Australian Government

Department of Home Affairs

THE ASSISTANCE AND ACCESS ACT ADMINISTRATIVE GUIDANCE

ISSUES PAPER

Purpose of this document

This issues paper has been circulated to representative members of industry with a clear interest in the development and implementation of the new industry assistance framework within Part 15 of the *Telecommunications Act 1997* (Telecommunications Act). Part 15 was introduced by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Assistance and Access Act) which received royal assent and came into effect on 8 December 2018.

The paper briefly outlines the operation of the legislation before asking questions to assist the Department of Home Affairs (the Department) in the preparation of formal guidance for implementation of the framework. The final guidelines will establish the administrative processes that structure requests for technical assistance between Commonwealth, State and Territory law enforcement and security agencies and the broader Australian communications industry.

The below questions are grouped by theme. They are not exhaustive and the Department is interested in further feedback on matters that will aid implementation of the scheme. Guidance material will also continue to take into account the matters suitable for administrative guidance that were suggested in private and public submissions to the Department as well as issues raised with the Parliamentary Joint Committee on Intelligence and Security.

About the legislation

Schedule 1 of the Assistance and Access Act introduced Part 15 of the Telecommunications Act which modernises the framework for law enforcement and security agencies with existing interception, surveillance and search warrant powers to seek assistance from industry critical to the supply of communications within Australia. The framework allows agencies to seek industry assistance to effectively operate in the digital era.

Specifically, the laws established three new vehicles for industry assistance:

- **Technical Assistance Requests (TAR)** allow agencies to request voluntary assistance from providers
- **Technical Assistance Notices (TAN)** allow agencies to require a provider give assistance within their existing capabilities, and
- **Technical Capability Notices (TCN)** allow the Attorney-General and Minister for Communications to require that a provider build a new capability.

As outlined in **section 317ZK**, any assistance, by default, is cost recoverable. Commercial terms are also available in suitable circumstances. This could include, for example, where a provider needs to deprioritise commercial contracts to meet requirements. Providers who assist receive civil and criminal immunities for actions related to the assistance.

The exercise of these powers requires extensive consultation with the affected provider. They are designed to ensure that agencies can work together with industry to identify the most practical, secure and proportionate means to meet critical law enforcement and national security objectives. By law, the interests of industry, cybersecurity and privacy are central considerations under new Part 15. **Section 317ZH** ensures that access to personal information remains subject to underlying authority, such as a judicial warrant.

Interaction with the *Telecommunications (Interception and Access) Act* (TIA Act)

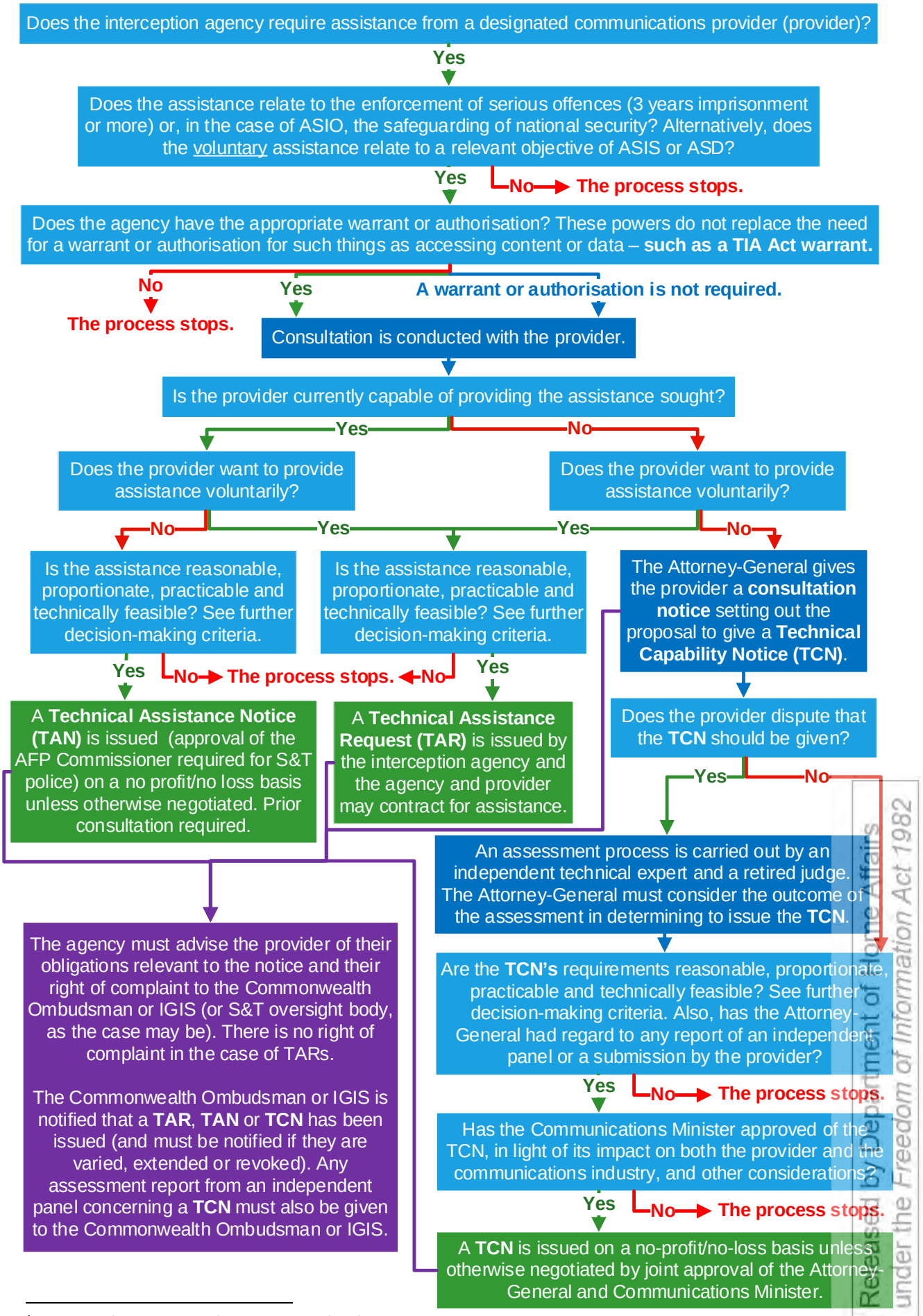
The law enforcement and intelligence communities rely on a range of warrants and authorisations to access the data and communications of the individuals they investigate – many of which belong to the TIA Act. The TIA Act is, first and foremost, a law that prohibits unlawful interception and access to communications. Exceptions to this prohibition are available in the form of independently approved warrants and provisions that authorise the disclosure of information. To exercise the powers in the TIA Act agencies must meet significant thresholds.

To date, agencies have primarily relied on the assistance of carriers and carriage service providers to execute some of the powers in the TIA Act and other Commonwealth legislation. However, these traditional communications providers are now just one of many entities critical to the supply and flow of communications. Today, application providers, device manufacturers and technology companies are integral participants in Australia's modern communications market. These providers are well-placed to enable the lawful access to communications that has always been permitted by key Australian law enforcement and security agencies through such regimes as the TIA Act but is increasingly challenging as the communications environment and technology evolves. Importantly, while the restrictions and exceptions under the TIA Act and other legislation will continue to apply to Australian agencies, the scope of the warrant regimes do not extend to these newer players.

The Assistance and Access Act's industry assistance powers formalise the relationship between Australian agencies and the broader communications industry. They do not replace the TIA Act regime or provide a new basis for interception. Instead, the Assistance and Access Act allows agencies to seek help directly from the providers who constitute the modern communications market, including with the exercise of existing warranted powers. In addition, industry assistance is flexible enough to be used to provide agencies with a broader range of technical assistance that is not connected to a warrant or authorisation, and does not require any additional lawful authority. An example of this is asking for technical information regarding a provider's systems that will assist the agency to builder their own, indigenous capabilities.

An outline of the **industry assistance process** is on the next page.

The Industry Assistance Process[1]



[1] ASIS and ASD are only empowered to issue TARs.

Safeguards and Limitations

There are a number of key limitations located throughout Part 15 of the Telecommunications Act. Some key safeguards are contained within **Division 7** of the Part. These include:

1. Requirements and requests must not contravene the prohibition against building or implementing systemic weaknesses or vulnerabilities **– section 317ZG**

2. A TAR, TAN or TCN must not be used to do things for which the requesting agency would otherwise require a warrant or authorisation **– section 317ZH**, and

3. (For a TCN) New capabilities must not require the construction of interception capabilities or data retention capabilities **– section 317ZGA**.

The **prohibition against systemic weakness** ('backdoors') was clarified and strengthened following the December 2018 review by the Parliamentary Joint Committee on Intelligence and Security.

Section 317B defines a systemic weakness/vulnerability as 'a weakness/vulnerability' that affects a *whole class* of technology…'. The term 'class of technology' is deliberately broad and captures general items of technology across and within a category of product. It encompasses all products which share similar functional attributes. For example, mobile communications technology, a particular model of mobile phone, a particular type of operating system within that phone or a particular type of software installed on an operating system. The wide scope is intended to protect the services and devices used by the general public and business community.

New **subsections 317ZG(4A), (4B)** and **(4C**) make clear that even requirements to assist suitably targeted and authorised agency activities must not have the inadvertent effect of weakening information security. That is, industry **cannot be asked to do things that would be likely to create a material risk of unauthorised access** to the information of an unrelated party. This ensures the privacy enjoyed by innocent parties remains unimpeached.

To attain third-party verification that legal protections are not being circumvented (and that requirements are otherwise reasonable, proportionate, practical technically feasible) industry may ask the Attorney-General to refer any requirements to build a new capability under a proposed TCN for review by a technical expert and a retired senior judge. The findings of this **assessment panel** must be considered by the Attorney-General and are highly influential. The issuing of a TCN also requires approval from the Minister of Communications.

Decision-makers must be satisfied that a TAR, TAN or TCN is **reasonable**, **proportionate, practical** and **technically feasible**. These decisions, by law, include consideration of industry interests, necessity, privacy, cyber security and intrusiveness. In addition to mandatory consultation, this ensures any representations of industry are taken into account.

Industry may also apply for **judicial review** of these executive decisions as an inherent part of the Australian legal system and, in the case of TCNs, may raise any perceived failure to consider the independent panel's findings as one grounds for this review.

The powers **do not replace the need for a warrant or authorisation** if the agency would currently require one. That is, interception of communications, access to metadata or search powers still require existing thresholds to be met. Further, providers **cannot be compelled to build interception, data retention or decryption capabilit**y (or build anything that removes a form of electronic protection, like encryption).

Key Questions for Industry

Concepts and capabilities

Part 15 of the Telecommunications Act introduces new concepts that set the conditions under which cooperation between industry and government is to occur. While these concepts are designed to be technologically agnostic, it is useful to agencies to hear how these ideas are received and understood in the context of live systems. It is also useful to understand provider capabilities to allow for informed, and reasonable, requests for assistance.

1. The legislation prohibits agencies requesting or requiring providers to implement or build backdoors into their technology (see **section 317ZG**). This is expressed as a prohibition against 'systemic weaknesses'.
   - **Q 1.1: How should agencies frame requests to you, or industry more broadly, to avoid conflicts with this limitation?**
   - **Q 1.2: What practical non-legislative undertakings would provide additional assurance to your suppliers, users or customers that your products remain secure?**
   - **Q 1.3: What other guidance would you like regarding these limitations?**
2. The legislation distinguishes between a provider's present capabilities and capabilities that would need to be requested to be built anew.
   As noted by Telstra's submission to the legislation's public consultation:

> **"…there would be cases where even if it does not currently have a relevant technical capability, the [provider] may still arguably be capable of developing that capability in terms of knowledge and resources." Page 5**

   - **Q 2.1: How should a provider's existing 'capability' be determined?**
   - **Q 2.2: Before the formal consultation for a TAN or TCN, would you like the opportunity to set out information about your present capabilities to the decision-maker?**
3. To ensure that agencies request assistance at the most appropriate, effective and least onerous point within the supply chain, large and small providers may be requested to provide assistance. As noted in the joint submission by the Communications Alliance, the Australian Information Industry Association and the Australian Mobile Telecommunications Association, guidance should inform:

> **"how a [provider's] size and ability with the obligations are to be assessed." Page 12**

   - **Q 3.1: What additional information (if any), should be provided to smaller as opposed to larger providers?**
   - **Q 3.2: How would you expect Government to distinguish between providers? (Capital, gross profit, staffing levels, market share etc…)**

Consultation procedures

The use of Part 15 relies heavily on agency consultation with providers to operate successfully. Consultation will determine if an instrument is necessary, and is needed to inform the most suitable instrument for assistance.

4. Consultation with providers is a precondition to using compulsive powers and is expected to be required to meet legal thresholds for voluntary assistance. Industry feedback is important to determine how best industry can assist in the circumstances (if at all).
   - **Q 4.1: How would you like to be alerted to an upcoming request for assistance? Before any notice or request is issued, would you prefer to be approached through a formalised process or on an ad-hoc basis?**

- **Q 4.2: How would you like subsequent consultations to occur?**
- **Q 4.3: What common concerns do you foresee being raised by consultation?**

5. Consultation will naturally involve industry responding to an agency's assistance proposal, however the form of consultation is not strictly set out in the legislation.
   - **Q 5.1: In what form would you like to be consulted (eg. submissions, teleconferences etc.)?**
   - **Q 5.2: Would this change in connection with the significance of the assistance?**
6. For any new capabilities developed under a TCN, a consultation of at least 28 days must occur. More or less consultation is likely to be needed in view of the difficulty of the assistance. From Optus' public submission to the legislation's public consultation:

> **"…28 days will likely be inadequate for a service provider to pull together a comprehensive response if the assistance required is of a complex nature where design options will need to be articulated and evaluated, costing and equipment information will need to be sourced from multiple vendors, resource availability will need to be determined as well as a project schedule being developed." Page 8**

   - **Q 6.1: To allow for preparation for more complex assistance, how far in advance of a consultation would you normally like to be notified?**
7. Depending on the power being exercised, consultation may be waived voluntarily by the provider, forgone in urgent circumstances by agencies or forgone where it is discretionary.
   - **Q 7.1: Noting that Part 15 is available for a wide range of assistance, what are some foreseeable circumstances where you could feasibly waive the consultation requirements or readily assist without substantive prior consultation?**
   - **Q 7.2: In circumstances where consultation is forgone by agencies (as permitted by the legislation), how would you like to be notified?**
   - **Q 7.3: How can agencies forestall concerns you may have when they seek urgent assistance (e.g. before an agreement is in place)?**
8. Industry has noted that assistance which calls for a new technology to be developed may be disruptive if it falls outside of a company's typical development cycles. From Telstra's submission to the legislation's public consultation:

> **"…the decision maker should take account of the [provider's] standard development and release cycles, the availability of relevant engineering and technical resources, the impacts on other planned service and network updates, the time required by a [provider] to undertake their normal rigorous implementation, integration and regression and quality testing etc." Page 5**

   - **Q 8.1: When would the development of a new capability create the least disruption to your regular operations?**
   - **Q 8.2: How can agencies avoid disrupting regular development timelines?**
   - **Q 8.3: Would you be willing to provide advanced information on resourcing constraints to ensure requests (if issued) can account for implementation impost ahead of consultation?**
9. Assistance agreements can be varied or revoked once put into place. Concerns exist that varying or revoking assistance agreements may adversely impact industry. Variations may also be made in response to issues raised by the original agreement.
   - **Q 9.1: What concerns do you have about the varying or revoking of assistance agreements and how can these be allayed, in addition to consultation?**

Q 9.2: Outside of legislative requirements, would you typically expect another full consultation before an assistance agreement is varied or revoked?

Verification and security

Companies that receive a large volume of requests from Government, particular multi-national corporations, have verification procedures in place to determine whether the request is valid. It will also be important to determine established points of contact to expedite assistance.

10. The Department is interested to hear about:
    - **Q 10.1: If any, what are the standard verification policies you employ for Government requests?**
    - **Q 10.2: Outside your own internal system of checks and balances, what information would you like in order to verify that a request is genuine and consistent with Australian law?**
11. Outside of the designated consultation period, it will be necessary for agencies to seek input from the provider at several stages prior to asking for assistance.
    - **Q 11.1: Do you have a contact point to communicate with agencies?**
    - **Q 11.2: What information, regarding points of contact and the organisational structures of agencies, will you need to facilitate communication with them?**

Contents and format of standard form agreements

To ensure cooperation can occur efficiently, the Government would like to develop standard form agreements for common aspects of assistance. It is important to identify which elements of these standard agreements will be most commonly or widely varied. As noted by Optus' submission to the legislation's public consultation:

> **"…a standard form contract might be mandated or determined to cover key areas, which is then only varied in pre-determined areas to insert a description of the assistance, the agreed cost and payment arrangements, and any relevant special conditions." Page 3**

12. Standard form agreements should include details of the baseline conditions, contact points, legislative obligations on the company and Government, the default timeframes for delivery, dispute resolution processes, and individualised schedules.
    - **Q 12.1: What other matters should a standard form agreement contain?**
13. Individualised schedules of standard agreements will include specific costs arrangements, details of the assistance to be provided and other special conditions.
    - **Q 13.1: What other matters should be contained in the special schedules?**

Methods for determining costs

Assistance under Part 15 is provided by default on a no-profit/no-loss basis for all costs reasonably incurred. General procedures to assess the cost of assistance will need to be developed in addition to procedures for departure from the default cost arrangement.

14. While costs assessments will not be unilaterally performed by the provider, the provider's preliminary assessment of their costs is likely to be persuasive. Cost assessments and disputes are governed by **section 317ZK**.

- **Q 14.1: Noting that Part 15 is available for a wide range of assistance, how do you anticipate costs would differ for different types of assistance?**
- **Q 14.2: What is the likely format of any costs assessment?**
- **Q 14.3: In general, would you be assisted by a standard form for assessing your costs?**

Information and advice desired from Government

The exercise of a particular Part 15 power must always be accompanied with certain information relating to making complaints and the scope of a provider's obligations. As a matter of good administrative practice, it may be prudent to include other information relating to immunities associated with the powers and advice on the powers' legal limitations.

15. Depending on the power deployed, different legal immunities attract and different obligations accrue. In addition to information that must be provided under the legislation (see compliance obligations in **section 317TAA** for example):
    - **Q 15.1: What information would you expect concerning your legal rights and obligations when asked to provide assistance?**

16. Exercise of the powers is subject to a number of safeguards and oversight mechanisms. The Inspector-General of Intelligence and Security, the Commonwealth Ombudsman and State and Territory inspection bodies have extensive oversight and complaints functions. Providers may refer requirements of a TCN for independent assessment. Judicial review of executive decisions is available for all powers.
    - **Q 16.1: What other information concerning safeguards and oversight requirements would you expect when asked to provide assistance?**

17. Assistance may involve interaction with a provider's systems. The joint submission by the Communications Alliance, the Australian Information Industry Association and the Australian Mobile Telecommunications Association noted that a provider should be able to:

> **"…test or otherwise check any software or equipment provided to it to ensure that these do not contain harmful features or otherwise negatively impact the security of the [provider's] equipment, network and operations." Page 12**

    Such testing would be expected to occur to meet statutory thresholds of reasonableness, technical feasibility, proportionally and practicality and is anticipated under **paragraph 317E(1)(c).** However, further guidance may be prudent.
    - **Q 17.1: What reasonable conditions should be met before the installation or use of software or equipment on a provider's networks?**

Decision-making criteria

All of the powers, voluntary or compulsory, are subject to decision-making thresholds (see **sections 317JAA, 317P** and **317V** in addition to **sections 317JA, 317RA** and **317ZAA**). It will be necessary to receive information from industry to meet these thresholds and, as a matter of good administrative practice, assure industry that the thresholds have been satisfied.

18. For assistance to take legal effect it must be reasonable, proportionate, practicable and technically feasible. Apple's submission to the Parliamentary Joint Committee on Intelligence and Security raised concerns around the assessment of these criteria:

> **"Whether a TAN or TCN is "reasonable" and "proportionate" or whether compliance with a notice is "practicable" and "technically feasible" should not rest only on the government's view, but should take into account the views of security experts, academics, and privacy considerations." Page 5**

- **Q 18.1: What undertaking from a decision-maker would you expect in order to reasonably assure you that they are satisfied that the requested assistance is reasonable, proportionate, practicable and technically feasible?**

19. When deciding reasonableness and proportionality, a decision-maker must consider factors such as a provider's interests, the intrusiveness of a notice, cybersecurity and necessity.
    - **Q 19.1: How do you anticipate you would represent your interests to the decision-maker?**
    - **Q 19.2: Should there be an agreed 'checklist' to ensure common industry interests are always considered? If so, what should the checklist cover?**
20. To ensure any assistance continues to meet statutory thresholds and may be changed or revoked if circumstances change, decision-makers must revoke a notice if they are no longer satisfied requirements are reasonable, practicable, proportionate or technically feasible (see **section 317R** for example)
    - **Q 20.1: What is your preference to communicate with the decision-maker regarding proposed changes or revocation?**
    - **Q 20.2: How quickly would you expect a decision-maker to make this assessment?**
21. Before assistance to build a new capability may be sought, the Minister of Communications must give their approval upon consideration of their own decision-making criteria in **section 317TAAA**, including the objectives of the notice, the impact on the provider and the competitiveness of the Australian telecommunications industry.
    - **Q 21.1: In general, what information do you consider important to give to the Minister of Communications before they weigh these criteria?**
    - **Q 21.2: Within the Minister of Communications' discretion to consider other things, what other factors do you consider relevant to making this decision?**

Sharing information

Part 15 powers will often be used in the course of operations by law enforcement and intelligence agencies. Describing assistance sought will often require reference to classified Government material and require secure systems and appropriately cleared personnel.

22. Existing arrangements for passing classified Government material may suit this regime.
    - **Q 22.1: What arrangements currently exist for handling classified Government material?**
    - **Q 22.2: Do you currently employ personnel able to view classified Government material?**
    - **Q 22.3: What, if any, are the existing limitations in the exchange of information with Government when administering related legislative schemes such as data retention or Interception Capability Plans?**
23. Consistent with **subsections 317ZF(14) - (16)** permission to publically disclose specifics of an assistance agreement may be sought from the agency with whom the agreement exists.
    - **Q 23.1: Would you be assisted by a standard process for seeking permission?**
    - **Q 23.2: In what circumstances would you anticipate needing to share information beyond your organisation?**
24. **Subsection 317ZF(13)** allows a provider to publish statistical information on the receipt of requests from Government (including where none have been received). Among other reasons, this has been included to allow company transparency reporting.

- **Q 24.1: Does your company already publish a transparency report?**
- **Q 24.2: How would you publish this information?**

25. The format of information will naturally depend on the type of information recovered through the assistance process.
    - **Q 25.1: What are some industry standard formats into which technical information, data logs or other information likely to be recovered through assistance may be provided?**

Processes for referring to independent panel

Proposed assistance to develop a new capability is referred for assessment by a panel consisting of a retired judge and a technical expert by the Attorney-General, if a provider disputes the proposed TCN.

26. It is not a requirement that the names of the assessors be public. However, there may be some circumstances where public knowledge of the assessors may add additional assurance to interested parties.
    - **Q 26.1: In what circumstances would you require the identity of assessors to be made public?**
27. Independent technical assessors may require knowledge of companies' systems to verify claims about the technological practicability of assistance.
    - **Q 27.1: Do you have preferences for the selection of independent experts?**
    - **Q 27.2: What undertakings would be required before an expert assessment of your systems?**
28. Deadlines for the independent panel to complete its work are not prescribed by the legislation and can be flexibly designed to suit providers.
    - **Q 28.1: Under what timeframes would you prefer the independent panel to operate when conducting their assessment and making their report?**

Conflict, Disagreement and Enforcement

Government and industry may not be able to agree on the terms of assistance. It may be necessary to use the Act's dispute-resolution mechanisms (see **section 317ZK**). Enforcement may be pursued if a provider does not comply with a notice (see **sections 317ZA** and **317ZB**).

29. Arbitrators may be appointed on agreement by both parties to determine disputes.
    - **Q 29.1: What class of persons would you consider suitable to decide on a dispute for technical assistance?**
30. In the case of a TAN, the Communications Access Co-ordinator (CAC) within the Department of Home Affairs is the relevant body to apply for enforcement orders. To determine whether enforcement should be pursued, the CAC may seek further information.
    - **Q 30.1: What information would you expect to receive from the CAC or Government prior to the CAC making a decision regarding the application for enforcement?**
31. Under **section 317ZB** it is a defence against non-compliance to prove that compliance with requirements in a notice would contravene a law of a foreign country (where compliance activity is undertaken in that foreign country).
    - **Q 31.1: Are there are clear circumstances in which you consider a conflict of laws may arise?**
    - **Q 31.2: How and when do you anticipate any potential conflict of law would be identified?**

Contact and next steps

Please return your response to the above questions (along with any additional advice you consider will assist the drafting of administrative guidance) to the Communications Access Co-ordinator inbox at cac@homeaffairs.gov.au by **15 February 2019**.

Once your feedback has been considered the Department will prepare draft administrative guidance on the use of the powers. To ensure you are able to comment on the final form and content of this guidance, the Department will circulate this draft for your comment. Once all comments are considered the Department will circulate finalised guidance material.

Australian Government

Department of Home Affairs

ASSISTANCE AND ACCESS

This document summarises the amendments made to Australian law by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. The Act is Australia's legislative response to the rapid evolution of communications technology and the challenges of encryption.

Table of Contents

The Assistance and Access Act 2018

The Australian Government supports cyber security tools, like encryption, that create a safe online environment for Australians. Encryption ensures that everyday digital transactions, like online banking or shopping, can occur securely. The Government has no interest in undermining these critical technologies.

Unfortunately, the same technologies are being employed by terrorists, paedophiles, drug smugglers and human traffickers to conceal illicit activities and facilitate crime. Criminals are increasingly sophisticated users of the internet and rapid technological change has caused valuable sources of evidence and intelligence to diminish, for example:

- over 95 per cent of the Australian Security Intelligence Organisation's (ASIO) most dangerous counter-terrorism targets use encrypted communications;
- encryption impacts intelligence coverage in nine out of ASIO's 10 priority cases; and
- it is estimated that by 2020 all electronic communications of investigative value will be encrypted.

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Assistance and Access Act) equips agencies with the tools they need to effectively operate in the digital era and keep the Australian community safe. The Assistance and Access Act introduced some key reforms to help our agencies access the evidence and intelligence they need by:

- enhancing industry cooperation with law enforcement and security agencies; and
- improving agency computer access powers.

Importantly, nothing in this legislation can require industry to break encryption. Instead, the measures enhance the existing ability of Australian agencies to undertake targeted, proportionate and independently oversighted surveillance activities.

The operation of the Assistance and Access Act will be subject to ongoing review by the Parliamentary Joint Committee on Intelligence and Security and by the Independent National Security Legislation Monitor.

Overview

The Act addresses law enforcement and intelligence agencies' challenges with the evolution of the communications environment, including the growth of encrypted communication.
The Act:

1. Enhances the obligations of businesses that provide communications services to assist agencies;
2. Establishes new 'computer access warrants' for law enforcement; and
3. Strengthens agencies' existing search and seizure powers for computers (including mobile devices) to access unencrypted data.

Schedule 1 – Industry Assistance

In the modern era, criminal activity is frequently conducted online and through communications systems. Australian agencies need the help of the communications industry to detect and disrupt this activity.

Schedule 1 of the Act establishes a framework for government and the communications industry to work together on law enforcement and national security investigations, allowing:

- Agencies to request voluntary assistance from providers with a **technical assistance request**.
- Agencies to require assistance from providers with a **technical assistance notice** where the provider is already capable of giving the required assistance.
- The Attorney-General and Minister for Communications to jointly require a provider develop a new capability with a **technical capability notice** where the provider is not already capable of offering that type of assistance.

