Australian Government

Department of Home Affairs

The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Parliamentary Joint Committee on Intelligence and Security

Table of Contents

Introduction

1. The Department of Home Affairs (the Department) welcomes the opportunity to inform the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) Inquiry into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act). This submission focuses on the purpose and outcome of the 167 Government amendments that were moved in the House of Representatives on 6 December 2018 and passed with the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill) that same day. The Government amendments reflect the Department's ongoing engagement with industry, peak bodies and oversight bodies following introduction of the the Bill, and scrutiny from Parliamentary committees, including the PJCIS, which tabled a report on the Bill on 5 December 2018.
2. Following a three-stage consultation process in which both industry and the public were given an opportunity to comment on the draft legislation, the Bill was introduced into the House of Representatives on 20 September 2018 and referred to the PJCIS by the Attorney-General for inquiry and report. The PJCIS review was extensive and involved public and private hearings with industry, peak bodies, advocacy groups and law enforcement and national security agencies including the Australian Federal Police (AFP), the Australian Security Intelligence Organisation (ASIO), the Australian Criminal Intelligence Commission (ACIC) and the Australian Signals Directorate (ASD). Based on this evidence and submissions from these stakeholders, the PJCIS made seventeen recommendations which were accepted by the Government.
3. To give effect to these recommendations and to otherwise enhance the safeguards in the legislation, the Government amended the Bill to increase transparency, and strengthen the existing accountability and oversight measures. Important limitations were augmented to ensure the security of devices and networks are maintained, and that the powers in the Act are only used when required to facilitate our law enforcement and national security agencies' legitimate and lawful operations. The Bill was also amended to establish multiple avenues for independent review of the legislation.
4. The Government made further amendments to the Bill which were minor and technical in nature and were intended clarify the function and operation of key measures. These amendments were based on the outcome of scrutiny on the Bill from other Parliamentary committees including the Senate Standing Committee for the Scrutiny of Bills and Parliamentary Joint Committee on Human Rights. The additional amendments also reflect ongoing engagement with key industry stakeholders, peak bodies and oversight bodies, including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security (IGIS), and address many of their concerns raised during the PJCIS review.
5. The Department continues to work closely with law enforcement and national security agencies and industry to facilitate the implementation of the Act. This will support the key measures in the Act, including the industry assistance measures in Schedule 1, so that they are being used consistently and appropriately. The Department has also been advised by Commonwealth law enforcement and national security agencies that the powers in the Act have been used to support their work.

Government amendments

Amendments to reflect the PJCIS recommendations

6. On 5 December 2018, the PJCIS tabled its report on the Bill which included seventeen recommendations. The Government expressed support for the PJCIS recommendations and moved amendments to the Bill in the House on 6 December 2018 which passed both chambers of Parliament that same day. Broadly speaking, the amendments further ensure the Act strikes an appropriate balance between maintaining privacy and the integrity of networks and devices, and ensuring that agencies can continue to protect the Australian community. The amended Bill also significantly strengthened the safeguards attached to the new industry assistance regime, introduced additional layers of oversight by the Commonwealth Ombudsman and IGIS, and established multiple avenues for review of the legislation.
7. See **Attachment A** for further analyses of the amendments made to the Bill to implement the PJCIS recommendations.
8. The Government amendments to the Bill in respect to the PJCIS recommendations include:
    - For law enforcement purposes, limiting the issuing of technical assistance requests (TARs), technical assistance notices (TANs) and technical capability notices (TCNs) to offences with a penalty of a minimum period of three year's imprisonment or more. This limits the issuance of an industry assistance notice to the investigation and prosecution of serious crimes such as terrorism and serious child sex offences.
    - To provide for additional oversight of the industry assistance powers, the Department has added new disclosure exemptions for State and Territory inspecting authorities to the non-disclosure provisions in Schedule 1. Amendments that add subsections 317ZF(5A)-(5C) allow TAR and TAN information to be disclosed by an Ombudsman official to an employee of a State or Territory inspecting authority for the purposes of exercising their inspection function. Similarly, amendments to add subsections 317ZF(12A)-(12D) allow a provider, their employees, their contractors, their contractors' employees or the Communications Access Co-ordinator to disclose TAR, TAN or TCN information to an employee of a State or Territory inspecting authority for the purpose of exercising their inspection function. Additionally, "State or Territory inspecting authority" is now defined in section 317B to clarify which State and Territory oversight bodies are empowered under the Act.
    - A maximum 12 month time-limit has been imposed on TANs and TCNs. The issuing agency is required to seek further approval for the extension of a notice or for a new notice to be issued if the time-limit for the original notice lapses.
    - Given the potential significance of new capabilities developed, both the Attorney-General and the Minister for Communications are required to approve the issuance of a TCN. The involvement of the Minister for Communications also provides another safeguard.
    - Introducing a definition for 'systemic weakness' and 'systemic vulnerability' to clarify and prohibit those proposed requirements in a request or notice which will lead to unlawful and systemic intrusions into devices and networks. This enhances the operation of existing safeguards that prevents the creation and implementation of 'backdoors.'
    - Requiring decision-makers to consider necessity and intrusiveness, in addition to other factors such as the impact on industry, cyber security and privacy, before utilising the powers.

- The PJCIS is legislated to review the Act in conjunction with its April 2019 review of the Data Retention regime. Further, the Independent National Security Legislation Monitor (INSLM) is legislated to review the Act within 18 months of commencement. The purpose of this review is to allow INSLM to consider the operation, effectiveness and implications of the Act in terms of terrorism or national security threats.
- In response to recommendation 12, the Department, in consultation with the Attorney-General's Department, continues to monitor the resourcing of the Commonwealth Ombudsman and IGIS with regards to their powers under the Act.
- Broadening the scope of sections 317ZG and 317ZH to include TARs. This ensures providers do not introduce a systemic weakness or vulnerability into their networks or devices.

9. Other amendments made to reflect the Government's support of PJCIS recommendations are highlighted in more detail below.

