THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) AMENDMENT BILL 2007

REPLACEMENT EXPLANATORY MEMORANDUM

(Circulated by authority of the Attorney-General, the Honourable Philip Ruddock MP)

THIS MEMORANDUM REPLACES THE EXPLANATORY MEMORANDUM PRESENTED TO THE HOUSE OF REPRESENTATIVES ON 14 JUNE 2007
OUTLINE

1. The Bill will amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to implement further recommendations from the Report on the Review of the Regulation of Access to Communications by Anthony Blunn AO (the Blunn Report).

2. The *Telecommunications (Interception) Amendment Act 2006* implemented the first stage of the legislative amendments. This Bill will amend the TIA Act to transfer relevant provisions of the *Telecommunications Act 1997* (the Telecommunications Act) to the TIA Act and will provide comprehensive and over-riding legislation that regulates access to telecommunications data for national security and law enforcement purposes. The legislation will also:
   - provide a mechanism for access to prospective telecommunications data, including establishing secondary use and disclosure offences and accountability mechanisms,
   - impose obligations on carriers and carriage service providers in relation to interception capability and delivery capability, and
   - preserve existing cost allocation principles between the telecommunications industry and interception agencies associated with interception and delivery capability.

3. This Bill will also improve the effectiveness of the Australian telecommunications access regime by:
   - Implementing in part recommendation 24 of the Blunn report, which recommended allowing access to the content of communications for the protection of data systems and the development or testing of new technologies,
   - widening the definition of exempt proceedings to allow disclosures for the purposes of proceedings in relation to the *Spam Act 2003*, and enabling the use of this evidence in court proceedings,
   - ensuring that interception warrants are available in relation to the investigation of any offence relating to child pornography, regardless of the maximum term of imprisonment that may be imposed by State and Territory criminal law, and
   - other minor amendments that will improve operational efficiency.

FINANCIAL IMPACT STATEMENT

The amendments made by the Telecommunications (Interception and Access) Amendment Bill 2007 will have no financial impact.
NOTES ON CLAUSES

Clause 1 Short title

Clause 1 is a formal provision specifying the short title of the Bill. It provides that the Act may be cited as the Telecommunications (Interception and Access) Amendment Act 2007.

Clause 2 Commencement

This clause provides for the commencement of the Bill.

Clauses 1 to 3 will commence on the day on which this Act receives the Royal Assent.

Schedule 1 transfers provisions from the Telecommunications Act to the TIA Act and requires administrative procedures to be put in place before commencement. Schedule 1 will therefore commence on a date to be fixed by proclamation. If at the end of six months after Royal Assent, Schedule 1 has not been proclaimed, it will commence on the following day.

Schedule 2 items 2 to 26 will commence on the day after this Act receives Royal Assent.

Schedule 2, Item 1 will commence immediately after 3 November 2006. Item 1 corrects a drafting error in the Telecommunications (Interception) Amendment Act 2006 and thus commences at the same time as the relevant provision of that Act.

Clause 3 Schedule(s)

Clause 3 provides that each Act that is specified in a Schedule is amended or repealed as set out in that Schedule.
Schedule 1 – Access to telecommunications data and co-operation with interception agencies

Part 1 – Main amendments

The purpose of this part is to transfer provisions in the Telecommunications Act relevant to access to telecommunications data by law enforcement and national security agencies to the TIA Act. The Blunn Report recommended the creation of comprehensive and over-arching legislation dealing with access to telecommunications data for the purposes of security and law enforcement, which should incorporate the relevant parts of the Telecommunications Act, principally elements of Parts 13, 14 and 15.

The amendments establish a regime for particular officers of the Australian Security Intelligence Organisation (ASIO) or an enforcement agency to lawfully authorise the disclosure of telecommunications data without breaching the general prohibitions on the disclosure of telecommunications data in sections 276, 277 and 278 of the Telecommunications Act.

The Telecommunications Act also provides that a carrier or carriage service provider must provide reasonably necessary assistance to an agency involved in safeguarding national security or enforcing the criminal law and laws imposing pecuniary penalties and protecting the public revenue. Carriers and carriage service providers provide this assistance in a number of ways, including having the capability to intercept telecommunications and deliver telecommunications data to the appropriate agency. Consistent with the recommendations of the Blunn Report, the provisions of the Telecommunications Act that deal with this capability, as well as those dealing with the associated assignment of costs, will be transferred to the TIA Act by the amendments in this part.

Item 1 – subsection 5(1)

Item 1 inserts a definition of ‘ACMA’ into subsection 5(1) of the TIA Act. ACMA is defined to mean the Australian Communications and Media Authority.

Item 2 – subsection 5(1)

Item 2 inserts a definition of ‘authorised officer’ in relation to an enforcement agency. An authorised officer is defined as the head or deputy head of an enforcement agency, persons acting in those positions, and individuals holding positions within that agency who are authorised to perform this function under new section 5AB.

The formulation of the definition reflects the differing management structures of enforcement agencies, particularly in the case of criminal law-enforcement agencies. An authorised officer has the power to authorise the disclosure of telecommunications data.
Item 3 – subsection 5(1)

Item 3 defines ‘Communications Access Co-ordinator’ by reference to the definition in new section 6R (inserted by Item 11).

Item 4 – subsection 5(1)

Item 4 inserts a definition of ‘criminal law-enforcement agency’. It is defined to mean a body covered by any of the paragraphs (a) to (k) of the definition of ‘enforcement agency’ in subsection 5(1). This definition is required as only criminal law-enforcement agencies will be able to access telecommunications data on a prospective basis. The definition is based on the current definition of criminal law-enforcement agency in subsection 282(10) of the Telecommunications Act, but does not include ‘a body or organisation responsible to the Australasian Police Ministers’ Council for the facilitation of national law enforcement support’ and the National Exchange of Police Information body, now known as the Ministerial Council for Police and Emergency Management – Police and the CrimTrac Agency respectively.

Item 5 – subsection 5(1)

Item 5 inserts a definition of ‘delivery point’. It is defined to mean a point nominated by a carrier or carriage service provider, or determined by ACMA under section 188 of the Act, of a location in relation to an agency, and is the location to which a carrier provides lawfully intercepted telecommunications content and intercept related information. Delivery points are significant to the cost allocation principles for the interception delivery capability obligations in Part 5-3 of the TIA Act and for the delivery capability obligations in Part 5-5 of the TIA Act.

Item 6 – subsection 5(1)

Item 6 amends subsection 5(1) to include a definition of ‘enforcement agency’. An authorised officer of one of these bodies will be able to authorise the disclosure of historical telecommunications data. The definition draws together the agencies described as ‘criminal law-enforcement agency’, ‘civil penalty-enforcement agency’ and ‘public revenue agency’ in section 282(10) of the Telecommunications Act. The definition includes bodies covered by the definition of ‘criminal law-enforcement agency’ in this subsection, as well as a body or organisation responsible to the Ministerial Council for Police and Emergency Management – Police, the CrimTrac Agency or any other body whose functions include administering a law imposing a pecuniary penalty or a law relating to the protection of the public revenue.

Items 7 and 8 – subsection 5(1)

Items 7 and 8 amend the definition of ‘interception agency’ to ensure that ASIO and agencies authorised to obtain interception warrants are consulted about interception capability plans prepared annually by carriers and nominated CSPs.
Item 9 – subsection 5(1)

Item 9 inserts a definition of ‘relevant staff member’ of an enforcement agency into subsection 5(1). A relevant staff member is the head of an agency, a deputy head of an agency or any employee, member of staff or officer of the enforcement agency. A relevant staff member of an enforcement agency is authorised to notify a carrier or carriage service provider of the making of an authorisation for the disclosure of historical or prospective telecommunications data.

Item 10 – After section 5AA

Item 10 inserts new section 5AB to give the head of an enforcement agency the authority to authorise a particular management position or management office in their organisation for the purposes of paragraph (c) of the definition of authorised officer in subsection 5(1). This will allow persons holding the authorised position or office to authorise the lawful disclosure of historical telecommunications data, or in the case of criminal law-enforcement agencies, historical and prospective telecommunications data.

New section 5AB reflects the current definition of an ‘authorised officer’ in section 282 of the Telecommunications Act. The use of the terms ‘management office’ or ‘management position’ are required to be broad in order to reflect the differing management structures for enforcement agencies, particularly in the case of criminal law-enforcement agencies. The head of an enforcement agency is able to take into account the operational requirements of their agencies in deciding which positions should be able to authorise the disclosure of telecommunications data.

For the purposes of Chapter 4 of the TIA Act (Access to telecommunications data), a management office or management position refers to a role of authority within an enforcement agency to which various management duties and functions are attached, and to which successive people can be appointed. It includes people who are temporarily appointed to that management office or management position. For example, a management office or management position in a criminal law-enforcement agency would include officers of the rank of Inspector (or equivalent) and above and may include unsworn or ‘non-police’ employees of equivalent rank. A management office or management position in a civilian based enforcement agency such as the Australian Taxation Office or the Australian Customs Service would include those employees at the Senior Executive Service (SES) level.

Subsection 5AB(2) requires the head of the enforcement agency to give the Communications Access Co-ordinator a copy of any authorisations made under this section. This will allow the Communications Access Co-ordinator to monitor the appropriate use of the authorisation power.

Subsection 5AB(3) states that these authorisations are not legislative instruments. This clarifies the fact that these authorisations are internal administrative matters and are not legislative instruments.
Item 11 – At the end of Part1-2

Item 11 inserts new section 6R that defines ‘Communications Access Co-ordinator’. The Communications Access Co-ordinator replaces the concept of Agency Co-ordinator in the Telecommunications Act and reflects the expanded role of the Communications Access Co-ordinator as the first point of contact for both the telecommunications industry and agencies in relation to access to telecommunications information.

Subsection 6R(1) states that the Communications Access Co-ordinator means the Secretary of the Department or such other person or body specified by the Minister by legislative instrument. The role of Agency-Coordinator is currently performed by a First Assistant Secretary position in the Attorney-General’s Department, nominated by the Minister. Subsection 6R(2) would allow the Minister to similarly specify a person or position to perform the role of Communications Access Coordinator.

Subsection 6R(3) states that unless stated otherwise, an act done by or in relation to the Communications Access Co-ordinator will be on behalf of, or in relation to, all interception agencies. This is because the Communications Access Coordinator coordinates the views of agencies and acts having regard to their advice.

Item 12 – After Chapter 3

Item 12 inserts a new Chapter 4 into the TIA Act. This new Chapter provides for access to telecommunications data by national security and law enforcement agencies.

Chapter 4 – Access to telecommunications data

Part 4-1 – Permitted access to telecommunications data

Telecommunications data is information about a telecommunication, but does not include the content or substance of the communication. Telecommunications data is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet based applications including internet browsing and voice over internet telephony.

For telephone-based communications, telecommunications data includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet based applications, telecommunications data includes the Internet Protocol (IP) address used for the session and the start and finish time of each session.

Telecommunications data specifically excludes the content or substance of a communication.

Currently, the use and disclosure of this data is generally prohibited under sections 276, 277 and 278 of the Telecommunications Act. Sections 282 and 283 allow access to this data for specific law enforcement and national security purposes.
New Chapter 4 transfers sections 282 and 283 of the Telecommunications Act to the TIA Act. The basis for lawful access will depend on whether the authorising body is ASIO, a criminal law-enforcement agency or an enforcement agency.

