Australian Government

Independent National Security Legislation Monitor

TRUST BUT VERIFY

A report concerning the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and related matters

SUMMARY OF RECOMMENDATIONS

Dr James Renwick CSC SC

3RD INSLM 2020 9TH REPORT

THE INDEPENDENT NATIONAL SECURITY LEGISLATION MONITOR

The *Independent National Security Legislation Monitor Act 2010* (Cth) provides for the appointment of the Independent National Security Legislation Monitor (INSLM). The INSLM independently reviews the operation, effectiveness and implications of national security and counter-terrorism laws; and considers whether the laws contain appropriate protections for individual rights, remain proportionate to terrorism or national security threats, and remain necessary.

In conducting the review, the INSLM has access to all relevant material, regardless of national security classification, can compel answers to questions, and holds public and private hearings. INSLM reports are provided to the Prime Minister, the Attorney-General or the Parliamentary Joint Committee on Intelligence and Security, and are tabled promptly in Parliament.

The INSLM does not deal with complaints but welcomes submissions on the reviews. The INSLM is a part-time role and is supported by a small permanent staff located in Canberra. Further information and contact details can be found at www.inslm.gov.au. There have been three INSLMs since the role began in 2010: Bret Walker SC, the Hon Roger Gyles AO, QC and Dr James Renwick CSC SC (pictured).

BACKGROUND TO FINDINGS AND RECOMMENDATIONS

1.1. The essential effects of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA) are as follows:

a. Schedule 1 gives police and intelligence agencies new powers to agree or require significant industry assistance from communications providers.

b. Schedules 2, 3 and 4 update existing powers and, in some cases, extend them to new agencies.

c. Schedule 5 gives the Australian Security Intelligence Organisation (ASIO) significant new powers to seek and receive both voluntary and compulsory assistance.

1.2. Schedules 1 and 5 have proven controversial; Schedules 2, 3 and 4 less so.

1.3. My task is to consider the operation, effectiveness and implications of TOLA and whether it is necessary, is proportionate to the threats it seeks to meet and treats human rights properly. Where powers have not yet been used, my task involves prediction.

1.4. *As to necessity*, I have concluded that, with 2 exceptions, TOLA is or is likely to be necessary. The first exception is that Schedule 1 must be amended to extend Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) to integrity agencies, including any future Commonwealth Integrity Commission. The other exception is in Schedule 5: one aspect of the voluntary assistance power and corresponding civil immunity in s 21A(1) of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) is unnecessary and should be amended.

1.5. *As to proportionality and proper rights protection*, TOLA will be compliant if, but only if, the central recommendations in this report are implemented. Most importantly, Schedule 1 should be amended to:

a. remove the power from agency heads to issue TANs and from the Attorney-General to approve TCNs[1]

b. vest those issuing and approval powers in the Administrative Appeals Tribunal (AAT) in a way which will preserve and protect both classified and commercial-in-confidence material and allow independent rulings on technical questions

[1] (Formerly) with the concurrence of the Minister for Communications.

such as 'systemic weakness' (definitions which, among others, should be amended)

c. create a new statutory office – the Investigatory Powers Commissioner (IPC). The IPC should be a retired judge who will be appointed to the AAT and have access to technical advice. The IPC will assist in approving the issue of TANs and TCNs (as above) while monitoring the operation of Schedule 1 and issuing guidelines. (This can be done with minimal expense.)

1.6. I have recommended that there be no change to the way that TARs are currently agreed between an interception agency head and a Designated Communications Provider (DCP) and the way the agreement then enables the relevant agency head to issue a TAR (although I have recommended the use of a prescribed form). This is in contrast with my recommendations on TANs and TCNs. It was almost unanimously agreed in non-government submissions that these notices should be authorised by either an independent tribunal member or a judicial officer and subject to meaningful judicial review once issued. Indeed, a number of stakeholders indicated that their main concern with the provisions in Schedule 1 was that no independent person is involved in the decision to issue a notice. The Australian Human Rights Commission raised human rights concerns on this point. Government submitters contended that there are already a number of conditions that apply to the issuing of compulsory notices, and these operate effectively and with sufficient oversight. My recommendations for TANs and TCNs build on these existing mechanisms to guarantee consideration of human rights, privacy and technical implications by the issuing authority.

1.7. A related key point is the distinction between TANs and TCNs, which provide technical 'access'; and warrants (and other similar instruments), which provide 'content'. TANs and TCNs do not provide the authority to obtain content from a DCP without an underlying warrant, and the Government has submitted that these notices are merely a mechanism to ensure that whatever data is obtained under a lawful warrant is accessible and comprehensible to the interception agency. I have not accepted the Government's argument as to the distinction in this regard.

1.8. I consider that there is a greater need for safeguards in the virtual world than in the physical world, for both reasons of trust and the wide and unknown impact of technology. At a public hearing of this review, Professor Peter Leonard, from the Law Council of Australia, stated in relation to trust:

> *In the digital world, digital trust of citizens is affected by activities that may not relate to their specific digital activities. So we always need to consider, as we look at the digital world, the effect on broader digital trust of citizens, and potentially undermining that trust. Now, often a degree of undermining that trust will be justified in national security or law enforcement, but I do think that*

you can't take the digital world as an exact analogue of the physical world, because of that different nature of the digital system.

The review

1.9. TOLA was enacted in December 2018 after targeted government consultation and limited time for parliamentary scrutiny. Many communications providers regarded this as unsatisfactory.

1.10. By s 7A of the *Independent National Security Legislation Monitor Act 2010* (Cth) (INSLM Act), the Parliamentary Joint Committee on Intelligence and Security (PJCIS) may refer to me any matter which it 'becomes aware of in the course of performing its functions … and … considers should be referred'.

1.11. In March 2019, having issued 2 reports on TOLA, the PJCIS requested that I consider the necessity and proportionality of that legislation in view of the threats it seeks to meet, and its effects on human rights, and report by June 2020.[2]

1.12. The review has held extensive consultations in Australia, the United Kingdom (UK) and the United States (US); held public and private hearings; and received many submissions, which are both listed and summarised in the appendices of the report.

1.13. The report complies not only with the request from the PJCIS but also with the requirements contained in s 6(1D) of the INSLM Act[3] to review TOLA. The report's aim is to assist the PJCIS in its pending review of TOLA and also, as the INLSM Act's object states, to 'assist Ministers'. I have had access to the as-yet unpublished Comprehensive Review of the Legal Framework of the National Intelligence Community and taken it into account.