Strengthening the role of oversight bodies

10. In response to recommendation 5, and following engagement with oversight bodies, the Government amended the Bill to broaden and enhance the role of existing oversight bodies (including the Commonwealth Ombudsman and the IGIS , and State and Territory bodies) to inspect and scrutinise the use of key powers in the Act. The resulting amendments ensure the oversight powers in the Act are effective and proportionate.
11. Broadly speaking, the amendments strengthen existing powers that authorise oversight bodies to examine the legality and propriety of the operation of the Act. In particular, the amendments enhance the ability of oversight bodies to inspect and gather information on the exercise of the industry assistance measures by the AFP, ASIO, the ACIC, and State and Territory interception agencies. This will ensure that these powers are used appropriately and as intended.
12. Further to recommendation 5 of the PJCIS report, and recommendations made by oversight bodies to both the PJCIS and the Department, the amendments to strengthen oversight in the Act include:
    - establishing clear channels for information exchange between oversight bodies to ensure the necessary information is available for assessing agency compliance with the legislation.
    - authorising disclosure of relevant information on an industry assistance measure to an oversight body which is necessary for the purpose of exercising powers, or performing functions or duties relevant to that oversight body.
    - augmenting existing reporting regimes to allow the Commonwealth Ombudsman to further scrutinise the use of industry assistance measures in conjunction with underlying interception and surveillance powers.
    - inclusion of requirements for ASIO to complete annual reports on the use of industry assistance powers which will be scrutinised by the Government and Parliament.
    - express notification requirements to ensure the IGIS and the Commonwealth Ombudsman are notified of the issuing, variation, extension and revocation of all industry assistance measures.
    - requiring providers to be notified of their right to make a complaint to the appropriate oversight body in relation to an industry assistance measure.
    - strengthening the prohibitions against 'systemic weakness' and protecting information to ensure the integrity of data, devices and networks are maintained. This extends to both voluntary and compulsory industry assistance measures (examined in greater detail below).

- limiting the decision-making criteria for issuing a compulsory industry assistance by requiring the decision-maker to consider the necessity of the notice. This ensures that decision-makers have regard to whether a technical assistance notice or technical capability notice is necessary for achieving legitimate beneficial outcomes for law enforcement and national security.
- requiring decision-makers to consider if the requirements under a compulsory industry assistance notice is the least intrusive known form of industry assistance when compared to other forms of industry assistance in relation to the impact on the privacy of innocent third parties.
- clarifying the application of the public interest exception in section 317ZK.
- requiring the Director-General of Security to report on concealment of access activities undertaken in the prescribed post-cessation period of an ASIO computer access warrant.
- limiting concealment activities in relation to ASIO computer warrants to prohibit the material interference, loss or damage to lawful computer users.
- requiring the Director-General of Security to notify the IGIS as soon as practicable that a voluntary assistance request under section 21A has been made.
- establishing broad reporting requirements that ensures assistance requests under section 34AAA are issued by the Attorney-General after considering previous requests made in relation to the relevant person, and the outcome of the requests.
- increasing transparency and oversight of the use of assistance requests under section 34AAA to facilitate Parliamentary scrutiny of these powers.

AFP Commissioner as a central coordinator and reviewer

13. In response to recommendation 7, the Government introduced section 317LA which requires TANs issued by State and Territory law enforcement to be subject to the approval of the Commissioner of the AFP. This amendment is currently in operation and administrative guidance has been developed (and continues to be refined) to centralise and streamline this process.
14. The Committee also recommended for the Bill to be amended to require the Commissioner, when approving a TAN, to "apply the same statutory criteria, and go through the same decision making process, as would apply if the AFP were the original issuing authority." Section 317LA provides scope for the AFP Commissioner to consider those matters they consider relevant when approving the issuing of a TAN.
15. The Department acknowledges the importance of centralising the issuing of TANs to maintain consistency, avoid duplication and enable the exchange of information across jurisdictions. However, in consultation with the AFP and State and Territory police, the Department has become aware of serious concerns relating to the sovereignty of co-equal policing agencies and questions relating to the proprietary of imposing federal control over an area of law administered by State and Territory authorities. This raises serious concerns for the AFP and State and Territory agencies, including:
    - requirements to share sensitive information across jurisdictions outside of joint operations
    - allowing the Commonwealth to 'second-guess' operational matters and decisions made by a police force in an independent jurisdiction relating to criminal matters which would overwhelming be tied to investigative imperatives and priorities within that jurisdiction
    - requiring the AFP to have intricate knowledge of State and Territory operations and expertise, and

- uncertainty about the nature and detail of information about ongoing operations and warrants that would need to be exchanged between jurisdictions to facilitate approval.

16. A potential effect of these amendments will be to reduce the effectiveness of the powers for State and Territory police (or even the willingness to use the powers) duplicate existing requirements and create an undue resource and process burden for both the AFP and State and Territory police forces. The amendment may also have the potential impact of causing structural conflict between co-equal policing agencies within the Australian federal framework.
17. Unlike other Commonwealth powers which States and Territory police are able to utilise, the industry assistance framework is not tied to offences in the federal jurisdiction. For example, under the *Surveillance Devices Act 2004,* State and Territory police can apply for surveillance devices to investigate federal offences punishable by three years imprisonment or more. Other regimes under the *Crimes Act 1914* allow for the use of powers tied to the investigation of federal offences or State offences with a federal aspect. In contrast, the industry assistance framework is designed to support the use of existing interception powers and other lawful means of accessing content and non-content data, including where the relevant warrant or authorisation has been executed to investigate a purely State-based criminal matter. For example, section 5D of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) contains a suite of State and Territory offences. State and Territory agencies (the same agencies empowered under new Part 15) may independently apply for privacy-intrusive interception and stored communications warrants to investigate these offences. Similarly, the disclosure of telecommunications data made be independently authorised by these same agencies for the enforcement of the criminal law, including State and Territory criminal law.
18. Existing industry assistance provisions in section 313 of the *Telecommunications Act 1997* (another Commonwealth administered power) does not establish an equivalent requirement for the AFP Commissioner or similar authority to review or authorise State and Territory police seeking technical help from carriers and carriage service providers. Maintaining a requirement to second-guess the operational merits of industry assistance that relate to purely state and territory-based investigations is significantly out of step with the distinctions between the federal, State and Territory policing authority.
19. Given the concerns expressed by federal, State and Territory police forces about the operation of this amendment, the Department queries whether section 317LA should be clarified to reinforce the coordination role of the AFP Commissioner. Existing Commonwealth bodies like the Communications Access Coordinator in the Department of Home Affairs perform a centralisation function with regard to lawful access to communications and the AFP Commissioner is well-place to perform centralisation role focused on matters like:
    - maintaining preferred points of contact between agencies and providers
    - reducing duplicate requests
    - enabling the exchange of relevant information across jurisdictions
    - advising on the types and forms of assistance commonly requested
    - establishing processes with providers and agencies for the efficient and effective delivery of notices, and
    - ensuring consistency in application, payment and cost recovery.

