Australian Government

Department of Home Affairs

Assistance and Access Bill 2018

Explanatory Document

August 2018

Table of Contents

Glossary of terms

Abbreviation	Term
AAT	Administrative Appeals Tribunal
ABF	Australian Border Force
ACLEI	Australian Commission for Law Enforcement Integrity
ACIC	Australian Criminal Intelligence Commission
ACMA	Australian Communications and Media Authority
AFP	Australian Federal Police
AGO	Australian Geospatial-Intelligence Organisation
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979*
ASIS	Australian Secret Intelligence Service
Criminal Code	*Criminal Code Act 1995*
Crimes Act	*Crimes Act 1914*
Customs Act	*Customs Act 1901*
IGIS Act	*Inspector-General of Intelligence and Security Act 1986*
IS Act	*Intelligence Services Act 2001*
MACMA	*Mutual Assistance in Criminal Matters Act 1987*
Regulatory Powers Act	*Regulatory Powers (Standard Provisions) Act 2014*
SD Act	*Surveillance Devices Act 2004*
SES	Senior Executive Service
Telecommunications Act	*Telecommunications Act 1997*
TIA Act	*Telecommunications (Interception and Access) Act 1979*
Bill	Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Purpose of this explanatory document

This explanatory document accompanies the exposure draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill).

The Bill provides national security and law enforcement agencies with powers to respond to the challenges posed by the increasing use of encrypted communications and devices. The proposed changes are designed to help agencies access intelligible communications through a range of measures, including improved computer access warrants and enhanced obligations for industry to assist agencies in prescribed circumstances. This includes accessing communications at points where it is not encrypted. The safeguards and limitations in the Bill will ensure that communications providers cannot be compelled to build systemic weaknesses or vulnerabilities into their products that undermine the security of communications. Providers cannot be required to hand over telecommunications content and data.

The Government welcomes public comment on the exposure draft. Please submit any comments to AssistanceBill.Consultation@homeaffairs.gov.au by 10 September 2018.

Overview

Background to the Bill

The challenges posed by encryption

Encryption is a vital part of internet, computer and data security, supporting Australian economic growth and protecting consumer data. Encryption enables Australians to confidently engage in activities online such as banking, shopping, communications and other services. The Australian Government depends on encryption to secure Government and citizen information, critical infrastructure and computer networks.

While the use of computers and smartphones is not new, encryption is increasingly enabled on devices and applications by default. More than 93 per cent of Google's services and data are encrypted, as are more than 84 per cent of the web pages loaded via their Chrome browser. This is a great outcome for cyber security. However, encrypted devices and applications are eroding the ability of our law enforcement and security agencies to access the intelligible data necessary to conduct investigations and gather evidence. 95 per cent of the Australian Security Intelligence Organisation's (ASIO) most dangerous counter-terrorism targets actively use encrypted messages to conceal their communications.

In many instances encryption is incapable of being overcome, limiting possible avenues for agencies to gain important information. However, in some instances, law enforcement agencies may access data by employing specialist techniques to decrypt data, or access data at points where it is not encrypted. This can take considerable time. In order to do this more effectively, Australia's agencies need assistance from companies and individuals involved in the supply of communications services and devices in Australia. Globalisation and the advent of the internet have significantly increased the volume of communications that cross national borders and crucial services and products are increasingly being sourced from offshore providers. The purpose of the Bill is to allow agencies to seek help from providers, both domestic and offshore, in the execution of their functions. The Bill also provides agencies with alternative-collection powers, allowing them, under warrant, to access devices. The Bill explicitly provides that the new industry assistance powers cannot be used to compel communications providers to build weaknesses into their products. Cyber security will be ensured and privacy will be protected through robust safeguards in the Bill and the existing warrant regime for access to telecommunications content.

Government response

On 14 July 2017, the Prime Minister and the then Attorney-General announced the Government would legislate to address the challenges posed by encryption. The Minister for Law Enforcement and Cyber Security now has responsibility for taking forward the package of reforms and announced the Government's intention to consult on the proposals on 6 June 2018.

The Department of Home Affairs has drafted the legislation in close cooperation with agencies, including the Australian Criminal Intelligence Commission (ACIC), Australian Federal Police (AFP) and ASIO. Throughout the drafting process, the Government has consulted with a range of international and domestic technology companies about the proposed reforms.

What does the Bill do?

The Bill introduces a suite of measures that will improve the ability of agencies to access intelligible communications content and data. Three distinct reforms will help achieve this purpose:

1. Enhancing the obligations of domestic providers to give reasonable assistance to Australia's key law enforcement and security agencies and, for the first time, extending assistance obligations to offshore providers supplying communications services and devices in Australia.
2. Introducing new computer access warrants for law enforcement that will enable them to covertly obtain evidence directly from a device.
3. Strengthening the ability of law enforcement and security authorities to overtly access data through the existing search and seizure warrants.

Schedule 1 – A new framework for industry assistance

National security and law enforcement agencies already work cooperatively with industry and other partners on a range of matters. Under section 313 of the *Telecommunications Act 1997* (Telecommunications Act), domestic carriers and carriage service providers are required to provide 'such help as is reasonably necessary' to law enforcement and national security agencies.

Schedule 1 of the Bill will enhance industry-agency cooperation by introducing a new framework for industry assistance, to operate alongside section 313. The Bill introduces new powers for agencies to secure assistance from the full range of companies in the communications supply chain both within and outside Australia. In consultation with industry, national security and law enforcement agencies and the Attorney-General will be able to specify what assistance or capability is required.

Specifically, the Bill inserts a new Part 15 into the Telecommunications Act. This Part will:

- Provide a legal basis on which a 'designated communications provider' can provide *voluntary assistance* under a **technical assistance request** to assist ASIO, the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD) and interception agencies in the performance of their functions relating to Australia's national interests, the safeguarding of national security and the enforcement of the law.
- Allow the Director-General of Security, or the head of an interception agency, to issue a **technical assistance notice** requiring a designated communications provider to give assistance they are *already capable of providing* that is reasonable, proportionate, practicable and technically feasible. This will give agencies the flexibility to seek decryption in appropriate circumstances where providers have existing means to decrypt. This may be the case where a provider holds the encryption key to communications themselves (i.e. where communications are not end-to-end encrypted).
- Allow the Attorney-General to issue a **technical capability notice**, requiring a designated communications provider to *build a new capability* that will enable them to give assistance as specified in the legislation to ASIO and interception agencies. A technical capability notice cannot require a provider to build or implement a capability to remove electronic protection, such as encryption. The Attorney-General must be satisfied that any requirements are reasonable, proportionate, practicable and technically feasible. The Attorney-General must also consult with the affected provider prior to issuing a notice, and may also determine procedures and arrangements relating to requests for technical capability notices.

Designated communications providers include foreign and domestic communications providers, device manufacturers, component manufacturers, application providers, and traditional carriers and carriage service providers. The measures of the Bill apply to the functions of a designated communications provider in so far as their services or products have a nexus to Australia.

Interception agencies are agencies with interception powers under the TIA Act: the Australian Federal Police, the Australian Commission for Law Enforcement Integrity, the Australian Criminal Intelligence Commission, state and territory police agencies and anti-corruption commissions.

The type of assistance that may be requested or required under the above powers include (amongst other things):

- Removing a form of electronic protection applied by the provider, if the provider has an existing capability to remove this protection.
- Providing technical information like the design specifications of a device or the characteristics of a service.
- Installing, maintaining, testing or using software or equipment given to a provider by an agency.
- Formatting information obtained under a warrant.
- Facilitating access to devices or services.
- Helping agencies test or develop their own systems and capabilities.
- Notifying agencies of major changes to their systems, productions or services that are relevant to the effective execution of a warrant or authorisation.
- Modifying or substituting a target service.
- Concealing the fact that agencies have undertaken a covert operation.

Assistance is expected to be provided on a **no-profit, no-loss** basis and **immunities** from civil liability are available for help given. The Bill maintains the default position that providers assisting Government should not absorb the cost of that assistance nor be subject to civil suit for things done in accordance with requests from Government.

The new industry assistance framework is designed to incentivise cooperation from industry, providing a regime for the Australian Government and providers to work together to safeguard the public interest and protect national security. However, in the unlikely event that **enforcement** action is required, the Commonwealth can apply for enforcement remedies, like civil penalties, injunctions or enforceable undertakings. Enforcement of notices for carriers and carriage service providers will continue to be regulated by the Telecommunications Act.

What are the limitations and safeguards?

The new industry assistance framework has several important limitations and robust safeguards to protect the privacy of Australians, maintain the security of digital systems and ensure agency powers are utilised only where necessary for core law enforcement and security functions.

Reasonable, proportionate, practicable and technically feasible. In every case, the decision-maker must be satisfied that requirements in a technical assistance notice and technical capability notice are reasonable and proportionate and compliance with the notice is practicable and technically feasible. This means the decision-maker must evaluate the individual circumstances of each notice. In deciding whether a notice is reasonable and proportionate it is necessary for the decision-maker to consider both the interests of the agency and the interests of the provider. This includes the objectives of the agency, the availability of other means to reach those objectives, the likely benefits to an investigation and the likely business impact on the

provider. The decision-maker must also consider wider public interests, such as any impact on privacy, cyber security and innocent third parties. In deciding whether compliance with the notice is practicable and technically feasible, the decision-maker must consider the systems utilised by a provider and provider expertise.

Agencies still need an underlying warrant or authorisation. The new framework is designed to *facilitate* industry assistance – not serve as an independent channel to obtain private communications. Importantly, Schedule 1 does not change the existing mechanisms that agencies use to lawfully access telecommunications content and data for investigations (see process diagram on page 12). New technical assistance notices and technical capability notices cannot require that providers hand over telecommunications content and data without an underlying warrant or authorisation. Access to this material will still require a warrant or authorisation under the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The TIA Act has strict statutory thresholds that must be met. For example, a judge or Administrative Appeals Tribunal (AAT) member can only issue a warrant authorising the interception of communications where he or she is satisfied that the intercepted information would assist in the investigation of a serious offence (generally offences punishable by at least 7 years – see section 5D of the TIA Act). The judge or AAT member must have regard to the nature and extent of interference with the person's privacy, the gravity of the conduct constituting the offence, the extent to which information gathered under the warrant would be likely to assist an investigation, and other available methods of investigation. The TIA Act also has prohibitions on communicating, using and making records of communications.

Systemic weaknesses or vulnerabilities cannot be implemented or built into products or services. The Bill expressly prohibits technical assistance notices or technical capability notices from requiring a provider to build or implement a systemic weakness or systemic vulnerability into a form of electronic protection. This includes systemic weaknesses that would render methods of authentication or encryption less effective. The Australian Government has no interest in undermining systems that protect the fundamental security of communications. The new powers will have no effect to the extent that requirements would reasonably make electronic services, devices or software vulnerable to interference by malicious actors. Importantly, a technical capability notice cannot require a provider to build a capability to remove electronic protection and puts beyond doubt that these notices cannot require the construction of decryption capabilities.

Notices must be revoked if requirements cease to be reasonable. 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. Accordingly, notices that have become obsolete or excessively burdensome must be discontinued. These same notices may be varied to account for changing commercial and operational circumstances.

Agencies cannot prevent providers from fixing existing systemic weaknesses. Notices cannot prevent a provider from fixing a security flaw in their products and services that may be being exploited by law enforcement and security agencies. Providers can, and should, continue to update their products to ensure customers enjoy the most secure services available.

Core interception and data retention will not be extended. The powers cannot be used to impose data retention capability or interception capability obligations. These will remain subject to existing legislative arrangements in the TIA Act.

Assistance that may be requested is defined. The types of things a provider may be required to do under a technical assistance notice is listed in the Bill. While this list is not exhaustive, as it relates to technical assistance notices, anything specified in these notices must be consistent with the matters specified in the legislation. In the case of technical capability notices, new capabilities can only be developed to ensure that a provider is capable of giving help as specified (exhaustively) in the Bill.

The scope of agency notices is limited to core functions. 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 and laws imposing pecuniary penalties, or

- assisting the enforcement of the criminal laws in force in a foreign country, or
- protecting the public revenue, or
- safeguarding national security.

This will ensure that the scope of the powers is consistent with the purposes for which agencies currently seek assistance from domestic carriers and carriage service providers under section 313 of the Telecommunications Act.

Industry must be consulted about new capabilities. Before a provider is required to comply with a technical capability notice, the Attorney-General must allow the provider 28 days to give feedback about the requirements. If the provider gives feedback, the Attorney-General must consider it. This consultation requirement can only be waived in limited and emergency circumstances, or with the consent of the relevant provider. This is likely to only occur where there is a risk of imminent harm to the public, or if it is likely that material evidence will be lost without the assistance of a provider.

Information is protected. Unauthorised disclosure of information about, or obtained under, a notice or request is an offence. This will ensure any assistance is provided on a confidential basis and information, including commercially sensitive information, is only shared as necessary for the effective discharge of powers under the Bill or the administration of the Part. The maximum penalty for the offence is 5 years imprisonment, which is equivalent to the penalty for unauthorised disclosure of information by entrusted persons in section 35P of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act).

How are the powers oversighted?

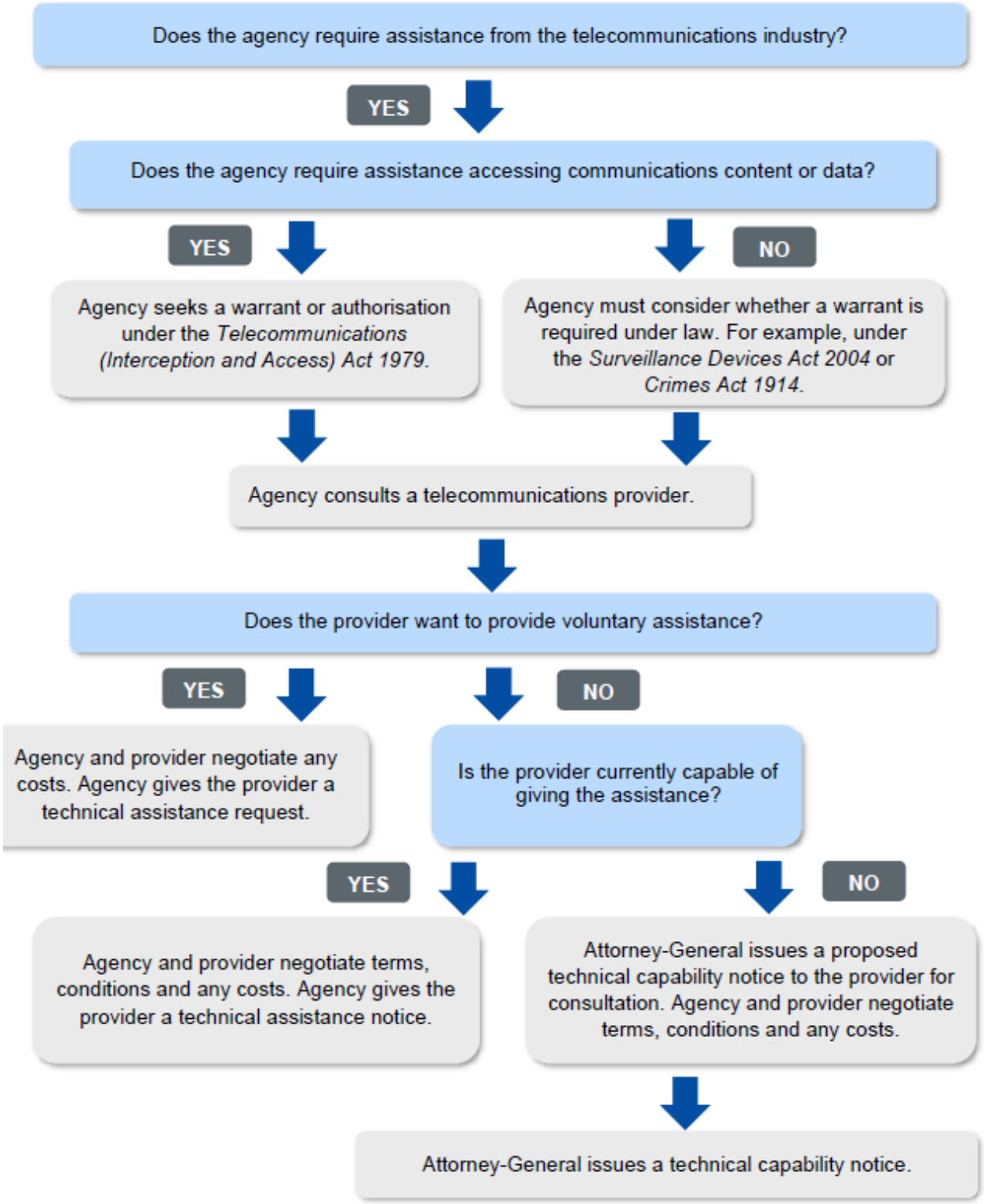
Powers reserved to senior decision-makers. The power to issue technical capability notices is reserved for the Attorney-General. Similarly, requirements under technical assistance notices can only be set by the head of ASIO or an interception agency, or a senior official in their organisation delegated by them. This ensures that these powers are restricted to the highest levels of Government and, in the case of technical capability notices, directly subject to Ministerial oversight. The people who occupy these positions are trusted to exercise suitable judgment about the propriety of requests and well equipped to consider the reasonableness and proportionality of any requirements.

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 that were given in that year. Reports will be included in the annual report under Chapter 4 of the TIA Act which discloses information on the use of telecommunications data by law enforcement agencies.

Inherent review by the courts. Australian courts will retain their inherent powers of judicial review of a decision of an agency head or the Attorney-General to issue a notice. This ensures that affected persons have an avenue to challenge a decision so that the court can determine whether the decision was lawfully made.

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 appointed by the Australian Communications Media Authority or the Attorney-General will determine terms and conditions.

Industry Assistance Process



Schedule 2 – New computer access warrants in the Surveillance Devices Act 2004

Agencies need to use other powers and techniques to access information at points where it is not encrypted. Schedules 2 to 5 address capability gaps and strengthen agencies' alternative-collection capabilities.

Schedule 2 of the Bill provides an additional power for Commonwealth, State and Territory law enforcement agencies to apply, in certain circumstances, for computer access warrants under the *Surveillance Devices Act 2004*, similar to those available to ASIO in section 25A of the ASIO Act. An eligible judge or AAT member must approve the warrant and authorise the activities that can be done under the warrant.

A computer access warrant will enable law enforcement officers to search electronic devices and access content on those devices. These warrants are distinct from surveillance device warrants, which enable agencies to use software to monitor inputs and outputs from computers and other devices.

The things that may be specified in a warrant include:

- entering premises for the purposes of executing the warrant
- using the target computer, a telecommunications facility, electronic equipment or data storage device in order to access data to determine whether it is relevant and covered by the warrant
- adding, copying, deleting or altering data if necessary to access the data to determine whether it is relevant and covered by the warrant
- using any other computer if necessary to access the data (and adding, copying, deleting or altering data on that computer if necessary)
- removing a computer from premises for the purposes of executing the warrant
- copying data which has been obtained that is relevant and covered by the warrant
- intercepting a communication in order to execute the warrant
- any other thing reasonably incidental to the above things.

A computer access warrant will also authorise the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to a computer under a computer access warrant. Concealment activities may occur at any time while the warrant is in force, or within 28 days after it ceases to be in force, or at the earliest time after this period at which it is reasonably practicable to do so.

Where a computer access warrant is in place, a law enforcement officer may apply to a judge or AAT member for an order requiring a person with knowledge of the device to provide reasonable and necessary assistance. This provision is similar to section 3LA of the Crimes Act, which allows a constable to apply to a magistrate for an order requiring a person to provide assistance where a search warrant is in place. This ensures that law enforcement agencies that have a warrant for computer access will be able to compel assistance in accessing devices.

What are the limitations and safeguards?

Thresholds for relevant offences. A law enforcement officer can only seek a warrant for relevant offences if the officer has reasonable grounds to suspect that: a relevant offence has been or will be committed, an investigation is or will be underway, and access to data is necessary to obtain evidence of the offence or information about the offenders. This is the same threshold that applies to surveillance device warrants.

Relevant offence is defined in section 6 of the SD Act to include (amongst others): an offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of 3 years or more or for life, or an offence against a law of a State that has a federal aspect and that is punishable by a maximum term of imprisonment of 3 years of more or for life.

Warrants issued by judges and AAT members. Computer access warrants are issued by judges and AAT members. In deciding whether to issue a warrant, he or she must be satisfied of the grounds of the application. The judge or AAT member must also have regard to the nature and gravity of the alleged offence, the likely evidentiary or intelligence value of any evidence that might be obtained, any previous warrant sought, the extent to which the privacy of any person is likely to be affected and the existence of any alternative means of obtaining the evidence or information.

The things that may be done are limited. A computer access warrant must specify the things that are authorised under the warrant. The things that may be specified are listed in the legislation. The judge or AAT member must consider whether each thing specified is appropriate in the circumstances.

Interference is not authorised. A computer access warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to the limitation is where the actions are necessary to execute the warrant.

No material loss or damage. A computer access warrant does not authorise the material loss or damage to other persons lawfully using a computer, except where necessary for concealment.

Warrants must be revoked if no longer required. The chief officer of the law enforcement agency to which the computer access warrant was issued must revoke the warrant if it is no longer required to obtain evidence of the offence. The chief officer also has an obligation to ensure that access to data is discontinued.

Information is protected. Unauthorised disclosure of information about, or obtained under, a computer access warrant is an offence. The maximum penalty for the offence is 2 years imprisonment or 10 years if the disclosure endangers the health or safety of any person or prejudices an investigation into an offence.

Using intercept material will require an interception warrant. The use, recording and communication of information obtained in the course of intercepting a communication in order to execute a computer access warrant is restricted. Where agencies want to gain intercept material for its own purpose, they must apply for, and be issued with, an interception warrant under Chapter 2 of the TIA Act.

How are the powers oversighted?

Reports to the Minister. The chief officer of a law enforcement agency must report to the Minister on every computer access warrant issued. The report must state whether the warrant or authorisation was executed, the name of the person primarily responsible for the execution, the name of each person involved in accessing data, the name of any person whose data was accessed, and the location at which the computer was located. The report must also give details of the benefit to the investigation.

Reports to the public. Agencies must report annually on the number of warrants applied for and issued during the year and the number of emergency authorisations.

Record keeping requirements. Agencies must keep records about computer access warrants, including in relation to decisions to grant, refuse, withdraw or revoke warrants. Agencies must also keep records of how the information in the warrant has been communicated.

Ombudsman inspections. The Ombudsman must inspect the records of law enforcement agencies to determine compliance with the law and report the results to the Minister ever six months. The Minister must table Ombudsman reports in the Parliament.

Schedule 2 – Amendments to computer access warrants in the ASIO Act

Schedule 2 also amends the computer access provisions in the ASIO Act to address particular operational challenges. The Bill will:

- enable ASIO to intercept communications for the purpose of executing a computer access warrant, removing the need to obtain a second warrant for that purpose
- permit ASIO to temporarily remove a computer or thing from a premises, for the purpose of executing a warrant, and to return that computer or thing, and
- enable ASIO to take steps to conceal its access to a computer following the expiry of the warrant, to address situations where ASIO no longer has access to the computer at the time the warrant expires.

The use, recording and communication of information obtained in the course of intercepting communications in order to execute a computer access warrant is restricted. This is to ensure that where ASIO seeks to gain intercept material for its own purpose, the Director-General of Security must apply for, and be issued with, an interception warrant under Chapter 2 of the TIA Act.

Schedule 3 – Enhanced search warrants in the Crimes Act 1914

Schedule 3 of the Bill will amend the search warrant framework under the Crimes Act to enhance the ability of criminal law enforcement agencies to collect evidence from electronic devices under warrant.

Computer access

Currently, the Crimes Act allows overt search warrants to be issued for the purpose of searching computers. The Bill will allow law enforcement agencies to collect evidence from electronic devices under an overt warrant remotely. Law enforcement agencies will be able to execute a warrant without having to be physically on the premises.

A new definition of 'account-based data' will be inserted to ensure that accessing a computer under warrant enables law enforcement officers to access information associated with an online account, like an email service or Facebook account.

The amendments will also extend the timeframes allowed for the examination of electronic devices moved under a warrant from 14 days to 30 days in order to account for the complexity of analysing data in modern electronic communications systems.

Independent approval is required. Warrants require the approval of an independent issuing officer employed by the court.

Thresholds apply. The issuing officer must be satisfied that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, evidential material on the premises or person.

The warrant is limited. The warrant must be executed within seven days after it is issued.

Details of the warrant must be given to the subject. The person executing the warrant must make details of the warrant available to the occupier of the premises or person.

Interference is not authorised. A warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to the limitation is where the actions are necessary to execute the warrant.

No material loss or damage. Material loss or damage to other persons lawfully using a computer is prohibited.

Assistance orders

Under the current section 3LA of the Crimes Act, law enforcement agencies can apply to a magistrate for an order to compel certain persons (including owners and users of a device) to assist in providing access to data held in a device. Currently, the device must be on warrant premises, moved for processing or seized for evidence. The Bill will amend section 3LA so that these orders also apply to person-based warrants under the Crimes Act. This will mean law enforcement will have the power to compel people to, for example, provide assistance to unlock a phone found in the course of an ordinary search of a person, or a frisk search of a person, authorised by a warrant under section 3E of the Crimes Act.

There must be reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device.

The Bill increases the penalties for not complying with orders requiring assistance where either a person-based or premises-based warrant is in force. The penalty in the Crimes Act will increase from a maximum of two years imprisonment to a maximum five years imprisonment for a 'simple offence' and up to ten years

imprisonment for a new aggravated offence where the order is related to an investigation into a serious crime. The current penalty is of insufficient gravity to incentivise compliance with the assistance obligation.

Independent approval is required. These amendments will not change the current arrangements whereby law enforcement officers must apply to a magistrate for an order for assistance to access a device. An underlying person-based or premises-based search warrant issued by an independent issuing officer must also be in place.

Schedule 4 – Enhanced search warrants in the Customs Act 1901

Computer Access

Schedule 4 of the Bill will amend the search warrant framework under the Customs Act to enhance the ability of the ABF to collect evidence from electronic devices under warrant. The amendments will provide the ABF with a new power to request a search warrant to be issued in respect of a person for the purpose of seizing a computer or data storage device.

The amendments will also extend the timeframes for the examination of electronic devices moved under a warrant from 72 hours to 30 days in order to account for the complexity of analysing data in modern electronic communications systems.

Independent approval is required. Warrants require the approval of judicial officer.

Thresholds apply. The judicial officer must be satisfied that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, evidential material on the premises or person.

The warrant is limited. The warrant must be executed within seven days after it is issued.

Details of the warrant must be given to the subject. The person executing the warrant must make details of the warrant available to the occupier of the premises or person.

Interference is not authorised. A warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to the limitation is where the actions are necessary to execute the warrant.

No material loss or damage. Material loss or damage to other persons lawfully using a computer is prohibited.

Assistance Orders

The Bill also increases the penalties for not complying with orders requiring assistance in accessing the electronic devices where a warrant is in force. Penalties for not complying with an order will increase to a maximum six months imprisonment for a simple offence and up to 10 years imprisonment for an aggravated offence where there is non-compliance with an order related to an investigation into a serious crime. There must be reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device. The current penalty is of insufficient gravity to incentivise compliance with the assistance obligation.

There must be reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device.

Independent approval is required. These amendments will not change the current arrangements whereby ABF employees must apply to a magistrate for an order for access. A warrant issued by a judicial officer remains the underlying authority for searching the computer on a premises or person.

