Australian Government

Department of Home Affairs

THE ASSISTANCE AND ACCESS ACT AN INTERIM GUIDE FOR:

SECURITY, INTELLIGENCE AND LAW ENFORCEMENT

Contents

Australian Government
Department of Home Affairs

Overview

Purpose of this guide

This interim guide is intended to assist security, intelligence and law enforcement agencies in the short-term use of the new industry assistance measures introduced by Schedule 1 of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

The guide explains the core elements of the powers, process requirements and key considerations for agencies when engaging with industry through the new regime. It is recommended that agencies seek legal advice if they remain uncertain about the application of the laws.

The guide is an interim step while more comprehensive guidance is developed. The Department will shortly commence consultation with Government and industry stakeholders in the development of comprehensive guidance on the use of the industry assistance measures, including standard forms and contracts that will underpin industry assistance.

Summary of Legislation

On 9 December 2018 the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 commenced into law. Now officially the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Assistance and Access Act), the legislation introduces a number of measures designed to address the ongoing problem of 'going dark'.

This guide focuses on Schedule 1 of the Assistance and Access Act which inserts Part 15 into the *Telecommunications Act 1997* (Telecommunications Act) and creates a new framework for industry assistance. This framework complements existing obligations of carriers and carriage service providers to provide assistance to law enforcement and other authorities under section 313 of the Telecommunications Act. In contrast to section 313 however, new Part 15 applies to a significantly wider range of industry members that constitute the modern communications environment and clarifies the form of assistance that can be expected from industry.

Specifically, Part 15 of the Telecommunications Act now contains three distinct new powers which allow an agency head or their delegate to issue, or seek the issue of, a:

1. **Technical assistance request (TAR)** for voluntary assistance. This grants civil immunity and limited criminal immunity for any assistance provided.

2. **Technical assistance notice (TAN)** for compulsory assistance. This power is to be used to request assistance a designated communications provider is already capable of providing.

3. **Technical capability notice (TCN)** for new capabilities. This notice can only be issued by the Attorney-General and requires a provider to create a specific capability where the provider is not currently able to assist.

It is important to note outright that these new measures **cannot be used in a manner that would jeopardise the cyber security of innocent parties** for the sake of facilitating greater government access to communications content and data. They are a mechanism for greater collaboration with the communications industry and should be used to partner with providers to address investigative challenges or enhance the execution of underlying warrants without undermining cyber security.

The Australian Government supports the use of security technologies, like encryption, that are critical to securing communications and information. Explicit safeguards are included in the Act to express this commitment in law.

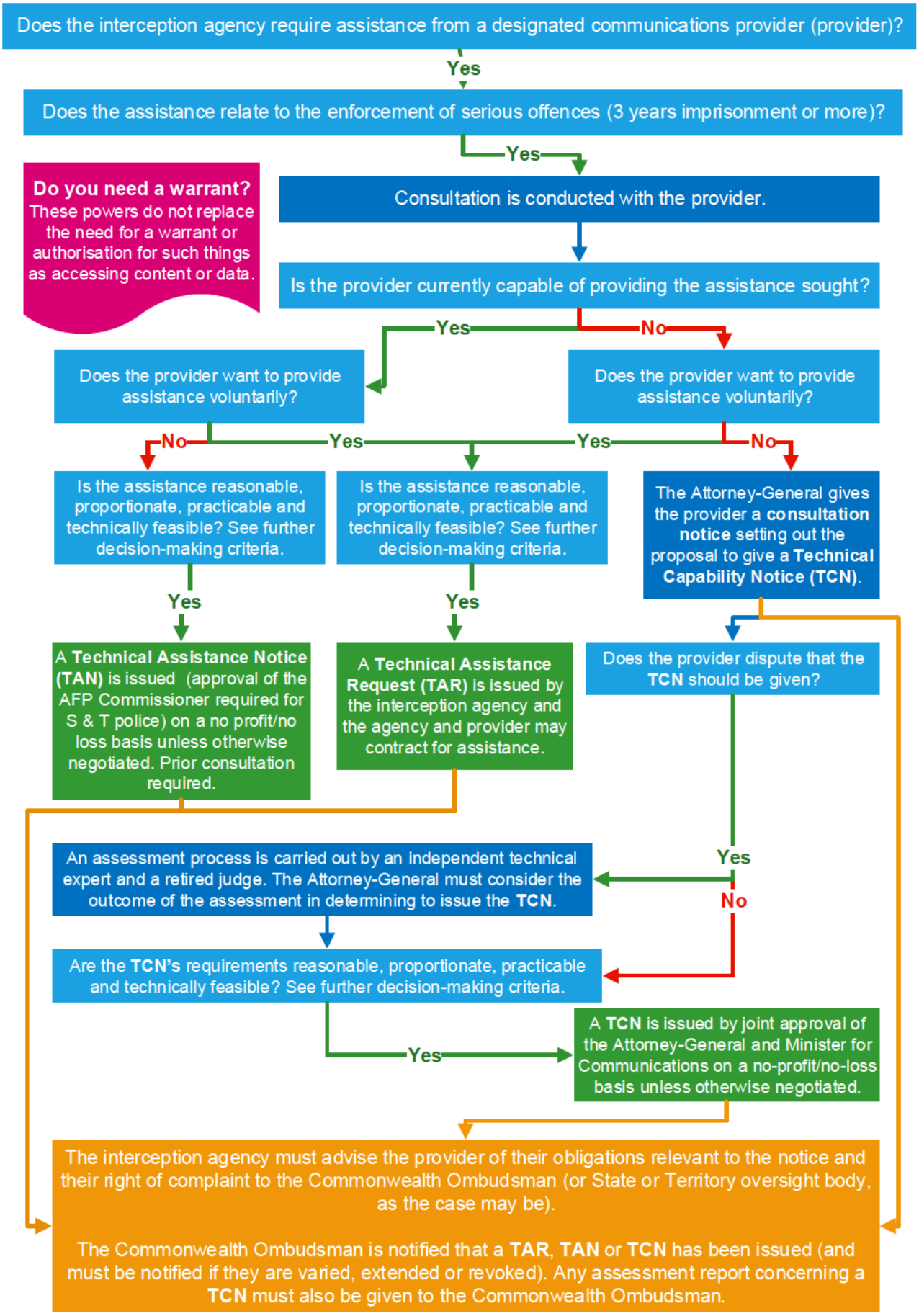
Part 15 creates a comprehensive framework around each of these powers. This guide will clarify key aspects of the scheme such as scope, enforcement, costs, terms and conditions and oversight.

The guide references relevant sections of the Telecommunications Act in **bold green.** Points in **bold red** are important factors of which decision-makers must be aware.

The Act as passed can be accessed at: https://www.legislation.gov.au/

Please direct any questions to cac@homeaffairs.gov.au.

The Industry Assistance Process



Operation of industry assistance measures

The following segment answers key questions about the industry assistance measures in Part 15 of the Telecommunications Act, including:

- *What types of powers are available?*
- *Who may be asked to provide assistance?*
- *Who can authorise the use of the powers?*
- *For what purposes can they be used?*
- *What kinds of assistance may be sought?*
- *What must decision-makers take into account?*
- *What limitations apply?*
- *How can a request or notice be changed after it has been made?*
- *What form must requests for assistance be in?*
- *How are they given to the provider?*
- *What are the costs, terms and conditions of compliance?*
- *How are requests for assistance enforced?*
- *How are industry assistance measures oversighted?*
- *What reporting requirements apply to their use?*
- *What other information is required in the request or notice?*
- *How is information shared?*

What types of powers are available?

New Part 15 of the Telecommunications Act establishes three new powers:

1. **Technical assistance request (TAR)** for voluntary assistance.

2. **Technical assistance notice (TAN)** for compulsory assistance. This power is to be used to request assistance a designated communications provider is already capable of providing.

3. **Technical capability notice (TCN)** for new capabilities. This notice can only be issued by the Attorney-General and requires a provider to create a specific capability where the provider is not currently able to assist

Detailed flow charts of the industry assistance process and the processes involved in exercising each power are at **Attachments A, B and C**.

Civil immunity (see **317G(1) & 317ZJ**) is available for providers who act:

- in accordance with a TAR, TAN or TCN, or
- in good faith purportedly in accordance with a TAR, TAN or TCN

The scope of the immunities is intended to ensure that providers are covered and do not bear risk when acting consistently with requests or requirements from agencies.

Who may be asked to provide assistance?

Prior to issuing a notice a key question should be – is the relevant entity captured?

Assistance may be sought from ***designated communications providers*** (providers). The scope of providers is intended to capture the range of entities integral to the modern Australian communications market. While many of these providers are based within Australia, some are not. The Act also applies to offshore entities who operate or supply communications services, devices or products for use, or likely use, within Australia.

This accounts for the now global nature of the communications environment where companies, or persons, can deliver communications services directly to Australia with little onshore infrastructure.

Importantly, the notices are not intended to be issued to *persons within an organisation.* Rather, notices will be served on the provider as an entity (although this could be a sole trader).

A full list of applicable providers who may be subject to the new powers is at **317C.** These include:

- Carriers and carriage service providers and anyone who facilitates the services of carriers and carriage service providers, eg.:
    - Telstra
    - Optus
    - Vodafone

- Electronic service providers (with at least one end-user in Australia) and anyone who facilitates the services of electronic service providers, e.g.:
    - Facebook
    - Google
    - Amazon Web Services

- Manufacturers of electronic equipment and anyone who facilitates the manufacture of electronic equipment (likely to be used in Australia), eg.:
    - Samsung
    - Nokia

Attachment D contains a more comprehensive list of the types of providers that fall under the scheme.