Added explicit pathway for facilitating warrants to *listed acts or things*

20. In response to recommendation 10, the Government amended section 317E to ensure the listed acts or things is exhaustive for compulsory industry assistance measures. To balance this amendment against the legislative intention of keeping the powers current with new technological developments,

it was necessary to add a new item to the list of acts or things. Section 317E(da) allows the industry assistance powers to be used in facilitation of an activity conducted under a warrant or authorisation under a law of the Commonwealth, a State or a Territory or the effective receipt of information in connection with a warrant or authorisation.

21. The introduction of subsection 317E(da) ensures that interception agencies are able to use the industry assistance measures as intended to give effect to a warrant or authorisation. This is an appropriate addition as it will only authorise activities that are immediately incidental to doing a thing that has been approved pursuant to an underlying authority subject to existing safeguards and thresholds, including judicial approval. Subsection 317E(da) will also ensure that the utility of the industry assistance measures continues to be relevant for law enforcement and security agency warrants, which continue to be updated and fitted to technological developments.
22. The aim of keeping legislation fit-for-purpose as the regulated industry evolves is genuine and legitimate; particularly when seeking assistance from an innovative and fluid sector such as the communications industry. Without forward-thinking legislation, it may be necessary to consider wholesale legislative reform in the near future. It would be irresponsible to design a regime that does not consider the implications of technological progress where the very issue the regime has been designed to address has been created by technological progress.
23. Additionally, this approach finds precedent in subsection 313(7) of the *Telecommunications Act 1997* which specifies that "giving help" in the context of domestic industry assistance includes giving effect to warrants and authorisations under the TIA Act. Given the broader potential use-cases of industry assistance, it was necessary to forgo enumeration of the potential warrants and authorisations in subsection 317E(da).

The independent legal and technical assessors

24. In response to recommendation 11, a robust review mechanism (section 317WA) was introduced into the Bill to allow a legal and technical expert to assess the proprietary of a TCN particularly in relation to systemic weaknesses and vulnerabilities. The Committee also recommended for the independent assessors to produce a "binding assessment". The Government implemented this recommendation by ensuring that any report produced by the independent panel must be considered by the Attorney-General when issuing a TCN. The independent assessors are bound to consider whether:
    - the requirements imposed by the notice are reasonable and proportionate,
    - compliance with the notice is practicable and technically feasible, and
    - the notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice.
25. Setting these mandatory criteria for the independent assessors ensures that they, by law, take into account the key matters of concern to a provider when compiling their report. This requirement for the Attorney-General to consider the outcomes of any report provided by the independent assessors is present in 317WA(11) (for original notices) and 317YA(10) (for variations). Given the technical and legal knowledge and experience of the assessors, the need for the Attorney-General to consider their findings and the requirement under 317V that the Attorney-General must also be satisfied of reasonableness, proportionality, practicable and technical feasibly, the assessment in the report will have the effect of being extremely influential and determinative. The contents of the report go directly to the Attorney-General's state of mind when considering whether to proceed to give a notice. This decision may be challenged in judicial review on the basis that the Attorney-General did not give sufficient weight to the report. Further, a copy of the report is given to the affected provider and relevant oversight body, ensuring all parties are aware of its contents.

26. The Department has received feedback about some potential limitations in the Committee's recommendation, as made and presently implemented. Currently, it requires both experts to consider and offer views over areas in which their expertise may be limited. The recommendation goes to requiring both assessors to be satisfied that the proposed notice meets the legal and technical critea. In the legislation this is given effect by subsection 317WA(7).
27. The Department queries whether an assessor appointed for their technical expertise is well positioned to consider the reasonableness and proportionality of requests, which are traditionally legal tests. Determining the reasonableness and proportionality of a notice is done so on a case-by-case basis after considering the broader circumstances of a requirement, like the details and needs of national security and law enforcement operations and broader questions of personal and social impact – not potential technical impact of requirements.
28. Equally, requiring that a retired judge assess the technical aspect of the requirements in a TCN, including potential security weaknesses it may create, asks them to make assessments that may be beyond their legal training and experience.
29. While the requirement for both assessors to work in tandem may ameliorate this issue, the Department would like to bring it to the Committee's attention.

Providers must seek permission before making public disclosures

30. In response to recommendation 13, the Department added subsections 317ZF(14)-(16) to the legislation. These provisions allow the decision maker who issued the TAN or TCN to authorise a provider, their employees, their contractors or their contractors' employees to disclose information in relation to a specific TAN or TCN. Disclosure must be in accordance with any conditions specified in the authorisation issued by the decision maker. This provision exceeds the Committee's recommendation, by extending the possibility of conditional disclosure to TANs, not just TCNs as described in the recommendation.
31. The amendments, as implemented, permit the conditional disclosure of the specified information upon request by the provider to the decision-maker. This approach implements the Committee's recommendation by providing discretion to the Attorney-General to adopt, by default, an inclination to on-disclose technical capability notice information in response to a persuasive application by a provider. Given the role of the Attorney-General and the advice that would be provided by agencies, the Attorney-General would take into account whether the disclosure would prejudice an investigation or compromise national security. The expectation that the Attorney-General would agree to such a request, and the considerations which may go to a refusal (like a compromise to national security, or revealing operational capabilities), are being set out in the administrative guidance being developed jointly with industry and agencies.
32. The Department recognises that there may be cases where revealing information, particularly information pertaining to a new capability, would neither prejudice an investigation nor compromise national security yet it would still be inappropriate to unconditionally reveal that information. For example, commercially sensitive information of a supplier or related-provider could be jeopardised if the Attorney-General authorised the disclosure of information at the unilateral request of a single provider. Given the complexities of capabilities, the multiple stakeholders who may utilise them and the inherent national security and law enforcement sensitives there is a paramount need for retain the ability to conditionally disclose information. Further, disclosures may risk prejudicing tradecraft that are not related to a single law enforcement investigation and may advise criminals on how to evade detection and investigations.