Schedule 5 – ASIO assistance powers

Schedule 5 provides that, subject to certain limitations, a person or body is not subject to civil liability where they:

- voluntarily provide assistance to ASIO in accordance with a request made by the Director-General, or
- give information or produce a document to ASIO unsolicited (i.e. without a request) if the person or body reasonably believes that it is likely to assist ASIO in the performance of its functions.

Schedule 5 also enables ASIO to require a person with knowledge of a computer or a computer system to provide assistance that is reasonable and necessary to ASIO in order to gain access to data on a device that is subject to an ASIO warrant. This amendment is an extension of the amendments in Schedules 3 and 4 which increase the penalties for not complying with orders requiring assistance in accessing electronic devices under the Crimes Act and Customs Act respectively.

Ministerial approval is required. The Director-General must apply to the Attorney-General for any order requiring a person to assist ASIO with access to a computer. The Attorney-General must be satisfied of the reasonable grounds for the order and of the fact that access will substantially assist ASIO's collection of intelligence important to the security of Australia.

Schedule 1

Amendments to the Telecommunications Act 1997

Division 1—Introduction

New Part 15 of the Telecommunications Act is divided into seven Divisions. Division 1 provides an outline of Part 15 and defines a number of key terms.

317A Simplified outline of this Part

Section 317A briefly describes the frameworks for technical assistance requests, technical assistance notices and technical capability notices.

317B Definitions

The following terms are defined:

access is defined as including access subject to a pre-condition (such as the use of a password), access by way of push technology and access by way of standing request. Push technology involves access that is not initiated by an end-user (pull technology).

ASIO affiliate has the same meaning as in section 4 of the ASIO Act. The definition captures persons performing functions or services for ASIO, but it does not include the Director-General or an ASIO employee.

ASIO employee has the same meaning as in section 4 of the ASIO Act. The definition captures persons employed by the Director-General for the performance of ASIO's functions and the exercise of ASIO's powers.

chief officer of an interception agency has the meaning given by section 317ZM. This is further elaborated below.

contracted service provider in relation to a designated communications provider is defined as persons who perform services for or on behalf of a provider. It does not include employees of the provider.

Corruption and Crime Commission (WA) means the Corruption and Crime Commission established by the *Corruption, Crime and Misconduct Act 2003* (WA).

designated communications provider is defined under section 317C. This definition is further elaborated upon below.

electronic service is defined under section 317D. This definition is further elaborated upon below.

eligible activities of a designated communications provider is provided for in section 317C. This definition is further elaborated upon below.

entrusted ASD person is defined as a person who:

- is a staff member of ASD; or
- has entered into a contract, agreement or arrangement with ASD; or
- is an employee or agent of a person who has entered into a contract, agreement or arrangement with ASD.

entrusted ASIO person has the same meaning as in section 4 of the ASIO Act. This means:

- an ASIO employee; or
- an ASIO affiliate; or
- a person who has entered into a contract, agreement or arrangement with ASIO.

entrusted ASIS person means a person who:

- is a staff member or agent of ASIS; or
- has entered into a contract, agreement or arrangement with ASIS; or
- is an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIS.

giving help is defined in relation to the agencies that are able to receive help by way of a technical assistance request, technical assistance notice or technical capability notice. When used in relation to ASIO, 'giving help' includes giving help to an ASIO affiliate or ASIO employee: that is, someone performing functions or services for ASIO under the ASIO Act; or someone employed by the Director-General under the ASIO Act. When used in relation to ASIS, 'giving help' includes giving help to a staff member of ASIS. When used in relation to ASD, 'giving help' includes giving help to a staff member of ASD. When used in relation to an interception agency, 'giving help' includes giving help to an officer of the agency.

IGIS official has the same meaning as in section 4 of the ASIO Act. The definition captures the Inspector-General of Intelligence and Security (the IGIS) and members of staff employed by the Inspector-General to perform functions and exercise powers under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act).

Independent Broad-based Anti-corruption Commission of Victoria is defined as the Independent Broad-based Anti-corruption Commission established by the *Independent Broad-based Anti-corruption Commission Act 2011* (Vic).

Independent Commissioner Against Corruption (SA) means the person appointed Commissioner under section 8 of the Inde*pendent Commissioner Against Corruption Act 2012 (SA*).

interception agency is defined as any of the below:

- the Australian Federal Police; or
- the Australian Commission for Law Enforcement Integrity; or
- the Australian Criminal Intelligence Commission; or
- the Police Force of a State or the Northern Territory; or
- the Independent Commission Against Corruption of New South Wales; or
- the New South Wales Crime Commission; or
- the Law Enforcement Conduct Commission of New South Wales; or
- the Independent Broad-based Anti-corruption Commission of Victoria; or
- the Crime and Corruption Commission of Queensland; or
- the Independent Commissioner Against Corruption (SA); or
- the Corruption and Crime Commission (WA).

These are the same agencies which have powers to intercept communications under a warrant issued by a judge or AAT member pursuant to the TIA Act.

Law Enforcement Conduct Commission of New South Wales means the Law Enforcement Conduct Commission constituted by the *Law Enforcement Conduct Commission Act 2016 (NSW).*

listed act or thing is provided for in section 317E. This definition is further elaborated upon below.

material is defined broadly to include material whether in the form of text, data, speech, music, other sounds or visual images (moving or otherwise). It also includes material in any other form or any combination of forms.

member of the staff of the Independent Commissioner Against Corruption (SA) means a person who is engaged under subsection 12(1) of the *Independent Commissioner Against Corruption Act 2012* (SA).

officer, when used in relation to an interception agency, has the same meaning given by section 317ZM.

staff member, when used in relation to ASIS or ASD has the same meaning as in the *Intelligence Services Act 2001* (IS Act). Section 3 of the IS Act states that staff member in relation to an agency is a member of the staff of the agency (including employees, consultants or contractors or seconded persons from other Commonwealth or State authorities).

supply, when used in relation to a facility, customer equipment or a component, is defined as including the supply (and re-supply) by way of sale, exchange, lease, hire or hire-purchase. Supply, when used in relation to software, includes provide, grant or confer rights, privileges or benefits.

technical assistance notice means a notice given under section 317L. This concept is further elaborated upon below.

technical assistance notice information is defined broadly to include information about any of the following:

- the giving of a technical assistance notice; or
- the existence or non-existence of a technical assistance notice; or
- the variation of a technical assistance notice; or
- the revocation of a technical assistance notice; or
- the requirements imposed by a technical assistance notice; or
- any act or thing done in compliance with a technical assistance notice.

It also includes any other information about a technical assistance notice.

technical assistance request means a request under paragraph 317G(1)(a). This concept is further elaborated upon below.

technical assistance request information is defined broadly to include information about any of the following:

- the existence or non-existence of a technical assistance request; or
- the giving of a technical assistance request; or
- the acts or things covered by a technical assistance request; or
- any act or thing done in accordance with a technical assistance request.

It also includes any other information about a technical assistance request.

technical capability notice means a notice given under section 317T. This concept is further elaborated upon below.

technical capability notice information is defined broadly to include information about any of the following:

- the giving of a technical capability notice; or
- consultation relating to the giving of a technical capability notice; or
- the existence or non-existence of a technical capability notice; or
- the variation of a technical capability notice; or
- the revocation of a technical capability notice; or
- the requirements imposed by a technical capability notice; or

- any act or thing done in compliance with a technical capability notice

It also includes any other information about a technical capability notice.

317C Designated communications provider etc.

Designated communications providers can be given technical assistance requests, technical assistance notices and technical capability notices under the Bill. Designated communications providers are defined in the table in section 317C to include the full range of participants in the global communications supply chain, from carriers to over-the-top messaging service providers. This reflects the multi-layered nature of the communications environment and the types of entities that could meaningfully assist law enforcement and national security agencies.

The categories of designated communications providers are drafted to ensure a connection to Australia. This geographical nexus enables Australian agencies to request assistance from offshore entities that have, or are likely to have, a key role in the provision of communications and related services in Australia while limiting the power to Australia's jurisdictional limits. Section 317C captures instances where a product or service is manufactured with default settings and shipped globally - that is, it is not exclusively or specifically intended for use in Australia - but is likely to be used in Australia.

Individuals, as well as body corporates, may be designated communications providers. A person may fit into one or multiple categories listed in the table in section 317C.

The ***eligible activities*** of a designated communications provider are activities to which technical assistance requests, technical assistance notices and technical capability notices must relate.

Item 1 of the table lists carriers or carriage service providers. Carriers and carriage service providers are defined in the Telecommunications Act. A carrier is an entity that owns a telecommunications network unit that supplies carriage services to the public. Carriage service providers use a telecommunications network unit to supply carriage services to the public. Carriage services include services for carrying communications. For example, telephone services, internet access service and VoIP services. As owners or operators of telecommunications network units used to supply carriage services, carriers must hold a licence issued by the ACMA.

Item 2 of the table lists carriage service intermediaries. Carriage service intermediaries are defined in the Telecommunications Act. Carriage service intermediaries are legal persons who arrange for the supply of carriage services by a carriage service provider to a third party.

Item 3 of the table lists persons that provide a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service. This provision is designed to ensure that other persons that have a significant role in the supply of carriage services and the passage of communications through carriage services can be asked or required to provide assistance.

Item 4 of the table lists persons that provide an electronic service that has one or more end-users in Australia. 'Electronic service' is defined in section 317D and means a service that allows end-users to access material using a carriage service, or a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service. For the purposes of item 4 a person must provide the electronic service to one or more end-users in Australia.

Item 5 of the table lists persons that provide a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia. This provision is designed to ensure that other persons that have a significant role in the provision of electronic services may be asked or required to provide assistance to Australian authorities.

Item 6 of the table lists persons that develop, supply or update software used, for use, or likely to be used, in connection with a listed carriage service or an electronic service that has one or more end-users in Australia. This category would include, for example, persons involved in designing trust infrastructure used in encrypted communications or software utilised in secure messaging applications.

Item 7 of the table lists persons that manufacture, supply, install, maintain or operate a facility. Facility is defined in the Telecommunications Act and means any part of the infrastructure of a telecommunications network or any line, equipment, apparatus, tower, mast, antenna, tunnel, duct, hole, pit, pole or other structure or thing used, or for use, in or in connection with a telecommunications network.

Item 8 of the table lists persons that manufacture or supply components for use, or likely to be used, in the manufacture of a facility for use, or likely to be used, in Australia. Equipment in the telecommunications network can be highly technical and comprised of multiple components.

Item 9 of the table lists persons that connect a facility to a telecommunications network in Australia. Examples may include mesh networks, private networks and entities involved in the provision of undersea cables.

Item 10 of the table lists persons that manufacture or supply customer equipment for use, or likely use, in Australia. Customer equipment is defined in section 21 of the Telecommunications Act and includes any equipment, apparatus, structure, thing or system that is used or ready for use or intended for use on the customer side of the boundary of a telecommunications network. Section 22 of that same Act establishes the boundary of a telecommunications network. The persons in item 10 include suppliers and manufacturers of mobile devices, modems and computing devices typically connected to the telecommunications network.

Item 11 of the table lists persons that manufacture, supply components for use, or likely use, in the manufacturer of customer equipment for use, or likely use, in Australia. This includes persons who manufacture circuit boards, subscriber identification modules (SIMs) or memory units of a mobile device.

Item 12 of the table lists persons that install or maintain customer equipment in Australia in a capacity other than that of an end-user of the equipment. This includes technical experts or contractors installing or maintaining customer equipment provided by a manufacturer, supplier or retailer, such as managed service providers. Persons with ongoing maintenance obligations, or persons acting at the point of installation, are able to provide essential assistance in the course of an investigation.

Item 13 of the table lists persons who connect customer equipment to a telecommunications network in Australia in a capacity other than that of an end-user of the equipment. This includes systems integrators.

Item 14 of the table lists constitutional corporations that manufacturer, supply, install or maintain data processing devices for use, or likely use, in Australia. Data processing device is defined in section 7 of the Telecommunications Act and means any article or material from which information is capable of being reproduced, with or without the aid of any other article or device. A data processing device may not necessarily be connected, or designed to be connected, to the telecommunications network. Item 14 includes persons who maintain data storage centres or manufacturer discrete storage devices.

Item 15 of the table lists constitutional corporations that develop, supply or update software that is capable of being installed on a computer or other equipment that is, or is likely to be, connected to a telecommunications network in Australia. This includes persons who develop application software or system software (including operating systems) that may be installed on a computer in Australia such as personal computers or mobile devices.

317D Electronic service

Under section 317C (Items 4 and 5), a person who provides an ***electronic service***, or a service that facilitates, or is ancillary or incidental to, the provision of an electronic service, is a designated communications provider.

Section 317D defines electronic service to mean a service that allows end-users to access material (see definition in section 317B) using a carriage service, or a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service. The definition is designed to be capable of capturing a range of existing and future technologies, including hardware and software. Examples of electronic services may include websites and chat fora,

secure messaging applications, hosting services including cloud and web hosting, peer-to-peer sharing platforms and email distribution lists, and others.

The definition does not extend to a broadcasting service or datacasting service (within the meaning of the *Broadcasting Services Act 1992*).

A person does not provide an electronic service merely because the person supplies a carriage service that enables material to be accessed or delivered or because the person provides a billing service, or a fee collection service, in relation to an electronic service. Suppliers of carriage services are excluded from the definition of electronic service because they are listed separately as designated communications providers in 317C.

317E Listed acts or things

Technical assistance requests and technical assistance notices may contain the listed acts or things in section 317E(1) but additional forms of assistance of a similar kind may also be specified in the technical assistance request or technical assistance notice. In contrast, technical capability notices must be directed towards ensuring a provider can give the types of assistance set out in section 317E(1) – with the exception of 317E(1)(a) which does not apply to technical capability notices. That is, 317E(1)(b) – (j) is exhaustive with respect to technical capability notices and non-exhaustive with respect to technical assistance requests and technical assistance notices. Additional types of capabilities may only be developed if set out in a legislative instrument determined by the Minister in accordance with subsection 317T(5).

The different application of 317E identifies the distinction between circumstances where a provider is already capable of giving assistance and circumstances where a provider might be required to build a capability so that they become capable of giving assistance. The powers in Part 15 are intended to be exercised flexibly to request or compel forms of assistance that a provider is already capable of giving, so long as it is of a similar kind or nature as the things specified in 317E. However, in cases where a provider is required to build a capability that goes beyond its own needs, the matters for which this capability can be built are limited in the legislation and subject to ongoing Parliamentary scrutiny.

317E(1)(a) provides removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider, as an act or thing that may be specified. Although agencies may specify removing electronic protection in a technical assistance request and technical assistance notice, agencies may not require providers to build a capability to remove electronic protection under a technical capability notice (see 317T(4)(c)(i)).

Removing one or more forms of electronic protection is intended to include decrypting encrypted communications. Requirements to decrypt or remove electronic protection under this subsection cannot oblige a provider to furnish the content or metadata of private communications to authorities. Consistent with the restrictions in section 317ZH, agencies must access communications content and data through established warrants and authorisations under the TIA Act. However, if the content or data obtained under such a warrant is encrypted, the Director-General of ASIO or the chief officer of an interception agency could issue a technical assistance notice under section 317L requiring a provider to assist with decryption where the provider is capable of doing so.

317E(1)(b) provides giving technical information as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. Technical information could include information about the design, manufacture, creation or operation of a service, the characteristics of a device, or matters relevant to the sending, transmission, receipt, storage or intelligibility of a communication. Examples include source code, network or service design plans, and the details of third party providers contributing to the delivery of a communications service, the configuration settings of network equipment and encryption schemes. It could also include providing demonstrations of technologies. Technical information does not include telecommunications data such as subscriber details or the source, destination or duration of a communication for which an authorisation under the TIA Act would be required.

Obligations to provide technical information apply regardless of whether the information is subject to intellectual property rights or contractual arrangements. Immunity from civil liability for any acts or things done in accordance (or in good faith purportedly in accordance) with a technical assistance request, technical assistance notice and technical capability notice will be available to persons that provide assistance.

Consistent with the decision-making criteria for technical assistance notices in section 317P and technical capability notices in section 317V, the decision-maker must evaluate the individual circumstances surrounding each notice in order to determine whether the provision of particular technical information is reasonable and proportionate. Some kinds of technical information are more sensitive than others, such as source code. It is incumbent on the decision-maker to consider whether it is appropriate to specify source code, having regard to the commercial interests of the provider and whether other technical information, or other kinds of assistance, could achieve a similar law enforcement or national security objective.

317E(1)(c) provides installing, maintaining, testing or using software or equipment as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. Assistance of a kind contemplated by 317E(1)(c) includes installing, maintain, testing or using software or equipment given to a provider by, or on behalf, of an agency. The deployment of agency procured or developed software or equipment within an existing network owned or operated by a provider can achieve law enforcement objectives without requiring providers to develop technology secondary to their core business.

Requirements to install software are subject to the global protections in the Bill against building or implementing a systemic weakness in a form of electronic protection in 317ZG. Accordingly, a provider could not be required to install or utilise any agency software or equipment that weakens security across non-target devices or services.

317E(1)(d) provides ensuring information obtained in connection with the execution of a warrant or authorisation is given in a particular format as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. Assistance of this kind includes reformatting data, providing information to authorities consistent with prescribed templates, ensuring information can be delivered in an appropriate and efficient manner and other obligations relating to the intelligibility of material obtained through a warrant or authorisation. **317E(1)(e)** lists facilitating or assisting access to the following things that are the subject of the eligible activities of a provider as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice:

- a facility
- customer equipment
- a data processing device
- a listed carriage service
- a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service
- an electronic service
- a service that facilitates, or is ancillary or incidental to, the provision of an electronic service
- software used, for use, or likely to be used, in connection with a listed carriage service
- software used, for use, or likely to be used, in connection with an electronic service, and
- software that is capable of being installed on a computer, or other equipment, that is, or is likely to be connected to a telecommunications network.

Access includes physical or online access. The terms ‘facility’, ‘customer equipment’, ‘data processing device’ and ‘listed carriage service’ are defined in the Telecommunications Act. ‘Electronic service’ is defined in section 317D. Access to the things listed above can assist agencies where they have developed a

technical solution but require help from providers to implement it or where providers are able to modify their systems (without creating a systemic weakness) to assist the execution of a warrant or authorisation to access information held on the above things.

Agencies cannot ask a provider to put their staff at risk when facilitating assistance of this kind 317E(1)(e). It is not reasonable or proportionate to require civilians to undertake hazardous activities in the context of a law enforcement or security agency investigation.

317E(1)(f) provides assisting with the testing, modification, development or maintenance of a technology or capability as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. Assistance consistent with this paragraph includes help testing, modifying, developing or maintaining the internal systems and capabilities of law enforcement and security agencies. Providers can ensure that agency systems are compatible with the networks, services or devices they manufacture, supply and operate. When expert providers and agencies collaborate to deploy agency capabilities the chances of efficient and effective deployment significantly increase.

Assistance of this kind is particularly helpful to agencies seeking to install or maintain equipment on a provider's network consistent with paragraph 317E(1)(c).

317E(1)(g) provides notifying particular kinds of changes to, or developments affecting, eligible activities of the provider, if the changes are relevant to the execution of a warrant or authorisation, as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. The changes that may be notified may include offering new or improved services or products, outsourcing arrangements, offshoring equipment or services, changes to services, procuring new equipment or changes to the management of services.

This item is limited to changes that may impact a particular warrant or authorisation. It is not uncommon for a particular application or service to receive multiple daily updates. Given the frequency of change and the commercial sensitivity of some updates, this item is limited to instances where the change would affect a warrant or authorisation on foot. By way of example, an agency may seek notification of changes to a specific service that a target is using in the context of a specific investigation. Notification of these changes will allow the agency to take steps to mitigate its impact on the investigation before it occurs.

317E(1)(h) provides modifying, or facilitating the modification of, any of the characteristics of a service provided by the provider as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. By way of example, modification of a service could include blocking the delivery of a specific service to a target.

317E(1)(i) provides substituting, or facilitating the substitution of, a service provided by the provider for additional services as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice.

As with assistance under 317E(1)(e), agencies cannot ask a provider to put their staff at risk. It is not reasonable or proportionate to require civilians to undertake hazardous activities in the context of a law enforcement or security agency investigation.

317E(1)(j) provides doing an act or thing 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 as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. In the course of an investigation, law enforcement and security agencies often need to exercise covert powers to gain evidence and intelligence about the activities of targets. The disclosure of these activities can jeopardise an investigation and prejudice the interests of law enforcement and security agencies. Assistance of a kind described in paragraph 317E(J) includes doing acts or things to ensure that a target does not become aware they are the subject of an investigation, minimising the risk that the investigation becomes compromised or that sensitive agency capabilities are revealed. A request or notice can only seek assistance of this kind if it is connected to a valid function or power conferred by law that relates to the legitimate purposes of enforcing the criminal law and laws imposing pecuniary penalties, assisting enforcement of the criminal laws in force in a foreign country, protecting the public revenue or if the

purpose is in the interests of Australia's national security, foreign relations or economic well-being. This ensures any activity a provider is asked to conceal is legitimate and consistent with the proper conduct of an agency.

Subsection 317E(2) ensures that providers cannot be asked to make false or misleading statements or engage in dishonest conduct for the purposes of 317E(1)(j). Providers have obligations to their customers as well as Government. Subsection 317E(2) confirms that providers cannot be asked to actively deceive a person for the purposes of concealing lawful agency activities.

317F Extension to external Territories

Division 1 extends to every external Territory of Australia.

Division 2—Voluntary technical assistance

Division 2 sets out the framework for the heads of ASIO, ASIS, ASD and interception agencies to request voluntary technical assistance from designated communications providers. A request from voluntary technical assistance is known as a technical assistance request. Immunity from civil liability for any acts or things done in accordance with a technical assistance request will be available to persons that provide assistance in accordance with this Division. Agency heads may enter into contractual agreements with providers relating to the provision of assistance.

317G Voluntary technical assistance provided to ASIO, ASIS, ASD or an interception agency

Section 317G allows the Director-General of Security, the Director-General of ASIS, the Director-General of ASD or the chief officer of an interception agency to give a voluntary technical assistance request to a provider to do things that are in connection with the eligible activities of the provider. This means that assistance under this framework is limited to the technical functions of a provider set out in the table in section 317C.

A technical assistance request can ask a provider do a thing currently within their capacity or request that they build a new capability to assist agencies. Both forms of assistance are entirely voluntary in nature and must be consistent with the powers and functions of the requesting agency.

The persons who can make technical assistance requests occupy the most senior position in their organisation and can exercise suitable judgment about the propriety of a request, and the relevant terms of any contract. Sections 317ZN, 317ZP, 317ZQ and 317ZR allow agency heads to delegate these powers to senior officials in their organisations who are also equipped to make these judgments.

Providers have immunity from civil liability for things done in accordance, or in good faith purportedly in accordance, with a voluntary technical assistance request. For example, if a provider is asked to give details of the development of a new service or technology, they will not be liable for any breach of intellectual property rights. The provision of civil immunity is similar to protections under subsection 313(5) of the Telecommunication Act for carriers and carriage service providers that do things in order to meet their obligations under that section to provide reasonably necessary help to law enforcement and national security agencies. It is full immunity for civil actions brought under Commonwealth law.

The things requested of a provider must be for the purpose of helping the relevant agency perform functions or powers conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to a ‘relevant object’, this being:

- enforcing the criminal law and law imposing pecuniary penalties; or
- assisting the enforcement of the criminal laws in force in a foreign country; or
- protecting the public revenue; 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.

This is consistent with the purposes for which agencies currently seek assistance from domestic carriers and carriage service providers under section 313 of the Telecommunications Act.

The things may also include matters that facilitate, or are ancillary or incidental to, an agency’s performance of a function or exercise of a power where the function or power relates to the above purposes. This will allow things necessary for the smooth execution of a request to be specified.

The things that may be specified in a technical assistance request include, but are not limited to, the listed acts or things set out in section 317E. Other types of assistance may be specified in a technical assistance request provided that the assistance is of the same kind, class or nature as those listed.

Terms

The below terms are not defined in the Bill but are intended to be interpreted in the following manner.

The term '*conferred by or under a law'* means that the function or power may be conferred by legislation or a legislative instrument made under a power delegated by the Parliament. For example, the function or power may be conferred by a regulation made under an Act of Parliament.

The meaning of '*enforcing the criminal law'* includes the process of investigating crime and prosecuting criminals. It also 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.

The reference to '*pecuniary penalties*' relates to penalties for breaches of Commonwealth, State and Territory laws that are not prosecuted criminally or that impose a penalty which serves as an administrative alternative to prosecution (often referred to as civil or administrative penalty provisions). Pecuniary penalties for the purposes of this provision do not encompass small-scale administrative fines. In Commonwealth, State and Territory legislation there are significant pecuniary penalties for serious breaches of the law, particularly laws regarding corporate misconduct.

The concept of '*public revenue*' includes State and Territory revenue in addition to Commonwealth revenue. Lawful obligations charged on a regular basis such as taxes, levies, rates and royalties are also included but occasional charges, such as fines, are not. '*Protecting the public revenue*' also includes the activities of agencies and bodies undertaken to ensure that those lawful obligations are met; for example routine collection, audits, investigatory and debt recovery actions.

The term '*revenue*' is not limited to incoming monies from taxation but could also extend to 'monies which belong to the Crown, or monies to which the Crown has a right, or monies which are due to the Crown'.[1] The term 'protection of public revenue' is intended to extend to protecting the revenue from which compensation or similar payments are paid, including circumstances where it is sought to ensure that wrongful payments are not made out of that revenue. The term does not include activities aimed at identifying and eliminating inefficient but lawful spending of public monies.

The inclusion of '*assisting the enforcement of the criminal laws in a foreign country*' ensures that technical assistance requests can be made in support of Australia's international obligations, such as those under Council of Europe Convention on Cybercrime. For example, requests may be made to facilitate the disclosure of stored communications to foreign law enforcement agencies, where the disclosure is also supported by a stored communications warrant under the TIA Act.

The reference to Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being reflects the functions of Australia's intelligence and security agencies as set out in the IS Act and the ASIO Act. It is intended to support voluntary technical assistance requests made by Australia's intelligence and security agencies. It is not intended to support voluntary assistance requests made by interception agencies.

317H Form of technical assistance request

A technical assistance request must be given in writing, although oral issue is permissible in urgent circumstances. If issued orally, a written record is must be made within 48 hours of the request and then, as soon as practicable, a copy must be given to the provider.

317HA Duration of technical assistance request

A technical assistance request comes into force when given or when specified in the request. Requests only remain in force until the expiry date specified in the request, or in cases where no expiry date was specified, at the end of 90 days after issue.

[1] Stephens v Abrahams (1902) 27 VLR 753 at 767; see also Lush v Coles (1967) 2 All ER 585 at 588.

317J Specified period etc.

A technical assistance request may include a request that a specified act or thing be done in a specified period of time, or specified manner, or in a way that meets one or more specified conditions.

This section reflects the distinction between the specific acts or things that may be asked of a provider in accordance with 317G and the manner in which those things should be executed. For example, a law enforcement agency may request that a provider remove security controls from a particular device consistent with 317E(a) and, additionally, request that these controls be removed in a short timeframe to assist with an urgent operation.

317JA Variation of technical assistance requests

The issuer of a technical assistance request must make variations to the request in writing. Oral variation is permissible in urgent circumstances but must be followed by a written copy.

Any acts or things specified in a varied technical assistance request must be connected to the eligible activities of a provider and connected to helping the agency perform a function or exercise a power conferred by law, so far as the function or power relates to:

- enforcing the criminal law and law imposing pecuniary penalties; or
- assisting the enforcement of the criminal laws in force in a foreign country; or
- protecting the public revenue; 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.

The things that may be specified in a varied technical assistance notice include, but are not limited to, the listed acts of things in new section 317E.