1.14. This report is suitable to be, and should be, made public save for a small but necessarily classified annexure, which I am only able to provide to the PJCIS and ministers.

---

[2] A copy of the referral letter and related press release is at Appendix A.

[3] (1D) The Independent National Security Legislation Monitor must:

(a) review the operation, effectiveness and implications of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*; and

(b) do so as soon as practicable after the 18-month period beginning on the day that Act receives the Royal Assent.

1.15. If, as I recommend, TOLA and related Acts are included in my 'own motion' powers of review in the INSLM Act, my successors will be able to update this review as necessary and as they see fit.

1.16. TOLA is a lengthy and complex Act which itself amends many laws, extends beyond national security and counter-terrorism concerns to crime generally, and operates in an environment of ever-changing technology. Also, as extensive engagement with this review has shown, it could affect many important and legitimate businesses both in Australia and overseas.

1.17. Because of these matters, and the need for extensive consultation, it has been the most complex and difficult report I have produced. I am therefore grateful for the indispensable support I have received from those providing briefings, submissions, and feedback; and, of course, those assisting me.

TOLA's 5 schedules

1.18. TOLA is an Act with 5 schedules which runs to over 200 printed pages. Apart from the *Telecommunications Act 1997* (Cth) itself, TOLA amends, sometimes extensively, complex and frequently amended Acts such as the ASIO Act, the *Crimes Act 1914* (Cth), the *Customs Act 1901* (Cth), and the *Surveillance Devices Act 2004* (Cth) (SD Act). I analyse TOLA in detail later. Here I note its essence.

1.19. *Schedule 1* is the main focus of this report. It contains amendments that enable police and intelligence agencies (but not integrity agencies) to either request or compel by notice a DCP – a term which deliberately covers a broad range of persons and companies in the communications supply chain – to provide technical assistance, thereby overcoming the problem of 'going dark', and making intelligible digital content and data.

1.20. The assistance which may be required from or agreed with a DCP is not only access to content and metadata but also technological assistance such as removing electronic protection, providing technical information, formatting information and facilitating access to devices and other *listed acts or things*.[4] Schedule 1 provides for:

a. a TAR, which is a request agreed by an agency and a DCP

b. a TAN, which is issued by an agency head

c. a TCN, which is issued by the Attorney-General with the concurrence of the Minister for Communications.

[4] Parliamentary Library, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Bills Digest No 49 of 2018–19, 3 December 2018) 6.

1.21. TARs (now being used), TANs and TCNs (not yet used but very likely to be used) cannot be specifically disclosed publicly or to DCP customers. They provide civil and criminal immunity according to their terms. There are a number of technical concepts or limits in Schedule 1, including whether a TAN or TCN is *reasonable and proportionate*, *technically feasible* or would result in a *systemic weakness or systemic vulnerability*.

1.22. The 3 most significant complaints about Schedule 1, which I largely accept as valid, concern:

a. the absence of independent authorisation for the notices

b. the inadequacy of various definitions of technical matters

c. the absence of independent technical assessment of proposed notices.

1.23. *Schedule 2* establishes powers which enable federal, State and Territory law enforcement agencies to obtain covert computer access warrants when investigating certain federal offences. It amends a number of Acts to reform the existing computer access warrants available to ASIO, introduces computer access warrants for law enforcement agencies, and establishes an avenue for foreign governments and international courts and tribunals to request assistance in accessing data via a computer access warrant.[5] Warrants are issued by the Attorney-General (for ASIO computer access warrants) or by an eligible judge or a nominated AAT member (for SD Act computer warrants requested by a law enforcement officer or on behalf of foreign governments), acting as *persona designata*.[6]

1.24. *Schedule 3* amends the existing search warrant framework under the Crimes Act to expand the ability of criminal law enforcement agencies to collect evidence from electronic devices.[7] Other amendments include authorising the adding, copying, deleting or altering of other data if that is necessary to give effect to a warrant, while making it clear a search warrant cannot authorise police to do anything likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use of a computer or cause other material loss or damage.[8] Warrants are issued by judicial officers or AAT members, acting as *persona designata* rather than as representatives of the courts or tribunals of which they are members. Further, Schedule 3 expands the scope of the Australian Federal Police's (AFP's) power to

[5] Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access Act) 2018* (2019).

[6] ASIO Act s 25A; SD Act s 27A(7).

[7] See additional powers in the Crimes Act, s 3F(2A)–(2B).

[8] Crimes Act, s 3F(2B)–(2C).

obtain an assistance order to compel an individual to provide certain information or assistance to police; and amends the criminal penalties for failing to comply with an assistance order.

1.25. *Schedule 4* amends the search warrant framework under the Customs Act to 'enhance the ability of the Australian Border Force (ABF) to collect evidence from electronic devices under warrant in person or remotely'.[9] TOLA expands the types of actions that a warrant may authorise under the Customs Act. It authorises ABF officers to search premises for evidential material in relation to a specified offence, including using electronic equipment to access 'relevant data' that is held in a computer or data storage device found during a search, to determine whether the data is evidential material of a kind specified in the warrant.[10] Similar new provisions apply as under the Crimes Act (amended by Schedule 3), including with regard to adding and copying data and remote access, material interference and increased penalties for noncompliance.[11] Approvals are the same as for Schedule 3. Further, Schedule 4 makes amendments to the ABF's power to obtain an assistance order, including by amending the criminal penalties for failing to comply with an assistance order.

1.26. *Schedule 5* provides 2 new powers or capacities to ASIO.

1.27. First, the Director-General of Security may issue a voluntary assistance request to a (legal or natural) person to engage in 'conduct' to assist ASIO in the performance of its functions (ASIO Act, s 21A(1)), and a person may volunteer to provide more limited assistance in relation to documents (ASIO Act, s 21A(5)). Where a person provides assistance requested by ASIO or volunteers assistance, immunity from civil liability ordinarily attaches to that conduct.

1.28. Secondly, at the request to the Director-General of Security the Attorney-General may issue a compulsory assistance order compelling a person to assist in accessing data held on a computer or data storage device (ASIO Act, s 34AAA).

1.29. My main concern with Schedule 5 is that s 21A provides a limited and certain capacity for assistance to be volunteered under sub-s (5) but a wider and uncertain power for ASIO to request conduct under sub-s (1). Given ASIO's other powers to obtain information and assistance, I consider it is only necessary for ASIO to have power under s 21A(1) to request what equally could be volunteered under s 21A(5).