Strengthening the prohibition against 'systemic weakness' and protecting information

33. In response to recommendation 9, the Government amended the definition of systemic weakness and systemic vulnerability in section 317B of the Act and introduced further qualifications to section 317ZG to strengthen the legal framework relating to information security.

34. In addition to implementing PJCIS recommendations, new definitions were introduced to account for broader feedback that the term be defined. Systemic weakness and systemic vulnerability now means 'a weakness or vulnerability that affects a whole class of technology, but does not include a weakness or vulnerability that is selectively introduced to one or more target technologies that are connected with a particular purpose. For this purpose, it is immaterial whether the person can be identified.' The key aspect of these definitions is the prohibition against any requirements which affects a whole class of technology. As set out in the supplementary explanatory memorandum, the term 'whole class of technology' is intended to capture actions that make general items of technology less secure; a 'class' is a category of technology that include a product line, or a facet within a product line, or any constituent element of a particular technology that is also widely applied and available. For example, a class of technology encompasses:

    - mobile communications technology
    - a particular model of mobile phone
    - a particular type of operating system within that model of mobile phone
    - a particular form of encryption or authentication that secures communications with that operating system

35. As the above indicates, the protection has been cast as broadly as possible to ensure that the consistent intent of the Government with regards to this Act is given effect. That is, no requirements in the Act should be able to weaken or make vulnerable the services and devices that are used by the general public, business community or legitimate and specialised subsets of either. Any requirement that interacts with the information security of products should impact a particular person/s of interest, or related parties.

36. This targeted nature is expressed in the second element of the definition which carves-out the permissible use of the powers for the sake of clarity. The selective introduction of a vulnerability or weakness, as it relates to a target technology connected with a particular person is allowable. The definition of target technology further reinforces the specificity and precision through which interaction with electronic protections such as encryption is permissible. This definition takes each likely item of technology, like a carriage service or electronic service, which may be supplied by a designated communications provider, and reinforces that a weakness or vulnerability may only be introduced to the particular technology that is used, or likely to be used by a particular person. For example, a single mobile device operated by a criminal, or likely to be used by a criminal, would be classified as a target technology for the purpose of paragraph (e) of that definition. However, a particular model of mobile devices, or any devices that are not connected with the particular person, would be far too broad to fall within the definition. This ensures that the services and devices enjoyed by innocent parties or persons not of interest to law enforcement and security agencies remain out of scope and unaffected. This is of course an additional protection to the need to have a valid warrant or authorisation (which are already inherently targeted) in place to lawfully access personal information.

37. To complement this definition and further bind the targeted use of the powers, amendments to subsections 317ZG(4A), (4B) and (4C) were made. Subsections 317ZG(4A) and (4B) reinforce that if a weakness or vulnerability is selectively introduced to a particular device or service, the activity **must not** jeopardise information security of any other person. Subsection 317ZG(4C) clarifies that

an activity would jeopardise the security of information if it will, or would be likely to, create a material risk that otherwise secure information (i.e. encrypted information) could be accessed by an unauthorised third party, like a cyber-criminal. In effect, the clarification ensures that even an inadvertent impact on broader cyber security that might arise from an agency's targeted activities is also in contravention of the Act.

38. Simply expressed:

    - Defining systemic weakness/vulnerability as a something that affects a whole class of technology ensures the general items of technology, like a type of operating system or commercially available encrypted messaging service, cannot be made less secure.
    - Clarifying that particular items of technology connected to a particular person, like a criminal's mobile phone, are not captured in this prohibition. This allows agencies to discharge their existing functions and aids the targeted surveillance already lawfully undertaken by Australian authorities.
    - Reinforcing in section 317ZG that these targeted activities must not negatively impact information security of other persons. This creates a legal guarantee that any requirements which create a material risk of unauthorised access to information held by any other person is prohibited, even if the activity primarily targets a particular phone or person.

39. The combined effect of the new definitions and amendments to 317ZG is comprehensive and ensures that a solid legal guarantee to information security applies to all activities under the framework, including voluntary activities.

40. The phrase 'for this purpose, it is immaterial whether the person can be identified' in the definitions in section 317B acknowledge the fact that some law enforcement investigations and national security exercises, while targeted, are not conducted in relation to a particular identified person. For example, an investigation into identity theft or distribution of child pornography may be assisted by accessing an internet sharing site, even though the identity of those perpetuating the offending are not yet known. Targeting of this nature is commonplace in undercover operations where the principal organisers are not known at the commencement of the investigation.

The exclusion of integrity bodies and crime commissions

41. In response to recommendation 3, the Government amended the definition of interception agency in section 317B to exclude State and Territory independent commissions against corruption from the scope of Schedule 1 powers. This has the effect of excluding those commissions that have the authority to use invasive powers to investigate serious misconduct and criminal activity of State public officers, including law enforcement.

42. The Department notes that independent anti-corruption commissions have an important oversight function and access to similarly intrusive powers, like interception warrants and telecommunications data under the TIA Act. State commissions, and Commonwealth bodies like the Australian Commission for Law Enforcement Integrity, play an important role in identifying and investigating serious misconduct and corruption across the public sector, and maintaining confidence in the conduct of public frameworks and officers. Importantly, their functions now permissibly extend to ensuring the correct use of the industry assistance measures by State law enforcement. Furthermore, the severity of these commissions' investigations means that much of their work readily passes the serious offence threshold added in response to the Committee's recommendation.

43. There is an inconsistency in entrusting these commissions with intrusive interception and surveillance powers but preventing them from obtaining the incidental powers to facilitate these activities and others through technical assistance. As noted in the Western Australian Corruption and Crime Commission submission to the PJCIS, the industry assistance measures will facilitate the

work of State commissions by improving their ability to access intelligible communications under warrant.

Extending the limitations in section 317ZH to technical assistance requests

44. In response to recommendation 17, the Government amended section 317ZH to prohibit the issuance of an industry assistance notice, including TARs, in substitute for a warrant or authorisation.

45. Subsection 317ZH(1) was also amended to ensure this prohibition does not apply to the warrants and authorisations in the *Intelligence Services Act 2001* (the IS Act). However, unlike a warrant, ministerial authorisations in the IS Act cannot require a provider to do anything (like hand over data for example), rather they authorise ASIS and ASD to undertake independent activities.