The new provisions distinguish between access to historical telecommunications data (data that is already in existence at the time of the request) and prospective data (data that is collected as it is created and forwarded to the agency in near real time). Access to prospective telecommunications data is only available to ASIO or a criminal law-enforcement agency because of the higher privacy implications of this type of access.

Chapter 4 contains a general prohibition on access to telecommunications data followed by a list of exceptions.

The general prohibitions at sections 276, 277 and 278 of the Telecommunications Act provide that carriers, carriage service providers, number data-base operators, emergency call persons and their respective associates, must protect the confidentiality of information that relates to:

- the contents of communications that have been, or are being, carried by carriers or carriage service providers;
- carriage services supplied; and
- the affairs or personal particulars of other persons.

Part 13 of the Telecommunications Act continues to contain both these general prohibitions and those exceptions that are not specific to national security and law enforcement purposes and are accessed more generally. These include instances where:

- the disclosure or use is required by, or under, a Commonwealth, State or Territory law;
- assisting the ACMA, the Australian Competition and Consumer Commission or the Telecommunications Industry Ombudsman;
- circumstances where there is a perceived threat to a person’s life or health;
- calls to emergency service numbers; and
- communications for maritime purposes.

Chapter 4 of the TIA Act contains provisions dealing with permitted access to telecommunications data and procedural requirements relating to authorisations, which were previously contained in the Telecommunications Act.

**Division 1 – Outline of Part**

171 – Outline of Part

New subsection 171(1) explains that the new Part provides exceptions to the general prohibition on the disclosure and use of telecommunications data under the Telecommunications Act. These are set out in Division 3 for ASIO and Division 4 for enforcement agencies.
New subsection 171(2) notes that new Division 5 provides for certain exceptions to the general prohibition on the use of telecommunications data that has been lawfully disclosed under Division 3 or 4.

New subsection 171(3) notes that new Division 6 creates an offence for secondary use and/or disclosure of lawfully obtained telecommunications data.

**Division 2 – General Provisions**

**172 – No disclosure of the contents or substance of a communication**

New section 172 makes clear that Divisions 3 and 4 of the Act cannot be used to access the content or substance of a communication. If an agency wishes to covertly obtain the content of a communication under the TIA Act, they would be required to use the provisions in Chapters 2 or 3 regulating telecommunications interception and access to stored communications respectively.

This section does not affect the lawful access to or disclosure of telecommunications information via other legislative means. For example, provisions in Part 13 of the Telecommunications Act permit the disclosure of information or a document, including the contents or substance of a communication, in limited circumstances.

Communications associated data will vary according to the type of telecommunications service. For fixed and mobile voice telephony, including voice calls, and voice- or text-messaging services, the term includes the details of the parties to the communication, the date, time and duration of the communication, the device used to send or receive the information, and (in some cases) the locations of the parties.

For Internet based telecommunications, such as email, web browsing, instant messaging, or internet voice calls (Voice over Internet Protocol or VoIP), data includes the sender’s and recipient/s’ Internet Protocol (IP) addresses, the devices from which they were sent from or to, and the time and date at which it was sent. The information does not include content such as the subject line of an email, the message sent by email or instant message or the details of Internet sessions, such as the Uniform Resource Locator/Identifier (URL/URI).

**173 – Effect of Divisions 3 to 6**

The transfer of national security and law enforcement specific exceptions from the Telecommunications Act to the TIA Act will result in exceptions to the general prohibitions on access to telecommunications data being contained in both the Telecommunications Act and the TIA Act.

New Section 173 ensures that new Divisions 3 to 5 of the TIA Act do not affect or limit the generality of anything else in Divisions 3 to 5 of the TIA Act or the prohibitions and exceptions remaining in Subdivision A of Division 3 of Part 13 of the Telecommunications Act.
Division 3 – The Organisation

New Division 3 of the TIA Act outlines the circumstances in which the Australian Security Intelligence Organisation (ASIO) can access telecommunications data.

174 – Voluntary disclosure

New subsection 174(1) permits an employee or a carrier or carriage service provider to disclose information relevant to ASIO in the performance of its functions. This provision is based on subsection 283(1) of the Telecommunications Act. Subsection 313(5) of the Telecommunications Act protects a carrier or carriage service provider from liability if the disclosure is made in good faith.

New subsection 174(2) makes it clear that this provision only applies in the case of a voluntary disclosure. New sections 175 and 176 deal with requests for information by ASIO.

175 – Authorisation for access to existing information or documents

New section 175 transfers the obligations currently set out in subsection 283(2) of the Telecommunications Act and deals with the disclosure of telecommunications data that is in existence before the time the provider from whom the disclosure is sought is notified that an authorisation has been made. New section 175 provides that the general prohibitions on disclosure in sections 276, 277 and 278 of the Telecommunications Act do not prohibit the disclosure of telecommunications data if the disclosure is authorised by the Director-General of Security, the Deputy-General of Security or an officer or employee of ASIO who has been approved by the Director-General of Security to authorise disclosures of telecommunications data. The note at the end of new subsection 175(2) refers to new section 184, which specifies requirements for the notification of authorisations.

New subsection 175(3) provides that an eligible person must not authorise the disclosure of telecommunications data unless he or she is satisfied that the disclosure would be in connection with the performance by ASIO of its functions. ASIO’s functions are set out in the Australian Security Intelligence Organisation Act 1979.

New subsection 175(4) allows the Director-General of Security to approve, in writing, an officer or employee of ASIO to be an eligible person to authorise the disclosure of telecommunications data.

176 – Authorisation for access to prospective information or documents

New section 176 deals with the disclosure of prospective telecommunications data on an ongoing basis. Due to the higher privacy impact of the disclosure of information on a prospective basis, a higher level of authorisation is required than for access to existing information. The access provided under new section 176 occurs in near real-time and is ongoing for the duration of the authorisation.

The need to distinguish between historical and prospective data is a reflection of the advances in technology, which enables telecommunications data to provide location
information. To reflect the increased privacy implications of accessing this information, it is necessary to distinguish this type of access to historical data and attach more restrictive conditions to access.

New subsections 176(1) and 176(2) provide that a carrier or carriage service provider may disclose telecommunications data that comes into existence during the period that an authorisation is in force, if the disclosure is authorised by an eligible person. An eligible person is the Director-General of Security, the Deputy Director-General of Security and an officer or employee of ASIO who either holds, or is acting in a position equivalent to or higher than, a Senior Executive Service Band 2 position in the Department.

New subsection 176(3) provides that an authorisation for the disclosure of prospective information may also authorise access to information that came into existence before the authorisation is received by the carrier or carriage service provider. This permits the authorisation to cover access to both historical and prospective telecommunications data, and avoids the need for a separate application under new section 175.

New subsection 176(4) provides that the person making the authorisation must not make the authorisation unless he or she is satisfied that the disclosure would be in connection with the performance of ASIO’s functions.

New subsection 176(5) provides that a prospective authorisation comes in to force when the person from whom information is sought or to whom the request is addressed receives notification that an authorisation has been made.

Note that new section 183 provides that a notification of an authorisation must be in written or electronic form and comply with any requirements as determined by the Communications Access Co-ordinator. It is not necessary for an actual copy of the authorisation to be provided to the person from whom the disclosure is sought. The note following new subsection 176(5) makes reference to new section 184, which provides that any officer or employee of ASIO (not only the authorising officer) may provide the notification.

A prospective authorisation operates for the period of time defined in the authorisation, which cannot exceed 90 days in duration, unless the authorisation is revoked earlier.

If at any time before the nominated period of time expires, a person who made a prospective authorisation is satisfied that the reasons for the granting of the authorisation no longer exist, he or she must revoke the authorisation. New section 184 requires that the person who was notified of the original authorisation be notified of the revocation of the authorisation.

**Division 4 – Enforcement agencies**

New Division 4 of the TIA Act outlines the circumstances in which enforcement agencies can access telecommunications data. An enforcement agency is defined by item 6 to mean bodies covered by the definition of ‘criminal law-enforcement
agency’, as well as a body or organisation responsible to the Australasian Police
Minister’s Council for the facilitation of national law enforcement support, the
CrimTrac Agency, or any other body whose functions include administering a law
imposing a pecuniary penalty or a law relating to the protection of the public revenue.

177 – Voluntary disclosure

New section 177 permits an employee of a carrier or carriage service provider to
disclose relevant information to an enforcement agency, for the enforcement of the
criminal law, a law imposing a pecuniary penalty or the protection of the public
revenue. This provision is based on subsection 282(1) of the Telecommunications
Act. Subsection 313(5) of the Telecommunications Act protects a carriage or carriage
service provider from liability if the disclosure is made in good faith.

New subsection 177(3) makes it clear that this provision only applies in the case of a
voluntary disclosure. New sections 178, 179 and 180 deal with requests for
information by enforcement agencies.

178 – Authorisations for access to existing information or documents –
enforcement of the criminal law

New section 178 permits disclosure of existing telecommunications data where the
disclosure is authorised by an authorised officer of an enforcement agency for the
enforcement of the criminal law. An authorised officer is defined by item 2 as the
head of the organisation, the deputy head of the organisation or a management
position or office that is authorised in writing by the head of the organisation.

Subsection 178(3) states that an authorised officer of an enforcement agency must not
authorise the disclosure of telecommunications data unless he or she is satisfied that
the disclosure is reasonably necessary for the enforcement of the criminal law. The
note following new subsection 178(2) makes reference to new section 184 that
specifies the requirements for the notification of authorisations.

179 – Authorisations for access to existing information or documents –
enforcement of a law imposing a pecuniary penalty or protection of the public
revenue

New section 179 permits disclosure of existing telecommunications data where the
disclosure is authorised by an authorised officer of an enforcement agency for the
enforcement of a law imposing a pecuniary penalty or the protection of the public
revenue.

Subsection 179(3) states that an authorised officer of an enforcement agency must not
authorise the disclosure of telecommunications data unless he or she is satisfied that
the disclosure is reasonably necessary for the enforcement of a law imposing a
pecuniary penalty or the protection of the public revenue.
180 – Authorisations for access to prospective information or documents

New section 180 deals with the disclosure of prospective information to a criminal law enforcement agency on an ongoing basis. The access provided under new section 180 occurs in near real-time and is ongoing for the duration of the authorisation.

The need to distinguish between historical and prospective data is a reflection of the advances in technology which enables the use of telecommunications data to provide location information. To reflect the increased privacy implications of access to prospective telecommunications data, three more restrictive conditions are attached to these authorisations:

- restricting the disclosure of prospective telecommunications data to an authorised officer of a criminal law-enforcement agency, for the investigation of offences which attract a maximum term of imprisonment of at least 3 years;
- limiting the timeframe for which an authorisation may be in force to 45 days; and
- requiring the authorising officer to have regard to the impact of the authorisation on the privacy of the individual concerned.

New subsections 180(1) and 180(2) provide that a carrier or carriage service provider may disclose telecommunications data that comes into existence during the period that an authorisation is in force if the disclosure is authorised by an authorised officer of a criminal law-enforcement agency.

New subsection 180(3) provides that an authorisation may also provide for access to information that came into existence before the authorisation is received by the carrier or carriage service provider.