317JB Revocation of technical assistance requests

The issuer of a technical assistance request may revoke the request. Revocation must be in writing to the person to whom the request was given.

317K Contract etc.

Section 317K provides authority for the relevant agency head to enter into arrangements with a provider in relation to acts or things done by the provider in accordance with a technical assistance request. This section provides a statutory basis for Commonwealth, State and Territory agencies to enter into contracts, including contracts of a financial nature, for the purposes of Division 2.

Division 3—Technical assistance notices

Division 3 sets out the framework for the Director-General of Security, or the chief officer of an interception agency, to give a designated communications provider a technical assistance notice requiring them to do specified acts or things where they are capable of doing so. A provider issued with a notice is obliged to comply with the requirements set out in the notice.

317L Technical assistance notices

Section 317L allows the Director-General of Security, or the chief officer of an interception agency, to give a provider a technical assistance notice requiring the provider to do things for the purpose of helping the relevant agency perform functions or powers conferred by or under 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
- protecting the public revenue; or
- safeguarding national security.

This is consistent with the purposes for which agencies currently seek assistance from domestic carriers and carriage service providers under section 313 of the Telecommunications Act.

The specified acts or things may also go to matters that facilitate, or are ancillary or incidental to, the agency's performance of a function or exercise of a power where the function or power relates to these purposes. This will allow things necessary for the smooth execution of a notice to be set as requirements.

All of the things specified in the notice must be connected to the eligible activities of the provider. This has the effect of limiting the assistance required by a notice to the technical functions of a provider set out in section 317C.

The things may include, but are not limited to, the listed acts or things set out in section 317E. Other types of assistance may be specified in a technical assistance notice provided that the assistance is of the same kind, class or nature as those listed. That assistance must also be connected to the eligible activities of the provider and related to the agencies functions.

The power to issue technical assistance notices is reserved for agency heads in the first instance. Persons occupying these senior positions are able to exercise judgement about the reasonableness of requiring a provider to comply with the acts or things specified in a notice. Sections 317ZN and 317ZR allow agency heads to delegate these powers to senior officials in their organisations who are also equipped to make these judgements.

317M Form of technical assistance notice

A technical assistance notice must be given in writing, although oral issue is permissible in urgent circumstances. If issued orally, a written record is must be made within 48 hours of issue and then, as soon as practicable, a copy must be given to the provider.

317MA Duration of technical assistance notice

A technical assistance notice comes into force when given or when specified in the notice. Notices only remain in force until the expiry date specified in the notice, or in cases where no expiry date was specified, at the end of 90 days after issue.

317N Compliance period etc.

A technical assistance notice may require a specified act or thing be done in a specified period of time, or specified manner, or in a way that meets one or more specified conditions.

This section reflects the distinction between the specific acts or things that may be required from a provider in accordance with 317L and the manner in which those things should be executed. For example, a law enforcement agency may request that a provider remove security controls from a particular device consistent with 317E(1)(a) and, additionally, request that these controls be removed in a short timeframe to assist with an urgent operation.

317P Decision-making criteria

Before giving a technical assistance notice, the Director-General of Security, or the chief officer of an interception agency, must be satisfied that the requirements imposed by the notice are reasonable and proportionate, and compliance with the notice is practicable and technically feasible.

Satisfaction for the purposes of this section is a subjective state of mind of the administrative decision-maker. It is a precondition to the exercise of the power. To meet the requisite state of satisfaction the decision-maker must consider the reasonableness and proportionality of the requirements imposed by the notice and the practicability and technical feasibility of compliance with that notice. The decision-maker's satisfaction must be formed on a correct understanding of the law.[2] The decision-maker must not take into account a consideration which a court can determine in retrospect 'to be definitely extraneous to any objects the legislature could have had in view.'[3]

This means the decision-maker must evaluate the individual circumstances of each notice. In deciding whether a notice is reasonable and proportionate, it is necessary for the decision-maker to consider both the interests of the agency and the interests of the provider. This includes the objectives of the agency, the availability of other means to reach those objectives, the likely benefits to an investigation and the likely business impact on the provider. It is important that the provider is the most appropriate person to provide the assistance sought by the agency. For example, a notice given to a provider who, while able to assist, did not control the relevant data and was not in a position to help as adequately as a more directly related provider would not be proportionate. In that instance it would need to be clear that the controller of the data was unable or unwilling to assist.

The decision-maker must also consider wider public interests, such as any impact on privacy, cyber security and innocent third parties. In deciding whether compliance with the notice is practicable and technically feasible, the decision-maker must consider the systems utilised by a provider and provider expertise.. To be satisfied, the decision-maker would need to consider material information given to the agency by the provider. It is expected that the agency would be engaged in a dialogue with the provider prior to issuing a notice. The decision-maker may also make inquiries with other persons who have relevant experience and technical knowledge.

317Q Variation of technical assistance notices

The Director-General of Security, or the chief officer of an interception agency, may make variations to a technical assistance notice given to a provider. Variations must be made in writing. Oral variation is permissible in urgent circumstances but must be followed by a written copy.

Any acts or things specified in a varied technical assistance notice must be connected to the eligible activities of a provider and connected to helping the agency perform a function or exercise a power conferred by law, so far as the function or power relates to:

- enforcing the criminal law and law imposing pecuniary penalties; or

[2] *Minister for Immigration and Multicultural Affairs v Eshetu* (1999) 197 CLR 611 at 651-654.
[3] *Water Conservation and Irrigation Commission (NSW) v Browning* (1947) 74 CLR 492 at 505.

- assisting the enforcement of the criminal laws in force in a foreign country; or
- protecting the public revenue; or
- safeguarding national security.

The things that may be specified in a varied technical assistance notice include, but are not limited to, the listed acts of things in new section 317E.

The Director-General of Security, or the chief officer of an interception agency, must not vary a notice unless satisfied that the requirements imposed are reasonable and proportionate and compliance with the varied notice is practicable and technically feasible.

These provisions ensure that the power to vary a notice is exercised consistently with the power to issue a notice and any varied requirements are within the bounds of what might have been required of a technical assistance notice at first instance.

317R Revocation of technical assistance notices

The Director-General of Security, or the chief officer of an interception agency, may revoke a technical assistance notice. Revocation must be in writing to the person to whom the notice was given.

The Director-General of Security, or the chief officer of an interception agency, must revoke a technical assistance notice if satisfied that the acts or things specified in the notice are not reasonable and proportionate or that compliance with the notice is not practicable and technically feasible. Changing business requirements, developments in technology or shifts in the operational priorities of agencies may render the acts or things specified in a notice inconsistent with these statutory requirements. The revocation provision establishes an avenue to discontinue notices that have become obsolete or excessively burdensome.

Division 4—Technical capability notices

Division 4 sets out the framework for the Attorney-General to give a designated communications provider a technical capability notice that is directed towards ensuring that the designated communications provider is capable of giving listed help to ASIO or an interception agency. However, a technical capability notice cannot be used to compel a provider to build a capability that would enable it to remove encryption, or any form of electronic protection, from products. The things specified in technical capability notices may require significant investment. The capabilities built under a technical capability notice may be utilised by multiple agencies. This is distinct from assistance required by a technical assistance notice under new section 317L which can oblige a provider to give help that they are already capable of providing to the requesting agency. However, if necessary, a technical capability notice can also require a provider to give help they are already capable of providing.

317S Attorney-General may determine procedures and arrangements relating to requests for technical capability notices

Section 317S enables the Attorney-General to determine procedures and arrangements relating to requests by Government agencies to the Attorney-General to issue a technical capability notice. A determination under this section is not a legislative instrument and failure to comply does not invalidate the technical capability notice.

Procedures may include administrative processes to centralise agency requests and protect sensitive information. The section explicitly provides that a determination may also require an agency to obtain the agreement of a third party before making a request. This will facilitate capability sharing between agencies and ensure existing capabilities are utilised before new capabilities are requested.

317T Technical capability notices

Section 317T allows the Attorney-General to give a provider a written technical capability notice requiring the provider to do things that are directed towards ensuring that the provider is capable of giving listed help to an agency in relation to the performance of a function or exercise of a power conferred by or under 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
- protecting the public revenue; or
- safeguarding national security.

This is consistent with the purposes for which agencies currently seek assistance from domestic carriers and carriage service providers under section 313 of the Telecommunications Act.

The power to issue technical capability notices is reserved for the Attorney-General. This ensures that the power to require a provider to build a capability, beyond that which it already has, is restricted to the highest levels of Government and directly subject to Ministerial oversight.

For administrative efficiency, a technical capability notice may also operate as a quasi-technical assistance notice. A technical capability notice can require a provider to do a thing it is already capable of doing. This means agencies will not need to seek two different notices, with different issuing persons, in order to require a provider to build a capability and then use that capability to give the agency help. It will also be possible for an agency to require a provider to provide immediate help while, or before, it builds a capability for the agency. It is appropriate for technical capability notices to have this dual function given that they have more stringent consultation and approval requirements than technical assistance notices.

Where a technical capability notice requires the provider to build a capability for the purpose of ensuring the provider can give listed help, 'listed help' means either:

- one or more of the listed acts or things in section 317E(1) (except for paragraph (a) of the list – for reasons explained below), or
- a thing the Minister determines by legislative instrument.

By contrast, technical assistance notices may contain the listed acts or things in section 317E, as well as additional forms of assistance of a similar kind. The different application of 317E for technical capability notices and technical assistance notices identifies the distinction between circumstances where a provider is already capable of giving assistance and circumstances where a provider might be required to build a capability so that they become capable of giving assistance. It is important that technical assistance notices can request forms of assistance that a provider is already capable of giving, so long as it is of a similar kind to the things specified in 317E. However, in cases where a provider is required to build a capability that goes beyond its own needs, the matters for which this capability can be built should be limited in the legislation and subject to ongoing Parliamentary scrutiny.

Before the Minister makes a determination under 317T(5) to add additional items to the things a capability can be made for, he or she must have regard to:

- the interests of law enforcement
- the interests of national security
- the objects of the Telecommunications Act
- the likely impact of the determination on designated communications providers, and
- any other relevant matter.

These considerations will ensure that any legislative instrument put before Parliament has been drafted with the needs of both Government, industry and the public in mind. To satisfy the conditions it is expected that the Minister will consult with industry before tabling an instrument.

A technical capability notice cannot require the provider to build a capability for the purpose of ensuring the provider can remove electronic protection (paragraph (a) of the listed acts or things in subsection 317E(1)). In other words, a technical capability notice cannot require the building of a decryption capability.

All things specified in the notice must be connected with the eligible activities of the provider. This has the effect of limiting the assistance required by a notice to the technical functions of a provider set out in section 317C.

A technical capability notice has no effect to the extent it requires a provider to ensure a telecommunications service or telecommunications system has interception or delivery capabilities. Delivery capability means the capability of a telecommunications service or system to enable lawfully intercepted information to be delivered to interception agencies. The TIA Act imposes on carriers and carriage service providers obligations to develop, install and maintain interception and delivery capabilities. Technical capability notices will not extend these obligations to additional categories of providers or qualify the nature of the existing obligations on carriers and carriage service providers.

Similarly, a technical capability notice has no effect to the extent it requires a provider to build and/or maintain a data retention capability. The retention of telecommunications data is also managed through the TIA Act.

The section specifically states that any expression used in the section has the same meaning as the TIA Act. This provides additional surety that technical capability notices cannot modify, or qualify in any way, legislated obligations on providers in relation to interception capabilities, delivery capabilities and data retention.

A technical capability notice must specify an '*applicable costs negotiator'* for the notice. This is the person who will settle the basis of compliance for the notice and the terms and conditions of any requirements in the notice. It is likely to be the head of the agency issuing the notice.

317TA Duration of technical capability notice

A technical capability notice comes into force when given or when specified in the notice. Notices only remain in force until the expiry date specified in the notice, or in cases where no expiry date was specified, at the end of 180 days after issue.

317U Compliance period etc.

A technical capability notice may require that a thing required in a notice be done in a specified period of time, specified manner, or way that meets a specified condition.

317V Decision-making criteria

Before giving a technical capability notice, the Attorney-General must be satisfied that the requirements imposed by the notice are reasonable and proportionate, and compliance with the notice is practicable and technically feasible. This criterion is exercised in the same manner as decisions made by the Director-General of Security or the chief officer of an interception agency, for issuing technical assistance notices.

The conditions of reasonableness, proportionality, practicality and technical feasibility will be harder to meet in the case of a technical capability notice. The simple fact that these notices require a provider to build something that goes beyond current business requirements will raise thresholds, particularly those of proportionality and reasonableness.

Satisfaction is a subjective state of mind of the administrative decision-maker. It is a precondition to the exercise of the power. To meet the requisite state of satisfaction the decision-maker must consider the reasonableness and proportionality of the requirements imposed by the notice and the practicability and technical feasibility of compliance with that notice. The decision-maker's satisfaction must be formed on a correct understanding of the law.[4] The decision-maker must not take into account a consideration which a court can determine in retrospect 'to be definitely extraneous to any objects the legislature could have had in view.'[5]

This means the Attorney-General must evaluate the individual circumstances of each notice. In deciding whether a notice is reasonable and proportionate, it is necessary for the Attorney-General to consider both the interests of the agency and the interests of the provider. This includes the objectives of the agency, the availability of other means to reach those objectives, the likely benefits to an investigation and the likely business impact on the provider. It is important that the provider is the most appropriate person to provide the assistance sought by the agency. For example, a notice given to a provider who, while able to assist, did not control the relevant data and was not in a position to help as adequately as a more directly related provider would not be proportionate. In that instance it would need to be clear that the controller of the data was unable or unwilling to assist.

The Attorney-General must also consider wider public interests, such as any impact on privacy, cyber security and innocent third parties. In deciding whether compliance with the notice is practicable and technically feasible, the Attorney-General must consider the systems utilised by a provider and provider expertise. To be satisfied, the Attorney-General would need to consider material information given to Government by the provider. It is expected that the relevant agency would be engaged in a dialogue with the provider prior to making a request to the Attorney-General. The Attorney-General may also make inquiries with other persons who have relevant experience and technical knowledge.

[4] *Minister for Immigration and Multicultural Affairs v Eshetu* (1999) 197 CLR 611 at 651-654.
[5] *Water Conservation and Irrigation Commission (NSW) v Browning* (1947) 74 CLR 492 at 505.

317W Consultation about a proposal to give a technical capability notice

The Attorney-General must undertake a consultation process before a provider is subject to a legal obligation to comply with a technical capability notice. The Attorney-General must give a provider a written notice setting out a proposal to give the notice and inviting that person to make a submission on the proposal.

The consultation period must run for at least 28 days. However, the Attorney-General may allow a provider more than 28 days to make representations. In practice, it is expected that consultation periods will be agreed between Government and industry, with discussions about the feasibility of a notice occurring prior to issue.

The consultation period may be shortened if the Attorney-General is satisfied of any of the following conditions:

- the notice should be given as a matter of urgency, or
- compliance with the consultation period is impracticable, or
- the provider waives the consultation requirement.

For example, a shorter timeframe may be required where a capability can be built to prevent imminent harm to the public or where there is a serious risk that material evidence will be lost without the assistance of a provider.

Consultation under section 317W does not restrict the Attorney-General from consulting with other persons. This could include other Ministers with an interest, such as the Minister for Communications and the Arts.

317X Variation of technical capability notices

The Attorney-General may make variations to a technical capability notice given to a provider. Variations must be made in writing. It may be necessary to vary the requirements of a notice to respond to developments in a providers services, the roll-out of new technology or a change in agency practices. Variation of a notice may also be required in response to shifts in operational priorities and emergency circumstances. Variation may be more efficient and effective than the issuing of a new technical capability notice.

Any acts or things specified in a varied technical assistance notice must be connected to the eligible activities of a provider and connected to helping the agency perform a function or exercise a power conferred by law, so far as the function or power relates to:

- enforcing the criminal law and law imposing pecuniary penalties; or
- assisting the enforcement of the criminal laws in force in a foreign country; or
- protecting the public revenue; or
- safeguarding national security.

The variation may be in relation to a capability required to be built under a technical capability notice or in relation to assistance (where the provider has an existing capability) required to be given under a technical capability notice.

Where the variation is in relation to a capability required to be built under a technical capability notice, the thing specified in the varied notice **must** be a listed act or thing in section 317E (other than the act of thing covered by paragraph 317E(1)(a)) or a thing the Minister determines by legislative instrument. Paragraph 317E(1)(a) lists removing electronic protection. This means that a varied technical capability notice cannot require the building of a decryption capability.

Where the variation is in relation to assistance the provider has the capability to provide, the thing specified in the varied notice **may** include, but is not limited to, a listed act or thing in section 317E.

The Attorney-General must not vary a notice unless satisfied that the requirements imposed are reasonable and proportionate and compliance with the varied notice is practicable and technically feasible.

These provisions ensure that the power to vary a notice is exercised consistently with the power to issue a notice and any varied requirements are within the bounds of what might have been required in a technical capability notice at first instance.

317Y Consultation about a proposal to vary a technical capability notice

The Attorney-General must consult with a provider before varying a technical capability notice. The consultation process is consistent with the process under 317W for the issuing of a notice. The Attorney-General must give a provider a written notice setting out a proposal to vary the notice and inviting that person to make a submission on the proposal.

The consultation period must run for at least 28 days. However, the Attorney-General may allow a provider more than 28 days to make representations.

The consultation period may be shortened if the Attorney-General is satisfied that the notice should be varied as a matter of urgency, compliance is impracticable or the provider waives the consultation requirement.

317Z Revocation of technical capability notices

The Attorney-General may revoke a technical capability notice. Revocation must be in writing to the person to whom the notice was given.

The Attorney-General must revoke a technical capability notice if satisfied that the acts or things specified in the notice are not reasonable and proportionate or that compliance with the notice is not practicable and technically feasible. Changing business requirements, developments in technology or shifts in the operational priorities of agencies may render the acts or things specified in a notice inconsistent with these statutory requirements. The revocation provision establishes an avenue to discontinue notices that have become obsolete or excessively burdensome.

Division 5—Compliance and enforcement

Division 5 establishes a framework for compliance with the requirements of a technical assistance notice or technical capability notice and sets out the enforcement remedies available to pursue compliance.

Separate regimes apply to carriers and carriage service providers and other categories of designated communications providers. Carriers and carriage service providers will continue to be regulated under the Telecommunications Act. Other enforcement options will apply to entities who are not subject to the regulatory measures in the Telecommunications Act.

The Communications Access Co-ordinator, a statutory body within the Department of Home Affairs, serves an administrative function and is the relevant applicant for the enforcement remedies available in this Division. The Co-ordinator may apply for civil penalties, enforceable undertakings and injunctions in the Federal Court or the Federal Circuit Court of Australia where a provider has not been compliant with their obligations under a technical assistance notice or technical capability notice.

The remedies available have been calculated to achieve the primary aim of deterrence and are proportionate to the seriousness of contravention. Non-compliance with technical assistance notices and technical capability notices may have significant consequences for law enforcement and national security.

Technical assistance notices and technical capability notices are not subject to merits review. As opposed to judicial review, which ensures that decisions were made within the legal limits of the relevant power, merits review aims to ensure the 'correct' decision is made. The merits review body remakes the decision. Excluding merits review in relation to decisions made under new Part 15 of the Act is consistent with most other decisions made for national security and law enforcement purposes – for example those made under the IS Act, ASIO Act, IGIS Act and the TIA Act. Decisions of a law enforcement nature were identified by the Administrative Review Council in its publication 'What decisions should be subject to merits review?' as being unsuitable for merits review.[6]

These new powers have in-built safeguards that are designed to ensure that the scope of the powers does not go beyond what is reasonable and necessary to assist agencies in the exercise of their functions and powers under law.

317ZA Compliance with notices—carriers and carriage service providers

Section 317ZA requires carriers and carriage service providers served with a technical assistance notice or technical capability notice to comply with that notice to the extent they are capable of doing so. Capable means that carriers and carriage service providers must have the resources, or the means to acquire the resources, for complying with a notice. This ensures that if extenuating circumstances prevent a carrier or provider from meeting the full requirements of a notice then they are only obliged to meet the requirements to the extent possible.

Contravention of this section attracts the pecuniary penalties in Part 31 of the Telecommunications Act. This means carriers and carriage service providers face the same penalties for not complying with technical assistance notices and technical capability notices, as other civil penalty provisions in the Telecommunications Act. For example, non-compliance with a notice carries the same civil penalties as a breach of a carrier licence held by the carrier. This is also consistent with the penalties associated with a carrier's failure to comply with the requirement to give reasonably necessary assistance under section 313 of the Telecommunications Act.

Persons are prohibited from aiding, abetting, inducing or conspiring to affect a contravention of subsection 317ZA(1).

[6] Administrative Review Council, *What decisions should be subject to merits review* (1999) 13.

317ZB Compliance with notices—designated communications provider (other than a carriage service provider)

317ZB requires designated communications providers (other than carriers and carriage service providers) served with a technical assistance notice or technical capability notice to comply with that notice to the extent they are capable of doing so. Capable means that providers must have the resources, or the means to acquire the resources, for complying with a notice

The civil penalty for non-compliance by body corporates is 47,619 penalty units (~ AUD $10 million) and the civil penalty for non-compliance by persons who are not body-corporates is 238 penalty units (~ AUD $50, 000). These penalties are equivalent with the penalties applicable to carriers and carriage service providers for breach of a carrier licence in Part 31 of the Telecommunications Act.

The penalty units are calculated to achieve deterrence and are set proportionally to the limits of seriousness of contravention. Failure to act in good faith with any requirements may jeopardise ongoing criminal investigations, result in the destruction of material evidence or, in extreme cases, expose the Australian public to serious and imminent harm.

Subsection 82(5) of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) does not apply to a contravention of section 317ZB. Subsection 82(5) of the Regulatory Powers Act provides that the pecuniary penalty for breach by a body corporate must not be more than five times the pecuniary penalty specified for breach by an individual. This measure is necessary to account for the broad array of entities that may be subject to technical assistance notices. It is appropriate for corporate entities to be subject to a higher upper penalty limit. However, a penalty one fifth of the maximum which corporate entities are subject to may be too high a penalty for individuals that may be subject to these powers.

Section 564 and section 572B of the Telecommunications Act do not apply to a contravention of this section. Section 564 provides that a court may grant injunctions in relation to contraventions of the Act and section 572B provides that a person may give an enforceable undertaking about compliance with the Act. These remedies have been provided for in sections 317ZC, 317ZD and 317ZE which implement Parts 4, 6 and 7 of the Regulatory Powers Act (civil penalty, enforceable undertaking and injunctions provisions, respectively).

317ZC Civil penalty provision

Section 317ZB is enforceable under Part 4 of the Regulatory Powers Act. This Part allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for contravention of an enforceable provision.

The Communications Access Co-ordinator may make an application to the Federal Court or Federal Circuit Court of Australia for an order that the person in contravention of the provision pay the Commonwealth a pecuniary penalty.

Part 4 of the Regulatory Powers Act, as it applies to this section, extends to every external Territory and acts, omissions, matters and things outside Australia. The extension of jurisdictions reflects the scope of providers that may be issued a technical assistance notice or technical capability notice.

317ZD Enforceable undertakings

Section 317ZB is enforceable under Part 6 of the Regulatory Powers Act. This Part enables an authorised person to accept written undertakings committing a person to particular action (or inaction) in order to prevent or respond to a breach of an enforceable provision. Undertakings are enforceable in their own right and they may be entered into instead of, or in addition to, the authorised person taking other disciplinary action.

The Communications Access Co-ordinator is an authorised person to accept undertakings and, in the case a provider breaches an undertaking, apply to the Federal Court or Federal Circuit Court of Australia for an order that the person comply.

Part 6 of the Regulatory Powers Act, as it applies to this section, extends to every external Territory and acts, omissions, matters and things outside Australia. The extension of jurisdictions reflects the scope of providers that may be issued a technical assistance notice or technical capability notice.

317ZE Injunctions

Section 317ZB is enforceable under Part 7 of the Regulatory Powers Act. Injunctions may be used to restrain a person from contravening section 317ZB or to compel compliance with the provision.

The Communications Access Co-ordinator may make an application to the Federal Court or Federal Circuit Court of Australia for an injunction under this section.

Part 7 of the Regulatory Powers Act, as it applies to this section, extends to every external Territory and acts, omissions, matters and things outside Australia. The extension of jurisdictions reflects the scope of providers that may be issued a technical assistance notice or technical capability notice.

Division 6—Unauthorised disclosure of information

Division 6 provides an offence for disclosing information relating to a technical assistance notice, technical capability notice and technical assistance request. The purpose of the provisions is to protect both designated communications providers and law enforcement and security agencies. It is designed to restrict the disclosure of commercially sensitive information, as well as highly sensitive information pertaining to investigations on foot and agency capabilities more broadly. Disclosure of this information could damage providers and compromise law enforcement and national security outcomes.

Exceptions to the unauthorised disclosure offence will enable the ready exchange of information where necessary for the administration of Part 15, or where relevant for the performance of the functions and powers of law enforcement, security and intelligence agencies.

317ZF Unauthorised disclosure of information

Section 317ZF creates an offence where any of the following persons disclose technical assistance notice information, technical capability notice information or technical assistance request information (or information obtained through a request or notice):

- a designated communications provider; or
- an employee of a designated communications provider; or
- a contracted service provider of a designated communications provider; or
- an employee of a contracted service provider of a designated communications provider; or
- an entrusted ASIO person; or
- an entrusted ASIS person; or
- an entrusted ASD person; or
- an officer of an interception agency; or
- an officer or employee of the Commonwealth, a State of a Territory; or
- an arbitrator appointed under section 317ZK, where parties disagree on the terms and conditions relating to a requirement in a technical assistance notice or technical capability notice.

A person is only subject to the offence where he or she received the information in connection with his or her capacity as one of the above persons. This connection ensures that a person who receives information innocently, or without reference to his or her functions under Part 15, will not commit an offence.

The offence does not include an express requirement of harm, and therefore, the prosecution is not required to prove harm beyond reasonable doubt. There is a high risk that the release of sensitive information contrary to this section will cause significant harm to essential public interests, including national security and protection of public safety. Therefore, it is assumed that disclosure is inherently harmful.

The offence of unauthorised disclosure of information required by a notice or request offence does not apply to providers who disclose their own information. This aspect of the prohibition is designed to protect sensitive information that providers give to agencies by ensuring agencies cannot disclose the information with an applicable exception. The provider retains discretion as to how they deal with their own information.

The maximum penalty for this offence is five years imprisonment. This penalty is appropriate and proportionate to the most serious conduct which may be captured by the offence. The information protected by this provision is highly sensitive, and the consequences of the commission of the offence may be dangerous or damaging to national security. The maximum penalty of five years is equivalent with the

penalties for unauthorised disclosure of information by entrusted persons in section 35P of the ASIO Act. It is also consistent with the Australian Law Reform Commission 2009 Report on Secrecy Law and Open Government in Australia which provides guidelines in considering the proportionality of penalties associated with the breach of secrecy provisions.

Exceptions

A person is permitted to disclose information:

- in connection with the administration or execution of this Part; or
- for the purposes of any legal proceedings arising out of or otherwise related to this Part or of any report of any such proceedings; or
- in accordance with any requirement imposed by law; or
- in connection with the performance of functions, or the exercise of powers by ASIO, ASIS, ASD, or an interception agency; or
- for the purpose of obtaining legal advice in relation to this Part; or
- to an IGIS official for the purpose of IGIS exercising powers or performing functions or duties under the IGIS Act; or
- if the person himself or herself is an IGIS official, in connection with his or her exercise of powers or performance of functions under the IGIS Act; or
- if the person is a designated communications provider disclosing the total number of technical assistance requests, technical assistance notices and technical capability notices in a period of at least 6 months.