Additional Government amendments – beyond the scope of the PJCIS recommendations

1. The Government made additional amendments to the Bill based on ongoing consultations with agencies and industry, and following the tabling of reports on the Bill from the Senate Standing Committee for the Scrutiny of Bills and Parliamentary Joint Committee on Human Rights. Broadly speaking, these amendments are minor and technical in nature, and clarify the intent and operation of existing provisions and safeguards.

2. See **Attachment B** for further analyses of the amendments made to the Bill that go beyond the scope of the PJCIS recommendations.

3. These amendments are discussed below.

Clarifying the purpose of TANs – 317L(2A)

4. Subsection 317L(2A) was added to the legislation to further elucidate the distinction between the intended purpose of TANs and TCNs. The subsection provides that a TAN must not be given for the purpose of ensuring a provider is capable of providing help to ASIO or an interception agency and therefore must be used to request help that a provider is already capable of giving. Assistance directed towards creating a new capability, ancillary to the existing business requirements of a provider, is the intended function of TCNs. TANs are not designed for this purpose.

New annual reporting requirements – 317ZS(1)(d)

5. Paragraph 317ZS(1)(d) adds a new annual reporting requirement on the use of industry assistance powers. This paragraph requires the Home Affairs Minister to list in the annual report the kinds of serious Australian offences that industry assistance has been used to enforce in the preceding year. This addition is indicative of the Government's commitment to transparency and explaining to the public how these new powers are being used to detect and disrupt serious crime by law enforcement agencies.

Clarified references to Ministers

6. In order to clarify the role of Ministers in the legislation, the Government has amended existing references to "the Minister" to "the Home Affairs Minister" at subsections 317T(5), 317T(6), 317T(6)(e), 317ZK(8), 317ZK(11), 317ZK(12), 317ZK(14) and 317ZS(1). Additionally, "Home Affairs Minister" is now defined in section 317B.

New consultation requirements before issuing TANs – 317PA

7. Section 317PA requires the Director-General of Security or the chief officer of an interception agency to consult with providers before issuing them with a TAN. This ensures consistency with the mandatory consultation required before a TCN can be given. In order to properly consider the criteria for issuing a TAN, consultation with the provider was always effectively required. With this addition, the consultation process becomes legally codified. The Department has made this amendment to better guide decision makers through the TAN process.

Technical fixes for penalty provisions – 570(3)(aa), 570(4C) and 570(4D)

8. Paragraph 570(3)(aa) was added by the Government to give effect to the existing compliance and enforcement provision of 317ZA which previously did not carry an equal penalty for carriers and carriage service providers. Subsections 570(4C) and 570(4D) are amendments consequential to the addition of paragraph 570(3)(aa). These amendments also ensure that all potential fines are expressed as penalty units, rather than lump sums, to account for inflation.

Changed from proclamation to royal assent – 2(1)

9. This amendment to item 2 of subsection 2(1) changes the commencement of Schedule 1 of the Act to begin the day after the Royal Assent rather than to be specified by proclamation. This was necessary to have the Act commence immediately to ensure Australia's law enforcement and intelligence agencies were appropriately equipped to address security threats over the Christmas and New Year period.

Changed relevant objectives for ASD – 317G(5)

10. In order to meet recommendation 2 of the PJCIS, subsection 317G(5) was rewritten. This sets out the purposes for which TARs may be issued. As a result of implementing this recommendation, the Government saw an opportunity to better specify the purposes for which ASD may issue TARs in order to reduce the burden of regulation on industry. As such, paragraph 317G(5)(c) now limits ASD's use of TARs to its function of providing material advice to and other assistance to specified bodies set out in sections 7(1)(ca) and 7(2) of the *Intelligence Services Act 2001*. This is indicative of ASD's cyber security function and demonstrates its role in assisting industry with investigating and preventing cyber-attacks and securing Australian data.

11. ASD's inclusion as a user of industry assistance is a feature unique to TARs, which means this amendment did not need to be replicated for TANs or TCNs.

Advice of right to complain when issuing TANs – 317MAA(3)-(6)

12. To ensure providers subject to compulsory assistance under TANs are aware of their right to complain, the Government has added subsections 317MAA(3)-(6) to the legislation. These subsections require that issuing agents advise providers of their right to complain to the Commonwealth Ombudsman, the relevant State or Territory inspecting agencies, or IGIS, depending on the issuing agency, when issuing a TAN. This is consistent with suggestions of the Inspector-General of Intelligence and Security, though not an express recommendation. This requirement is important to ensure providers are informed of the applicable remedies and that any complaints can come to the attention of the Department or the Parliament.

Moved TCN limitations from Division 4 to Division 7 – 317T(8)-(11)

13. For better regime organisation, the Department has moved existing limitations previously at subsections 317T(8)-(11) on the use of TCNs from Division 4, which deals with TCNs, to the collected limitations division, Division 7. This amendment centralises Schedule 1's limitations into one, accessible location.

New limitation on TCNs – 317ZGA(4)

14. The Government has added a new limitation to the use of TCNs to address concerns that industry assistance can be used to conduct mass surveillance operations or extend data retention obligations. Subsection 317ZGA(4) explicitly prevents providers being asked to store the web browsing history, or associated metadata, of their users. This amendment was made to clarify the intention that the existing Data Retention regime in Part 5-1A of the TIA Act is the explicit vehicle for expanding or contracting the data set, not TCNs.

Added express authority for Commonwealth Ombudsman to inspect records of industry assistance powers used with specified warrants and authorisations

15. The Department has added new authority for the Commonwealth Ombudsman to inspect any records an agency may have concerning the agency's use of industry assistance powers when this has been done in concert with an interception warrant, stored communications warrant or authorisation under Division 3, 4 or 4A of Part 4-1 of the TIA Act. The Commonwealth Ombudsman's inspection of these records is for the purpose of determining the agency's compliance with Part 15 of the Telecommunications Act – which contains the industry assistance powers. This is additional to their explicit inspection function under section 317ZRB.
16. A principal way in which industry assistance powers will be used will be in the execution or facilitation of these warrants and authorisations. As such, providing the Commonwealth Ombudsman with explicit access to the agency's records during their inspections of these existing powers may provide a valuable avenue for oversight into the operation of industry assistance.

Operationalisation of the Act

The use of the powers in the Act

17. The Department understands that Commonwealth law enforcement and national security agencies have used the powers in the Act to support operations and investigations. The Department refers to the submissions from agencies for further details on the use of the powers.

