2010 - 2011

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

CYBERCRIME LEGISLATION AMENDMENT BILL 2011

EXPLANATORY MEMORANDUM

(Circulated by authority of the Attorney-General,
the Honourable Robert McClelland MP)

CYBERCRIME LEGISLATION AMENDMENT BILL 2011

OUTLINE

1. The main purpose of this Bill is to make amendments necessary to facilitate Australia's accession to the Council of Europe Convention on Cybercrime (the Convention). The Bill amends the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), the *Criminal Code Act 1995* (the Criminal Code), the *Mutual Assistance in Criminal Matters Act 1987* (the MA Act) and the *Telecommunications Act 1997* to ensure that Australian legislation meets all the Convention's requirements, subject to certain reservations. Only after Australian legislation is compliant can Australia accede to the Convention.

2. Cyber crime is a growing threat to Australian consumers, businesses and government. The international nature of cyber crime is such that no nation alone can effectively combat the problem. It is essential that Australia has in place appropriate arrangements, both domestically and internationally, to be in the best possible position to combat cyber crime.

3. The Convention is the first international treaty on crimes committed either against or via computer networks, dealing particularly with online fraud, offences related to child pornography and unauthorised access, use or modification of data stored on computers. The Convention's main objective is to pursue a common criminal policy aimed at the protection of society against cyber crime, especially by adopting appropriate legislation and fostering international co-operation. The Convention also contains a series of powers and procedures relating to accessing important evidence of cyber crimes, including by way of mutual assistance.

4. An explanatory report, prepared by the Council of Europe, accompanies the Convention. Where this Bill is enacting a requirement of the Cybercrime Convention, the Bill should be interpreted as operating in a way consistent with the Convention. To that extent, the explanatory report may be valuable in interpreting this Bill.

5. Australia is mostly compliant with the Convention's obligations, including the requisite cyber crime offences, the majority of police powers such as interception and access to stored communications and data and most elements of international cooperation. The Bill makes the following amendments to existing powers which ensure full compliance with the Convention's obligations:

- requires carriers and carriage service providers (C/CSPs) to preserve the stored communications and telecommunications data for specific persons when requested by certain domestic agencies or when requested by Australian Federal Police on behalf of certain foreign countries

- ensures Australian agencies are able to obtain and disclose telecommunications data and stored communications for the purposes of a foreign investigation

- provides for the extraterritorial operation of certain offences in the TIA Act

- amends the computer crime offences in the *Criminal Code Act 1995* so that they have adequate scope, and

- creates confidentiality requirements in relation to authorisations to disclose telecommunications data.

FINANCIAL IMPACT STATEMENT

The amendments made by the Cybercrime Legislation Amendments Bill 2011 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 *Cybercrime Legislation Amendment Act 2011*.

Clause 2 Commencement

Clause 2 provides for the commencement of the Bill.

Schedules 1 and 2, the stored communications preservation regime and the amendments in relation to mutual assistance regime, commence on the 28th day after Royal Assent. This delay is primarily to ensure carriers and carriage service providers have sufficient time to make any necessary technical changes to be able to comply with new legislative requirements.

Schedule 3, computer offence amendments, commence on the 28th day after this Act receives Royal Assent, or the day on which Australia becomes a party to the Council of Europe Convention on Cybercrime, whichever occurs later. The reason for this timing is to ensure full Constitutional support for the provisions.

Schedules 4 and 5, telecommunications data confidentiality provisions and miscellaneous changes related to jurisdiction and the availability of real-time access to telecommunications data, commence on the 28th day after royal assent. This delay is to ensure these schedules commence at the same time as schedules 1 and 2.

Clause 3 Schedule(s)

Clause 3 provides that each Act that is specified in a Schedule is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1 – Preservation regime for stored communications

Telecommunications Act 1997

Telecommunications (Interception and Access) Act 1979

Schedule 1 amends the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) and the *Telecommunications Act 1997* to oblige Carriers and Carriage Service Providers (C/CSPs) to preserve targeted stored communications when requested by certain domestic agencies or when requested by Australian Federal Police on behalf of certain foreign countries.

Schedule 1 implements requirements of the Council of Europe Convention on Cybercrime (the Convention). Article 16 requires Parties to establish powers enabling domestic agencies to obtain the preservation of stored computer data (stored communications, including traffic data) for up to 90 days, particularly where there are grounds to believe that the data is particularly vulnerable to loss or modification. The purpose of the 90 day preservation period is to maintain the integrity of that computer data for a period of time as long as necessary to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

Article 16 also requires that each party adopt such measures as necessary to oblige the person who is preserving the data to keep confidential the undertaking of such procedures.