This means a person is permitted, for example, to disclose information for the purposes of giving, or varying, a technical assistance request, technical assistance notice or technical capability notice. A person is also permitted to disclose information for the purpose of complying with a technical assistance request, technical assistance notice or technical capability notice.

For the purpose of the exception relating to legal proceedings, 'legal proceedings' include civil proceedings a provider is party to and relevant to claims of civil immunity under 317G or 317ZJ. It also includes legal proceedings relevant to the telecommunications and computer offences under Part 10.6 and Part 10.7 of the *Criminal Code Act 1995* (Criminal Code).

Subsections 317ZF(6)-(11) make clear that the Director-General of ASIS, the Director-General of ASD Director-General of Security, the Communications Access Co-ordinator and the chief officer of an interception agency may share information with one another without committing an offence. However, the sharing of information permitted under subsections (6)-(11) must be for purposes relating to those persons' performance of functions, or their exercise of powers. These subsections are consistent with the practical assistance agencies frequently provide to one another and existing information-sharing arrangements. It is important for the effective execution of their national security and law enforcement functions. The efficient exchange of information is particularly necessary where shared capabilities are developed under a technical capability notice.

Before disclosing any information, the Communications Access Co-ordinator must be notified of the proposed disclosure. This is designed to assist the Communications Access Co-ordinator in his or her administration of the powers in the Act.

Providers may also disclose statistical information about the total number of notices or requests issued to them in a period of at least 6 months. This allows providers to publish aggregates of notices or requests received from Australia in transparency reports. It does not allow for the publication of statistics by issuer or agency and must relate to total numbers only. Any statistic that identifies the issuing agency would be in breach of the unauthorised disclosure offence.

Consistent with the evidential principles in the Criminal Code, the defendant bears an evidential burden to demonstrate that the disclosure was lawful due to the application of an exception. This means the defendant must point to evidence that suggests a reasonable possibility that the matter exists or does not exist. The matters within the exceptions are peculiarly within the knowledge of the defendant and it would be significantly more difficult and costly for the prosecution to disprove. The prosecution will still be required to prove each element of the offence beyond a reasonable doubt before a defence can be raised by the defendant. Further, if the defendant discharges an evidential burden, the prosecution will also be required to disprove these matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.

Division 7— Limitations

Division 7 sets out limits on technical assistance notices and technical capability notices, frameworks for civil immunity for things done in compliance with a notice, the terms and conditions on which assistance is provided and the financial arrangements that govern this assistance. The Division also establishes the procedure for service of notices.

317ZG Designated communications provider must not be required to implement or build systemic weakness or systemic vulnerability etc.

A technical assistance notice or technical capability notice has no effect to the extent it requires a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection. Electronic protection includes forms of encryption or passcode authentication, such as rate limits on a device.

This limitation ensures that providers **cannot** be asked to implement or build so-called 'backdoors' into their products or services.

These limitations protect the fundamental security of systems and products. They are designed to ensure that any assistance required under a technical assistance notice or technical capability notice does not create weaknesses that can be deployed across a service or product line. The limitations ensure that requirements under a notice cannot jeopardise the security of a wide range of electronic services, devices or software by default, making them vulnerable to interference by malicious actors.

For the avoidance of doubt, this includes a prohibition on building a new decryption capability or actions that would render systemic methods of authentication or encryption less effective. The reference to systemic methods of authentication or encryption does not apply to actions that weaken methods of encryption or authentication on a particular device/s. As above, the term systemic refers to actions that impact a broader range of devices and service utilised by third-parties with no connection to an investigation and for whom law enforcement have no underlying lawful authority by which to access their personal data.

The prohibition clearly limits the ability of a notice to compel a provider to re-design services that feature end-to-end encryption. If a proposed re-design had the effect of removing the default protection that all users of end-to-end encrypted services benefit from and, consequently, made their communications less secure, it would be categorised as requiring a provider to build a systemic weakness or vulnerability into a form of electronic protection.

A technical assistance notice or technical capability notice also has no effect to the extent it prevents a provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection. This means that a notice cannot be used to prohibit a provider from fixing security flaws across their services or devices.

Notices may still require a provider to enable access to a particular service, particular device or particular item of software, which would not systemically weaken these products across the market. For example, if an agency were undertaking an investigation into an act of terrorism and a provider was capable of removing encryption from the device of a terrorism suspect without weakening other devices in the market then the provider could be compelled under a technical assistance notice to provide help to the agency by removing the electronic protection.

The mere fact that a capability to selectively assist agencies with access to a target device exists will not necessarily mean that a systemic weakness has been built. The nature and scope of any weaknesses and vulnerabilities will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required.

Likewise, a notice may require a provider to facilitate access to information prior to or after an encryption method is employed, as this does not weaken the encryption itself. A requirement to disclose an existing vulnerability is also not prohibited.

317ZH General limits on technical assistance notices and technical capability notices

A technical assistance notice or technical capability notice has no effect to the extent it requires a designated communications provider to do an act or thing which would require a warrant or authorisation under the TIA Act, the SD Act, the Crimes Act, the ASIO Act, or the IS Act. This ensures that a technical assistance notice or technical capability notice cannot be used as an alternative to a warrant or authorisation under any of those acts. For example, a technical assistance notice or technical capability notice cannot require a provider to intercept communications; an interception warrant under the TIA Act would need to be sought. However, a notice may require a provider to assist with the access of information or communications that have been lawfully intercepted.

Similarly, a technical assistance notice or technical capability notice has no effect to the extent it requires a designated communications provider to use a surveillance device or access data held in a computer where a State or Territory law requires a warrant or authorisation for that use or access. This ensures that a technical assistance notice or technical capability notice cannot be used as an alternative to a warrant or authorisation under State or Territory law.

These provisions do not exclude a technical assistance notice or technical capability notice requiring a designated communications provider to assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or Territory or give effect to a warrant or authorisation under a law of the Commonwealth.

These provisions also do not exclude technical capability notices from requiring a provider to develop a capability if the capability would assist in giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory or give effect to a warrant or authorisation under a law of the Commonwealth.

This provision makes clear that any and all limitations in the aforementioned Acts apply to the operation of notices both within and outside Australia. Simply, a notice cannot require a domestic or offshore provider to produce private communications or data. An underlying warrant or authorisation would need to be sought to access this information in every instance.

317ZJ Immunity

Section 317ZJ provides designated communications providers with immunity from civil liability for, or in relation to, any act or thing done in compliance, or in good faith in purported compliance, with a technical assistance notice or technical capability notice. It is full immunity for civil actions brought under Commonwealth law.

‘Purported compliance’ means that providers are not liable to an action or other proceeding in the exceptional circumstances where some elements of a technical assistance notice or technical capability notice are deemed invalid. A provider acts in good faith if the provider acts with honesty according to the standards of a reasonable person.

The immunity applies to officers, employees and agents of providers who perform an act or thing in connection with the provider’s actions to comply, or purportedly comply in good faith, with a technical assistance notice or technical capability notice.

317ZK Terms and conditions on which help is given etc

The default position for cost recovery for a provider’s compliance with requirements under a technical assistance notice or technical capability notice is no-profit/no-loss. Section 317ZK provides that the provider is not expected to bear the reasonable costs of complying with a requirement. ‘Reasonable costs’ of compliance may be different from the actual costs of meeting the requirements in a notice. For example, if a provider’s expenditure is higher than necessary to satisfy their obligations, they are entitled to recover costs equivalent to the expenditure that would have been reasonable.

However, different cost arrangements may be agreed by the provider and '*applicable costs negotiator*' – in the case of a technical assistance notice, this is the Director-General of Security or the chief officer of an interception agency and in the case of a technical capability notice, it is a person specified by the Attorney-General. Commercial terms may be appropriate where agencies require a provider to develop a large bespoke capability that would ordinarily be the subject of a significant procurement. The availability of commercial terms will give the agency the flexibility to enter into an arrangement containing both financial incentives and risk-management measures to secure satisfactory and timely performance. Where these parties fail to reach an agreement, an arbitrator approved by both parties will determine the terms and conditions of compliance. In the event that both parties cannot agree on the appointment of an arbitrator, an arbitrator is appointed by the ACMA if the provider is a carrier or carriage service provider or by the Attorney-General for other classes of designated communications provider.

An arbitrator appointed by the Attorney-General or the ACMA must be appointed in accordance subsections 317ZK(6)-(14). The relevant Minister can specify one or more persons, or a class of persons, to be suitable for appointment as an arbitrator. Before making these specifications, the relevant Minister must consult with the Attorney-General.

If arbitration is conducted by an arbitrator appointed by the ACMA, then the cost of arbitration must be shared equally between the parties. Where the arbitrator is appointed by the Attorney-General, the relevant Minister may make provisions relating to the conduct of arbitration, including provisions relating to the costs of arbitration.

In limited circumstances it may be appropriate that the costs of complying with a technical assistance notice or technical capability notice are not recoverable. Subsections 317ZK(1) and 317ZK(2) create a public interest exception where, if the Director-General of Security or the chief officer of an interception agency is satisfied it would be contrary to the public interest for a notice to be settled in accordance with the provisions in section 317ZK, the default processes do not apply. The Attorney-General may also invoke an identical public interest exception for compliance with a technical capability notice. It will not be appropriate to compensate a provider subject to a notice, for example, where the notice has been issued to remediate a risk to law enforcement or security interests that has been recklessly or wilfully caused by the provider. The threshold for exercising this public interest exemption is high. The Director-General of Security, the chief officer of an interception agency or the Attorney-General, as the case may be, must be satisfied that waiving the established compliance processes is in the public interest, and turn their mind to a range of commercial, law-enforcement and security considerations, including:

- the interests of law enforcement
- the interests of national security
- the objects of the Telecommunications Act
- the extent to which compliance with the requirement will imposed a regulatory burden on the provider
- the reasons for the giving of the technical assistance notice or technical capability notice, and
- such other matters that the decision-maker considers relevant.

317ZK has no effect to the extent (if any) to which its operation would result in an acquisition of property otherwise than on just terms.

317ZL Service of notices etc.

Section 317ZL is a deeming provision setting out when a summons, process, technical assistance notice or technical capability notice is taken to have been served on, or given to, a designated communications provider or to a body corporate incorporated outside Australia.

Service of a required summons, process or notice on a designated communications provider has taken place if:

- it is left at, or sent by pre-paid post to, an address given by the provider, or
- it is sent to an electronic address given by the provider.

Service of a required summons, process or notice on a designated communications provider that is a body corporate that is incorporated outside Australia, does not have a registered or principal office in Australia, and has an agent in Australia, has taken place if:

- it is given to an agent of the body corporate in Australia, or
- it is left at, or sent by pre-paid post to, an address in Australia where the body corporate carries on business or conducts activities.

317ZM Interception agency—chief officer and officer

The table in section 317ZM defines a chief officer of an interception agency and officer of an interception agency.

Item 1 of the table lists the AFP. Chief officer means the Commissioner in section 6 of the *Australian Federal Police Act 1979*. Officer means a member of the AFP under section 40B of that Act or a special member under section 40E of that Act.

Item 2 of the table lists ACLEI. Chief officer means the Integrity Commissioner appointed under section 175 of the *Law Enforcement Integrity Commissioner Act 2006*. Officer means either the Integrity Commissioner or a staff member of ACLEI within the meaning of subsection 11(1) of that Act.

Item 3 of the table lists the Australian Crime Commission, now known as the Australian Criminal Intelligence Commission (ACIC). Chief officer means the Chief Executive Officer of the ACIC appointed under section 37 of the *Australian Crime Commission Act 2002*. Officer means either the Chief Executive Officer of ACIC, or an examiner appointed under subsection 46B(1) of that Act, or a member of the staff of the ACIC within the meaning of section 4 of that Act.

Item 4 of the table lists the Police Force of a State or the Northern Territory. Chief officer means the Commissioner of Police, however designated, of that State or Territory. Officer means an officer of that Police Force.

Item 5 of the table lists the Independent Commission Against Corruption of New South Wales. Chief officer means the Chief Commissioner appointed under section 104 of the *Independent Commission Against Corruption Act 1988* (NSW). Officer means an officer of the Commission within the meaning of section 3 of that Act but it does not include a person engaged under section 104B of that Act to provide the Commission with services, information or advice.

Item 6 of the table lists the New South Wales Crime Commission. Chief officer means the Commissioner appointed under section 8 of the *Crime Commission Act 2012* (NSW). Officer means an officer of the Commission within the meaning of section 72 of that Act but it does not include a person engaged by the Commission as a consultant under subsection 74(2) of that Act.

Item 7 of the table lists the Law Enforcement Conduct Commission of New South Wales. Chief officer means the Chief Commissioner appointed under section 18 of the *Law Enforcement Conduct Commission Act 2016* (NSW). Officer means either the Chief Commissioner, or the Commissioner for Integrity appointed under section 18 of that Act, or a member of the staff of the Commission within the meaning of section 21 of that Act.

Item 8 of the table lists the Independent Broad-based Anti-corruption Commission of Victoria (IBAC). Chief officer means the Commissioner appointed under section 20 of the *Independent Broad-based Anti-corruption Commission Act 2011* (Vic.). Officer means a sworn IBAC Officer within the meaning of section 3 of that Act.

Item 9 of the table lists the Crime and Corruption Commission of Queensland. Chief officer means the chairperson within the meaning of the *Crime and Corruption Act 2001* (Qld). Officer means a commission officer as defined by paragraph (a) of the definition of commission officer in the Dictionary to that Act. Officer

does not mean a person engaged under section 256 of that Act to provide the Commission with services, information or advice.

Item 10 of the table lists the Independent Commissioner Against Corruption (SA). Chief officer means the Commissioner appointed under section 8the *Independent Commissioner Against Corruption Act 2012* (SA). Officer means either: the Commissioner, or the Deputy Commissioner appointed under section 9 of that Act, or a member of the staff of the Independent Commissioner Against Corruption (SA) within the meaning of section 12 of that Act.

Item 11 of the table lists the Corruption and Crime Commission (WA). Chief officer means the Commissioner appointed under section 9 of the *Corruption, Crime and Misconduct Act 2003* (WA). Officer means an officer of the Commission within the meaning of section 3 of the *Corruption, Crime and Misconduct Act 2003* (WA). Officer does not mean a person engaged under section 182 of that Act to provide the Commission with services, information or advice.

317ZN Delegation by Director-General of Security

Section 317ZN allows the Director-General of Security to delegate any of his or her functions or powers under Divisions 2, 3 or 6 to a senior position-holder in the ASIO Act. Under section 4 of that Act, a senior position-holder means an ASIO employee or an ASIO affiliate who holds, or is acting in, a position that is: equivalent to or higher than a position occupied by a Senior Executive Service (SES) employee; or known as Coordinator.

The purpose of this delegation power is to enable persons with appropriate seniority and expertise to perform functions or powers. In doing so, it allows for processes to be streamlined in order to assist ASIO to discharge its statutory functions. In accordance with usual administrative law practices, the delegation must be in writing and specify to whom the function or power is delegated. The delegate must also comply with any written directions of the Director-General of Security.

Consistent with paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901*, the powers of the Director-General of Security that may be delegated do not include that power to delegate. This means that sub-delegation of powers and functions of the Director-General of Security is prohibited.

317ZP Delegation by Director-General of Australian Secret Intelligence Service

Section 317ZP allows the Director-General of ASIS to delegate any of his or her functions or powers under new Divisions 2 and 6 to a staff member of ASIS who holds, or is acting in, a position in ASIS that is equivalent to, or higher than, a position occupied by a SES employee.

This delegation supports the efficient exercise of the powers under new Part 15 and ensures these powers are limited to persons of appropriate seniority and expertise.

Consistent with paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901*, the powers of the Director-General of ASIS that may be delegated do not include that power to delegate.

317ZQ Delegation by Director-General of the Australian Signals Directorate

Section 317ZQ allows the Director-General of ASD to delegate any of his or her functions or powers under new Divisions 2 and 6 to a staff member of the ASD who holds, or is acting in, a position in the ASD that is equivalent to, or higher than, a position occupied by an SES employee.

This delegation supports the efficient exercise of the powers under new Part 15 and ensures these powers are limited to persons of appropriate seniority and expertise.

Consistent with paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901*, the powers of the Director-General of ASD that may be delegated do not include that power to delegate.

317ZR Delegation by the chief officer of an interception agency

Section 317ZR allows the chief officer of an interception agency, listed in Column 1 of the item, to delegate any of his or her functions or powers under new Divisions 2, 3 or 6 to persons mentioned in Column 2 of the item. This delegation supports the efficient exercise of the powers under new Part 15 and ensures these powers are limited to persons of appropriate seniority and expertise.

Consistent with paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901*, the powers of the chief officer of an interception agency that may be delegated do not include that power to delegate.

A delegate must comply with any written directions of the chief executive.

Item 1 of the table provides that the chief officer of the AFP may delegate his or her functions or powers to either a Deputy Commissioner in section 6 of the *Australian Federal Police Act 1979* or a senior executive AFP employee within the meaning of section 25 of that Act.

Item 2 of the table provides that the chief officer of ACLEI may delegate his or her functions or powers to either an Assistant Integrity Commissioner appointed under section 185 of the *Law Enforcement Integrity Commissioner Act 2006* or a staff member of ACLEI within the meaning of subsection 11(1) of that Act who is an SES employee or acting SES employee.

Item 3 of the table provides that the chief officer of ACIC may delegate his or her functions or powers to a member of the staff of the ACIC within the meaning of section 4 of the *Australian Crime Commission Act 2002* who is an SES employee or acting SES employee.

Item 4 of the table provides that the chief officer of a Police Force of a State or the Northern Territory may delegate his or her functions or powers to either an Assistant Commissioner of the Police Force or a person holding equivalent rank, or a Superintendent of the Police Force or a person holding equivalent rank.

Item 5 of the table provides that the chief officer of the Independent Commission Against Corruption of New South Wales may delegate his or her functions or powers to either a Commissioner appointed under section 5 of the *Independent Commission Against Corruption Act 1988* (NSW), or an Assistant Commissioner appointed under section 6A of that Act, or an officer of the Commission within the meaning of section 3 of that Act (other than a person engaged under section 104B of that Act) who is at executive level. A person is at executive level if the person occupies an office or position at an equivalent level of a Public Service senior executive within the meaning of the *Government Sector Employment Act 2013 (NSW)*.

Item 6 of the table provides that the chief officer of the New South Wales Crime Commission may delegate his or her functions or powers to an officer of the Commission within the meaning of section 72 of the *Crime Commission Act 2012* (NSW) (other than a person engaged under subsection 74(2) of that Act) who is at executive level. A person is at executive level if the person occupies an office or position at an equivalent level of a Public Service senior executive within the meaning of the *Government Sector Employment Act 2013 (NSW)*.

Item 7 of the table provides that the chief officer of the Law Enforcement Conduct Commission of New South Wales may delegate his or her functions or powers to either the Commissioner for Integrity appointed under section 18 of the *Law Enforcement Conduct Commission Act 2016* (NSW), or a member of the staff of the Commission within the meaning of section 21 of that Act who is at executive level. A person is at executive level if the person occupies an office or position at an equivalent level of a Public Service senior executive within the meaning of the *Government Sector Employment Act 2013 (NSW)*.

Item 8 of the table provides that the chief officer of IBAC may delegate his or her functions or powers to either a Deputy Commissioner of the Commission appointed under section 23 of the *Independent Broad-based Anti-corruption Commission Act 2011* (Vic.), the Chief Executive Officer of the Commission appointed under section 33 of that Act, or a sworn IBAC officer within the meaning of section 3 of that Act who is at executive level. A person is at executive level if the person occupies an office or position at an equivalent level of an executive within the meaning of the *Public Administration Act 2004 (VIC).*

Item 9 of the table provides that the chief officer of the Crime and Corruption Commission of Queensland may delegate his or her functions to a senior executive officer within the meaning of paragraphs 245(3)(b) and 245(3)(a) of the *Crime and Corruption Act 2001* (Qld).

Item 10 of the table provides that the chief officer of the Independent Commissioner Against Corruption (SA) may delegate his or her functions to either the Deputy Commissioner within the meaning of the *Independent Commissioner Against Corruption Act 2012* (SA) or a member of staff of the Independent Commissioner Against Corruption within the meaning of that Act who is at executive level. a person is at executive level if the person occupies an office or position at an equivalent level of an executive employee within the meaning of the *Public Sector Act 2009 (SA)*.

317ZS Annual reports

317ZS introduces annual reporting requirements. The Minister must cause a written report to be prepared that sets out the number of technical assistance notices and technical capability notices given under section 317L and section 317T respectively during the financial year.

Reports will be included in the annual report under Chapter 4 of the TIA Act which discloses information on the use of telecommunications data by law enforcement agencies.

317ZT Alternative constitutional basis

Section 317ZT provides an alternative constitutional basis for Part 15. It ensures that, in cases where the constitutional support for making a request, or issuing a notice to a provider is not made out under other heads of power in the Constitution, the scope of 317E (listed acts or things) should be read down as if the corporation's power was the sole basis for constitutional authority.

Schedule 2

Part 1—Amendments

Amendments to the Australian Security Intelligence Organisation Act 1979

Section 4 definition of intercept a communication

Section 4 defines terms in the ASIO Act.

This item inserts a definition of 'intercept a communication passing over a telecommunications system' which is the same under the TIA Act. In sections 5F, 5G, 5H and 6 of the TIA Act a communication which is listened to, or recorded by any means, without the knowledge of the person making it, between being sent or transmitted by the person sending it and becoming accessible to the intended recipient, is intercepted passing over a telecommunications system.

This ensures that the terminology used across both Acts in relation to the interception of communications is consistent.

The definition facilitates new provisions that allow for interception to occur where necessary to execute a computer access warrant. New paragraph 25A(4)(ba) permits intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing things specified in the computer access warrant. Those provisions are discussed below.

The definition also facilitates new provisions that allow for interception to occur where necessary to execute an identified person warrant in relation to accessing data held in computers. New paragraph 27E(2)(ea) permits intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing anything authorised under an identified person warrant in relation to accessing data held in computers. Those provisions are discussed below.

Subsection 24(4) definition of relevant device recovery provision

Section 24 states that the authority conferred by a relevant warrant or relevant device recovery provision may be exercised on behalf of ASIO by the Director-General or persons he or she appoints in writing.

This item includes new subsection 25A(8) in the list of provisions defined as 'relevant device recovery provisions' for the purposes of section 24. Subsection 25A(8) allows ASIO to conceal activities undertaken under a computer access warrant following the expiry of that warrant (this is explained further below).

This means the authority conferred by new subsection 25A(8) can only be exercised by the Director-General, or a person or class of persons approved by the Director-General in writing. This item provides a safeguard against the arbitrary exercise of the range of activities permitted by the new subsection.

Subsection 24(4) definition of relevant device recovery provision

Similar to the preceding item, this item includes new subsections 27A(3C) and 27E(6) in the list of provisions defined as 'relevant device recovery provisions' for the purposes of section 24.

Subsection 27A(3C) permits the temporary removal of computers or other things for the purposes of concealing access. Subsection 27E(6) permits the concealment of access to a computer or thing under an identified person warrant (this is explained further below).

As with the preceding item, this provides a safeguard against the arbitrary exercise of the range of activities permitted by these new subsections by requiring the person or class of persons exercising these powers to be approved by the Director-General personally.

Paragraph 25A(4)(ab)

This item replaces paragraph 25A(4)(ab) with a new paragraph. It reformats the content into a numbered list and is a stylistic amendment only.

After paragraph 25A(4)(ab)

Subsection 25A(4) lists the things that may be authorised in a computer access warrant.

This item inserts a new paragraph permitting the removal of a computer or other thing from premises, for the purposes of doing anything specified in the warrant before returning the computer of other thing to the premises.

ASIO does not currently have authority to temporarily remove a computer from a premises for the purposes of executing a computer access warrant. However, ASIO does have authority to temporarily remove objects from premises for the installation or maintenance of a surveillance device (see paragraph 26B(4)(b)).

The ability to remove computers from premises is important in situations where ASIO may require specialist equipment, which cannot be brought onto the premises in a covert fashion, in order to access the computer. The deprivation of property is an intrusive measure. The item limits the degree of intrusion by confining the authority to a specific purpose and requiring the return of the computer or thing once the purpose is achieved. The removal of a computer or other thing is only permitted for the purposes of doing anything specified in the computer access warrant before the computer or other thing must be returned to the premises.

The authority is only available under a warrant issued by the Attorney-General. Under subsection 25A(2), the Attorney-General must be satisfied there are reasonable grounds for believing that access by ASIO will substantially assist the collection of intelligence in accordance with the Act in respect of a matter that is important in relation to security. Oversight is conducted by the IGIS to ensure the power is exercised lawfully, with propriety and with respect for human rights.

After paragraph 25A(4)(b)

This item inserts a new paragraph 25A(4)(ba) to permit the interception of a communication passing over a telecommunication system, if the interception is for the purposes of doing anything specified in the computer access warrant.

It is almost always necessary for ASIO to undertake limited interception for the purposes of executing a computer access warrant. Currently, ASIO is required to obtain a computer access warrant to gain access to a device and a telecommunications interception warrant under section 9 or 9A of the TIA Act for this interception to establish computer access.

The threshold requirements for issuing computer access warrants and telecommunication interception warrants currently differ. In some circumstances, ASIO can obtain a computer access warrant, but cannot obtain a telecommunications interception warrant. This reduces the likelihood of a successful execution of the validly issued computer access warrant. It is undesirable for ASIO's ability to execute a computer access warrant to be dependent on its ability to obtain a separate telecommunications interception warrant. Ordinarily, warrants authorise a person to undertake all activities normally required to give effect to the warrant, independently of any other warrant or authorisation.

The current arrangements also cause administrative inefficiency by requiring ASIO to prepare two warrant applications, addressing different legal standards, for the purpose of executing a single computer access warrant. The process requires the Attorney-General to consider each application separately and in accordance with each separate criterion.

At the end of section 25A

This item inserts new subsection 25A(8) relating to concealment of access under computer access warrants.

Currently, ASIO does not have authority to retrieve or delete remnants of its computer access activities, or to conceal the activities it has undertaken pursuant to a computer access warrant, following the expiry of the warrant. By contrast, ASIO does have authority to undertake a range of activities to recover surveillance devices following the expiry of the relevant surveillance device warrant under subsection 26B(5) of the ASIO Act.

ASIO cannot always reliably predict whether, or when, it will be able to safely retrieve its devices without compromising a covert security intelligence operation. For example, a person may unexpectedly relocate their computer or device prior to the expiry of the warrant, precluding ASIO from taking the necessary steps to conceal the fact that it had accessed the device under warrant.

Once the warrant has expired ASIO may not be able to obtain a further computer access warrant to undertake retrieval and concealment activities, as retrieving and concealing would (by definition) not necessarily meet the statutory threshold of 'substantially assisting the collection of intelligence'.

Subsection 25A(8) allows ASIO to perform these concealment activities at any time while the warrant is in force, or within 28 days after it ceases to be in force, or at the earliest time after this period at which it is reasonably practicable to do so.

The period of time provided to perform these concealment activities recognises that, operationally, it is sometimes impossible for ASIO to complete this process within 28 days of a warrant expiring. The requirement that the concealment activities be performed 'at the earliest time after that 28-day period at which it is reasonably practicable to do so' acknowledges that this authority should not extend indefinitely, circumscribing it to operational need.

After subsection 27A(3B)

This item inserts a new subsection 27A(3C) relating to concealment of access under computer access warrants for foreign intelligence. It is ASIO's function to obtain and communicate foreign intelligence within Australia under paragraph 17(1)(e).