Implementation of the Act

18. Implementation of the Act and its measures is currently underway. While significant progress has already been made, the efforts of the Department to ensure the regime is implemented effectively and reasonably are ongoing.
19. The Department is currently working with law enforcement and national security agencies to facilitate the implementation of the Act. In late 2018, the Department developed and disseminated interim guidance material to support those law enforcement and national security agencies empowered by

the Act. The purpose of the interim guidance material was to aid the urgent use of key powers in the Act by agencies during the Christmas and New Year period and to explain the thresholds and obligations when using the industry assistance powers.

20. The Department continues to engage with agencies across Australia, small and large domestic communications providers, multi-national companies operating in Australia and industry representative groups to develop comprehensive guidance and training material to ensure the operation of key measures in the Act is well understood, and that stakeholders can discharge their obligations. This process is ongoing. The guidelines will develop standard forms and administrative arrangements to guide the consistent use of the powers, including guidance that makes clear Government obligations with respect to consultation, information security and oversight of the powers. The Department will also hold meetings across Australia to discuss the Act with industry stakeholders that are likely to be impacted by the legislation.
21. In conjunction with the AFP, the Department has delivered on-site training on the use of the powers to NSW Police and Victoria Police. This training highlighted:
    - the legal processes that agencies must satisfy while using the powers

      the administrative requirements of seeking approval from the AFP Commissioner for the use of TANs
    - the strict thresholds and safeguards that must be met, and
    - operational use cases.
22. Further training will be delivered to other State and Territory police forces in February 2019.
23. The Department has identified and approached a number of eminent academics, cyber security professionals and retired judges to seek expressions of interest in the role of independent assessor for new capabilities, consistent with section 317WA of the legislation.
24. Former justices of the High Court, Federal Court, State Supreme Courts and District Courts have expressed firm interest in the role of judicial assessor. Several technical experts, independent from Government and with deep knowledge of cyber security systems, have also indicated interest in the position.
25. The Department has begun to create a pool of legal and technical experts that may be appointed upon when required to review the requirements in a notice. The technical experts include a range of expertise and knowledge to ensure that the appropriate persons can be approached in respect to the type of technology, networks or systems. Other experts can be considered by the Attorney-General, depending on the circumstances of the request and could include recommendations made by providers.

Conclusion

26. The Act reflects the Government's acceptance of the PJCIS' seventeen recommendations and the outcome of further engagement with key stakeholders including oversight bodies and industry, and scrutiny from other Parliamentary Committees. The Government amendments to the Bill as introduced and passed on 6 December 2018 strengthens existing safeguards to protect the privacy of Australians, enhances the security of the digital ecosystem and ensures agency powers are utilised where necessary, proportionate and reasonable. The amendments also broaden and facilitate the function of oversight bodies including the Commonwealth Ombudsman and the IGIS to increase public scrutiny on the use of the powers in the Act.
27. The Department has noted some potential issues with the operation of the Act as in operation.
28. The Department is steadfastly progressing with the implementation and operationalisation of the Act. This involves continuing support to agencies and industry to ensure consistent, reasonable and clear use the powers and dedicated training exercises. The Department is also engaging with industry to dispel common misconception, build confidence and to reiterate the intended purpose and operation of the Act.

Attachment A

PJCIS Recommendation	Response	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
1. The Committee recommends that the Parliament immediately pass the Telecommunications (Assistance and Access) Bill 2018, following the inclusion of amendments recommended in this report.	Passed on 6th December 2018.		
2. The Committee recommends that the industry assistance measures under Schedule 1 of the Telecommunications (Assistance and Access) Bill 2018, so far as they relate to criminal law enforcement, apply to offences with a penalty of a maximum period of three year's imprisonment or more.	Implemented. Law enforcement can only use industry assistance powers when enforcing the criminal law for 'serious Australian or foreign offences'. 'Serious offences' have been defined as offences carrying a penalty of three years or more imprisonment.	14, 21, 22, 23, 34, 35, 51, 52	317B, 317E(j), 317G(5), 317L(2), 317T(3)
3. The Committee recommends that State and Territory law enforcement agencies be retained within the scope of the Bill, with the exception of State and Territory independent commissions against corruption which the Committee recommends should be excluded from the scope of Schedule 1 of the Bill.	Implemented. "Interception agency" has been redefined to remove anti-corruption and State crime commissions from using industry assistance powers.	5, 9, 10, 11, 12, 114, 116, 117, 118, 119, 120, 121, 122, 123, 125, 126, 127, 128, 129, 130,	317B, 317ZM, 317ZR
4. The Committee recommends that the Bill be amended to incorporate recommendations from the Commonwealth Ombudsman to establish clear authority to inspect and gather information on the exercise of the industry assistance measures by the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission, and State	Implemented. • Inspection of industry assistance records. • Notification and reporting requirements for industry assistance powers. • Tabling Ombudsman's report. • Inspection of notices connected	13, 26, 28, 32, 41, 42, 44, 48, 49, 62, 64, 68, 71, 74, 78, 82, 83, 113, 132 136, 137, 138 147, 151, 152, 153,	317B, 317HAB(4), 317JA(18), 317JB(9), 317MAA(4), 317ZF(2)(g), 317MAB(2), 317MA(1F), 317Q(13), 317R(6), 317TAB(2), 317TA(1E), 317WA(7),