Article 29 requires Parties to establish powers enabling a domestic agency to be able to obtain the preservation of stored computer data (including traffic data) at the request of other parties to the Convention. The Convention specifies necessary components of an international preservation request, including that the party seeking preservation must intend to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

Article 29 also specifies that preservation should be for a period not less than 60 days and, following the receipt of such a mutual assistance request, the data shall continue to be preserved pending a decision on that request.

Under the Convention, the obligation to preserve information does not automatically require the release of preserved information. Rather, one Party's law enforcement agencies can request that another Party preserve the information in anticipation of obtaining a lawful authority to access the information.

Schedule 1 implements these requirements by establishing two classes of domestic preservation notices which allow for domestic agencies to preserve certain stored communications that a carrier holds until the communications can be accessed under a warrant. This prevents the communications from being destroyed before a warrant is obtained.

Under this system, certain agencies can give a preservation notice to a carrier requiring the carrier to preserve all stored communications that the carrier holds that relate to the person or telecommunications service specified in the notice. The carrier will breach its obligations under section 313 of the *Telecommunications Act 1997* if it does not comply with the notice.

There are three types of preservation notices:

- historic domestic preservation notices (which preserve communications held by the carrier on the day the notice is received that might assist the Organisation in carrying out its

function of obtaining intelligence relating to security or a contravention of certain Australian laws for up to 90 days)

- ongoing domestic preservation notices (which preserve communications held by the carrier during a 29 day period after the notice is received that might assist the Organisation in carrying out its function of obtaining intelligence relating to security or a contravention of certain Australian laws for up to 90 days), and

- foreign preservation notices (which cover stored communications held by the carrier on the day the notice is received that might relate to a contravention of certain foreign laws).

Division 2 deals with domestic preservation notices. In the case of historic domestic preservation notices (which cover stored communications held by the carrier during the rest of the day the notice is received), an issuing agency (which is an enforcement agency or the Organisation) can give a historic domestic preservation notice if the relevant conditions in new section 107J are satisfied, including that the agency intends to apply for a warrant under the TIA Act to access the preserved stored communications. There are also certain grounds in new section 107L on which the preservation notice must be revoked.

In the case of ongoing domestic preservation notices (which cover stored communications held by the carrier in the period starting when the notice is received and ending 29 days later), an issuing agency (which is restricted to interception agencies or the Organisation) can give an ongoing domestic preservation notice if the relevant conditions in new section 107J are satisfied, including that the agency intends to apply for a warrant under the TIA Act to access the preserved stored communications. There are also certain grounds in new section 107L on which the preservation notice must be revoked.

Division 3 deals with foreign preservation notices. Only the Australian Federal Police can give a foreign preservation notice to a carrier and it can only do so if a foreign country has made a request for the preservation in accordance with new section 107P. There are also certain grounds on which the notice must be revoked.

Division 4 has miscellaneous provisions relating to all types of preservation notices (such as provisions about the giving of evidentiary certificates by carriers and issuing agencies).

A domestic preservation regime will assist ASIO and law enforcement agencies to address timing issues caused by C/CSPs retaining information for inconsistent periods of time and issues caused by delays in obtaining warrants if an issuing authority is unavailable. Existing time pressures mean that, in some circumstances, stored communications are unavailable when requested under a warrant because the C/CSP has deleted the information. Enabling the more expeditious preservation will also assist in information being available for foreign investigative purposes subject to the mutual assistance process. The distinction between historic and ongoing notices will allow agencies to select a tool that is suitable for particular investigations. No communications will be disclosed unless a warrant is subsequently issued which authorises the disclosure of those communications.

Telecommunications Act 1997

Item 1 – Paragraph 313(7)(c)

Item 1 inserts Paragraph 313(7)(c) into the Telecommunications Act to oblige C/CSPs to comply with both the domestic and international preservation regimes contained in the TIA Act. The amendment makes compliance with preservation notices a condition of a carrier licence. For

further information about carrier licence conditions see section 61 and Schedule 1 of the Telecommunications Act.

Telecommunications (Interception and Access) Act 1979

Item 2 – Subsection 5(1) definition of certifying official

Item 2 inserts a definition of ***certifying official*** for use in the context of the domestic preservation regime. The definition of ***certifying official*** combines a certifying officer of an agency and a certifying person of the Organisation. The purpose of this new definition is to simplify the drafting of the preservation notice regime.

Items 3 and 4 – Subsection 5(1) definitions of domestic preservation notice and foreign preservation notice

Items 3 and 4 insert references to the definitions of ***domestic preservation notice*** and ***foreign preservation notice*** into the definitions section of the TIA Act.

Item 5 – Subsection 5(1) definition of historic domestic preservation notice

Item 5 inserts a definition of ***historic domestic preservation notice*** into the definitions section of the TIA Act. The definition refers to subparagraph 107H(1)(b)(i) which details the operation of historic domestic preservation notices.