NOTE: a provider listed in **317C** can only be asked to do things that are connected to what the legislation calls the providers '*eligible activities*'. A provider's 'eligible activities' are also listed in **317C** and are connected to their relative functions as communications suppliers.

These activities are related to the use or impact of their services within Australia. Agencies should be aware that a 'jurisdictional nexus' between the provider and Australia as described in **317C** must be made out.

Who can authorise the use of the powers?

The use of the powers is restricted to:

- the Australian Federal Police (AFP),
- the Australian Criminal Intelligence Commission (ACIC),
- the Australian Security Intelligence Organisation (ASIO),

- the Australian Secret Intelligence Service (ASIS),
- the Australian Signals Directorate (ASD) and
- State and Territory Police forces.

State and Territory Police forces, the AFP and the ACIC are referred to collectively as 'interception agencies' in the legislation.

The legislation provides that the head of each agency may issue a TAR or a TAN. The head of the agency may also delegate any or all of their functions under the new regime to senior officials within their organisation. **317ZN to 317ZR** of **Division 8** of **Part 15** specify to whom the head of an agency may delegate the new powers. For example, **317ZR** notes the potential delegates for each interception agency. These delegates should be a person of seniority.

A TCN may only be issued by the Attorney-General. Agencies may request that the Attorney-General issue a TCN but must do so in accordance with any guidelines provided for in **317S** (if any).

State and Territory Police Forces – Approval by the AFP Commissioner

To improve information sharing, reduce duplication and ensure that Australian agencies are engaging with providers in a consistent and reasonable manner the Commissioner of the AFP has an approval role for TANs from State and Territory agencies.

State and Territory police forces must not give a TAN unless the decision-maker has first given the AFP Commissioner a proposal of the TAN and the AFP Commissioner has approved the giving of the TAN (see **317LA**). Variations of TANs may be made by the head of an interception agency without the approval of the AFP Commissioner.

Approval by the Minister for Communications

Given the significance of the new capabilities which may be developed, and their potential impact on industry, the Minister for Communications must approve the giving of a TCN in addition to the Attorney-General (see **317TAAA** & **317XA**).

This 'double-lock' executive decision will ensure that the concerns of the communications industry are taken into account at multiple stages of the decision-making process.

For what purposes can they be used?

The purposes for which the powers can be exercised are tied to the lawful functions and activities of the agency who is issuing, or who will benefit from, the notice or request. They are as follows:

- **ASIS**: the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being (TARs only)
- **ASD**: providing material, advice and other assistance to a person or body mentioned in subsection 7(2) of the *Intelligence Services Act 2001* on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means (TARs only)
- **ASIO**: safeguarding national security
- **Interception agencies:** enforcing the criminal law so far as it relates to serious Australian or foreign offences

Powers can only be used when related to a ***serious offence***. This is spilt into Australian and foreign offences but means an offence against a law that is punishable by a maximum term of imprisonment of 3 years or more or for life.

What kinds of assistance may be sought?

Agencies may request or require a provider to do a number of things. The scope of possible requirements is deliberately broad to ensure technological neutrality and to capture the breadth and complexity of both the relevant services and investigatory needs. These include:

- Providing technical information, for example:
    - explaining how data is stored on a device or receiving more detail about the design and make of a service or computer

- Installing, maintaining, testing or using software or equipment, for example:
    - Testing tools built by law enforcement that facilitate targeted access to a device or service under warrant.

- Ensuring that information obtained under a warrant or authorisation is provided in a particular format, for example:
    - 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.

- Doing an act or thing which would assist in executing a warrant under a law of the Commonwealth, a State or Territory, for example:
    - ensuring that a telecommunications service covered by a warrant can be properly executed.

- Providing access to services, devices or facilities of a provider, for example:
    - requesting a shared data centre provide access to a customer's computer rack to enable the installation of a data surveillance device under warrant.

- Activities to conceal that any-thing has been done under these powers or other powers used in a related investigation, for example:
    - extending a customer's data allowance to hide the fact that surveillance data is being uploaded by the device to police.

The full list of acts and things appears in **317E.** The kinds of assistance available depend upon the type of power being exercised.

The list in **317E** is *non-exhaustive* in the case of voluntary assistance requests but *exhaustive* for the compulsive powers.

A key question to ask, or determine in concert with a provider, is – do they currently have the capability to give this kind of assistance?

If they **are** capable of giving the assistance, then a TAR or TAN may be issued to request or require it.

If they **are not** capable of giving the assistance then a TAR can be issued to request that they build the capability or an agency may request that the Commonwealth Attorney-General issue a TCN to require them to be capable of giving this kind of assistance.

Additionally, where a provider has the ability to do so at the time the assistance is sought, providers may be asked (under a TAR) or compelled (under a TAN) to remove a form of electronic protection. However, none of the new powers can be used to ask or require providers to build a new capability to remove a form of electronic protection.

What must decision-makers take into account?

The decision-maker must be satisfied of certain matters, and turn their mind to specific criteria, before issuing a TAR or TAN.

The decision-maker must be satisfied that the request or requirement is reasonable and proportionate and that compliance with them is practicable and technically feasible (see **317JAA** for TARs and **317P** for TANs).

In determining whether a request or notice is reasonable and proportionate the decision-maker must have regard to the following matters (see **317JC** for TARs and **317RA** for TANs):

- the interests of national security;
- the interest of law enforcement;
- the legitimate interests of the relevant provider;
- the objectives of the request or notice;
- the availability of other means to achieve these objectives;
- whether the requirements are the least intrusive form of industry assistance insofar as it might impact innocent third parties;
- whether the requirements are necessary;
- the legitimate expectations of the Australian community relating to privacy and cybersecurity; and
- such other matters the decision-maker considers relevant.

Similarly for a TCN, the Attorney-General must not issue a TCN unless satisfied that the requirements imposed by the notice are reasonable and proportionate and that compliance with them is practicable and technically feasible (see **317V**).

In determining whether the requirements of a TCN are reasonable and proportionate the decision-maker must have regard to all of the matters outlined above. Further, the Attorney-General must not give a TCN to a provider unless the Attorney-General has notified the Minister for Communications about the proposal to give a TCN and the Minister for Communications has approved the giving of the notice. In deciding whether not to approve the giving of the notice, the Minister for Communications must take into account the following matters (see **317TAAA(6)**):

- the objectives of the notice;
- the legitimate interests of the designated communications provider; and
- the impact of the notice on the efficiency and international competitiveness of the Australian telecommunications industry;
- any representation may by the Attorney-General to the Minister about the proposal to give a TCN; and
- such other matters the Minister considers relevant.

Consultation requirements

The decision-making criteria is comprehensive. However, to fully understand some matters like the interests of a provider or technical feasibility it is expected that consultation with the affected

provider will be necessary. As a matter of practice and to minimise the risk of any adverse impact on providers or the wider public, consultation should be undertaken at all stages, regardless of whether it is a TAR, TAN or TCN. Urgent circumstances or well-established relationships with providers may mean that truncated consultation periods are practical and necessary.

In any event, **317PA** establishes mandatory consultation requirements before a TAN is given to a provider. This may be waived if the decision-maker is satisfied the assistance is urgent or the provider waives compliance.

Before a TCN is issued, there is a mandatory 28 day (minimum) consultation period. The requirement to consult will not apply if the Attorney-General is satisfied that the TCN should be given as a matter of urgency, compliance with the consultation requirement is impracticable or it is waived with consent from the provider (see **317W**).

What limitations apply?

There are a number of key limitations on TARs, TANs and TCNs contained within **Division 7** of Part 15 in the Telecommunications Act. Broadly, these include:

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

2. Requirements and requests 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**

Additionally, a TAN or TCN only remains in force for a maximum of 12 months at a time. As discussed below, this can be extended.

No systemic weaknesses or vulnerabilities

The key prohibition in the Assistance and Access Act is the limitation against any of the powers from requesting or requiring that a provider build or implement a ***systemic weakness*** or ***systemic vulnerability*** into a form of ***electronic protection***

What is a form of ***electronic protection***?

Electronic protection is a defined term in **317B** and includes methods of authentication and encryption.

What is a ***systemic weakness/vulnerability***?

Systemic weakness and systemic vulnerability are defined terms within **317B**. They mean *a vulnerability or weakness that affects a whole class of technology, but do not include a vulnerability or weakness selectively introduced to one or more target technologies that are connected with a particular person*. *For this purpose, it is immaterial whether the person can be identified.*

There are a few terms to unpack:

- The term '*class of technology'* is not a defined term and therefore retains its ordinary meaning. Technological classes include particular mobile device models, carriage services, electronic services or software. The term is intended to encompass old and new technology and technology subclasses within a broader class of technology (for example, an iOS mobile operating system within a particular type of mobile device).
- The term ***target technology*** is defined in **317B**. Broadly, it means a particular electronic service, carriage service, software (including updates), installed or to be installed on a computer or item of equipment, customer equipment or data processing device, used, or likely to be used, by a particular person, regardless of whether the person can be identified or not.
- The term '*connected*' is not defined, but the term is intended to capture technologies associated with the particular person (i.e. a shared computer within a family). The term is intended to be narrower than the broader notion of 'connectivity' with the internet.

The intended effect of these combined terms and definitions is to prohibit requirements that would impact entire models, types or systems of technologies and create a material risk that otherwise secure information would be accessed by unauthorised third parties (**317ZG(4A), (4B) and (4C)**).