PJCIS Recommendation	Response	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
and Territory interception agencies. This includes express notification requirements and information sharing provisions which would complement the inspection activities of State and Territory oversight bodies.	to TIA and SD warrants. • Disclosure exceptions for Ombudsman. • Judges may specify any conditions on an SD computer access warrant. • Clarified interaction between emergency authorisations in SD Act and TIA warrants. • Added compensation relating to computer access warrants. • 317ZH limitation applies to TARs.	154 155 157	317X(7), 317Z(4), 317ZF(5A)-(5C), 317ZKA(2), 317ZKA(4), 317ZRB 83(4), 84(1), 186B(1A) of the *Telecommunications (Interception and Access) Act 1979* 27D(1)(b)(xii), 32(4), 49B, 55, 64(2) of the *Surveillance Devices Act 2004* 5(1) of the *TIA Act* 63AB(3)-(6)
5. The Committee recommends that the Bill be amended to incorporate suggestions from the Office of the Inspector-General of Intelligence and Security (IGIS) to strengthen oversight of the powers in Schedule 1 of the Bill, as it applies to the Australian Security Intelligence Service (ASIO), the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD). This includes: • explicit notification and reporting requirements when issuing, varying,	Implemented. • Record-keeping requirements. • Notification obligations when issuing, varying, extending or revoking. • Reasonable and proportionate requirements for TARs. • Notification of right to complaint. • Disclosure exceptions for IGIS officials. • Added consideration of "necessity" and intrusion on third-	2 24, 25, 26, 27, 28, 32, 40, 41, 42, 44, 48, 49, 50, 61, 62, 64, 65, 71, 73, 74, 75, 81, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 112, 113, 140, 141, 142, 143,	94(2BA) and 94(2BB) of the *ASIO Act* 317H(5), 317HAA(5)-(6), 317HAB(1)-(4), 317JA(15)-(17), 317JAA, 317JB(6)-(8), 317M(5), 317MAA(3), 317MAB(1), 317MA(1E), 317Q(12), 317R(5), 317TAA(2)-(3),

PJCIS Recommendation	Response	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
extending or revoking a notice or request under Schedule 1; • limits on the exercise of Schedule 1 powers (including extending prohibition on systemic weakness to voluntary notices, ensuring decision-makers consider necessity and intrusion on innocent third parties when issuing a notice); • defences for IGIS officials; and • clear information sharing provisions. The IGIS and the Ombudsman should provide assurances directly to the Committee that the amendments agreed to by the Government address their concerns.	parties to decision-making criteria. • Providing for the 'parsing' of requirements in 317ZK and allowing for public interest exception to be applied in a more targeted manner. • Clarifying the scope of 317ZH and ensuring the prohibition against replicating warrants and authorisations apply to warrants and authorisations required by the requesting agency only. • Extended "systemic weakness" prohibition to voluntary requests.	144, 145, 146, 147, 148, 149 159 162, 163, 164, 165, 166, 167	317TAB(1), 317TA(1D), 317X(6), 317YA(9), 317ZAA(ea), 317ZAA(eb), 317Z(3), 317ZKA(1), 317ZF(2A), 317ZF(2B), 317ZH(1), 317ZH(6)-(9), 317ZK(1)(c)-(e), 317ZK(2)(a)-(b), 317ZK(3)(c)-(f), 317ZK(3A), 317ZK(6A)-(6B), 317ZK(17)-(20), 317ZKA(3), 25A(4A), 25A(9)-(10), 27A(3D)-(3E), 27E(3A), 27E(7)-(8), 34A, 27D(1)(b)(xii) of the *ASIO Act* 27E(2A), 27E(8)-(9) of the *SD Act* 63AC(3)-(5) 21A(2), 21A(2A), 21A(3A), 34(1A),

PJCIS Recommendation	Response	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
			34AAA(3A)-(3D), 34ZH(1)-(2), 84(2BC) of the *ASIO Act*
6. The Committee recommends that the Bill be amended to provide that Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) be subject to statutory time limits, and that any extension, renewal or variation of a TAN or TCN also be subject to a statutory time limit.	Implemented. TANs and TCNs cannot be issued with an expiry date later than 12 months but may be renewed for a further 12 months with the provider's agreement.	43, 44, 48, 63, 67, 71	317MA(1A)-(1G), 317Q(11)-(13), 317TA(1A), 317W(7)-(9), 317X(5)-(8)
7. The Committee recommends that the Bill set out a tiered approval system for state and territory initiated Technical Assistance Notices (TANs), under which TANs would be submitted for approval to the Commissioner of the AFP before being issued to the recipient. The intention of this process of approval would be to ensure consistency in decision making, and reporting, across jurisdictions. To give effect to this intention, the Commissioner of the AFP must apply the same statutory criteria, and go through the same decision-making process, as would apply if the AFP were the original issuing authority.	Implemented. TANs issued by State and Territory law enforcement must be approved by the Commissioner of the AFP.	39	317LA
8. The Committee recommends that the Bill be amended to include a requirement that Technical Capability Notices be jointly authorised by the Attorney-General and the Minister for Communications, the latter being able to provide a direct avenue for the	Implemented. Before a TCN may be issued it must be approved by the Minister for Communications having considered the effect on the targeted provider and the broader industry.	59, 72	317TAAA, 317XA

PJCIS Recommendation	Response	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
concerns of the relevant industry to be considered as part of the approval process.			
9. The Committee notes the evidence of the Director-General of the Australian Signals Directorate that a "systemic weakness" is a weakness that "might actually jeopardise the information of other people as a result of that action being taken". The Committee also notes the evidence of the Director-General of Security, that the powers in Schedule 1 will not be used to require a designated communications provider to do anything that jeopardises the security of the personal information of innocent Australians. Having regard to those assurances, the Committee recommends that the Bill be amended to clarify the meaning of the term 'systemic weakness', and to further clarify that Technical Capability Notices (TCNs) cannot be used to create a systemic weakness.	Implemented. A definition of "systemic weakness" has been added to clarify that the information security of non-targeted individuals cannot be diminished.	6, 16, 17, 89	317B, 317ZG(4A)-(4C)
10. The Committee recommends that Schedule 1 of the Bill be amended to apply the 'systemic weakness' limitation to all 'listed acts or things'. The Committee also recommends that the definitions of 'listed acts or things' and 'listed help' be exhaustive in the Bill.	Implemented. The "systemic weakness" limitation applies to all "listed acts or things" as intended. The list is now exhaustive for compulsory powers (TANs and TCNs).	20, 37, 38, 46, 47, 56, 57, 69, 70	317E(1)(da), 317L(3), 317Q(8), 317T(7), 317X(3)
11. The Committee recommends that the Bill be amended to allow a designated communications provider, who has been given a capability notice under subsection 317W(1)	Implemented. Providers may now request an assessment of a TCN by an independent technical expert and a retired judge for	66, 68, 73, 76, 77	317W(7)-(9), 317WA, 317YA, 317ZF(1)(b)(x)-(xa), 317ZF(1)(d)(ixa)-(ixb)

PJCIS Recommendation	Response	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
of the Bill in relation to a proposed Technical Capability Notice (TCN), to request a binding assessment of: • whether the proposed technical capability notice would contravene section 317ZG of the Bill; • the requirements imposed by the notice are reasonable and proportionate; • compliance with the notice is practicable and technically feasible; and • the notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice. This request would be made in writing to the Attorney-General within a reasonable time limit specified in the consultation notice. The Committee recommends that two persons be jointly appointed to conduct the assessment: • One of these persons should have knowledge that would enable them to assess whether proposed TCN would contravene section 317ZG of the Bill, and should be cleared for security purposes to the highest level required by staff members of ASIO, unless the Attorney-General approves a lower security level. • The second assessor must be a person who has served as a judge in one or	compliance with the Act's requirements and limitations. The assessors are bound to consider whether the proposed requirements in a notice contravene section 317ZG, and the thresholds of reasonableness and proportionality, practicality, technical feasible and intrusiveness.		