This provision permits ASIO to do specified things, and things reasonably incidental to a specified thing, to conceal the fact that anything has been done in connection with a foreign intelligence warrant that authorises ASIO to do acts or things referred to under a computer access warrant.

Subsection 27A(3B) is consistent with the approach taken in subsection 27A(3A) for the recovery of surveillance devices installed or used under a foreign intelligence warrant.

Paragraph 27E(2)(d)

This item replaces paragraph 27E(2)(d) with a new paragraph. It reformats the content into a numbered list and is a stylistic amendment only.

After paragraph 27E(2)(d)

This item inserts provisions allowing for the removal of a computer or thing from the premises for the purposes of an identified person warrant. Specifically, it allows ASIO to remove and return a computer or other thing from premises for the purposes of doing anything authorised under an identified person warrant in relation to the computer.

Identified person warrants may be issued where the Minister is satisfied that a person is engaged, or reasonably suspected of being engaged or likely to engage in, activities prejudicial to security, and that issuing a warrant in relation to that person will, or is likely to, substantially assist the collection of intelligence relevant to security. This is a higher threshold than for standard computer access warrants under section 25A.

Identified person warrants can give conditional approval for ASIO to access records or other things in or on premises, access data held in computers, use one or more kinds of surveillance devices, access postal

articles that are in the course of post, and access articles that are being delivered by a delivery service provider.

This item will ensure that things that may be authorised under an identified person warrant in relation to data held in computers mirrors those things that may be authorised under a computer access warrant once amended (see paragraph 25A(4)(ac)). It will ensure consistency between the functionality of these two warrants where either is issued for the purpose of computer access.

After paragraph 27E(2)(e)

This item inserts new paragraph 27E(2)(ea) allowing a communication passing over a telecommunications system to be intercepted if the interception is for the purposes of doing anything authorised under an identified person warrant in relation to accessing data held in computers.

This item will ensure that things that may be authorised under an identified person warrant in relation to data held in computers mirrors those things that may be authorised under a computer access warrant once amended (see paragraph 25A(4)(ba)). This will ensure consistency between the functionality of these two warrants where either is issued for the purpose of computer access.

At the end of section 27E

This item inserts a new subsection 27E(6) relating to concealment of access under an identified person warrant in relation to accessing data held in computers. It mirrors the new subsection relating to concealment of access under a computer access warrant (see subsection 25A(8)) and is underpinned by similar policy considerations.

This item permits ASIO to do anything reasonably necessary to conceal the fact that anything has been done under the warrant, and provides ASIO with the ability to retrieve devices following the expiry of a warrant in order to undo any additions, deletions or alterations made in the target computer.

ASIO may perform these concealment activities at any time while the warrant is in force, or within 28 days after it ceases to be in force, or at the earliest time after this period at which it is reasonably practicable to do so.

The period of time provided to perform these concealment activities recognises that, operationally, it is sometimes impossible to complete this process within 28 days of a warrant expiring. The requirement that the concealment activities be performed ‘at the earliest time after the 28-day period at which it is reasonably practicable to do so’ acknowledges that this authority should not extend indefinitely, circumscribing it to operational need.

Subsection 33(1)

This item repeals subsection 33(1) which provides that computer access warrants (section 25A), foreign intelligence warrants (section 27A) and authorisations under identified person warrants to access data held in computers (section 27E) do not authorise the interception of a communication passing over a telecommunications system.

This provision is inconsistent with the amendments discussed above which introduce measures allowing for the interception of a communication passing over a telecommunications system in certain limited circumstances under each of these warrants.

Paragraph 34(2)(b)

Under subsection 34(2), the Director-General is required to report to the Minister on particular things done under a warrant issued under section 25, 25A, 27A, 27C or 29 which materially interfered with, interrupted or obstructed the lawful use by other persons of a computer or other electronic equipment or a data storage device.

Paragraph 34(2)(b) will be amended to ensure that any concealment activities done under the new subsections 25A(8), 27A(3C) and 27E(6) will be captured by this reporting requirement. This supplements the requirement for all warrants issued under Division 2 of the ASIO Act to be reported on in relation to the extent to which the action taken under each warrant assisted ASIO in carrying out its functions.

This item recognises that the authority for ASIO to conceal access and temporarily remove computers and other things under a computer access warrant is an intrusive measure, which requires proportionate safeguards. ASIO computer access warrants should not ordinarily interfere with a person's use of a computer. Requiring ASIO to bring material interferences to the Minister's attention will ensure that he or she is aware of issues and can consider the implications when deciding whether to issue future warrants.

At the end of section 34

This item clarifies that anything done to conceal access to a computer, or other thing, under a computer access warrant or an identified person warrant is to be taken, for the purposes of section 34, as having been done under that warrant.

This will ensure that concealment activities are captured by section 34 and will be subject to reporting requirements.

Subsection 34AA(5) (definition of relevant authorising provision)

This item amends the evidentiary certificate provisions in section 34AA of the ASIO Act in so far as they relate to the new activities authorised by computer access warrants and identified person warrants.

The Director-General or a Deputy Director-General will be able to issue a written certificate setting out facts in relation to concealment activities under a computer access warrant and identified person warrant (in relation to data held in computers).The Director-General or a Deputy Director-General will also be able to issue a written certificate in relation to temporary removal of computers or other things under a computer access warrant.

The certificates provide prima facie evidence of the matters stated in it for the purposes of proceedings.

Amendments to the Mutual Assistance in Criminal Matters Act 1987

Subsection 3(1) (definition of protected information)

This item includes new paragraph 44(1)(aa) of the SD Act within the definition of ***protected information*** for the purposes of the *Mutual Assistance in Criminal Matters Act 1987* (MACMA). This means that any information (other than general computer access intercept information) obtained from access to data under either the new computer access warrant or emergency authorisation for access to data held in a computer is protected information.

This extends the current definition of protected information which refers to information obtained from the use of a surveillance device or tracking device under warrant or authorisation (see paragraphs 44(1)(a), (b) and (c) of the SD Act).

This ensures that where information is obtained in response to a computer access warrant for a domestic investigation, the Attorney-General may authorise the provision of that information to a foreign country in response to a mutual assistance request, subject to existing restrictions under section 13A of the MACMA

Part IIIBB—Assistance in relation to data held in computers

New Part IIIBBA will allow foreign authorities to make a request to the Attorney-General to authorise an eligible law enforcement officer to apply for a computer access warrant for the purposes of obtaining evidence to assist in a foreign investigation or investigative proceeding.

Investigations and prosecutions frequently involve criminal use of the internet and cross border storage of information. Australia's mutual assistance framework is critical in enabling Australian and foreign authorities access to information necessary to conduct investigations and undertake criminal proceedings, amongst other things.

These amendments do not allow a foreign country's authorities to exercise computer access powers within Australia, rather, when authorised by the Attorney-General, it allows for Australian law enforcement to undertake these activities on their behalf under authority of the appropriate computer access warrant.

The Attorney-General in exercising his or her discretion on authorising the use of this power for a foreign country will be subject to specific restrictions:

- The investigation, or investigative proceeding, must relate to a criminal matter involving an offence against the law of a foreign country punishable by a maximum penalty of imprisonment for 3 years or more, imprisonment for life or the death penalty (note that the Attorney-General may refuse to provide assistance if they believe that providing the assistance may result in the death penalty being imposed).
- The investigation or investigative proceeding at (a) must have commenced in the requesting country.
- The requesting country must specifically request that the Attorney-General arrange for access to the data held on the target computer.
- A computer must meet the definition of '*target computer'* which is restricted under the proposed section 15CC(2) of the MACMA where the definition of ***computer*** has the same meaning as the SD Act.

In addition to the above, new section 15CC(1)(c) allows the Attorney-General, in authorising the use of the power under the MACMA, to require that a requesting country provide appropriate undertakings. This will ensure that the computer evidence provided as a result of the computer access warrant is only used for the authorised purpose for which it was obtained and consistent with conditions around the destruction of the

document or thing containing the data. The Attorney-General may also require undertakings on any other matter he or she considers appropriate.

Amendments to the Surveillance Devices Act 2004

Title

The long title of the SD Act will be amended to 'an Act to set out the powers of Commonwealth law enforcement agencies with respect to surveillance devices and access to data held in computers, and for related purposes.'

After paragraph 3(a)

New paragraph 3(aaa) amends the purposes of the SD Act to reflect the new power in the Act for law enforcement agencies to access data held in computers. It adds as a purpose the establishment of procedures for law enforcement officers to obtain warrants and emergency authorisations for access to data held in computers, consistent with the position of surveillance devices warrants and authorisations. This relates to criminal investigations and the location and safe recovery of children to whom recovery orders relate.

After paragraph 3(aa)

New paragraph 3(aaaa) amends the purposes of the SD Act to reflect the new power in the Act for law enforcement agencies to access data held in computers. It adds as a purpose the establishment of procedures for law enforcement officers to obtain warrants for access to data held in computers in control order cases, consistently with the position of surveillance devices warrants and authorisations. This relates to protecting the public from a terrorist act, preventing the provision of support for or facilitation of a terrorist act, preventing the provision of support for or facilitation of hostile activity by a foreign country or determining whether a control order has been or is being complied with.

After paragraph 3(b)

New paragraph 3(ba) amends the purposes of the SD Act to include restrictions on the use, communication and publication of information that is obtained through accessing data held in computers or that is otherwise connected with computer data access operations.

Paragraph 3(c)

Paragraph 3(c) will be amended so that the purposes of the SD Act include imposing requirements for the secure storage and destruction of records, and the making of reports, in relation with computer data access operations.

Subsection 4(1)

This item amends subsection 4(1) to clarify that the SD Act is not intended to affect any other law of the Commonwealth, a State or any law of a self-governing Territory that prohibits or regulates computer access.

The item clarifies this relationship to other laws in respect of computer access, consistently with the position of surveillance devices.

After subsection 4(4)

New subsection (4A) clarifies that a warrant or an emergency authorisation may be issued or given under the Act for access to data held in a computer, in relation to a relevant offence or a recovery order. This replicates the clarification in existing subsection 4(4) relating to warrants and emergency authorisations regarding surveillance devices.

After subsection 4(5)

New subsection (5A) clarifies that a warrant may be issued or given under the Act for access to data held in a computer, in relation to a control order. This replicates the clarification in subsection 4(5) relating to control orders regarding surveillance devices.

Subsection 6(1)

This item inserts definitions of ***carrier*** and ***communication in transit***.

Carrier means either a carrier or ***carriage service provider*** within the meanings of the Telecommunications Act.

The definition of ***communication in transit*** means a communication (within the meaning of the Telecommunications Act) passing over a telecommunications network (within the meaning of that Act). This definition is consistent with the definition in the ASIO Act.

These definitions are inserted to facilitate provisions that allow for interception to occur where necessary to execute a computer access warrant. Paragraph 27E(2)(h) permits intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing anything specified in the warrant in accordance with subsection 27E(2). Those provisions are discussed below.

Subsection 6(1) (definition of computer)

This item repeals the definition of ***computer*** and replaces it with the definition of computer that is in section 22 of the ASIO Act.

The definition of computer within the ASIO Act is preferred for consistency between Acts in the statute book. This will ensure consistency between powers conferred under those Acts.

The repealed definition defined computer as any electronic device for storing or processing information. Repeal of this definition is not to be read as the former provision not being correct. Rather, the former definition was merely limited. The new definition takes into account the increasing use of distributed and cloud-based services for processing and storing data, and networks of computers through which data commonly passes and on which it is stored. It is no longer realistic for law enforcement agencies to identify one particular computer on which relevant data is stored in the context of an investigation. Individuals commonly have multiple computers and access a variety of networks, and the intention of the provisions is to enable law enforcement agencies to access those networks under one computer access warrant rather than seeking a warrant for each device.

For the avoidance of doubt, mobile phones are intended to be captured by the definition of computer.

Communication devices for storing and processing information which would not colloquially be termed ‘computers’, but which use computers or computing technology as their functional basis, are still intended to be captured within the new definition. For example security systems, internet protocol cameras and digital video recorders may be computers for the purpose of facilitating computer access.

Subsection 6(1)

This item provides the definitions for terms that facilitate the operation of the computer data access provisions.

The definition of ***computer access warrant*** has the meaning given it by section 27C or subsection 35A(4) or (5). Section 27C allows an eligible judge or nominated AAT member to issue a warrant, upon he or she being satisfied of the relevant conditions contained in section 27C(1), including that there are reasonable grounds for the suspicion that access to data will be necessary in the course of the investigation. Computer access warrant under subsections 35A(4) and (5) means a warrant issued by an eligible judge or nominated AAT member after they have given an emergency authorisation.

The definition of ***control order access warrant*** is a computer access warrant issued in response to an application under subsection 27A(6). Under subsection 27A(6) a law enforcement officer may apply for the issue of a computer access warrant if a control order is in force and he or she suspects that access to data held in a computer would be likely to substantially assist in either protecting the public from a terrorist act, preventing the provision of support for a terrorist act or a hostile activity, or determining whether the control order is being complied with.

The definition of ***data*** includes information in any form, as well as any program or a part of any program.

Data held in a computer includes data held in any removable data storage device for the time being held in a computer, and data held in a data storage device on a computer network of which the computer forms a part. This definition envisages both internal network storage, such as a back-up copy of data, and external storage, such as internet-based and cloud-based storage.

The definition of ***data storage device*** is consistent with the definition in section 4 of the ASIO Act and with the definition in the Criminal Code. The item defines data storage device to mean a thing containing, or designed to contain, data for use by a computer. This refers to things containing or designed to contain data for use by a computer. They do not need to be powered to qualify as a device. A compact disc (CD), for example, is a data storage device. A data storage device becomes a constituent part of a computer once it is inserted into an optical drive for access to its data. A disc, compact disc, secure digital card (also known as an SD card), or any other thing that contains information that is made legible, accessible or usable by a computer are data storage devices. The definition is designed to cover future technological advancements.

Subsection 6(1) (definition of data surveillance device)

This item amends the definition of ***data surveillance device*** to accommodate for the new definition of ***computer*** in the SD Act (see above).

Data surveillance device means any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device. However, a data surveillance device cannot be used to record or monitor the inputs or outputs of a computer network, as this may amount to interception. If agencies need to conduct interception, they need to apply for an interception warrant under the TIA Act, not a data surveillance device warrant under the SD Act.

Subsection 6(1)

This item inserts two new definitions into subsection 6(1).

General computer access intercept information is defined to have the same meaning as in the TIA Act. Amendments in this Bill insert a definition into the TIA Act to mean information obtained under a general computer access warrant by intercepting a communication passive over a telecommunications system. This is distinct from a computer access warrant obtained by ASIO and distinct from computer data etc. obtained under a computer access warrant.

Intercepting a communication passing over a telecommunications system has the meaning given to it by the TIA Act. The TIA Act defines interception of a communication passing over a telecommunications system as consisting of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication (see sections 5F, 5G. 5H and 6.)

Subsection 6(1) (definition of mutual assistance application)

This item replaces the definition of ***mutual assistance application*** to reflect the new power to apply for computer access warrants under the SD Act.

Subsection 6(1) (definition of mutual assistance authorisation)

This item amends the definition of ***mutual assistance application*** to reflect the new power to apply for computer access warrants under the SD Act.

Subsection 6(1) paragraph (db) of the definition of relevant offence

This item is a consequential amendment to capture new computer access warrants within the definition of relevant offences for integrity operations.

Subsection 6(1) (definition of remote application)

This item amends the definition of ***remote application*** in the SD Act to include reference to section 27B of the Act. New section 27B allows for remote applications for computer data access warrants.

Subsection 6(1)

This item includes a definition of ***telecommunications facility*** within the SD Act. The term is defined to mean a facility within the meaning of the Telecommunications Act. New section 27E of the SD Act provides for a ***telecommunications facility*** to be used to obtain access to data under a new computer access warrant.

Subsection 6(1) (definition of unsworn application)

This item includes references to provisions in relation to the new computer access warrants within the existing definition of ***unsworn application*** in the SD Act.

Subsection 6(1) (definition of warrant)

This item expands the existing definition of ***warrant*** to include the new computer access warrants in the SD Act.

At the end of subsection 10(1)

This item expands the existing types of warrant that may be issued under Part 2 of the SD Act to include computer access warrants. This is consequential to insertion of Division 4 to Part 2 of the SD Act which establishes the framework for law enforcement agencies to obtain computer access warrants.

Subsection 10(2)

This item clarifies that a surveillance device warrant (or a retrieval warrant) may be issued in respect of more than one kind of surveillance device and more than one surveillance device of any kind.

This is a consequential amendment to ensure the expanded definition of warrant, including a computer access warrant, does not apply in relation to subsection 10(2).

Division 4—Computer access warrants

This item introduces Division 4 to Part 2 of the SD Act. Division 4 establishes the framework for law enforcement agencies can obtain computer access warrants. A computer access warrant enables officers to search electronic devices remotely and access content on those devices. These warrants are in addition to warrants for data surveillance devices, which enable the use of software to monitor inputs and outputs from certain devices.

27A Application for computer access warrant

New section 27A allows a law enforcement officer (or another person on the law enforcement officer's behalf) to apply for the issue of a computer access warrant in respect of offence investigations, recovery orders, mutual assistance investigations, integrity operations and control orders. Section 27A replicates the structure and thresholds of section 14 of the SD Act. It may often be necessary for an agency to obtain both a surveillance device warrant and a computer access warrant in the course of one investigation.

Warrants sought for offence investigations

A warrant can be sought in the context of an offence investigation if the law enforcement officer has reasonable grounds to suspect that:

- one or more relevant offences has been, are being, are about to be, or are likely to be, committed

- an investigation into those offences is being, will be, or is likely to be, conducted, and
- access to data held in a computer is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of:
    - the commission of those offences, or
    - the identity or location of the offenders.

Relevant offence is defined in section 6 of the SD Act to include (amongst others): an offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of 3 years or more or for life.

Subsection 27A(2) provides that, if the application is being made by or on behalf of a State or Territory law enforcement officer, the reference to a relevant offence does not include a reference to a State offence that has a federal aspect. This means that only Commonwealth law enforcement officers may make an application for a computer access warrant to investigate State offences with a federal aspect.

State law enforcement may utilise computer access warrants for investigations into federal offences.

Warrants sought for recovery orders

A warrant can be sought in the context of a recovery order if:

- a recovery order is in force, and
- the law enforcement officer suspects on reasonable grounds that access to data held in a computer may assist in the location and safe recovery of the child

A recovery order is either an order section 67U of the *Family Law Act 1975*, or an order for a warrant for the apprehension or detention of a child under regulations 15(1) or 25(4) of the *Family Law (Child Abduction Convention) Regulations 1986*.

Warrants sought for mutual assistance investigations

A warrant can be sought in relation to a mutual assistance investigation if the law enforcement officer:

- is authorised to do so under a mutual assistance authorisation, and
- suspects on reasonable grounds that access to data held in a computer is necessary, in the course of the investigation or investigative proceeding to which the authorisation relates, for the purpose of enabling evidence to be obtained of:
    - the commission of the offence to which the authorisation relates, or
    - the identity or location of the persons suspected of committing the offence.

Warrants sought for integrity operations

A warrant can be sought in the context of an integrity operation if:

- an integrity authority is authorising an integrity operation in relation to an offence by a staff member of a target agency, and
- the federal law enforcement officer suspects on reasonable grounds that access to data held in a computer may assist the conduct of the integrity operation by enabling evidence to be obtained relating to the integrity, location or identity of any staff member of the target agency.

An integrity authority is an authority under Part IAB of the Crimes Act authorising either a controlled operation or an integrity testing operation.

Warrants sought for control orders

Control orders are a protective mechanism under Division 104 of the Criminal Code that allows the AFP to request that a court impose obligations, prohibitions and restrictions (controls) on a person for the purpose of protecting the public from a terrorist attack.

A warrant can be sought in relation to control orders if:

- a control order is in force
- the law enforcement officer suspects on reasonable grounds that access to data held in a computer to obtain information relating to the person would be likely to substantially assist in:
    - protecting the public from a terrorist act
    - preventing the provision of support for, or the facilitation of, a terrorist act
    - preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or
    - determining whether the control order, or any succeeding control order, has been , or is being, complied with.

The language 'law enforcement officer, or another person on his or her behalf' has been used in each provision to allow support staff engaged in the usual course of an investigation to assist or provide services. They are not specified in order to reflect that arrangements may differ between agencies.

Applications for computer access warrants must be supported by an affidavit setting out the grounds on which the warrant is sought. In some circumstances, where immediate access to data is necessary and it is impracticable for an affidavit to be prepared before an application in made, an application may be made before an affidavit is prepared. In those cases, the applicant must send a duly sworn affidavit to a judge or AAT member no later than 72 hours after the making of the application.

The definition of 'target computer' should be read in conjunction with the new definition of 'computer' in the SD Act. While an application for a warrant must identify a target computer, this does not prevent accessing data associated with the target computer on another computer (section 27E). The concept of the target computer is intended to ensure that if an individual has more than one relevant computer, only one warrant will be necessary. For example, there may be multiple computers on the premises and it may only be discovered upon entering that a particular computer is not connected to the anticipated computer system. With the variety of computers and electronic devices now commonly used by individuals, it is highly probable that a person may store data on a number of computers (for example, a laptop, a phone and a tablet).

27B Remote application

New section 27B permits the application for a computer access warrant to be made by telephone, fax, e-mail or by other means of communication where the law enforcement officer believes it is impracticable for the application to be made in person.

27C Determining the application

New section 27C sets out the requirements of which an eligible judge or nominated AAT member must be satisfied before issuing a computer access warrant. New section 27C is modelled on the section 16. The issuing authority must be satisfied that there are reasonable grounds for the suspicion founding the application for the warrant.

For a computer access warrant relating to a control order, in paragraph 27C(1)(e), the judge or AAT member must be satisfied that a control order is in force in relation to the person, and that access to data would likely substantially assist in protecting the public from a terrorist act, or preventing the support or facilitation of a terrorist act, or preventing the support or facilitation of hostile activity in a foreign country, or for determining whether a control order is being complied with. Similarly, in relation to applications made remotely, the eligible judge or AAT member must be satisfied that it was impracticable for the application to have been made in person.

Subsection 27C(2) sets out the considerations to which an issuing authority must have regard in determining whether a computer access warrant should be granted. The issuing authority must have regard to the extent to which the privacy of any person is likely to be affected and the existence of any alternative means of obtaining the evidence or information sought to be obtained. This applies to all matters for which a computer access warrant may be obtained.

For a warrant sought in relation to a relevant offence, the issuing authority must also have regard to the nature and gravity of the alleged offence, the likely evidentiary or intelligence value of any evidence that might be obtained, and any previous warrant sought.

For a warrant sought to assist in the locating and safe recovery of a child, the issuing authority must have regard to the circumstances which gave rise to the making of the order, and to any previous warrant sought.

For a warrant sought in relation to a mutual assistance authorisation, the issuing authority must also have regard to the nature and gravity of the alleged offence, and the likely evidentiary or intelligence value of any evidence that might be obtained but only to the extent that this is possible to determine from information obtained from the foreign country in question.

In determining whether a computer access warrant should be issued for an integrity operation, the issuing authority must have regard to the nature and gravity of the offence, and the likely evidentiary or intelligence value of any evidence or information sought to be obtained.

There are several mandatory considerations in determining an application relating to a control order. They reflect the specifications that must be made in the application under subparagraph 27A(6)(b)(i)-(iv). The issuing authority must also consider the possibility that the person has engaged in a terrorist act, has provided support to or facilitated a terrorist act, has provided support for or facilitation of the engagement in a hostile activity in a foreign country, has contravened a control order, or might do any of these things.

27D What must a computer access warrant contain?

Every computer access warrant, regardless of which offence it is in relation to, must contain the name of the applicant, the date the warrant is issued, either the computer or the premises to which the warrant relates, the period during which the warrant is in force and the name of the law enforcement officer primarily responsible for executing the warrant. If the target computer is, or includes, a computer associated with, used by, or likely to be used by, a person, the warrant must also specify the person, whether by name or otherwise. Although the persons involved in the installation, maintenance or retrieval of a computer access device are not required to be named in the warrant itself, new subparagraph 49(2B)(b)(ii) requires that reports on computer access to the Minister must name each person involved in accessing data under the warrant.

In addition, if the warrant relates to one or more alleged relevant offences, then the warrant needs to specify those. If the warrant relates to a recovery order, the warrant must specify the date the order was made and the name of the child to whom the order relates. If the warrant relates to a mutual assistance authorisation, it must specify the relevant offence or offences against the law of a foreign country. If the warrant is issued for the purposes of an integrity operation, it must specify the integrity authority for the operation and each alleged relevant offence.

Subsection 27D(2) specifies that if a control order access warrant is issued, that warrant must also specify the name of the person subject to the control order, the date the control order was made, and whether the control order is an interim order or a confirmed control order.

Subsection 27D(3) provides that a computer access warrant may only be issued for a period of no more than 90 days, and no more than 21 days if it relates to an integrity operation.

Subsection 27D(4) provides that where a warrant authorises the use of a computer access device on a vehicle, the warrant need only specify a class of vehicle, thus minimising the risk of computer access being thwarted by frequent vehicle changes. The warrant may specify, for example, ‘a vehicle used by a specific person’, and this would be classified as a class of vehicle.

27E What a computer access warrant authorises

A computer access warrant must authorise the doing of specified things in relation to the relevant target computer. The use of ‘must authorise’ differs from the current section 18 of the SD Act which uses the term ‘may authorise’ simply because a surveillance device warrant is structured to be issued around a premises, a specified object or in respect of conversations. These location distinctions are not relevant to a computer access warrant which has as its target object the computer itself, rather than an indistinct surveillance outcome which could require a device being placed in a variety of ways.

Subsection 27E(2) sets out the things that may be specified provided the eligible judge or nominated AAT member considers it appropriate in the circumstances. As distinct from the previous paragraph, the word ‘may’ is used to clarify that all of the following particulars in paragraphs 27E(2)(a)-(i) are not required in every circumstance.

Paragraph 27E(2)(a) lists entering specified premises for the purposes of doing the things mentioned in this subsection. Installation and retrieval of computer access devices may not always be performed remotely, and may involve some entry onto property.

Paragraph 27E(2)(b) makes it clear that premises other than the premises specified in a warrant (that is, third party premises) can be entered for the purpose of gaining access to or exiting the subject premises for the purposes of executing the computer access warrant. This may be because there is no other way to gain access to the subject premises (for example, in an apartment complex where it is necessary to enter the premises through shared or common premises). It may also occur where, for operational reasons, the best means of entry might be through adjacent premises (for example, where entry through the main entrance may involve too great a risk of detection). The need to access third party premises may also arise due to 'emergency' and unforeseen circumstances (for example, where a person arrives at the subject premises unexpectedly during a search and it is necessary to exit through third party premises to avoid detection).

Paragraph 27E(2)(c) lists using the target computer, using a telecommunications facility operated or provided by the Commonwealth or a carrier, using any other electronic equipment or using a data storage device, for the purpose of obtaining access to data that is held in the target computer at any time while the warrant is in force, in order to determine whether the relevant data is covered by the warrant. This is to ensure that data that is unknown or unknowable at the time the warrant has been issued can be discovered by using other means, in order to determine whether it is covered by the warrant. Access to a secondary device, such as a USB for example, may also be necessary to determine whether any data relevant to an investigation is held on the target computer. This would include access to any external storage devices, such as cloud-based data or any back-ups on other devices. Other electronic equipment might also include specialist communications equipment used within telecommunications transmittal devices.

The words 'held in the target computer at any time while the warrant is in force' means that computer access warrants authorise ongoing access to data held in the target computer over the life of the warrant. Data does not have to be stored on the target computer but can be passing through it.