[9] Explanatory Memorandum, p 5, para 19.

[10] TOLA Act, Sch 4, Item 4A.

[11] TOLA Act, Sch 4, Items 2, 4A, 5, 6, 7 and 18.

Key principles and findings

1.30. The stated purpose of TOLA is to amend a range of Commonwealth legislation to allow law enforcement and national security and intelligence agencies to 'better work in the increasingly complex digital environment' and 'introduce measures to better deal with the challenges posed by ubiquitous encryption'.[12] Some of the many issues raised in these notions are discussed in more detail in the chapters on technology and privacy and in the appendix summarising the detailed and helpful submissions I have received. Here I set out the key findings I have made and principles I have acted on.

The threat landscape

1.31. In assessing the necessity of the provisions of TOLA, I must consider the current threat landscape.

1.32. In previous reports, I have noted that the level of threat of a terrorist act occurring in Australia remains at 'probable', and the evidence I have considered for the present review indicates that this position remains unchanged.

1.33. This review has caused me to consider broader security and other threats to the political, commercial and societal interests of the nation. There are real threats of foreign interference in facets of our lives that we may take for granted. The extent of the use of the internet by hostile foreign states and their agents to engage in espionage and foreign interference is still not fully appreciated, partly because of the covert and disguised means these actors use in their online activity.

1.34. Because the World Wide Web and the related Internet of Things (together, the internet)[13] have a large and growing role in all aspects of life around the globe, but particularly in a technologically advanced democracy such as Australia, the threats TOLA seeks to meet extend beyond the counter-terrorism and national security activities that I normally consider as INSLM to the behaviour of criminal and other bad actors more generally.

1.35. There is an ever-present threat of criminals engaging in online activities to perpetrate general but serious crimes, such as child sexual exploitation and sophisticated frauds. The breadth of these threats is facilitated by means which are increasingly complex

[12] Telecommunications and Other Legislation Amendment (Assistance and Access Bill) 2018 (TOLA Bill), Explanatory Memorandum, p 2, para 1.

[13] Which I use in this report as encompassing the World Wide Web.

and difficult to detect. As the Minister for Home Affairs recently said, 'almost every crime type and national security concern has an online element'.[14]

1.36. To counter what is called 'going dark' by reason of encryption, agencies must adapt their techniques and laws must be updated. I am satisfied from the evidence I have received from intelligence, police and integrity agencies that encryption of content and, to a lesser extent, metadata has made their essential tasks significantly more difficult and in some instances impossible. I accept the necessity of a legislative response to 'going dark'.

Proportionality

Context

1.37. Necessity is one aspect of my review. The other is proportionality. Any legislative response to threats must be adapted, and proportionate, to the risk of them occurring. International human rights law and the INSLM Act both require consideration of proportionality and the related question of human rights protections.

1.38. What makes this review unusually challenging is not only the complexity of the law but also the technological context, which includes events that can be viewed, metaphorically, as the shifting tectonic plates of our times. As Professor Sir David Omand[15] has recently written, in terms I gratefully adopt:

> *We are living through the beginning of a revolution in human affairs enabled by the digitization of information and the means of communication through the Internet, the World Wide Web, and mobile devices (with the Internet of Things rapidly growing). We are now dependent on this technology for economic and social progress, for international economic development, and for national security and public safety. Trust has to be built both in the open Internet as a safe place to innovate, to do business, to shop, and to interact socially, and in the ability of the authorities to be able to uphold the law in cyberspace. That trust cannot be taken for granted. The Internet, and the World Wide Web that it carries, were not originally designed with security in mind, and many seek to exploit this weakness for their own antisocial, criminal, or aggressive ends. A global coincidence over the last fifteen years has shaped the rapid development*

[14] Telecommunications Legislation Amendment (International Production Orders) Bill 2020, Explanatory Memorandum (circulated by authority of the Minister for Home Affairs, the Hon Peter Dutton MP).

[15] University College London. Formerly head of Government Communications Headquarters (GCHQ) and the United Kingdom's Security and Intelligence Coordinator.

of digital intelligence and heightened ethical concerns: the post–Cold War growth in demand for information about individuals to manage the threats from terrorists (especially after 9/11), international criminals, and other individuals of concern has coincided with the ability of the Internet and Web-based technologies, developed for commercial purposes, to supply detailed data about individuals in ways never before possible. Demand for and supply of such data have been interacting dynamically, and the process continues.[16]

The internet, privacy and trust: key conclusions

1.39. Although many matters which arose in this review are open for debate, in my opinion at least the following matters are clearly established.

1.40. As the internet became indispensable to the legitimate operations of, and interactions between, governments, corporations and other organisations, and individuals, it was also used by criminals and other bad actors for their illicit purposes.

1.41. The internet was not designed with security in mind. To remedy this inherent weakness, widespread data content encryption and, to an increasing extent, metadata encryption has been used. Encryption seeks to maintain general confidence in the security of the internet. It is not only appropriate but also essential that it seeks to provide effective security and protection for:

a. internet communications and transactions

b. government, commercial and private data

c. the maintenance of legitimate personal rights to privacy, and its near relative, anonymity.

1.42. *Privacy* can be an elusive concept and each legal jurisdiction has its own approach. Thus:

a. international law recognises a right to privacy, while giving some leeway to nation states in how they respond

b. European Union (EU) law enables the right to be forgotten

c. the 4th Amendment to the *Constitution of the United States* is of significance to Australia in obtaining mutual assistance for the purposes of intelligence and countering crime

[16] Sir David Omand and Mark Phythian, *Principled Spying: The Ethics of Secret Intelligence*, (Georgetown University Press, 2018) Ch 5.

d. although Australia has enacted the *Privacy Act 1988* (Cth), neither the Constitution nor the common law of Australia recognises a specific right to privacy. Instead, the common law mainly protects privacy through the requirement that, absent consent, there must be a legal basis for interference with personal property.

1.43. In particular, Australia has inherited from English law and still maintains:

a. *a common law rule* that holders of public office can only seize or access private property as authorised by law

b. *the historically entrenched practice* that this is typically done by warrant, issued by persons independent of the agency which seeks to exercise the warrant.[17]

1.44. This rule:

a. applies to accessing and copying data content and metadata on personal devices such as computers and mobile phones, just as much as it does to searches of people or premises

b. has rightly been said to recognise the 'link between protection of personal property and protection of freedom of thought and political expression'[18]

c. as it states a fundamental right, is protected by the principle of legality, so that a statute which seeks to overcome it will only be effective in doing so by clear statement of intent or by necessary implication.