Schedule 1 of the Act provides that:

- Any assistance or capability requested must be **reasonable, proportionate, practicable** and **technically feasible**.
- Assistance to law enforcement must be related to investigating offences with a maximum penalty of at least three years imprisonment or more.
- Providers may be asked to build or use capabilities that can provide targeted access to data where this does not remove electronic protection or jeopardise the information security of general users.

Schedule 1 of the Act **does not**:

- Allow for assistance that creates "systemic weaknesses" or backdoors into encrypted devices and communication systems. This includes requesting or requiring providers to:
    - refrain from fixing vulnerabilities or making their services more secure,
    - build a decryption capability; or
    - reduce the broader security of their systems.
- Allow agencies to see the content of personal communications, or intercept communications – these things continue to be governed by existing legislation and warrant regimes.
- Compel providers to build a capability to remove electronic protection.
- Extend existing data retention or interception obligations to new providers.

Other safeguards to Schedule 1 of the Act include:

- Review of technical capability notices upon referral by providers to determine if they abridge any of the Act's limitations, such as the backdoors prohibition.

- A whole-Act review by the Independent National Security Legislation Monitor after 18 months.
- Decisions by agencies and the Attorney-General will be subject to judicial review.
- Any requests by State and Territory police must be approved by the Australian Federal Police to coordinate compulsory requests across Australia.
- Extensive oversight from dedicated bodies including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security.

Schedule 2 – Computer Access Warrants

Schedule 2 of the Act creates **computer access warrants**, which allow law enforcement:

- To covertly access devices to investigate serious crimes.
- To search devices such as laptops, mobile phones and USBs, and collect information.
- To conceal the fact that a device has been accessed.

Schedule 2 of the Act also amends ASIO's existing warrant regime with the power to conceal the fact that a device has been accessed.

Law enforcement computer access warrants must be **issued by an independent authority** (a judge or AAT member) and cannot authorise interference with, or material loss or damage to, a computer.

Computer access warrants can be sought only for serious offences (offences that attract a penalty of three years or more).

Schedule 3 and 4 – Strengthening search and seize powers

Schedules 3 and 4 of the Act extend the maximum penalties associated with the power of a Magistrate to require an individual to unlock a device where they know the password:

- In the Crimes Act, from two years to five years imprisonment – ten years for serious offences.
- In the Customs Act, from six months to five years imprisonment – ten years for serious offences.

Schedules 3 and 4 of the Act also extend the time available for examining electronic devices seized under warrant:

- In the Crimes Act, from 14 to 30 days.
- In the Customs Act, from 72 hours to 30 days.

Schedule 3 also allows police to access account-based data (i.e. social media accounts) via a search warrant.

Schedule 5 – Voluntary assistance for ASIO

Schedule 5 of the Act:

- Provides civil immunity to persons who voluntarily assist ASIO.
- Allows ASIO to apply to the Attorney-General to require a person to unlock a device where they know the authentication protocol.
- Creates a penalty for non-compliance of a maximum five years imprisonment.

The Industry Assistance Framework

Encryption and other forms of electronic protection are valuable cyber security tools.

The new legal framework for industry assistance in Schedule 1 strengthens the ability of intelligence agencies and law enforcement to adapt to the new digital era. It ensures the companies that provide communications services and devices in Australia have an obligation to help agencies, including to assist in the execution of a warrant.

Who does this apply to?

The obligations apply to any provider of communications services and devices in Australia, irrespective of where they base their corporation, servers or manufacturing. The legislation refers to these providers as ***designated communications providers***.

Operating in the Australian market comes with obligations to assist in protecting Australian citizens from those using its marketed services and devices for serious crimes, including terrorism.

While the Australian Government has received voluntary assistance from many technology and communications providers, it is the Government's view that it is not fair to expect unequal compliance from different providers.

What assistance must be provided?

The legislation establishes a ***list of acts or things*** in section 317E that articulates what assistance can be provided to Australia's law enforcement and intelligence agencies.

The ***listed acts or things*** are relevant to each provider in respect of its ***eligible activities***. These are the services and products that a provider offers or operates in the Australian market. A provider is not required to provide help that is unrelated to their relevant eligible activities.

Listed acts or things

A listed act or thing includes[1]:

- removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider where the provider is already capable of removing this protection (***Note:*** *a provider cannot be required to build a capability that removes a form of electronic protection)*;
- providing technical information;
- installing, maintaining, testing or using software or equipment or assisting with those activities;
- assisting with access to devices or services;[2]
- notifying agencies of a change to a service;
- concealing that any other thing has been covertly performed in accordance with the law; and
- doing an act or thig that facilitates giving effect to a warrant or authorisation or enables the effective receipt of information.

[1] This is not a complete or legally accurate list, and is for information only. The full list is available in the legislation at s317E.
[2] Private communications and data may only be accessed with lawful authority pursuant to the existing warrant framework.

Each of these things is subject to the limitation against building systemic weaknesses or accessing personal information.

This list is exhaustive for the compulsory powers under the Act but not the voluntary powers.

How will this be requested?

The legislation establishes **three new tools** for requesting assistance possible in the ***listed acts or things***.

The Technical Assistance Request (TAR)

This is a **voluntary** request that may be issued by the head of an **interception agency** (Federal, State and Territory law enforcement and the Australian Criminal Intelligence Commission), the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Agency (ASIS) or the Australian Signals Directorate (ASD) for prescribed purposes. If a designated communications provider is asked to provide assistance on a **voluntary** basis under a TAR, that provider and their officers, employees and agents are granted civil immunity for things done in assistance.

The Technical Assistance Notice (TAN)

This is a **compulsory order** that may be issued by the head of an interception agency or ASIO. If a designated communications provider is requested to provide assistance under a TAN, they must give that assistance if their current capabilities allow them to do so. A TAN does not require a provider to build a capability or functionality they do not already possess in order to comply with a TAN.

The Technical Capability Notice (TCN)

This is a **compulsory order** that may be issued jointly by the Attorney-General and the Minister for Communications, at the request of the head of an interception agency or ASIO. If a designated communications provider is ordered to provide assistance under a TCN, they must provide that assistance, including building a capability to provide that assistance.

Importantly, a TCN is expressly prohibited from requiring the building of a capability to decrypt information or remove electronic protection.

What will this cost?

By default, complying with a TAR, a TAN or a TCN is cost recoverable on a no-profit-no-loss basis. Providers may also be able to enter into commercial terms for the provision of assistance.

In limited circumstances and only when it is in the public interest, a provider can be required to comply without compensation. This exception cannot be exercised until a decision maker takes into account regulatory burdens and the effect on competitiveness, among other things.

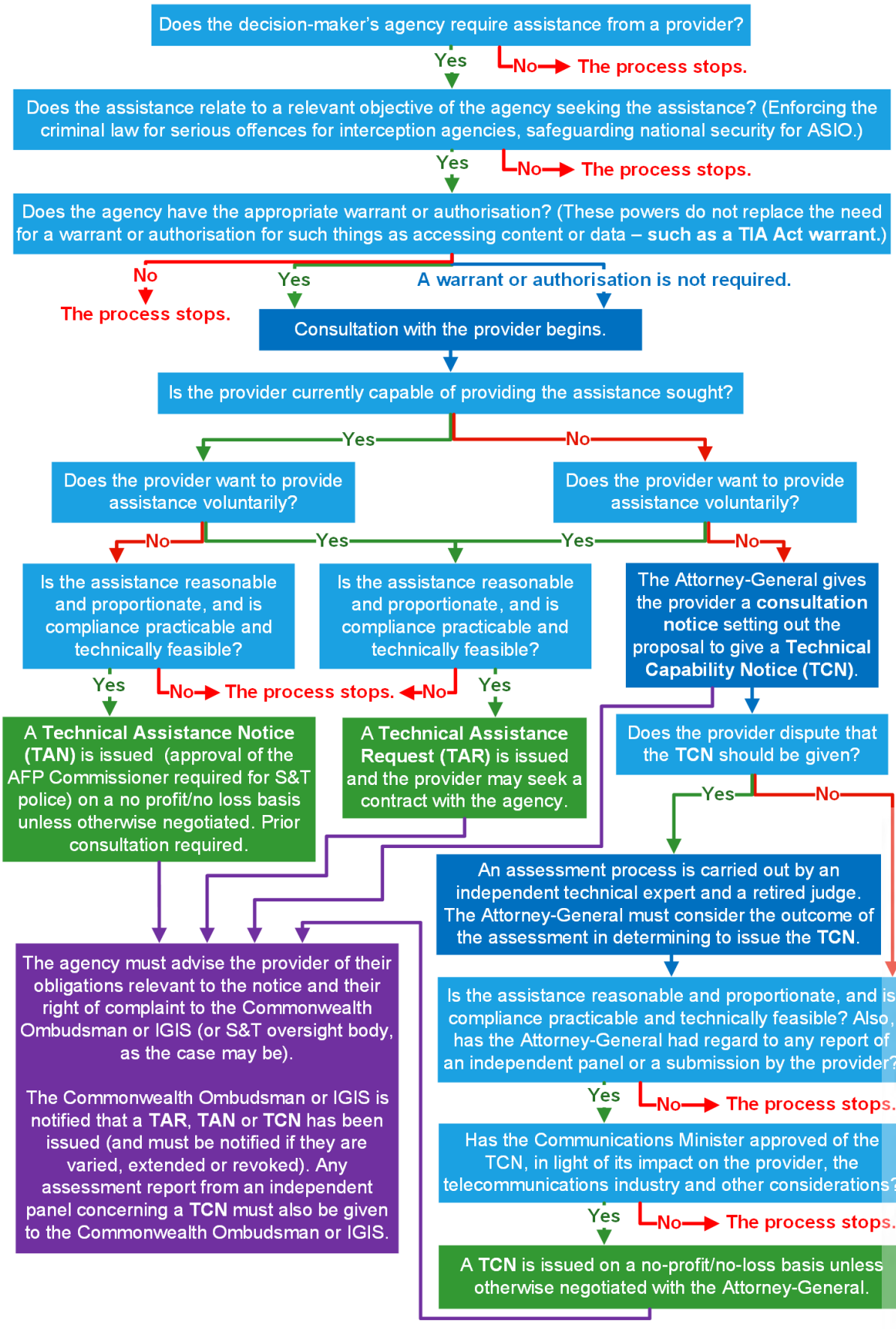
How is this enforced?

If you are a carrier or carriage service provider, you are subject to the existing regulatory regime under the *Telecommunications Act 1997*. This includes a pecuniary penalty of up to AUD $10 million for each case of non-compliance.

If you are a service provider other than a carrier or carriage service provider, a company can be fined up to approximately AUD $10 million for each case of non-compliance. An individual can be fined up to approximately AUD $50,000 for each case of non-compliance.

A person may also be imprisoned for up to five years if there is an unauthorised disclosure of information, as detailed in 317ZF.

Industry Assistance Process[3]



[3] ASIS and ASD are only empowered to issue TARs.

Limitations and Safeguards

Overview

There are a number of key limitations located throughout Part 15 of the Telecommunications Act. Some key safeguards are contained within **Division 7** of Part 15. These include:

1. Requirements and requests must not contravene the prohibition against building or implementing systemic weaknesses or vulnerabilities **– 317ZG**
2. A TAR, TAN or TCN must not be used to do things for which the requesting agency would otherwise require a warrant or authorisation **– 317ZH**
3. (For a TCN) New capabilities must not require the construction of interception capabilities or data retention capabilities **– 317ZGA**

No systemic weaknesses.

Systemic weakness, so-called 'backdoors', weaken the digital security of Australians and others.

This is why notices under the Act cannot require a provider to implement or build systemic weaknesses into electronic protection. The Australian Government has no interest in undermining systems that protect the fundamental security of communications. This includes an explicit prohibition on building a decryption capability or requiring that providers make their encrypted systems less effective.

Notices cannot prevent a provider from fixing a security flaw in their products. Providers can, and should, continue to update their products to ensure customers enjoy the most secure services available.

The **prohibition against systemic weakness** ('backdoors') was clarified and strengthened following a review by the Parliamentary Joint Committee on Intelligence and Security.

What is a systemic weakness?

Section **317B** defines a systemic weakness/vulnerability as 'a weakness/vulnerability' that affects a *whole class* of technology…'. The term 'class of technology' is deliberately broad and captures general items of technology across and within a category of product. It encompasses, for example, mobile phone technology, a particular model of mobile phone, a particular type of operating system within that phone model or a particular type of software installed on an operating system. The wide scope is intended to protect the services and devices used by the whole, or legitimate segments of, the general public and business community.

Further elements of the definition clarify that the inherently targeted surveillance activities of agencies are not captured by this definition. However, new subsections **317ZG(4A), (4B)** and **(4C**) make clear that even requirements to assist in these legitimate and authorised agency activities must not have the inadvertent effect of weakening information security. That is, industry **cannot be asked to do things that would be likely to create a material risk of unauthorised access** to the information of a person not connected to an investigation.

The intent and application of the protection is to provide for targeted, proportionate access **and prevent weakening cybersecurity.**

What is 'electronic protection'?

Electronic protection includes encryption. However, the Act's prohibition against systemic weaknesses also extends to other forms of electronic protection, including authentication systems like passwords.

Agencies need an underlying warrant to undertake surveillance.

The new framework does not serve as an independent channel to obtain private communications, metadata or undertake surveillance. Section 317ZH of the Act states that if a warrant or authorisation was required before, it is still required. Interception of communications, access to metadata or search powers still require existing thresholds to be met. Further, providers **can't be asked to build an interception, data retention or decryption capabilit**y (or build anything that removes a form of electronic protection, like encryption).

In order to undertake these privacy-intrusive activities, agencies must seek a warrant or authorisation under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) or *Surveillance Devices Act 2004*. Agencies must meet the applicable thresholds and receive independent approval.

Additional safeguards for TCNs.

Independent assessments of any new capability.

To attain third-party verification that the Act's legal protections are not being circumvented (and that requirements are otherwise reasonable, proportionate, practical and technically feasible) industry may refer any requirements to build a new capability for review by a technical expert and a retired senior judge. The findings on this **assessment panel** are extremely influential on the decision to issue a notice by the Attorney-General. Industry may also apply for **judicial review** of executive decisions as an inherent part of the Australian legal system.

Added safeguards against data retention, interception and others.

None of the powers can be used to require the construction of a data retention, interception or decryption capability. Additional safeguards exist to prevent new capabilities built under a TCN from extending telecommunications interception, data retention or users' browsing history. These are set out at 317ZGA.

Reasonable, proportionate, practicable and technically feasible.

Decision-makers must be satisfied that a TAR, TAN or TCN is **reasonable**, **proportionate, practical** and **technically feasible**. These decisions, by law, include consideration of industry interests, necessity, privacy, cyber security and intrusiveness. In addition to mandatory consultation, this ensures any representations of industry are taken into account and decision-makers turn their mind to the impact on the Australian public.

Decision-makers must revoke a technical assistance notice or technical capability notice if satisfied that any ongoing requirements are no longer reasonable, proportionate, practical or technically feasible. This ensures that any requirements on industry are under constant assessment and continue to meet the necessary thresholds, even as circumstances change.

Review by the courts, experts and arbitration.

Affected people and companies have an avenue to challenge a decision to issue a notice. Judicial review by the courts is available under the *Judiciary Act 1903*.

Independent technical experts may be appointed to report on any potential security weaknesses associated with requirements of TCNs.

Arbitration for disputes on terms and conditions.

In the exceptional cases where providers and Government disagree on the terms and conditions for compliance with a notice, an arbitrator will determine terms and conditions.

Are there any additional oversight mechanisms?

The scope of notices is limited to core agency functions and a serious offence threshold.

Things specified in notices must be for the purpose of helping an agency perform its core functions conferred under law, as they specifically relate to:

- enforcing the criminal law for serious Australian offences; or
- assisting the enforcement of the criminal laws in force in a foreign country for serious foreign offences; or
- safeguarding national security.

As a result of these requirements, law enforcement agencies are only permitted to use these powers in the course of enforcing a criminal offence with a penalty of three years or more imprisonment, domestically or overseas.

Providers must be informed of their obligations and their right of complaint.

If a notice or request is given under the Act, the issuer must give advice relating to the provider's obligations. This ensures that smaller providers will clearly understand their requirements. When issued with a TAN or TCN, providers must also be informed of their right to lodge a complaint with the Commonwealth Ombudsman or IGIS, depending on the issuing agency.

Information is protected.

Unauthorised disclosure of information about, or obtained under, a notice is an offence. This will ensure any assistance is provided on a confidential basis and the sharing of information, including commercially sensitive information is restricted.

Additional reporting requirements add to transparency.

The public will have visibility of the use of the new powers through annual reporting requirements. The Minister is required to publish a written report every financial year that sets out the number of technical assistance notices and technical capability notices. Providers may produce transparency reports disclosing the number of notices received in a six month period. Providers may also apply for conditional disclosure exemptions to reveal the nature of assistance they have provided.

Powers reserved to senior decision-makers.

The power to issue TCNs is reserved for the joint authorisation of the Attorney-General and Minister for Communications. Requirements under TANs can only be set by the head of ASIO or an interception agency or a senior official in their organisation delegated by them.

Approval of State and Territory notices by AFP.

Before a TAN can be issued by a police force of a State or Territory it must be approved by the AFP Commissioner. The Commissioner will act as centralised coordinator and is intended to reduce duplicate requests, enable the exchange of relevant information across jurisdictions and advise on the types and forms of assistance commonly requested.

Joint ministerial approval of TCNs.

Before a TCN can be issued, it must be approved by the Minister for Communications in consideration of the notice's objectives, the legitimate interests of the provider, the notice's impact on the international competitiveness of the Australian communications industry and any representations made by the Attorney-General. This joint approval mechanism is an additional avenue for industry to feed directly into the decision-making process.

Extensive oversight by the Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman.

The powers will be oversighted by the IGIS (for ASIO, ASD & ASIS) and the Commonwealth Ombudsman (AFP, ACIC and State & Territory Police). This oversight includes:

- Notification to these bodies when the powers are issued, variations, extension, revocation.
- Clear inspection and reporting authority, including explicit discretion for the Commonwealth Ombudsman to conduct an inspection, report on that inspection and have that report tabled in Parliament.
- Information sharing provisions which allow exchange of information under the regime between Commonwealth, State and Territory oversight bodies.

Review by the Independent National Security Legislation Monitor (INSLM).

The operation of the Assistance and Access Act and each of its five schedules will be reviewed by the INSLM after it has been in effect for 18 months.

Assistance and Access Myth-busters

This law will create backdoors and undermine information security.

The Assistance and Access Act contains an express prohibition against building or implementing any weakness or vulnerability in software or physical devices that would jeopardise the security of innocent users. This is found in **section 317ZG** of the Act which also makes clear that any assistance that makes a systems' encryption or authentication less effective for general users is strictly prohibited. This same section prohibits the construction of new decryption capabilities and rules out any requirements that would prevent a company from patching existing security flaws in their systems.

All proposed requirements to build a new capability can be referred to an independent assessment panel consisting of a technical expert and a retired judge. This panel must consider whether the proposed requirements contravene the explicit prohibition against backdoors.

In fact, the Act has no ability to compel a company to build any type of capability that removes a form of electronic protection, like encryption. That is, if the company is not already capable of decrypting something – nothing in the Act can require them to build a capability to do it.

This law does not have adequate oversight.

All requests and requirements on industry are subject to extensive independent oversight by either the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or State and Territory oversight bodies. The relevant Commonwealth body is notified whenever a notice for assistance is issued, varied, extended or revoked. When an agency issues a notice, they must notify the company of their right to complain to the relevant body. Both the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security have the authority to inspect agency use of these powers by relevant agencies at any time. These bodies may make reports to Parliament on the outcome of their inspections.

Compulsory powers carry additional oversight measures to ensure they are used appropriately. For example, where a State or Territory law enforcement agency issues a notice to compel technical assistance, it must first be reviewed by the Australian Federal Police Commissioner.

Strict oversight also applies before a company can be compelled to build a new capability. Technical capability notices may only be issued by the Attorney-General. The Attorney-General's decision must also be reviewed and approved by the Minister for Communications. This creates a double-lock approval to ensure the assistance sought has been thoroughly scrutinised and is reasonable, proportionate, practicable and technically feasible.

A company may also refer any requirement to build a capability to an independent assessment panel consisting of a retired senior judge and a technical expert. This panel must consider whether proposed requirements will inadvertently create a backdoor. Further, any decision to compel assistance may be challenged through judicial review proceedings.

Public transparency is insufficient.

Given the sensitive work done by law enforcement, security and intelligence agencies and the need to protect commercially sensitive information, it will not always be possible to disclose sensitive details of how assistance has been provided. This principle is consistent with the current protections given to operational intelligence held by Australia's law enforcement and intelligence community.

Visibility over the use of the industry assistance powers is possible through mandated annual reporting requirements which require law enforcement agencies to record the number of times each power is used within a 12-month period and also disclose the type of offences the powers were used to investigate. This data will be included in the annual report required to be prepared under **subsection 186(2)** of the *Telecommunications (Interception and Access) Act 1979* alongside data concerning the use of related warrants and authorisations.

Companies and their specified personnel are also authorised to make statistical disclosures to reveal the number of requests and notices received over the course of a six-month period and reveal whether that assistance was voluntary or compulsory. Additionally, where a company provides assistance they may seek authorisation from the issuing agency to disclose information about this assistance. This process will ensure operational details are protected, while giving companies the possibility to inform interested parties about the help they are giving to authorities. Provision for these disclosures appears in **subsections 317ZF(13)** and **317ZF(14) – (17)**.

Police will use this law to prosecute minor offences.

The industry assistance powers are only available to agencies in limited circumstances. There is an express requirement that the industry assistance powers can only be used by police to enforce the criminal law for serious offences, being offences that involve a penalty of at least three years imprisonment.

To access communications content and data an underlying warrant or authorisation is still required. For example, the legislation does not replace the need for police to seek a warrant from an independent authority to intercept communications. Generally these warrants are available for offences punishable by a maximum of seven years imprisonment or more.

The availability of these powers may expand due to scope creep.

The list of agencies with access to industry assistance powers can only be expanded through legislative amendment, which would include further parliamentary scrutiny. Only Australia's core law enforcement, security and intelligence agencies are able to utilise the industry assistance powers.

The Five Eyes alliance may take advantage of this law.

The Assistance and Access Act is an Australian solution to an Australian problem – it was not requested by, or designed for, Australia's Five Eyes partner countries. While the Five Eyes share intelligence for security purposes, foreign assistance in connection with information obtained under this legislation will be undertaken consistent within the established mutual legal assistance process or through existing, and bounded, channels of cooperation. Foreign partnerships are critical to the detection and disruption of transnational crime and attacks that are coordinated through several countries.

The industry assistance powers for intelligence gathering are limited to collecting intelligence connected with Australia. This is because the Act requires a geographical nexus between the activities of a company and Australia. Further, access to content or non-content data through industry assistance powers requires a valid warrant or authorisation.

Capabilities built by the Government will leak.

The Assistance and Access Act focuses on creating a pathway for industry to deliver assistance to law enforcement and intelligence agencies where necessary. Examples of the kinds of help that may be sought through industry assistance powers include specifying the technical details of a system or device, or altering the nature of a user's service to allow a warranted surveillance device to be operated without alerting the target.

Both industry and law enforcement and security agencies have robust procedures in place to protect sensitive information and have made significant investments in the development of strong cyber security protocols that will be used to secure information relating to any form of assistance. Additionally, Australia's law enforcement and security agencies are experienced in managing operational sensitivities and will take steps to minimise risks or exposure of information.

This law will lead to mass surveillance.

The Assistance and Access Act does not authorise mass surveillance. The Act expressly prohibits the Government from requiring a company to build an interception capability or a data retention capability. Any requirements must be reasonable, proportionate, practicable and technically feasible and are subject to independent oversight and judicial review.

If conducted, digital surveillance must be consistent with existing legal regimes, like the warrant process for intercepting telecommunications in the *Telecommunications (Interception and Access) Act 1979.* The powers available under these laws are inherently targeted.

This law can compel employees to work in secret without the knowledge of their organisation.

Media reporting that has proposed this scenario is incorrect and misleading. The industry assistance framework is concerned with getting help from companies not people acting in their capacity as an employee of a company. Requests for assistance will be served on the corporate entity itself in line with the deeming service provisions in **section 317ZL**. A notice may be served on an individual if that individual is a sole-trader and their own corporate entity.

A company issued a notice can disclose information about it under **paragraph 317ZF(3)(a)** in connection with the administration or execution of that notice. This allows an employer to disclose information to their employee and vice versa in the normal course of their duty.

Additionally, a company may disclose statistical information about the fact that they have received a notice consistent with **subsection 317ZF(13)**. Further, companies and their specified personnel may disclose notice information for the purposes of legal proceedings, in accordance with any requirements of law or for the purpose of obtaining legal advice. The notices themselves are therefore not 'secret' but information about their substance is controlled to protect sensitive operational and commercial information.

This law will harm Australia's tech sector.

The Assistance and Access Act and, specifically, the industry assistance powers are not unique to Australia or western democracy. This legislation comes after the passage of the UK's *Investigatory Powers Act 2016* and New Zealand's *Telecommunications (Interception Capability and Security) Act 2013*, both of which deal with similar subject matter and provide powers to compel assistance from private companies.

During the development of the Australian legislation, the Government recognised concerns that the possibility of undisclosed changes to a company's services could harm products' competiveness at market. To answer these concerns, the legislation includes provisions for companies to publish statistics regarding the number of requests or notices they have received in a six month period under **subsection 317ZF(13)** – including where this number is zero – and make conditional disclosures to interested parties about assistance given under **subsections 317ZF(14)-(17)**. In practice, this will leave most companies unaffected, as they will be able to disclose that they have not been asked to provide assistance, while companies who do assist can demonstrate that their systems are not compromised by the

assistance they have provided, consistent with the law's explicit protections against the creation of backdoors or the degradation of security features.

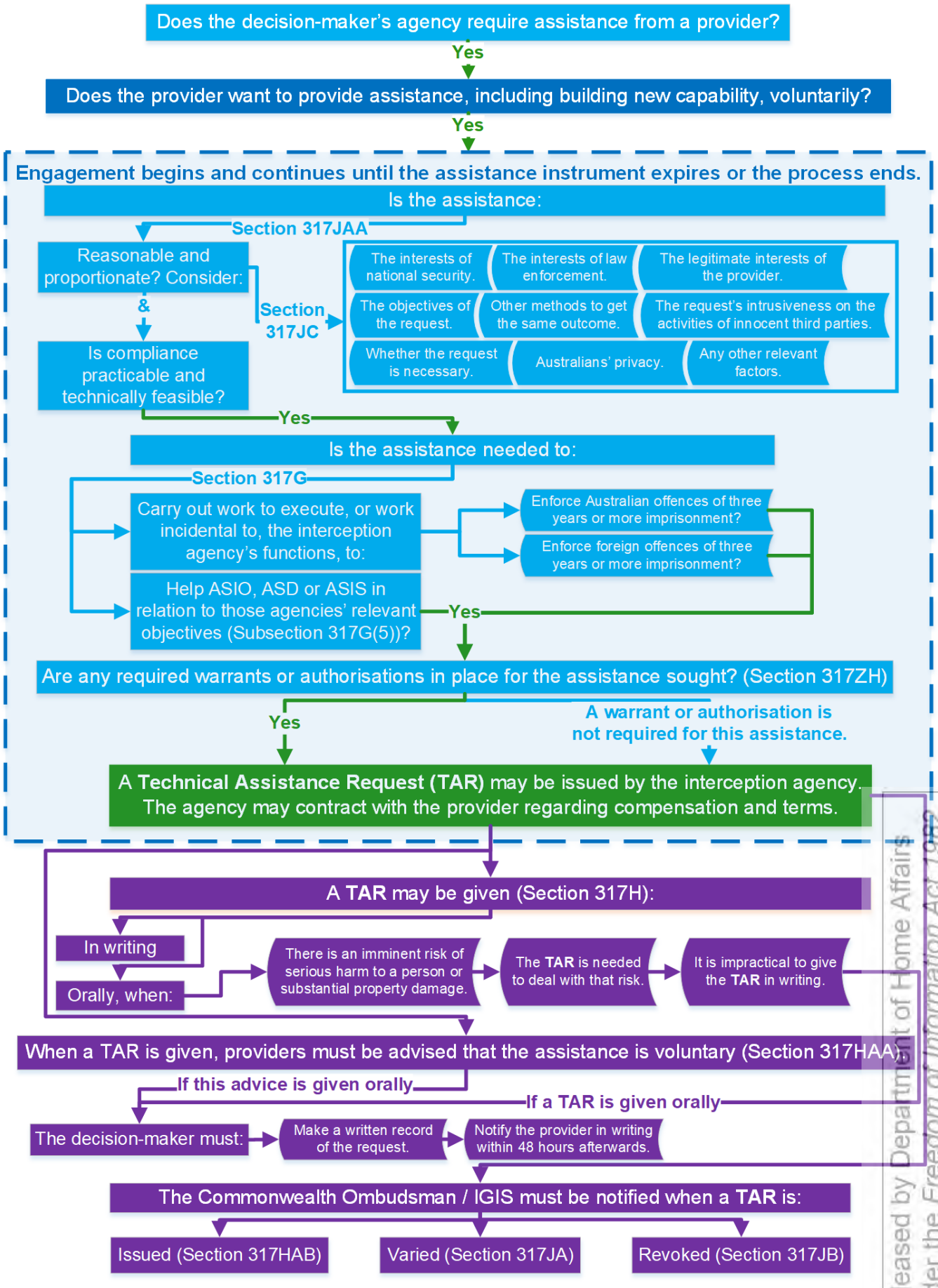
Australian companies and their employees will be hardest hit by this law.