Paragraph 27E(2)(d) lists adding, copying, deleting or altering other data in the target computer if necessary to achieve the purpose mentioned in paragraph (c). Data may need to be copied and analysed before its relevancy or irrelevancy is determined.

Paragraph 27E(2)(e) lists using any other computer or a communication in transit to access relevant data if it is reasonable in all the circumstances, having regard to other methods of obtaining access to the data. If necessary to achieve that purpose, paragraph (e) allows adding, copying deleting or altering other data in the computer or the communication in transit. This ensures that law enforcement agencies can effectively use a third party computer or a communication in transit. Accessing a communication in transit means accessing any communication passing over a telecommunications network, between the target device and the service provider, as long as this access does not amount to interception. Whether access to a communication in transit is interception or not is dependent on what material could be or is gleaned from the action. Collecting contextual data which indicates a person's use of a computer would not constitute interception, whereas accessing the content of a person's communications would amount to interception. Permissible interception is provided for in paragraph 27E(2)(h).

The power to add, copy, delete or alter other data can only be used where necessary for the purpose of obtaining access to relevant data held in the target computer. This provision recognises that in some cases direct access to a target computer will be difficult or even impossible. The use of third party computers and communications in transit to add, copy, delete or alter data in the computer or the communication in transit may facilitate that access.

In recognition of the privacy implications for third parties, in authorising the warrant the judge or nominated AAT member must have regard to any other method of obtaining access to the relevant data which are likely to be as effective as accessing a third party's computer. This does not require all other methods of access to be exhausted, but rather takes into account the circumstances as a whole, including balancing the risk of intrusion upon privacy with the risk of detection.

Paragraph 27E(2)(f) allows the removal of a computer or other thing from the premises for the purposes of executing the warrant, and the returning of the computer or other thing once it is no longer required. This includes the removal, for example of a USB key, a remote access token, or a password written on a piece of paper, from the premises, along with the computer.

Paragraph 27E(2)(g) allows the copying of any data which has been accessed if it either: appears relevant for the purposes of determining whether the relevant data is covered by the warrant, or is covered by the warrant. Data that is subject to some form of electronic protection is taken to be relevant for the purposes of determining whether it is relevant data covered by the warrant (subsection 27E(3)). These provisions ensure that data either accessed on a computer remotely or accessed on a computer at the premises specified in the warrant can be copied onto another computer. This will be necessary in order for data to be analysed on a different computer located elsewhere or using different software. It will also be necessary for the collection of evidence.

Paragraph 27E(2)(h) permits intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing anything specified in the warrant in accordance with 27E(2). Often it will be necessary for a law enforcement agency to intercept communications for the purposes of executing a computer access warrant. This subsection ensures that they will be able to do so, but only for those purposes of making computer access practicable or technically possible.

A computer access warrant cannot authorise the collection of evidence by interception for an investigation into an offence under the TIA Act. If agencies require interception other than to facilitate a computer access warrant, they must seek an interception warrant from an eligible issuing authority under the TIA Act.

Paragraph 27E(2)(i) allows a computer access warrant to authorise the doing of anything reasonably incidental to any of the things specified in paragraphs 27E(2)(a) to (h).

When data is covered by a warrant

Subsection 27E(4) is a clarifying provision that reiterates the thresholds in section 27A which must be met before a law enforcement officer may apply for a computer access warrant.

Certain acts not authorised

Subsection 27E(5) mirrors subsection 25A(5) of the ASIO Act. A computer access warrant does not authorise the addition, deletion or alteration of data, or the doing of any thing that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to the limitation has been included so that an agency may undertake such actions where they are otherwise necessary to execute the warrant.

A computer access warrant cannot be used to disrupt or deny a service to a computer, even where that computer is being used for illegal purposes. Computer access warrants are evidence-gathering tools and are not intended to enable agencies to engage in disruption, or any activities which would generally be beyond the functions of such agencies.

However, subsection 27E(7) does permit an agency to do that which is necessary in order to conceal the fact that any thing has been done under the warrant or under that subsection. This may include, for example, forcing a device to do a thing that disrupts its operation in order to conceal things done under the warrant.

Warrant must provide for certain matters

Under subsection 27E(6) a computer access warrant must authorise the use of force against persons or things that is necessary and reasonable to do the things specified in the warrant. Any unauthorised use of force against a person that does not comply with these requirements may attract criminal and civil liability. If the warrant authorises entry onto premises, then the warrant must state whether entry is authorised to be made at any time, or during a set period of time.

Concealment of access etc.

Subsection 27E(7) provides that a computer access warrant will also authorise the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to a computer under a computer access warrant. Subsection 18(4) of the SD Act provides a similar provision in relation to surveillance device warrants. Likewise, under paragraph 25A(4)(c) of the ASIO Act, an ASIO computer access warrant authorises the doing of any thing reasonably necessary to conceal the fact that any thing has been done under the warrant.

Concealment of access is essential for preserving the effectiveness of covert warrants under the SD Act.

Paragraphs 27E(7)(d) and (e) also authorise the entering of premises where the computer that has been accessed is located, or premises for gaining entry or access to where the computer is located, for the purposes of concealing the action that has been taken.

Paragraph 27E(7)(f) authorises removing the computer or another thing from any place where it is situated, and returning it, for the purposes of concealing access. The ability to temporarily remove a computer from the premises is important in situations where an agency may have to use specialist equipment to access the computer but cannot for practical reasons bring that equipment onto the premises in a covert manner.

In some instances it will be necessary to retrieve a physically implanted computer access device from a computer in order for the access to be concealed. Doing anything reasonably necessary for concealment as envisaged by paragraph 27E(7)(c) includes retrieving such a device.

Although there is a separate retrieval framework for surveillance devices upon expiry of a surveillance device warrant in the SD Act, retrieval provisions for computer access follows the structure of section 25A of the ASIO Act. This structure acknowledges the importance of ensuring that agencies have the ability to determine when access to premises or to a planted device will best ensure the operation remains covert. It will not always be possible to predict when safe retrieval of a device can be performed without compromising an investigation.

Paragraph 27E(7)(g) allows using another computer or communication in transit to conceal activities under a warrant, and if necessary adding, copying, deleting or altering other data in the computer or the communication in transit. However, this must be reasonable in all the circumstances, having regard to other methods of concealment.

Paragraph 27E(7)(h) allows the interception of a communication if it is for the purposes of concealment.

Paragraph 27E(7)(i) allows anything reasonably incidental to paragraphs (c) to (h). This will enable concealment activities to be executed smoothly.

Paragraph 27E(7)(k) allows the above concealment activities to be done at any time while the warrant is in force, or within 28 days after it ceases to be in force, or at the earliest time after this period at which it is reasonably practicable to do so.

The period of time provided to perform these concealment activities recognises that, operationally, it is sometimes impossible to complete this process within 28 days of a warrant expiring. The requirement that the concealment activities be performed ‘at the earliest time after the 28-day period at which it is reasonably practicable to do so’ acknowledges that this authority should not extend indefinitely, circumscribing it to operational need.

27F Extension and variation of computer access warrant

An officer may apply at any time while the warrant is in place for an extension of the warrant or a variation of its terms. This builds flexibility into the warrant process and accounts for extended investigations and unexpected circumstances.

The application must be made to an eligible judge or nominated AAT member. The judge or member must consider the same matters required to issue computer access warrants at first instance (see subsection 27C(2)) and be satisfied that the grounds on which the application for the warrant was made still exist (see subsection 27C(1)).

The provisions that apply to computer access warrants apply to varied or extended computer access warrants. This ensures that any varied specifications are within the bounds of what might have been authorised in the computer access warrant at first instance. For example, a varied computer access warrant may specify any of the list of things in subsection 27E(2). The warrant cannot authorise the addition, deletion or alteration of data that interferes with a person’s use of a computer unless it is for the purposes of the warrant.

An application for extension may be made more than once.

This section does not prevent the issue of a further warrant in relation to the same investigation, applied for under section 27A.

27G Revocation of computer access warrant

A computer access warrant may be revoked by an eligible judge or nominated AAT member. If the warrant is revoked and the officer is already in the process of executing the warrant, the officer does not have any civil or criminal liability for actions done before he or she was made aware of the revocation.

The chief officer of the law enforcement agency to which the warrant was issued must revoke the warrant if satisfied that the warrant is no longer required for the purpose of enabling evidence to be obtained of the commission of the relevant offence for which it was obtained originally, or enabling evidence of the identity or location of the offender.

27H Discontinuance of access under warrant

Subsection 27H(2) places an obligation on the chief officer of a law enforcement agency to take steps to discontinue computer access where he or she is satisfied that the grounds on which a computer access warrant, issued in relation to a relevant offence, have ceased to exist. For example, the alleged offender may be in custody, so there would be no need to collect evidence of the location of the offender. Similarly, under subsection 27H(3) if the warrant was sought in relation to the recovery of a child and the chief officer of the agency is satisfied that the use of computer access to recover the child is no longer necessary, the chief officer must revoke the warrant. Subsection 27H(4) has the same effect but in relation to warrants sought for a mutual assistance authorisation. Subsection 27H(5) deals with integrity operations, and subsection 27H(6) relates to warrants sought for a control order.

Subsections 27H(7) and 27H(8) complement section 27G in that the chief officer must, if made aware that an issuing authority has revoked the warrant or a control order is no longer in force, take steps to discontinue computer access.

Subsections 27H(9) and 27H(10) places an obligation on the law enforcement officer who is primarily responsible for executing the warrant to immediately inform the chief officer. This person will be in many cases the officer to whom the warrant was issued under section 27C and who made the application under section 27A. However, as a person may apply for a warrant on behalf of the law enforcement officer, this may not always be the case. There may also be staffing and organisational changes during the period the warrant is in place. Subsections 27H(9) and 27H(1) also recognise that there may be multiple people working on the execution of a particular warrant, by obligating the person deemed primarily responsible. This position has not been legislated because agencies frequently structure investigations differently.

After subsection 28(1)

This item amends the emergency authorisation provisions in the SD Act to allow law enforcement officers to apply to an appropriate authorising officer (usually the head of the agency or deputy-head of the agency – see section 6A) for access to data held in computers in the course of an investigation of a relevant offence. New subsection 28(1A) provides that the law enforcement officer must suspect that there is an imminent risk of serious violence or substantial property damage, that access to the data in the target computer is immediately necessary for dealing with that risk, that the circumstances are so serious and the matter is so urgent that access to that data is warranted, and that it is not practicable to apply for a computer access warrant.

Subsections 28(2), (3) and (4)

This item amends subsections 28(2), (3) and (4) to account for the addition of subsection 28(1A) regarding emergency authorisations made for access to data in a computer where there is a serious risk to person or property.

Under subsection 28(2), a police officer of a State or Territory cannot apply for an emergency authorisation for State offences with a federal aspect as such offences are not included as a ‘relevant offence’ for the purposes of section 28. Thus, a police officer of a State or Territory can only apply for emergency authorisations to investigate Commonwealth offences.

Under subsection 28(3), such an application may be made orally, in writing, by telephone, email or fax or any other means of communication.

Subsection 28(4) provides that, if the appropriate authorising officer is satisfied that there are reasonable grounds supporting the officer’s suspicion of the matters in subsection 28(1), the authorising officer may give an emergency authorisation.

After subsection 29(1)

This item amends the emergency authorisation provisions in the SD Act to allow law enforcement officers to apply to an appropriate authorising officer (usually the head of the agency or deputy-head of the agency – see section 6A) for access to data held in computers in urgent circumstances relating to a recovery order. New subsection 29(1A) provides that the officer must suspect that the circumstances are so urgent as to warrant the immediate use of access to data held in the target computer.

The circumstances must also be such that it is not practicable to apply for a computer access warrant. The threshold in relation to a recovery order is slightly lower than for an investigation related to a relevant offence. There are three tests to satisfy in this instance because of the urgency and seriousness inherent in recovering a child.

Subsections 29(2) and (3)

This item amends subsections 29(2) and (3) to account for the addition of subsection 29(1A) regarding emergency authorisations made for access to data in a computer where there are urgent circumstances relating to a recovery order.

To issue an emergency authorisation, the authorising officer must be satisfied that there are reasonable grounds supporting the officer's suspicion that such an authorisation is required.

Under subsection 29(2), an application under this section is able to be made orally, in writing, by telephone, fax, email or other means of communication.

After subsection 30(1)

This item enables emergency authorisations to be made in regard to access to data held in a computer where there is a risk of loss of evidence. The provisions match the existing requirements and powers available for surveillance device emergency authorisations where there is a risk of loss of evidence under section 30.

A law enforcement officer will be able to apply for an emergency authorisation in the conduct of an investigation for offences specified in subsection 30(1A) where that law enforcement officer reasonably suspects that the access to data in a computer is immediately necessary to prevent the loss of any evidence that is relevant to the investigation of the specific offence. The suspicion must be that the circumstances are so serious and the matter is of such urgency that access to data held in a computer is warranted and that it is not practical to apply for a computer access warrant.

The offences in subsection 30(1A) are given special provision in the Act as the Government recognises the seriousness of these offences and/or the difficulty of obtaining evidence of their commission.

Subsection 30(2)

This amendment also ensures that applications for an emergency authorisation made for access to data in a computer can be made orally, in writing, by telephone, fax, email or any other means of communication.

Subsection 30(3)

This item is consequential.

At the end of section 30

This item provides that an appropriate authorising officer may give an emergency authorisation in relation to the conduct of an investigation into a specified offence set out in subsection 30(1A), where the authorising officer is satisfied that the investigation is being conducted into an offence under subsection 30(1A), and there are reasonable grounds for the law enforcement officer's suspicion that access to data in a computer is necessary to prevent the loss of relevant evidence, the matter is serious and urgent and applying for a computer access warrant under the normal circumstances is not practicable.

Subsections 32(1) and (2)

This item is consequential.

After subsection 32(2)

New subsection 32(2A) provides that an emergency authorisation may authorise anything that a computer access warrant authorises. This mirrors the subsection 32(2), which applies to surveillance devices.

After subsection 32(2A)

New subsection 32(3A) provides that a law enforcement officer may only access data held in a computer if he or she is acting in performance of his or her duty. This mirrors subsection 32(3), which applies to surveillance devices.

Subsection 33(2)

This item is consequential.

After subsection 33(2)

New subsection 33(2A) provides that an application for an emergency authorisation for access to data held in a computer must specify the name of the applicant for the approval, and if a warrant is sought, the nature and duration of the warrant. The authorisation must be supported by an affidavit stating grounds for issue and be accompanied by a copy of the written record made under section 31 of the SD Act.

This mirrors subsection 33(2), which applies to surveillance devices.

Subsection 34(1)

This item is consequential.

After subsection 34(1)

New subsection 34(1A) sets out the considerations that a judge or nominated AAT member must take into account before deciding whether to approve an emergency authorisation for computer access issued by an appropriate authorising officer under new subsection 28(1A), in circumstances where the law enforcement officer reasonably suspects that there is an imminent risk of serious violence to a person or substantial damage to property.

The judge or nominated AAT member must, being mindful of the intrusive nature of accessing data held in a computer, turn his or her mind to the following factors:

- the nature of the risk of serious violence to a person or substantial damage to property
- the extent to which issuing a computer access warrant would have helped reduce or avoid the risk
- the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk
- how much the use of such methods would have helped reduce or avoid the risk
- how much the use of such methods would have prejudiced the safety of the person or property because of delay or for another reason, and
- whether or not it was practicable in the circumstances to apply for a computer access warrant.

In considering these factors, the judge or member stands in the shoes of the appropriate authorising officer at the time he or she made the decision to issue the emergency authorisation in light of the information that was available to them at the time of that decision. In this way, the judge or member determines whether accessing data held in a computer without court approval was justified at the time, given the information that was before the appropriate authorising officer.

This subsection is similar to subsection 34(1), which sets out the considerations that must be taken into account before a judge or member may approve emergency authorisation for the use of a surveillance device, in circumstances where the law enforcement officer reasonably suspects that there is an imminent risk of serious violence to a person or substantial damage to property.

Subsection 34(2)

This item is consequential.

After subsection 34(2)

New subsection 34(2A) sets out the considerations that a judge or nominated AAT member must take into account before deciding whether to approve an emergency authorisation for computer access issued by an appropriate authorising officer under new subsection 29(1A), where a recovery order is in force.

The judge or nominated AAT member must, being mindful of the intrusive nature of accessing data held in a computer, turn his or her mind to the following factors:

- the urgency of enforcing the recovery order
- the extent to which accessing data would assist in the location and safe recovery of the child to whom the order relates
- the extent to which law enforcement officers could have used alternative methods to assist in the location and safe recovery of the child
- how much the use of such methods might have prejudiced the effective enforcement of the recovery order, and
- whether or not it was practicable in the circumstances to apply for a computer access warrant.

In considering these factors, the judge or member stands in the shoes of the appropriate authorising officer at the time he or she made the decision to issue the emergency authorisation in light of the information that was available to them at the time of that decision. In this way, the judge or member determines whether accessing data held in a computer without court approval was justified at the time, given the information that was before the appropriate authorising officer.

This subsection is similar to subsection 34(2), which sets out the considerations that must be taken into account before a judge or member may approve emergency authorisation for the use of a surveillance device, where a recovery order is in force.

Subsection 34(3)

This item is consequential.

At the end of section 34

New subsection 34(4) sets out the considerations that a judge or nominated AAT member must take into account before deciding whether to approve an emergency authorisation for computer access issued by an appropriate authorising officer under new subsection 30(1A), in circumstances where the law enforcement officer is conducting an investigation into specified Commonwealth offences.

The judge or nominated AAT member must, being mindful of the intrusive nature of accessing data held in a computer, turn his or her mind to the following factors:

- the nature of the risk of the loss of evidence
- the extent to which issuing a computer access warrant would have helped reduce or avoid the risk
- the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk
- how much the use of such methods would have helped reduce or avoid the risk, and
- whether or not it was practicable in the circumstances to apply for a computer access warrant.

In considering these factors, the judge or member stands in the shoes of the appropriate authorising officer at the time he or she made the decision to issue the emergency authorisation in light of the information that was available to them at the time of that decision. In this way, the judge or member determines whether accessing data held in a computer without court approval was justified at the time, given the information that was before the appropriate authorising officer.

This subsection is similar to subsection 34(3), which sets out the considerations that must be taken into account before a judge or member may approve emergency authorisation for the use of a surveillance device, in circumstances where the law enforcement officer is conducting an investigation into specified Commonwealth offences.

Section 35 (heading)

This item makes a consequential amendment to reflect the inclusion of new section 35A, which allows a judge or nominated AAT member to approve emergency authorisation for access to data held in a computer. The item clarifies that existing section 35 allows a judge or nominated AAT member to approve emergency authorisation for the use of a surveillance device.

Subsection 35(1)

This item is consequential.

Subsection 35(2)

This item is consequential.

Subsection 35(3)

This item is consequential.

35A Judge or nominated AAT member may approve giving of an emergency authorisation for access to data held in a computer

New subsection 35A sets out the conditions on which an eligible judge or nominated AAT may approve an emergency authorisation in relation to investigating relevant offence (subsection 35A(1)), enforcing a recovery order (subsection 35A(2)) or preventing the loss of evidence (subsection 35A(3)).

Before approving an emergency authorisation in relation to investigating a relevant offence, the eligible judge or nominated AAT member must be satisfied of the grounds underlying the emergency authorisation. He or she must be satisfied that at the time the authorisation was given:

- there was a risk of serious violence to a person or substantial damage to property
- accessing data held in the target computer may have helped reduce the risk, and
- it was not practicable in the circumstances to apply for a computer access warrant.

Similarly, before approving an emergency authorisation for the purposes of enforcing a recovery order, the eligible judge or nominated AAT member must be satisfied that:

- there was a recovery order in force at the time the authorisation was given, and
- reasonable grounds existed to suspect that:
    - the enforcement of the recovery order was urgent
    - accessing data held in the target computer may have assisted in the prompt location and safe recovery of the child, and
    - it was not practicable in the circumstances for a law enforcement officer to apply for a computer access warrant.

Before approving an emergency authorisation to prevent the loss of evidence, the eligible judge or nominated AAT member must be satisfied that:

- reasonable grounds existed to suspect that:
    - there was a risk of loss of evidence
    - accessing data held in the target computer may have helped reduce that risk, and
- it was not practicable in the circumstances for a law enforcement officer to apply for a computer access warrant.

If the eligible judge or nominated AAT member approves an emergency authorisation for computer access, he or she may issue a computer access warrant or, if access to data is no longer required, order that access cease.

If the eligible judge or nominated AAT member does not approve an emergency authorisation for computer access, he or she may order that access to data cease or, if computer access was not warranted at the time of the authorisation but is currently justified, issue a computer access warrant.

In any case, the eligible judge or nominated AAT member may order that any information obtained from or relating to the exercise of powers under an emergency authorisation or any record of that information be dealt with in a manner specified in the order. The judge or member may not order that such information be destroyed because such information, while improperly obtained, may still be required for a permitted purpose, such as an investigation. Part 6 of the Act governs what can be done with such information.

Section 36

This item is consequential.

Section 41 (definition of appropriate consenting official)

This item repeals and substitutes the definition of ***appropriate consenting official*** so that it means an official of a foreign country with the authority to give consent to either the use of surveillance devices in that country or on a vessel or aircraft of that country, or to access to data held in computers in that country or on a vessel or aircraft.

Section 42 (heading)

This item is consequential, limiting the application of section 42 to surveillance device warrants. Sections 43A and 43B provide for extraterritorial operation of computer access warrants

Subsection 42(1)

This item is consequential.

After paragraph 42(2)(a)

This item is consequential.

After paragraph 42(2)(b)

This item is consequential.

Subsection 42(2)

This item is consequential.

Paragraph 42(3)(a)

This item is consequential.

Subsections 42(6) and (9)

This item is consequential.

43A Extraterritorial operation of computer access warrants

Part 5 of the SD Act provides for how surveillance device warrants operate extraterritorially. If in the course of an investigation a law enforcement agency needs to place a surveillance device in a foreign country or on a vessel or aircraft beyond Australia's territorial waters that is registered under the law of a foreign country, the agency must have the permission of a foreign official of that country. This only applies to federal law enforcement officers. State and Territory officers may not engage in extraterritorial surveillance (section 42). In this way, extraterritorial surveillance is carried out under an Australian warrant, with the agreement of the

foreign State, which ensures that such surveillance is subject to appropriate accountability and probity measures under domestic law.

The same principle will apply to access to data held in a computer in a foreign country or on a vessel or aircraft that is registered under the law of a foreign country and is in waters beyond Australia's territorial sea. The law enforcement officer conducting the investigation would have to seek the consent of an appropriate foreign official in order for the warrant to be granted.

If a computer access warrant has already been granted by the issuing authority and during the course of executing that warrant it becomes apparent that there will be a need for access to data held in a computer in a foreign country (or on a foreign vessel or aircraft) the warrant is taken to permit that access if the access has been agreed to by an appropriate consenting official of the foreign country. This means that a law enforcement officer does not need to seek a further warrant, or a change in the warrant conditions from the issuing authority, as long as consent from the foreign official has been granted.

For clarity, the application of computer access warrants extraterritorially to vessels registered under the law of a foreign country is not intended to conflict with sovereign immunity that is provided, for example, to visiting warships of a foreign nation.

In the course of computer access, authorised by an emergency authorisation, the law enforcement officer will have to seek a warrant from an eligible judge or AAT member upon determining that access to data held in a computer in a foreign country will be necessary. The judge or AAT member cannot issue the warrant unless satisfied that the access has been agreed to by an appropriate consenting official of the foreign country.

The chief officer of the law enforcement agency that applied for the warrant must give the Minister written evidence that the surveillance has been agreed to by an appropriate consenting official of the foreign country. The chief officer is to provide this evidence of consent as soon as practicable after the access to data has commenced under a warrant in a foreign country or on a foreign vessel or aircraft where such consent is required. An instrument providing evidence to the Attorney-General is not a legislative instrument. It is administrative rather than legislative in character. It does not determine or alter the law but instead is an instrument relating to a specific situation and serving a specific operational purpose.

In some instances the consent of a foreign official is not required notwithstanding the fact that the data may be held in a computer offshore. Where the person executing the warrant is physically present in Australia and the location of the data is unknown, or cannot reasonably be determined, the consent of a foreign official is not required. Persons of interest to law enforcement may use email accounts and messaging platforms provided by technology companies with international reach. The data associated with these services is increasingly stored in offshore data centres. Data about one account may be held in multiple data centres at any one time and data may move between different centres. Sometimes data may only be held in one place for a days or a few hours. This frequently makes the location of data unknowable or indeterminable.

43B Evidence obtained from extraterritorial computer access not to be tendered in evidence unless court satisfied properly obtained

Information which is obtained from accessing data held in a computer offshore cannot be tendered as evidence in court unless the court is satisfied that the consent was agreed to by an appropriate consenting official. An appropriate consenting official means an official of a foreign country with the authority to give consent to either the use of surveillance devices in that country or on a vessel or aircraft of that country, or to access data held in computers in that country or on a vessel or aircraft.

Subsection 44(1) (after paragraph (a) of the definition of protected information)

Information which is obtained from accessing data either under a computer access warrant or under an emergency authorisation for access to data is included in the definition of ***protected information***. This means that the use of this information is restricted in Part 6 of the Act. Information obtained under a surveillance device is also protected.

There are no amendments to section 45, which contains the prohibitions on use, recording, communication or publication of protected information. As section 45 refers to 'protected information' as listed in section 44, it is not necessary to amend that section.

Section 45 contains two offences. Under subsection 45(1) a person cannot use, record, communicate, publish or admit into evidence protected information that does not fall into any of the exceptions in section 45. The penalty for doing so is a maximum of 2 years imprisonment. Subsection 45(2) is a more serious offence where dealing with the information endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence. The penalty is a maximum penalty of 10 years imprisonment.

Subsection 44(1) (at the end of subparagraph (d)(iii) of the definition of protected information)

This item is consequential.

Subsection 44(1) (after subparagraph (d)(iii) of the definition of protected information)

Where information has been obtained through access to data held in a computer in a foreign country, or on a vessel or aircraft of a foreign country, without the agreement of a consenting official, that information is classified as protected information.

Subsection 44(1) (after subparagraph (d)(iii) of the definition of protected information)

This item adds a note pointing to Part 2-6 of the TIA Act, which contains protections for general computer access intercept information.

Section 46 (heading)

This item is a consequential amendment to section 46 in order to reflect the inclusion of computer access warrants within the SD Act.

Section 46(2)

This item is consequential.

After subsection 46A(1)

New subsection 46A(1A) contains the requirements for a record or report obtained from access to data relating to a control order warrant to be destroyed where the information has been obtained before a control order came into force. If the chief officer of an agency is satisfied that the information is no longer likely to assist in connection with the protection of the public from a terrorist act, preventing the provision of support for or the facilitation of a terrorist act, or preventing the provision of support for or facilitation of engagement in a hostile activity in a foreign country, he or she must cause the record or report to be destroyed as soon as practicable.

Subsection 46A(2)

This item is consequential.

47A Protection of computer access technologies and methods

New section 47A gives protection to sensitive information relating to computer access technologies and methods in order to prevent its release into the public domain. Releasing such information could harm future capabilities and investigations. Section 47 is a protection additional to other statutory protections such as public interest immunity. Section 47A replicates section 47, which provides protections for surveillance technologies and methods. This section is intended to protect technologies that develop over time and not to limit law enforcement agencies with an exhaustive list.