1.45. With rare exceptions – most notably, some ASIO warrants issued by the Attorney-General[19] – independent serving judges and tribunal members issue these warrants to executive agencies and police in Australia. They act in a personal capacity, '*persona designata*', rather than exercising power as the court or tribunal to which each belongs. This practice is rightly seen as a vital democratic safeguard in Australia – so much so that departing from it requires justification.

1.46. Pre-TOLA, coercive statutory powers for access to intelligible data content and metadata were heavily relied on by intelligence, police and integrity agencies. (I

[17] *Smethurst v Commissioner of Police* [2020] HCA 14 [23] (Kiefel CJ; Bell and Keane JJ): 'The power to search has always been regarded as an exceptional power, to be exercised only under certain justifying conditions. One essential condition, found in statutes authorising the issue of warrants for search and seizure, both Commonwealth and State and Territory, is that the object of the search be specified by reference to a particular offence.'

[18] Ibid [155] (Gageler J, citing Lord Camden in *Entick v Carrington* (1765) 19 St Tr 1029).

[19] Leaving aside warrants issued as part of the judicial function.

should note that I do not generally see it as my role in this review to revisit the justification for such powers, many of which have operated for some time.) As encryption steadily deprived them of this access, the effectiveness of those powers diminished. A key justification put forward for TOLA is that it will reverse this trend.

1.47. A fundamental principle guiding me in this review is that, just as we do not accept lawlessness in the physical world, we should not accept lawlessness in the virtual world. Therefore, in principle, the surveillance powers that apply in the physical world should also apply to the virtual world unless there are good reasons that they should not.

1.48. In this report, I apply this fundamental principle together with a *companion principle* – that of 'trust but verify', which I have adopted from *A Question of Trust* as the theme of this work. The companion principle is that in the sceptical world in which Australian democracy operates:

> *trust depends on verification rather than reputation, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency.*[20]

1.49. In this report I reject the notion that there is a binary choice that must be made between the effectiveness of agencies' surveillance powers in the digital age on the one hand and the security of the internet on the other. Rather, I conclude that what is necessary is a law which allows agencies to meet technological challenges, such as those caused by encryption, but in a proportionate way and with proper rights protection. Essentially this can be done by updating traditional safeguards to meet those same technological challenges – notably, those who are trusted to authorise intrusive search and surveillance powers must be able to understand the technological context in which those powers operate, and their consequences. If, but only if, the key recommendations I set out in this report in this regard are adopted, TOLA will be such a law.

Safeguards updated for new technology

1.50. My UK counterpart, Jonathan Hall QC, in his most recent report[21] has rightly written of terrorism legislation:

---

[20] David Anderson QC, Independent Reviewer of Terrorism Legislation, *A Question of Trust: Report of the Investigatory Powers Review* (UK Government, London, 2015) [246]

[21] Jonathan Hall QC, Independent Reviewer of Terrorism Legislation, *The Terrorism Acts In 2018: Report of the Independent Reviewer of Terrorism Legislation on the Operation of the Terrorism Acts 2000 and 2006* (UK Government, 2020)

[2.30] Modern technology calls into question legislation written in an earlier era, and terrorism legislation is no exception. Interrogating a phone can reveal more data than searching a house; information is electronic, and accessed, rather than physical, and seized; contact is encrypted and routed around the world; worldwide publication is open to every person with a smartphone.

1.51. The same holds true for TOLA, whose scope and purpose extends well beyond countering terrorism. Take the familiar example of the personal mobile phone/device, which:

a. is an essential aspect of modern life: its use is not really optional for anyone seeking to fully participate in Australian life

b. amalgamates the functions that were once performed by several devices: telephone, address book, calendar, emails, internet browser, camera, video camera, calculator, thermometer, pedometer, heart monitor, dictaphone and more

c. is a 'data rich' environment – it contains not only an unprecedented amount of data content that its user may be broadly aware of but also highly revealing metadata about the user's movements, communications and thoughts that the user may be unaware of and, in some cases, is not capable of being aware of

d. is the paradigm example of monetisation of our personal data, usually with our technical consent but rarely, if ever, with our informed consent

e. when its contents are revealed, can be devastating for the user's privacy. As the US Supreme Court recently said of movement metadata of one man due to his phone's tracking capacity, it was 'revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations"'.

1.52. DCPs are able to analyse and then profit from personal and commercial information that we reveal when we use the web – for example, they can 'data mine' using proprietary algorithms. This has resulted in some 'tech titan' DCPs having enormous (although opaque) power that is in some ways greater than many nation states.

1.53. All of that information, frequently unknown and even unknowable to the user of a mobile but entirely new in its size, scope and type, if it is available to a DCP, is available to the Government and its agencies if there is a law permitting intelligible access (if that is technically possible). TOLA is such a law.

<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2020/03/Terrorism-Acts-in-2018-Report.pdf>.

Schedule 1

A double-lock for TANs and TCNs – a proportionate and more technically sound decision-making process

1.54. In relation to Schedule 1, for the reasons set out in greater detail in the report, TANs and TCNs should be authorised by a body which is independent of the issuing agency or government. These are powers designed to compel a DCP to reveal private information or data of its customers and therefore the usual practice of independent authorisation should apply.

1.55. I reject the argument advanced by agencies that 'a key safeguard in Schedule 1 powers is that they cannot authorise access to data', access being granted by separate warrant issued by a tribunal member or judge. This argument elevates form over substance; after all, Schedule 1 states that its purpose is to reverse the effect of going dark by making intelligible or otherwise useful the content of data already, or in future to be, accessed by warrant. Having accepted that as a key justification in the context of necessity, I cannot ignore it when considering proportionality and rights protection.

1.56. A key safeguard in Schedule 1 is the general limitation that TANs and TCNs must be reasonable and proportionate. The factors to be weighed up in making that decision are comprehensive and, appropriately, cover such key issues as the interests of the issuing agency and the DCP, the necessity and objectives of the notice, its impact on third parties, the availability of other means to achieve the objectives of the notice, and the legitimate expectations of the Australian community relating to privacy and cybersecurity. But those factors should be weighed up by someone independent of the Government or the agency. That should also be so when determining whether complying with the notice is not 'practicable', not 'technically feasible' or would create a 'systemic weakness' or 'systemic vulnerability'.