Companies that supply communications services and devices in Australia, regardless of whether they are incorporated in Australia or not, may be the subject of technical assistance obligations under the Assistance and Access Act. The measures do not place a greater burden on Australian companies nor do they allow authorities to compel Australian citizens working for communications companies offshore. Additionally, Australian companies who primarily conduct business overseas are only obliged to assist Australian authorities to the extent that their activities relate to products and services being used within Australia. Services provided by Australian companies to persons offshore that relate to activities offshore are not classified as '*eligible activities*' for the purposes of the legislation and are thus not captured by these laws.

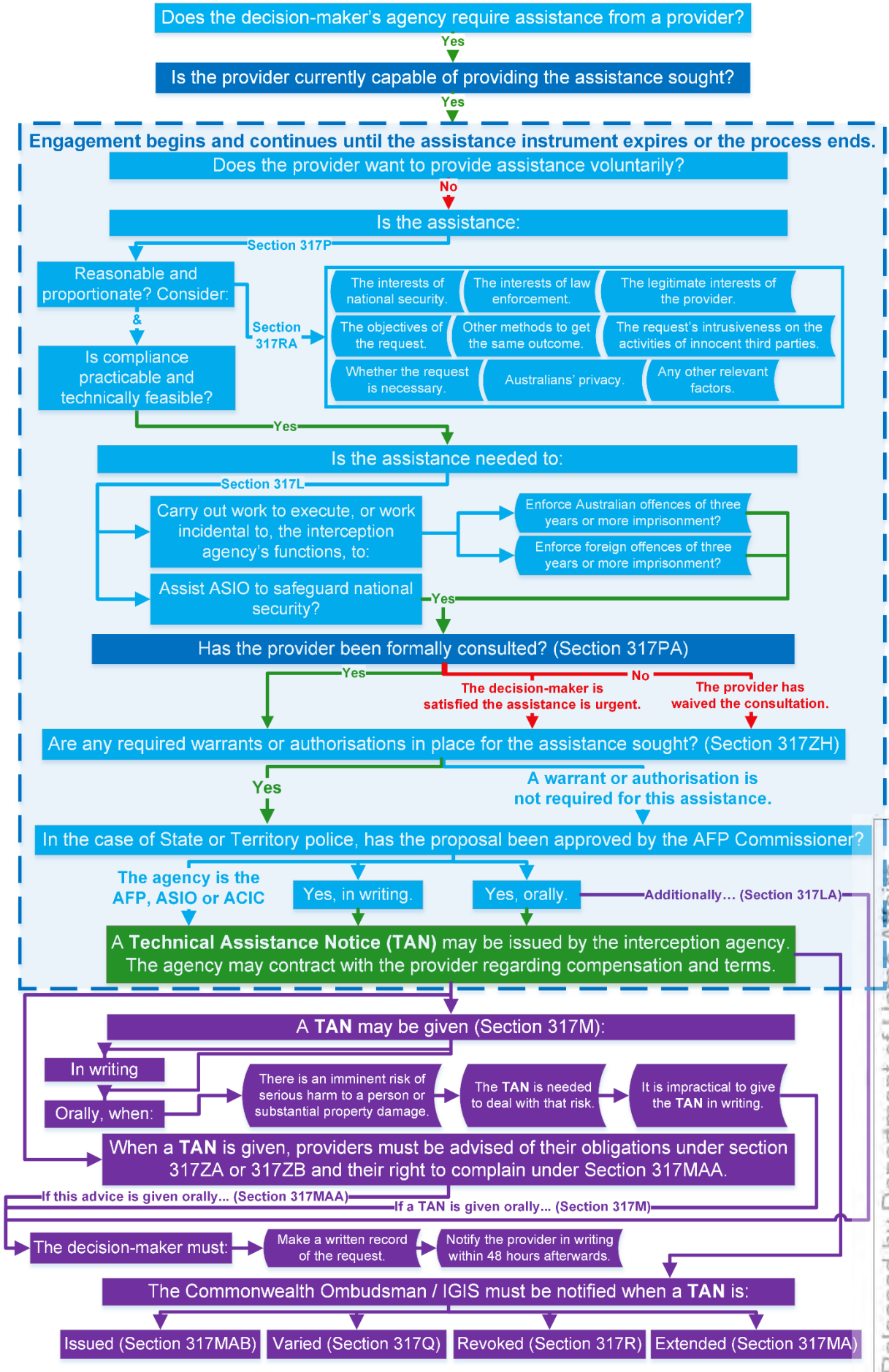
The Act's provision for penalties against individuals is not intended to apply to employees of a non-compliant company. If a company does not comply with their assistance obligations, any enforcement action that may be undertaken will apply to the enterprise. Penalties for individuals in the legislation are for the purpose of potential enforcement proceedings against sole-traders and individuals acting as businesses.

Criminal offences for the disclosure of sensitive and protected information (including sensitive commercial information) apply equally to Government officials and agency personnel and are consistent with secrecy provisions in other Commonwealth laws. Importantly, a suite of exceptions to the offence of unauthorised disclosure applicable to providers and specified personnel are listed in **subsections 317ZF(3)**, **(12B)**, **(13)**, **(15)** and **(16)**.

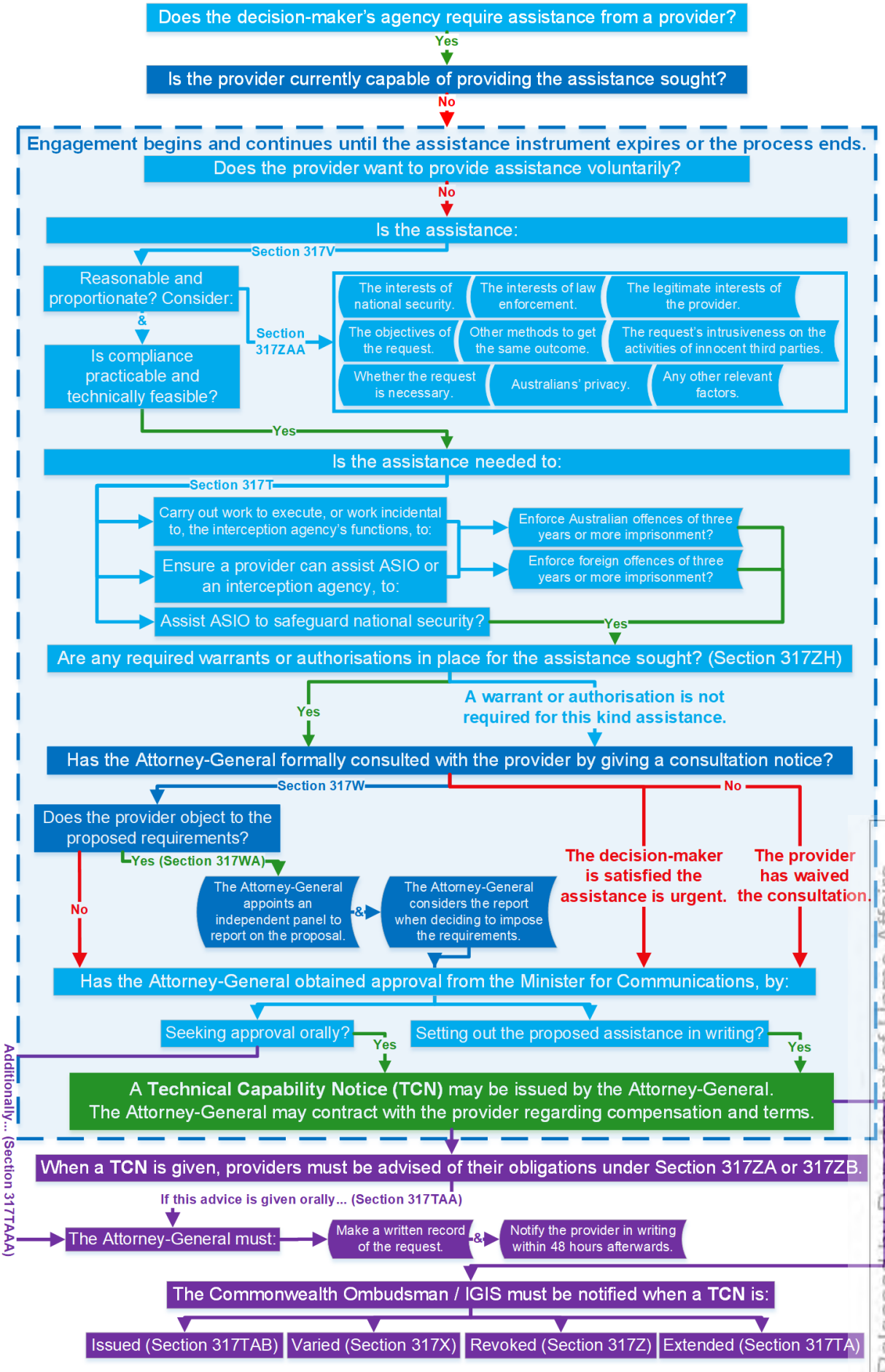
Technical Assistance Request Process



Technical Assistance Notice Process



Technical Capability Notice Process



Assistance Examples

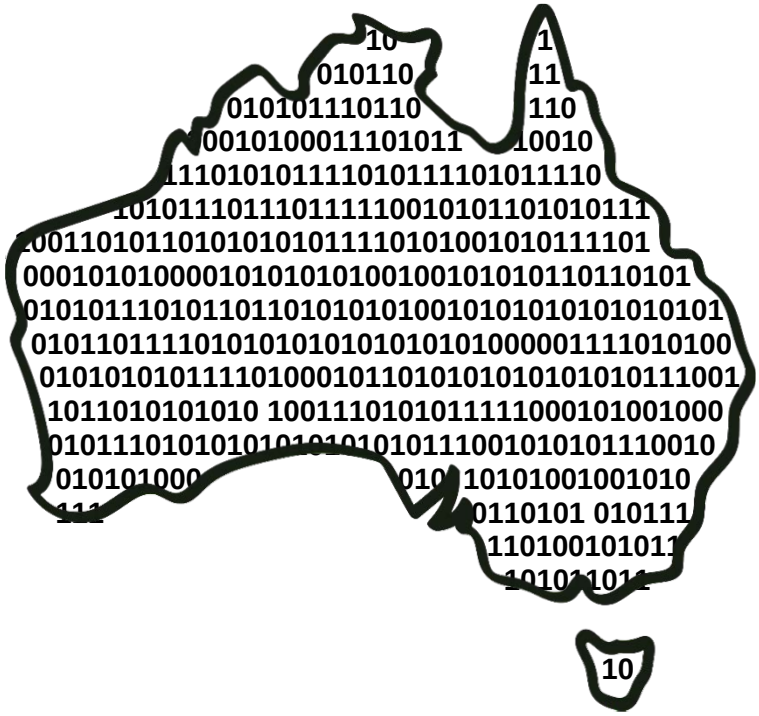
Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	- Requesting an ISP provide the password they have enabled on a customer supplied home modem to facilitate a review of its logs during a search warrant to identify connected devices. - Requesting a cloud storage provider changes the password on a remotely hosted account to assist with the execution of an overt account based warrant.
(b)	Providing technical information	- An application provider providing technical information about how data is stored on a device (including the location of the encryption key) to enable forensically extracted data to be reconstructed. - An international cloud hosted storage provider providing details of where a customer's data is hosted to enable a Mutual Legal Assistance Treaty process to be progressed to the host country seeking lawful access. - A mobile device provider providing a copy of their WiFi AP location maps generated through bulk analysis of customers data to correlate with location records extracted during a forensic examination of a device.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	- Requesting a cloud service provider provide a copy of the contents of a hosted account in a particular format pursuant to the execution of an overt account based warrant. - Requesting that data held in a proprietary file format extracted from a device during a forensic examination pursuant to an overt search warrant is converted into a standard file format.
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer equipment, an electronic service etc.	- Requesting a shared data centre provide access to customers computer rack to enable the execution of a computer access warrant or installation of a data surveillance device under warrant.
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	- Requesting that a social media platform assist with testing or development of a tool to automate the creation of online personas and historical content to facilitate online engagement.

Sub section 317E(1)	Listed act or thing	Examples
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation.	- Requesting an ISP advise of any technical changes to their network which could impact on an existing interception.
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	- Requesting a carrier increase the data allowance on a device that is subject to a surveillance device warrant to enable the surveillance device to be remotely monitored without consuming the targets data. - Temporarily blocking internet messaging to force a device to send the messages as unencrypted SMS's.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service provided by the provider; or a service provided by another designated communications provider.	- Requesting a carrier force a roaming device to another carriers network to enable the enhanced metadata collection capabilities of the new carrier to collect information pursuant to a prospective data authorisation.
(j)	An act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties; or - assisting the enforcement of the criminal laws in force in a foreign country; or - the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	- Requesting that the provider not inform the customer of the assistance provided to enable a computer access warrant. - Requesting that the provider delete an audit log in a customer's device relating to a computer access warrant. - Requesting a provider restore a password that was temporarily changed to enable a computer access warrant. - Requesting a provider allocate a specific dynamic IP address relating to remote access pursuant to a computer access warrant to conceal the access.

Industry assistance under Part 15 of the *Telecommunications Act 1997* (Cth)

Administrative guidance for agency engagement with designated communications providers

.....



V. 0.2

CONTENTS

ACRONYMS AND TERMS

- *Acts Interpretation Act 1901* (Acts Interpretation Act)
- *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act)
- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Australian Signals Directorate (ASD)
- Australian Security Intelligence Organisation (ASIO)
- *Australian Security Intelligence Organisation Act 1979* (ASIO Act)
- Australian Secret Intelligence Service (ASIS)
- Communications Access Coordinator (CAC)
- *Criminal Code Act 1995* (Criminal Code)
- Independent National Security Legislation Monitor (INSLM)
- *Independent National Security Legislation Monitor Act 2010* (INSLM Act)
- *Inspector-General of Intelligence and Security Act 1986* (IGIS Act)
- *Intelligence Services Act 2001* (IS Act)
- *Mutual Assistance in Criminal Matters Act 1987* (MACMA)
- *Privacy Act 1988* (Privacy Act)
- *Telecommunications Act 1997* (Telecommunications Act)
- *Telecommunications (Interception and Access) Act 1979* (TIA Act)
- *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Assistance and Access Act)

INTRODUCTION

On 9 December 2018 the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* came into law updating the digital collection powers of Australian agencies and reforming the framework through which they seek help from industry. Australia's existing industry assistance scheme was modernised with the addition of Part 15 of the *Telecommunications Act 1997* (Telecommunications Act). This Part introduces a new regime to seek assistance from the contemporary Australian communications market in support of national security and law enforcement investigations.

This document outlines administrative processes and best-practice for the use of the measures in Part 15. This guidance has been designed for use by both Government stakeholders and members of the communications industry to ensure that all parties have a clear understanding of their rights, obligations and expectations. It should be used by persons interacting with the assistance framework, whether they are within an agency seeking assistance or within a company providing assistance. The guide also sets out the limitations of the regime and establishes the administrative parameters of Part 15.

Industry assistance: old and new

Traditional Australian telecommunications providers have long had an obligation to provide reasonably necessary assistance to Australian authorities under section 313 of the Telecommunications Act. However, this regime does not recognise the growing role of new, innovative and global providers in the Australian communications supply chain. Increasingly, the communications services and devices used by Australians are being supplied by a wide range of providers both within and outside of Australia. The nature, operation and location of these services is a significant departure from the way communications have been delivered to Australia in the past.

Part 15 is an evolution of the older regime in section 313 and responds to shifts in the Australian communications market and changes in technology.[1] It narrows the scope of agencies that can seek assistance and introduces new consultation requirements to account for the wider range of stakeholders within the framework. Neither regime, old or new, are avenues to collect personal information or circumvent the legal protections applied to private data under Australian law. The focus of the Part 15 measures is assistance, not the collection of private information.

Lawful access to data

Australian law enforcement and intelligence communities rely on a range of warrants and authorisations to access the data and communications of the individuals they investigate – many of which are obtained under the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The TIA Act prohibits unlawful interception and access to communications. Exceptions to these prohibitions include collection under warrants issued by independent persons and authorisations for the disclosure of information. To exercise the powers in the TIA Act, agencies must meet significant thresholds.

As noted above, application providers, device manufacturers and technology companies are now integral participants in Australia's modern communications market. These providers are well-placed to enable the lawful access to communications by key Australian law enforcement and security agencies that has always been permitted through such regimes as the TIA Act.

[1] Section 313 remains in operation to ensure the smooth delivery of industry assistance from Australian carriers and carriage service providers to the wider range of authorities entitled to assistance under that regime and to support existing and continuing relationships with these companies.

Importantly, while the restrictions and exceptions under the TIA Act and other legislation will continue to apply to Australian agencies, the scope of the existing warrant framework may not extend to these newer players.

The industry assistance powers in Part 15 address this shortcoming by formalising the relationship between Australian agencies and the broader communications industry. They do not replace the warrant and authorisation regimes under TIA Act, the *Surveillance Devices Act 2004*, the *ASIO Act 1979* or provide a new basis for interception. Instead, Part 15 allows agencies to seek help directly from the providers who constitute the modern communications market, including in tandem with the exercise of existing warranted powers. In addition, industry assistance is flexible enough to be used to provide agencies with a broader range of technical assistance that is not connected to a warrant or authorisation, and does not require any additional lawful authority. An example of this is asking for technical information regarding a provider's systems that will assist the agency to build their own, indigenous capabilities.

Responsible and collaborative assistance

Encrypted communications is just one outcome of the revolution in communications technology. While the prevalence of encryption contributes to a significant loss of intelligence and evidence, it is of singular importance in protecting private communications and digital services. That is why the measures in Part 15 do not, and cannot, undermine the security that strong encryption provides. Instead, Part 15 is focused on identifying other ways of overcoming the technological impediments to investigations that new technology creates.

Government has a responsibility to the communications industry to ensure that assistance is always proportionate to the matter being investigated. Jeopardising cybersecurity, unreasonably intruding on privacy, crippling commercial viability or circumventing due process are not acceptable outcomes of any partnership. This is why the processes in this guide and the safeguards in the legislation must be central to agency and provider considerations.

The industry assistance framework is designed to be inherently collaborative so that mutually agreeable outcomes may be reached for both parties. While the scale of technological change is often difficult to keep apace and can sometimes leave authorities in the dark, Australian agencies are committed to working collaboratively with the very providers who drive this change to protect public safety and maintain the integrity of our digital lives.

CONCEPTS DICTIONARY

DESIGNATED COMMUNICATIONS PROVIDER

Designated communications providers (providers) is a wider class than carriers or carriage service providers and includes a company whose electronic product or service is used by one or more end-users within Australia. More detailed guidance on this definition can be found in section 317C of the Telecommunications Act and Appendix D.

ASSISTANCE INSTRUMENTS: TARS, TANS AND TCNS

The new industry assistance framework in Part 15 of the Telecommunications Act established a graduated approach to seeking help from providers through three **assistance instruments**.

1. **Technical assistance requests** (TARs) allow providers to offer assistance on a voluntary basis using their present capability or by building a new capability. Providers may contract with agencies regarding the terms of their assistance, including financial arrangements. Providers receive immunity from civil suit and specific computer offences contained in the *Criminal Code Act 1995* for any conduct done in accordance with the TAR.
2. **Technical assistance notices** (TANs) require providers to offer assistance that they have the present capability to provide. TANs cannot be used to obtain assistance that the provider does not have the present capability to offer. Providers are compensated on a no-profit / no-loss basis, and receive immunity from civil suit and specific computer offences contained in the Criminal Code for any conduct done in accordance with the TAN.
3. **Technical capability notices** (TCNs) require providers to offer assistance that they have the present capability to provide, and to build new capability to offer assistance they could not otherwise provide. Providers are compensated on a no-profit / no-loss basis, and receive immunity from civil suit and specific computer offences contained in the Criminal Code for any conduct done in accordance with the TCN.

When an assistance instrument is issued it identifies the assistance sought and triggers the conferral of the civil immunities and limited criminal immunities on the provider.[2]

SYSTEMIC WEAKNESS

Industry assistance cannot be used if it would systemically weaken a form of electronic protection. This means that backdoors cannot be built or implemented into software or hardware as a result of an assistance instrument. Any assistance instrument that would create a **systemic weakness** or **systemic vulnerability** is prohibited and legally ineffective to the extent it would create these weaknesses or vulnerabilities.

The term is defined in section 317B as a weakness/vulnerability that affects a *whole class* of technology…' The term 'class of technology' is deliberately broad and captures general items of technology across and within a category of product. It encompasses all products which share similar functional attributes. For example, mobile communications technology, a particular model of mobile phone, a particular type of operating system within that phone or a particular type of software installed on an operating system. This definition is intentionally wide to capture product ranges, and layers of technologies within products.

The scope of this definition is complemented by the safeguards in subsections **317ZG(4A), (4B)** and **(4C)** which make clear that requirements to assist must not inadvertently weaken the

[2] Further detail on the procedure for each of the industry assistance measures can be found in the Appendix of this document.

information security of other persons, even if agency activities are suitably targeted and authorised. That is, industry cannot be asked to do things that may risk unauthorised access to the information of an unrelated party. This ensures the privacy and data security of non-target parties remains intact.

Put simply, the law treats anything that would jeopardise the integrity and security of data, services and products used by the general public and business community as a systemic weakness.

EXISTING CAPABILITY

Industry assistance distinguishes between assistance that can be offered by using a capability that a provider currently possesses and assistance that requires the development of a new capability before it can be provided. **Existing capability** should be assessed during consultation with the provider. The limitations of the provider's existing capability is a factor in determining which assistance instrument should be issued.

DECISION-MAKER

The **decision-maker** in any given situation is the authority empowered to issue a TAR, TAN or TCN – though not all of these powers are available to all decision-makers. For a TAR and TAN, decision-makers are chief officers and delegated officials. Decision-makers can be divided into three categories:

1. **Interception agencies** which are the AFP, the police forces of each state and the Northern Territory, and the ACIC. Interception agencies are empowered to issue TARs and TANs, and may ask the Attorney-General to issue a TCN on their behalf. Police forces of a State or the Northern Territory must have their TANs approved by the Commissioner of the AFP.
2. **Intelligence agencies** which are ASIO, ASD and ASIS. ASD and ASIS are empowered only to issue TARs. ASIO may issue TARs and TANs, and may ask the Attorney-General to issue a TCN on their behalf.
3. The **Attorney-General** is the decision-maker for the issuing of TCNs on behalf of the agencies empowered to seek assistance through TCNs. The agreement of the Minister for Communications is also required before a TCN can be issued.

REASONABLE AND PROPORTIONATE

In order to issue an assistance instrument, the decision-maker must first be satisfied that the conduct sought is **reasonable and proportionate**. To determine this, the decision-maker should balance the following considerations:

1. The interests of national security.

   This consideration is relevant to ASIO, whose relevant objective when exercising industry assistance powers is the safeguarding of national security. This consideration will also be relevant to the functions of ASD and ASIS, and may be considered by decision-makers at other agencies as circumstances require.

2. The interests of law enforcement.

   This consideration is relevant to interception agencies, whose relevant objective when exercising industry assistance powers is enforcing the criminal law as it relates to serious offences (three years and above). Typical interests of law enforcement include prevention, detection, investigation, prosecution and punishment of breach of the law.

3. The legitimate interests of the designated communications provider to whom the assistance instrument relates.

Consider any consequences for providers as a result of their compliance with an assistance instrument – particularly consider adverse business or financial consequences for the provider's ability to continue to trade and operate.

4. The objectives of the assistance instrument.

Consider the purpose that the assistance sought aims to accomplish, the importance of that purpose when balanced against the other considerations and the consequences if the assistance cannot be obtained.

5. The availability of other means to achieve the objectives of the assistance instrument.

Consider alternative methods of meeting objectives, the desirability of the alternative, the onerousness of the alternative, and any adverse consequences of the alternative when compared with the proposed method.

6. Whether the assistance instrument is the least intrusive form of industry assistance known to the decision-maker, as far as non-target persons are concerned.

Compare the assistance sought to any other kinds of assistance known to the decision-maker that could accomplish the same objective and consider if those other types of assistance are more or less intrusive on the interests of individuals who are not of interest to the decision-maker's agency.

7. Whether the assistance instrument is necessary.

Consider if the assistance is as targeted as needed to achieve the objective and whether any activities are superfluous. A key consideration here is whether a particular provider is the appropriate one to give the assistance sought. Assistance that is necessary will primarily relate to providers who, in the circumstances, are in the best position to offer the requisite help. Importantly, this consideration does not require the assistance instrument to be 'essential' only that it be reasonably necessary in light of the circumstances.

8. The legitimate expectations of the Australian community relating to privacy and cybersecurity.

Consider the public interest in maintaining personal privacy as it relates to the protection of individuals' private lives, but not as it relates to the concealment of serious criminal activity. Limitations attached to privacy-intrusive activities and requirements set by representative bodies, like Parliament, can guide this assessment. Public reporting, polling data and other public material can also inform legitimate expectations.

9. Such other matters as the decision-maker considers relevant to the present case.

Where peculiar and unique circumstances arise that may affect the decision-making process and are not captured by the other criteria, consider these unique features as separate criteria.

PRACTICABLE AND TECHNICALLY FEASIBLE

In addition to being satisfied that the assistance instrument is reasonable and proportionate, the decision-maker must also be satisfied that compliance with the request or notice is **practicable and technically feasible**. While a weighing exercise must occur to determine if an assistance instrument is reasonable and proportionate, an assistance instrument that is impracticable or not technically feasible may be impossible to execute.

An assistance instrument is practicable when the assistance sought resemble to an activity that is within the provider's typical capacity to perform and can be performed by the provider without needing to divert sizeable resources towards fulfilling it, An assistance instrument may be impracticable if it requires things that are highly unusual and difficult or if it is an onerous departure from the activities typically performed by the provider.

An assistance instrument is technically feasible when the assistance sought relates to an existing capability that is within the provider's power to operate. Conversely, an assistance instrument may not be technically feasible if it is unclear what technical procedure would need to occur in order to provide the assistance or produce the outcome sought or if no technical procedure exists that could produce the outcome that is sought from the assistance.