Subsection 47A(1) provides that a person may object to the disclosure of information on the ground that the information could reasonably be expected to reveal details of computer access technologies or methods. It is not intended for section 47A to give protection to simple aspects of computer access, such as the action of

turning on a computer or the fact that a computer was turned on. The section is for sensitive technologies and methods that need to be closely held. However these are not excluded explicitly from section 47A because it is within the discretion of the person presiding over the proceeding whether that information is of sufficient sensitivity (subsection 47A(2)).

Subsection 47A(3) obliges the person presiding over the proceeding to take into account whether disclosure of the information is necessary for the fair trial of the defence and whether it is in the public interest. This ensures that the availability of capability protection for law enforcement is not absolute. The public interest in protecting sensitive operational and capability information must be weighed against the defendant's right to a fair trial and other public interest concerns.

Subsection 47A(4) is a saving provision which provides that this section does not affect any other law under which a law enforcement officer cannot be compelled to disclose information or make statements in relation to the information.

Subsection 47A(5) requires the person presiding over the proceeding to make any order he or she considers necessary if satisfied that publication of any information disclosed could reveal computer access technologies or methods. This does not apply if doing so would conflict with the interests of justice (subsection 47A(6)). It is appropriate to protect this information without proving harm or the disclosure would be contrary to the public interest. It is assumed that disclosure is inherently harmful. Law enforcement capabilities are fundamental to ongoing investigations and their ability, including over the long-term, to protect essential public interests, including national security and public safety.

Computer access technologies or methods means technologies or methods relating to using a computer, a telecommunications facility, any other electronic equipment, or a data storage device, for the purposes of obtaining access to data, or for adding, copying, deleting or altering other data in a computer. These activities must have been deployed in giving effect to a warrant or an emergency authorisation.

Proceeding includes a proceeding before a court, tribunal or Royal Commission.

Subsection 49(2)

This item is consequential.

After subsection 49(2A)

New subsection 49(2B) provides the reporting requirements relating to computer access warrants and emergency authorisations. There is no amendment to subsection 49(1) as the current language would apply to computer access warrants and emergency authorisations granted for computer access. That subsection states that the chief officer of a law enforcement agency must make a report to the Minister and give a copy of each warrant and authorisation to the Minister.

The report must state whether the warrant or authorisation was executed, the name of the person primarily responsible for the execution, the name of each person involved in accessing data, the name of any person whose data was accessed, and the location at which the computer was located. The report must also give details of how the accessed data benefited the investigation of a relevant offence, child recovery operation or integrity operation (as applicable to the grounds of the warrant application).

Where the computer warrant is a control order access warrant, the report must detail the use to be made of any evidence or information obtained by accessing data and the benefit of accessed data in:

- protecting the public from a terrorist act
- preventing the provision of support for, or the facilitation of, a terrorist act
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or
- determining whether a control order has been or is being complied with.

The report must also detail the general use to be made of any evidence or information obtained by accessed data.

The reporting requirements recognise that accessing a person's data under a computer access warrant is a privacy intrusive measure which requires proportionate safeguards.

Subsection 49A(1)

Within six months after a warrant for computer access relating to a control order is issued, the chief officer of the agency must notify the Commonwealth Ombudsman that the warrant has been issued and must give the Commonwealth Ombudsman a copy of the warrant.

Paragraph 49A(2)(a)

If any conditions in a control order access warrant are contravened, the chief officer of the relevant agency must notify the Commonwealth Ombudsman of that contravention as soon as practicable.

After paragraph 49A(2)(b)

If the chief officer of the law enforcement agency fails to revoke a control order warrant once it is no longer required (therefore contravening subsection 27G(2)), the chief officer of the relevant agency must notify the Commonwealth Ombudsman as soon as practicable.

After paragraph 49A(2)(c)

If a law enforcement officer uses, records, communicates or publishes protected information obtained under a control order access warrant (therefore committing an offence under section 45), the chief officer of the agency must notify the Commonwealth Ombudsman of that contravention as soon as practicable.

If a law enforcement officer fails to keep in a secure place or destroy information obtained under a control order access warrant as required under section 46(1), the chief officer of the relevant agency must notify the Commonwealth Ombudsman as soon as practicable.

Subsection 49A(3)

A failure to report to the Commonwealth Ombudsman on the issuing of a control order access warrant or about a contravention of a control order access warrant does not affect the validity of that warrant.

Paragraphs 50(1)(g)(h) and (i)

The annual reporting requirements in the SD Act apply to computer access warrants and authorisations.

Under section 50, agencies must report on the number of warrants applied for and issued during the year and the number of emergency authorisations. The report must also specify the number of warrants and authorisations that were refused in the year and the reasons for their refusal. The report is to be submitted to the Minister as soon as practicable, within a three month period, following the end of each financial year (subsection 50(3)).

Paragraph 50(1)(j)

The annual report must include any other information relating to access to data held in computers that the Minister considers appropriate.

Subsection 50A(6) definition of control order information

This item repeals the definition of ***control order information*** and substitutes a definition which takes into account the new computer access powers in the Act. In so far as it relates to computer access, control order information includes information that, if made public, could lead a reasonable person to conclude that a control order access warrant authorising access to data is in force.

Paragraph 51(b)

Instruments revoking computer access warrants under subsection 27G(4) must be kept by law enforcement agencies.

Copies of computer access warrants (including any variations) and applications for emergency authorisation must also be kept by agencies. However, no amendments to section 51 of the SD Act are required to give

effect to this, as the current language would apply to computer access warrants and emergency authorisations.

Paragraphs 52(1)(e), (f), (g) and (h)

Section 52 lists the other records that the chief officer of an agency is required to ensure are kept. They relate to the decision to grant, refuse or withdraw warrants and authorisations, as well as the use and communication of information obtained. Subsection 52(1) is amended to provide that the chief officer of a law enforcement agency must cause to be kept this information relating to computer access.

Paragraph 52(1)(j)

Details of destruction of records or reports relating to computer access must also be kept.

After subparagraph 53(2)(c)(iiic)

Section 53 requires agencies to maintain a register of warrants and authorisations. The purpose of the register is to provide an overview for the Commonwealth Ombudsman when inspecting such records under Division 3 of the Act. This item ensures that control order access warrants kept on the register include the date the control order was made.

At the end of subsection 62(1)

New paragraph 62(1)(c) ensures that an appropriate authorising officer, or a person assisting him or her, may issue a written certificate setting out the facts relevant with respect to the communication, using or recording information obtained from access to data.

An appropriate authorising officer, or a person assisting him or her, may also issue a written certificate setting out the facts of what has been done by the law enforcement officer or a person providing technical expertise in connection with the execution of the warrant or the emergency authorisation. However, no amendments to subsection 61(1) of the SD Act are required to give effect to this, as the current language would apply to computer access warrants and emergency authorisations.

Evidentiary certificates are intended to streamline the court process by reducing the need to contact numerous officers and experts to give evidence on routine matters. Evidentiary certificates also assist agencies to protect sensitive capabilities.

Subsection 62(3)

This is a consequential amendment to take into account new emergency authorisations for access to data. Subsection 62(3) provides that evidentiary certificates are not admissible in evidence in any proceedings to the extent the certificate sets out facts with respect to an emergency authorisation unless the authorisation has been approved.

64A Person with knowledge of a computer or a computer system to assist access etc.

A law enforcement officer may apply to an eligible judge or AAT member for an order requiring a specified person to provide any information or assistance is that reasonable and necessary to allow the law enforcement officer to access data held in a computer subject to a computer access warrant. This provision is similar to section 3LA of the Crimes Act, which allows a constable to apply to a magistrate for an order requiring a person to provide assistance where a search warrant is in place.

This item ensures that law enforcement agencies that have a warrant for computer access will be able to compel assistance in accessing devices. Although the SD Act provides for the issuing of warrants permitting covert activity, there may be circumstances in the course of an investigation where a person who is not the suspect or target will have knowledge of a computer system and be able to provide access to relevant data, without compromising the covert nature of the investigation. Alternatively, there may be a point in the investigation where the benefits of compelling information from a person in order to enable access to data outweigh the disadvantages of maintaining the secrecy of the investigation.

There are limits to when an eligible judge or AAT member may grant the assistance order. Where the order relates to a computer access warrant or authorisation with respect to a relevant offence, the judge or AAT member must be satisfied that there are reasonable grounds for suspecting that access to data is necessary in the course of the investigation to enable evidence of the commission of the offences or the identity or location of the offenders. The judge or AAT member must be satisfied that the person specified in the order is either:

- reasonably suspected of having committed any of the offences to which the warrant or emergency authorisation relates
- the owner or lessee of the computer or device
- an employee of the owner or lessee of the computer or device
- a person engaged under a contract for services by the owner or lessee of the computer or device
- a person who uses or has used the computer or device, or
- a person who is or was a system administrator for the system including the computer or device.

The specified person must also have relevant knowledge of the computer or the measures applied to protect data held in the computer.

The judge or AAT member must take into account similar considerations for orders relating to child recovery, mutual assistance, control orders and the loss of evidence.

The penalty for not complying with a request compelling assistance under section 64A is a maximum of imprisonment for 10 years. This is consistent with the amended penalty in Schedule 3 for committing the aggravated offence under amended subsection 3LA(5) of the Crimes Act. There is no equivalent five year penalty for the simple offence in the Crimes Act because there are no equivalent simple offences under the SD Act, that is, offences which carry a penalty of less than a maximum of three years imprisonment are not relevant offences under the SD Act.

After subsection 65(1)

New subsection 65(1) ensures that, where there is a defect or irregularity in relation to the warrant or emergency authorisation and except for that defect or irregularity the warrant or authorisation would be sufficient authority for accessing the data, then access to the data is valid and the information can be used in evidence. This treats computer access warrants and authorisations the same as surveillance device warrants and authorisations.

Section 65(2)

This item ensures that subsection 65(2) which applies to defects and irregularities in relation to surveillance device warrants and surveillance device emergency authorisations also applies to computer access warrants and authorisations. Under this subsection, a defect or irregularity is:

- in or in connection with the issue of a document purporting to be a warrant or authorisation, or
- in connection with the execution or purported execution of the warrant or authorisation (or document purporting to be a warrant or authorisation).

A defect or irregularity is not a substantial defect or irregularity.

After subsection 65A(2)

A person is not criminally liable for any actions done under a control order access warrant issued on the basis of an interim control order where the interim order is subsequently declared to be void. This item replicates the existing provisions for control orders.

Section 65B (heading

This item repeals the heading in 65B to account for 65B now providing for both control order warrants and control order access warrants.

After subparagraph 65B(1)(a)(i)

If a control order access warrant was issued on the basis of an interim control order, and a court subsequently declares that the interim order is void, any information obtained under the warrant an be used, communicated or published if the person reasonably believes that doing so is necessary for preventing or reducing the risk of the commission of a terrorist act or serious harm to a person or property.

Amendments to the Telecommunications Act 1997

Section 313 of the Telecommunications Act provides an obligation for carriers and carriage service providers to give agencies 'such help as is reasonably necessary' to enforce the criminal law, protect the public revenue and safeguard national security. New paragraph 313(7)(caa) ensures that 'giving help' includes giving effect to authorisations to develop and test interception capabilities under section 31A of the TIA Act.

Amendments to the Telecommunications (Interception and Access) Act 1979

Subsection 5(1)

This item inserts the following definitions.

ASIO computer access intercept information means information obtained by ASIO under the listed sections in the ASIO Act by intercepting a communication passing over a telecommunications system. This is distinct from information obtained under a computer access warrant by executing computer access itself.

ASIO computer access warrant means a warrant issued under the listed provisions in the ASIO Act.

General computer access intercept information means information obtained by law enforcement under a general computer access warrant by intercepting a communication passing over a telecommunications system. This is distinct from information obtained under a computer access warrant by executing computer access itself.

General computer access warrant means a warrant issued under section 27C of the SD Act, which is the provision specifying that an eligible judge or AAT member may issue a warrant for computer access.

Subsection 5(1) (at the end of the definition of restricted record)

This item excludes general computer access intercept information from the definition of restricted record. The purpose is to ensure that agencies in possession of original general computer access intercept information are not subject to the obligations imposed by the TIA Act relating to those records. Instead, their record management will be governed by the SD Act.

Subsection 5(1) (paragraph (b) of the definition of warrant)

This item adds general computer access warrants and ASIO computer access warrants to the definition of 'warrant' in the TIA Act. The effect of this amendment is that interception for the purposes of either of these warrants is not prohibited. ASIO and law enforcement agencies will at times need to intercept information in order to execute computer access warrants. This Item ensures that interception is lawful.

Under subsection 7(1) of the TIA Act, interception of a communication passing over a telecommunications system is prohibited. Subsection 7(2)(b) provides the relevant exception; the prohibition does not apply in relation to the interception of a communication under a warrant.

After paragraph 7(2)(b)

This item provides additional exceptions to the prohibition in subsection 7(1) of the TIA Act against interception of a communication passing over a telecommunications system. This ensures that intercepting communications to execute a computer access warrant under the ASIO Act and SD Act is lawful.

Under paragraph 7(2)(ba), the interception of a communication under subsections 25A(4) or (8), 27A(1) or (3C), or 27E(2) or 27E(6) of the ASIO Act is permitted.

Under paragraph 7(2)(bb), the interception of a communication under subsection 27E(7) of the SD Act is permitted.

Subsection 31(1)

This item amends subsection 31(1) of the TIA Act to permit the head of a security authority to request the Attorney-General to authorise the security authority to work with a carrier in order to test or develop interception technologies. Currently, subsection 31(1) only allows testing by employees of a security authority.

This amendment is not intended to, in any way, impact or read down current testing arrangements between security authorities or law enforcement agencies and carriers under the exception to the prohibition on interception in paragraph 7(2)(ab) of the TIA Act.

This item provides a route for security authorities to conduct their testing, or the testing of other interception agencies, with the assistance of carriers. The current exception to the prohibition to interception in paragraph 7(2)(ab) is restrictive in allowing testing only in relation to 'the installation, connection or maintenance of equipment used, or to be used, for the interception of communications under warrants.' It is sometimes necessary for agencies to test in ad hoc circumstances.

A request under subsection 31(1) may specify any number of carriers or carriage service providers to be covered by the authorisation. However, a request is not required to specify a carrier if the security authority can undertake the testing without assistance. The head of the security authority can request multiple authorisations, which include any combination of carriers.

Subsection 31A(1)

Amendments to subsection 31A(1) will enable the Attorney-General, upon receiving a request, to authorise a security authority to work with a carrier to test interception technologies. The authorisation must be in writing and specify the period for which it will have effect. Authorisations cannot be made for a period greater than six months.

After subsection 31A(4)

New subsection 31A(4A) clarifies that, although an authorisation may allow employees of the security authority and employees of the carrier to test interception technologies, this does not mean that the testing must involve one or more of the employees acting together at the same time. They do not need to be in one another's presence. For example, it is permissible for a carrier to undertake some activities related to testing, and then hand information to the security authority to undertake other activities. An officer of the security authority is not required to be present during any phase of testing activities.

31AA Carrier to be notified of authorisation etc.

New section 31AA contains notification requirements where the Attorney-General has issued an authorisation for carriers to test interception technologies with a security authority.

The head of the security authority must give carriers named in an authorisation a copy of the authorisation as soon as practicable. There is no obligation on the head of the security authority to provide advance notification to a carrier of the issue of an authorisation, ahead of providing a copy of the authorisation.

If an authorisation is varied or revoked, the head of the security authority must notify the carriers specified in the authorisation immediately. A copy of the variation or revocation must be given as soon as practicable.

31E Employees of security authorities

New section 31E clarifies that both an ASIO employee and ASIO affiliate are taken to be employees of ASIO.

A staff member of an agency in the IS Act, that is also a security authority, is taken to be an employee of the security authority. Agency is defined in the IS Act to mean ASIS, the Australian Geospatial-Intelligence Organisation (AGO) or ASD. A security authority is defined in the TIA Act as a Commonwealth authority that has functions primarily relating to security, the collection of foreign intelligence, the defence of Australia or the conduct of Australia's international affairs.

63AB Dealing in general computer access intercept information

The use, recording and communication of information obtained in the course of intercepting a communication in order to execute a computer access warrant is restricted. This is to ensure that where agencies want to gain intercept material for its own purpose, they must apply for, and be issued with, an interception warrant under Chapter 2 of the TIA Act.

New section 63AB provides two exceptions to the general prohibition on dealing in computer access intercept information. First, section 63AB allows a person, for the purposes of doing a thing authorised by a general computer access warrant, to communicate to another person, make use of, make a record or, or give in evidence in a proceeding general computer access intercept information. The intention is that intercepted information can be used or communicated for a purpose reasonably incidental to the purposes of carrying out computer access.

Second, section 63AB allows a person to communicate general computer access intercept information to another person or make use or a record of that information if the information relates to involvement of a person in activities that, generally, exist in life threatening or emergency situations. These include:

- activities that present a significant risk to a person's safety, or a threat to security
- acting for or on behalf of a foreign power
- activities that pose a risk to the operational security of ASIO, ASIS, AGO or ASD
- activities that relate to the proliferation of weapons of mass destruction, and
- activities that relate to a contravention by a person of a UN sanction enforcement law.

In these very serious circumstances, a person may communicate, use or record intercept information that would otherwise be prohibited.

63AC Dealing in ASIO computer access intercept information

New section 63AC replicates the exceptions in section 63AB for persons dealing with intercept material under the authority of an ASIO computer access warrant.

At the end of section 63B

New subsection 63B(5) provides an exception on the prohibition against dealing with intercept material for carrier employees acting under a section 31A authorisation in order to develop or test technologies or interception capabilities.

Employees of the carrier can gather, record and use the test and development information and may also communicate the information to employees of the security authority who sought the authorisation as well as other employees of the same carrier or employees of another carrier listed in the authorisation. Should it be required that a carrier provide information to another carrier, that second carrier (or any subsequent carrier) is subject to the same conditions in subsection 63B(5), being that the subsequent carrier may record or use the information and may share the information on to the security authority or another carrier in its original format or in a modified format. This is to ensure that if a daisy-chain style test is required (recognising that modern communications information may pass over a number of systems), there are no impediments to the use and disclosure of information.

The limitation remains that the use and disclosure must be related to a testing or development purpose. A carrier is not to use the information provided to it or gathered by it for any other purpose.

Information collected under an authorisation may be retained for subsequent authorisation periods, should a subsequent authority require use of that information for the same purposes. This would include long term testing, where testing requires a baseline for comparison or where testing commenced in one testing authorisation period and was completed in a subsequent testing authorisation period. Where the information is no longer required, it should be destroyed.

Information collected under an authorisation may be retained for subsequent authorisation periods, should a subsequent authority require use of that information for the same purposes. This would include long term testing, where testing requires a baseline for comparison or where testing commenced in one testing

authorisation period and completed in a subsequent testing authorisation period. Where the information is no longer required, it should be destroyed.

Paragraph 64(1)(a)

This item constrains the permitted dealing of ASIO computer access intercept information. It ensures that ASIO computer access intercept information is not permitted to be communicated, made use of, or recorded even if in connection with the performance by ASIO of its functions or the performance of the IGIS of his or her functions, or for the purposes of security.

Paragraph 65(1)(a)

This item ensures that the Director-General of Security may not communicate to another person ASIO computer access intercept information, even if in accordance with subsections 18(3), (4A), or 19A(4) of the ASIO Act. Those provisions allow ASIO to share information with federal and state authorities, ASIS, ASD and AGO.

At the end of section 65 (After the note)

This item provides limitations on the use and disclosure of testing and development information acquired under an authorised in section 31A of the TIA Act (Part 2-4) for security authorities. The sharing of testing and development information acquired under a section 31A authorisation is not permitted unless it is for testing and development purposes. Where the purpose is to share information to test and develop capabilities or analyse systems or support systems, ASIO may share the information with a staff member of an authority of the Commonwealth or a State, ASD, ASIS, AGO, or a body listed in paragraph 19A(1)(d) or (e) of the ASIO Act. This can be for testing purposes of the receiving agency or for the testing purposes of ASIO.

This provision will allow ASIO to undertake lead role functions in relation to testing interception capabilities and associated systems. ASIO is under no obligation to test or facilitate testing on behalf of permitted agencies listed above, but may do so at the request of permitted agencies.

Information generated by those permitted agencies under section 31A can be shared to ASIO for testing and development purposes. This is true irrespective of whether the section 31A authorisation was sought by, executed by or named ASIO.

Paragraph 65A(1)(a)

This item is consequential to limit the use of information obtained under a section 31A authorisation to develop or test technologies or interception capabilities.

Paragraph 67(1)(a)

Under section 67, an officer or staff member of an agency may, for a permitted purpose, in relation to the agency, communicate to another person, make use of, or make a record of lawfully intercepted information and interception warrant information. This item ensures that general computer access intercept information is not able to be communicated, used or recorded for these purposes.

Section 68

Under section 68, the chief officer of an agency may communicate lawfully intercepted information under certain circumstances. This item ensures general computer access intercept information cannot be communication under section 68.

Subsection 74(1)

Under section 74, a person may give lawfully intercepted information in evidence in an exempt proceeding. This item ensures that a person may not give general computer access intercept information or ASIO computer access intercept information in evidence in an exempt proceeding.

Subsection 75(1)

Under section 75, a person may give information that has been intercepted in contravention of the prohibition against interception in subsection 7(1), due to an irregularity in a warrant, in evidence in an exempt proceeding. This item ensures that a person may not give general computer access intercept information or ASIO computer access intercept information in evidence in an exempt proceeding.

Paragraph 77(1)(a) and (b)

This item provides that intercept material is admissible in evidence in so far as new sections 63AB and 63AC permit. Those sections permit the dealing of general computer access intercept information and ASIO computer access information where very serious circumstances exist or where there is a purpose reasonably incidental to the purposes of carrying out computer access.

After paragraph 108(2)(ca)

New paragraph 108(2)(cb) provides an exception to the prohibition in subsection 108(1) on accessing a stored communication. The prohibition does not apply to accessing a stored communication under a general computer access warrant.

Part 2—Application Provisions

Application—computer access warrants

All amendments made under the provisions of Schedule 2 apply only to warrants, authorisations and orders issued after the commencement, being the day after the Bill receives the Royal Assent.

Part 3—Amendments contingent on the commencement on the commencement of the Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018

Schedule 2, Part 3 is to commence the later of a) immediately after the commencement of Schedule 2, Part 1 or b) immediately after the commencement of Part 6 of Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018.* If the events of paragraph b) do not occur then Schedule 2, Part 3 is not to commence.

Amendments to the International Criminal Court Act 2002

Division 12B—Requests for access to data held in computers

79B Authorising applications for computer access warrants

This item inserts a new section which enables the Attorney-General to authorise applications for computer access warrants under the SD Act when a request is received from the International Criminal Court.

New subsection 79B(1) sets out the criteria that must be satisfied before the Attorney-General may authorise an application for a computer access warrant, including that the International Criminal Court has made a request in relation to access to data held in a computer, that the Attorney-General is satisfied that an investigation is being conducted by the Prosecutor, or a proceeding is before the International Criminal Court, and that the International Criminal Court has given appropriate undertakings on the use of data, the destruction of information and any other matters that the Attorney-General thinks appropriate.

New subsections 79B(2) and (3) clarify the scope and meaning of terms used in subsection (1). For consistency, the definitions are the same as in the SD Act.

The amendment enables Australian authorities to use the new computer access warrants to obtain information on behalf of the International Criminal Court pursuant to a request. This is consistent with the approach taken to requests for mutual legal assistance from foreign countries as set out in new section 15CC of the MACMA.

The threshold requirements for computer access under the SD Act will apply when an application is made.

Commencement of this item is subject to commencement of Part 6 of Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*. Subject to those provisions commencing, this item will commence immediately after the commencement of Part 1 of Schedule 2 of this Act or commencement of Part 6 of Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*, whichever is the latter. Part 6 of Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018* inserts provisions that ensure that Australia is able to provide the same level of assistance to the International Criminal Court as can be provided to foreign countries under the MACMA.

Amendments to the International War Crimes Tribunals Act 1995

Division 1B—Requests for access to data held in computers

32B Authorising applications for computer access warrants

This item inserts a new section which enables the Attorney-General to authorise applications for computer access warrants under the SD Act that are requested by a Tribunal established under the *International War Crimes Tribunals Act 1995*.

New subsection 32B(1) includes the criteria for the Attorney-General to authorise an application, including that a Tribunal has made a request in relation to access to data held in a computer, that the Attorney-General is satisfied that a proceeding is before, or an investigation is being conducted by, the Tribunal and that the Tribunal has given appropriate undertakings on the use of data, the destruction of information and any other matters that the Attorney-General thinks appropriate.

New subsection 32B(2) and (3) clarify the scope and meaning of terms used in subsection (1). For consistency, the definitions are the same as in the SD Act.

The amendment enables Australian authorities to use the new computer access warrant powers to obtain information on behalf of a war crime tribunal pursuant to a request. This is consistent with the approach taken to requests for mutual legal assistance from foreign countries as set out in new section 15CC of the MACMA.

The threshold requirements for computer access under the SD Act will apply when an application is made.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*. That Act inserts provisions that enable assistance to be provided to war crimes tribunals that are established under the *International War Crimes Tribunals Act 1995*.

Amendments to the Surveillance Devices Act 2004

Subsection 6(1) (definition of international assistance application)

This item amends the definition of international assistance application in the SD Act to add reference to applications for a computer access warrant made under an international assistance authorisation.

The *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018* inserts a definition of international assistance application into the SD Act, and provides processes for assistance to the International Criminal Court and war crimes tribunals in relation to surveillance device warrants.

This amendment will allow an international assistance application relating to new computer access warrants to be made to assist the International Criminal Court and war crimes tribunals, consistently with the approach taken for mutual legal assistance.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018.*

Subsection 6(1) (paragraph (a) of the definition of international assistance authorisation)

This item adds new section 15CC(1) of the MACMA to the definition of international assistance authorisation under the SD Act.

The *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018* inserts a definition of international assistance authorisation into the SD Act, and provides processes for assistance to the International Criminal Court and war crimes tribunals in relation to surveillance device warrants.

New section 15CC(1) allows the Attorney-General to authorise requests by foreign countries for assistance in relation to data held in computers under new computer access warrant provisions.

This amendment will allow an international assistance authorisation relating to new computer access warrants to be made to assist the International Criminal Court and war crimes tribunals, consistently with the approach taken for mutual legal assistance.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018.*

Subsection 27A(4)

This item replaces subsection 27A(4) to refer to 'international assistance authorisations' instead of 'mutual assistance authorisations.' This amendment is consequential to reflect the new definition of international assistance authorisation outlined above.

New section 27A allows law enforcement to apply for a computer access warrant in specified circumstances, including in relation to an international assistance authorisation.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Paragraphs 27C(1)(c) and (2)(a)

This item replaces the reference to 'mutual assistance authorisation' with 'international assistance authorisation.' This amendment is consequential to reflect the new definition of international assistance authorisation outlined above.

New section 27C deals with the determination of applications for computer access warrants, including specific criteria for decision-making in the case of a warrant sought in relation to an international assistance authorisation.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Paragraph 27C(2)(f)

This item replaces new paragraph 27C(2)(f) to reflect the new definition of international assistance authorisations. This amendment is consequential.

New section 27C deals with the determination of applications for new computer access warrants, including mandatory considerations for the issuing authority in the case of a warrant sought in relation to an international assistance authorisation.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Subparagraph 27D(1)(b)(iv)

This item replaces the reference to 'mutual assistance authorisation' with 'international assistance authorisation.' This amendment is consequential to reflect the new definition of international assistance authorisation outlined above.

New section 27D provides for what a computer access warrant must contain, including where the warrant relates to an international assistance authorisation.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Paragraph 27E(3)(c)

This item replaces the reference to 'mutual assistance authorisation' with 'international assistance authorisation.' This amendment is consequential to reflect the new definition of international assistance authorisation outlined above.