1.57. I accept that the decision-makers under TOLA (be they agency heads or the Attorney-General) will receive advice on technical matters, but the real question is one of independence and the appearance of it. This independence engenders the necessary trust in the minds of members of the public that the powers are being exercised in a manner that is no more than is necessary. A proper appreciation of the impact of an intrusive TOLA power depends upon the issuer being independent of the agency concerned and, importantly, having technical knowledge. The powers under TOLA cannot be exercised, let alone their impact understood, in the absence of independent technical expertise.

1.58. It was a consistent and, indeed, unanimous theme across non-government submissions that TANs and TCNs should be authorised by either an independent tribunal member or a judicial officer with the benefit of expert technical advice. A

number of submissions drew upon the UK's double-lock model of judicial authorisation which, as I explain later, involves an independent exercise of decision-making with the assistance of technical advisers.

1.59. Law enforcement agencies, intelligence agencies and the Department of Home Affairs submitted that TOLA already contains safeguards as to independence and technical advice.

1.60. The desirability of a decision-maker independent of the executive and its agencies is recognised in the Government's Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (IPO Bill), which is a critical step that enables Australia to seek a bilateral agreement with the US under their *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act). The IPO Bill would enable Australia to give effect to such a bilateral agreement by creating a new international production order framework that allows Australian law enforcement and intelligence/security agencies to issue or obtain extraterritorial orders for electronic data on foreign DCPs (where there is an agreement in place).

1.61. Under the regime proposed under the IPO Bill, the Director-General of Security, a Deputy Director-General or ASIO employee may approve an application for an International Production Order (IPO), which then goes to the Attorney-General for consent, after which the application is sent to a nominated member of the Security Division of the AAT to approve *persona designata*. In view of the extensive powers already conferred upon the AAT, the mechanisms outlined in the IPO Bill and the other conclusions I have come to, I recommend the following:

a. A new statutory office – the IPC – should be created to monitor the operation of the system of TANs and TCNs. The IPC should be a retired judge of the Federal Court or the Supreme Court of a State or Territory. The IPC would be appointed by the Governor-General, on the advice of the Attorney-General, following mandatory consultation on the appointment with the Leader of the Opposition.

b. The IPC should be 'dual hatted' – the Commissioner should be appointed as a part-time Deputy President within the AAT and designated as the head of a new Investigatory Powers Division (IPD) of the AAT, with powers and procedures based upon the existing Security Division. One of the first tasks of the IPC, following wide consultations with interested persons, would be to recommend in detail how that system should work.

c. The IPC would be required to concur in the appointment by the Governor-General of a suitable number of eminent, independent technical experts who would also be assigned to the new IPD as part-time Senior Members.

d. On the advice of the technical advisers, the IPC would approve and, where necessary, conduct hearings concerning TANs and TCNs.

e. There should also be a registrar of the new IPD who would ensure proper protection of sensitive and classified material.

f. In order to encourage industry support, there should be consultation with industry groups as to who should be appointed to these roles.

g. To promote the interests of transparency and accountability, the IPC would provide the Attorney-General and the PJCIS with an annual report on the operation of Schedule 1 and any other functions that are later conferred upon the IPC and the IPD. There should be the capacity to provide a classified annexure to these reports as necessary.

No change to TARs

1.62. For the reasons I give later in this report, I do not consider that there is any need to alter the present arrangements relating to TARs (except to recommend that a prescribed form be used). The TAR is not a coercive instrument. A DCP may freely choose to comply or not comply with a TAR without any legal consequence.

Extension to integrity and anti-corruption agencies

1.63. Integrity and anti-corruption agencies should have the same access to Schedule 1 TOLA powers as police do. These agencies are already empowered under other legislative schemes to exercise various investigative powers.

The definitions of 'systemic weakness' and 'systemic vulnerability'

1.64. I have been persuaded that the definitions of 'systemic weakness' and 'systemic vulnerability' are overlapping, create confusion and are not fit for purpose.

1.65. There is little difference conceptually, or in normal or technical usage, between a 'systemic weakness' and 'systemic vulnerability'. These terms are already used interchangeably in industry and public discourse; there is no further need to use both in the TOLA.

1.66. I have made other recommendations to amend the definition of 'systemic weakness' to bring it into line with the many helpful submissions I received from industry as to the application of those definitions to the technologies at hand. I am satisfied that these amendments, when considered and applied by the IPC, with the assistance of technical advisers, will best ensure that the integrity of the technology and systems used by DCPs is not compromised or the effects limited.

Schedule 2

1.67. I am satisfied that the computer access warrant and associated powers conferred by Schedule 2 are both necessary and proportionate, subject to some amendments.

1.68. I am satisfied that agencies should retain the power to engage in telecommunications interception for the purposes of a computer access warrant without being required to obtain a separate warrant under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) authorising that interception.

1.69. However, to the extent that computer access warrants permit steps to be taken to conceal the activities of the agency in accessing the relevant computers outside of a 28-day period following the expiry of the warrant, I consider that the agency should be required to obtain external approval for those steps. These warrants authorise actual, or potentially significant, incursions into privacy and property, whether it is in the accessing of the computer or the premises on which the computer is located. The decision-maker should be given the opportunity to consider and approve the steps that the agency proposes to use to conceal its activities where they occur a month or more after the warrant has expired.

1.70. To the extent that a computer needs to be removed, I do not consider it a satisfactory limitation that the computer be returned 'within a reasonable period'.[22] Instead, I recommend the item's return 'as soon as is reasonably practicable'.

Schedules 3 and 4

1.71. I am generally satisfied that the powers conferred by Schedules 3 and 4 are both necessary and proportionate, but there are some matters that should be addressed and further monitored.

1.72. It should be declared that the powers under Schedules 3 and 4 do not authorise the detention of a person to whom the order applies *where the agency in question does not otherwise have any lawful basis on which to do this.* A simple statutory recognition of this would go a long way toward appeasing fears frequently expressed to me.

1.73. I note that Schedules 3 and 4 introduce significant new offences and increase the penalties for noncompliance with an assistance order. The introduction of a monetary penalty as an alternative to imprisonment appears to be an appropriate and proportionate addition, but I consider it appropriate that the prospect of imprisonment for the new offences remains. Despite some concerns about the broadening of offences and increases in penalties, I accept the necessity and proportionality of the increase in criminal penalties for failure to comply with an assistance order and of the introduction of aggravated offences in relation to the

[22] ASIO Act ss 25A(4A), 27E(3A); see also *Surveillance Devices Act 2004* (Cth) s 27E(2A). Where the computer access warrant has been obtained by ASIO, this is subject to a situation in which the return of the item would be prejudicial to security. Where that is the case, it is permissible to retain the item until it is no longer the case.

more general offences. However, I do recommend that agencies and external stakeholders continue to monitor any prosecutions or penalties.