The assessment of technical feasibility also involves what is technical feasible within to the bounds of the legal safeguards in the legislation. For example, while it may be feasible to enable access to a user's encrypted data carried over an end-to-end encrypted service, such an action may create a material risk that unauthorised parties could access the data of other, unconnected, users. This activity **would not** be technically feasible within the parameters of the legislation because it would contravene the prohibition against systemic weaknesses.

In the case of either a TAR or TCN being used to develop a new capability, the concepts of practicability and technical feasibility cover broader conduct than is possible under a TAN – TANs being inherently limited to obtaining assistance that is within the provider's existing capability to provide. However, conduct may still be impracticable or not technically feasible in the case of a TAR or TCN where the provider is uncertain that the capability can be built to specification. This may occur in cases where required external expertise is unavailable to assist development due to a technology's proprietary nature or where it is unclear that the proposed capability could in fact be used to provide the assistance sought.

ENFORCING THE CRIMINAL LAW

Assistance provided to interception agencies, all of which have a law enforcement function, must be provided for the relevant objective of **enforcing the criminal law** for offences attracting penalties of three years or more imprisonment. Assistance that may be sought to assist in the enforcement of the criminal law may be assistance that aids a criminal investigation of a relevant offence, a criminal prosecution of a relevant offence, a future criminal investigation or prosecution of a relevant offence, or assistance to prevent the perpetration of a criminal offence.

This concept includes precursory and secondary intelligence gathering activities that support the investigation and prosecution of suspected offences. The term 'criminal law' includes any Commonwealth, State or Territory law that makes particular behaviour an offence punishable by fine or imprisonment.

Interception agencies may obtain general technical assistance to improve their ability to investigate or prosecute a relevant offence or improve a provider's ability to offer assistance in future investigations or prosecutions of a relevant offence. However, assistance of this kind remains subject to existing requirements to obtain a warrant or authorisation – as discussed below – before it can be used to obtain personal data.

EXISTING WARRANTS – IN RELATION TO AN AGENCY

A warrant or authorisation under other existing legislation is not *always* required to utilise Part 15. An agency may seek assistance from industry that does not involve access to information or the undertaking of activities that requires a warrant or authorisation. Examples of activities that **do** require warrants or authorisations include the interception of communications, access to metadata or the use of a surveillance device.

Accordingly, industry assistance is not available if the assistance sought by the decision-maker's agency requires a warrant or authorisation, and the agency has not obtained the appropriate warrant or authorisation. Where a law requires the agency to obtain a warrant or authorisation to undertake an activity or access information, this must be in place before the provider can offer the assistance sought.

As noted above, there are various forms of assistance that may be sought which do not relate to warranted or authorised activities. This may be the case for the construction of new and lasting capabilities (the use of these capabilities is a different matter). In these circumstances, no underlying warrant or authorisation is needed to authorise the activity.

Providers may also be asked to be ready to give assistance before the requesting agency has obtained the warrant or authorisation that is required to perform the assistance. In these circumstances, providers should refrain from carrying-out the assistance until notified that the required warrant or authorisation is in place.

CONSULTATION

Preliminary and ongoing engagement

Engagement that occurs before and after the formal consultation period on a discretionary, ad-hoc basis and without prejudice is referred to in this guidance material as **preliminary and ongoing engagement**. Discussion held during these periods is used to gauge the limits of the provider's existing capability and their willingness to offer voluntary assistance or preference for a legal obligation as they undertake assistance activities. The answers to these questions will determine which assistance instrument is appropriate. Ongoing engagement that occurs after an assistance instrument is issued may be used to discuss any extension, variation or revocation of the assistance instrument and any other issues raised by either party for the remaining lifetime of the assistance instrument.

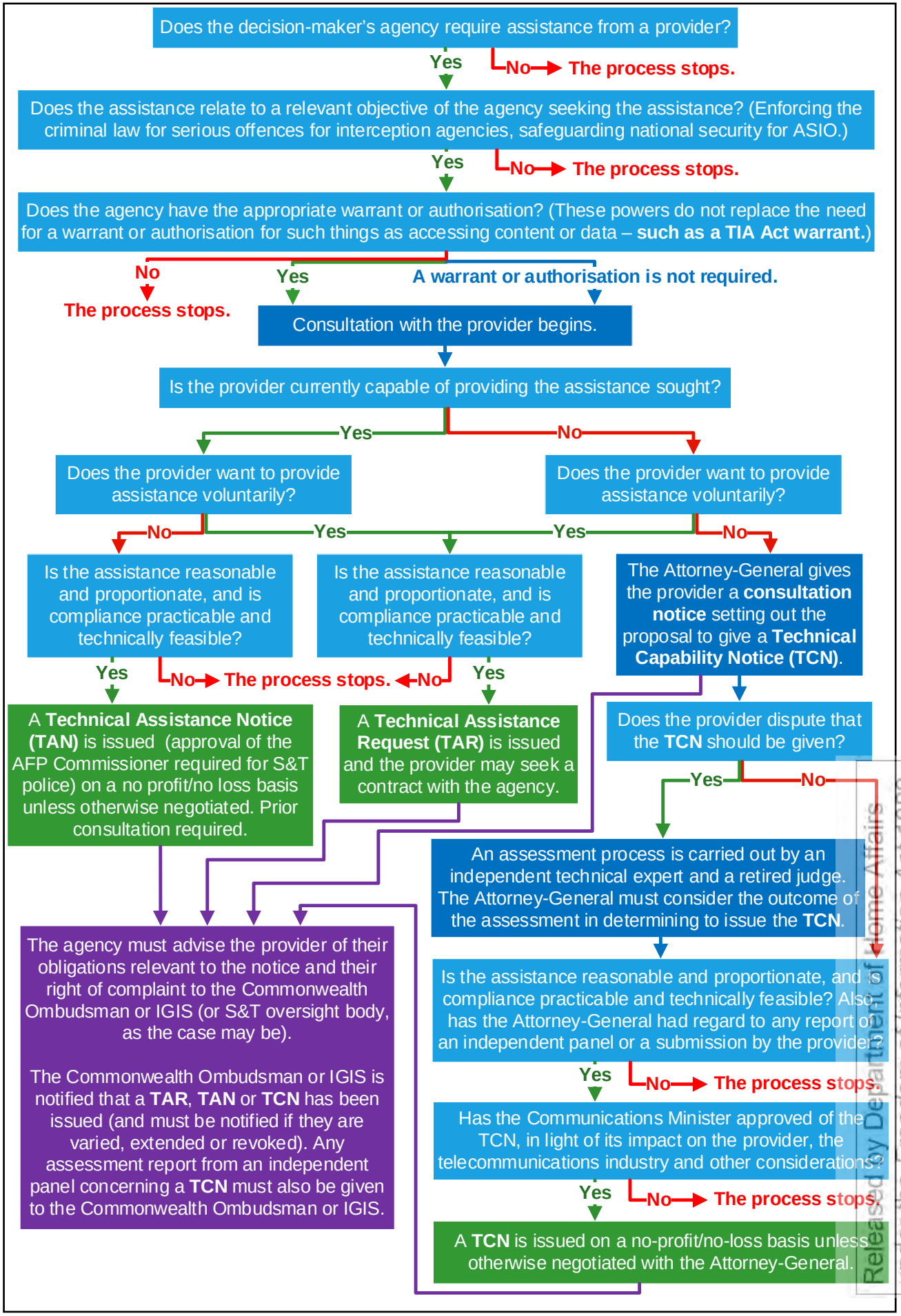
Formal consultation

Consultation prescribed by the legislation is known as **formal consultation**. Formal consultation carries specific legal requirements and feeds directly into the decision-making process that ultimately determines the provider's assistance obligations.

Consultation notice

A **consultation notice** is a written document given to a provider at the beginning of a formal consultation period. The notice specifies the beginning and end dates for the consultation, the proposed assistance instrument to be issued and the details of the assistance required. Consultation notices should be shaped by preliminary engagement with the provider.

ASSISTANCE PROCESS



ENGAGEMENT AND CONSULTATION

The above process is connected to a broader dialogue between Government and industry consisting of **preliminary engagement, formal consultation** and **ongoing engagement.**

This process of preliminary engagement begins when the provider is first approached regarding the possibility of offering assistance. Formal consultation then begins when the assistance instrument is issued or other legislative mechanisms are commenced and then merges into ongoing engagement. Ongoing engagement continues until the assistance instrument is no longer in effect. Figure X elaborates:

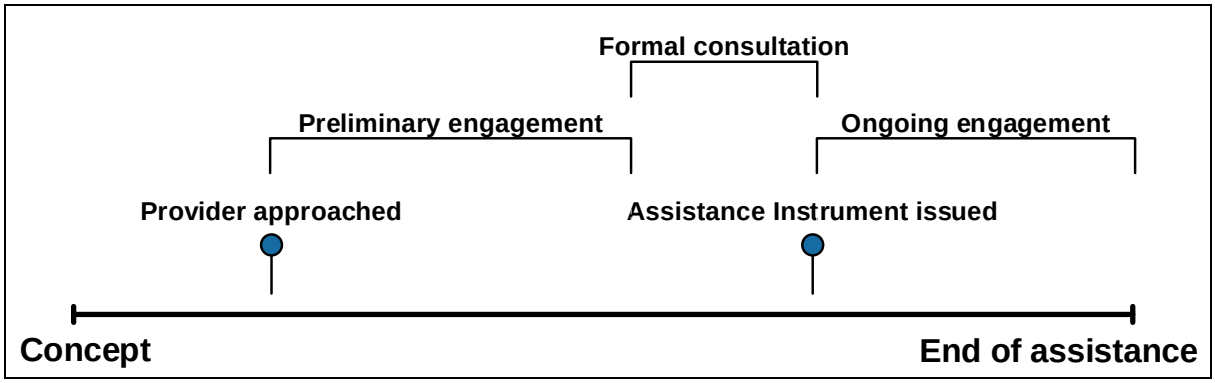


Figure X. Consultation and engagement timeline

The processes and expectations in each stage of engagement and consultation are outlined below.

PRELIMINARY ENGAGEMENT

Industry assistance relies on robust, comprehensive consultation and engagement to operate effectively. While formal consultation is required when issuing TANs or TCNs, it is important to communicate and engage continuously outside of this formal period for all types of assistance to ensure the parties have a shared understanding of their roles. While parties should engage in good faith during early consultation, the preliminary nature of this discussion means that it can occur "without prejudice" allowing possibilities to be canvassed without creating binding expectations regarding, for example, the provider's capabilities or the agency's timeframes for delivery. Only after this discussion should formal consultation, where it is required, be used to consolidate mutually acceptable terms between parties that have been generated through the broader engagement process.

Preliminary engagement should be used to answer several key gateway questions such as:

- the urgency and nature of the assistance
- the provider's willingness to offer assistance
- whether they would like to be engaged on a voluntary basis or have a legal compulsion present
- what the current capabilities of the provider are (this will also determine which assistance instrument is appropriate)

Robust and dedicated preliminary discussions are expected and will ensure that the central concerns of both parties and issues like the technical feasibility of assistance are suitably addressed. This window provides a good opportunity to assess each of the decision-making criteria to draft a decision acceptable to the provider.

Agencies should approach preliminary engagement without expectations of the precise technical solution required to offer the assistance they require. Instead, providers should be approached regarding the desired outcome and allowed to advise of the easiest and safest technical pathway to attaining it. This approach is consistent with the decision-making criteria set out in the legislation and recognises that providers themselves are best-placed to assess the technical limitations and possibilities of their systems and find a suitable mechanism to deliver assistance.

This kind of engagement is also an appropriate vehicle for answering more practical, but no less essential, questions regarding providers' resourcing commitments and development programme so as to cause the least possible interference to ordinary operations.

Providers are expected to maintain the confidentiality of discussions during this period.

MAKING CONTACT WITH PROVIDERS

Who to contact

The industry assistance framework represents a new approach to cooperation between government agencies and private companies that extends from assistance obligations in section 313 of the Telecommunications Act. As a descendent of earlier schemes, it is appropriate for agencies to rely on their existing relationships – where they have them – when using these powers. Larger providers are more likely to have operated under similar regulation previously and may have created a team dedicated to engaging with government to service law enforcement and intelligence needs. In these instances, it will only be necessary to locate this team by contacting the provider through a general contact portal.

A list of provider contacts within internet-focused companies used by American law enforcement can be found at this address: https://www.search.org/resources/isp-list/.

In cases where there is no dedicated law enforcement liaison team and the relevant provider is not likely to have offered previous assistance to agencies it may be prudent to meet with the provider and offer material to explain their obligations and establish trusted contacts between the parties. Ensuring that a provider is aware of their obligations under a notice or request is also a legal requirement and must occur as part of the formal process.

Contacting an individual within an organisation

If the most appropriate contact is an individual within an organisation, it **must** be made clear at this early stage that the assistance is sought from the organisation, company or corporate entity itself **and not** from the individual in their capacity as an employee of their company. In this sense, the individual is a representative of the corporate entity to whom the assistance request must be directed.

In these engagements exceptions to the use and disclosure rules which allow information about assistance to be disclosed for the purpose of administering or executing a notice are relevant (see paragraph 317ZF(3)(a)). This allows employees to disclose information within an organisation for the purpose of actioning assistance.

What information do providers need to communicate with agencies?

Where a provider is asked to assist for the first time, or otherwise asks for guidance about communicating with the agency, they should be given the details of a single point of contact (SPOC) within the agency through whom they can expect to receive all further correspondence. Providers should be informed of the SPOC's decision-making authority, which may be limited to passing correspondence, and informed who in the agency is authorised to make decisions under the legislation. Correspondence requiring higher level authorisation should nonetheless be transmitted through the SPOC where possible.

A provider may also be given a list of authorised contacts within the agency that can be quickly compared against any communication received in order to assess the authenticity of a communication.

NOTIFYING PROVIDERS OF UPCOMING FORMAL CONSULTATION

Because advice offered during formal consultation may carry potential legal consequences for how the provider's obligations are determined, it is important that providers have advance notice of an upcoming consultation and the time to prepare. However, as this is not a legal requirement, this notification is discretionary and may be given in whatever form the agency deems appropriate. As a best-practice model, agencies should assess the advance notification period required generously and provide their notification to the provider in writing, including a specified start date for the formal consultation period.

Notification of upcoming formal consultation becomes less stringent in circumstances where assistance of this kind has been provided previously or the agency has been informed by the provider that offering the assistance will not be challenging.

PRELIMINARY ENGAGEMENT WITHOUT PREJUDICE

Preliminary engagement will guide the formal consultations to allow the decision-maker to issue a legally binding assistance instrument. As such, statements and advice exchanged during this preliminary engagement should not be considered definitive until they have been confirmed during the subsequent, formal consultation.

This flexibility allows parties to discuss the possibilities of cooperation freely without fear that optimistic or initial ideas will be relied upon when setting the provider's assistance obligations. Agencies should raise any information provided during preliminary engagement again during

formal consultation to confirm that it is accurate and, once confirmed, only then rely upon it for decision-making purposes.

Despite this flexibility, this type of engagement should not be half-hearted. Forthright and frank discussions during preliminary engagement will allow formal consultation requirements to be more easily discharged and ensure the final decision is suitable to the provider's circumstances and the agency's assistance needs. Conversely, a failure to cover all areas of potential dispute or disagreement during this preliminary engagement may mean that a longer formal consultation is required during which parties may be less willing to discuss possible approaches or offer creative solutions.

FORM OF PRELIMINARY ENGAGEMENT

Preliminary and ongoing engagement does not carry form requirements. Providers may differ in their communication preferences and agencies should be responsive to these preferences wherever possible while mindful that it may be inappropriate to communicate sensitive information over certain channels.

There is no limit to the format of discussions that may occur as a result of the informal nature of preliminary engagement. Providers may prefer to be approached initially over phone and conduct later engagement through an exchange of emails or hold teleconferences on an ad-hoc basis as necessary. Parties should decide to hold discussions through whichever method of communication is most convenient and does not jeopardise sensitive information.

REPRESENTATIONS REGARDING THE DECISION-MAKING CRITERIA

Providers may wish to give input regarding the decision-making criteria that comprise the "reasonable and proportionate, practicable and technically feasible" issuing threshold (see 317JC for TARs, 317RA for TANs and 317ZAA for TCNs). Providers are best placed to understand their own legitimate interests which include any impact on the provider's business affairs, research and development efforts, personnel allocation, public appearance or other feature likely to impact the viability of the provider's business.

Providers may also wish to provide views and information on any of the other criteria as relevant and wish to express views regarding the relative weight to be given to the decision-making criteria in the circumstances. These representations should be used to identify critical areas for discussion and further consideration during the formal consultation.

Providers may also wish to make other representations where they are relevant to the decision-making criteria, including:

- The impact of assistance on the functionality of a product or service.
- The risk of tools being abused or stolen.
- Whether assistance can enable lawful access to a single users' data without impacting broader information security (if not, then the assistance will not meet the legal thresholds in section 317ZG).

Where providers do not proactively offer input regarding the relevant content and weight of the decision-making criteria, the decision-maker should provide comment ahead of formal consultation. Additionally, it is important to alert providers of their opportunity to comment on the decision-making criteria so they are given sufficient time to prepare comments, should they wish to, for consideration ahead of the decision to issue an assistance instrument.

Agencies may also use the preliminary engagement period as an opportunity to explain and contextualise the decision-making criteria as they understand them to apply in the circumstances. This advice will assist providers to make properly targeted and highly-relevant

representations that speak directly to the decision-making criteria and have the greatest likelihood of influencing the ultimate decision.

DETERMINING EXISTING CAPABILITY

Understanding the technical limits of a provider's ability to comply with an assistance instrument is a critical precondition to making a decision under the industry assistance regime. For example, TANs are only available to obtain assistance that a provider is currently able to offer and, as such, will be invalid if they require activities that are outside of existing capability (see subsection 317L(2A)). However, determining the limits of existing capability may not be a simple process or even possible for agencies as the necessary information is unlikely to be easily accessible. Providers themselves may need to perform an assessment of their systems to determine if the assistance can be offered without significant additional development.

This situation may be further complicated when providers and agencies do not share a common understanding of what amounts to an existing capability. For example, a provider's systems may not have a pre-built mechanism for performing the assistance sought but the provider may nonetheless employ personnel with expertise that enables them to easily perform the activity regardless of the system's apparent limitations.

Given these complexities, providers are best placed to advise agencies of the limitations of their existing capability and to resolve any ambiguity that arises from these questions. It is the role of agencies during this assessment process to sufficiently specify the outcome of the assistance they are seeking. This will enable the provider to conduct an appropriately limited assessment of their systems or allow them to set out relevant advice about their systems so the agency may make an assessment of their existing capability. Without a sufficiently narrow description of the desired assistance outcome, the provider may need to undertake an assessment far broader than necessary in the circumstances, causing undue delay.

Given the potentially broad scope of this assessment process, particularly in the case of more complex, technical assistance, it will be prudent to address the limitations of a provider's existing capability during preliminary engagement. Where providers determine that an assessment of their systems is required, additional time in advance of formal consultation may be required to make preparations to assess their systems. Agencies should accommodate these preferences as far as possible by giving generous advance notice to the provider of an upcoming formal consultation.

Where providers determine that they cannot offer a form of assistance, they may be asked to provide an explanation of how they made this assessment. The reasons for the unavailability of the assistance should be reasonable in the circumstances. In the case of trivial or less technically challenging kinds of assistance, the reasons provided for lacking capability may be scrutinised by the agency with a view to suggest an alternative, workable approach. Where an agency disagrees with the provider's assessment of their capability limits, this should also be raised during preliminary consultation.

BEING MINDFUL OF DEVELOPMENT CYCLES

As part of a consultation, agencies should seek to understand the provider's development cycle and predetermined resource allocation. Providers often make long-term resource commitments to project development based around their product release schedule – which itself may be confidential information, withheld from the public. Providing certain kinds of assistance to agencies may require them to reassign staff and disrupt their work schedules.

As such, it is important to identify when assistance can be offered at the least disruptive point in the provider's development cycle. Given the confidential nature of this information, providers may only be comfortable offering this advice after an agency initiates a formal consultation

immediately prior to issuing an assistance instrument. However, the provider's willingness to offer this information should be gauged early in the consultation process, and during preliminary engagement if possible, as it may have a significant impact on drawing the timeline for the final agreement.

Development outside of life-cycle will require consideration of the provider's development methodology, the method used to limit a capability to a single target device, the need to deploy a capability in a so-called "maintenance phase" and the challenge of limiting knowledge of the capability to only developers working on the project.

Agencies should also use preliminary engagement to discuss any real world factors that are likely to effect the provider's ability to offer assistance. These may include seasonal factors such as additional loads on the provider's systems over holiday periods or periods of "freeze" which typically occur on networks over December and January. Providers may also have preferences for when a capability could be deployed to minimise disruption to regular operations.

Considering these factors is particularly important when asking a provider to undertake capability development as this is more likely to be a resource-intensive process that may require significant reassignment of personnel.

SECURITY PROCEDURES FOR INFORMATION EXCHANGE

In light of the need to interact with a diverse range of providers at different levels of preliminary and formal engagement, there is a need to limit the extent that classified or otherwise sensitive information needs to be shared. Limiting the dissemination of such information is best practice in most circumstances. This is particularly true of preliminary and ongoing engagement that occurs on a discretionary basis and may be conducted primarily through unprotected channels.

Both agencies and providers should be aware that the unauthorised disclosure provisions may apply before a formal instrument has been issued. The definitions of *technical assistance notice information, technical assistance request information* and *technical capability notice information* to which these restrictions apply may capture aspects of preliminary discussions about the giving of an assistance instrument.

Where possible during preliminary engagement, agencies should separate the technical requirements of the assistance from information relating to the underlying investigation. This may enable engagement to occur primarily by reference to unclassified technical details that can be shared with limited security consideration. Similarly, providers should withhold commercially sensitive information to the extent they can engage in the consultation without relying upon it.

Where circumstances prevent preliminary engagement from occurring with only technical information, the technical information cannot be separated from other classified information, or the technical information itself raises security concerns, it may be necessary to use a secure method of communication to conduct the engagement. These channels may vary between agencies and providers but may include the GovDex platform and in-person engagement with appropriately cleared personnel using safe-hand methods.

Preliminary engagement is limited in its ability to facilitate the discussion of classified and confidential information due to its informality. Where multiple pieces of critical information are classified, it may be prudent to end preliminary engagement early and continue discussion during a formal consultation process. This will help to ensure that the information is handled with an appropriate degree of care and circumspection, and is not unduly disseminated over unsecured channels.

SHARED CAPABILITIES

It is possible for capabilities developed under Part 15 to be utilised and shared by multiple agencies across multiple jurisdictions. To ensure that there is central oversight and awareness of capability requests under a TCN, the Attorney-General may determine procedures and arrangements to be followed for requesting a TCN. These can require State and Territory agencies to approach certain Commonwealth partners before making a request for a TCN. This will allow the Commonwealth agency to determine if the current capability exists, or could be usefully shared among particular agencies and jurisdictions. It will also allow agencies in each jurisdiction to begin preliminary engagement with the relevant provider to discuss the feasibility of a shared capability and begin to assess and proportionate costs (see below for more detail).

In some cases, a requested capability will be unique to a particular agency and the centralised process will be unnecessary.

FORMAL CONSULTATION

Consultation is a legislative requirement prior to issuing a TAN or TCN. To distinguish from informal consultation that occurs outside of legislative requirements, legislatively mandated consultation is referred to as "formal consultation".

In addition to the formal consultation requirements, consultation will in almost all cases (including a TAR) be necessary for a decision-maker to meet the requisite legal thresholds and be satisfied of the reasonableness, practicality, proportionality and technical feasibility of an assistance instrument. The requirement to consider the interests of a provider, the impact on cyber security and the technical implications of the requested assistance will naturally involve detailed discussions with a provider.

Formal consultation offers an opportunity to reinforce understanding reached during the preliminary engagement regarding a proposed TAN or TCN. Formal consultation also presents providers with an opportunity to highlight concerns and interests to the decision-maker and feed directly into the decision-making process.

INITIATING AND CLOSING FORMAL CONSULTATION

Formal consultation begins on the date specified by the consultation notice given to the provider by the agency seeking assistance. The giving of a consultation notice is a legislative requirement of the TCN issuing process (see section 317W) and administrative best practice in the TAN issuing process. Consultation notices specify the start and end dates of the formal consultation, and the specifications of the assistance required, as discussed and refined during preliminary engagement.

Issuing a consultation notice is also important for setting out which assistance instrument – between a TAN or TCN – is proposed to be issued. This is a crucial step as it specifies whether the issuing authority considers that the provider has the capability to provide the identified assistance – having discussed this during preliminary engagement.

As the starting point for the legally prescribed aspects of industry assistance, consultation notices also explain the provider's rights and potential obligations up to and following the issue of an assistance instrument in addition to the safeguards and limitations that cover the assistance itself. This ensures providers understand their rights of complaint and the grounds for appeal if they disagree with the conduct of a decision-making agency during formal consultation or the ultimate decision once issued.

Additional advice when issuing TANs

Giving a consultation notice may be unnecessary where the provider has waived the formal consultation period for a TAN or is otherwise comfortable with the interactions that occurred during preliminary engagement for a TAN. Where the provider is comfortable being issued with a TAN without first receiving a consultation notice and undergoing further consultation, the preliminary engagement may satisfy the legislative requirement to consult the provider. This approach may be appropriate where a provider is asked to give assistance they have previously offered once again or the assistance is otherwise substantially similar to that required by a previous TAN. Agencies should not feel required to give a consultation notice in these circumstances.

FORM OF CONSULTATION

There is an expectation that representations made during formal consultation can be relied upon by the decision-maker. As such, there is a need to record communications in the form of an exchange of submissions or, in the case of meetings, meeting memorandums that are

agreed to by both parties. Good documentation practices ensure that the decision-maker has a reliable record on which to base any decision to issue an assistance instrument and allows them to refer to the representations that have been exchanged if called upon to give reasons supporting their ultimate decision. However, the format of the consultation will also need to be determined by reference to the complexity and urgency of the assistance proposal.

Detailed record-keeping should be preferred where possible as it will assist inspections on the use of the industry assistance framework by the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman and the relevant State and Territory oversight bodies. Additionally, comprehensive records of formal consultation help ensure that the decision to issue an assistance instrument is protected from any challenge on the basis of insufficient formal consultation.

Similar to the methods used during preliminary engagement, providers' may differ in their preferences with regards to communication methods during formal engagement. Being flexible and responsive to these preferences is also important to ensure the consultation is procedurally fair.

ENSURING PROCEDURAL FAIRNESS

In light of the decision-making agency's ability to place legal obligations on the provider – particularly when consulting a smaller provider that may not have offered assistance previously – there is the potential for an imbalance of power to emerge during discussions. As such, agencies should make positive efforts to address any pressure inadvertently exerted on the provider by this imbalance. Ensuring the provider is comfortable at the beginning of formal consultation and feels prepared to offer their fully-considered views in a venue acceptable to them is important to establish rapport and build procedural fairness into the consultation process.

Where providers remain unclear regarding their legal rights during this process or have any outstanding questions, this may interfere with procedural fairness and formal consultation presents an opportunity to provide definitive answers. Ensuring that a provider has full understanding of their obligations is necessary throughout the lifecycle of an assistance instrument.

Establishing procedural fairness goes beyond making sure all legal requirements are discharged and the provider is given a proper hearing for their concerns. It also includes giving the provider the information required to properly engage with the formal consultation process and avoiding the exertion of pressure by setting requirements that may effectively limit the provider's right to be heard by the decision-maker. Where procedural fairness is not provided, the ultimate decision to issue an assistance instrument may be opened to court challenge.

LEGAL REQUIREMENTS OF CONSULTATION

Formal consultation requirements differ according to the assistance instrument in question. The flexibility or rigidity of these requirements will reflect the voluntary or compulsory nature of the assistance instrument and the potential complexity of the assistance possible under the assistance instrument.