A historic domestic preservation notice will require a carrier to preserve all stored communications it holds on the day it receives the notice (that relate to a relevant person and/or telecommunications service(s)), and receives up until the end of that day. A carrier may hold on any particular day stored communications that it received on its systems several days or weeks earlier. Provided the carrier still holds those stored communications on the day on which the historic domestic preservation notice is issued to it, those stored communications must be preserved, in addition to any further stored communications received during the rest of that day.

Item 6 – Subsection 5(1) paragraph (a) of the definition of interception agency

Item 6 amends paragraph 5(1)(a) of the definition of ***interception agency*** to include a reference to new Part 3-1A. The change ensures that ***interception agency*** has a specific meaning in new Part 3-1A.

Item 7 – subsection 5(1) new paragraph (ba) of the definition of interception agency.

Item 7 inserts a new definition of ***interception agency*** for the purpose of new Part 3-1A. For the purposes of Part 3-1A an enforcement agency is a Commonwealth agency or an eligible authority of a State in relation to which a declaration under section 34 is in force.

Item 8 – Subsection 5(1) definition of issuing agency

Item 8 inserts a definition of ***issuing agency*** for use in the context of the preservation regime. The ***issuing agency*** is whichever agency issues a particular notice and may be an enforcement agency, an interception agency or the Organisation. The purpose of this new definition is to simplify the drafting of the preservation notice regimes.

Item 9 – Subsection 5(1) definition of ongoing domestic preservation notice

Item 9 inserts a definition of ***ongoing domestic preservation notice*** into the definitions section of the TIA Act. The definitions refers to subparagraph 107H(1)(b)(ii) which details the operation of ongoing domestic preservation notices.

An ongoing domestic preservation notice will require a carrier to preserve all stored communications it holds on the day it receives the notice (that relate to a relevant person and/or telecommunications service(s)), and receives up until the end of the 29th day after the day the carrier receives the notice. A carrier may hold on any particular day stored communications that it received on its systems several days or weeks earlier. Provided the carrier still holds those stored communications on the day on which the ongoing domestic preservation notice is issued to it, those stored communications must be preserved, in addition to any further stored communications received until the end of the 29th day after the carrier receives the notice.

Item 10 – Subsection 5(1) definition of preservation notice

Item 10 inserts a definition of ***preservation notice***. ***Preservation notice*** means a domestic preservation notice or a foreign preservation notice. The purpose of this new definition is to simplify the drafting of the preservation notice regimes.

Item 11 – Subsection 5(1) definition of preservation notice information

Item 11 inserts a reference to the definition of ***preservation notice information*** contained in new section 6EAA of the TIA Act.

Item 12 – Subsection 5(1) definition of preserve

Item 12 inserts a definition of ***preserve*** in relation to stored communications for the purpose of the preservation regime. ***Preserve*** means to maintain the integrity of the relevant communication, or a copy of the communication. The phrase 'maintain the integrity' includes ensuring that the relevant information or data is not edited, deleted or otherwise changed. The distinction between the original and a copy is intended to allow C/CSPs some technological flexibility in how they comply with the requirement. For example, to permit C/CSPs to make a copy of the original and maintain the integrity of the copy and thereby comply with the preservation requirement even if the original is deleted.

Item 13 – Subsection 5(1) definition of relates

Item 13 inserts a definition of ***relates*** which operates differently when the communications relate to a person to when the communications relate to a service.

Stored communications relate to a person if the person made or received the communication. Stored communications relate to a particular telecommunications service if the communications has passed over a telecommunications system by way of that service.

Item 14 – Subsection 5(1) definition of relevant period

Item 14 inserts a definition of ***relevant period*** which operates differently for historic domestic preservation notices and ongoing domestic preservation notices. For historic domestic preservation notices, ***relevant period*** means a period that starts when the carrier receives the notice and ends at the end of that day. For ongoing domestic preservation notices, ***relevant period*** means a period that starts when the notice is received and ends at the end of the day 29 days later. The 29 days does not include the day on which the notice was received.

Item 15 – Subsection 5(1) definition of working day

Item 15 inserts a definition of ***working day***. ***Working day*** means a week day which is not a public holiday in any State or Territory. This definition is for use in connection with new section 107R in relation to the issuing of revocations for foreign preservation notices. A working day is meant to be a day in which both the AFP and the relevant C/CSP located in any State or Territory is at work and in a position to action revocations appropriately.