Schedule 5

1.74. I have concluded that Schedule 5 should be amended to limit its breadth and clarify its scope.

1.75. Section 21A(1) of the ASIO Act empowers the Director-General of Security to 'request a person or body to engage in conduct' that assists ASIO. In my view, as 'conduct' is undefined, it may operate too broadly and, as so drafted, has not been shown to be necessary. I recommend that s 21A(1) be limited to the types of voluntary assistance that are specified in s 21A(5).

1.76. Several stakeholders submitted that the powers conferred on the Director-General of Security under s 21A(1) represent a significant step, as previously the power to confer immunity from civil liability on a person assisting ASIO was limited to the Attorney-General.[23] That function may be further sub-delegated to a 'senior position-holder' under s 16A of the ASIO Act, and I recommend that this power be exercised by an officer now not lower than a Deputy Director-General.

1.77. The legislation is silent on the interaction between the new powers introduced in Schedules 1 and 5. The power to issue a TAR, includes a number of important safeguards and it is necessary to make clear that s 21A does not empower the Director-General to circumvent those protections by making the request under s 21A instead.

1.78. Submitters raised the question of whether a person subject to an assistance order (under s 34AAA) is effectively being detained during the period in which they are required to provide the assistance, by being effectively prevented from leaving a specified place prior to the completion of the designated assistance task, under pain of criminal penalties. The Director-General of Security expressly rejected this proposition and the AFP likened its s 3LA power to other powers that compel production or attendance, including production orders, summonses and subpoenas. I am comforted by the agencies' clear assurances on this matter and therefore do not recommend amendments to introduce protections for a person under detention. I still consider it necessary to make it clear, in the ASIO Act, that an assistance order under s 34AAA does not authorise detention of a person to whom this order applies.

[23] See IGIS submission

Reporting and record-keeping and own motion review powers

1.79. In a number of respects the TOLA reforms fail to provide for adequate, or sometimes any, reporting or record-keeping. Trust is essential to the exercise of the powers conferred by TOLA and the public's acceptance of them. Trust is eroded where the public has inadequate insight into or knowledge of the exercise of the powers. While confidential and sensitive information must be appropriately protected, that is not a licence to keep all such information from the public if it can be conveyed within limits.

1.80. Finally, my successors should be able, of their own motion, to revisit these complex and important matters when they consider it necessary, and the INSLM Act should be amended accordingly.

SUMMARY OF RECOMMENDATIONS

Schedule 1

Recommendation 1

I recommend that State and Territory anti-corruption commissions be given power to agree to or apply for all 3 types of industry assistance notice – that is, TARs, TANs and TCNs. This power should also be given to the foreshadowed Commonwealth Integrity Commission, when and if it is established.

Recommendation 2

I recommend no change to the capacity of the relevant agencies and a DCP to freely agree a TAR with each other, other than that a prescribed form be used.

Recommendation 3

I recommend that the powers of approval of TANs and TCNs, presently vested in agency heads (for TANs) and the Attorney-General (for TCNs), instead be vested in the AAT and assigned to a new Investigatory Powers Division (IPD). The new IPD, building on the powers and procedures in the Security Division, would operate in a similar way to protect classified material of agencies that are applying for TANs and TCNs and the commercial-in-confidence material of DCPs that are resisting the issue of those notices. The IPD should be able to sit in private as necessary. It would be able to utilise existing AAT powers and procedures, including alternative dispute resolution, to decide for itself whether to issue a TAN or TCN. It would hear submissions and receive evidence from the applying agency and the DCP and be in a position to promptly determine technical questions, such as whether a notice is practicable, reasonable and proportionate or would create a systemic weakness. The Attorney-General's approval would be required for a federal agency to lodge an application for a TCN with the AAT, but this should not be required for any State or Territory body or the Commonwealth Integrity Commission, if and when it is established.

Recommendation 4

I recommend that the IPD consist of a new part-time Deputy President, who would also be the Investigatory Powers Commissioner (IPC), and other eminent lawyers and technical experts as needed. So that they can build up the necessary specialised expertise, and because these powers will not be exercised ex parte, the exercise of these powers should *not* be *persona designata*.

Recommendation 5

I recommend the creation of the IPC as a new statutory office holder, whose functions would be:

a. monitoring the operation of TOLA Schedule 1, including by sharing information with other oversight bodies (such as the Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman) and reporting annually on its operation to the Attorney-General and the PJCIS

b. as an additional, part-time Deputy President of the AAT, taking part in the issue of TANs and TCNs as head of the IPD

c. concurring in the appointment of other part-time technical and legal decision-makers assigned to the new IPD who will also be able to assist the IPC in the monitoring roles

d. developing and approving the prescribed form for TAR, TAN and TCN applications and issuing guidelines

e. with the concurrence of the AAT President, issuing practice notes for the IPD.

Recommendation 6

In recognition of the importance of the IPC and the need for the role to be, and be seen to be, filled by someone who is independent of government, is eminent in the law and its application, enjoys bi-partisan support and is not diverted by judicial duties, I recommend that the IPC be a retired judge of the Federal Court or the Supreme Court of a State or Territory, appointed by the Governor-General, on the advice of the Attorney-General, following mandatory consultation on the appointment with the Leader of the Opposition. I would expect there would also be consultation with industry, but I would not mandate it.

Recommendation 7

I recommend amending the definitions in TOLA of 'serious Australian offence' and 'serious foreign offence' so that they align with the definition in existing s 5D of the TIA Act. The effect of this is that, by and large, it would not be open to an agency to obtain an industry assistance notice in respect of an offence punishable by only 3 years' imprisonment.

Recommendation 8

As to *systemic weakness and vulnerability*, I recommend removing all references to 'systemic vulnerability' in Schedule 1, as it is redundant.

Recommendation 9

I recommend that s 317ZG(4A) state prohibited effects as follows:

(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in sub-s (1)(a) to implement or build a systemic weakness into a form of electronic protection means a reference to any act or thing that creates a material risk that otherwise secure information will be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party.