New section 27E provides for what a computer access warrant authorises, including when data is covered by a warrant sought in relation to an international assistance authorisation.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Paragraph 27H(4)(a)

This item replaces the reference to 'mutual assistance authorisation' with 'international assistance authorisation.' This amendment is consequential to reflect the new definition of international assistance authorisation outlined above.

New subsection 27H(4) deals with discontinuance of access under a computer access warrant, including obligations for the chief officer to take steps to ensure access is discontinued in circumstances where the warrant has been authorised under an international assistance authorisation.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Subparagraph 27H(4)(b)(i)

This item removes the reference to 'offence against a law of a foreign country to which an authorisation relates' and replaces it with 'any offence to which the authorisation relates.' This amendment is consequential to reflect the new definition of international assistance authorisation to include assistance to the International Criminal Court and war crimes tribunals. The jurisdiction of the International Criminal Court and war crimes tribunals may relate to crimes under international law and are not limited to crimes against the laws of a particular country.

New subsection 27H(4) deals with discontinuance of access under a computer access warrant, including obligations for the chief officer to take steps to ensure access is discontinued where access to data is no longer required for the purpose of enabling evidence to be obtained of the commission of an offence.

Paragraph 27H(9)(c)

This item replaces the reference to 'mutual assistance authorisation' with 'international assistance authorisation.' This item also removes the reference to 'offence against a law of a foreign country to which an authorisation relates' and replaces it with 'any offence to which the authorisation relates.'

The amendment is consequential to reflect the new definition of international assistance authorisation outlined above. International assistance authorisation includes assistance to the International Criminal Court and war crimes tribunals. The jurisdiction of the International Criminal Court and war crimes tribunals may relate to crimes under international law and are not limited to crimes against the laws of a particular country.

New subsection 27H(9) deals with discontinuance of access under a computer access warrant, including obligations on a law enforcement officer to inform the chief law enforcement officer where they believe that access to data under the warrant is no longer necessary for the purpose of enabling evidence to be obtained of the commission of an offence.

Subsection 64A(4)

This item replaces the reference to 'mutual assistance authorisation' with 'international assistance authorisation.' The amendment is consequential to reflect the new definition of international assistance authorisation outlined above.

New section 64A allows for assistance orders to be made requiring a person with knowledge of a computer or a computer system to assist a law enforcement officer to access a computer subject to a computer access warrant, including a warrant issued in relation to an international assistance assistance authorisation.

Application of amendments

The amendments in Part 3 of Schedule 2 apply to any requests made to the Attorney-General by the International Criminal Court, a Tribunal or a foreign country on commencement of the item.

The amendments will have retrospective application to any request that is made before commencement of the item if, immediately before that commencement, the Attorney-General had yet to make a decision on the request.

The amendments will apply to requests whether conduct, a crime or an offence to which the request relates occurred before, on or after commencement.

Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Schedule 3

Amendments to the Crimes Act 1914

Subsection 3C(1)

This item inserts definitions of ***account-based data***, ***carrier***, ***communication in transit***, ***electronic service*** and ***telecommunications facility*** into the Crimes Act.

Account-based data has the meaning in section 3CAA.

Carrier, communication in transit and ***telecommunications facility*** draw their meaning from the Telecommunications Act.

Electronic service has the same meaning as in *Enhancing Online Safety Act 2015*.

Section 3CAA Account-based data

New Section 3CAA defines ***account-based data***.

The purpose of including this definition is to ensure that accessing a computer or data storage device under warrant permits the executing officer or a constable assisting to use that computer or data storage device – or any other equipment – for the purpose of obtaining access to account-based data.

Account-based data in relation to a person includes data associated with an account for an electronic service with end-users that is held by the person. This could be data associated with an email service, a Facebook account, an Instagram account, a Reddit subscription, a Twitter profile, a log-in to a commentary section on a news website or messaging services such as WhatsApp, Signal, and Telegram.

A person is taken to hold an account with the electronic service if they use, pay or manage an account, whether or not the account is in a particular name of a person or whether a person actually created the account. A person who inherits an account, establishes an account in a false name, shares an account, has an account established in their name, or attempts to anonymise an account, is still taken to hold the account

The definition of ***account-based data*** in relation to a person is not limited to the person who holds an account.

Account-based data in relation to a person also includes data associated with an account for an electronic service with end-users that is used or is likely to be used be the person. This could include data associated with an account held by another person (such as a family member, friend or business associate) but utilised by the first-mentioned person.

Account is defined in section 4 of the *Enhancing Online Safety Act 2015*. It includes a free account, a pre-paid account and anything that may reasonably be regarded as the equivalent of an account.

After subsection 3F(2)

New subsections 3F(2A) and (2B) make additions to the list of things authorised by a warrant issued under section 3E of the Crimes Act. The amendments provide that the executing officer or a constable assisting may use a computer or device found during the search, a telecommunications facility, other electronic equipment or a data storage device at any time when the warrant is in force. These activities must be for the purpose of obtaining access to relevant data (subsection 3F(2A)) or account-based data (subsection 3F(2B)) in order to determine whether the data is evidential material. The executing officer or constable assisting may copy, delete or alter data if necessary to achieve this purpose.

Relevant data is defined in the Crimes Act and is distinguishable from ***account-based data*** by being stored within the computer or data storage device. Account-based data may be held on the device or within another computer such as an external server or cloud.

This amendment will allow an officer or constable assisting to utilise specialist equipment to analyse computers and digital equipment.

Subsection 3F(2C) provides that subsections (2A) and (2B) do not authorise the addition, deletion or alteration of data when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless it is necessary to do one or more things specified in the warrant. In no

circumstances is it authorised for material loss or damage to be caused to other persons lawfully using a computer.

Subsections 3F(2D) and (2E) clarify that an officer or constable assisting may access data in accordance with this section remotely. Often the remote access of devices is best practice. Notification of access is always required.

Subsection 3K(3A)

Amendments to subsection 3K will extend the time in which a computer or data storage device may be moved to another place for analysis from 14 days to 30 days. Things that are not computers or data storage devices will continue to be subject to the 14 day time limit for analysis.

The time it takes to process data has increased as technology has advanced and computers have become more complex. The extended time limit will allow proper forensic processes to be undertaken.

Computers and data storage devices may include any items that compute or retain data.

Examples of a computer include a mobile telephone, laptop, tablet and smart watch. For clarity, where a computer forms a part of a greater whole, it is permissible to relocate and examine the greater whole rather than remove the computer. For example, often vehicles contain computers. For forensic best practice, the entire vehicle may be relocated and examined rather than removing particular elements. This avoids potential damage to systems and devices.

Data storage devices include any things that contain or are designed to contain data for use by a computer. Data storage devices are not required to have a computational component. They are also not required to be powered. Examples of a data storage device include a compact disc (CD), Secure Digital card (SD card), Universal Serial Bus (USB) or any other thing that contains information that is made legible, accessible or usable by a computer. This includes future storage solutions not yet envisioned.

Subsection 3K(3B)

This item is consequential.

Subsection 3K(3D)

This item is consequential.

At the end of section 3K

Once a computer or data storage device is moved for processing, new subsections 3K(5) and (6) allow examination to occur by using the computer or device, a telecommunications facility, any other electronic equipment or a data storage device. These activities must be for the purpose of obtaining access to relevant data (subsection 3K(5)) or account-based data (subsection 3K(6)) in order to determine whether the computer or device is a thing that may be seized. Data may be copied, deleted or altered if necessary to achieve this purpose.

Subsection 3K(7) provides that subsections (5) and (6) do not authorise the addition, deletion or alteration of data when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless it is necessary to do one or more things specified in the warrant. In no circumstances is it authorised for material loss or damage to be caused to other persons lawfully using a computer.

Subsections 3K(8) and (9) clarify that processing of a computer or data storage device in accordance with this section may occur remotely. Often the remote access of devices is best practice.

Subsection 3LAA(1)

This item amends subsection 3LAA(1) to accommodate the new concept of account-based data. If electronic equipment is moved to another place under subsection 3K(2), the executing officer or a constable assisting may operate the equipment to access data, data held at another place and account-based data.

After subsection 3LA(1)(a)(i)

New subparagraph 3LA(1)(a)(ia) allows a constable to apply to a magistrate requiring a specified person to provide information or assistance that is reasonably necessary to access data held in a computer or device found during a search of a person that is authorised by a warrant under section 3E.

This amendment reflects the portability of modern computers and data storage devices, including mobile telephones and USBs

Subsection 3LA(5)

This item bifurcates the existing offence in section 3LA into a simple offence and an aggravated offence.

The simple offence remains the same as the previous offence in section 3LA, but increases the penalty from two years imprisonment or 120 penalty units to five years imprisonment or 300 penalty units, or both.

The intention of raising the penalty for the simple offence is to reflect the significant harm to investigations and prosecutions caused by a person failing to assist law enforcement access computers and data storage devices covered by an order issued under section 3LA.

The aggravated offence applies where a person omits to do an act and the offence to which the relevant warrant relates is a serious offence. The penalty for the aggravated offence is 10 years imprisonment or 600 penalty units, or both.

The new aggravated offence reflects the gravity of non-compliance with an investigation into a serious offence. Given the current penalties for committing an offence against section 3LA, there is no incentive for a person to comply with an order if they have committed an offence with a higher penalty and evidence is available on their device.

After paragraph 3N(2)(a)

This item is consequential.

After subsection 3ZQV(3)

New subsection 3ZQV(3) prohibits electronic equipment that has been seized from being operated to determine whether data generated after the expiry of the warrant is evidential material.

Application of amendments

All amendments made under the provisions of this schedule apply only to warrants and orders issued after the commencement, being the day after the Bill receives the Royal Assent.

Schedule 4

Amendments to the Customs Act 1901

Subsection 183UA(1)

This item defines the following terms:

Communication in transit has the same meaning as in the Telecommunications Act.

Recently used conveyance in relation to a search of a person means a conveyance that the person had operated or occupied at any time within the 24 hours before the search commenced. Search warrants issued in new section 199A, pertaining to a person, include searching recently used conveyances.

Subsection 183UA(1) (definition of search warrant)

This item amends the definition of ***search warrant*** to include new person-based search warrants in section 199A for the purposes of the Customs Act.

Subsection 183UA(1)

This item defines the following terms:

Serious offence has the same meaning as in Part 1AA of the Crimes Act. It will encapsulate certain offences in the Customs Act, including:

- Division 1AA – Export of goods for a military end-use
- Section 50(7) – Prohibited imports licencing (narcotics)
- Section 112(2BC) – Prohibited exports licencing (narcotics)
- Section 64ADA – Disclosure of cargo reports to port authorities, and
- Section 233 and associated sections – Smuggling and unlawful importation and exportation / dealing in UN sanctioned goods.

This definition is included to enable the creation of an aggravated offence for not complying with an order made under section 201A of the Customs Act. The intention of this amendment is not to permit the Australian Border Force (ABF) to investigate serious crimes under the Crimes Act, but to include a provision that triggers serious crimes in the Customs Act.

Section 198 when search warrants relating to premises can be issued

This item amends the heading of section 198 so as to differentiate it from the new section 199A.

Section 199 the things that are authorised by a search warrant relating to premises

This item amends the heading of section 199 so as to differentiate it from new section 199B.

After Subsection 199(4)

New subsection 199(4A) make additions to the list of things authorised by a search warrant relating to a premises. The amendments provide that the executing officer or a constable assisting may use a computer or device found during the search, a telecommunications facility, other electronic equipment or a data storage device at any time when the warrant is in force. These activities must be for the purpose of obtaining access to relevant data in order to determine whether the data is evidential material. The executing officer or constable assisting may copy, delete or alter data if necessary to achieve this purpose.

This amendment will allow an officer or constable assisting to utilise specialist equipment to analyse computers and digital equipment.

Subsection 199(4B) provides that subsection (4A) does not authorise the addition, deletion or alteration of data when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless it is necessary to do one or more things specified in the warrant. In no

circumstances is it authorised for material loss or damage to be caused to other persons lawfully using a computer.

Subsection 199(4C) clarifies that an officer or constable assisting may access data in accordance with this section remotely. Often the remote access of devices is best practice. Notification of access is always required.

After section 199

New sections 199A and 199B provide for limited search warrants to be issued in regards to a person.

These search warrants are limited to an ordinary search or frisk search for a computer or data storage device. These search warrants are not a general search warrant power relating to persons. This power is necessary to account for the large amount of evidentiary material that is now held on or accessible by computers and data storage devices.

The ABF has existing powers to apply for a search warrant in regards to premises. Premises-based warrants are more permissive in that they allow ordinary searches and frisk searches of any persons on the premises. The new, limited, person-based search warrants provide a more proportionate response option for the ABF, allowing them to execute a targeted warrant when that is all that is required. For example, locations which are usually subject to premises-based search warrants – including businesses, warehouses and transport locations – are often populated and broadly-used.

A person may also operate multiple businesses in separate locations. Rather than applying for a premises-based warrant for each business premises, this amendment will allow the ABF to seek a warrant to search the computer or data storage device for that person.

The ABF has standing powers in relation to things in customs control, being items in a customs place such as a port or airport. These provisions are not intended to read down those powers.

Reference in paragraph 199B(1)(c) to prohibited goods that are ‘unlawfully carried by the person’ draws the definition of prohibited goods from the Customs Act. Reference to seizable items draws the definition from the Customs Act. The intention of this provision is to ensure that an officer executing a search authorised under section 199A may seize items that are clearly and illegitimately in the possession of the person being searched. This could include narcotics, firearms or other prohibited goods. This would also extend to any recently used conveyance, should prohibited goods or seizable items be found.

It is not the intention of paragraph 199(1)(c) to provide a backdoor means for officers to search persons for such prohibited goods or seizable items. The intention of the warrant is to obtain evidentiary material found in a computer or data storage device. Only goods found incidental to this search may be seized. Searches primarily for goods other than computers and data storage devices should be conducted under a section 198 search warrant for a premises, a section 203 seizure warrant or another provision available to ABF officers. The section 199A search warrant is not a general, broad-based search warrant.

Dealing with items seized under section 199A is not amended by this legislation.

For clarity, provisions in paragraph 199B(1)(c) regarding prohibited goods unlawfully carried, require an executing officer or person assisting to form a reasonable belief that the goods are prohibited goods and that they are carried unlawfully. It is reasonable for an executing officer or person assisting to assume that prohibited goods are not carried lawfully, given their nature, i.e. an amount of marijuana is by its objective nature an illicit substance, and does not require a subjective assessment. It would be unreasonable for an executing officer or person assisting to assume that prohibited goods are lawfully carried, barring some demonstration of material indicating otherwise. The onus is on the person subject to a search and seizure to provide material demonstrating that prohibited goods are carried lawfully, such as a prescription, import licence or firearms licence. If material demonstrating the goods were lawfully carried can be provided following seizure, those goods may be returned subject to provisions in sections 203R and 203S of the Customs Act. Should the goods already be delivered to the custody of the AFP, the provisions relating to seizure of goods under the Crimes Act would apply to those goods rather than provisions in the Customs Act. The person concerned must also deal with the AFP directly regarding the return of the goods. The ABF is not required to act as an intermediary in these circumstances.

A search warrant issued in respect of a person, that under section 199B permits a search of a recently used conveyance, also allows lawful entry to that recently used conveyance. This is consistent with the Crimes Act.

Subsection 200(1)

This item is consequential.

Subsection 200(2)

This item is consequential.

Paragraph 200(2)(b)

This item is consequential.

Paragraph 200(3)(a)

This item is consequential.

Paragraph 200(3)(b)

This item is consequential.

Subsection 200(3A)

This item extends the period for which a computer or data storage device can be moved for examination to determine whether it contains or constitutes evidentiary material to 30 days. The current 72 hour period is inadequate to account for many of the internal authorisation and relocation processes which must occur to ensure transparency and accountability, as well as secure relocation of devices once moved. This results in few items of potential evidential value being moved for analysis.

The 72 hour period is also inadequate for proper forensic processes to be undertaken, even where relocation and approval occurs within the timeframe. The time it takes to process data has increased as technology has advanced and computers have become more complex. To ensure forensic best-practice for computers and data storage devices, an adequate time period is necessary.

Subsection 200(3A) applies to computers or data storage devices relocated or examined under section 198 or section 199A of the Customs Act. That is, the new subsection applies to items obtained from a person based or premises-based search warrant.

Examples of a computer include a mobile telephone, laptop, tablet, smart watch. For clarity, where a computer forms a part of a greater whole, it is permissible to relocate and examine the greater whole rather than remove the computer. For example, often vehicles contain computers. For forensic best practice, the entire vehicle may be relocated and examined rather than removing particular elements. This avoids potential damage to systems and devices.

Data storage devices include any things that contain or are designed to contain data for use by a computer. Data storage devices are not required to have a computational component. They are also not required to be powered. Examples of a data storage device include a compact disc (CD), Secure Digital card (SD card), Universal Serial Bus (USB) or any other thing that contains information that is made legible, accessible or usable by a computer. This includes future storage solutions not yet envisioned.

Subsection 200(3B)

This item is consequential.

Subsection 200(3C)

New subsection 200(3D) aligns the timeframes for extension for relocating and examining computers and data storage devices to the extension timeframes established in the Crimes Act. This provision will establish a maximum extension timeframe of 14 days for computers and data storage devices.

Subsection 200(4)

This item is consequential.

After section 201

New section 201AA replicates provisions in the Crimes Act, and those in the Customs Act related to existing premises based warrants, to allow the use of electronic equipment moved under other provisions (the person based search warrant inserted by this schedule) to access data on that electronic equipment, and for related purposes.

If evidentiary material is found on the item, it may be seized.

Paragraphs 201A(1)(a), (b) and (c)

This item allows orders in section 201A to be made against person-based or premises-based search warrants. Section 201A is amended to apply when a computer or data storage device has been found in the course of executing a warrant under section 198 or section 199A, or apply to any computer or data storage device seized under the Subdivision.

Paragraph 201A(2)(a)

For completeness, reference to data storage devices is included to enable searches of those devices.

Subparagraph 201A(2)(b)(ii)

For completeness, reference to data storage devices is included to enable searches of those devices.

Subparagraph 201A(2)(b)(iii)

For completeness, reference to data storage devices is included to enable searches of those devices.

At the end of paragraph 201A(2)(b)

This item inserts three additional categories of person who can be compelled to provide assistance with accessing a device under order. These definitions are consistent with those in the Crimes Act. The intention is to ensure that powers are consistent, and that powers are fully effective by including all such persons that should reasonably be expected to provide assistance with accessing a device under an order.

Subparagraph 201A(2)(c)(i)

For completeness, reference to data storage devices is included to enable searches of those devices.

Subparagraph 201A(2)(c)(i)

For completeness, reference to data storage devices is included to enable searches of those devices.

Subparagraph 201A(2)(c)(i)

For completeness, reference to data storage devices is included to enable searches of those devices.

Subparagraph 201A(2)(c)(ii)

For completeness, reference to data storage devices is included to enable searches of those devices.

Subsection 201A(3)

This item bifurcates the existing offence in section 201A into a simple offence and an aggravated offence.

The simple offence remains the same as the previous offence in section 201A, but increases the penalty from two years imprisonment or 120 penalty units to five years imprisonment or 300 penalty units, or both.

The intention of raising the penalty for the simple offence is to reflect the significant harm to investigations and prosecutions caused by a person failing to assist law enforcement access computers and data storage devices covered by an order issued under section 201A.

The aggravated offence applies where a person omits to do an act and the offence to which the relevant warrant relates is a serious offence. The penalty for the aggravated offence is 10 years imprisonment or 600 penalty units, or both.

The new aggravated offence reflects the gravity of non-compliance with an investigation into a serious offence. Given the current penalties for committing an offence against section 201A, there is no incentive for a person to comply with an order if they have committed an offence with a higher penalty and evidence is available on their device.

Paragraph 201B(1)(a)

This item is consequential.

Paragraph 201B(1)(d)

This item is consequential.

Paragraph 202(1)(a)

This item is consequential.

Paragraph 202A(2)(a)

This item is consequential.

Subsection 203K(5)

This item is consequential.

Subsection 203M(4)

This item is consequential.

Application of amendments

All amendments made under the provisions of this Schedule apply only to warrants and orders issued after the commencement, being the day after the Bill receives the Royal Assent.

Schedule 5

Amendments to the Australian Security Intelligence Organisation Act 1979

After subsection 16(1)

This item provides that the Director-General may, by writing, delegate any or all of his or her functions or powers under the new section 21A, Voluntary assistance provided to the Organisation, to a senior position-holder of ASIO, which is defined in the ASIO Act as an SES employee or equivalent, or a Coordinator.

The default position in paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901* applies, that is the powers that may be delegated do not include that power to delegate. Due to the sensitivity of the decisions being made (decisions to request assistance or issue evidentiary certificates), it is appropriate that this power be confined to SES employees or equivalent and not be sub-delegated.

21A Voluntary assistance provided to the Organisation

Section 21A establishes two frameworks which provide protection from civil liability for voluntary assistance provided in accordance with a Director-General request and for unsolicited disclosure of information.

Subsection 21A(1) provides that if the Director-General requests a person or body to engage in conduct that the Director-General is satisfied is likely to assist ASIO in the performance of its functions and:

- the person engages in the conduct in accordance with the request, and
- the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory, and
- the conduct does not result in significant loss of, or serious damage to, property

the person or body is not subject to any civil liability for, or in relation to, that conduct. The requirement for the Director-General to be satisfied that the conduct is likely to assist ASIO in the performance of its functions is intended to provide greater legal certainty to recipients of requests, by allowing them to rely on the Director-General's satisfaction.

A request by the Director-General may be made orally or in writing. If a request is made orally then the Director-General must make a written record of the request within 48 hours of it being made.

The Director-General may enter into a contract, agreement or arrangement with a person or body in relation to conduct engaged in by the person or body in accordance with such a request.

Subsection 21A(5) provides protection from civil liability for persons or bodies making unsolicited disclosures of information to ASIO. The amendment provides that if a person or body engages in conduct that consists of, or is connected with giving information to ASIO, or giving or producing a document to ASIO, or making one or more copies of a document and giving those copies to ASIO, and:

- the person reasonably believes that the conduct is likely to assist ASIO in the performance of its functions, and
- the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory, and
- the conduct does not result in significant loss of, or serious damage to, property, and
- a Director-General request discussed above does not apply to the conduct

the person or body is not subject to any civil liability for, or in relation to, the conduct.

Given this amendment relates to unsolicited help, the policy intention is to ensure that someone who reasonably believes that their help will assist benefits from the immunity, even if they are mistaken about what may assist ASIO, or what the ASIO's functions are.

Subsection 21A(6) provides that ASIO may make and retain copies of, or take and retain extracts from, a document given or produced to ASIO in accordance with a Director-General request or an unsolicited disclosure of information.

Subsection 21A(8) provides that the Director-General may give a certificate in writing certifying one or more facts relevant to the question of whether he or she was satisfied that particular conduct was likely to assist ASIO in the performance of its functions.

Subsection 21A(9) provides that in any proceedings that involve determining whether the provisions relating to a Director-General request or unsolicited disclosure of information applies to particular conduct, a certificate given by the Director-General is prima facie evidence of the facts certified. The evidentiary certificate would only deal with factual matters, being the factual basis on which the Director-General reached his or her belief, and would not deal with legal matters that would be properly the role of the courts to determine.

In the event that the operation of section 21A results in an acquisition of property, within the meaning of paragraph 51(xxxi) of the Constitution, from a person otherwise than on just terms, this item provides that the Commonwealth is liable to pay a reasonable amount of compensation to the person. If the Commonwealth and the person do not agree on the amount of compensation, the person may institute proceedings in the Federal Court of Australia for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

Section 34AA Person with knowledge of a computer or a computer system to assist access to data

New section 34AAA provides that the Director-General may request the Attorney-General to make an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow ASIO to do one or more of the following:

(a) access data held in, or accessible from, a computer or data storage device that:

- is the subject of a warrant under section 25A, 26 or 27A; or
- is the subject of an authorisation under section 27E or 27F; or
- is on premises in relation to which warrant under section 25, 26 or 27A is in force; or
- is on premises in relation to which an authorisation under section 27D or 27F is in force; or
- is found in the course of an ordinary search of a person, or a frisk search of a person, authorised by warrant under section 25 or 27A; or
- is found in the course of an ordinary search of a person, or a frisk search of a person, authorised under section 27D; or
- has been removed from premises under a warrant under section 25, 26 or 27A; or
- has been removed from premises under section 27D; or
- has been seized under section 34ZB;

The types of assistance that ASIO may seek under this power include compelling a target or a target's associate to provide the password, pin code, sequence or fingerprint necessary to unlock a phone subject to a section 25 computer access warrant. Another example is where a specialist employee of a premise subject to a section 25 search warrant could assist ASIO officers interrogate the relevant electronic database or use the relevant software so that they can obtain a copy of particular records or files.

(b) copy data held in, or accessible from, a computer, or data storage device, described in paragraph (a) to another data storage device;

(c) convert into documentary form or another form intelligible to an ASIO employee or ASIO affiliate:

- data held in, or accessible from, a computer, or data storage device, described in paragraph (a) above; or
- data held in a data storage device to which the data was copied as described in paragraph (b); or
- data held in a computer or data storage device removed form premises under a warrant under section 25, 26 or 27A; or
- data held in a computer or data storage device removed from premises under section 27D.

The Attorney-General can make the order if the Attorney-General is satisfied that:

(a) if the computer or data storage device:

- is the subject of a warrant under section 27A; or
- is on premises in relation to which a warrant under section 27A is in force; or
- is found in the course of an ordinary search of a person, or a frisk search of a person, authorised by a warrant under section 27A; or
- has been removed from premises under a warrant under section 27A;

both:

- access by ASIO to data held in, or accessible from, the computer or data storage device will be for the purpose of obtaining foreign intelligence relating to a matter specified in the relevant notice under subsection 27A(1); and
- on the basis of advice received from the Defence Minister or the Foreign Affairs Minister, the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being; and

(b) if paragraph (a) does not apply – there are reasonable grounds for suspecting that access by ASIO to data held in, or accessible from, the computer or data storage device will substantially assist the collection of intelligence in accordance with this Act in respect of a matter that is important in relation to security; and

(c) the specified person is:

- reasonably suspected of being involved in activities that are prejudicial to security; or
- the owner or lessee of the computer or device; or
- an employee of the owner or lessee of the computer or device; or
- a person engaged under a contract for services by the owner or lessee of the computer or device; or
- a person who uses or has used the computer or device; or
- a person who is or was a system administrator for the system including the computer or device; and

(d) the specified person has relevant knowledge of:

- the computer or device or a computer network of which the computer or device forms or formed a part; or
- measures applied to protect data held in, or accessible from, the computer or device.

This power enables ASIO to compel those who are able to provide ASIO with knowledge or assistance on how to access to data on computer networks and devices to do so. Similar powers are available to the police under section 3LA of the Crimes Act which allows a constable to apply to a magistrate for an order requiring a specified person with knowledge of a computer or a computer system to assist in accessing data on a computer or data storage device.

Where the computer or data storage device is not on premises in relation to which a warrant is in force, the order must: specify the period within which the person must provide the information or assistance; and specify the place at which the person must provide the information or assistance; and specify the conditions (if any) determined by the Attorney-General as the conditions to which the requirement on the person to provide the information or assistance is subject.

A person commits an offence if the person is subject to an order under this section; and the person is capable of complying with the order; and the person omits to do an act; and the omission contravenes the order. A person would be incapable of complying with an order where, for example, the person was in possession of information, documents or things but the information, document or thing had been removed from their possession, or deleted or destroyed by another person. The penalty is imprisonment for 5 years or 300 penalty units, or both.