Item 16 – Section 6EAA definition of preservation notice information

Item 16 creates the full definition of ***preservation notice information***, referred to in Item 7. The definition is intended to broadly cover anything which could imply the existence of a preservation notice. A broad definition is required to ensure that confidentiality of any information which could imply the existence of a preservation notice to avoid undermining the need to covertly access stored communications. The definition is intended to be consistent with the definition of interception warrant information and stored communications warrant information.

Item 17 – Chapter 3 (heading)

Item 17 substitutes a new heading for Chapter 3. The new heading adds the concept of preservation to Chapter 3.

Item 18 – Part 3-1A Preserving stored communications

Item 18 creates new Part 3-1A in relation to preserving stored communications.

Division 1 – Outline of this Part

107G Outline of this Part

Creates an outline for new Part 3-1A.

Division 2 – Domestic preservation notices

107H When a domestic preservation notice can be given

New section 107H establishes the requirements of a domestic preservation notice – specifically that the C/CSP must preserve all communications that relate to the specified person, or all the communications that relate to the specified service(s), and which the C/CSP holds at any time during the relevant period. The relevant period is different for historic and ongoing notices. 107H(2) refers to the conditions in 107J in which each type of domestic preservation notice can be issued.

107H(3) prevents an agency from listing multiple people on a single notice. Paragraph 107H(3)(c) intends to allow agencies to assist a carrier by specifying services which the agency believes relate to the person. When an agency is investigating a person with a common name, the paragraph will allow the agency to provide extra particulars and prevent confusion. An agency is not prevented from including services on a person notice to assist in identifying the relevant stored communications.

107J Condition for giving a domestic preservation notice

New section 107J establishes the conditions for when an issuing agency can issue each type of domestic preservation notice.

For historic notices, where the issuing agency is an enforcement agency, the agency must be investigating a serious contravention. The agency must also consider that there are reasonable grounds for suspecting that there are, or might be during the relevant period, stored communications that might assist in connection with the investigation; and that there are reasonable grounds for suspecting that there are stored communications which relate to the person or service covered by the notice.

These conditions reflect operational realities, including the possibility that an agency is aware stored communications relating to a particular person exist, but not which C/CSP has those communications. The section intends to provide agencies broader scope in the preservation of information than in seeking the actual disclosure of information.

The agency must also intend to access the communications with a Part 2-5 warrant or a stored communications warrant if, at a later time, the agency considers such a warrant would be likely to assist in connection with the investigation. The requirement connects the preservation regime with the mechanisms in the TIA Act for gaining lawful access to the communications.

For historic notices, where the issuing authority is the Organisation, the Organisation must consider that there are reasonable grounds for suspecting that there are, or might be during the relevant period, stored communications which might assist the Organisation in carrying out its function of obtaining intelligence relating to security; and that there are reasonable grounds for suspecting that there are stored communications which relate to the person or service covered by the notice. Additionally, the Organisation must intend to access the communications with a Part 2-2 warrant.

For ongoing notices, where the issuing agency is an interception agency, the agency must be investigating a serious contravention. The agency must also consider that there are reasonable grounds for suspecting that there are, or might be during the relevant period, stored communications that might assist in connection with the investigation; and that there are reasonable grounds for suspecting that there are stored communications which relate to the person or service covered by the notice. These conditions reflect operational realities, including the possibility that an agency is aware stored communications relating to a particular person exist, but not which C/CSP has those communications. The section intends to provide agencies broader scope in the preservation of information than in seeking the actual disclosure of information because lower levels of certainty may exist early in investigations.

The agency must also intend to access the communications with a Part 2-5 warrant or a stored communications warrant if, at a later time, the agency considers such a warrant would be likely to assist in connection with the investigation. The requirement connects the preservation regime with the mechanisms in the TIA Act for gaining lawful access to the communications.

The agency cannot issue another ongoing domestic preservation notice if that agency already has an ongoing domestic preservation notice in force for that person or telecommunications service(s). The reference to 'same person' means an actual person and does not intend to impede an investigation where one target may be using multiple pseudonyms. The phrase 'in force' refers new section 107K which specifies that a carrier a notice is 'in force' from when the carrier receives it until up to 90 days later.

For ongoing notices, where the issuing authority is the Organisation, the Organisation must consider that there are reasonable grounds for suspecting that there are, or might be during the relevant period, stored communications which might assist the Organisation in carrying out its function of obtaining intelligence relating to security. Security is defined in section 4 of the *Australian Security Intelligence Organisation Act 1979* as the protection of, and of the people of, the Commonwealth and the several States and Territories from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference whether directed from, or committed within, Australia or not, and the protection of Australia's territorial and border integrity from serious threats and the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned above.

For an ongoing notice, the Director-General of Security must also consider there are reasonable grounds for suspecting that there are stored communications which relate to the person or service covered by the notice. Additionally, the Organisation must intend to access the communications with a Part 2-2 warrant.