Failing to observe formal consultation requirements may provide grounds to invalidate an assistance instrument where this failure interferes with the procedural fairness of the decision-making process or contravenes a legal requirement. Therefore, even in cases where a provider asks to forgo a formal consultation, efforts should be made to satisfy the procedural requirements provided by the legislation.

TARs do not require formal consultation

Formal consultation is not legally required before a decision-maker issues a TAR.

Practically, an agency will need to discuss their assistance request with the provider to the extent necessary to determine that the provider is willing to offer assistance voluntarily and the terms under which the assistance is to be provided. Ongoing engagement may also be needed before any variation or revocation of a TAR occurs.

As noted above, it is expected that some exchange of information and consultation will be needed to satisfy the decision-making thresholds of a TAR in sections 317JAA and 317JC.

The necessity of these consultations depends on the provider's desire to offer assistance and the need to allay any concerns they may have regarding the requested assistance. If a provider is unsatisfied with the level of consultation, they may refuse to offer assistance requested by a TAR.

Legal TAN consultation requirements

Consultation of a proposed TAN is a legal requirement before a TAN can be issued to a provider. While there are no legal provisions for how this consultation is to occur this does not alleviate the requirement for agencies to engage in meaningful and constructive dialogue with a provider.

In light of this discretion, the period for the consultation should be agreed with the provider in advance and agencies should refer to best practice principles when giving a consultation notice or otherwise informing the provider of the timeframe and proposed assistance.

Additionally, and as further detailed below, a consultation period may be waived under subsections 317PA(2) and (3) where the Director-General or Chief Officer is satisfied that the TAN should be given as a matter of urgency.

Legal TCN consultation requirements

A TCN consultation must begin with the Attorney-General giving a consultation notice. This consultation notice must:

- set out a proposal to give the TCN, and

  This proposal should detail the nature of the assistance required and the specifications of any capability that the provider will be required to build.

- invite the provider to make a submission to the Attorney-General on the proposal.

  As part of the consultation, the Attorney-General must consider any submission received within the time limit specified by the consultation notice.

The period of time for the consultation provided in the consultation notice must be *at least* 28 days however a suitable length for the formal consultation should be agreed with the provider. In many cases a period longer than 28 days will be necessary, particularly for proposed capabilities with a degree of complexity. In these cases the proposals may require a thorough examination by both parties to ensure they do not contravene the prohibition against systemic weaknesses and ensure that the integrity of a providers systems remain intact.

As set out in subsection 317W(3), this consultation may be waived where the Attorney-General is satisfied that the TCN should be given as a matter of urgency or the consultation may be truncated when it is impracticable to hold a 28 day consultation.

A separate consultation must occur before a TCN can be varied. This new consultation carries the same legal requirements as when the original TCN was proposed.

REFERRALS TO THE INDEPENDENT PANEL

Providers given a consultation notice that proposes the issuing of a TCN may write to the Attorney-General within the consultation period specified by the consultation notice requesting that an assessment of the proposed TCN be conducted. Once the provider has referred the consultation notice for review, the Attorney-General **must** appoint two assessors to carry out an assessment of whether the proposed TCN should be issued.

One of the assessors must be a person:

- with knowledge that allows them to assess whether a proposed TCN would create a systemic weakness, and
- be cleared to the highest level required by staff members of ASIO or such a lower level as the Attorney-General approves.

The other assessor must be a person:

- who has served as a judge in a prescribed court for a period of at least five years and has since retired.

> Prescribed courts are the High Court, the Federal Court of Australia, the Supreme Court of a State or Territory, or the District Court (or equivalent) of a State or Territory.

The appointment of the assessors is a matter for the Attorney-General under advice of the relevant agency and the provider. While the identities of the assessors may not be made public, the relevant parties to the proposed assistance instrument will have insight into the assessors' appointment and be given the opportunity to independently vet their backgrounds and relevant experience.

Where confidential and trade-sensitive information must be shared with the assessors in order to carry-out their review, the assessors will be required to make appropriate non-disclosure undertakings to protect this information. These non-disclosure undertakings will also ensure assessors only make disclosures of relevant information to Government agencies and do not otherwise reveal information outside of the remit of their review. Assessors are also subject to the non-disclosure requirements in section 317ZF. Otherwise, assessors will be chosen partly on the basis of their ability to operate with sufficient discretion to avoid harming the provider's business activities and in consideration of any conflict of interest.

A copy of any report made by the assessor is required, by law, to be given to the provider, the Attorney-General and the relevant independent oversight body. This ensures that any finding can be scrutinised, and actioned upon, by the necessary party. By law, the findings of any assessor must be considered by the Attorney-General before a decision to issue a TCN is made and will be extremely influential in any considerations by this decision-maker. Providers and oversight bodies will therefore be aware of the outcomes of an assessment when considering the Attorney-General's issuance, or non-issuance, of a notice. This will provide context if a provider should seek judicial review of the administrative decision.

The independence of the assessors will be ensured by allowing them to set their own time limits for the review (within reason) and allowing them to make their own determinations regarding the legal thresholds and safeguards provided by the legislation. The opinions of the assessors will be provided on the basis that they offer accurate analysis and avoid negatively impacting systems during their testing.

CONSIDERATIONS FOR THE MINISTER FOR COMMUNICATIONS

The Attorney-General must not give a TCN unless the Minister for Communications has approved the giving of the TCN. The Minister for Communications is required to assess the

impact of the proposed assistance on the telecommunications industry. Providers may wish to make representations to the Minister for Communications regarding the decision-making criteria listed in section 317TAAA(6).

Providers may also wish to make representations to the Minister regarding:

- the potential impact on a range of industries
- whether the assistance is sought from a point in the supply chain that is the least onerous
- the availability of remedies for any harm suffered by the provider
- the potential reputational costs to the provider
- In addition to the Minister's decision-making criteria listed in the legislation, the Minister may also choose to consider, as part of the discretionary criterion, a number of additional items to make his determination.[3]

The Minister may also have the opportunity to review any documentation that were made available to the Attorney-General, including representations made during formal consultation and the report of the independent assessment panel, if one was appointed.

For additional guidance in this area, please contact the Department of Communications and the Arts via their contact page at https://www.communications.gov.au/who-we-are/contact-us.

WAIVER OF FORMAL CONSULTATION

Formal consultation prior to issuing a TAN or TCN may be waived in certain circumstances. Where this occurs, an appropriately senior executive within the organisation of the provider should be notified directly through a phone call or similar means of communication. This will minimise the dissemination of the information throughout the organisation and allow decisive action to be taken to quickly offer the assistance.

Provider-waived consultation

Providers may elect to waive the consultation required before the issue of a TAN or TCN. Under the legislation providers may waive consultation for any reason they choose.

For example, where the assistance is a kind that has been offered previously and the provider considers that consultation is unnecessary for this reason, waiving consultation may make sense. Another example may be a provider who states a preference to be issued with a compulsory assistance instrument so that their actions are anchored to a legal obligation rather than a voluntary TAR. In this case, the provider may not have concerns regarding the assistance itself and may waive the formal consultation in order to expedite the timeframe.

Consultation forgone by an agency

The decision-maker may forgo consultation before the issue of a compulsory assistance instrument in circumstances where they consider the assistance instrument should be given as a matter of urgency.

The decision-maker has discretion to determine what circumstances are sufficiently urgent to require assistance be provided without formal consultation. Generally, urgent circumstances are those where there is a high likelihood of imminent loss of life or large-scale property damage if the assistance is not offered immediately. However, the exact boundaries of the meaning of urgency are a matter for the decision-maker in the case.

Providers that are unsatisfied by the reason for waiving consultation, may seek a court injunction while the decision undergoes judicial review. However, given that the reason for

[3] The considerations for the Minister for Communications will be subject to separate guidance material developed by the Department of Communications and the Arts.

urgency may relate to an imminent threat to national security, sharing the complete details of the urgent circumstances with the provider may raise particularly difficult security concerns. Waivers of consultation on the basis of urgency should be used rarely and only in extreme circumstances to ensure providers are willing to comply with an urgent assistance instrument rather than pursue judicial intervention in the courts. Equally providers should respect the gravity of an assistance instrument issued in urgent circumstances and not seek to forestall it unnecessarily.

Where an agency forgoes consultation because of urgency, they should undertake forthrightly to accept the reasonable conditions and costings offered by the provider where, under ordinary circumstances, they may have negotiated. This is appropriate given the need to expedite the assistance process and given the provider's cooperation is being offered outside of the ordinary procedure. This will also ensure that the ability to waive consultation is not exercised lightly. More broadly, a strong relationship with the provider will be important when seeking urgent assistance.

In light of the complexity and resource-intensiveness of building new capability, it is unlikely that a TCN could be considered a matter of urgency such that waiving consultation is appropriate. However, an urgent TCN may be appropriate where it is unclear whether the provider has the capability required and lacks the time to perform the capability assessment needed to gather this information. In this case, the provider may need the additional compulsion offered by a TCN to use newly built tools in order to provide the assistance.

CONSULTATION WHEN VARYING OR REPLACING A TCN

The decision to vary an assistance instrument may impose a similar impact on a provider as the decision to issue the original instrument – and this is particularly true in the case of variations of TCNs. As such, it is legally required that a new consultation process occur to consider the varied TCN.

This new consultation occurs as if the variation was itself a new TCN and requires that a new consultation notice be issued from which a new independent assessment panel may be appointed, and the variation must be approved by the Minister for Communications. In practice, where a TCN variation does not fundamentally change the nature of the original TCN, the information generated by the previous TCN consultation may suffice and it is not envisaged that a fresh independent assessment would be necessary.

A replacement TCN, that is the same or substantially the same as a TCN previously given to the provider, also requires that the Attorney-General consult the provider. However, there are no legal requirements regarding the nature of this consultation.

ONGOING ENGAGEMENT

Following issue of an assistance instrument at the conclusion of a formal consultation period, ongoing engagement may still be needed to answer any questions that arise from the instrument to confer regarding the design of the assistance, or to discuss the timeline for delivery and testing. Several matters might be outstanding after an assistance instrument is issued and new practical concerns may continue to arise. It is appropriate that these be addressed directly through ongoing engagement.

Ongoing engagement may continue as required for the lifetime of the assistance instrument to answer questions raised by either party and ensure the assistance is operating as designed. In some cases, such as when an agency requires the use of a provider's capability to collect or access information, direct communication will be necessary on each occasion, including to notify of the existence of a required warrant or authorisation.

Ongoing engagement is also a useful vehicle for discussing proposals to revoke, vary or extend an assistance instrument. While formal consultation is required when varying or replacing a TCN, other extensions, variations and revocations of assistance instruments do not require formal consultation.

An agency must notify the relevant independent oversight body (the Commonwealth Ombudsman or the Inspector-General of Intelligence and Security) within seven days whenever an assistance instrument is extended, varied or revoked.

EXTENSION

Decision-makers may decide to extend an assistance instrument that is either a TAN or a TCN for up to 12 months. This extension is only effective with the provider's consent. Therefore it is necessary for the decision-maker to engage with the provider before making this decision to ensure they are comfortable with the new period of expiration.

As there is no 12 month limit on TARs, the necessary lifespan of the voluntary assistance should be determined during preliminary engagement and formal consultations to avoid the need for re-issue. Decision-makers may effectively extend a TAR by issuing a new TAR in the same terms as the expired TAR. Providers should be consulted where a decision-maker wishes to issue a new TAR in such circumstances.

Before issuing an extension notice, the decision-maker must engage with the provider to determine whether the proposed new timeframes for delivery would be appropriate and feasible. The agency and provider must also negotiate the necessary amendments to the contractual arrangements attached to the original assistance instrument. For extensions, changes to the contractual agreement will likely be limited to key dates and deliverables timelines.

Once the decision-maker and provider have agreed to the changes to the notice, an extension notice will be given to the provider. Extension notices will be provided, in writing, as an attached schedule to the original notice. The extension notice will specify the period which the assistance instrument will remain in force and the new expiry date. The provider will also receive the amended contractual agreement attached to the notice.

The extension provisions are the only vehicles to extend the lifespan of a notice. This cannot be achieved through variation.

VARIATION

Decision-makers may vary an assistance instrument that is either a TAR or TAN without undergoing formal consultation when satisfied that it would be reasonable, proportionate,

practicable and technically feasible to do so. However, it is important and expected that any variation to a TAR or TAN is discussed with the provider through ongoing engagement. In effect, it is likely that consultation will assist with satisfying the legal thresholds set out in the decision-making criteria.

Depending on the size and complexity of the assistance, varying an assistance instrument may have a significant or a negligible impact on the provider. In situations where the variation is a minor change, agreement may be easily negotiated between parties without the need for substantial new engagement. More significant variations will naturally require a longer period of ongoing engagement to ensure the provider is comfortable with the varied assistance instrument and to provide the decision-maker enough information to satisfy the decision-making criteria.

Consultation when proposing to vary an assistance instrument is also important to ensure the provider is comfortable that the variation does not fundamentally change the character of the assistance instrument and that continued cooperation will be possible. Where a provider represents to a decision-maker that a variation makes fundamental changes to the kind of assistance provided by the original assistance instrument, the decision-maker should consider if a new assistance instrument (and if required accompanying contractual agreement) should be issued instead of the variation.

For variations, agencies and providers may also be required to negotiate variations to existing contractual agreements outlining the terms and conditions of compliance. Depending on the complexity of the assistance required, the contractual agreement may require substantial changes to ensure that the interests of the agency and provider are met. That is why it is important for agencies and providers to work cooperatively in developing the varied assistance delivery plan to ensure that agencies meet their objectives and provider's operations are unaffected.

Following engagement with the provider, the decision-maker may decide to issue a variation notice. Variation notices will be provided, in writing, as an attached schedule to the original assistance instrument. The variation notice will stipulate the listed acts or things the provider is required to perform as part of the variation, and relevant information concerning safeguards and limitations.

REVOCATION

Where a provider believes that an assistance instrument is no longer reasonable and proportionate or practicable and technically feasible and believes it should be revoked, they may make representations during ongoing engagement to this effect. The decision-maker must then revoke the assistance instrument where they are satisfied that the assistance instruments are no longer reasonable and proportionate, or that compliance is no longer practicable and technically feasible (see sections 317JB for TARs, 317R for TANs and 317Z for TCNs). This revocation requirement is an opportunity for reassessment of the notices when circumstances change and new information comes to light.

Decision-makers also have the ability to revoke any assistance instrument freely if they decide to in the circumstances. However, revoking an assistance instrument should not be done lightly. Where a decision-maker chooses to revoke an assistance instrument, they should consult with the provider to ensure the provider will not be adversely affected by the early conclusion of the assistance instrument. In order to offer assistance, providers may have altered their development timeline for other projects and relocated personnel. As such, revocation of an assistance instrument can have financial consequences for the provider. Early conclusion through elected revocation may also have financial consequences for the decision-maker's agency where a contract between the parties addresses such a situation.

After consultation, if the decision-maker is satisfied that the assistance instrument no longer meets the requirements set out in the decision-making criteria, they must issue a revocation notice. Revocation notices will be provided, in writing, as an attached schedule to the original assistance instrument. The revocation notice will advise that the assistance instrument is no longer in effect and that legal obligations to provide assistance have been revoked. Any contractual arrangements between an agency and a provider should be separately terminated in accordance with the terms and conditions of that contract.

COSTS ASSESSMENT

DETERMINING COSTS

Providers are not expected to bear the reasonable costs of complying with an assistance instrument for assistance themselves. Reasonable costs refer to the costs necessary to satisfy the requirements under an assistance instrument, not the provider's expenditure. Costs incurred by a provider that cannot be reasonably attributed to the requirements in a TAN or TCN or are otherwise excessive are not recoverable. .

In receiving a request for voluntary assistance, a provider may negotiate with the relevant issuing agency on financial arrangements and terms. However, when a provider receives a notice compelling assistance, they are expected, by default, to comply on the basis that they will neither profit nor lose money. Costs are determined by the applicable costs negotiator, that is, the head of the issuing agency for TANs, or a person specified by the Attorney-General for TCNs.[4] The role of applicable costs negotiator is non-delegable and therefore reserved for the head officer of issuing agencies or the Attorney-General.

NO-PROFIT/NO-LOSS

No-profit/no-loss compliance will apply to a notice unless the provider and the applicable costs negotiator agree otherwise or the decision-maker is satisfied that it would be contrary to the public interest (see subsection 317ZK(3)). The provider and applicable costs negotiator may decide to forgo no-profit/no-loss compliance and agree to determine costs in commercial terms. Commercial terms may be appropriate in cases where a large bespoke capability is required or the assistance needs to be actioned as a priority. This will allow an agency to enter into an arrangement with financial incentives and risk-management measures to secure satisfactory and timely performance from the provider.

The no-profit/no-loss basis of compliance may not be appropriate in exceptional circumstances where it is against the public interest to fully compensate a provider (see below).

MAKING A COST ASSESSMENT

During preliminary engagement, the agency and provider are expected to engage in collaborative discussion concerning cost arrangements. It is best practice for the issuing agency to request that the provider conduct a preliminary assessment on the costs for providing assistance. The provider may conduct a preliminary cost assessment in accordance with their own standard practices. The nature of the preliminary cost assessment will depend on the provider's business and the assistance being sought. The preliminary assessment undertaken by the provider and the operational needs of the issuing agency will then be considered during the formal cost assessment made by the applicable costs negotiator. As a general note, the applicable cost negotiator should also have regard for:

- the complexity of assistance
- the size and capability of the provider
- the opportunity costs associated with providing the assistance, and
- other matters the applicable cost negotiator considers relevant.

[4] The Attorney-General may determine procedures and arrangements relating to requests for TCNs which will be the subject of separate guidance material.

The provider and applicable costs negotiator should reach an agreement as to costs, having regard to both assessments. If an agreement cannot be reached an arbitrator, approved by both parties, may be appointed to determine an alternative rate of compensation (see below).

SHARED CAPABILITIES

Where a capability developed by a provider is requested by multiple agencies, it will be the responsibility of relevant agencies to determine and allocate costs accordingly. The provider should only have to deal with a single point of contact, the **applicable costs negotiator**, with the proportioning of costs negotiated among Government parties. To the extent that individual agencies need to seek assessments from the provider, this should be as streamlined as possible.

PUBLIC INTEREST EXCEPTION

The decision-maker may also enter into an alternative cost arrangement if they are satisfied that no-profit/no-loss compliance would be contrary to the public interest. An alternative cost arrangement may mean that a provider receives only partial compensation for their assistance or is required to assist without compensation. In making this determination, the decision-maker must consider:

- the interests of law enforcement (where the notice was issued by an interception agency)
- the interests of national security (where the notice was issued by ASIO)
- the objects of the Act
- the regulatory burden of complying with the mandated assistance on the provider, and
- other matters the decision-maker considers relevant.

The threshold to satisfy this test is high and it is expected a decision-maker will only be able to meet the requirements in exceptionally rare circumstances. For example, where a provider's conduct has wilfully created a security risk or specifically designed their services for illicit use. It may also be appropriate in cases where the provider subject to a notice acted recklessly or negligently in providing the required assistance and it would be inappropriate to compensate the provider.

Section 317ZK allows a decision-maker to 'turn-off' some or all aspects of the cost-recovery framework. For example, it may be appropriate not to compensate the provider fully for assistance rendered but it may still be appropriate to settle the terms and conditions of compliance by agreement. In this case, the decision-maker can remove the need for no-profit/no-loss assistance by satisfying the statutory test but retain the availability for arbitration in the case of disputes (see 317ZK(4)).

APPOINTING AN ARBITRATOR TO RESOLVE DISPUTES

If the provider and applicable costs negotiator fail to agree on the terms and conditions of compliance with a notice, an arbitrator, approved by both parties, may be appointed to resolve the dispute. Both parties may wish to consider a number of items in appointing arbitrators. At a minimum, arbitrators should have relevant arbitration experience and be thoroughly assessed and appropriately cleared to conduct the necessary activities for arbitration. It may be valuable, especially in cases where providers are required to provide complex assistance, for appointed arbitrators to have relevant technological knowledge.

If both parties cannot agree on the appointment of an arbitrator, the ACMA will appoint the arbitrator if the provider is a carrier or carriage service provider. For all other types of designated communications provider, the Attorney-General appoints the arbitrator where parties cannot agree. Arbitrators will be able to be appointed from a selection of persons, or

specified class of persons, nominated by the Minister for Home Affairs (in consultation with the Attorney-General).

Carriers and carriage service providers will be required to share the cost of arbitration equally with the issuing agency. Where a provider is neither a carrier nor carriage service provider, the Minister for Home Affairs may make provisions relating to the conduct of arbitration, including provisions relating to the costs of arbitration.[5]

The type of persons suitable to be arbitrators will generally be persons of integrity, independent from both parties, with expertise in telecommunications law or professional qualifications as mediators or arbitrators. These considerations will inform advice to the Minister regarding appointments. The Minister may also seek input from the provider when selecting an arbitrator from a list compiled by the Department of Home Affairs.

[5] Instruments for managing arbitration will be set out in additional guidance material.

SERVICE AND STANDARD FORMS

SERVING ASSISTANCE INSTRUMENTS

TARs, TANs and TCNs should be served to the relevant provider in written format. Agencies seek assistance by serving an assistance instrument appropriate to the type of assistance required. Assistance instruments will specify certain information and advice that must be communicated to providers in addition to certain, discretionary matters. Further information and guidance concerning the specific details of the required assistance should be determined in consultation with the provider and be issued as an attachment to the assistance instrument in a standard form contract.

The process for service of TANs and TCNs is set out in section 317ZL.

Points of Service

In the initial instance, an agency should approach the provider about the possibility of giving assistance through their designated single point of contact. Alternative channels for further engagement, including for the issue of assistance instruments, may be determined by the agency and provider during these early consultations. Providers should provide a postal address, and/or electronic address for service. Agencies should serve assistance instruments through the preferred channel indicated by the provider.

Any documentation in relation to an assistance instrument is deemed to be served on a provider if it has been left at or sent to the nominated address, or sent to the nominated electronic address, of the provider.

Service may also be made by giving the assistance instrument, or leaving the assistance instrument, at an address where a body carries on a business or conducts activities at an address in Australia. Service may also be effected if an assistance instrument is served on an agent, located in Australia, of an offshore body corporate. Further guidance for service requirements are provided by sections 28A and 587 of the Acts Interpretation Act.

Service should always be directed at a corporate entity and in a manner that ensures the corporate entity is aware of the assistance instrument.

Requirements when issuing an assistance instrument orally

All assistance instruments should be served on providers, by default, in writing. However, there are limited circumstances which allow a TAR or TAN to be initially issued orally and then subsequently written down. TARs and TANs may only be issued orally if the assistance instrument is necessary to deal with an imminent risk of serious harm to a person or damage to property, and it is not practicable to give the assistance instrument in writing. If an assistance instrument is issued orally, a written record must be made within 48 hours of issue. Written copies of these records must be given to the provider as soon as practicable after the record is made.

In cases where it is reasonable to do so, providers may expect an undertaking as to the seriousness of the situation from the agency where giving specific details is infeasible.

SEEKING APPROVAL FROM THE AFP COMMISSIONER

The AFP Commissioner plays a central coordination role for the issue of TANs by State and Northern Territory police forces (see section 317LA). In order to issue a TAN, State and Northern Territory police forces must provide written notice to the AFP Commissioner setting out a proposal and seeking approval to issue the notice.

Importantly, the AFP Commissioner will play a central role in reducing duplicate requests, facilitating inter-agency information-sharing, and advising on the type of assistance required to achieve the agency's objective. The AFP Commissioner will also be able to ensure that the measures in the legislation are being applied consistently and assist in managing cost arrangements for the delivery of assistance. State and Northern Territory police forces are expected to engage closely with the AFP through established channels on the development of TANs.

Approval to issue the notice should be given by the AFP Commissioner in writing. Approval should only be given orally in urgent circumstances and a written record must be made within 48 hours of giving the approval. Once the provider has received approval from the AFP Commissioner, they may follow the appropriate channels to issue the notice.

AFP Procedures

Written requests for approval of a TAN are to be submitted to the External Enquiries Team (EET) by email: TID-Technical-Notices@afp.gov.au or for further administrative assistance by calling (02) 5126 9146. EET is the AFP's centralised coordination and quality assurance site for all TANs.

The EET will engage Digital Surveillance Team (DSC) to reduce duplication across jurisdictions, facilitate a coordinated and consistent method of engagement with designated communication providers and may value add through recommending other forms of assistance.

As the central coordination point for TANs, EET will seek approval through the AFP Commissioner and notify the State or Territory applicant of the outcome on completion.

An urgent TAN, per section 317M Form of technical assistance notice, may be verbally requested from the chief officer of a Police Force of a State or Northern Territory to the AFP Commissioner.

A State or Northern Territory police force maintains responsibility for their variations, revocations and annual reporting responsibilities.

DELEGATING AUTHORITY

In some cases, decision-makers may choose to delegate some or all of their functions under the Act to other senior position holders in their organisation. Delegation enables persons with the appropriate seniority and expertise to perform functions under the Act by streamlining processes and assisting agencies in discharging their statutory functions. The delegation must be in writing and clearly specify to whom the function is delegated. The delegate must also comply with any written directions provided by the decision-maker. Agencies should advise providers of the delegated positions in their respective organisation.

ASIO

The Director-General of Security may delegate any or all of the functions in relation to voluntary assistance, TANs and the use and disclosure of information to a person who holds a position that is equivalent to, or higher than, a position occupied by a Senior Executive Service employee or a person designated as an office of Coordinator by the Director-General.

ASIS

The Director-General of the Australian Secret Intelligence Service may delegate any or all of the functions in relation to voluntary assistance and the use and disclosure of information to a person who holds a position that is equivalent to, or higher than, a position occupied by an Senior Executive Service employee.

ASD

The Director-General of the Australian Signals Directorate may delegate any or all of the functions in relation to voluntary assistance and the use and disclosure of information to a person who holds a position that is equivalent to, or higher than, a position occupied by a Senior Executive Service employee.

AFP

The AFP Commissioner may delegate any or all of the functions in relation to voluntary assistance, TANs and the use and disclosure of information to the Deputy Commissioner or a senior executive AFP employee declared by the Commissioner.

ACIC

The CEO of the ACIC may delegate any or all of the functions in relation to voluntary assistance, TANs and the use and disclosure of information to a position occupied by a Senior Executive Service employee.

State and Territory Police Forces

The Commissioner of Police may delegate any or all of the functions in relation to voluntary assistance, TANs and the use and disclosure of information to an Assistant Commissioner, a Superintendent or a person holding an equivalent rank.

CONSULTATION NOTICES

Consultation notices for TCNs

The Attorney-General must undertake a consultation process before a provider is required to comply with a TCN. The Attorney-General must give the provider a written **consultation notice** inviting the provider to make a submission on the proposed TCN.

Consultation notices will specify a timeframe for the consultation period which must be at least 28 days, unless the provider has waived consultation or the proposed notice should be given as a matter of urgency. Providers will also be advised of the details of the proposed assistance, matters determined in preliminary engagement, safeguards and thresholds, immunities, non-disclosure requirements and the proposed terms and conditions of assistance in the notice. A consultation notice for a TCN will also notify a provider of their right to refer a TCN for independent assessment.

Consultation notices for TANs

Unlike consultation notices for TCNs, there is no legislative requirement to give a consultation notice for a TAN or form requirements regarding their contents. Additionally, the consultation notice may be given by any member of the agency, not merely the decision-maker.

However, consultation is a legal requirement prior to issuing a TAN and agencies may wish to use an administrative consultation notice to document that this process has occurred. Such a consultation notice should include many similar features as that for a proposed TCN such as information regarding the assistance proposal and advice regarding the provider's rights and obligations. Consultation notices for TANs will also specify the timeframe for the consultation period, which is not restricted by a requirement of at least 28 days.

More information regarding consultation notices is included in the Formal Consultation section above.

MATTERS CONTAINED IN ASSISTANCE INSTRUMENTS

Assistance instruments serve to clearly set out the rights, responsibilities and obligations of the provider. The assistance instrument template has been designed to be accessible to all providers, regardless of the assistance required, and are directed at the corporate entity by

default. Cost arrangements and contractual questions, where these arise, will be set out in an attached standard form agreement.