New subsection 180(4) provides that the person making the authorisation must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the investigation of an offence that is punishable by imprisonment for at least 3 years.

New subsection 180(5) provides that the person making the authorisation must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure. This would include, for example, an assessment of the value of the information sought compared to the privacy of the user or users of the telecommunications service in question.

New subsection 180(6) provides that a prospective authorisation comes into force when the person from whom the telecommunications data is sought receives notification of the authorisation. The authorisation operates for a period of time that is defined by the authorisation not exceeding 45 days, or until the authorisation is revoked. The note following subsection 180(6) makes reference to new section 184 which specifies the requirements for the notification of authorisations.

New subsection 180(7) provides that any authorised officer must revoke an authorisation if he or she is satisfied that the reasons for the granting of the authorisation no longer exist.
Division 5 – Uses of telecommunications data connected with provision of access

181 – Uses of telecommunications data connected with provision of access

New section 181 provides an exception to the general prohibitions at sections 276, 277 and 278 of the Telecommunications Act on the use (as distinct from the initial disclosure) of telecommunications data, provided that the use of the data is for the purposes of, or connected with, the lawful original disclosure of information under either Division 3 (ASIO access to telecommunications data) or Division 4 (enforcement agencies access to telecommunications data) of Chapter 4.

For example, where a carrier discloses telecommunications data to a police officer in response to an authorisation relating to an investigation of a criminal offence, the receiving agency is permitted to use that information for all aspects of that investigation including providing it to other members of the investigative team.

Division 6 – Secondary disclosure/use offence

New Division 6 regulates the subsequent disclosure and use of lawfully obtained telecommunications data by officers of an enforcement agency.

182 – Secondary disclosure/uses offence

New section 182 creates an offence where a person discloses or uses telecommunications data received by reason of a lawful disclosure to an enforcement agency under Division 4. Commission of the offence attracts a penalty of two years imprisonment.

New subsection 182(2) outlines the circumstances in which secondary disclosures are permitted. An enforcement agency may pass telecommunications data on to a third party for specified purposes set out in this section. These are a disclosure to ASIO for the performance of its functions, or a disclosure that is reasonably necessary for the enforcement of the criminal law, the enforcement of a law imposing a pecuniary penalty, or the protection of the public revenue. The purposes for which telecommunications data may be used are based on the primary disclosure uses currently permitted by sections 282 and 283 of the Telecommunications Act.

For example, if during the course of an investigation of a person for taxation fraud, the Australian Taxation Office obtains telecommunications data that suggests the involvement of that person in child pornography (based on the nature of IP addresses that person has been visiting), the Australian Taxation Office could lawfully disclose this information to a relevant police agency to investigate.

Similarly, new subsection 182(3) sets out the circumstances in which secondary disclosure is permitted.
The note following new subsections 182(2) and (3) indicates that where a person is charged in relation to a contravention of new section 182, the defendant bears an evidential burden of proof to demonstrate that the disclosure or use was lawful.

**Part 4-2 – Procedural requirements relating to authorisations**

New Part 4-2 outlines the procedural requirements associated with the making of an authorisation, by ASIO or an enforcement agency, for access to telecommunications data. These requirements include ensuring that:

- the authorisation, revocations and notifications are in the proper format
- authorisations are properly notified to the person from whom the disclosure is sought, and
- the authorisations are kept by ASIO or the enforcement agency.

New Part 4-2 also outlines the responsibility of enforcement agencies to report to the Minister regarding the number of authorisations issued. It also empowers the Communications Access Co-ordinator to specify additional requirements in relation to authorisations, revocations and notifications in the form of a legislative instrument.

**183 – Form of authorisations and notifications**

New section 183 provides that an authorisation, a revocation and notification of an authorisation or revocation by ASIO or an enforcement agency must comply with any requirements determined by the Communications Access Co-ordinator and be in either written or electronic form. This may include a paper document sent by mail, a fax, an email or a communication transmitted by a specialised electronic authorisation system.

New subsection 183(2) gives the Communications Access Co-ordinator the authority, by legislative instrument, to determine the requirements for an authorisation to access telecommunications data made under Division 3 or 4 of Chapter 4. The purpose of this provision is to allow the Communications Access Co-ordinator to manage compliance with the legislation and improve the operational efficiency of the regime. This provision relates only to the procedural obligations of requesting agencies and does not create any additional obligations for carriers or carriage service providers.

New subsection 183(3) provides that before making a determination in relation to authorisations, the Communications Access Co-ordinator must consult with ACMA and the Privacy Commissioner. This is to ensure that the interests of the telecommunications industry, as well as broader privacy interests are properly taken into consideration in relation to any determination made.

**184 – Notification of authorisations or revocations**

New subsection 184(1) requires an officer or an employee of ASIO to notify the carrier or carriage service provider from which the telecommunications data is sought when an authorisation is made. The authorisation comes into force once the notification of the authorisation has occurred.
New subsection 184(2) requires an officer or an employee of ASIO to notify the carrier or carriage service provider when an authorisation is revoked.

New Subsection 184(3) and (4) specify equivalent notification requirements for enforcement agencies.

185 – Retention of authorisations

New section 185 requires enforcement bodies to retain any authorisations for access to telecommunications data made under new Chapter 4 of the TIA Act for a period of three years.

These requirements operate in conjunction with sections 305, 306 and 307 of the Telecommunications Act, which require carriers and carriage service providers to retain the details of the notifications they receive and report to the ACMA on the number of disclosures made.

186 – Report to Minister

New section 186 requires enforcement agencies to report annually, and no later than within 3 months of the end of the financial year, to the Minister regarding their access to telecommunications data. This information will assist in monitoring the granting of authorisations to access telecommunications data.

Each enforcement agency’s report must include statistics on the number of authorisations made during the previous financial year for:

- the disclosure of existing telecommunications data for the enforcement of the criminal law
- the disclosure of existing telecommunications data for the purpose of enforcing a law imposing a pecuniary penalty or the protection of the public revenue
- the disclosure of prospective telecommunications data for the enforcement of the criminal law, and
- any other mater requested by the Minister in relation to those authorisations.

New subsections 186(2) and (3) require the Minister to prepare a report containing the information provided by enforcement agencies and to table the report in each house of Parliament within 15 sitting days after the report is completed.

New subsection 186(4) provides that a report made under this section must not be made in a manner that is likely to enable the identification of a person and through this ensures that reporting on access to telecommunications data does not impact on the privacy of individuals.

Chapter 5 – Co-operation with interception agencies

New Chapter 5 sets out the obligation for carriers and carriage service providers to ensure that communications carried over their telecommunications system are capable
of being intercepted. New Chapter 5 is based on relevant provisions in Parts 14 and 15 of Telecommunications Act.

**Part 5-1 – Definitions**

187 – Definitions

New section 187 provides the definitions of *interception capability* and *delivery capability*. These definitions aim to provide identical obligations to those currently in section 320 of the Telecommunications Act. Slight differences in language are intended to ensure consistency with the terminology of the new provisions with those already in place in the TIA Act. The changes also update the terminology to better accommodate the wider range of telecommunications applications now in use.

New subsection 187(1) notes that the two concepts of interception capability and delivery capability do not overlap.

New subsection 187(2) defines *interception capability* to mean the capability to enable a communication passing over the system to be intercepted and for lawfully intercepted information to be transmitted to the relevant delivery points.

This definition draws on the definition of telecommunications service, telecommunications system and communication which are contained in Section 5 of the TIA Act.

As such, the definition of interception capability continues to mean the ability to intercept and deliver content of any of a wide variety of telecommunications services, including voice conversations, emails, instant messaging and web browsing.

In new subsection 187(3), *delivery capability* is a telecommunications service that involves, or will involve, the use of a telecommunications system, means the capability of that kind of service or of that system to enable lawfully intercepted information to be delivered to interception agencies from the delivery points applicable in respect of that kind of service.

**Part 5-2 – Delivery Points**

A delivery point is a defined place to which intercepted information can be delivered. Part 5-2 requires a carrier or carriage service provider to nominate delivery points, and provides the process for resolving instances where an agency does not agree to the location of the nominated delivery point, and the process for changing a delivery point. This Part is based on section 314A of the Telecommunications Act.

188 – Delivery Points

New section 188 provides a process for defining delivery points.

New subsection 188(1) requires a carrier or carriage service provider to nominate at least one place in Australia to be a delivery point in respect of each kind of
telecommunications service and each interception agency, from which intercepted information can be delivered to that agency. The carrier or carriage service provider must inform the Communications Access Co-ordinator of the nominated delivery point. The number of nominated delivery points may vary according to the carrier/agency’s location, the nature of the carrier’s network and the kinds of services which are provided.

New subsections 188(2)–(5) deal with disagreements over delivery points. New subsection 188(2) provides that the Communications Access Co-ordinator may at any time notify a carrier or carriage service provider that an interception agency does not agree with the location of the nominated delivery point. New subsection 188(3) provides that the carrier or carriage service provider, being so notified, must nominate a new delivery point, and inform the Communications Access Co-ordinator accordingly.

New subsection 188(4) provides that, if the new nominated delivery point is still unsatisfactory to the interception agency, the Communications Access Co-ordinator must inform the carrier or carriage service provider accordingly, and refer the matter to the ACMA for determination. New subsection 188(5) provides that, after hearing the views both of the carrier or carriage service provider and the interception agency as to the best location of the delivery point, the ACMA must determine the final location of the delivery point.

New subsection 188(6) provides that in determining the location of a delivery point, the carrier or carriage service provider, the interception agency or the ACMA must have regard to: (a) the configuration of the service; (b) the relative costs to the carrier and to the interception agency of any particular delivery point; (c) the reasonable needs of the interception agency; (d) the reasonable commercial requirements of the carrier; and, (e) the location of any delivery points already existing in relation to any particular interception agency.

New subsection 188(7) provides that the location of the nominated delivery point need not be the place where the interception takes place if, according to the criteria in new subsection 188(6), a more suitable location exists.

New subsections 188(8)–(10) deal with subsequent changes to delivery points determined by the ACMA.

New subsection 188(8) provides that, if the location of the delivery point as determined by the ACMA becomes unsuitable as a result of a material change in the circumstances of the carrier, the carrier may nominate another place, and must inform the Communications Access Co-ordinator accordingly. New subsection 188(9) provides that an interception agency may request another place as the delivery point, in which case, the carrier or carriage service provider must nominate another delivery point and inform the Communications Access Co-ordinator accordingly.

New subsection 188(10) states that subsections 188(2) – (7) apply to a nominations made under new subsections 188(8) and (9) (dealing with changing delivery points). This ensures the provisions covering disagreements over nominated delivery points,
and the factors to be taken into account in determining a delivery point set out in subsection 188(6) apply.

Part 5-3 – Interception capability

Part 5-3 consists of two Divisions. New Division 1 (new sections 189–191) deals with obligations on carriers and carriage service providers to provide interception capability. The new Division 2 (new sections 192 and 193) provides a mechanisms for the Communications Access Coordinator to grant exemptions from these obligations.

Division 1 – Obligations

189 – Minister may make determinations

New section 189 enables the Attorney-General to make written determinations on the interception capability or special assistance capability in respect of certain specified carriage services. This is based on section 322 of the Telecommunications Act.