The Organisation cannot issue another ongoing domestic preservation notice if that agency already has an ongoing domestic preservation notice in force for that person or telecommunications service. The reference to 'same person' means an actual person and does not intend to impede an investigation where one target may be using multiple pseudonyms.

The phrase 'in force' refers new section 107K which specifies that a carrier a notice is 'in force' from when the carrier receives it until up to 90 days later.

107K When a domestic preservation notice is in force

New section 107K identifies the period for which a preservation notice is in force. A notice comes into force when the carrier receives the notice. The carrier must maintain the integrity of the preserved information for the period in which the notice is in force.

A notice ceases to be in force, meaning that the C/CSP can delete the preserved information, at the earliest of a 90 day period, upon receiving a revocation, or five days after the issuing of either a Part 2-2 warrant or a Part 2-5 warrant which authorises the disclosure of the information. The TIA Act provides that stored communications warrants are in force for five days before they expire.

107L Revoking a domestic preservation notice

New section 107L provides the circumstances for the revocation of domestic preservation notices. The first circumstance is where an issuing agency decides, for whatever reason, to revoke the preservation notice. This is intended to be used in circumstances where an agency decides, for whatever reason, that the communications no longer need to be preserved.

The second circumstance is where one of the requirements in new section 107J ceases to apply. This is intended to apply where the progress of an investigation changes the views of the agency about the need to access communications. For instance, if a decision is made that a particular

person whose communications were preserved is no longer a suspect and do not relate to the investigation, the agency should revoke the notice. Additionally, if an issuing agency decides for whatever reason that it no will no longer obtain a warrant under the TIA Act, even if the agency still considers that the communication would be likely to assist, the preservation notice must be revoked.

107M The persons who act on the issuing agency's behalf

New section 107M identifies persons who can issue or revoke a domestic preservation notice.

In the case of an enforcement agency using an historic domestic preservation notice, only a person authorised to apply for a stored communications warrant may issue or revoke the notice. This is because new paragraph 107J(1)(c) requires that a preservation notice only be issued if there is an intention to access the communications with a stored communications warrant or an interception warrant. Ensuring an overlap between the persons authorised to apply for a stored communications warrant and persons authorised to issue a preservation notice ensures that intention in new paragraph 107J(1)(c) can be properly formed when the preservation notice is issued.

In the case of the Organisation using an historic domestic preservation notice, only a certifying person may issue or revoke the notice.

In the case of an enforcement agency using an ongoing domestic preservation notice, only an authorised officer of the agency may issue or revoke the notice. This is because new paragraph 107J(1)(c) requires that a preservation notice only be issued if there is an intention to access the communications with a stored communications warrant or an interception warrant. Ensuring an overlap between the persons authorised to apply for a stored communications warrant and persons authorised to issue a preservation notice ensures that intention in new paragraph 107J(1)(c) can be properly formed when the preservation notice is issued.

In the case of the Organisation using an ongoing domestic preservation notice, only the Director-General of Security may issue the notice. An ongoing domestic preservation notice can be revoked in the same way as a historic domestic preservation notice – by a certifying person.

Division 3 – Foreign preservation notices

107N When a foreign preservation notice can be given

New section 107N(1) provides that, when the Australian Federal Police (AFP) receives a request to preserve stored communications that is compliant with the conditions set out in new section 107P, it must issue a foreign preservation notice in relation to those stored communications. A foreign preservation notice requires the preservation of all stored communications that the carrier holds at any time from receiving the notice until the end of that day which relate to the specified person or telecommunications service.

107N(2) prevents the AFP from listing multiple people on a single notice. Paragraph 107N(2)(c) intends to allow the AFP to assist a carrier by specifying services which the AFP believes relate to the person. For investigations relating to a person with a common name, the paragraph will allow the AFP to provide extra particulars and prevent confusion.

Article 27 of the Cybercrime Convention includes circumstances in which the receiving party could elect not to issue a preservation notice in response to compliant requests. However, new section 107N requires the AFP to issue notices in response to all compliant requests. The intention is that the content of the communication will only be disclosed to foreign jurisdictions through the mutual

assistance process which has inbuilt safeguards functionally identical to the grounds for refusing preservation requests. Because of the urgent nature of preservation, it is best to action preservation requests expeditiously and leave complicated assessments to the full mutual assistance process.

107P Condition for giving a foreign preservation notice

New section 107P identifies the conditions on which a foreign country may request the AFP to preserved stored communications. These conditions include that the country intends to submit a formal mutual assistance request, that the communications relate to an identified person or telecommunications service and are relevant to a serious foreign contravention.