PJCIS Recommendation	Response	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
more prescribed courts for a period of 5 years; and who no longer holds a commission as a judge of a prescribed court. • Both persons must agree that: o The requirements imposed by the notice are reasonable and proportionate; o Compliance with the notice is practicable and technically feasible; and o The notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice. • The report prepared by the technical expert and the retired judge must also be provided to the Inspector-General of Intelligence and Security (for oversight of ASIO) and the Commonwealth Ombudsman (for oversight of the AFP).			
12. The Committee recommends that the Government continues to ensure that the IGIS and other Commonwealth oversight bodies have sufficient resources to ensure that they can properly execute their additional responsibilities under the Bill.	Accepted. The Department will work with the Attorney-General's Department, the Commonwealth Ombudsman and the IGIS to monitor resourcing and ensure oversight bodies have adequate funds to discharge their new functions under the Act.		
13. The Committee recommends that the Bill be amended to allow a provider to request	Implemented. Providers may now seek approval to	85	317ZF(14)-(17)

PJCIS Recommendation	Response	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
that the Attorney-General approve disclosure of a technical capability. It would be expected that the Attorney-General would agree to such a request except to the extent that doing so would prejudice an investigation or compromise national security. This would complement existing provisions in the Bill that enable a provider to disclose publically the fact that they were issued a technical capability notice.	disclose information about assistance offered from the Attorney-General.		
14. The Committee recommends that the Bill include express provision for a statutory review of the Bill's operation by the Independent National Security Legislation Monitor, within 18 months of the Bill commencing.	Implemented. The INSLM is required to conduct their review after the Act has been inforce for 18 months.	3	6(1)(e), 6(1D) of the *Independent National Security Legislation Monitor Act 2010*
15. The Committee recommends that the Bill include an amendment which puts beyond any doubt suggestions the Bill may impact Parliamentary privilege.	Implemented. Provision has been added to clarify that nothing in any of the Act's schedules abridges Parliamentary privilege.	131, 150, 160, 161	317ZRA 27J of the *Surveillance Devices Act 2004* 3SA of the *Crimes Act 1914* 202B of the *Customs Act 1901*
16. The Committee recommends that, once the Bill (as amended) is passed by the Parliament, the Committee: • commences a review of the new legislation;	Implemented. The PJCIS is required to conduct a further review of the legislation.	139	187N, 187N(1) of the *Telecommunications (Interception and Access) Act 1979*

PJCIS Recommendation	Response	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
• for the purposes of the review, be allowed to hold further public hearings; and • complete its review of the new legislation by 3 April 2019.			
17. The Committee recommends that the Government: • Amend clause 317ZG of Schedule 1 to explicitly prohibit an interception agency from asking a designated communications provider to voluntarily implement or build a systemic weakness or vulnerability under a technical assistance request; and • Amend clause 317ZH of Schedule 1 so that the 'general limits' on technical assistance notices and technical capability notices apply equally to technical assistance requests.	TARs are now subject to the same limitations as TANs and TCNs.	23, 28, 29, 30, 31, 32, 33, 86, 87, 88, 90, 92	317G(5), 317JAA, 317JA(11)-(19), 317JB(1A), 317JB(2A), 317JB(3A), 317JB(5), 317JC, 317ZG, 317ZG(1), 317ZG(1)(a), 317ZG(5), 317ZH(1)

Attachment B

Department Amendment	Reason	Amendment number (as listed in the Supplementary EM)	Affected sections (*Telecommunications Act 1997* unless otherwise stated)
Clarifying purpose of TANs.	Confusion of TANs v TCNs	36	317L(2A)
New annual reporting requirements	Best practice.	134	317ZS(1)(d)
Identifying Home Affairs Minister	Concerns from Dept. Comms	7, 53, 54, 55, 108, 109, 110, 111, 133	317T(5), 317T(6), 317T(6)(e), 317ZK(8), 317ZK(11), 317ZK(12), 317ZK(14), 317ZS(1)
Adds consultation requirements for TANs	Best practice and in response to industry feedback.	18, 19, 45	317PA
Technical fixes for penalties provisions	Fixes were needed to make provision operate consistently across providers – conversion to penalty units is good practice.	135	570(3)(aa), 570(4C), 570(4D)
Changed to begin on royal assent.	Necessary to make powers available over Christmas	1	2(1)
Changed relevant objectives for ASIO, ASIS and ASD	Consequence of changing systemic weakness definition and adding serious offence threshold. Also changed to better reflect ASD's cyber-security function.	23	317G(5)
Added State and Territory Inspecting authorities	Best practice.	15, 78, 79, 80, 84	317B,317ZF(2), 317ZF(5A)-(5C), 317ZF(12A)-(12D)
Requirement to advise providers of right to complain.	Best practice and ensure providers are aware of available remedies.	41	317MAA(3)-(6)
Moved TCN limitation provisions from Division 4 to Division 7	Division 7 is designated for limitations making it more appropriate to contain these provisions.	58, 91	317T(8)-(11), 317ZGA(1)-(3)
Added new limitation on TCNs	Makes explicit that TCNs cannot be used to collect browsing history.	91	317ZGA(4)

Department Amendment	**Reason**	**Amendment number (as listed in the Supplementary EM)**	**Affected sections (*Telecommunications Act 1997* unless otherwise stated)**
Added new authority for Ombudsman to inspect records of industry assistance powers used in connection with warrants	Added avenue of inspection to provide clear authority for regular inspection of the use of Part 15 of the Telecommunications Act in conjunction with underlying interception and surveillance powers.	136, 137, 138	83(4), 84(1), 186B(1A) of the *Telecommunications (Interception and Access) Act 1979*