New section 189 includes minor variations to ensure consistency with the terminology of the TIA Act and omits redundant references to special assistance capability.

New subsection 189(1) provides that the Minister may, by legislative instrument, make determinations on interception capabilities applicable to specific telecommunications services.

New subsection 189(2) requires that a determination must specify an international standard or guidelines, or the relevant part of the international standard, on which the determination is based. It must also provide for interception capability by adopting, applying or incorporating the whole or a part of the international standard, with only such modifications as are necessary to facilitate the application of the standard in Australia. Finally, the determination must be accompanied by a copy of the international standard or of the relevant part of the international standard.

New subsection 189(3) provides that the international standard specified in a determination must deal primarily with the requirements of interception agencies in relation to the interception of communications passing over a telecommunications network and related matters, and may be a part of an international agreement or arrangement or a proposed international agreement or arrangement.

New subsection 189(4) lists the matters which the Minister must to take into account before making a determination, which are: the interests of law enforcement and national security; the objects of the Telecommunications Act; and the privacy of the users of telecommunications systems. New subsection 189(5) permits the Minister to take into account any other matter considered relevant, and might include technological or industry factors for example.

The inclusion of the objects of the Telecommunications Act in new paragraph 189(4)(b) is to maintain the existing application of the objects of that Act to any decision under section 322. The objects of the Telecommunications Act are stated at
section 3 and include the provision of a regulatory framework that promotes the long-
term interests of end-users of carriage services, or of services provided by means of
 carriage services; and the efficiency and international competitiveness of the
 Australian telecommunications industry.

190 – Obligations of persons covered by a determination

New section 190 transfers the obligations currently set out in section 323 of the
Telecommunications Act.

New subsection 190(1) provides that if a determination is made in relation to a
particular kind of telecommunication service, each carrier and carriage service
provider supplying that kind of service must comply with the determination.
New subsection 190(2) provides that if a carrier is required to have an interception
capability, a carrier or carriage service provider must develop, install and maintain the
interception capability.

191 – Obligations of persons not covered by a determination in relation to a kind
of telecommunications service

New section 191 transfers the obligations currently set out in section 324 of the
Telecommunications Act.

New subsection 191(1) provides that, where a specific determination under section
189 does not apply, a carrier must maintain a general interception capability that
enables them to execute an interception warrant and transmit the intercepted
information to a delivery point. New subsection 191(2) provides that, to comply with
new subsection 191(1), carriers and carriage service providers are required to develop,
install and maintain the general interception capability.

Division 2 – Exemptions

192 – The Communications Access Co-ordinator may grant exemptions

New section 192 transfers the capacity to grant exemptions from interception
capability obligations currently contained in section 326 of the Telecommunications
Act.

New subsection 192(1) provides that the Communications Access Co-ordinator may
exempt a person from all or some of the interception capability obligations in respect
of a specified kind of telecommunications service.

This provision recognises that in certain instances, a carrier may not achieve complete
technical compliance in relation to a particular service or some aspect of that service,
but that the non-compliance has limited implications for law enforcement or national
security agencies.

New subsection 192(2) requires that any exemption may only be granted in writing.
New subsection 192(3) provides that the exemption may be unconditional or subject
to any condition. Such conditions may include limits on the time for which the
exemption applies, limits on the numbers of customers or the geographic scope of a particular type of service, or requirements for ongoing consultations with agencies.

New subsection 192(4) provides that the exemption is not a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act 2003*. This clarifies the fact that these exemptions are administrative in nature and apply only to individual carriers or carriage service providers and also by reason of the sensitive nature of interception capability obligations. If such documents were not kept confidential, the limitations of interception capability and, by implication, how to avoid interception, could become publicly apparent.

New subsection 192(5) provides that where a person has applied in writing for an exemption from all, or particular, interception capability obligations and the Communications Access Co-ordinator does not respond within 60 days, an exemption is deemed to have been granted to that person. This provision is intended to ensure that the Communications Access Co-ordinator resolves applications in a timely manner and provides certainty for carriers and carriage service providers as to their legal obligations under the TIA Act at any given time.

New subsection 192(6) provides that the deeming exemption under new subsection 192(5) is temporary as the deemed exemption only has effect until the Communications Access Co-ordinator communicates a decision on the application to the applicant.

New subsection 192(7) requires that, in granting an exemption, the Communications Access Co-ordinator must take into account both the interests of law enforcement and national security, and the objects of the Telecommunications Act. New subsection 192(8) enables the Communications Access Co-ordinator to take into account any other relevant matter when deciding whether or not to grant an exemption, which might include relevant technological or industry factors.

193 – ACMA may grant exemptions for trial services

New section 193 transfers the obligations currently set out is based on section 327 of the Telecommunications Act.

New subsection 193(1) provides that the ACMA may exempt a person from all or some of the interception capability obligations in respect of a trial service.

Service providers sometimes trial services on a small scale to assess technical and commercial viability. The lack of interception capability on such trial services may create little if any operational risk to law enforcement or national security. This provision allows ACMA to grant an exemption from interception obligations in these cases. ACMA may tailor the exemption and any conditions to the particular circumstances of each case.

New subsection 193(2) provides that the ACMA, before granting the exemption for a trial service, must consult any appropriate interception agency and satisfy itself that the exemption is unlikely to create a risk to national security or law enforcement.

New subsection 193(3) provides that the exemption for a trial service may only be
granted in writing. New subsection 193(4) provides that the exemption for a trial service may be unconditional or subject to any condition.

New subsection 193(5) provides that the exemption is not a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act 2003*. This clarifies the fact that these exemptions are administrative in nature and apply only to individual carriers or carriage service providers and also by reason of the sensitive nature of interception capability obligations. If such documents were not kept confidential, the limitations of interception capability and, by implication, how to avoid interception, could become publicly apparent.

**Part 5-4 – Interception capability plans**

Part 5-4 is based on sections 329 – 332D of the Telecommunications Act.

Part 5–4 (new sections 194–202) requires carriers and nominated carriage service providers to comply with the obligations to prepare and submit an annual Interception Capability Plan (IC Plan). IC Plans are designed to be a systematic way of addressing, ahead of time, the base interception capability of carriers and nominated carriage service providers.

**194 – Definitions**

New section 194 defines *carriage service provider* and *carrier* as having the same meanings as in the Telecommunications Act. *Nominated carriage service provider* is defined as a carriage service provider that is declared under subsection 197(4) by the Minister to be a nominated carriage service provider.

It should be noted that the definition of carriage service provider for the purposes of this part differs to that applicable to the remainder of the TIA Act. In the general definition contained in section 5 ‘carrier’ means both carrier and carriage service provider. In this part alone, they retain separate meanings. This is because only carriage service providers nominated by the Minister under new subsection 197(4) are required to submit an annual IC Plan.

**195 – Nature of an interception capability plan**

New section 195 reproduces the IC Plan requirements currently set out in subsections 329(1) and (2) of the Telecommunications Act.

New subsection 195(1) provides that an IC Plan must be in writing and comply with requirements set out in subsections 195(2) and (3).

New paragraph 195(2)(a) requires the IC Plan to include a statement of the carrier or provider’s policies and strategies for compliance with its legal obligation to provide interception capabilities for each particular kind of telecommunications service that it provides.
New paragraph 195(2)(b) requires the IC Plan to include a statement of compliance with that legal obligation. This may include detailed indications of the exact types of information that may be supplied in relation to a particular type of service.

New paragraph 195(2)(c) requires the IC Plan to include a statement of any relevant developments in the business of the carrier or provider within 5 years of the commencement of the plan that, if implemented, are likely to affect interception capability. These factors could include a change in the security policy of the carrier, the introduction of new telecommunications products or services, a significant change in the location of the company or parts of the company, or a change in marketing or pricing of services.

New paragraph 195(2)(d) requires the IC Plan to provide a statement of the locations at which communications are physically intercepted. This information is needed for the consideration of matters such as delivery points and associated delivery processes.

New paragraph 195(2)(e) requires the IC Plan to include a list of employees of the carrier or provider who have responsibility for interception and other related matters. This is necessary to ensure the proper protection of interception information and includes information about warrants issued, and material gathered under those warrants.

New paragraph 195(2)(f) also requires carriers and providers to address in their IC Plan any other matters determined by the Minister, by legislative instrument under subsection 195(4). This may include new requirements needed on the basis of security or technology developments and mirrors the requirements in section 329(2) of the Telecommunications Act.

New subsection 195(3) provides that the IC Plan must be approved by the chief executive officer (however described) of the carrier or provider or by a person who has been authorised in writing by the chief executive officer to approve the IC Plan.

New subsection 195(4) provides the determination making power referred to in new paragraph 195(2)(f).

New subsection 195(5) provides that the Minister must consult the ACMA before making a determination.

New subsection 195(6) provides that an IC Plan is not a legislative instrument for the purposes of section 5 of the Legislative Instruments Act 2003. This reflects the commercially and operationally confidential nature of the information contained within the IC Plan.

196 – Time for giving IC Plans by carriers

New section transfers the IC Plan lodgement time for carriers that is currently set out in section 330 of the Telecommunications Act.
Under new subsection 196(1), IC Plans are to be provided to the Communications Access Co-ordinator. ACMA’s role as the arbiter of disputes between carriers and agencies is set out under subsection 198(5).

New subsection 196(1) provides that a carrier must provide an IC Plan to the Communications Access Co-ordinator by 1 July each year. This date may be changed with the agreement of the Communications Access Co-ordinator in respect of a particular 12 month period. Under the transitional provisions, an IC Plan in force at the time at which this provision comes into effect, will remain valid (see Schedule 1 Part 3, Item 66).

New subsection 196(2) provides that if a later date is agreed to by the Communications Access Co-ordinator, the Communications Access Co-ordinator must inform the ACMA.

New subsection 196(3) deals with future carriers and provides that a person or body that becomes a carrier must provide an IC Plan to the Communications Access Co-ordinator within 90 days of becoming a carrier.

197 – Time for giving IC Plans by nominated carriage service providers

New section 197 transfers the IC Plan lodgement time for nominated carriage service providers, which is currently set out in section 331 of the Telecommunications Act.

As with new subsection 196(1), IC Plans are only to be provided to the Communications Access Co-ordinator, and not ACMA as in the existing provision. ACMA’s role as the arbiter of disputes between carriers and interception agencies is set out under subsection 198(5).

New subsection 197(1) provides that a nominated carriage service provider must provide an IC Plan to the Communications Access Co-ordinator by 1 July each year. This date may be changed by agreement of the Communications Access Co-ordinator in respect of a particular 12 month period. Under the transitional provisions, an IC Plan in force at the time at which this provision comes into effect, will remain valid, (see Schedule 1 Part 3, Item 66).

New subsection 197(2) provides that if a later date is agreed to by the Communications Access Co-ordinator, the Communications Access Co-ordinator must inform the ACMA.

New subsection 197(3) deals with future nominated carriage service providers and provides that a person or body that becomes a carrier must provide an IC Plan to the Communications Access Co-ordinator within 90 days of becoming a carrier. However, new paragraph 197(1)(b) would still apply to enable the Communication Access Co-ordinator to extend the timeframe for the lodgement of the following IC Plan if the first IC Plan is lodged shortly before 1 July in any given year. This replaces subsection 331(2).