New subsection 107P(2) lists the particulars that a foreign country must include in a preservation request to the AFP. The requirement to be in writing intends to include facsimiles, e-mails and other similar means of communications. New subsection 107P(2) requires that the request specify the reasons why the stored communications need to be preserved. The specification should explain the connection between the communications and the relevant serious foreign contravention and explain why the communications may be important to the investigation.

107Q When a foreign preservation notice is in force

New section 107Q provides that a foreign preservation notice comes into force when the carrier receives the notice and ceases to be in force when a revocation under new section 107R is received or a stored communications warrant authorising the disclosure of the communications ceases to be in force. The TIA Act provides that stored communications warrants are in force for five days before they expire.

The domestic preservation notice provision contained in new section 107K has a default end date of 90 days. While new section 107K has a default end date of 90 days, new section 107Q contains no default period. This is because the Convention ties the end of preservation to steps within the mutual assistance process. As C/CSPs are not in a position to be aware of these process, section 107R places the burden on the AFP to inform the C/CSP of when the notice ceases to be in force.

107R Revoking a foreign preservation notice

New section 107R provides for three circumstances in which the AFP must revoke a foreign preservation notice.

The first circumstance is that 180 days have elapsed since the carrier was given the notice and the foreign country did not make a formal mutual assistance request for access to the communications. The purpose of this provision is to give carriers certainty that they will not be preserving stored communications indefinitely for investigations which have ceased.

The second circumstance is where the relevant foreign country makes a mutual assistance request which the Attorney-General refuses. The third circumstance is where the foreign country withdraws the mutual assistance request.

In all circumstances the AFP must revoke the preservation notice by the end of the third working day after the end of the relevant period. The revocation must be in writing.

107S The persons who act on the AFP's behalf

New section 107S requires that foreign preservation notices must be given or revoked only by an authorised officer of the AFP. This section is intended to be consistent with new section 107M, but applicable in the more specific instance of foreign preservation notices.

Division 4 – Provisions relating to preservation notices

New Division 4 creates an evidentiary certificate regime for preservation notices consistent with the existing evidentiary certificate regime for a carrier with respect to the execution of warrants, see current sections 18, 129 and 130.

107T Evidentiary certificates relating to actions by carriers

New section 107T provides that the Managing Director, Secretary of a carrier or an authorised employee of a carrier may issue a written certificate setting out facts which detail the acts done by employees of the carrier to comply with a preservation notice. This may include, for instance, that an employee of the carrier made a copy of the communications covered by the notice and moved that copy to a different system where it would be preserved.

Written evidentiary certificates are intended to be conclusive proof of the matters stated in the document. This is intended to ensure that employees of the carrier are not required to testify in each proceeding which relies on evidence obtained under a stored communications warrant which was previously subject to preservation, simply to explain the technical aspects of the preservation.

107U Evidentiary certificates relating to actions by issuing agencies

New section 107U provides that a certifying official of an issuing agency can create an evidentiary certificate setting out facts about actions done by an officer or staff member of the agency in connection with the preservation. This may include, for instance, matters relating to the issuing of a notice and giving it to a carrier.

The written certificate is taken to be, in an exempt proceeding, as *prima facie* evidence of the matters stated in the document. This ensures that employees of the agency are not required to testify in each proceeding which relies on evidence obtained under a stored communications warrant which was previously subject to preservation, simply to explain that the information was lawfully obtained.

107V Certified copies of preservation notices

New section 107V allows for the creation of certified copies of preservation notices. Such copies are to be treated the same as the original. The purpose of this provision is to simplify document management for issuing agencies.

107W How notices are to be given to carriers

New section 107W obliges agencies to give preservation notices and revocations to the authorised representative of the carrier. This includes sending the notices or revocations to the appropriate contact point via e-mail. This section ensures that notices are given to the appropriate people within a carrier's organisation. This is because carriers are potentially large bodies with offices in multiple jurisdictions.

Item 19 – Subparagraph 108(2)(f)(ia)

Item 19 inserts subparagraph 108(2)(f)(ia) to ensure that persons lawfully engaging in duties relating to the installation, connection or maintenance of equipment for accessing stored communications pursuant to preservation notices are not committing an offence under the TIA Act.

Item 20 – Division 1 of Part 3-4 (heading)

Item 20 amends the Division heading by adding 'etc.' to include dealing with preservation notice information.

Item 21 – Subparagraph 133(1)(b)(ii)

Item 21 inserts subparagraph 133(1)(b)(ii) to make the communication, use, recording or giving in evidence of preservation notice information an offence. This is pursuant to Article 16(3) of the Cybercrime Convention.

Item 22 – Section 134

Item 22 repeals current section 134 and replaces it with a similar section which includes the concept of ***preservation notice information*** in addition to the current concept of stored communications warrant information. Preservation notice information is likely to disclose the same kinds of confidential information as warrant information and maintaining the confidentiality of the information is a requirement of Article 16(3) of the Cybercrime Convention.