However, the definitions of systemic weakness or vulnerability explicitly allow for selective, targeted activities that weaken forms of electronic protection in a service or device of a particular person of interest. The caveat is that this targeted weakening must not have the effect of undermining wider cyber security protections for innocent third parties.

Please also see the clarifying terms in **317ZG** which make explicit that the prohibition against systemic weakness or vulnerability includes:

- building or implementing a new decryption capability (**317ZG(2)**);
- rendering wider systems of authentication or encryption less effective (**317ZG(3)**); and
- acts or things that will, or are likely to, jeopardise the security of any information held by non-target persons (**317ZG(4A)**).

A warrant or authorisation is still required

If the agency is seeking to undertake activities that would require a warrant or an authorisation under a Commonwealth, State or Territory law, the warrant or authorisation is still required. For example, a provider cannot be asked to furnish things like the content of communications or telecommunications data absent an interception warrant or data authorisation under the *Telecommunications (Interception and Access) Act 1979.* Further, a TAR, TAN or TCN cannot require or request a provider to use a surveillance device or access data held in a computer if a law of a State or Territory would require a warrant or authorisation for that use or access. The limitations in **317ZH** applies to TARs, TANs and TCNs. This limitation also applies to overseas providers who currently cannot be issued a warrant or authorisation.

Importantly, these limitations do not prevent requiring or requesting a provider to do things that would assist in, or facilitate, giving effect to a warrant or authorisation. For example, a provider can still be asked to install a surveillance device obtained under warrant or undertake activities that will facilitate the interception of services covered by an interception warrant.

No interception or data retention capabilities

The Attorney-General cannot issue a TCN requiring a provider to build an interception, delivery or data retention capability (see **317ZGA**). These capabilities are already defined and limited by other

legislation, like the *Telecommunications (Interception and Access) Act 1979,* and continue to be governed by existing regimes.

Agencies cannot seek to request a TCN to build capabilities of this kind.

Varying, Extending or Revoking a Notice.

The Act ensures that TARs, TANs and TCNs can be varied, extended and revoked.

Variation: All requests and notices may be varied – this ensures that both minor and more significant changes can made as circumstances require. In order for a request or notice to be varied, the decision-maker must reach the same state of satisfaction and take into account all of the same matters that were considered in the making of the original request or notice.

A variation cannot extend the duration of a notice. An extension must be sought in these cases.

- *Relevant sections* – **317JA** (TARs), **317Q** (TANs) & **317X; 317XA; 317Y; 317YA** (TCN)

Extension: in relation to a TAN or TCN, if no expiry date is specified, the notice will expire 90 days after the notice is issued. Any specified expiry date must be later than 12 months after the notice was given. The period a notice is in force can be extended with the agreement of the provider; each period is not to exceed 12 months. If a notice does expire, a new notice may also be issued in the same terms as the expired notice, allowing continuing obligations and assistance to be set.

By default, a TAR will expire after 90 days unless an expiry date is specified in the request. There is no maximum time limit for TARs to remain in force (**317HA**).

- *Relevant sections* - **317MA** (TANs), **317TA** (TCN)

Revocation: a TAR, TAN or TCN can be revoked by a decision-maker. Revocation is *mandatory* if a decision-maker is satisfied that the request or notice is not reasonable and proportionate or compliance with the request or notice is not practicable or technically feasible. A written notice must be given to the provider.

- *Relevant sections* – **317JB** (TARs), **317R** (TANs), **317Z** (TCNs)

As discussed below, relevant oversight bodies must be notified whenever a request or notice is issued, varied, extended or revoked. For interception agencies, notices must be given to the Commonwealth Ombudsman. Notifications must occur **within 7 days** after the relevant event.

What form must they be in?

Generally speaking, a TAR or TAN must be in writing (see **317H** for TARs; **317M** for TANs) unless specific circumstances exist. A request or notice may only be given orally, in urgent circumstances and a written record must be made within 48 hours of issuing the request or notice.

Written copies of any oral records must be given to the provider and records must be retained while notices are in force (in addition to any other requirements, for example under the *Archives Act 1983*).

How Notices are served?

Notices, summons or processes in any proceedings connected with **Part 15** (including a TAN or TCN) may be served on a provider in accordance with **317ZL**.

Section **317ZL** deems a notice, summons or process to be served or given if:

- in relation to providers:
    - It is left at, or sent by pre-paid post to, the nominated address for service given by the provider; or
    - If it is sent to the nominated electronic address for service given by the provider;
- in relation to a body corporate that is incorporated outside Australia and the body corporate does not have a registered office or a principal office in Australia:
    - if the body corporate has an agent in Australia, it is served on or given to the agent;
    - if the body corporate carries on business, or conducts activities, at an address in Australia, it is left at, or sent by pre-paid post, to a place where the body corporate carries on business or conducts activities in Australia.

317ZL does not prevent service being effected through section 587 and 588 of the Telecommunications Act or section 28A of the *Acts Interpretation Act 1901*.

What are the costs, terms and conditions of compliance?

When a provider receives a voluntary request, they may negotiate with the relevant issuing body for compensation. When a provider is compelled to give assistance because they have been issued a TAN or a TCN, they do so, by default, on the basis that they neither profit nor lose money (***no-profit/no-loss compliance***). No-profit/no-loss compensation only includes the reasonable costs of compliance. This may be lower than those costs calculated by the provider.

No-profit/no-loss compliance will apply unless the provider and the applicable costs negotiator otherwise agree (allowing commercial terms to be reached, for example), or the relevant decision-maker is satisfied that no-profit/no-loss compliance is against the public interest. This is not expected to be widely used and should be the exception not the rule. Considerations that must be taken into account to determine what is in the public interest are:

- The interests of law enforcement (where the notice was issued by a law enforcement 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.
- The reasons for imposing the mandated assistance.
- Whether the provider has acted recklessly or negligently in relation to this assistance activity.
    - This consideration is not expressly listed in the Act but should be considered as a matter of policy.

The full list of considerations appears in **317ZK(2)**.

If a provider does not agree with the rate of compensation, an arbitrator may be appointed to determine an alternative rate. Compliance means a provider offers assistance in accordance with the

terms and conditions as agreed with the agency or, in the case of a dispute, as agreed with the arbitrator. This process of appointing an arbitrator is detailed in 317ZK(4)-(16).

How are Notices enforced?

The Assistance and Access Act creates an environment for providers to cooperate with law enforcement, security and intelligence agencies. The use of these powers will primarily be collaborative rather than adversarial as many providers are willing to give forthright assistance without the need for legal compulsion.

However, the Act also provides the ability to commence enforcement proceedings against a provider where they refuse to comply with their legal obligations. These provisions are set out in Division 5.

Carriers and carriage service providers are obliged to comply with any requirements under a TAN or TCN to the extent that they are capable of doing so (317ZA(1)). Further, a person – most likely an employee – must not cause, or seek to cause, a carrier or carriage service provider to contravene their TAN or TCN obligations (317ZA(2)). These provisions are subject to the civil penalty provisions in Part 31 of the *Telecommunications Act 1997* and consistent with breaches of existing assistance obligations under section 313.

Providers (other than carriers and carriage service providers) are obliged to comply with any requirements made under a TAN or TCN to the extent that they are capable of doing so (317ZB(1)). The civil penalty for contravention of this obligation is 47,619 penalty units (approximately 10 million dollars) for body corporates and 238 penalty units (approximately 50 thousand dollars) for other entities, such as individuals. Injunctions and enforceable undertakings may be ordered by the Federal Courts or the Federal Circuit Court in relation to the offences listed under 317ZB(1).

It is a defence against non-compliance for a provider to make out that an act or thing that they may be required to do in a foreign country would contravene a law of that foreign country. This defence has been established to ensure that providers are not put in the position whereby compliance with Australian law will mean they breach the laws of a relevant foreign jurisdiction.

For the purpose of enforcement proceedings for contravention of 317ZB the Communications Access Co-ordinator (cac@homeaffairs.gov.au), located within the Department of Home Affairs, is an authorised applicant and will determine whether proceedings should be initiated or not.

How are these powers oversighted?

Use of industry assistance powers are subject to requirements that the Commonwealth Ombudsman or Inspector-General of Intelligence and Security, depending on the agency using the powers, be notified:

	Event			
Power	**Issue**	**Variation**	**Extension**	**Revocation**
TAR	317HAB	317JA	N/A	317JB
TAN	317MAB	317Q	317MA	317R
TCN	317TAB	317X	317TA	317Z

A decision that the no-profit/no-loss compliance under 317ZK does not apply must also be reported to either the Inspector-General of Intelligence and Security or the Commonwealth Ombudsman, depending on the agency making the decision (317ZKA).

The Commonwealth Ombudsman may inspect the records of a law enforcement agency to determine their compliance with these notification requirements. The Commonwealth Ombudsman may then make a written report on the results of these inspections and give it to the Home Affairs Minister.

The inspection powers of the Commonwealth Ombudsman appear in **317ZRB**.

The Commonwealth Ombudsman is also empowered, under existing laws, to inspect the exercise of powers under the *Telecommunications (Interception and Access) Act 1979*, the *Surveillance Devices Act 2004* and activities conducted under the industry assistance regime in connection with warrants or authorisations granted by either legislation.

Officials of the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman are exempted from the unauthorised disclosure provisions that protect TAR, TAN and TCN information (**317ZF**). These officials may disclose this information as necessary in the course of performing their oversight duties. In the case of an Ombudsman official, these disclosures may include giving information to a State or Territory inspecting authority charged with oversighting an interception agency based in that jurisdiction.