The following headings detail the information contained in each assistance instrument.

Details of the assistance requested

The issuing agency will list the assistance sought from the provider as it relates to the assistance categories listed in section 317E of the Telecommunications Act. The provider will also be advised that compliance with the assistance instrument is voluntary (for TARs) or mandatory (for TANs and TCNs).

Safeguards

The safeguards segment of an assistance instrument notes that the assistance sought must be connected to the eligible activities of the provider as listed in section 317C of the Telecommunications Act. Assistance must also relate to the issuing agency's functions as set out in section 317G, 317L and 317T (corresponding with TARs, TANs and TCNs), must not create systemic weaknesses or vulnerabilities, and must be given in tandem with a warrant or authorisation in force – where this is required.

Immunities

This part advises that assistance instruments confer immunity on providers and their officers, employees and agents. This immunity prevents civil liability in relation to an act or thing done in compliance, or in good-faith in purported compliance, with the assistance instrument. The immunity also excludes criminal responsibility for acts or things done in compliance with the assistance instrument for an offence against subsection 474.6(5) and Part 10.7 of the Criminal Code.

Non-disclosure requirements

This part provides advice regarding the extent of the non-disclosure rules which govern interactions with the industry assistance regime under section 317ZF of the Telecommunications Act. Generally, it is an offence to disclose information relating to assistance sought by Government agencies. Exceptions to this offence are available for disclosures required to administer the assistance, seek legal advice, publish transparency reports, or to make conditional disclosures with the approval of the issuing agency. This part also identifies the other legal provisions that provide exemptions to the disclosure offence.

Terms and conditions of assistance

In this part, procedural aspects and legal requirements of the assistance instrument are discharged. Providers are advised that the assistance instrument may be extended or varied by the issue of an extension or variation form. Providers are also advised that they are only required to comply with the assistance instrument to the extent that they are capable of doing so. This part further notes the requirement that the issuing agency notify the relevant oversight body within seven days of issue.

This part also advises that providers have a right of complaint when issued with an assistance instrument. Providers may complain to the relevant oversight body for the agency that issued the assistance instrument. This is the IGIS in the case of ASIO, ASD and ASIS. This is the Commonwealth Ombudsman in the case of AFP, ACIC, and State and Northern Territory Police. Additionally, in the case of State and Northern Territory Police, providers are advised that they may contact the inspecting authority of the relevant State or the Northern Territory to complain about an assistance instrument they have been issued.

The contact details of the relevant point of contact within the issuing agency should the provider need to discuss details of the assistance instrument are also provided by this part.

Authorisation

This part provides signed authorisation from the relevant decision-maker. In the case of a TAN, this part will provide an additional signed authorisation from the AFP Commissioner or delegate when the TAN was issued by the police force of a State or the Northern Territory. In the case of a TCN, this part will provide the signed authorisation from the Minister for Communications, approving the issuing of the TCN.

Note: Assistance instruments may be extended, varied or revoked by the issuing agency. Extensions, variations and revocations will be issued with a supplementary document setting out the details of the extension, variation or revocation of the notice.

USING STANDARD FORM CONTRACTS

The issuing agency and relevant provider are expected to engage informally prior to the issuing of an assistance instrument. During these early consultations, the agency and provider are expected to work collaboratively to negotiate a contract – if this is required – outlining the terms of compliance with an assistance instrument. Agencies will be provided with a contract template covering a range of items that may be relevant to assistance delivery. The agreement negotiated between the agency and provider will only include items that are specific to the requirement for assistance.

A key item to be included in the contract will be the cost arrangements associated with providing the assistance. Other items to be included will be dependent on the provider and the type of assistance they are required to deliver. Additional items to be included in the contract may include deliverables timelines, testing requirements, risk assessment and proposed mitigations or clauses to manage the variation or revocation of assistance obligations.

AUTHENTICATING SERVICE

Establishing collaborative working relationships between agencies and providers will be the most effective method of authenticating service. In order to foster cooperation, agencies and providers should establish consistent and reliable points of contact to assist with the issuance and service of assistance instruments. Agencies and providers should work to establish a single point of contact to eliminate the inefficiency associated with multiple points of contact. Whenever possible, providers should be approached for preliminary engagement by an agency officer with whom they have an established and trusted working relationship.

Prior to issuing an assistance instrument, agencies should engage closely with providers to ensure a mutual understanding of their views and obligations. This robust consultation process will provide a platform for agencies and providers to communicate effectively and work together to establish the terms of providing assistance. Providers will be able to determine the legitimacy of a request through close engagement during consultation.

Providers are encouraged to scrutinise requests for assistance and, as necessary, enquire to ascertain the authenticity of an assistance instrument if they find the request to be unusual or think it may be unlawful through non-compliance with the requirements and safeguards under the legislation. Providers may also contact the relevant independent oversight organisation (who by law are required to be notified of the assistance instrument) if they believe an assistance instrument or agency is irregular or does not meet legislative requirements.

Some providers will be experienced in responding to government requests under existing regimes. Where this is the case, engagement between agencies and providers should occur through prescribed channels in accordance with existing standard practices. For example, standard verification procedures may involve communication from government systems or

correspondence with agency authentication headers intact. The use of an agreed channel will help to verify that the request for assistance is genuine.

However, some providers, especially smaller providers, will not be experienced in engaging with agencies. These providers are likely to require additional support from agencies in establishing processes and procedures to respond to assistance instruments.

GIVING REASONS

After the conclusion of a formal consultation and the decision to issue an assistance instrument, providers may request an explanation of the decision. This document should address the relevant decision-making criteria from the legislation as they apply in the present circumstances and ultimately explain why certain criteria outweighed others and overcame any concerns raised by the provider. Reasons may also detail any other consultation the decision-maker has undertaken in deciding to issue the assistance instrument and outline why the provider has been chosen as the appropriate leverage point in the supply chain.

Giving reasons alongside the assistance instrument, or having reasons available to the provider, is a best practice approach at the point of issue. Making reasons available ensures that providers have confidence in the decision-making process and can see that the concerns identified during the consultation have been considered and given appropriate weight. Offering reasons is also important to allow providers to challenge the decision through judicial review should they be unsatisfied.

However, operational, capability and national security concerns may mean that free disclosure of reasons cannot occur, or must occur in a redacted form. Decision-makers have the discretion to decide which aspects of their reasons should be disclosed and may appropriately choose to withhold details relating to organisational priorities or consultation with other agencies regarding alternative capability. Where reasons are sought in order to appeal the decision to issue an assistance instrument, providers may seek to have the full reasons disclosed to a judge in a closed setting.

INFORMATION SHARING RULES

Section 317ZF of the Telecommunications Act outlines the relevant information sharing rules.

TECHNICAL INFORMATION THAT MAY NOT BE DISCLOSED

It is an offence for certain persons involved in the issuing, assessment and delivery of assistance instruments to disclose information relating to that request or notice. Information pertaining to these measures is likely to be highly sensitive commercial and operational information. The offence for unauthorised disclosure is designed to protect the security of providers' systems and law enforcement and national security investigations and outcomes.

PERMISSIBLE DISCLOSURES

The disclosure of information may be permitted in limited circumstances. For example, information may be disclosed in connection with the administration or execution of an assistance instrument, for the purposes of legal proceedings relating to that assistance instrument, or to assist an oversight body in exercising their functions.

Information may also be shared for the purpose of **obtaining legal advice** or in **legal proceedings** that relate to Part 15.

Importantly, if an individual within an organisation receives an assistance instrument in their capacity as a representative of that organisation, they may **share information about the instrument within their organisation as necessary to implement requirements**. As all assistance instruments are directed to a corporate entity, disclosure is necessary to bring the assistance instrument to the attention of other persons within the organisation.

Information may also be disclosed as **required by law**, either within the Telecommunications Act or other statute.

Information should be exchanged through secure transmission and, depending on the nature of the information, may require additional protective measures. The method of information exchange should be discussed during preliminary engagement.

INFORMATION-SHARING FOR AGENCIES

The heads of intelligence agencies, the chief officers of interception agencies, and the Communications Access Coordinator (CAC) within the Department of Home Affairs may share information for purposes relating to their functions and the exercise of powers. Agencies may only share information in accordance with procedures under section **317ZF**. Information-sharing between agencies is important to ensure the effective execution of national security and law enforcement procedures. In sharing information, agencies should employ existing practices and procedures to ensure that information may only be shared when necessary. As such, the CAC must be notified when information is proposed to be shared between specified agencies for the purpose of the receiving agencies' functions, to facilitate the CAC's administrative role for the use of powers. The CAC will have oversight of information sharing in all jurisdictions to facilitate this administrative role.

CONDITIONAL DISCLOSURE REQUESTS

There may be circumstances where a provider wishes to disclose information about an assistance instrument to relevant stakeholders, including members of their supply chain. Providers may be permitted to disclose information relating to a notice to relevant stakeholders with authorisation from the decision-maker that issued the underlying assistance instrument. If the provider wishes to disclose information relating to an assistance instrument, they should approach the decision-maker, or their delegate, with a proposal to make a disclosure.

The provider and decision-maker are expected to consult closely to determine the legitimacy and conditions of the proposed disclosure. The provider may only disclose information if they receive written authorisation from the decision-maker in accordance with the terms outlined in the authorisation. Importantly, allowing a conditional disclosure does not require the variation of the assistance instrument in force to reflect this decision. The written authorisation for a conditional disclosure is not subject to form requirements.

Where a provider foresees the need to make a conditional disclosure of an assistance instrument, this should be raised with the issuing agency during preliminary engagement. This will allow the agency to assess the desirability of continuing with the assistance instrument in light of the provider's desire to disclose its details and allow both parties to reach agreement prior to the delivery of the assistance. Where this is impossible or the desire to make a conditional disclosure is otherwise unforeseen, this can be discussed at a later stage.

Agencies are expected to authorise disclosure as appropriate unless there are compelling national security, operational or investigative reasons. The reasons for refusing a disclosure request should be documented and clearly communicated to a provider. As an executive decision, refusing to allow a conditional disclosure may be the basis for a legal challenge.

TRANSPARENCY REPORTS

Providers may disclose statistical information in a **transparency report** concerning the total number of assistance instruments issued to them in a period of at least six months. Many providers will be experienced in publishing a transparency report, and should do so in accordance with their existing standard practices. Publishing a transparency report will allow providers to assure their consumers and stakeholders that they have either not provided assistance, or they have and their systems have not been compromised. As a result of the operational sensitivities associated with providing assistance, providers may only publish aggregates of notices and requests received from Australia in these transparency reports. Transparency reports do not allow for the publication of any information that may identify an issuing authority or any specific details of the assistance requested without authorisation from the issuing authority. Publication of this information would be in contravention of the unauthorised disclosure offence.

DISAGREEMENT AND ENFORCEMENT

Compliance and enforcement is dealt with in Division 5 of Part 15 of the Telecommunications Act

COMPLIANCE OBLIGATIONS

Providers must comply with a requirement under a notice to the extent that they are capable of doing so. This is separate from the concept of 'existing capability' that distinguishes assistance under a TAN or TCN, which concerns the technical capacity of a provider. Rather, capability for the purposes of sections 317ZA and 317ZB goes to whether the provider has the resources or other means to actually comply with requirements. Circumstances like bankruptcy, or other financial or specific legal restrictions, may render a provider incapable of compliance.

This matter should already be addressed through the comprehensive consultation process which aims to ensure that the assistance required is reasonable, proportionate, practicable and technically feasible. A provider will only be issued with a notice if the decision-maker is satisfied that the provider has the necessary resources, or ability to acquire the resources, to be able to comply with a notice.

If extenuating or unanticipated circumstances prevent a provider from meeting the full requirements of a notice, the provider is obliged to meet the requirements to the extent possible. In these instances, providers should be able to demonstrate how the extenuating circumstances have affected their ability to deliver the required assistance, and that the assistance they have provided is to the highest standard they are capable of delivering.

If a provider fails to meet their compliance obligations they may be subject to enforcement proceedings.

DECISION TO PURSUE ENFORCEMENT

To the greatest extent possible, a collaborative approach should be taken in the utilisation of industry assistance measures. Many providers may be willing to offer assistance on a voluntary basis, without the need for legal compulsion. However, enforcement proceedings may be pursued against a provider where they refuse to comply with their legal obligations under a TAN or a TCN.

If an agency finds a provider to be non-compliant, they may approach the Communications Access Coordinator at the Department of Home Affairs for consideration. The CAC can be reached at cac@homeaffairs.gov.au. The CAC will review the agency's case for non-compliance, and may decide to pursue enforcement against a provider if they are of the view that the provider is in contravention with their legal obligations. In considering a provider's compliance, the CAC should take into consideration the full set of materials related to the notice compelling assistance. Consideration of the full set of materials will provide assurance in cases where a provider is believed to be non-compliant but has acted in good faith and failed to deliver the requested capability.

In making the decision to pursue enforcement, the CAC may have regard for items such as:

- Written records of engagement between the issuing agency and provider (both informal and formal).
- Details of the decision-maker's assessment that the requested assistance is reasonable, proportionate, practicable and technically feasible.
- The original assistance instrument compelling assistance and any subsequent variation or extension notices.

- The standard form agreement outlining the terms of compliance and cost arrangements.
- Reports and findings from any independent assessment by oversight bodies or the independent panel and arbitrator.
- Statements from the issuing and provider.
- Any other items the CAC considers relevant to making this decision.

The provider will be notified that they may be subject to enforcement proceedings, and invited to make a submission for the CAC's consideration. Notification and communication will occur through the preferred channels indicated by the provider. The CAC will carefully review all relevant material before deciding whether to initiate enforcement. If the CAC considers a provider to be non-compliant, they will provide, in writing, details of their assessment including how the provider was held to be deficient and what would be required to comply. The CAC will also indicate to the provider the penalties they may face if they continue to refuse to comply. The provider will then be given a timeframe – to be determined by reference to the circumstances - to demonstrate their intention to comply before enforcement is pursued.

INITIATING ENFORCEMENT PROCEEDINGS

The CAC may consider a provider to be non-compliant with a notice and decide to apply for civil penalties, enforceable undertakings or injunctions against the provider. The CAC will apply for these enforcement proceedings through the Federal Court or Federal Circuit Court. Enforcement proceedings will only be pursued if the CAC is satisfied that the provider has not complied with a requirement under a notice to the extent they are capable of doing so, having regard to any assessments made (as detailed above).

At the time of initiating enforcement, the provider should be sufficiently informed by the agency and the CAC of their non-compliance and the intention to pursue enforcement proceedings. Notification of enforcement proceedings will be initiated through established avenues.

Non-compliance with a notice may have serious negative consequences for law enforcement and national security. The penalties for non-compliance are intended to deter providers from contravening their legal obligations.

Civil Penalties:

- 47, 619 penalty units (approx. $10 million AUD in 2019) for body corporates
- 238 penalty units (approx. $50,000 AUD in 2019) for individuals who are sole traders (not employees within an organisation).

These are maximum penalties, actual amounts would be set by the Court taking into account the circumstances of the contravention.

DEFENCE: CONFLICT OF LAWS

It is a defence against non-compliance for a provider if an act or thing they are required to do in a foreign country would contravene a law of that foreign country. This defence ensures that providers will not be put in a position where compliance with Australian law would result in a breach of the law in a foreign jurisdiction.

An assistance instrument should not be issued in cases where the assistance would contravene the laws of a foreign country. Where there is reasonable belief that a conflict of laws may arise by providing required assistance, prompt action should be undertaken to remedy the situation.

Agencies and providers should be forthcoming in responding to these concerns, and provide each other with all relevant information and advice as required. Providers will be best place to

advise of possible contraventions of foreign laws in the other jurisdictions that they are operating and should endeavour to a communicate this risk clearly to the relevant agency. Upon identifying a possible conflict of laws, agencies and providers may be required to adapt assistance delivery plans during informal consultation, or vary/ revoke the assistance instrument served.

In some cases, a contravention of foreign laws may not be identified until after an assistance instrument has been issued. However, enforcement proceedings should not be initiated, as the civil penalty defence against non-compliance will apply regardless of whether the contravention is discovered before or after a notice is issued.

DECISIONS THAT MAY BE SUBJECT TO JUDICIAL REVIEW

Any decision to compel assistance may be subject to judicial review – this is a feature of Australian law. If a provider does not consider a assistance instrument to be reasonable, proportionate or that the instrument does not meet legislative requirements, they are able to challenge the decision through the High Court, the Federal Court of Australia or the Supreme Court of a State or Territory (depending on the circumstances of the relevant notice).

Additionally, any decision made under Part 15 that is an exercise of executive power may be open to court challenge through judicial review. These decisions include the decision not to compensate a provider for their assistance and the decision to refuse a request to conditionally disclose the details of an assistance instrument.

OVERSIGHT, TRANSPARENCY AND INDEPENDENT SCRUTINY

Robust transparency, oversight and independent scrutiny arrangements will ensure that the industry assistance measures are used appropriately by agencies. All assistance instruments issued under the Act are subject to strong safeguards and limitations. Providers will be informed of the notification obligations, right to complaint, and other important protections in relation to providing assistance in the assistance instrument of the notice. If providers require further information concerning their rights and obligations they should contact the issuing agency, relevant oversight body, or the Department of Home Affairs.

LIMITATIONS

A number of key limitations apply to all assistance instruments and both providers and agencies should be conscious that any assistance instrument which contravenes these requirements will be invalid.

No systemic weaknesses or vulnerabilties (section 317ZG)

An assistance instrument must not jeopardise the data, information or cyber security of the public or business community. While it is permissible to selectively weaken the security of targeted devices and services, this must not create a material risk that the services and devices of other, unrelated users will be made vulnerable to unauthorised access. Any targeted activity that would, or would be likely to, have this effect is not permitted under the legislation. The definition of systemic weakness in the concepts dictionary refers.

Warrants and authorisations required (section 317ZH)

An assistance instrument must not request or require assistance if the assistance covers an activity for which that particular agency would require a warrant or authorisation. While an assistance instrument may facilitate the execution of a warrant or authorisation, they do not replace the need for a warrant or authorisation.

For example, it is not permissible to request that a provider undertake an interception absent an interception warrant. In this circumstance, the interception warrant serves as an authority for accessing the live communications and the assistance instrument may stipulate certain activities or undertakings that aid in accessing, processing or delivering the lawfully accessed communications.

A warrant or authorisation is not required before an assistance instrument can be issued, but this limitation does restrict the scope of activities that may be required or requested.

Agencies should be aware of the spread of their relevant powers when contemplating an assistance instrument.

No interception or data retention capabilities (section 317ZGA)

A TCN must not require a provider to build an interception capability, a delivery capability or a data retention capability. These capabilities are already administered under the TIA Act and a TCN is not a vehicle to replace this existing regime.

NOTIFICATION OBLIGATIONS

TARs and TANs

For all TARs and TANs, the decision-maker or their delegate is required to notify the relevant independent oversight body within seven days of serving the assistance instrument. The Inspector-General of Intelligence and Security (IGIS) will receive notification of the issue, variation, extension (for TANs) or revocation of all assistance instruments made by the

Director-General of the relevant intelligence agency. The Commonwealth Ombudsman will receive notification for the same items for assistance instruments made by the chief officer of the relevant interception agency. The Commonwealth Ombudsman is empowered to share information with the relevant State and territory inspecting authority.

In issuing TANs, the relevant decision-maker is required to notify the provider of their right to make a complaint about the notice to the relevant independent oversight body. Providers will be informed that complaints concerning notices issued by ASIO may be submitted to the IGIS. If the notice was issued by an interception agency, providers will be advised that complaints may be made to either the Commonwealth Ombudsman or to the State or Northern Territory inspecting authority for the relevant agency.

The method and form of these notifications will be left to the preferences of the agency and inspecting authority.

TCNs

All TCNs are subject to direct ministerial oversight, as they must be issued by the Attorney-General with approval from the Minister for Communications. The Attorney-General must not issue a TCN without providing written notice to the Minister for Communications and receiving approval.

The Attorney-General must notify the IGIS for notices assisting ASIO, or the Commonwealth Ombudsman for notices assisting interception agencies, within seven days of serving the assistance instrument. Variations and extensions to a TCN are subject to the same ministerial oversight and notification obligations as the original notice. The relevant independent oversight body must also be notified within seven days if a TCN is revoked.

During the consultation period for issuing or varying a TCN, the provider will be notified by the Attorney-General of their right to request an assessment of the notice by an independent panel consisting of a technical expert and retired senior judge.

The Attorney-General is responsible for the appointment of independent assessors. In appointing the assessment panel, the Attorney-General must take into consideration the interests of the provider and the nature of the capability required. The Attorney-General should share the identity and experience of independent assessors with the provider in confidence, and provide opportunity for the provider to dispute the appointment of an assessor if they do not meet the requirements to conduct an independent assessment.

If the provider requests an assessment from the independent panel, the panel will carry out an assessment and prepare a report to be given to the Attorney-General, the provider, and the relevant independent oversight body.

ANNUAL REPORTING REQUIREMENTS

Interception agencies

Transparency over the use of industry assistance measures is supported by mandated annual reporting requirements (see section 317ZS). Law enforcement agencies are directed, in order to comply with reporting requirements placed on the Department of Home Affairs, to record the number of times each power is used and the type of offences the powers were used to investigate within a 12-month period. Law enforcement agencies should use their established record-keeping and reporting practices in meeting the requirements under the TIA Act for the new powers.

The Minister for Home Affairs must cause a written report to be prepared on the use of TARs, TANs and TCNs as soon as practicable after the 30 June of each year. The report on the use of powers must be included in the report for the TIA Act relating to the same year. Law

enforcement agencies should continue to work collaboratively with the Department of Home Affairs, as they have under existing regimes, during the annual reporting process. The Department of Home Affairs will provide separate advice regarding the details of reporting requirements.

Intelligence agencies

Annual reports prepared by the Director-General of Security under section 94 of the ASIO Act must include the numbers TARs, TANs and TCNs given by ASIO in the relevant year. This report is given to both the relevant Minister and the Leader of the Opposition. It is also tabled in Parliament after being modified to ensure that the matters in the report do not prejudice security, the defence of the Commonwealth, the conduct of the Commonwealth's international affairs or the privacy of individuals.

INSPECTIONS

Interception agencies

The Commonwealth Ombudsman may inspect the records of an interception agency relating to the industry assistance measures to determine the extent of compliance with Part 15. The Ombudsman inspections will enhance transparency and accountability for agencies' use of powers by assessing their compliance with the legislation and making recommendations for better practice.

Interception agencies have been subject to oversight from the Ombudsman through their use of powers under the TIA Act. As such, interception agencies should continue to cooperate with the Ombudsman and provide them with any assistance necessary to conduct an inspection.

In addition to the unique inspection function under Part 15 of the Telecommunications Act, the Ombudsman, or relevant State and Territory inspecting authority, may scrutinise the use of assistance instruments as part of the regular inspections that occur under the TIA Act or SD Act.

The Ombudsman may make a written report to the Minister for Home Affairs on the findings of an inspection. The Ombudsman's report must not include information that may prejudice an investigation or prosecution or compromise an interception agency's operational activities or methodologies. The Minister for Home Affairs must table this report in Parliament within 15 sitting days after receipt.

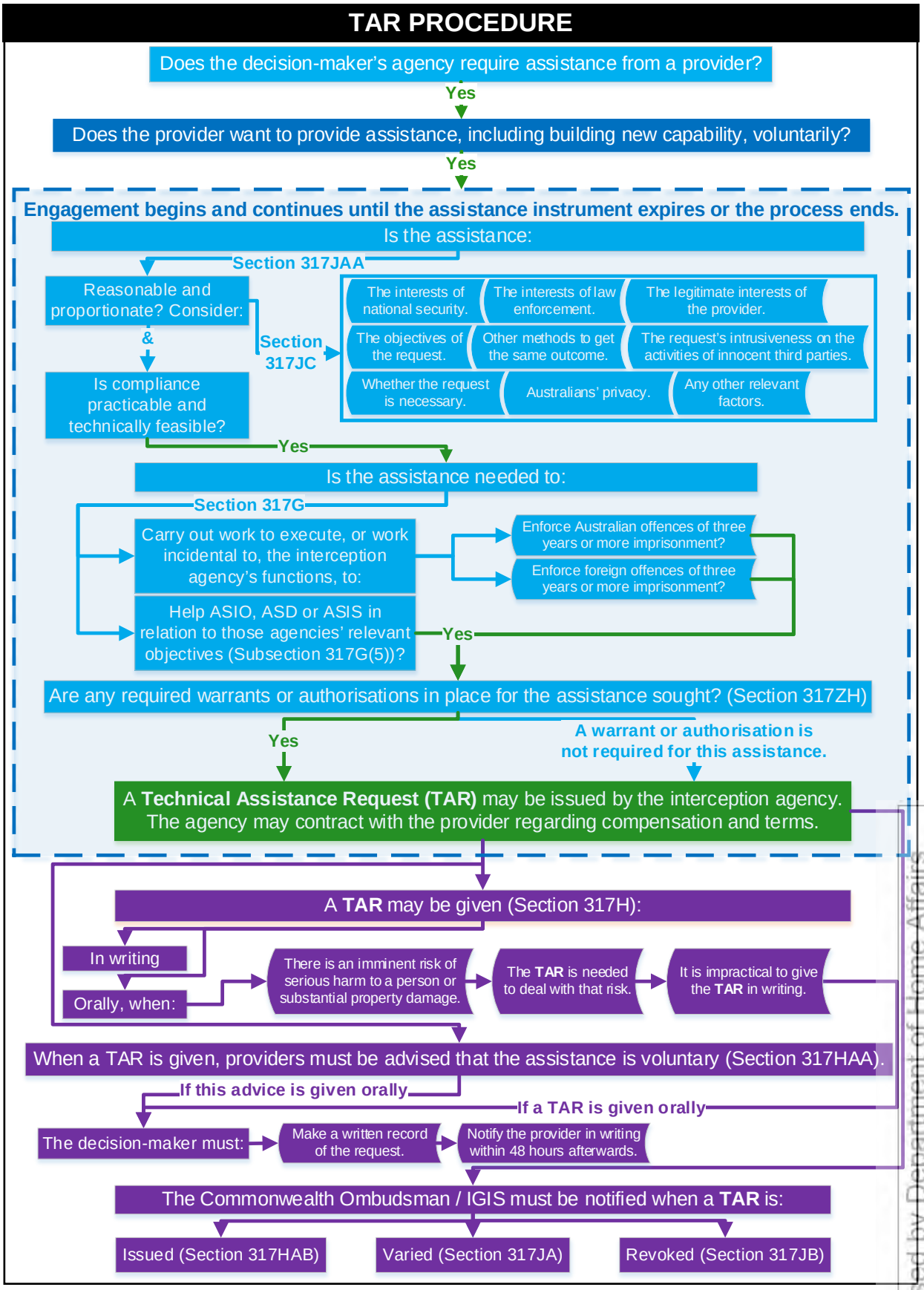
Intelligence agencies

The Inspector-General of Intelligence and Security has the authority to inspect and report on the activities of intelligence agencies under this regime. The role of the Inspector-General of Intelligence and Security relates to legal and administrative compliance as well as propriety of agency conduct.