I further recommend the introduction of the following definitions:

a. 'Otherwise secure information' means 'information of, any person who is not the subject, or is not communicating with the subject, of an investigation'.

b. 'Unauthorised third party' means 'anyone other than a party to the communication, the agency requesting the relevant TAR, TAN or TCN and/or integrity agencies'.

Recommendation 10

I recommend clarification of definitions through the use of non-exhaustive statutory examples:

a. Clarify that 'target technology' in s 317B refers to the specific instance used by the intended target.

b. Include non-exhaustive examples of what is excluded from the meaning of 'electronic protection' in s 317B.

Recommendation 11

I recommend that a 'Designated Communications Provider' not be taken to include a natural person (where that natural person is an employee of a DCP) but only apply to natural persons insofar as required to capture sole traders.

Recommendation 12

I recommend that the AFP no longer have any role in the consideration of industry assistance notices requested by or issued on behalf of State and Territory police.

Schedules 2, 3 and 4

Recommendation 13

I recommend that agencies retain the power to engage in limited telecommunications interception, for the purposes of a computer access warrant, without the need to obtain a separate warrant under the TIA Act authorising that interception.

Recommendation 14

I recommend that an agency be required to seek external authorisation to exercise a concealment of access power if it proposes to take that step more than 28 days after the warrant has expired.

Recommendation 15

I recommend that the legislation be amended to require that a computer or thing which is removed from warrant premises during the execution of a computer access warrant (or related authorisation) be returned to warrant premises if returning the computer or thing is no longer prejudicial to security or, otherwise, as soon as is it reasonably practicable to do so.

Recommendation 16

I recommend that agencies and external stakeholders continue to monitor the prosecutions and convictions (to the extent that information is made publicly available) so as to permit any trends to be discerned as more time passes.

Recommendation 17

I recommend that both s 3LA of the Crimes Act and s 201A of the Customs Act be amended to state, for the avoidance of doubt, that neither authorises the detention of a person to whom the order applies where the agency in question does not otherwise have any lawful basis to detain the person.

Recommendation 18

I recommend that a monetary penalty be retained as an alternative to a penalty of imprisonment for failing to comply with an industry assistance order.

Schedule 5

Recommendation 19

I recommend that the power to request conduct in s 21A(1) be limited in scope to the conduct which can be volunteered under s 21A(5).

Recommendation 20

I recommend that s 21A(1)(e) and s 21A(5)(e) be amended to confine the scope of that immunity from civil liability by requiring instead that 'the conduct does not result in *serious personal injury or death to any person or* significant loss of, or serious damage to, property' (emphasis added).

Recommendation 21

I recommend that s 21A arrangements be approved by the Director-General of Security or a Deputy Director-General.

Recommendation 22

I recommend that s 21A of the ASIO Act be amended to make clear that nothing in s 21A authorises the Director-General of Security to make a request of a person that is properly the subject of a TAR.

Recommendation 23

I recommend that the ASIO Act be amended so as to expressly state, for the avoidance of doubt, that the power does not authorise the detention of a person to whom the order applies where ASIO does not otherwise have any lawful basis on which to do this.

INSLM Act

Recommendation 24

I recommend that the definition of 'counter-terrorism and national security legislation' in s 4 of the INSLM Act be amended to include TOLA so that future INSLMs may review it of their own motion as necessary.

Reporting, disclosure and oversight

Recommendation 25

I recommend that relevant agencies keep a record of the number of assistance orders that are executed and provide them annually to the IPC.

Recommendation 26

I recommend that the various assistance order provisions be amended to mandate that the agency in question report to its oversight agency (such as the Commonwealth Ombudsman or the IGIS) as to the number of assistance orders that it executes each year and, other than for ASIO, publish those figures in the public annual reports of the relevant agencies and the oversight bodies. I recommend that statistics on the use of TOLA powers, including a broad description of the acts or things implemented, be made public annually by the IPC (tabled in Parliament within 15 sitting days of receipt) provided that publication would not reveal operationally sensitive or classified information.

Recommendation 27

I recommend that agencies be required to keep records of the number of requests they make of carriers or carriage service providers under s 313 of the Telecommunications Act and to report on those matters annually to the IPC.

Recommendation 28

I recommend that the capacity of the Commonwealth Ombudsman to undertake a joint investigation with State Ombudsman or Independent Commission Against Corruption oversight bodies such as Inspectors-General be made explicit within s 317ZRB of the Telecommunications Act.

Recommendation 29

As to the Ombudsman's powers of reporting, I recommend that s 317ZRB(7) be repealed so that the Minister cannot remove material from an Ombudsman report under that provision.

Recommendation 30

I recommend that Commonwealth officials be authorised to disclose TAR/TAN/TCN information to the public and to State, Territory and Commonwealth officials when that disclosure is in the national or public interest. A decision to disclose based on those factors may be made by the relevant agency or departmental head or the relevant minister.

Recommendation 31

I recommend that the information disclosure provisions be amended so as to permit DCPs to obtain not merely legal advice but also technical advice in relation to requests or potential request of TARs and issue or potential issue of TANs and TCNs.

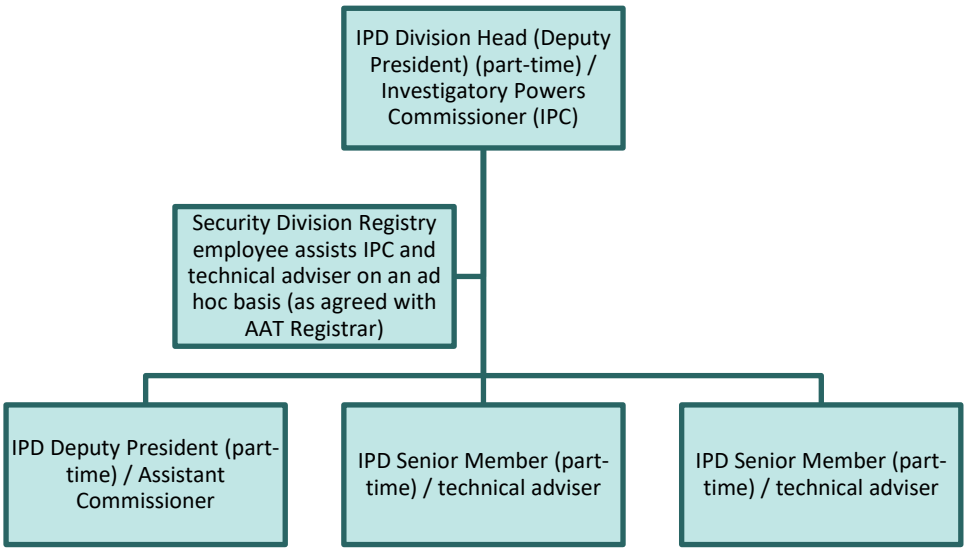
Recommendation 32

As to Schedules 3 and 4, I recommend that there is no need to keep any record of any assistance order that an agency issues but which is ultimately not executed.