What reporting requirements apply?

The use of industry assistance powers is subject to annual reporting requirements.

Interception agencies must notify the Home Affairs Minister of their use of the industry assistance powers throughout the year ending 30 June. This notice must include the number of TARs, TANs and TCNs issued during that period and, specifically, the number of TCNs that were directed towards ensuring providers are capable of giving help to interception agencies. Additionally, if any TARs, TANs or TCNs were given in relation to the enforcement of an Australian offence with a penalty of three years or more imprisonment, these offences must be listed.

ASIO must detail their use of the powers as part of their classified annual report required by **94** of the *Australian Security Intelligence Organisation Act 1979*. Similarly, ASIS and ASD must detail their use of the powers in their classified annual reports required by **42** and **42A** of the *Intelligence Services Act*.

What other information is required in the request or notice?

The Act stipulates that when issuing a request or notice certain information and advice must be given to a provider. This is to ensure that the provider is aware of their obligations under law and know the potential remedies available.

TARs (317HAA): The decision-maker must advise the provider that compliance with the request is voluntary.

TANs (317MAA): The decision-maker must give the provider advice relating to their obligations under a notice, that is, their obligations under either **317ZA** or **317ZB** as applicable. As a matter of policy, the advice must also contain information about the penalties for non-compliance and the provider's right to seek judicial review.

- The decision-maker must also advise the provider of their right to make a complaint about the conduct of the agency to a relevant oversight body.

TCNs (317TAA): The decision-maker must give the provider advice relating to their obligations under a notice, that is, their obligations under either **317ZA** or **317ZB** as applicable. As a matter of policy, the advice must also contain information about the penalties for non-compliance and the provider's right to seek judicial review.

NOTE: All advice discussed above may be given orally or in writing. If made orally it must be written down within 48 hours.

How is information shared?

Unauthorised disclosure of information pertaining to TARs, TANs or TCNs is an offence under **317ZF**. Authorised disclosure broadly includes disclosure that is made outside of the course of an investigation or associated legal proceedings, disclosure in the performance and exercise of agency powers and functions, disclosure to and within relevant oversight bodies, as well as disclosure in compliance with a relevant law of the Commonwealth, a State or Territory.

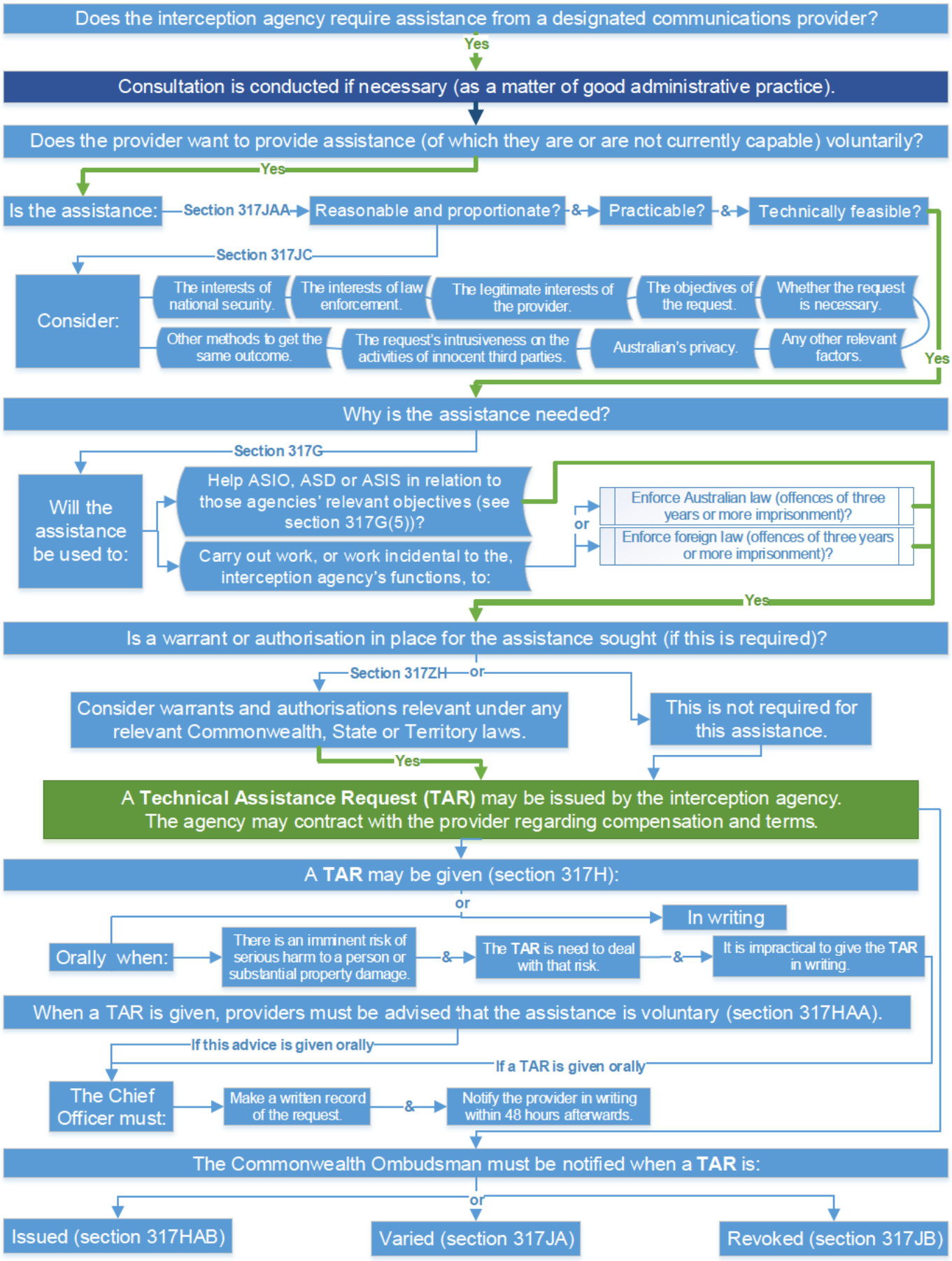
Proposed disclosures of TAR, TAN or TCN information between agencies are subject to the notification of the Communications Access Co-ordinator appointed under the *Telecommunications (Interception and Access) Act 1979*. This requirement appears under **317ZF(12)**. Until administrative processes to govern this notification process are put in place, please send a notification to cac@homeaffairs.gov.au of the fact of the proposed disclosure – no further details will be necessary.

Disclosures are also authorised for the purpose of oversight by State and Territory inspecting authorities, collecting statistics on the use of industry assistance powers and, with the approval of the issuing agency, disclosures of specified information to the public.

Agencies or the Attorney-General, as the case may be, can permit a provider to make conditional disclosures of TAR, TAN or TCN information. This disclosure mechanism will allow providers to request on-disclosure of information throughout their supply chain or to other interested parties (see **317ZF(14) – (16)**).

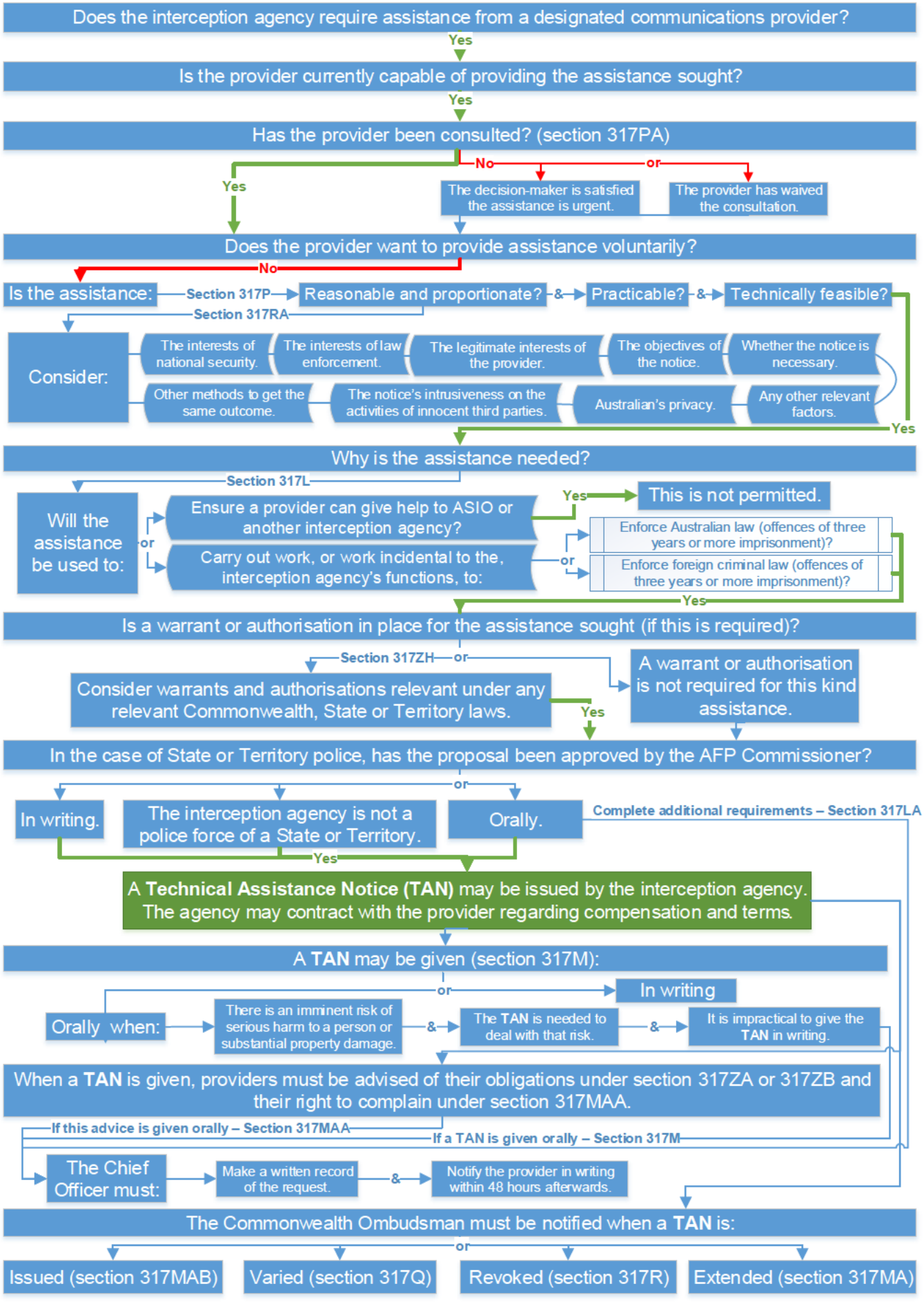
The Technical Assistance Request Process