New subsections 197(4) and (5) set out the Minister’s power to declare a nominated carriage service provider. New subsection 197(4) provides that the Minister may
declare a carriage service provider to be a nominated carriage service provider. The effect is that the nominated carriage service provider is required to lodge an IC Plan. This enables the Communications Access Co-ordinator to ensure that interception capability obligations are met in particular identified circumstances, without the need to create a general obligation on all carriage service providers.

The new subsection 197(5) provides that the declaration is not a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act 2003*.

**198 – Consideration of IC Plans**

New section 198 transfers the obligations currently set out in section 332C of the Telecommunications Act. New section 198 which sets out a process, managed by the Communications Access Co-ordinator, by which agencies are given an opportunity to comment on IC Plans, carriers or nominated service providers to respond to those comments, and for the ACMA to resolve any disputes.

New subsection 198(1) provides that, after receiving an IC Plan, the Communications Access Co-ordinator must within 60 days either approve the IC Plan, or request that the IC Plan be amended to take account of specified matters.

New subsection 198(2) deals with consultation with interception agencies. It provides that as soon as possible after receiving an IC Plan, the Communications Access Co-ordinator must provide copies of the IC Plan to relevant interception agencies for their comment and an information copy to the ACMA.

New subsection 198(3) deals with requests to amend an IC Plan. It provides that if the Communications Access Co-ordinator receives a comment from the agencies, which the Co-ordinator considers reasonable, the Co-ordinator must provide a copy or summary to the carrier or provider. The carrier or nominated carriage service provider is required to respond within 30 days of receiving the comments or summary.

Allowing the Communications Access Co-ordinator to provide a copy or a summary of comments received replaces the existing requirement that the Agency Co-ordinator must provide all comments to a carrier or nominated carriage service provider. This discretion will allow the Communications Access Co-ordinator to pass on only those comments that are considered reasonable or to summarise a number of similar agency comments into one consolidated response. It also reflects the fact that in some cases, elements of an agency response may contain classified information intended to assist the Communications Access Co-ordinator but that should not pass to the carrier or nominated carriage service provider. However, any comment that is relied upon for a decision by the Communications Access Co-ordinator is required to be provided to the carrier or nominated carriage service provider.

New subsection 198(4) provides that the carrier or provider may respond to a request to amend an IC Plan either by amending the IC Plan in accordance with the request or indicating that it does not accept the request.
New subsections 198(5) and (6) deal with the ACMA’s power to resolve disagreements between interception agencies and a carrier or provider in relation to an IC Plan.

New subsection 198(5) provides that if a carrier or provider does not accept a request to amend an IC Plan, the Communications Access Co-ordinator must refer the request and the carrier’s or provider’s comments to the ACMA for determination.

New subsection 198(6) provides that the ACMA must make a determination in writing that either:

- no amendment of the IC Plan is required; or
- if the request is a reasonable one, and the carrier’s or provider’s response is not reasonable, specify amendments that are required to be made to the IC Plan.

The ACMA must provide a copy of the determination to the carrier or provider.

New subsection 198(7) provides that a carrier or provider must amend the IC Plan in accordance with the ACMA’s determination and provide an amended IC Plan to the Communications Access Co-ordinator.

New subsection 198(8) provides that the ACMA’s determination is not a legislative instrument for the purposes of section 5 of the Legislative Instruments Act 2003 as subsection 198(8) only applies to a particular carrier or provider and has no general effect.

### 199 – Commencement of IC Plans

New section 199 deals with the commencement of IC Plans. This section transfers the obligations currently set out in section 332A of the Telecommunications Act.

New section 199 provides that an IC Plan commences on the day the Communications Access Co-ordinator notifies the carrier or nominated carriage service provider that the IC Plan has been approved. The IC Plan remains in force until a subsequent plan has been approved by the Communications Access Co-ordinator. This is a change from section 332A, which states that an IC Plan commenced on the day that it was received by the ACMA. It is appropriate that the IC Plan operate by reference to approval by the CAC, given the CAC’s control role in consideration of IC Plans, and to ensure that only compliant plans are operative.

### New section 200 – Compliance with IC Plans

New section 200 requires the carrier or nominated carriage service provider to comply with the IC Plan. This transfers the obligation currently set out in section 332B of the Telecommunications Act.

New section 200 provides that the carrier or provider must comply with the IC Plan by ensuring that all its business activities are consistent with the IC Plan. The effect...
of new section 200 is to ensure that a carrier or provider maintains interception capability in accordance with the IC Plan.

201 – Consequences of changed business plans

New section 201 requires the carrier or nominated carriage service provider to submit an amended IC Plan if its business plans change in such a way as to affect the accuracy of the prior IC Plan. This reproduces the obligation set out in section 332D of the Telecommunications Act.

New subsection 201(1) provides that if an IC Plan of a carrier or provider ceases to be adequate because of changes to its business plans, the carrier or provider must, as soon as practicable, prepare and provide a new IC Plan to the Communications Access Co-ordinator for approval.

New subsection 201(2) provides that a new plan is only required if the changes to the business plans are likely to have a material adverse effect on the ability of the carrier or provider to comply with its interception obligations under Part 5-3 of the TIA Act. For example, a material adverse effect may arise if a carrier or nominated carriage service provider provides new services or products, such as where a telecommunications company provides new Internet Protocol (IP) based products like ‘pushed email services’ or Voice over the Internet Protocol (VoIP). It could also include a substantial change in the carrier’s or nominated carriage service provider’s network architecture. These provisions reflect the underlying obligation of Part 5-3 that a carrier or nominated carriage service provider must ensure that all services they offer are able to be intercepted.

As noted in new subsection 198(1), the receipt of an amended plan restarts the consideration process.

202 – Confidential treatment of IC Plans

New section 202 reproduces the IC Plan confidentiality obligation currently set out in subsection 329(3) of the Telecommunications Act.

New section 202 provides that the Communications Access Co-ordinator, the ACMA and interception agencies must treat an IC Plan as confidential and must not disclose the contents of an IC plan to anyone not referred to in this section, without the written approval of the carrier or nominated carriage service provider.

New section 202 reflects the sensitivity of the information contained in an IC Plan, from both a commercial and national security perspective.

Part 5-5 – Delivery capability

New Part 5-5 transfers the obligations currently set out in section 332J of the Telecommunications Act. It deals with agency specific delivery capability arising from the implementation of new or altered technology. New Part 5-5 allows the Communications Access Co-ordinator to make a determination in respect of delivery
capabilities, without the current requirement that the determination be based on a new or altered technology.

Delivery capability refers to the delivery of lawfully intercepted information from the delivery point to the interception agency. The cost allocation principles set out in Part 5-6 require that the costs of developing, installing and maintaining a delivery capability be borne by the interception agencies.

**New section 203 – Communications Access Co-ordinator may make determinations**

New subsection 203(1) provides that the Communications Access Co-ordinator may make determinations on delivery capability in respect of a specified kind of telecommunications service involving the use of a telecommunications system supplied by one or more specified carriers and one or more specified interception agencies. This is to allow a determination to be applicable to any number of carriers or nominated carriage service providers and any number of agencies.

It should be noted that the definition of carrier for Part 5-5 includes carriage service providers (the terms ‘carrier’ and ‘carriage service provider’ having a separate meaning only in Part 5-4).

New subsection 203(2) provides that the determination must relate to all or any of the following: (a) the format in which intercepted information is to be delivered from the delivery point to an interception agency (as distinct from information to the delivery point in the case of interception capability); (b) the place and the manner in which it is to be delivered; or (c) any ancillary information that is to accompany the intercepted information.

This subsection serves to limit the scope of such determinations, and in particular, prevents the use of the determinations to redefine the meaning of interception capability.

New subsection 203(3) provides that the Communications Access Co-ordinator must consult the ACMA before making the determination.

New subsection 203(4) provides that the Communications Access Co-ordinator’s determination is not a legislative instrument. This is because of the type of information to be contained in the determinations, which are likely to include format and encoding specifications, file naming conventions and lawful interception identifiers. This information is sensitive in that it can provide information on the scope of interception capability. However, whilst not publicly available, determinations would be made available to any carriers and carriage service providers required to comply with them. It should also be noted that the determinations will not be used to broaden the definition of interception capability.
204 – Obligations of persons covered by a determination

New subsection 204(1) provides that a carrier or carriage service provider that is subject to a Communications Access Co-ordinator’s determination must comply with the determination.

New subsection 204(2) provides that if a carrier or carriage service provider is required to have a delivery capability, they are required to ensure that this capability is developed, installed and maintained.

205 – Obligations of persons not covered by a determination in relation to a kind of telecommunications service

This is a new section that operates in relation to any carrier who provides a telecommunications service of a particular kind not dealt with by Communications Access Co-ordinator determinations. It operates in a similar way as the requirement to provide an interception capability in the absence of a determination and makes clear that carriers are required to provide a general delivery capability in the absence of a determination.

New subsection 205(1) provides that in such cases, carriers must ensure that the kind of service or system has a delivery capability (that is, it is able to be delivered to an agency).

New subsection 205(2) provides that this delivery capability includes the obligation to ensure that the capability is developed, installed and maintained.

Part 5-6 – Allocation of costs

New Part 5–6 outlines the allocation of costs of complying with the obligation to have an interception capability and a delivery capability. It preserves the cost allocations currently set out in the Telecommunications Act.

Division 1 – Outline of Part

206 – Outline of part

New section 206 explains that under Division 2, the cost of developing, installing and maintaining an interception capability imposed on a carrier or carriage service provider under Part 5-3 is to be borne by the carrier or carriage service provider. Under Division 3, the costs of developing, installing and maintaining a delivery capability under Part 5-5 is to be borne by the relevant interception agency.

The note following new subsection 206(2) clarifies that this Part does not deal with the cost of complying with an authorisation under Division 3, 4 or 5 of Part 4-1, that is, requests from the Organisation and enforcement bodies for telecommunications data. This issue is still governed by section 314 of the Telecommunications Act.
Division 2 – Interception Capability

207 – Costs to be borne by the carriers

New section 207 transfers the cost allocation provisions currently set out in subsection 332L(1) of the Telecommunications Act.

New section 207 provides that a carrier or carriage service provider must bear the capital and ongoing costs associated with the development, installation and maintenance of its interception capability obligations as set out in the new sections 190 and 191.

Interception capability refers to the ability to enable a communication to be intercepted and for lawfully intercepted information to be transmitted to the applicable delivery point.

Division 3 – Delivery capability

New section 208 – Costs to be borne by the interception agencies

New section 208 provides that the relevant interception agency must bear the capital and ongoing costs associated with the delivery capability obligations imposed on a carrier or carriage service provider under the new Part 5–5. These costs are calculated in accordance with the new section 209.

209 – Working out costs of delivery capability

New section 209 deals with working out the costs an interception agency must bear in respect of specific delivery capabilities. This transfers the obligation currently set out in subsection 332N of the Telecommunications Act. Note however, that the concept of ‘agency specific delivery capabilities’ has not been continued in the TIA Act as it was limited to requirements arising from the implications of new or altered technology.

New subsection 209(1) provides that each carrier or carriage service provider that is obliged to ensure the development, installation and maintenance of a delivery capability must do so on such terms and conditions that are agreed in writing between the carrier or carriage service provider and the interception agency concerned. If there is no agreement, the terms and conditions are to be determined in writing by the ACMA.

