General's Guidelines, which apply across all of ASIO's functions and activities. As noted above, this recommendation is closely related to recommendations 2, 6 and 7 of the Committee's 2013 Report, and recommendation 19 of the Committee's Advisory Report. As such, the Government intends to finalise its detailed response to these recommendations following the delivery of the report of the review of access to the content of communications, by 13 April 2017.
Recommendation 11 The Committee recommends that the Government review the application of the interception-related industry assistance obligations contained in the *Telecommunications (Interception and Access) Act 1979* and *Telecommunications Act 1997*.	**Supported** The Government will review the interception-related industry assistance obligations contained in the Act, in consultation with agencies and members of the telecommunications industry. The review will include careful consideration of the need to minimise the regulatory burden on the telecommunications industry, and will be

Recommendation	Government response
	closely linked to the development of detailed responses to the Committee's recommendations relating to: • the introduction of an attribute-based interception regime (Recommendation 7) • the expansion of the regulatory enforcement options available to the Australian Communications and Media Authority (Recommendation 12) • amending the Act to include provisions which clearly express the scope of industry's obligations to provide assistance to law enforcement and national security agencies (Recommendation 13) • amending the Act to clarify that the existing industry assistance obligations apply to all providers of telecommunications services accessed within Australia (including ancillary service providers), on a no-profit, no-loss basis (Recommendation 14) • the development of an appropriate framework to preserve lawful access to the content of encrypted communications under warrant as a part of investigations into serious criminal activity and threats to national security, which does not compromise the security of communications for ordinary Australians (Recommendation 16), and • whether to develop statutory timelines for industry assistance to law enforcement and national security agencies (Recommendation 17).

Recommendation	Government response
Recommendation 12 The Committee recommends the Government consider expanding the regulatory enforcement options available to the Australian Communications and Media Authority to include a range of enforcement mechanisms in order to provide tools proportionate to the conduct being regulated.	**Supported** The Government will consider enforcement options available to ACMA, including lower-order options, as well as options designed to facilitate negotiated solutions to alleged non-compliance. As noted above, this recommendation is closely linked to recommendations 7, 13, 14, 16 and 17.
Recommendation 13 The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to include provisions which clearly express the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.	**Supported** The Government will consider amendments to more clearly express the scope of the industry assistance obligations, mindful of the merits of laws that can be applied flexibly, particularly in response to changing technology. As noted above, this recommendation is closely linked to recommendations 7, 12, 14, 16 and 17.
Recommendation 14 The Committee recommends that the *Telecommunications (Interception and Access Act) 1979* and the *Telecommunications Act 1997* be amended to make it clear beyond doubt that the existing obligations of the telecommunications interception regime apply to all providers (including ancillary service providers) of telecommunications services accessed within Australia. As with the existing cost sharing arrangements, this should be done on a no-profit and no-loss basis for ancillary service providers.	**Supported in principle** The Government strongly supports the principle that all companies operating in or supplying services to Australia should be subject to and comply with Australian law. However, the Government acknowledges that designing an appropriate regulatory framework for a globalised industry, such as the telecommunications industry, while minimising the regulatory burden raises complex issues. Accordingly, the Government will consider appropriate amendments to place beyond doubt the scope of the industry assistance obligations. As noted above, this recommendation is closely linked to recommendations 7, 12, 13, 16 and 17.
Recommendation 15 The Committee recommends that the Government should develop the	**Supported in part** The Government supports the application of obligations across the industry, to minimise

Recommendation	Government response
implementation model on the basis of a uniformity of obligations while acknowledging that the creation of exemptions on the basis of practicability and affordability may be justifiable in particular cases. However, in all such cases the burden should lie on the industry participants to demonstrate why they should receive these exemptions.	national security and law enforcement risks associated with unregulated industry participants, and to ensure a more even playing field in an increasingly converged communications environment. However, given the fragmentation and diversification of the modern telecommunications industry, the Government considers that it may be appropriate to tailor, to some degree, the nature of the obligations imposed on distinct classes of providers, while minimising any increase in regulatory complexity. This would allow industry assistance obligations to better reflect the increasing diversity of the telecommunications industry, and would allow Government to minimise the regulatory burden associated with these social licence obligations by avoiding imposing unnecessary or inapt obligations on particular classes of providers.
Recommendation 16 The Committee recommends that, should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations.	**Supported** The Australian Government supports strong encryption, which underpins modern, secure communications technologies. These technologies are fundamental to a digital economy, and provide an unparalleled opportunity for exercise of the fundamental freedoms of expression, peaceful assembly and association. However, the use of encrypted communications for serious criminal purposes and purposes prejudicial to security represents an increasingly significant barrier to the ability of governments to bring serious offenders to justice. Accordingly, the Government will explore, in consultation with agencies and the telecommunications industry, the development of appropriate legislative

Recommendation	Government response
	provisions, including safeguards, oversight and accountability measures.
Recommendation 17 The Committee recommends that, if the Government decides to develop timelines for telecommunications industry assistance for law enforcement and national security agencies, the timelines should be developed in consultation with the investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. The Committee further recommends that, if the Government decides to develop mandatory timelines, the cost to the telecommunications industry must be considered.	**Supported** The Government recognises the potential regulatory burden of introducing industry assistance timelines and will consult with relevant agencies and the telecommunications industry about any proposal to develop timelines for the provision of industry assistance to law enforcement and national security agencies.
Recommendation 18 The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following: • clear protection for the privacy of communications; • provisions which are technology neutral; • maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes; • clearly articulated and enforceable industry obligations; and • robust oversight and accountability which supports administrative efficiency.	**Supported** The Government will comprehensively revise the Act in a progressive manner, rather than as a single legislative package. An iterative approach will allow the Government to make substantial and practical improvements to the telecommunications privacy and access framework sooner than would otherwise be possible. This approach will also allow the Committee, to which all substantive packages of amendments will be referred, Parliament, industry, and Australian public to consider each stage of this reform process in greater detail.

Recommendation	Government response
The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies. The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the: • Independent National Security Legislation Monitor; • Australian Information Commissioner; • ombudsmen and the Inspector-General of Intelligence and Security. In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.	
Recommendation 19 The Committee recommends that the Government amend the *Telecommunications Act 1997* to create a telecommunications security framework that will provide: • a telecommunications industry-wide obligation to protect infrastructure and the information held on it or passing across it from unauthorised interference; • a requirement for industry to provide the Government with information to assist in the assessment of national security risks to telecommunications infrastructure; and • powers of direction and a penalty regime to encourage compliance. • The Committee further recommends that the Government, through a	**Supported** The Government will introduce legislation giving effect to Recommendation 19 this year, following the release of an exposure draft of the legislation for public consultation. The Attorney-General will refer that legislation and associated Regulation Impact Statement to the Committee for public inquiry and report.

Recommendation	Government response

Regulation Impact Statement, address:
• the interaction of the proposed regime with existing legal obligations imposed upon corporations;
• the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
• consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and
• impacts on competition in the market-place, including:
  ○ the potential for proposed requirements to create a barrier to entry for lower cost providers;
  ○ the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and
  ○ any other relevant effects.	