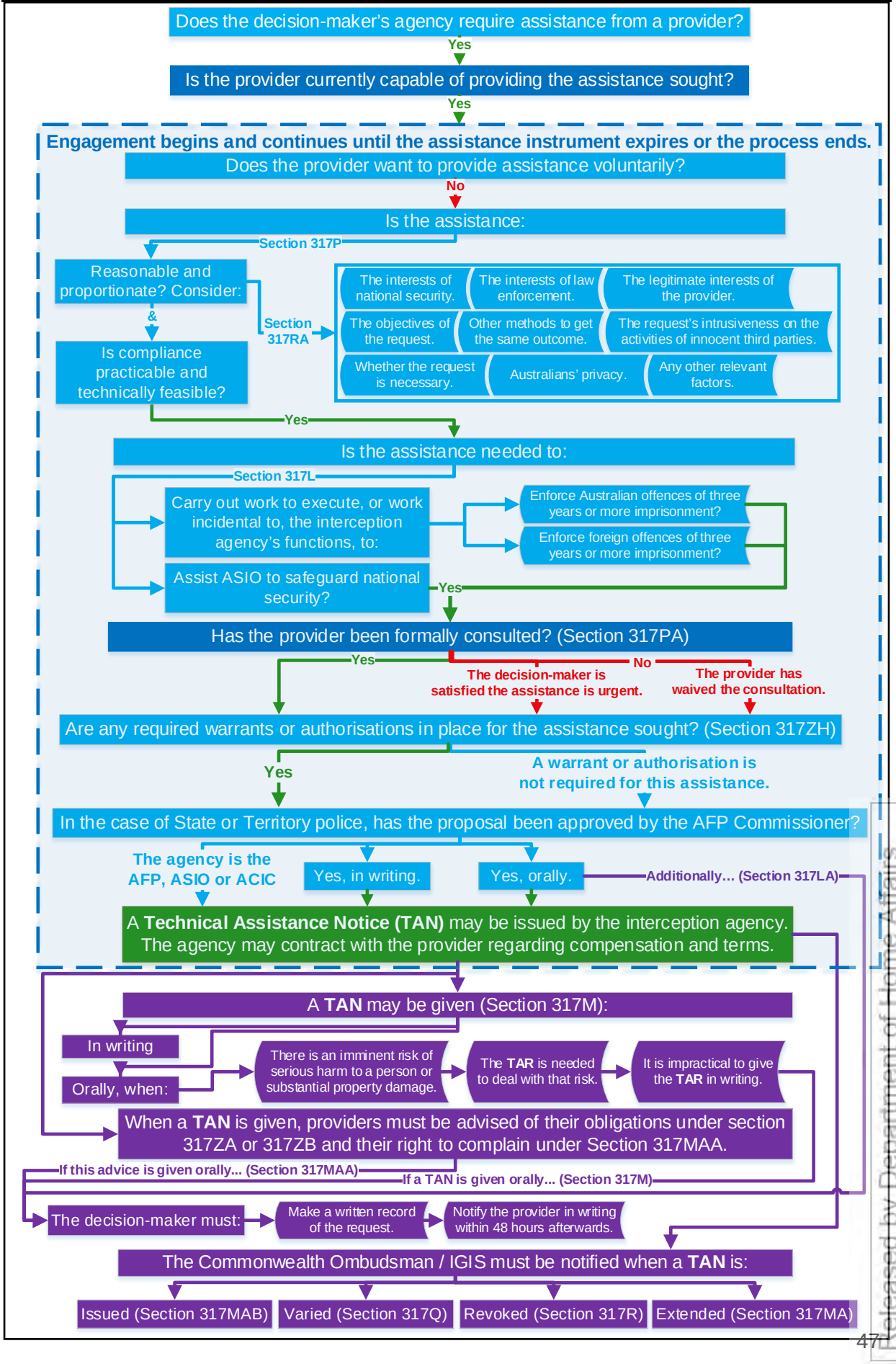
INDEPENDENT NATIONAL SECURITY LEGISLATION MONITOR REVIEW

The use of the industry assistance measures is subject to independent scrutiny from the Independent National Security Legislation Monitor (INSLM). The INSLM is required to review the operation, effectiveness and implications of the Act as soon as practicable after June 2020. The INSLM will consider whether Part 15 contains the appropriate protections for individual rights, is proportionate to terrorism and national security threats, and remains necessary. In conducting the review, the INSLM will have access to all relevant material regardless of national security classification, can compel answers to questions, and may hold public and private hearings.

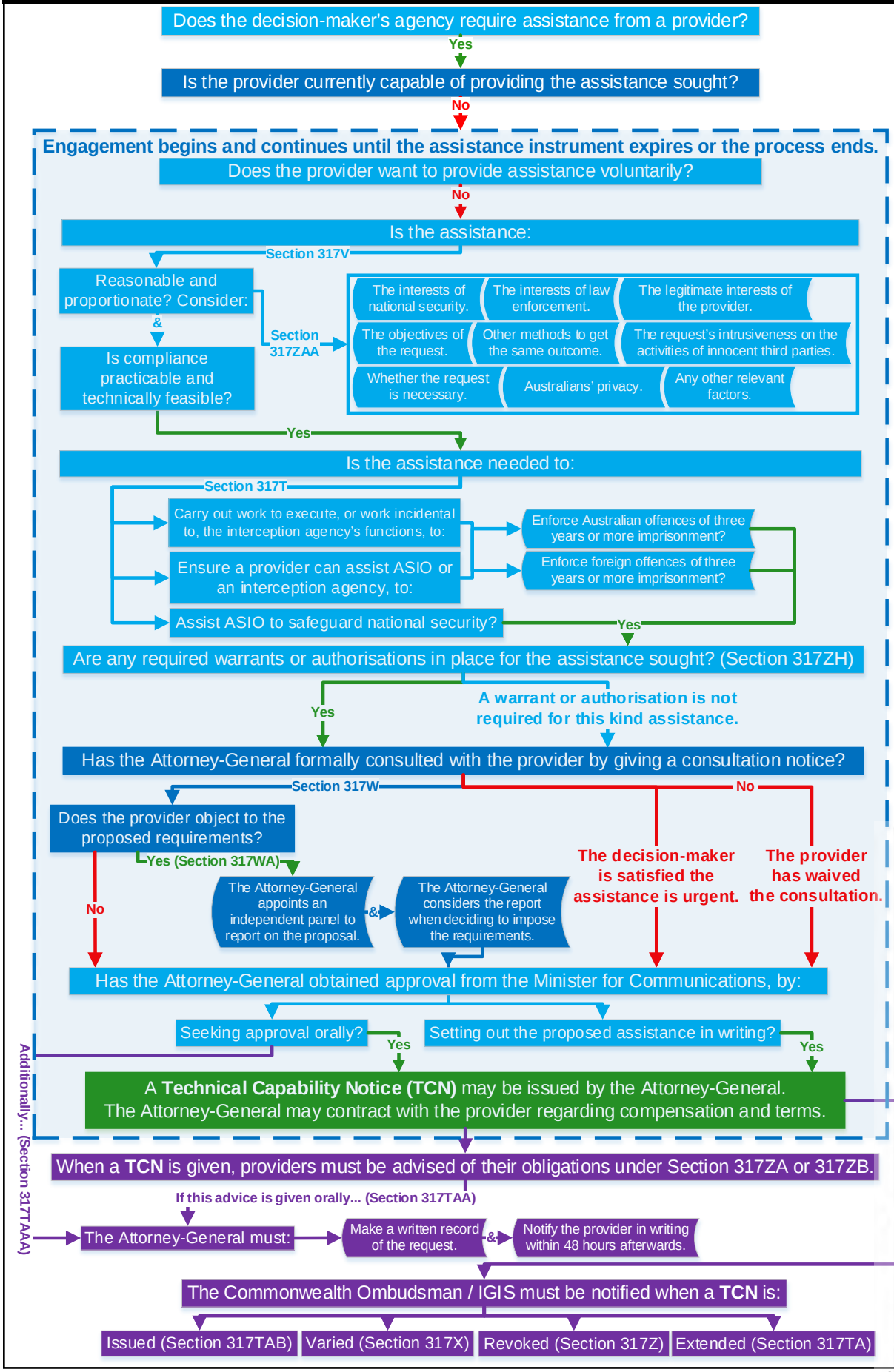
APPENDIX



TAN PROCEDURE



TCN PROCEDURE



Australian Government

Department of Home Affairs

ASSISTANCE AND ACCESS

This document summarises the amendments made to Australian law by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. The Act is Australia's legislative response to the rapid evolution of communications technology and the challenges of encryption.

Table of Contents

The Assistance and Access Act 2018

The Australian Government supports cyber security tools, like encryption, that create a safe online environment for Australians. Encryption ensures that everyday digital transactions, like online banking or shopping, can occur securely. The Government has no interest in undermining these critical technologies.

Unfortunately, the same technologies are being employed by terrorists, paedophiles, drug smugglers and human traffickers to conceal illicit activities and facilitate crime. Criminals are increasingly sophisticated users of the internet and rapid technological change has caused valuable sources of evidence and intelligence to diminish, for example:

- over 95 per cent of the Australian Security Intelligence Organisation's (ASIO) most dangerous counter-terrorism targets use encrypted communications;
- encryption impacts intelligence coverage in nine out of ASIO's 10 priority cases; and
- it is estimated that by 2020 all electronic communications of investigative value will be encrypted.

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Assistance and Access Act) equips agencies with the tools they need to effectively operate in the digital era and keep the Australian community safe. The Assistance and Access Act introduced some key reforms to help our agencies access the evidence and intelligence they need by:

- enhancing industry cooperation with law enforcement and security agencies; and
- improving agency computer access powers.

Importantly, nothing in this legislation can require industry to break encryption. Instead, the measures enhance the existing ability of Australian agencies to undertake targeted, proportionate and independently oversighted surveillance activities.

The operation of the Assistance and Access Act will be subject to ongoing review by the Parliamentary Joint Committee on Intelligence and Security and by the Independent National Security Legislation Monitor.

Overview

The Act addresses law enforcement and intelligence agencies' challenges with the evolution of the communications environment, including the growth of encrypted communication.
The Act:

1. Enhances the obligations of businesses that provide communications services to assist agencies;
2. Establishes new 'computer access warrants' for law enforcement; and
3. Strengthens agencies' existing search and seizure powers for computers (including mobile devices) to access unencrypted data.

Schedule 1 – Industry Assistance

In the modern era, criminal activity is frequently conducted online and through communications systems. Australian agencies need the help of the communications industry to detect and disrupt this activity.

Schedule 1 of the Act establishes a framework for government and the communications industry to work together on law enforcement and national security investigations, allowing:

- Agencies to request voluntary assistance from providers with a **technical assistance request**.
- Agencies to require assistance from providers with a **technical assistance notice** where the provider is already capable of giving the required assistance.
- The Attorney-General and Minister for Communications to jointly require a provider develop a new capability with a **technical capability notice** where the provider is not already capable of offering that type of assistance.

Schedule 1 of the Act provides that:

- Any assistance or capability requested must be **reasonable, proportionate, practicable** and **technically feasible**.
- Assistance to law enforcement must be related to investigating offences with a maximum penalty of at least three years imprisonment or more.
- Providers may be asked to build or use capabilities that can provide targeted access to data where this does not remove electronic protection or jeopardise the information security of general users.

Schedule 1 of the Act **does not**:

- Allow for assistance that creates "systemic weaknesses" or backdoors into encrypted devices and communication systems. This includes requesting or requiring providers to:
    - refrain from fixing vulnerabilities or making their services more secure,
    - build a decryption capability; or
    - reduce the broader security of their systems.
- Allow agencies to see the content of personal communications, or intercept communications – these things continue to be governed by existing legislation and warrant regimes.
- Compel providers to build a capability to remove electronic protection.
- Extend existing data retention or interception obligations to new providers.

Other safeguards to Schedule 1 of the Act include:

- Review of technical capability notices upon referral by providers to determine if they abridge any of the Act's limitations, such as the backdoors prohibition.

- A whole-Act review by the Independent National Security Legislation Monitor after 18 months.
- Decisions by agencies and the Attorney-General will be subject to judicial review.
- Any requests by State and Territory police must be approved by the Australian Federal Police to coordinate compulsory requests across Australia.
- Extensive oversight from dedicated bodies including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security.

Schedule 2 – Computer Access Warrants

Schedule 2 of the Act creates **computer access warrants**, which allow law enforcement:

- To covertly access devices to investigate serious crimes.
- To search devices such as laptops, mobile phones and USBs, and collect information.
- To conceal the fact that a device has been accessed.

Schedule 2 of the Act also amends ASIO's existing warrant regime with the power to conceal the fact that a device has been accessed.

Law enforcement computer access warrants must be **issued by an independent authority** (a judge or AAT member) and cannot authorise interference with, or material loss or damage to, a computer.

Computer access warrants can be sought only for serious offences (offences that attract a penalty of three years or more).

Schedule 3 and 4 – Strengthening search and seize powers

Schedules 3 and 4 of the Act extend the maximum penalties associated with the power of a Magistrate to require an individual to unlock a device where they know the password:

- In the Crimes Act, from two years to five years imprisonment – ten years for serious offences.
- In the Customs Act, from six months to five years imprisonment – ten years for serious offences.

Schedules 3 and 4 of the Act also extend the time available for examining electronic devices seized under warrant:

- In the Crimes Act, from 14 to 30 days.
- In the Customs Act, from 72 hours to 30 days.

Schedule 3 also allows police to access account-based data (i.e. social media accounts) via a search warrant.

Schedule 5 – Voluntary assistance for ASIO

Schedule 5 of the Act:

- Provides civil immunity to persons who voluntarily assist ASIO.
- Allows ASIO to apply to the Attorney-General to require a person to unlock a device where they know the authentication protocol.
- Creates a penalty for non-compliance of a maximum five years imprisonment.

The Industry Assistance Framework

Encryption and other forms of electronic protection are valuable cyber security tools.

The new legal framework for industry assistance in Schedule 1 strengthens the ability of intelligence agencies and law enforcement to adapt to the new digital era. It ensures the companies that provide communications services and devices in Australia have an obligation to help agencies, including to assist in the execution of a warrant.

Who does this apply to?

The obligations apply to any provider of communications services and devices in Australia, irrespective of where they base their corporation, servers or manufacturing. The legislation refers to these providers as ***designated communications providers***.

Operating in the Australian market comes with obligations to assist in protecting Australian citizens from those using its marketed services and devices for serious crimes, including terrorism.

While the Australian Government has received voluntary assistance from many technology and communications providers, it is the Government's view that it is not fair to expect unequal compliance from different providers.

What assistance must be provided?

The legislation establishes a ***list of acts or things*** in section 317E that articulates what assistance can be provided to Australia's law enforcement and intelligence agencies.

The ***listed acts or things*** are relevant to each provider in respect of its ***eligible activities***. These are the services and products that a provider offers or operates in the Australian market. A provider is not required to provide help that is unrelated to their relevant eligible activities.

Listed acts or things

A listed act or thing includes[1]:

- removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider where the provider is already capable of removing this protection (***Note:*** *a provider cannot be required to build a capability that removes a form of electronic protection)*;
- providing technical information;
- installing, maintaining, testing or using software or equipment or assisting with those activities;
- assisting with access to devices or services;[2]
- notifying agencies of a change to a service;
- concealing that any other thing has been covertly performed in accordance with the law; and
- doing an act or thig that facilitates giving effect to a warrant or authorisation or enables the effective receipt of information.

[1] This is not a complete or legally accurate list, and is for information only. The full list is available in the legislation at s317E.
[2] Private communications and data may only be accessed with lawful authority pursuant to the existing warrant framework.

Each of these things is subject to the limitation against building systemic weaknesses or accessing personal information.

This list is exhaustive for the compulsory powers under the Act but not the voluntary powers.

How will this be requested?

The legislation establishes **three new tools** for requesting assistance possible in the ***listed acts or things***.

The Technical Assistance Request (TAR)

This is a **voluntary** request that may be issued by the head of an **interception agency** (Federal, State and Territory law enforcement and the Australian Criminal Intelligence Commission), the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Agency (ASIS) or the Australian Signals Directorate (ASD) for prescribed purposes. If a designated communications provider is asked to provide assistance on a **voluntary** basis under a TAR, that provider and their officers, employees and agents are granted civil immunity for things done in assistance.

The Technical Assistance Notice (TAN)

This is a **compulsory order** that may be issued by the head of an interception agency or ASIO. If a designated communications provider is requested to provide assistance under a TAN, they must give that assistance if their current capabilities allow them to do so. A TAN does not require a provider to build a capability or functionality they do not already possess in order to comply with a TAN.

The Technical Capability Notice (TCN)

This is a **compulsory order** that may be issued jointly by the Attorney-General and the Minister for Communications, at the request of the head of an interception agency or ASIO. If a designated communications provider is ordered to provide assistance under a TCN, they must provide that assistance, including building a capability to provide that assistance.

Importantly, a TCN is expressly prohibited from requiring the building of a capability to decrypt information or remove electronic protection.

What will this cost?

By default, complying with a TAR, a TAN or a TCN is cost recoverable on a no-profit-no-loss basis. Providers may also be able to enter into commercial terms for the provision of assistance.

In limited circumstances and only when it is in the public interest, a provider can be required to comply without compensation. This exception cannot be exercised until a decision maker takes into account regulatory burdens and the effect on competitiveness, among other things.

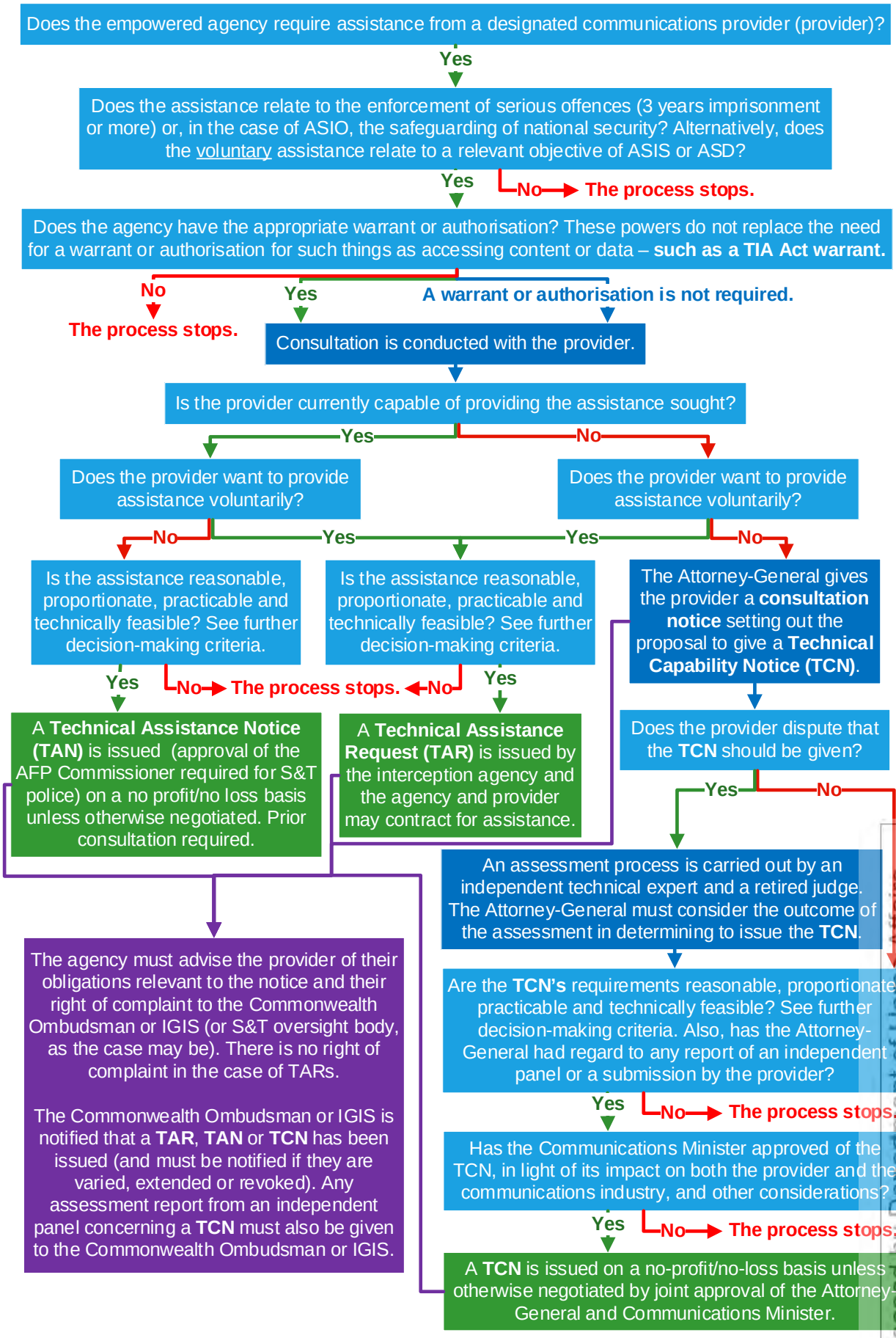
How is this enforced?

If you are a carrier or carriage service provider, you are subject to the existing regulatory regime under the *Telecommunications Act 1997*. This includes a pecuniary penalty of up to AUD $10 million for each case of non-compliance.

If you are a service provider other than a carrier or carriage service provider, a company can be fined up to approximately AUD $10 million for each case of non-compliance. An individual can be fined up to approximately AUD $50,000 for each case of non-compliance.

A person may also be imprisoned for up to five years if there is an unauthorised disclosure of information, as detailed in 317ZF.

Industry Assistance Process[3]



[3] ASIS and ASD are only empowered to issue TARs.

Limitations and Safeguards

Overview

There are a number of key limitations located throughout Part 15 of the Telecommunications Act. Some key safeguards are contained within **Division 7** of Part 15. These include:

1. Requirements and requests must not contravene the prohibition against building or implementing systemic weaknesses or vulnerabilities **– 317ZG**
2. A TAR, TAN or TCN must not be used to do things for which the requesting agency would otherwise require a warrant or authorisation **– 317ZH**
3. (For a TCN) New capabilities must not require the construction of interception capabilities or data retention capabilities **– 317ZGA**

No systemic weaknesses.

Systemic weakness, so-called 'backdoors', weaken the digital security of Australians and others.

This is why notices under the Act cannot require a provider to implement or build systemic weaknesses into electronic protection. The Australian Government has no interest in undermining systems that protect the fundamental security of communications. This includes an explicit prohibition on building a decryption capability or requiring that providers make their encrypted systems less effective.

Notices cannot prevent a provider from fixing a security flaw in their products. Providers can, and should, continue to update their products to ensure customers enjoy the most secure services available.

The **prohibition against systemic weakness** ('backdoors') was clarified and strengthened following a review by the Parliamentary Joint Committee on Intelligence and Security.

What is a systemic weakness?

Section **317B** defines a systemic weakness/vulnerability as 'a weakness/vulnerability' that affects a *whole class* of technology…'. The term 'class of technology' is deliberately broad and captures general items of technology across and within a category of product. It encompasses, for example, mobile phone technology, a particular model of mobile phone, a particular type of operating system within that phone model or a particular type of software installed on an operating system. The wide scope is intended to protect the services and devices used by the whole, or legitimate segments of, the general public and business community.

Further elements of the definition clarify that the inherently targeted surveillance activities of agencies are not captured by this definition. However, new subsections **317ZG(4A), (4B)** and **(4C**) make clear that even requirements to assist in these legitimate and authorised agency activities must not have the inadvertent effect of weakening information security. That is, industry **cannot be asked to do things that would be likely to create a material risk of unauthorised access** to the information of a person not connected to an investigation.

The intent and application of the protection is to provide for targeted, proportionate access **and prevent weakening cybersecurity.**

What is 'electronic protection'?

Electronic protection includes encryption. However, the Act's prohibition against systemic weaknesses also extends to other forms of electronic protection, including authentication systems like passwords.

Agencies need an underlying warrant to undertake surveillance.

The new framework does not serve as an independent channel to obtain private communications, metadata or undertake surveillance. Section 317ZH of the Act states that if a warrant or authorisation was required before, it is still required. Interception of communications, access to metadata or search powers still require existing thresholds to be met. Further, providers **can't be asked to build an interception, data retention or decryption capabilit**y (or build anything that removes a form of electronic protection, like encryption).

In order to undertake these privacy-intrusive activities, agencies must seek a warrant or authorisation under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) or *Surveillance Devices Act 2004*. Agencies must meet the applicable thresholds and receive independent approval.

Additional safeguards for TCNs.

Independent assessments of any new capability.

To attain third-party verification that the Act's legal protections are not being circumvented (and that requirements are otherwise reasonable, proportionate, practical and technically feasible) industry may refer any requirements to build a new capability for review by a technical expert and a retired senior judge. The findings on this **assessment panel** are extremely influential on the decision to issue a notice by the Attorney-General. Industry may also apply for **judicial review** of executive decisions as an inherent part of the Australian legal system.

Added safeguards against data retention, interception and others.

None of the powers can be used to require the construction of a data retention, interception or decryption capability. Additional safeguards exist to prevent new capabilities built under a TCN from extending telecommunications interception, data retention or users' browsing history. These are set out at 317ZGA.

Reasonable, proportionate, practicable and technically feasible.

Decision-makers must be satisfied that a TAR, TAN or TCN is **reasonable**, **proportionate, practical** and **technically feasible**. These decisions, by law, include consideration of industry interests, necessity, privacy, cyber security and intrusiveness. In addition to mandatory consultation, this ensures any representations of industry are taken into account and decision-makers turn their mind to the impact on the Australian public.

Decision-makers must revoke a technical assistance notice or technical capability notice if satisfied that any ongoing requirements are no longer reasonable, proportionate, practical or technically feasible. This ensures that any requirements on industry are under constant assessment and continue to meet the necessary thresholds, even as circumstances change.

Review by the courts, experts and arbitration.

Affected people and companies have an avenue to challenge a decision to issue a notice. Judicial review by the courts is available under the *Judiciary Act 1903*.

Independent technical experts may be appointed to report on any potential security weaknesses associated with requirements of TCNs.

Arbitration for disputes on terms and conditions.

In the exceptional cases where providers and Government disagree on the terms and conditions for compliance with a notice, an arbitrator will determine terms and conditions.

Are there any additional oversight mechanisms?

The scope of notices is limited to core agency functions and a serious offence threshold.

Things specified in notices must be for the purpose of helping an agency perform its core functions conferred under law, as they specifically relate to:

- enforcing the criminal law for serious Australian offences; or
- assisting the enforcement of the criminal laws in force in a foreign country for serious foreign offences; or
- safeguarding national security.

As a result of these requirements, law enforcement agencies are only permitted to use these powers in the course of enforcing a criminal offence with a penalty of three years or more imprisonment, domestically or overseas.

Providers must be informed of their obligations and their right of complaint.

If a notice or request is given under the Act, the issuer must give advice relating to the provider's obligations. This ensures that smaller providers will clearly understand their requirements. When issued with a TAN or TCN, providers must also be informed of their right to lodge a complaint with the Commonwealth Ombudsman or IGIS, depending on the issuing agency.

Information is protected.

Unauthorised disclosure of information about, or obtained under, a notice is an offence. This will ensure any assistance is provided on a confidential basis and the sharing of information, including commercially sensitive information is restricted.

Additional reporting requirements add to transparency.

The public will have visibility of the use of the new powers through annual reporting requirements. The Minister is required to publish a written report every financial year that sets out the number of technical assistance notices and technical capability notices. Providers may produce transparency reports disclosing the number of notices received in a six month period. Providers may also apply for conditional disclosure exemptions to reveal the nature of assistance they have provided.

Powers reserved to senior decision-makers.

The power to issue TCNs is reserved for the joint authorisation of the Attorney-General and Minister for Communications. Requirements under TANs can only be set by the head of ASIO or an interception agency or a senior official in their organisation delegated by them.

Approval of State and Territory notices by AFP.

Before a TAN can be issued by a police force of a State or Territory it must be approved by the AFP Commissioner. The Commissioner will act as centralised coordinator and is intended to reduce duplicate requests, enable the exchange of relevant information across jurisdictions and advise on the types and forms of assistance commonly requested.

Joint ministerial approval of TCNs.

Before a TCN can be issued, it must be approved by the Minister for Communications in consideration of the notice's objectives, the legitimate interests of the provider, the notice's impact on the international competitiveness of the Australian communications industry and any representations made by the Attorney-General. This joint approval mechanism is an additional avenue for industry to feed directly into the decision-making process.

Extensive oversight by the Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman.