New subsection 209(2) provides that the terms and conditions are to be consistent with the following principles: (a) the most cost effective means of ensuring the development, installation and maintenance of that capability is employed; (b) the carrier is to incur the costs; and, (c) a carrier may, over time, recover those costs from the relevant interception agency for which the agency is liable under new section 208.

New subsection 209(3) provides that a carrier may enter into an agreement with more than one interception agency.
New subsection 209(4) provides that any agreement should include a provision that if a disagreement arises regarding the costs for delivery capability, the agency may request the ACMA to arbitrate. If so requested, the ACMA must determine the costs in dispute.

New subsection 209(5) provides that regulations may deal with the conduct of arbitration by the ACMA.

New subsection 209(6) provides that a carrier must continue to comply with its delivery capability obligations while the dispute is being resolved.

New subsection 209(7) provides that if the ACMA determines that the costs (which are to be borne by the interception agency), be reduced, the carrier or carriage service provider must adjust the amount claimed from the interception agency accordingly, including adjusting the amount already claimed, if any, and adjust its means of calculating future costs.

New subsection 209(8) states that any agreement between a carrier and an agency of a State or the Commonwealth is deemed to be with the State or the Commonwealth.

New subsection 209(9) provides that the ACMA’s determination is not a legislative instrument for the purposes of section 5 of the Legislative Instruments Act 2003 as subsection 209(9) only applies to a specific dispute and has no general effect.

210 – Examination of lower cost options

New section 210 transfers the obligations currently set out in subsection 332P of the Telecommunications Act.

New subsection 210(1) provides that as part of the arbitration under section 209, the ACMA may request a carrier: (a) to examine, at the carrier’s or carriage service provider’s expense, the possibility of a lower cost option for providing the delivery capability; and, (b) to report back to ACMA, within a specified period, on the results of the examination.

New subsection 210(2) provides that the carrier must comply with that request.

New subsection 210(3) provides that the request is not a legislative instrument for the purposes of section 5 of the Legislative Instruments Act 2003 as it only applies to a specific carrier.

211 – ACMA may require independent audit of costs

New section 211 transfers the obligations currently set out in subsection 332Q of the Telecommunications Act.

New subsection 211(1) provides that as part of the arbitration under section 209, ACMA may require a carrier to arrange for an audit of the costs claimed to have been incurred in respect of a delivery capability.
New subsection 211(2) provides that the auditor is to be selected by the carrier, but must be approved by ACMA.

New subsection 211(3) provides that if the auditor is not approved by ACMA, ACMA may either select a new auditor or undertake the audit itself.

New subsection 211(4) provides that if ACMA selects an auditor, ACMA may specify the period of time in which the auditor must report to the ACMA.

New subsection 211(5) provides that if a carrier receives a notice from the ACMA requiring the carrier to arrange for an audit under subsection 211(1), the carrier must: (a) co-operate fully with the carrying out of the audit; and, (b) bear the costs of the audit.

New subsection 211(6) provides that the request for audit is not a legislative instrument for the purposes of section 5 of the Legislative Instruments Act 2003 as subsection 211(6) only applies in a particular case.

**Schedule 1 Part 2 – Consequential amendments**

*Australian Communications and Media Authority Act 2005*

**Item 13 – After subparagraph 8(1)(j)(iv)**

Item 13 incorporates the powers conferred on the Australian Communications Media Authority by the new chapters 4 and 5 of the TIA Act into ACMA’s telecommunication related functions. This includes monitoring and reporting to the Minister on the operation of chapters 4 and 5 where specified.

*Criminal Code Act 1995*

**Item 14 – Paragraph 476.5(2A)(b) of the Criminal Code**

Item 14 updates the reference contained in paragraph 476.5(2A)(b) of the Criminal Code Act 1995 (‘Liability for certain acts’) from section 283 of the Telecommunications Act to new Division 3 of Part 4-1 of the TIA Act.

*Intelligence Services Act 2001*

**Item 15 – Paragraph 14(2A)(b)**

Item 15 updates the reference contained in the Intelligence Services Act 2001 (‘Liability for certain acts’) from section 283 of the Telecommunications Act to Division 3 of Part 4-1 of the TIA Act.

*Telecommunications Act 1997*

Amendments to the Telecommunications Act reflect the transfer of provisions from the Telecommunications Act to the TIA Act.
Item 16 – Section 5

Item 16 omits from the simplified outline of the Telecommunications Act at Section 5 that ‘a carrier or carriage service provider may be required to have an interception capability’. This is because of the transfer of interception capability requirements from the Telecommunications Act to the TIA Act.

Item 17 – Section 6 (table item 18)

Item 17 removes from the main index of the Telecommunications Act the reference to co-operation with law enforcement agencies. This is required as a result of the repeal of Part 15 of that Act at item 52.

Item 18 – Section 7 (after paragraph (b) of the definition of ACMA’s telecommunications powers)

Item 18 inserts the powers conferred on ACMA in Chapters 4 and 5 of the TIA Act into the definition of ACMA’s telecommunication powers.

Item 19 – Section 7 (definition of agency)

Item 19 omits the definition of ‘agency’ from section 7. This reflects the transfer of all relevant interception related provisions in Parts 14 and 15 of the Telecommunications Act to the TIA Act.

Items 20 and 21 – Section 7 (definition of agency co-ordinator)

Items 20 and 21 omit the term ‘agency co-ordinator’ and substitute ‘Communications Access Co-ordinator’. This reflects the transfer of all relevant provisions to the TIA Act and the renaming of the agency co-ordinator as the Communications Access Co-ordinator.

Item 22 – Section 7 (definition of IC plan)

Item 22 repeals the definition of ‘IC Plan’ to reflect the transfer of all relevant provisions to the TIA Act.

Item 23 – Section 7 (definition of interception related information)

Item 23 repeals the definition of ‘interception related information’ to reflect the transfer of all relevant provisions to the TIA Act.

Item 24 – Section 7A

Item 24 repeals section 7A (the definition of ‘agency co-ordinator’) to reflect the transfer of all relevant provisions to the TIA Act.
Items 25, 26 and 27 – Subsections 53A(1) and (2), section 56A and subsection 59(8)

Items 25, 26 and 27 remove the term ‘agency co-ordinator’ and substitute ‘Communications Access Co-ordinator’ to reflect the transfer of all relevant provisions to the TIA Act and the renaming of the agency co-ordinator to the Communications Access Co-ordinator.

Items 28, 29 and 30 – Subsections 276(3), 277(3) and 278(3)

Items 28, 29 and 30 provide guidance at the end of Note 1 of sections 276, 277 and 278. These sections set out the offences for primary disclosure and use of information and the note as amended refers to various exceptions to the prohibition on disclosure, now including the exceptions in Chapter 4 of the TIA Act that allow access to communications for national security and law enforcement agencies to purposes. This reflects the transfer of related provisions from sections 282 and 283 of the Telecommunications Act to the TIA Act.

Item 31 – Subsection 280(2) (definition of enforcement agency)

Item 31 updates the definition of ‘enforcement agency’ to have the same meaning as in the TIA Act to reflect the transfer of section 282 to the TIA Act.

Item 32 – Sections 282 and 283

Item 32 repeals sections 282 and 283 dealing with the disclosure or use of information or documents reasonably necessary for national security, law enforcement purposes or the protection of public revenue under certain circumstances to reflect the transfer of these sections from the Telecommunications Act to Chapter 4 of the TIA Act.

Item 33 – At the end of section 294

Item 33 amends section 294 to include a reference to Divisions 3-5 of Part 4-1 of the TIA Act. This ensures that the new provisions for access to telecommunications associated data in Chapter 4 of the TIA Act will not affect the operation of the remaining exceptions in the Telecommunications Act.

Items 34 and 35 – Subsections 295(1) and 295(2)

Items 34 and 35 amends section 295 of the Telecommunications Act to refer to Chapter 4 of the TIA Act. Section 295 of the Telecommunications Act determines the burden of proof in proceedings for offences of unauthorised disclosure or use of information.

Subsection 295(2) states that in proceedings against a person for unauthorised disclosure of information, that person bears the burden of proof in demonstrating that the disclosure was made in accordance with one of the exceptions listed in Division 2 or in new Chapter 4 of the TIA Act.
Item 36 – Section 298

Item 36 repeals section 298, which provides an exception to the general offence of disclosure or use of information where the disclosure or use is reasonably necessary for the enforcement of the criminal law, the enforcement of a law imposing a pecuniary penalty or for the protection of public revenue. This reflects the transfer of this section and related section 282 of the Telecommunications Act to chapter 4 of the TIA Act.

Item 37 – Section 305

Item 37 repeals section 305 of the Telecommunications Act (‘Certificates issued by authorised officers of enforcement agencies’) and substitutes new section 305 to reflect the transfer of authorisation provisions from the Telecommunications Act to the TIA Act.

In addition to the change in terminology from ‘certificate’ to ‘authorisation’, new section 305 provides that where a carrier, carriage service provider or number-database operator or an associate of a carrier, carriage service provider or number-database operator is notified of an authorisation made under new Division 4 of Part 4-1 of the TIA, they must retain the notification for 3 years.

New section 305 changes the current requirement that a certification must be provided to the carrier, carriage service provider or number-database operator up to 5 days after the information is requested. The new section 305 provides that an authorisation occurs when a carrier, carriage service provider or number-database operator is notified.

Item 38 – Paragraph 306(1)(b)

Item 38 replaces paragraph 306(1)(b) of the Telecommunications Act in relation to record keeping for historical disclosures to reflect the transfer of sections 282 and 283 of the Telecommunications Act to the TIA Act.

Item 39 – Paragraph 306(5)(d)

Item 39 replaces paragraph 306(5)(d) of the Telecommunications Act in relation to record keeping for historical disclosures to reflect the transfer of section 282 of the Telecommunications Act to the TIA Act. New paragraph 306(5)(d) provides that where a disclosure of information is made under the TIA Act, the record taken must include the name of the person who made the authorisation and the date of the making of the authorisation.

Item 40 – Paragraph 306(5)(e)

Item 40 omits the term ‘agency’ within paragraph 306(5)(e) of the Telecommunications Act and substitutes the term ‘body’ to reflect the inclusion of record keeping requirements for disclosures made in accordance with the TIA Act to agencies at items 38 and 39 and provide a distinction between these agencies and any other ‘body’ or person to whom disclosures are made.
Item 41 – After section 306

Item 41 inserts a new provision which is based on the existing record keeping arrangements for the disclosure of historical communications associated data under section 306 of the Telecommunications Act and inserts a new section 306A to provide for the records of prospective authorisations made under the TIA Act that are to be kept by carriers, carriage service providers and number-database operators.

Carriers, carriage service providers and number-database operators must make a record of prospective disclosures authorised under section 180 of the TIA Act within 5 days of the authorisation ceasing to be in force and retain that record for 3 years. This will facilitate the monitoring function of the Privacy Commissioner under section 309 of the Telecommunications Act.

Associates of carriers, carriage service providers and number-database operators must make a record of prospective disclosures authorised under section 180 of the TIA Act within 5 days of the authorisation ceasing to be in force and give a copy of the record to the associated carrier, carriage service provider or number-database operator within 5 days of making the record. The carrier, carriage service provider or number-database operator must retain the record for 3 years.