ATTACHMENT A



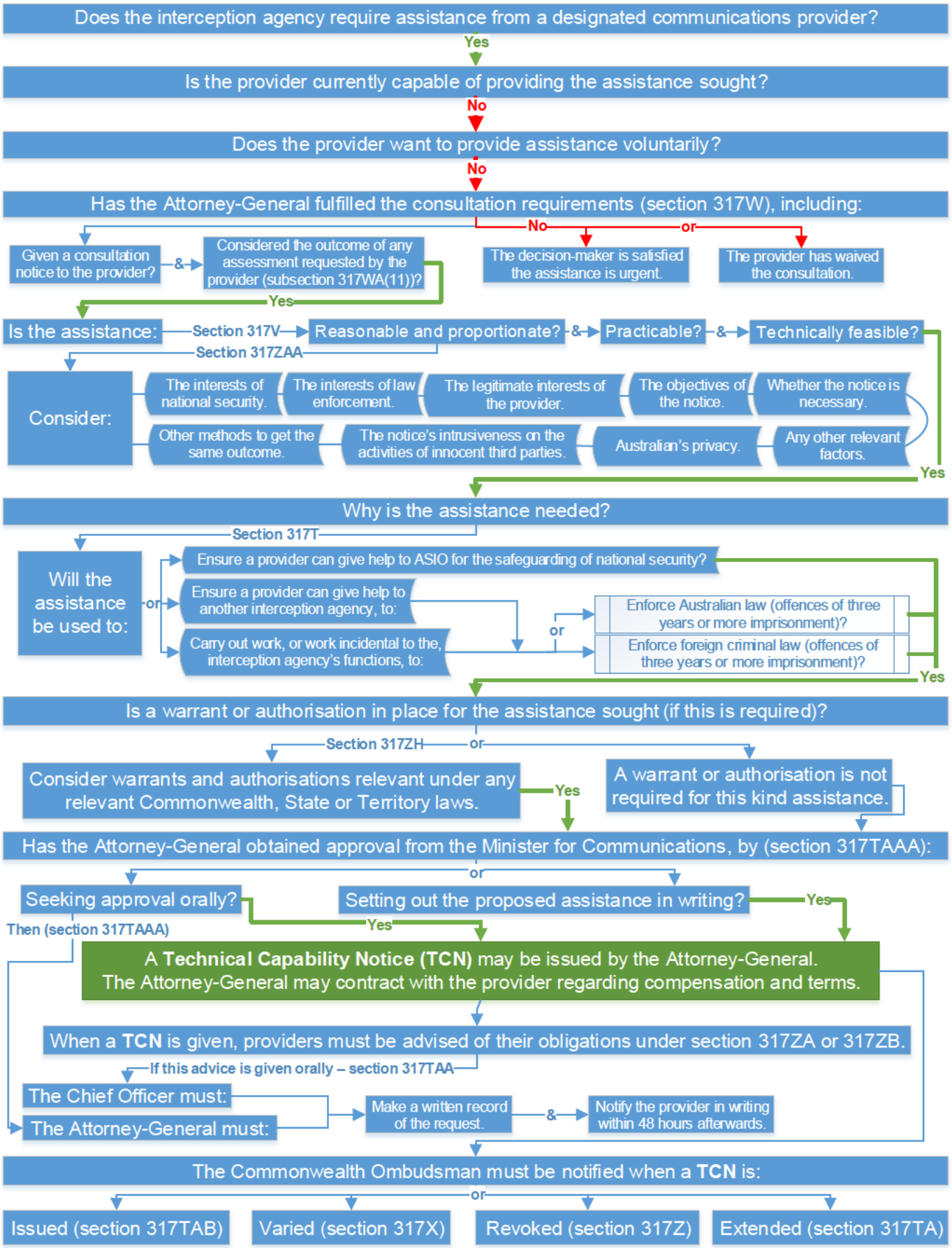
The Technical Assistance Notice Process

ATTACHMENT B



The Technical Capability Notice Process

ATTACHMENT C



Examples of designated communications providers

ATTACHMENT D

Item	Section 317C – Types of Designated Communications Provider	Examples
1	the person is a carrier or carriage service provider	Telstra; NBN Co; TPG; Optus; Vodafone; Macquarie Telecom
2	the person is a carriage service intermediary	Dodo or datacentres that provider a connection for a fee to an ISP (e.g. Equinix)
3	the person supplies a service that facilitates the supply of a carriage service	Softel – a UK based systems integrator/ managers service provider. Their offering includes customised software development.
4	the person provides an electronic service	Microsoft, Google, Facebook; WhatsApp
5	the person supplies a service that facilitates the provision of an electronic service	Amazon Web Services or other Content Delivery Network – they host content (e.g. Facebook videos) on proxy servers, closer to the end user, to increase effective download speeds.
6	the person develops, supplies or updates software used, or for use, in connection with a carriage service or an electronic service	Google; Microsoft; Nokia; Cisco; Virtual Private Network developers; add-on developers
7	the person manufacturers, supplies, installs, maintains or operates a facility	Macquarie Telecom or other Data centres (e.g. Equinix), companies who supply cables and wires for the telecommunications network
8	the person manufactures or supplies components for use in the manufacture of a facility	Cisco or systems integrators like DimensionData
9	the person connects a facility to a telecommunications network	Undersea cable operators like PIPE Pacific Cable. Providers of multiple cloud serve offerings like Megaport
10	the person manufactures or supplies customer equipment	Microsoft, Google, Apple; Samsung and other device manufacturers
11	the person manufactures or supplies components for use in the manufacture of customer equipment	Broadcom – they manufacture semiconductors for use in wireless and broadband applications
12	the person installs or maintains customer equipment and does so otherwise than in a capacity of the end-user of the equipment	Apple Store
13	the person connects customer equipment to a telecommunications network and does so otherwise than in the capacity of the end-user of the equipment	McDonalds; Westfield or other free wifi providers
14	the person is a constitutional corporation who manufacturers, supplies, installs or maintains data processing devices	Dell; Cisco; IBM
15	the person is a constitutional corporation who develops, supplies or updates software that is capable of being installed on a computer, or other equipment that is, or is to be, connected to a telecommunications network.	Adobe; any Australian retailer who offers a mobile phone application for online shopping or offers an application for mobile viewing

Operational examples from agencies

ATTACHMENT E

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.

Sub section 317E(1)	Listed act or thing	Examples
(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.
(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.

Intelligence agencies

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.
(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

Sub section 317E(1)	Listed act or thing	Examples
		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.
(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	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.

Sub section 317E(1)	Listed act or thing	Examples
	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.	- 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.

Assistance and Access Act - Relevant Agencies

ATTACHMENT F

Jurisdiction	Agency	TAR	TAN	TCN	Computer Access Warrant	Search Warrant – Crimes Act	Search Warrant – Customs Act*	Comments
Commonwealth	ABF	✗	✗	✗	✗	✗	✓	
	ASIS	✓	✗	✗	✗	✗	✗	
	ASD	✓	✗	✗	✗	✗	✗	
	ASIO	✓	✓	✓	✗	✗	✗	ASIO Act - CAW
	AFP	✓	✓	✓	✓	✓	✗	
	ACIC	✓	✓	✓	✓	✗	✗	
	Australian Commission for Law Enforcement Integrity	✗	✗	✗	✓	✗	✗	
NSW	NSW Police	✓	✓	✓	✓ (FO)	✓ (FA)	✗	
	NSW Crime Corruption Commission	✗	✗	✗	✓ (FO)	✗	✗	
	NSW ICAC	✗	✗	✗	✓ (FO)	✗	✗	
	Law Enforcement Conduct Commission	✗	✗	✗	✓ (FO)	✗	✗	
Victoria	Victoria Police	✓	✓	✓	✓ (FO)	✓ (FA)	✗	
	Independent Broad-based Anti-corruption Commission	✗	✗	✗	✓ (FO)	✗	✗	
Queensland	QLD Police	✓	✓	✓	✓ (FO)	✓ (FA)	✗	
	Crime and Corruption Commission	✗	✗	✗	✓ (FO)	✗	✗	
Western Australia	WA Police	✓	✓	✓	✓ (FO)	✓ (FA)	✗	
	Corruption and Crime Commission	✗	✗	✗	✓ (FO)	✗	✗	
South Australia	SA Police	✓	✓	✓	✓ (FO)	✓ (FA)	✗	
	Independent Commissioner Against Corruption	✗	✗	✗	✓ (FO)	✗	✗	
Northern Territory	NT Police	✓	✓	✓	✓ (FO)	✗	✗	
Tasmania	Tasmania Police	✓	✓	✓	✓ (FO)	✓ (FA)	✗	