Recommendation 33

I recommend that ASIO's exercise of powers under Schedule 5 be detailed in its annual report (in a classified appendix as necessary) and that this information be provided to the PJCIS, the Leader of the Opposition, the IGIS, the INSLM, the Attorney-General and the Minister for Home Affairs.

Phase 1 of the operation of the Investigatory Powers Division (IPD) of the AAT



INVESTIGATORY POWERS DIVISION

Appointees to the Investigatory Powers Division of the AAT (non-exhaustive functions)

Investigatory Powers Commissioner (IPC)

- Issues guidelines on the procedures of the IPD (in concurrence with the AAT President)
- Creates prescribed forms for TAN and TCN applications (must be used by interception agencies)
- Consults with oversight and integrity bodies (including the IGIS, the Integrity Commissioner, the Commonwealth Ombudsman and State and Territory anti-corruption bodies) on interception agencies' use of TOLA powers
- May attend audits/inspections of interception agencies' premises/records in relation to the agencies' use of TOLA powers

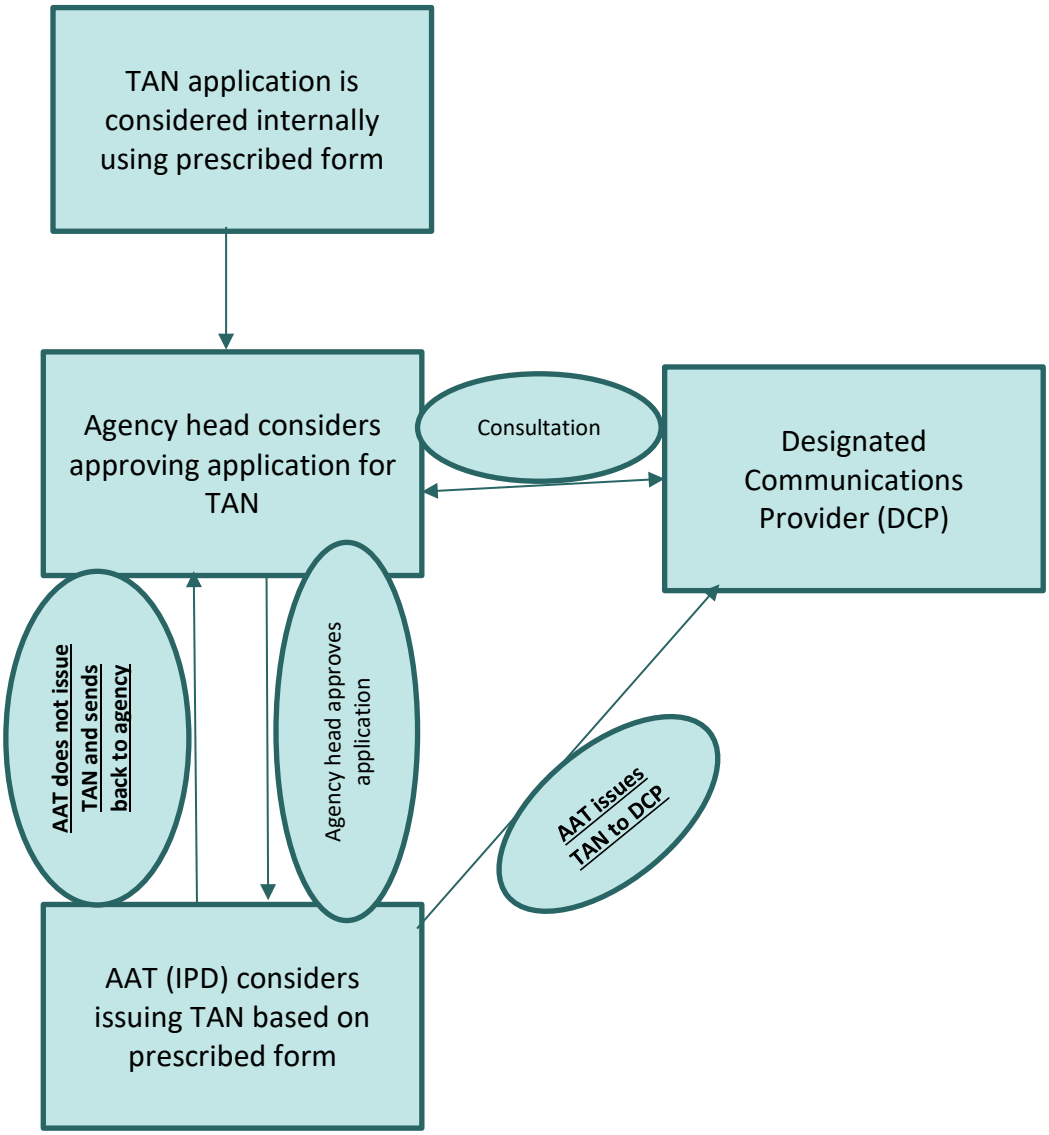
Assistant Commissioner

- May advise the IPC on appropriate guidelines for procedures of the IPD
- May advise the IPC on content and format of prescribed forms for TAN and TCN applications
- May consult with oversight and integrity bodies (including the IGIS, the Integrity Commissioner, the Commonwealth Ombudsman and State and Territory anti-corruption bodies) on interception agencies' use of TOLA powers
- May attend audits/inspections of interception agencies' premises/records in relation to the agencies' use of TOLA powers

Technical adviser

- May provide technical advice to the IPC on appropriate guidelines for procedures of the IPD
- May advise the IPC and Assistant Commissioners on content and format of prescribed forms for TAN and TCN applications
- May consult with oversight and integrity bodies (including the IGIS, the Integrity Commissioner, the Commonwealth Ombudsman and State and Territory anti-corruption bodies) on interception agencies' use of TOLA powers, including on request from an oversight or integrity body head
- May attend audits/inspections of interception agencies' premises/records in relation to the agencies' use of TOLA powers

New process for Technical Assistance Notices (TANs)



New process for Technical Capability Notices (TCNs)