Subsection 306A(5) sets out the details that must be included in a record of a disclosure required by subsections 306A(2) or (3). Paragraph 306A(b) allows for the ongoing nature of a prospective authorisation and multiple disclosures, but only requires one record to be kept in relation to the authorisation.

Subsection 306A(6) makes it clear that the record or a copy of it may be given or kept in electronic or written form.

Subsection 306A(7) makes it an offence to contravene the record-keeping requirements of this section. The penalty, in the case of a natural person, is a maximum of 300 penalty units and in the case of a body corporate is a maximum of 1500 penalty units (under s. 4AA of the Crimes Act 1914, a penalty unit is worth $110 – see also section 4B(3) of that Act).

Item 42 – Subsection 307(1)

Item 42 amends subsection 307(1) to create an offence of incorrectly making a record in purported compliance with the new section 306A, the penalty for which is imprisonment for 6 months.

Item 43 – Subparagraphs 308(1)(b)(i) and (ii)

Item 43 amends subparagraphs 308(1)(b)(i) and (ii) to require the reports given to ACMA of authorised disclosures to include authorised prospective disclosures recorded under new section 306A.
Items 44 and 45 – Paragraphs 309(2)(a) and (b)

Items 44 and 45 amend paragraphs 309(2)(a) and (b) to provide that the Privacy Commissioner also monitors compliance with the record-keeping requirements under section 306A relating to prospective disclosures.

Item 46 – Subsections 313(7) and (8)

Item 46 repeals subsection 313(7) and (8) and substitute the new subsection 317(7). This provides that a reference in section 313 of the Telecommunications Act to giving help to officers and authorities of the Commonwealth, States and Territories includes, but is not limited to, the provision of interception services, stored communications information and telecommunications data under the TIA Act and disclosing information authorised by or under law in accordance with section 280 of the Telecommunications Act.

The terms and conditions on which such help is to be provided is provided under section 314 of the Telecommunications Act.

Items 47 and 48 – Subsections 314(2) and (3)

Items 47 and 48 amend subsections 314(2) and (3) to reflect the transfer of relevant cost sharing provisions from the Act to the TIA Act. These cost allocation principles relating to interception capability and the transmission of intercept related information contained in section 314A are repealed at item 51 and replaced by new Part 5-6 of the TIA Act.

Item 49 – Subsections 314(3A) and (3B)

Item 49 repeals subsections 314(3A) and (3B) to reflect the transfer of relevant provisions in relation to interception capability from the Telecommunications Act to the TIA Act.

Item 50 – At the end of section 314

Item 50 inserts a new subsection 314(8) to clarify that the terms and conditions on which help is to be given under section 314 does not apply to the cost allocation associated with interception capability and delivery capability addressed in Part 5-3 or 5-5 of the TIA Act.

Item 51 – Section 314A

Item 51 repeals section 314A of the Telecommunications Act in relation to delivery points to reflect the transfer of these provisions to new Part 5-2 of the TIA Act.

Item 52 – Part 15

Item 52 repeals Part 15 of the Telecommunications Act in relation to co-operation with agencies to reflect the transfer of all relevant provisions from the Telecommunications Act to new Part 5-2 of the TIA Act.
Items 53 and 54 – Subclause 1(2) of Schedule 1 (at the end of the definition of this Act) and subclause 1(2) of Schedule 2 (at the end of the definition of this Act)

Items 53 and 54 amend subclause 1(2) of Schedule 1 and subclause 1(2) of Schedule 2 to provide that compliance with Chapter 5 of the TIA Act is a standard carrier licence condition and a standard carriage service provider rule. Carriers and carriage service providers must therefore comply with all obligations in Chapter 5 of the TIA Act.

Telecommunications (Interception and Access) Act 1979

Items 55 and 56 – Chapter 5 (heading) and Part 5-1 (heading)

Items 55 and 56 are technical drafting amendments that rename the existing Chapter 5 of the TIA Act to a new Chapter 6, to allow the new Chapter 5 – Co-operation with interception agencies to be inserted.

Schedule 1 Part 3 – Application, saving and transitional provisions

Item 57 – Definitions

Item 57 provides that in this Part, ACMA means the Australian Communications and Media Authority, and the TIA Act means the Telecommunications (Interception and Access) Act 1979.

Item 58 – Transitional – certificates of the Organisation

Item 58 provides that a certificate for the disclosure of telecommunications data issued to a carrier or carriage service provider under the authority of paragraph 283(2)(b) for the purposes of making a disclosure to the Organisation will remain in effect after the commencement of the Amendment Act, as if it were an authorisation made under paragraph 175(2) of the TIA Act. This provision is conditional on no disclosure having been made prior to the commencement of the amendments to the TIA Act. This ensures that a certificate issued under the Telecommunications Act authorising the disclosure of telecommunications data remains valid notwithstanding the transfer of the authorising sections to the TIA Act.

Item 59 – Transitional – certificates of enforcement agencies

Item 59 is a transitional provision similar to item 58, except that item 59 relates to law-enforcement bodies. Subitem 1 relates to the enforcement of the criminal law, subitem 2 relates to the enforcement of a law which carries a pecuniary penalty or the protection of the public revenue. Thus, certificates for the disclosure of telecommunications data issued to a carrier or carriage service provider under the authority of paragraph 282(3), (4) or (5) remain in effect after the commencement of the Amendment Act, as if it were an authorisation made under paragraph 178(2) or paragraph 179(2) of the TIA Act. This ensures that a certificate issued under the Telecommunications Act authorising the disclosure of telecommunications data remains valid notwithstanding the transfer of the authorising sections to the TIA Act.
Subitem 3 of item 62 states that Part 4-2 of the TIA Act (procedural requirements relating to authorisations) will not apply in relation to this item. This means that certificates issued prior to the commencement of the TIA Act will not be rendered invalid by reason of non-compliance with the new procedural requirements.

**Item 60 – Saving – secondary disclosure/use offences**

Item 60 is a saving provision which states that despite the repealing of section 298, of the Telecommunications Act which outlines the offence of the secondary disclosure of telecommunications data, a relevant disclosure made before or after the repeal will still be deemed an offence.

**Item 61 – Saving – record keeping**

Subitem 1 of Item 61 is a saving provision that ensures the continuing effect of the rules contained in section 305 requiring that copies of certificates authorising disclosure of telecommunications data must be provided to the carrier/carriage service provider and be retained by the carrier for three years.

Subitem 2 provides that paragraph 306(5)(d) remains in operation after the repeal of section 306 of the Telecommunications Act in relation to a disclosure made before the repeal of section 306. In this context, section 306 requires that a record of a disclosure must be made and retained for three years.

Subitem 3 explains that where a carrier has made a disclosure to a criminal law-enforcement body, civil law-enforcement body or a body which protects the public revenue pursuant to a certificate under subsections 282(3), (4) or (5), there is no need for a new certificate to be issued once paragraph 306(5)(d) is repealed.

**Item 62 – Transitional – applications for carrier licences**

Item 62 is a transitional provision that provides that where there is a pending application for a carrier licence with the ACMA at the time that the amending legislation takes effect, a reference to the Agency Co-ordinator shall be read as a reference to the Communications Access Co-ordinator.

**Item 63 – Transitional – delivery points**

Item 63 is a transitional provision that relates to delivery points which were in place prior to the commencement of the amending legislation. Item 63 provides that a delivery point for the purposes of section 314A of the Telecommunications Act will be a delivery point for the purposes of section 188 of the TIA Act. Further, where a delivery point was determined by the ACMA before the commencement of the new Act, section 188 applies as if the new point was one determined by the AMCA.

Subitem 3 indicates that if there is a disagreement, nomination or request undergoing a resolution process at the time of the commencement of the amending legislation, then section 314A will continue to apply. Once the location of a delivery point has been determined under section 314A, the delivery point is regarded as a delivery point.
under section 188 of the TIA Act. If the delivery point was one determined by the ACMA, new section 188 of the TIA Act applies as if the translated delivery point was one determined by the ACMA.

**Item 64 – Transitional – exemptions from interception capability**

Item 64 is a transitional provision which sets out that an exemption issued by the Agency Co-ordinator under subsection 326(1) of the Telecommunications Act before the commencement of the amending legislation, will be an exemption for the purposes of subsection 192(1) when the amending legislation commences.

Subitem 2 of Item 64 states that a pending application for an exemption at the commencement of the amending legislation will have the same effect as an application made under new section 192. It also deems that the Communications Access Co-ordinator will be taken to have received the application on the same date that the application was received by the Agency Co-ordinator.

Subitem 3 provides that an exemption granted by the ACMA under the Telecommunications Act continues to have force after the amending legislation commences.

**Item 65 – Transitional – nominated carriage service providers**

Item 65 is a transitional provision which provides that a declaration of a carriage service provider as a nominated carriage service provider in force under subsection 331(3) of the Telecommunications Act continues after the commencement of the amending legislation as if it were a declaration under subsection 197(4) of the TIA Act. The effect of this provision is that where a carriage service provider has been required to provide an interception capability plan, that obligation remains in force upon commencement of the amending Act.

**Item 66 – Transitional – IC plans**

Item 66 is a transitional provision in relation to interception capability plans. Subitem 1 of item 66 states that an IC plan in force prior to the commencement of the amending legislation continues to have effect under Part 5-4 of the TIA Act after the commencement of the amending legislation.

Subitem 2 provides that an IC plan which has not been processed at the time of the commencement of the amendment legislation will be taken to have been applied for under Part 5-4 of the TIA Act and must be dealt with in accordance with the new procedures set out in section 198 of the TIA Act.

Subitem 3 provides that something that is required to be done under section 198 of the TIA Act and that has already been done under section 332C of the Telecommunications Act, is deemed to have been done for the purposes of section 198.
Item 67 – Section 8 of the Acts Interpretation Act 1901

Item 67 provides that nothing in Part 3 of Schedule 1 limits the operation of section 8 (Effect of repeal) of the Acts Interpretation Act 1901, in relation to amendments or repeals made by this schedule.

Item 68 – Transitional regulations

Item 68 provides that the Governor-General may make regulations of a transitional nature.

Schedule 2 – Other Amendments

The purpose of this Schedule is to make other necessary amendments to the TIA Act to improve the ongoing effective operation of the interception and access regime in Australia.

These amendments will amend the TIA Act to:

  a) make offences relating to child pornography serious offences for the purpose of Section 5D of the TIA Act, whether or not the penalty for such an offence is imprisonment for 7 years;
  b) clarify that certain activities undertaken by security and law enforcement agencies in relation to network protection are exempt from the general prohibition on interception of telecommunications;
  c) provide circumstances in which security agencies may intercept telecommunications for the purposes of determining the effectiveness of an interception capability;
  d) update applicable reference to Commonwealth proceeds of crime offences; and
  e) correct minor drafting errors within the TIA Act.