FO = Federal offences only; FA = State offence with a federal aspect; * = for Customs Act police or an ADF member may apply for warrants in limited circumstances

Australian Government

Department of Home Affairs

The Assistance and Access Act

The story so far…

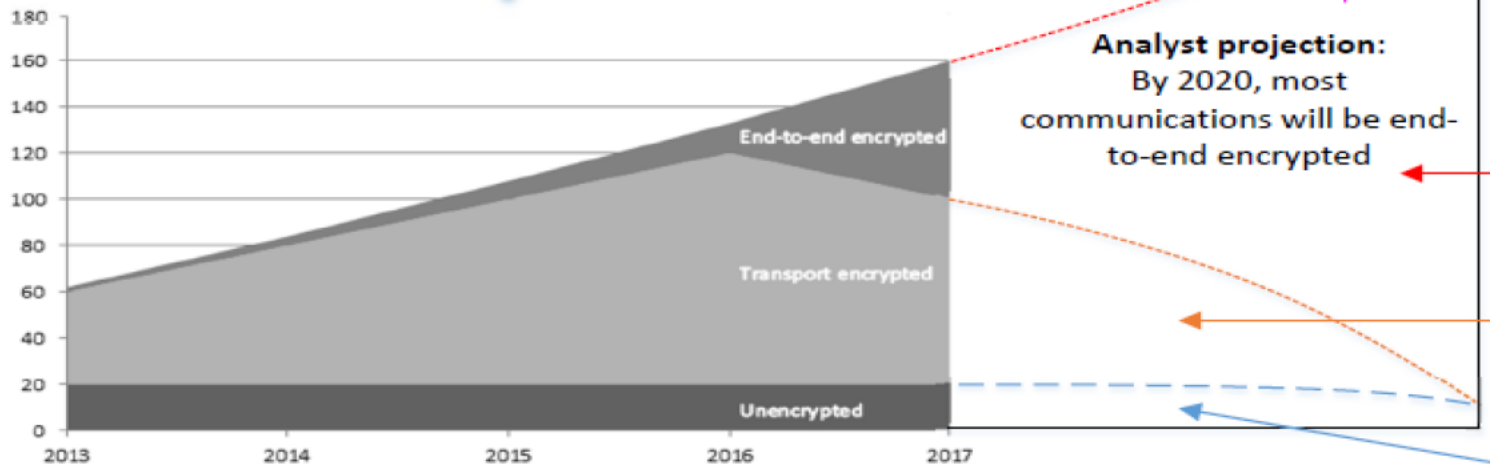
- Developed in consultation with law enforcement and industry.
- Passed the Australian Parliament on 6 December 2018. Became law on 8 December 2018.
- Now under review by the Parliamentary Joint Committee on Intelligence and Security.
- Implementation is ongoing and formal guidance is being developed.

FOI Document #2

Encryption

GOING DARK

Daily Global Mobile Messages (billions)



Analyst projection:
By 2020, most communications will be end-to-end encrypted

End-to-end encryption
Data in transit is encrypted
Server is encrypted

Transport encryption
Data in transit is encrypted
Server is not encrypted

Unencrypted
No encryption, such as SMS

Amount of data **lawfully intercepted** by the AFP that uses some form of encryption:

>90%

Percentage of priority cases where encryption has **eroded** ASIOs technical intelligence coverage:

>90%

Number of ASIO's **most concerning** counter-terrorism targets that actively use encrypted messaging to conceal communications

>95%

A holistic approach

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

...but its not about 'breaking' encryption

A couple of new powers

- New computer access warrants under the *Surveillance Devices Act 2004*
- Enhanced search warrant powers under the *Crimes Act 1914* and *Customs Act 1901.*
- Enhanced powers for ASIO to assist with access to data.
- A new industry assistance framework in the *Telecommunications Act 1997*

Computer Access Warrants

- New Division 4 of the *Surveillance Devices Act 2004* (section 27A)
- Mirrors existing ASIO computer access powers

What can you do?

- Covert, warranted, access to computers, inc. mobile devices
  - Focused on 'end-point' access
  - Available for investigation of federal offences, 3 years and over
  - Allows use of computer systems, telecommunication and interception
  - Can conceal use after the fact

Limitations and oversight

- Approved by a Judge or eligible AAT member
- Oversighted by Commonwealth Ombudsman, (inspections, record-keeping, reporting)
- Jurisdictional limitations – appropriate consenting official
- Cannot unduly interfere with communications or cause material loss or damage

Enhanced Search Warrants

- Amendments to the *Crimes Act 1914*

What can you do?

- Apply for search warrants for federal offences or State offences with a federal aspect
- Remotely execute the warrant using telecommunications networks or computers
    - notification to occupier or warrant subject still required
- Access 'account-based data' (i.e. social media accounts)
- Increased time for examination of devices found during execution of a warrant

AND...

- Increased penalties for non-compliance with an order to assist with access from an electronic device
    - From 2 – 5 years or 10 years for serious offences

Industry Assistance Framework

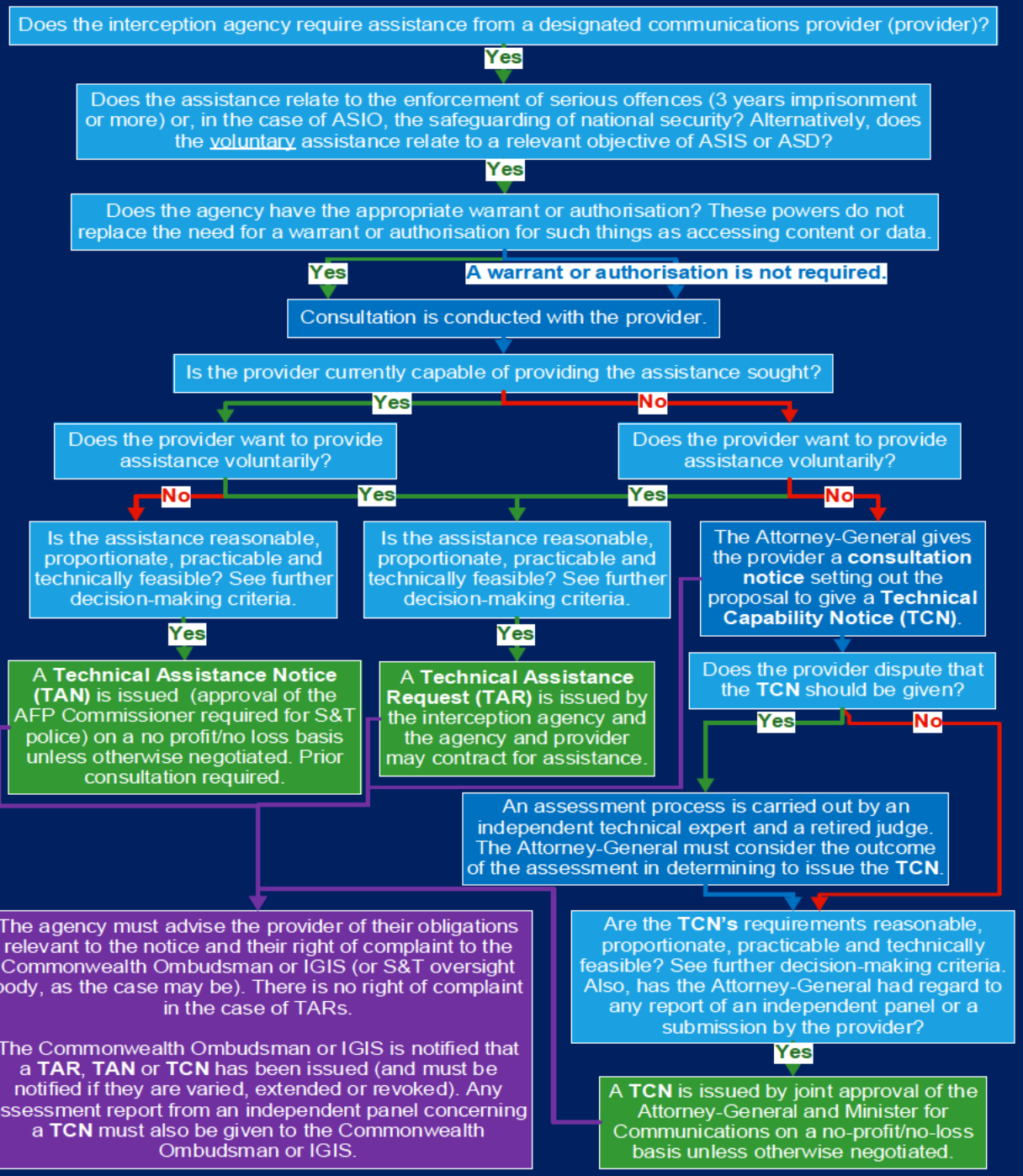
- New Part 15 of the *Telecommunications Act 1997*

- Three new powers
  - **Technical Assistance Requests (TAR)** allow agencies to request voluntary assistance from providers and attaches civil immunities to these requests
  - **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

Australian Government

Department of Home Affairs

FOI Document #2



Who does it apply to?