Item 23 – After subsection 135(4)

Item 23 inserts new subsections 135(4A) and 135(4B) to create permitted circumstances for dealing with preservation notice information by employees of carriers. These new subsections are intended to be consistent with existing subsections 135(5) and 135(6) which relate to stored communications warrant information. The changes are necessary to maintain the confidentiality of preservation notice information as required by Article 16(3) of the Cybercrime Convention.

Items – 24 and 25 After paragraphs 136(1)(a), 137(1)(a), 138(1)(a), 138(2)(a) and 139(1)(a) and Subsection 146(2)

Items 24 and 25 insert the concept of preservation notices in appropriate paragraphs in sections 136, 137, 138 and 139 and 146. These insertions allow for the dealing and communication of ***preservation notice information*** in the same circumstances as dealing and communication is permitted for stored communications warrant information. This includes the giving of evidence in civil proceedings. These changes ensure preservation notice information is treated consistently with stored communication warrant information and are necessary to comply with Article 16(3) of the Cybercrime Convention.

Items – 26 and 27 Part 3-5 (heading) and Division 1 of Part 3-5 (heading)

Items 26 and 27 insert the concept of preservation into the headings of Chapter 3, Part 3-5 and Chapter 3, Part 3-5 Division 1. The Part currently only relates to stored communications access records, such as the issuing or revocation of stored communications warrants. This Bill expands the Division to include records regarding preservation so that the preservation and revocation activities are also subject to appropriate record keeping and inspection requirements.

Item 28 – Section 150A

Item 28 inserts new section 150A to require the chief officer of enforcement agencies to ensure preservation notices, revocations and evidentiary certificates are kept in each agency's records. The new section gives enforcement agencies flexibility in how they keep these records, such as maintaining a file or folder for each type of document.

Item 29 – Division 1 of Part 3-5 (heading)

Item 29 inserts the concept of preservation into the heading of Division 2 of Part 3-5. This change is to reflect that preservation notices are to be subject to inspection by the Ombudsman.

Items 30 and 31 – Paragraph 152(a) and Subsection 153(3)

Items 30 and 31 insert a new reference to new section 150A into existing sections 152 and 153. This change is to allow the Ombudsman to confirm that agencies are keeping records as required by new section 150A, and include the results of inspections in the Ombudsman's report.

Item 32 – Part 3-5 Division 3 Inspection of preservation notice records by Inspector-General of Intelligence and Security

Item 32 creates new Division 3 and new section 158A. New section 158A refers to provisions in the *Inspector-General of Intelligence and Security Act 1986* which give the Inspector-General of Intelligence and Security the function of inquiring into and conducting inspections with regards to the preservation notice scheme in the TIA Act.

The purpose of the section is to highlight the Inspector-General of Intelligence and Security's functions. The section does not intend to change or alter any functions, obligations or powers expressed in the *Inspector-General of Intelligence and Security Act 1986.*

Item 33 – Section 161A

Item 33 inserts new section 161A into the TIA Act to expand the annual reporting obligations for enforcement agencies in Division 2 of Part 3-6 to include statistics on the number of preservation and revocation notices issued. In the case of the AFP, the annual reporting obligation is also expanded to include statistics about foreign preservation notices and revocations. The annual reporting obligations are an important element of the oversight regime contained in the TIA Act.

Schedule 2 – Amendments relating to mutual assistance

Mutual Assistance in Criminal Matters Act 1987

Telecommunications (Interception and Access) Act 1979

Schedule 2 of the Bill will amend the *Mutual Assistance in Criminal Matters Act 1987 (*MA Act), the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and *Telecommunications Act 1997* to implement Australia's international cooperation obligations under the Convention. Australia is already compliant with the majority of international cooperation obligations under the Convention. The amendments in this Schedule will ensure all obligations are met.

Part 1 of Schedule 2 will implement Australia's obligations under Article 31 of the Convention. Article 31 requires Australia to ensure that a foreign country can secure access to stored computer data, including data that has been preserved pursuant to Article 29. The obligations of Article 29 will be implemented by the amendments contained in Schedule 1.

Part 1 of Schedule 2 will amend the MA Act and the TIA Act to allow a stored communication warrant to be obtained for foreign law enforcement purposes. A stored communication warrant currently can only be obtained for domestic investigations.

Part 2 of Schedule 2 will implement Australia's obligations under Articles 30 and 33 of the Convention. Article 30 of the Convention requires Australia to facilitate the expeditious partial disclosure of traffic data to foreign countries to enable the identification of service providers in another State involved in the transmission of a communication and the path of the communication.