Part 1 – Amendments

Telecommunications (Interception) Amendment Act 2006

Item 1 – Item 8 of Schedule 5

Item 1 corrects a misdescription of text in an amending item in the Telecommunications Interception Amendment Act 2006, which incorrectly referred to paragraph 53(1)(c) of the Telecommunications (Interception) Act 1979 as it was then named. Item 1 amends the reference to paragraph 53(1)(d).
Telecommunications (Interception and Access) Act 1979

**Item 2 – Subsection 5(1) (subparagraphs (d)(ii), (e)(ii) and (g)(iii) of the definition of certifying officer)**

Item 2 updates the reference in the definition of certifying officer to reflect the repeal of the Public Sector Management Act 1988 (NSW) and its replacement by the Public Sector Employment and Management Act 2002.

**Item 3 – Subsection 5(1)**

Item 3 amends subsection 5(1) of the TIA Act to include a definition of ‘security authority’. A security authority is a Commonwealth body which has functions relating primarily to security, the collection of foreign intelligence, the defence of Australia, or the conduct of the Commonwealth’s international affairs. The definition would include ASIO, the Department of Defence and the Department of Foreign Affairs and Trade.

The definition relates to the network protection provisions at item 12 below, and the new Part 2-4 Authorisation of interception for developing and testing interception capabilities, at item 16 below.

**Item 4 – Subsection 5(4A)**

Item 4 inserts a definition of an ‘employee of a security authority’, and includes a person who is engaged by the security authority or whose services are made available to the security authority. The definition relates to specific exceptions to the general prohibitions on interception that can apply to employees of security authorities.

**Item 5 – Paragraph 5B(1)(b)**

Section 5B is a list of proceedings that are deemed to be exempt proceedings for evidentiary purposes under the TIA Act. For example, the TIA Act provides that interception material can be adduced as evidence in an exempt proceeding. Item 5 expands the definition of exempt proceeding to include proceedings under the Spam Act 2003.

**Item 6 – Subparagraphs 5D(2)(b)(viii) and (ix) dealing with child pornography**

Section 5D is a list of offences deemed to be ‘serious offences’ for the purposes of obtaining an interception warrant under the TIA Act. The majority of these offences are punishable by imprisonment for life or for a period, or maximum period, of at least 7 years. Subparagraphs 5D(2)(b)(viii) and (ix) deal with certain offences in relation to child pornography. These subparagraphs are replaced at Item 7 by new subsection 5D(3A) deeming all child pornography offences to be a ‘serious offence’ under the TIA Act.
Items 7 – Subsection 5D(3A)

Item 7 inserts a new subsection deeming child pornography offences to be a ‘serious offence’ under the TIA Act. The amendment reflects the serious nature of child pornography offences, and ensures that telecommunication interception warrants and stored communications may be sought to assist in the investigation of these offences.

Item 8 – Paragraph 5D(4)(c) – amend reference to an Act

Item 8 amends the definition of ‘serious offence’ in section 5D by updating the reference to the Victorian money laundering offences in paragraph 5D(4)(c), by deleting reference to section 122 of the *Confiscation Act 1997* and inserting references to sections 194, 195 or 195A of the *Crimes Act 1958*.

Item 9 – Paragraph 5D(4)(f)

Item 9 amends the definition of ‘serious offence’ in section 5D by updating the reference to the South Australian money laundering offence in paragraph 5D(4)(f), by deleting reference to section 10b of the *Crimes (Confiscation of Profits) Act 1986* and inserting reference to section 138 of the *Criminal Law Consolidation Act 1935*.

Item 10 – Paragraph 5D(4)(i)

Item 10 amends the definition of serious offence by inserting a reference to the money laundering provisions of the *Criminal Code Act* of the Northern Territory.

Item 11 – Subsection 5F(2)

Currently subsection 5F(2) creates an exemption to the normal definition of ‘passing over the telecommunications system’ for the purposes of a computer network operated by or on behalf of the Australian Federal Police. Item 11 expands the operation of this exemption to cover Commonwealth agencies, security authorities and eligible authorities of a State, all of which are defined in subsection 5(1).

Networks are protected from security risks by the use of gateway control systems. The use of these systems (such as virus protection software) does not generally violate interception legislation. This is based on the definition of ‘interception’ in the TIA Act, which only refers to listening to or recording (copying) a communication in its passage over a telecommunications system. Importantly, the definition does not include ‘reading’, which means that software designed to block and scan emails or other communications for malicious content does not breach the TIA Act, even if the communications are quarantined or discarded without reaching the intended recipient. In addition, although copying can constitute interception, this is only the case while the communications is ‘passing over a telecommunications system’. Accordingly, once the communication is available to the intended recipient (for example, an email sitting on a mail server available for collection), copying of this communication does not constitute interception. However, some network protection activities that take place at the threshold of a network may constitute a technical breach of the TIA Act.
To enable the proper protection of identified highly secure networks, item 11 widens the existing provisions to increase the number of agencies who may monitor all outbound and inbound communications for the purposes of enforcing professional standards and protecting and maintaining their corporate network. This is achieved by ensuring that monitoring, recording or copying a written communication while it is still in the ‘confines’ of the network is not interception for the purposes of the TIA Act.

**Item 12 – Subsection 5G(2)**

Currently subsection 5G(2) applies only to intended recipients who are employees of the Australian Federal Police. Item 12 expands the operation of this provision to cover Commonwealth agencies, security authorities and eligible authorities of a State, all of which are defined in subsection 5(1).

**Item 13 – Paragraphs 7(2)(a), (aa), (ab) and (ac)**

For drafting consistency, the word ‘or’ is inserted at the end of each paragraph.

**Item 14 – Paragraph 7(2)(d) – interceptions authorised under section 31A**

Subsection 7(2) provides exceptions to the general prohibition on interception. Item 14 inserts paragraph 7(2)(d) to provide an exception where the interception is authorised under new section 31A which permits interception for the purpose of developing and testing interception capability.

**Item 15 – Subsection 9A(1A) inserted by item 7 of Schedule 1 to the Telecommunications (Interception) Amendment Act 2006**

To correct a drafting error, item 15 renumbers subsection 9A(1A) as 9A(1C).

**Item 16 – insert new Part 2–4 – Authorisation of interception for developing and testing interception capabilities**

New paragraph 7(2)(d) provides an exception to the prohibition against interception for the purposes of developing and testing interception capability. New Part 2–4 will be inserted to allow the heads of security authorities, which have functions that include activities relating to developing or testing technologies, to request authorisations from the Attorney-General to intercept communications for the purposes of developing or testing technologies or interception capabilities.

**31 – Applications for authorisation**

New section 31 enables the head of a security authority that has a function of developing or testing technologies or interception capabilities to apply to the Attorney-General for permission to intercept communications for the purposes of developing or testing technologies or interception capabilities.

New subsection 31(2) prescribes the manner in which the application may be made to the Attorney-General. The request must be in writing; must include details of the
development or testing of technologies or interception capabilities in relation to which authorisation is sought; must include details of the extent to which the development or testing would involve, or would be likely to involve, interception of communications; must refer to the functions of the authority that the development or testing would support; must state the grounds for seeking the authorisation; must summarise the outcomes of any previous authorisations and, must nominate the period (not exceeding 6 months) for which the authorisation is sought.

31A – Attorney-General may authorise interception for developing and testing interception capabilities

Under new section 31A, the Attorney-General will be able to authorise the interception as requested under the new section 31. Authorisations will be subject to a condition either prohibiting interception other than for the purposes of development or testing of technologies or interception capabilities, or prohibiting communicating, using or recording such communications except for such purposes. The authorisation may be subject to any other condition specified in the authorisation.

New subsection 31A(3) provides that the authorisation must be in writing, and must specify a period not exceeding 6 months for which the authorisation will have effect. Under subsection 31A(4), the head of the security authority must keep a copy of the authorisation available for inspection by the Minister responsible for the authority.

New subsection 31A(5) provides that the authorisation is not a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act 2003* as subsection 31A(5) only applies in a particular case.

31B – Authorisation of employees of a security authority

New section 31B provides for the head of a security authority to authorise employees to intercept communications where the Minister has authorised the security authority under section 31A.

New subsection 31B(2) provides for the head of a security authority to grant a delegation in writing to an officer of the authority for the purposes of paragraph (1)(b). The effect of this section is to restrict any activities involving interception of communications to a limited number of specified and duly authorised officers.

31C – Destruction of records

New section 31C provides that the head of the security authority must cause the destruction of information or records in the authority’s possession that were obtained pursuant to the authorisation. The information or records so obtained must be destroyed as soon as practicable after the development or testing has concluded.
31D – Reports to the Attorney-General

New section 31D provides that within 3 months of an authorisation ceasing to have effect, the head of the security authority must provide a report to the Attorney-General detailing the outcome of the activity, and the destruction of any information or records obtained during the period in which the authorisation was in force.

Item 17 – Subsection 61(1)

Item 17 repeals and substitutes subsection 61(1) dealing with who can issue and sign evidentiary certificates on behalf of the carrier. Currently, only the managing director and secretary of a carrier may issue and sign evidentiary certificates. Item 17 extends this to an employee of the carrier authorised in writing by the managing director or secretary. This amendment acknowledges that this administrative role can be effectively and promptly performed at a delegated level, and affords carriers more flexibility in the issuing of certificates.

Item 18 – subsection 61(2)

To reflect the changes made to subsection 61(1), item 18 amends subsection 61(2), to add a reference to an ‘employee’ referred to subsection 61(1).

Item 19 – paragraph 139(2)(a)

Item 19 inserts a reference to ‘another enforcement agency’ in paragraph 139(2)(a). This will allow information to be disclosed to another agency to investigate an offence by the recipient agency. Current provisions only permit the disclosure for the purposes of investigation of an offence by the disclosing agency.

Item 20 – paragraph 139(4)(ba)

Under section 139, in addition to specific investigations, lawfully accessed stored communications information can be disclosed to another agency in connection with a relevant proceeding. Item 20 extends this to proceedings under the Spam Act 2003.

Item 21 – paragraph 139(4)(f) – police disciplinary proceedings

Similarly, item 21 extends the proceedings for which disclosure of lawfully accessed stored communications information to another agency is permitted, to police disciplinary proceedings.
Part 2 – Application and transitional proceedings

Item 22 – Application – exempt proceedings

Item 22 ensures that a proceeding brought under the Spam Act 2003, which makes use of lawfully obtained information is regarded as an exempt proceeding for the purposes of section 5B regardless of whether the proceeding under the Spam Act 2003 was brought before or after the commencement of Item 5.

Item 23 – Application – serious offences

Item 23 makes clear that the amendments to allow warrants to be sought for the investigation of child pornography offences constituted by conduct occurring either before or after the commencement of item 7. That is, it will not matter that the relevant acts were committed before the amendment.

Item 24 – Transitional – continuation of evidentiary certificates

Item 24 ensures that an evidentiary certificate in force before the commencement of the amendment of section 61 continues to be in force.

Item 25 – Application – permitted dealings with accessed information

Item 25 provides that amendments made to the definition of ‘relevant proceedings’ for the purposes of items 20 and 21, also apply to proceedings commenced before or after the commencement of items 20 and 21.

Item 26 – Transitional – issue of evidentiary certificates in relation to old warrants

The amendments made by the Telecommunications (Interception) Amendment Act 2006 changed the name of the part of the TIA Act that dealt with the issuing of telecommunications interception warrants from Part VI to Part 2–5. The purpose of item 26 is to ensure that evidentiary certificates in relation to warrants issued, remain valid after the relevant sections were reordered to be in Part 2–5 of the TIA Act.