Item	Section 317C – Types of Designated Communications Provider	Examples
1	the person is a carrier or carriage service provider	Telstra; NBN Co; TPG; Optus; Vodafone; Macquarie Telecom
2	the person is a carriage service intermediary	Dodo or datacentres that provider a connection for a fee to an ISP (e.g. Equinix)
3	the person supplies a service that facilitates the supply of a carriage service	Softel – a UK based systems integrator/ managers service provider. Their offering includes customised software development.
4	the person provides an electronic service	Microsoft, Google, Facebook; WhatsApp
5	the person supplies a service that facilitates the provision of an electronic service	Amazon Web Services or other Content Delivery Network – they host content (e.g. Facebook videos) on proxy servers, closer to the end user, to increase effective download speeds.
6	the person develops, supplies or updates software used, or for use, in connection with a carriage service or an electronic service	Google; Microsoft; Nokia; Cisco; Virtual Private Network developers; add-on developers
7	the person manufacturers, supplies, installs, maintains or operates a facility	Macquarie Telecom or other Data centres (e.g. Equinix), companies who supply cables and wires for the telecommunications network
8	the person manufactures or supplies components for use in the manufacture of a facility	Cisco or systems integrators like DimensionData
9	the person connects a facility to a telecommunications network	Undersea cable operators like PIPE Pacific Cable. Providers of multiple cloud serve offerings like Megaport
10	the person manufactures or supplies customer equipment	Microsoft, Google, Apple; Samsung and other device manufacturers
11	the person manufactures or supplies components for use in the manufacture of customer equipment	Broadcom – they manufacture semiconductors for use in wireless and broadband applications
12	the person installs or maintains customer equipment and does so otherwise than in a capacity of the end-user of the equipment	Apple Store
13	the person connects customer equipment to a telecommunications network and does so otherwise than in the capacity of the end-user of the equipment	McDonalds; Westfield or other free wifi providers
14	the person is a constitutional corporation who manufacturers, supplies, installs or maintains data processing devices	Dell; Cisco; IBM
15	the person is a constitutional corporation who develops, supplies or updates software that is capable of being installed on a computer, or other equipment that is, or is to be, connected to a telecommunications network.	Adobe; any Australian retailer who offers a mobile phone application for online shopping or offers an application for mobile viewing

How does it apply to a DCP ?

- Can only be issued in relation to the **eligible activities** of a provider (see **317C**)
- **Eligible activities** = the communications-related functions of the provider
  - i.e. a carrier's eligible activities = the operation by the person of telecommunications networks or facilitates in Australia.
  - Facebook's eligible activities = the provision by Facebook of it's electronic service to end-users

- There must be a **jurisdiction nexus** to Australia.
  - i.e. the relevant activities go to the provision or use of services and devices in Australia or relevant activities within Australia.

Who can authorise the use of the powers?

- For a **TCN** – The Commonwealth Attorney – General
- For a **TAN** and **TAR** – Your agency head or a senior delegate

4	Police Force of a State or the Northern Territory	(a) an Assistant Commissioner of the Police Force or a person holding equivalent rank; or (b) a Superintendent of the Police Force or a person holding equivalent rank

Approval by the AFP Commissioner

- Applies to any **TAN** sought by State and Territory Police
- Recommendation of the Parliamentary Joint Committee on Intelligence and Security

317LA Approval of technical assistance notices given by the chief officer of an interception agency of a State or Territory

(1) The chief officer of an interception agency of a State or Territory must not give a technical assistance notice to a designated communications provider unless:

(a) the chief officer has given the AFP Commissioner a written notice setting out a proposal to give the technical assistance notice; and

(b) the AFP Commissioner has approved the giving of the technical assistance notice.

(2) An approval under paragraph (1)(b) may be given:

(a) orally; or

(b) in writing.

(3) If an approval under paragraph (1)(b) is given orally, the AFP Commissioner must:

(a) make a written record of the approval; and

(b) do so within 48 hours after the approval was given.

(4) For the purposes of this section, ***AFP Commissioner*** means the Commissioner (within the meaning of the *Australian Federal Police Act 1979*).

Contact: s. 47E(d)

What can you request or compel?

- Relevant purpose – enforcement of criminal law as it relates to **serious Australian or foreign offences**
  - = offence attracting three years imprisonment or more
- May request assistance with '**listed acts or things**' in **317E,** including:
  - Providing technical information
  - Assisting in, or facilitating in, giving effect to a warrant or authorisation
  - Facilitating or assisting access to a mobile device, computer or electronic service

A key question....

- Can the DCP already provide this type of assistance? (**TAN/ TAR)**
- **OR** is the DCP currently not capable of giving the requisite assistance? (**TCN**)

Some examples….

- 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.
- 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.
- 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.
- 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.
- 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.

Reasonable, proportionate, practical and technically feasible

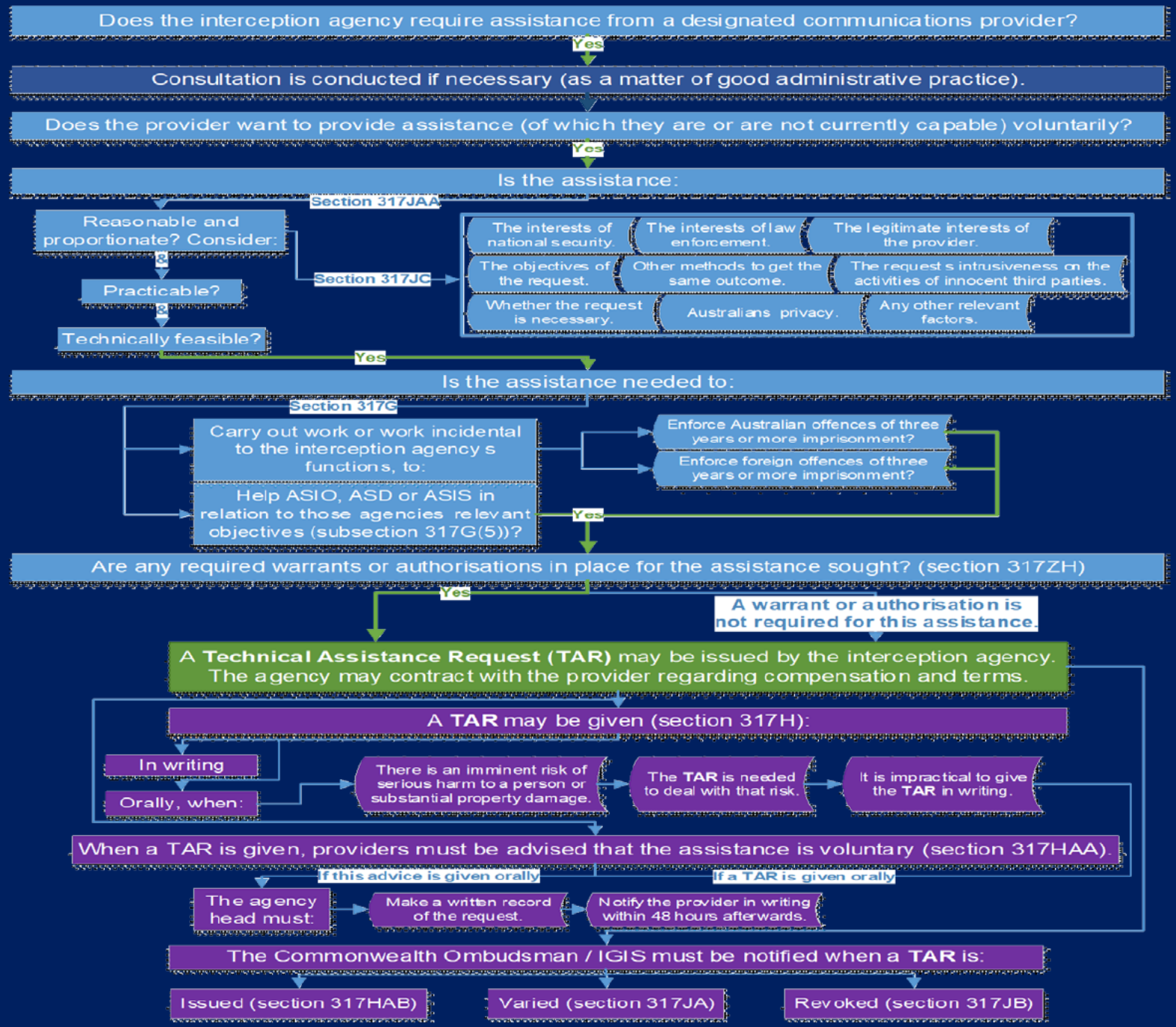
- This includes:
  - the interests of national security;
  - the interest of law enforcement;
  - the legitimate interests of the relevant provider;
  - the objectives of the request or notice;
  - the availability of other means to achieve these objectives;
  - whether the requirements are the least intrusive form of industry assistance insofar as it might impact innocent third parties;
  - whether the requirements are necessary;
  - the legitimate expectations of the Australian community relating to privacy and cybersecurity; and
  - such other matters the decision-maker considers relevant.