The powers will be oversighted by the IGIS (for ASIO, ASD & ASIS) and the Commonwealth Ombudsman (AFP, ACIC and State & Territory Police). This oversight includes:

- Notification to these bodies when the powers are issued, variations, extension, revocation.
- Clear inspection and reporting authority, including explicit discretion for the Commonwealth Ombudsman to conduct an inspection, report on that inspection and have that report tabled in Parliament.
- Information sharing provisions which allow exchange of information under the regime between Commonwealth, State and Territory oversight bodies.

Review by the Independent National Security Legislation Monitor (INSLM).

The operation of the Assistance and Access Act and each of its five schedules will be reviewed by the INSLM after it has been in effect for 18 months.

Assistance and Access Myth-busters

This law will create backdoors and undermine information security.

The Assistance and Access Act contains an express prohibition against building or implementing any weakness or vulnerability in software or physical devices that would jeopardise the security of innocent users. This is found in **section 317ZG** of the Act which also makes clear that any assistance that makes a systems' encryption or authentication less effective for general users is strictly prohibited. This same section prohibits the construction of new decryption capabilities and rules out any requirements that would prevent a company from patching existing security flaws in their systems.

All proposed requirements to build a new capability can be referred to an independent assessment panel consisting of a technical expert and a retired judge. This panel must consider whether the proposed requirements contravene the explicit prohibition against backdoors.

In fact, the Act has no ability to compel a company to build any type of capability that removes a form of electronic protection, like encryption. That is, if the company is not already capable of decrypting something – nothing in the Act can require them to build a capability to do it.

This law does not have adequate oversight.

All requests and requirements on industry are subject to extensive independent oversight by either the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or State and Territory oversight bodies. The relevant Commonwealth body is notified whenever a notice for assistance is issued, varied, extended or revoked. When an agency issues a notice, they must notify the company of their right to complain to the relevant body. Both the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security have the authority to inspect agency use of these powers by relevant agencies at any time. These bodies may make reports to Parliament on the outcome of their inspections.

Compulsory powers carry additional oversight measures to ensure they are used appropriately. For example, where a State or Territory law enforcement agency issues a notice to compel technical assistance, it must first be reviewed by the Australian Federal Police Commissioner.

Strict oversight also applies before a company can be compelled to build a new capability. Technical capability notices may only be issued by the Attorney-General. The Attorney-General's decision must also be reviewed and approved by the Minister for Communications. This creates a double-lock approval to ensure the assistance sought has been thoroughly scrutinised and is reasonable, proportionate, practicable and technically feasible.

A company may also refer any requirement to build a capability to an independent assessment panel consisting of a retired senior judge and a technical expert. This panel must consider whether proposed requirements will inadvertently create a backdoor. Further, any decision to compel assistance may be challenged through judicial review proceedings.

Public transparency is insufficient.

Given the sensitive work done by law enforcement, security and intelligence agencies and the need to protect commercially sensitive information, it will not always be possible to disclose sensitive details of how assistance has been provided. This principle is consistent with the current protections given to operational intelligence held by Australia's law enforcement and intelligence community.

Visibility over the use of the industry assistance powers is possible through mandated annual reporting requirements which require law enforcement agencies to record the number of times each power is used within a 12-month period and also disclose the type of offences the powers were used to investigate. This data will be included in the annual report required to be prepared under **subsection 186(2)** of the *Telecommunications (Interception and Access) Act 1979* alongside data concerning the use of related warrants and authorisations.

Companies and their specified personnel are also authorised to make statistical disclosures to reveal the number of requests and notices received over the course of a six-month period and reveal whether that assistance was voluntary or compulsory. Additionally, where a company provides assistance they may seek authorisation from the issuing agency to disclose information about this assistance. This process will ensure operational details are protected, while giving companies the possibility to inform interested parties about the help they are giving to authorities. Provision for these disclosures appears in **subsections 317ZF(13)** and **317ZF(14) – (17)**.

Police will use this law to prosecute minor offences.

The industry assistance powers are only available to agencies in limited circumstances. There is an express requirement that the industry assistance powers can only be used by police to enforce the criminal law for serious offences, being offences that involve a penalty of at least three years imprisonment.

To access communications content and data an underlying warrant or authorisation is still required. For example, the legislation does not replace the need for police to seek a warrant from an independent authority to intercept communications. Generally these warrants are available for offences punishable by a maximum of seven years imprisonment or more.

The availability of these powers may expand due to scope creep.

The list of agencies with access to industry assistance powers can only be expanded through legislative amendment, which would include further parliamentary scrutiny. Only Australia's core law enforcement, security and intelligence agencies are able to utilise the industry assistance powers.

The Five Eyes alliance may take advantage of this law.

The Assistance and Access Act is an Australian solution to an Australian problem – it was not requested by, or designed for, Australia's Five Eyes partner countries. While the Five Eyes share intelligence for security purposes, foreign assistance in connection with information obtained under this legislation will be undertaken consistent within the established mutual legal assistance process or through existing, and bounded, channels of cooperation. Foreign partnerships are critical to the detection and disruption of transnational crime and attacks that are coordinated through several countries.

The industry assistance powers for intelligence gathering are limited to collecting intelligence connected with Australia. This is because the Act requires a geographical nexus between the activities of a company and Australia. Further, access to content or non-content data through industry assistance powers requires a valid warrant or authorisation.

Capabilities built by the Government will leak.

The Assistance and Access Act focuses on creating a pathway for industry to deliver assistance to law enforcement and intelligence agencies where necessary. Examples of the kinds of help that may be sought through industry assistance powers include specifying the technical details of a system or device, or altering the nature of a user's service to allow a warranted surveillance device to be operated without alerting the target.

Both industry and law enforcement and security agencies have robust procedures in place to protect sensitive information and have made significant investments in the development of strong cyber security protocols that will be used to secure information relating to any form of assistance. Additionally, Australia's law enforcement and security agencies are experienced in managing operational sensitivities and will take steps to minimise risks or exposure of information.

This law will lead to mass surveillance.

The Assistance and Access Act does not authorise mass surveillance. The Act expressly prohibits the Government from requiring a company to build an interception capability or a data retention capability. Any requirements must be reasonable, proportionate, practicable and technically feasible and are subject to independent oversight and judicial review.

If conducted, digital surveillance must be consistent with existing legal regimes, like the warrant process for intercepting telecommunications in the *Telecommunications (Interception and Access) Act 1979.* The powers available under these laws are inherently targeted.

This law can compel employees to work in secret without the knowledge of their organisation.

Media reporting that has proposed this scenario is incorrect and misleading. The industry assistance framework is concerned with getting help from companies not people acting in their capacity as an employee of a company. Requests for assistance will be served on the corporate entity itself in line with the deeming service provisions in **section 317ZL**. A notice may be served on an individual if that individual is a sole-trader and their own corporate entity.

A company issued a notice can disclose information about it under **paragraph 317ZF(3)(a)** in connection with the administration or execution of that notice. This allows an employer to disclose information to their employee and vice versa in the normal course of their duty.

Additionally, a company may disclose statistical information about the fact that they have received a notice consistent with **subsection 317ZF(13)**. Further, companies and their specified personnel may disclose notice information for the purposes of legal proceedings, in accordance with any requirements of law or for the purpose of obtaining legal advice. The notices themselves are therefore not 'secret' but information about their substance is controlled to protect sensitive operational and commercial information.

This law will harm Australia's tech sector.

The Assistance and Access Act and, specifically, the industry assistance powers are not unique to Australia or western democracy. This legislation comes after the passage of the UK's *Investigatory Powers Act 2016* and New Zealand's *Telecommunications (Interception Capability and Security) Act 2013*, both of which deal with similar subject matter and provide powers to compel assistance from private companies.

During the development of the Australian legislation, the Government recognised concerns that the possibility of undisclosed changes to a company's services could harm products' competiveness at market. To answer these concerns, the legislation includes provisions for companies to publish statistics regarding the number of requests or notices they have received in a six month period under **subsection 317ZF(13)** – including where this number is zero – and make conditional disclosures to interested parties about assistance given under **subsections 317ZF(14)-(17)**. In practice, this will leave most companies unaffected, as they will be able to disclose that they have not been asked to provide assistance, while companies who do assist can demonstrate that their systems are not compromised by the

assistance they have provided, consistent with the law's explicit protections against the creation of backdoors or the degradation of security features.

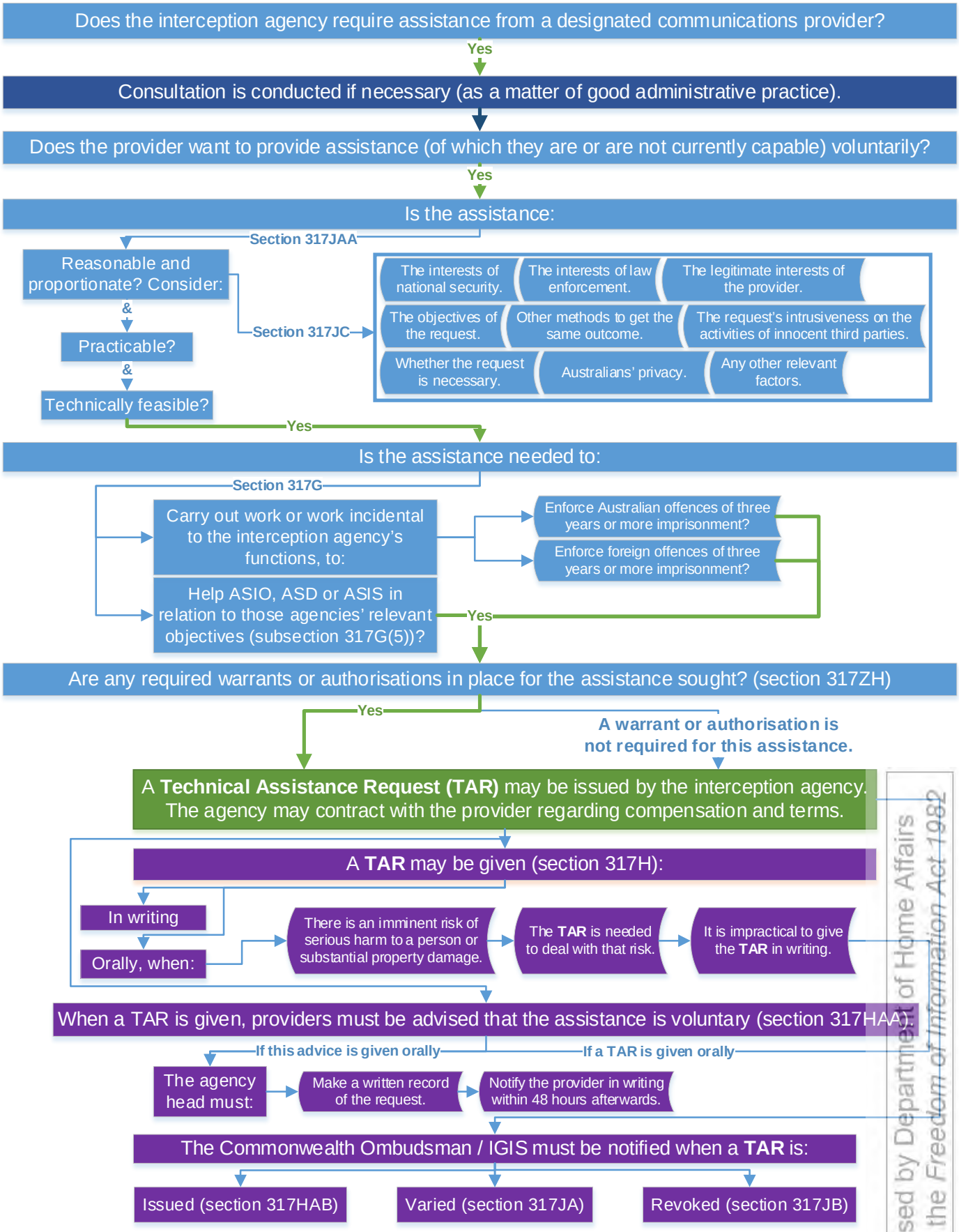
Australian companies and their employees will be hardest hit by this law.

Companies that supply communications services and devices in Australia, regardless of whether they are incorporated in Australia or not, may be the subject of technical assistance obligations under the Assistance and Access Act. The measures do not place a greater burden on Australian companies nor do they allow authorities to compel Australian citizens working for communications companies offshore. Additionally, Australian companies who primarily conduct business overseas are only obliged to assist Australian authorities to the extent that their activities relate to products and services being used within Australia. Services provided by Australian companies to persons offshore that relate to activities offshore are not classified as '*eligible activities*' for the purposes of the legislation and are thus not captured by these laws.

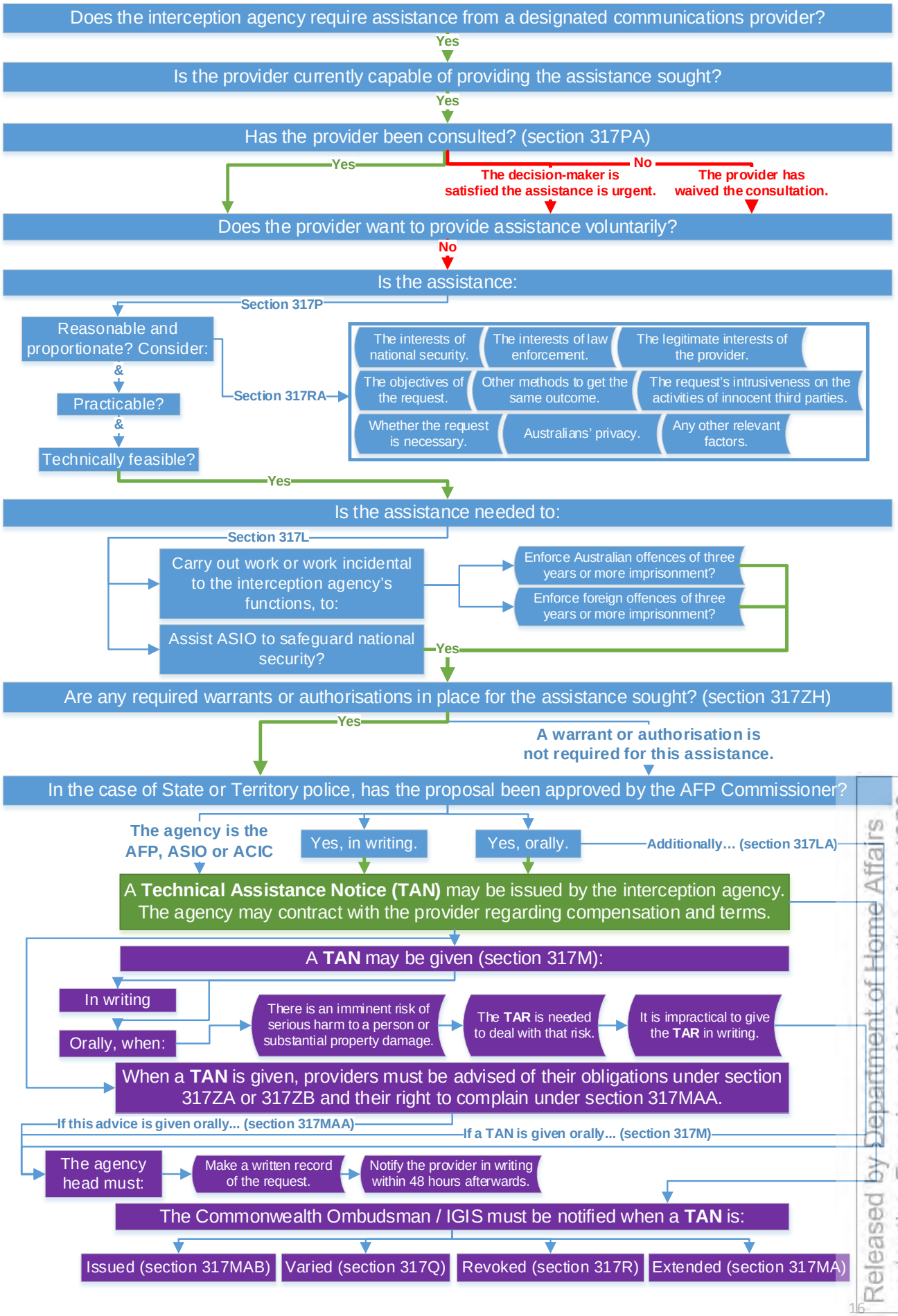
The Act's provision for penalties against individuals is not intended to apply to employees of a non-compliant company. If a company does not comply with their assistance obligations, any enforcement action that may be undertaken will apply to the enterprise. Penalties for individuals in the legislation are for the purpose of potential enforcement proceedings against sole-traders and individuals acting as businesses.

Criminal offences for the disclosure of sensitive and protected information (including sensitive commercial information) apply equally to Government officials and agency personnel and are consistent with secrecy provisions in other Commonwealth laws. Importantly, a suite of exceptions to the offence of unauthorised disclosure applicable to providers and specified personnel are listed in **subsections 317ZF(3)**, **(12B)**, **(13)**, **(15)** and **(16)**.

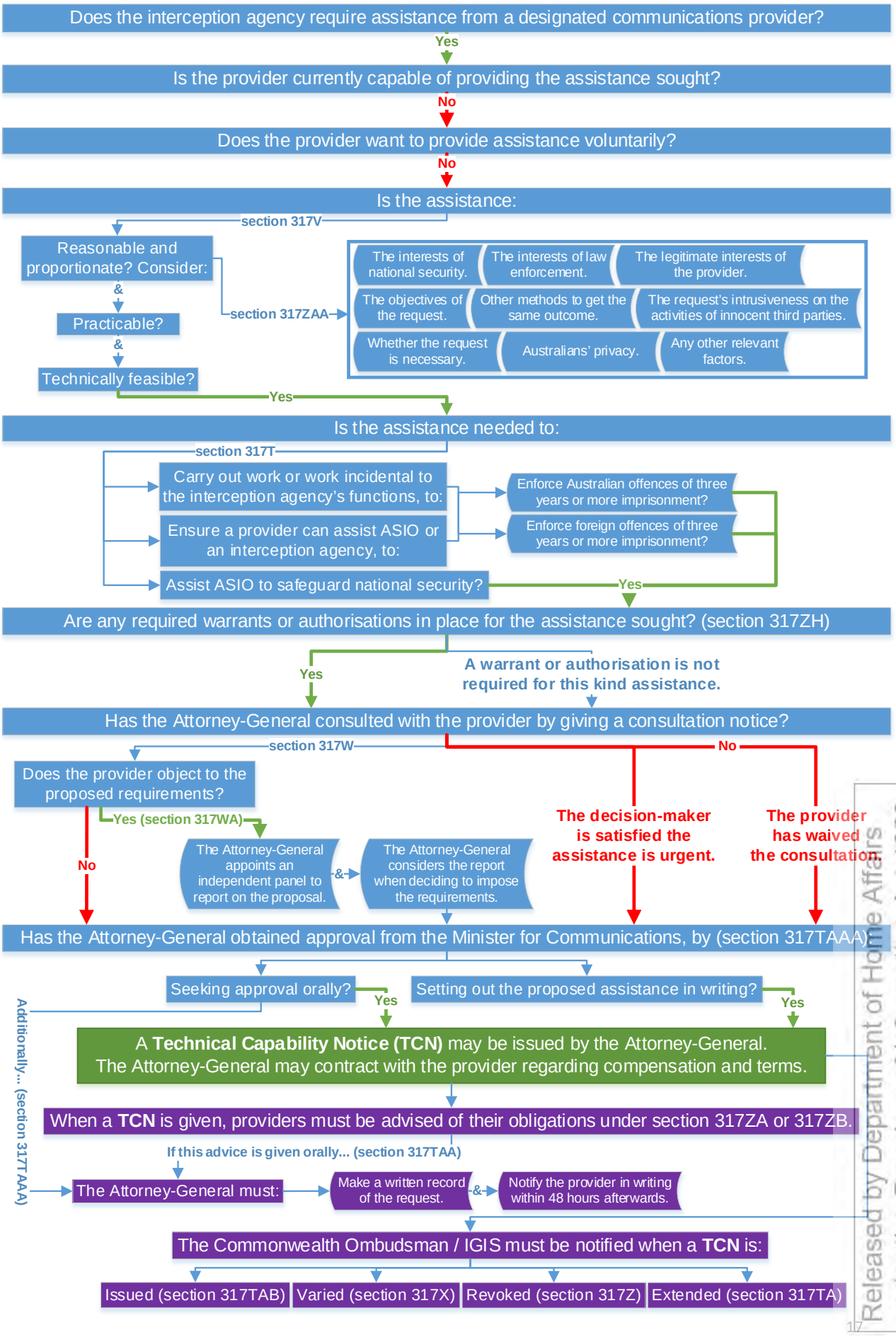
Technical Assistance Request Process



Technical Assistance Notice Process



Technical Capability Notice Process



Assistance Examples From Agencies

Law Enforcement

Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	- Requesting an ISP provide the password they have enabled on a customer supplied home modem to facilitate a review of its logs during a search warrant to identify connected devices. - Requesting a cloud storage provider changes the password on a remotely hosted account to assist with the execution of an overt account based warrant.
(b)	Providing technical information	- An application provider providing technical information about how data is stored on a device (including the location of the encryption key) to enable forensically extracted data to be reconstructed. - An international cloud hosted storage provider providing details of where a customer's data is hosted to enable a Mutual Legal Assistance Treaty process to be progressed to the host country seeking lawful access. - A mobile device provider providing a copy of their WiFi AP location maps generated through bulk analysis of customers data to correlate with location records extracted during a forensic examination of a device.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	- Requesting a cloud service provider provide a copy of the contents of a hosted account in a particular format pursuant to the execution of an overt account based warrant. - Requesting that data held in a proprietary file format extracted from a device during a forensic examination pursuant to an overt search warrant is converted into a standard file format.
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer equipment, an electronic service etc.	- Requesting a shared data centre provide access to customers computer rack to enable the execution of a computer access warrant or installation of a data surveillance device under warrant.
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	- Requesting that a social media platform assist with testing or development of a tool to automate the creation of online personas and historical content to facilitate online engagement.

Sub section 317E(1)	Listed act or thing	Examples
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation.	- Requesting an ISP advise of any technical changes to their network which could impact on an existing interception.
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	- Requesting a carrier increase the data allowance on a device that is subject to a surveillance device warrant to enable the surveillance device to be remotely monitored without consuming the targets data. - Temporarily blocking internet messaging to force a device to send the messages as unencrypted SMS's.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service provided by the provider; or a service provided by another designated communications provider.	- Requesting a carrier force a roaming device to another carriers network to enable the enhanced metadata collection capabilities of the new carrier to collect information pursuant to a prospective data authorisation.
(j)	An act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties; or - assisting the enforcement of the criminal laws in force in a foreign country; or - the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	- Requesting that the provider not inform the customer of the assistance provided to enable a computer access warrant. - Requesting that the provider delete an audit log in a customer's device relating to a computer access warrant. - Requesting a provider restore a password that was temporarily changed to enable a computer access warrant. - Requesting a provider allocate a specific dynamic IP address relating to remote access pursuant to a computer access warrant to conceal the access.

Sub section 317E(1)	Listed act or thing	Examples
(a)	Removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider.	ASIO establishes physical access to a target's mobile phone and manages to acquire a copy of the phone's contents. The opportunity is rare and unique in that the target normally employs fairly good security awareness and tradecraft. Stored within the database of an application on the phone are historical conversations with other subjects of interest that indicate the group are in the initial stages of planning a mass casualty attack at an upcoming music festival. Unfortunately the copy of the phone's contents only reveals a snapshot in time of the targets' intentions and ASIO cannot formulate an informed assessment of the group's intended activities. The application used by the group stores messages on a server in the cloud and makes use of various authentication mechanisms to authorise access to user accounts, limiting ASIO's ability to establish contemporary coverage of the group. On seeking appropriate warrants authorising ASIO to lawfully gain coverage of the target's communications, ASIO seeks out the designated communications provider (DCP) with capacity to deactivate the relevant authentication mechanisms allowing, ASIO to authenticate the target's account to provide up-to-date and ongoing coverage of the group's intentions and threat to Australia's security.
(b)	Providing technical information	In the example above, once ASIO overcomes the relevant protection mechanisms to access the relevant communications, without further technical assistance from the DCP, ASIO could expend significant time and resources attempting to understand the structure of the database associated with the chat application. The database may be complex with messages, parties to a conversation and associated attached media all stored in different portions of the database making an assessment of the subjects involved in the plan and their intentions quite difficult. It could take ASIO months to organise the data in a legible format. Using a Technical Assistance Notice, ASIO would seek out the DCP responsible for the application to gather technical information about how the application makes use of a database to store local copies of communications that have been sent and received by the application, enabling efficient and timely analysis of the relevant communications.

Sub section 317E(1)	Listed act or thing	Examples
(C)	Installing, maintaining, testing or using software or equipment	An anonymous call is placed to the National security Hotline indicating that a Terrorist cell is planning a bombing attack against the SMH Fun run in Sydney. ASIO receives this tip-off just two weeks before the event and only knows one of the group members involved. To avoid detection the group do not communicate via phone calls or face to face meetings but instead plan their attack online using application that encrypts messages as they are sent by users. Sent messages are received by the application's central server where they are decrypted and then re-encrypted with the intended recipient's key before being delivered to the intended recipient's device. ASIO secures an appropriate warrant and asks the communications provider to store copies of the target's communication before they are re-encrypted with recipient keys. To facilitate this, ASIO works with the DCP to install ASIO-controlled equipment that stores the communications. Interestingly, ASIO would store the communications in an encrypted format to prevent unauthorised access to the warranted material prior to it being disseminated back to ASIO.
(d)	Ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format.	ASIO may require that information data obtained by a carrier in response to a warrant be provided in a format that is compatible with ASIO's systems and allows for appropriate analysis.
(e)	Facilitating or assisting access to that which is the subject of eligible activities of the provider including, a facility, customer equipment, an electronic service etc.	Further to the example above, ASIO, in conjunction with the DCP, identifies a physical data centre that represents the best location to acquire copies of the target's unencrypted communications; however, the data centre is owned and operated by a third-party company. ASIO in conjunction with the chat application DCP work with the data centre DCP to arrange appropriate rack space, power and cabling for the ASIO server equipment.
(f)	Assisting with the testing, modification, development or maintenance of a technology or capability.	Further to the example above, ASIO assesses that any perceivable impact on the target's electronic service (the chat application) may result in an acceleration of the target's attack planning because ASIO assess the target exhibits a heightened level of paranoia, is erratic and prone to violence. ASIO works carefully with the DCP to ensure that the installed equipment has no perceivable effects on the target's usage of the app and is entirely covert in its operation.

Sub section 317E(1)	Listed act or thing	Examples
(g)	Notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation.	In the above example, the DCP intends to change the physical location of their infrastructure and notifies ASIO in advance of the change so ASIO can plan for the relocation of the ASIO equipment to ensure coverage of the target's communications is maintained.
(h)	Modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider.	It's feasible, in the example above, that ASIO's work with the DCP, ensuring that the installed equipment has no perceivable effects on the target's usage of the application, could require some modification, or substitution of, characteristics of a service provided by the DCP – or indeed, substitution of the service itself - in order to ensure the ongoing covert nature of ASIO's operation.
(i)	Substituting, or facilitating the substitution of, a service provided by the designated communications provider for: another service provided by the provider; or a service provided by another designated communications provider.	
(j)	An act or thing done to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to: - enforcing the criminal law and laws imposing pecuniary penalties - assisting the enforcement of the criminal laws in force in a foreign country; or - the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.	Further to the above example, it's also feasible that various other activities would be required to ensure the ASIO's operation remains covert, including: - Requiring that the assistance provided is kept confidential by the provider. - Asking the staff involved in providing the service to sign confidentiality agreements. - Requesting that a cover story to be adopted when explaining the nature of assistance being provided. - Adjusting billing, account access, data transfer logs etc. to hide evidence of access to a target device or service. - Facilitating covert physical access to a facility.