Australian Government

Department of Home Affairs

FOI Document #2

TARS

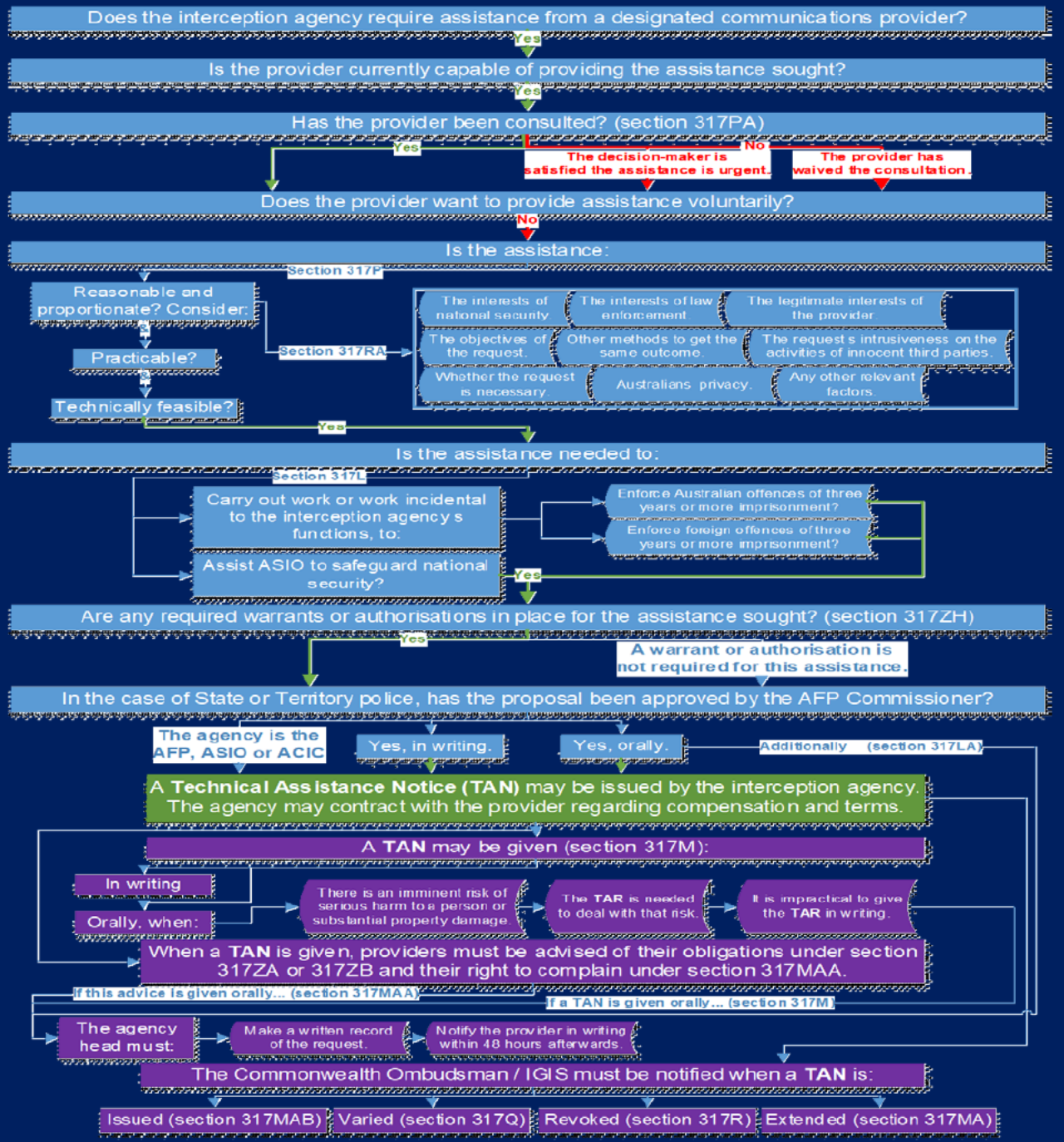


Australian Government

Department of Home Affairs

FOI Document #2

TANS

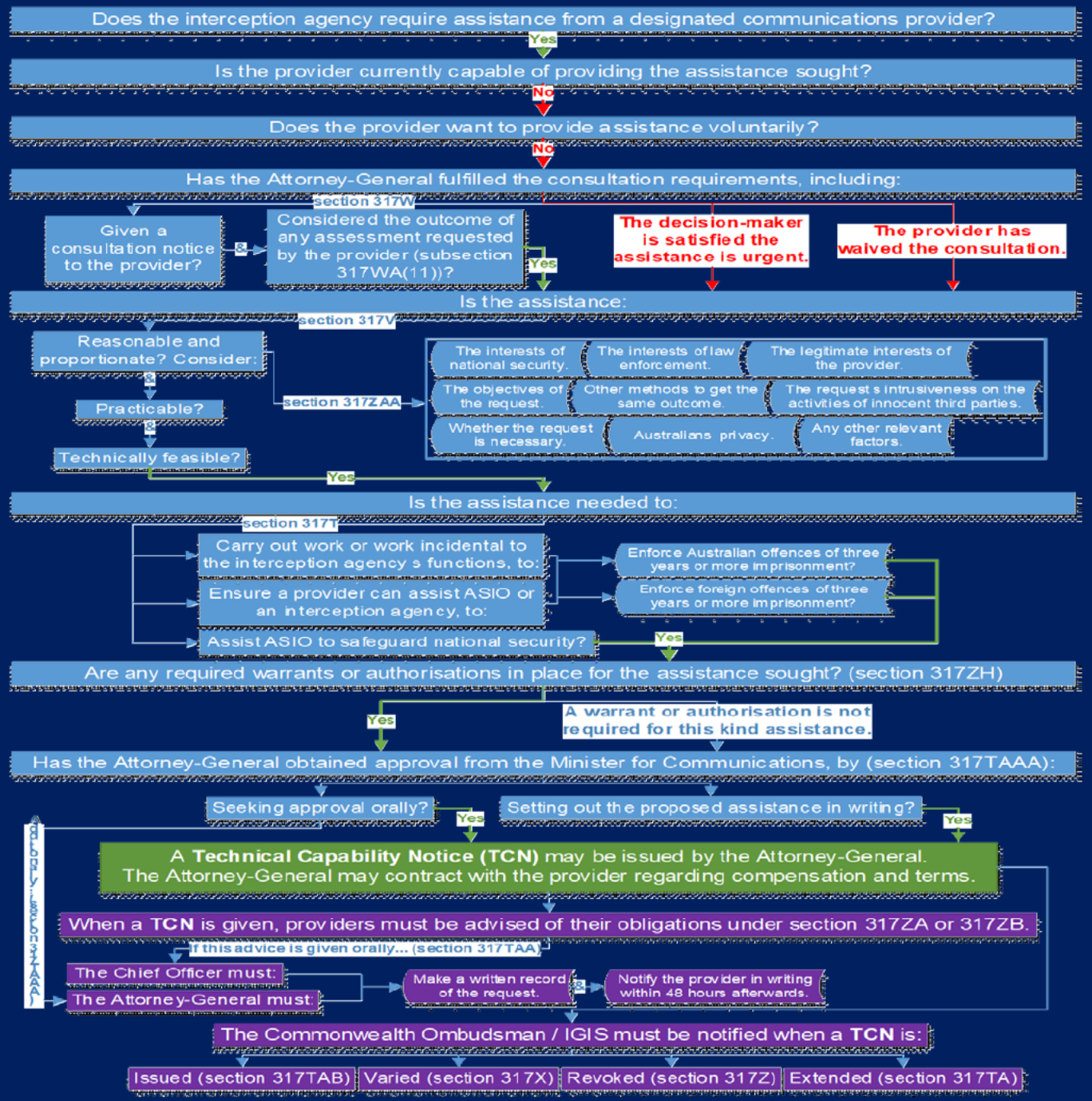


Australian Government

Department of Home Affairs

FOI Document #2

TCNS



No backdoors. Seriously.

317ZG

If you needed a warrant before, you will need a warrant now.

317ZH

Oversight

- **Commonwealth Ombudsman** with provisions to facilitate oversight by State and Territory inspection bodies
- Annual Reporting – numbers & offence types
- Oversight bodies have the authority to scrutinise report on the powers during regular TI & telecommunications data inspections

Costs & Terms

317ZK

- Default basis is **no-profit/no-loss**
- Opportunity to engage on commercial terms if needed
- If a strict public interest thresholds is met you may not compensate, or fully compensate, provider

....what about shared capabilities?

- Act is silent but flexible.
- Underlying conditions and processes can be set to determine costs and conditions of use by agencies across jurisdictions.

Enforcement

- Non-compliance is a civil penalty
  - Companies - $10 Million
  - Individuals (who are corporate entities) - $50,000
- Can also apply for injunctions, enforceable undertakings etc..
- Centralised - the **Communications Access Co-Ordinator** applies to the Federal Court
- Defence for conflict of laws

....what about foreign companies?

Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

- Cloud Act enacted for <u>two purposes</u>:
  - to remedy the jurisdictional issues identified in the US Supreme Court case United States v. Microsoft Corp (2018); and
  - to allow the US Executive to enter into bilateral, executive agreements for cross-border access to data by extending jurisdiction of domestic warrants across borders with willing bilateral partners.
- For the purposes of negotiating bilateral agreements with foreign governments, the CLOUD Act effectively has four separate categories of requirements and certifications, such as minimum standards concerning **human rights and rule of law (judicial authorisation of warrants)**.
- Purpose of access - *<u>preventing, detecting, investigating or prosecuting</u>* a 'Covered Offence' (Covered Offence means '*conduct that constitutes a Serious crime, including terrorist activity*', Serious Crime being defined as '*an offence punishable by a term of imprisonment of three years or more*').
- s. 33(a)(iii) [redacted]

Questions?

Contacts

s. 47E(d)

Home Affairs: cac@homeaffairs.gov.au