Under current law, existing telecommunications data, such as subscriber details and call charge records, can currently only be disclosed to other countries for foreign law enforcement purposes following a formal mutual assistance request from the foreign country. This process can be time-consuming. The amendments in Part 2 will remove the need for a foreign country to submit a formal mutual assistance request, instead enabling existing telecommunications data to be provided to a foreign law enforcement agency on a police to police basis.

Article 33 requires Australia to provide mutual assistance to foreign countries in the real-time collection of traffic data of specified communications transmitted by means of a computer system. Further, Article 33 requires the assistance to be provided with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Currently, the TIA Act only enables an authorised officer from an Australian criminal law enforcement agency to collect and disclose prospective telecommunications data for domestic law enforcement purposes. Part 2 will amend the MA Act and the TIA Act to enable the collection of prospective telecommunications data for foreign law enforcement purposes where the foreign country has made a mutual assistance request and the Attorney-General has authorised provision of the assistance.

Part 3 of Schedule 2 will make minor amendments to the Telecommunications Act to ensure that carriers and carriage service providers (C/CSPs) are able to recover any costs incurred when assisting the enforcement of the criminal laws in force in a foreign country (as they can currently recover costs for domestic assistance). This will ensure consistency for C/CSPs regardless of

whether they are providing assistance for domestic law enforcement or foreign law enforcement purposes.

Mutual Assistance in Criminal Matters Act 1987

Part 1 – Stored Communications

Subsection 3(1) of the MA Act sets out definitions that are relevant to the operation of the Act. Items 1, 2 and 3 will insert new definitions relevant to the changes that will be made by this Schedule.

Item 1

New section 15B (which will be inserted by item 4) will establish a process for Australia to respond to a foreign country's request for stored communications that are held by a carrier where there are reasonable grounds to believe that they are relevant to a foreign investigation or investigative proceeding.

This item will insert a definition of ***carrier*** in subsection 3(1) of the MA Act. ***Carrier*** will be given the same meaning as in the TIA Act. The TIA Act gives the term ***carrier*** the same meaning as in the Telecommunications Act. The Telecommunications Act defines a carrier as someone who holds a carrier licence and defines a C/CSP as a person who supplies a listed carriage service to the public.

Item 2

This item will insert a definition of ***investigative proceeding***. It will be defined by reference to paragraphs (a) and (b) of the existing definition of *proceeding* in the MA Act:

- gathering evidential material that may lead to the laying of a criminal charge (paragraph (a)), or
- assessing evidential material in support of the laying of a criminal charge (paragraph (b)).

Under some legal systems, a suspect may be formally charged with an offence later in the legal process than in Australia. Accordingly, the inclusion of 'investigative proceeding' in addition to 'investigation' will enable the Attorney-General to authorise Australian law enforcement to apply for a stored communications warrant to assist foreign law enforcement at any point where evidence is still being gathered before charges have been laid.

Item 3

New section 15B which will be inserted by item 4 will establish a process for Australia to respond to a foreign country's request for stored communications where there are reasonable grounds to believe that they are relevant to a foreign investigation or investigative proceeding.

Item 3 will insert a definition of ***stored communication*** in subsection 3(1) of the MA Act. Stored communication will be defined by the meaning given to the term in the TIA Act. That is, it will mean a communication that:

- is not passing over a telecommunications system (so as to distinguish from telecommunications interception)

- is held on equipment that is operated by, and in the possession of, a carrier, and

- cannot be accessed on that equipment by a person who is not a party to the communication without the assistance of an employee of the carrier.

Item 4

Item 4 will insert new Part IIIA into the MA Act to govern assistance in relation to access to stored communications.

Section 15B – Requests by foreign countries for stored communications

Currently, prescribed Australian agencies may apply for a warrant to covertly access stored communications (for example, email records) to assist in the investigation of domestic offences. However, there is no mechanism to enable a stored communications warrant to be obtained to assist with a foreign investigation.

Section 13 of the MA Act allows stored communications material (such as email records) which has been covertly accessed in the course of an Australian investigation to be provided to a foreign country through take evidence or production order proceedings before a magistrate. However, this mechanism can be time-consuming and is limited to information which has already been obtained in the course of an Australian investigation.

New section 15B will establish the means by which Australia may respond to a foreign country's request for access to stored communications for foreign law enforcement purposes. It will enable the Attorney-General to authorise the Australian Federal Police (AFP) or State police to apply for a stored communications warrant under section 110 of the TIA Act if:

- a request for access to the stored communications has been received from the foreign country

- an investigation or investigative proceeding into a criminal matter has commenced in the requesting country

- the offence the subject of the investigation or investigative proceeding is punishable by a maximum penalty of three or more years imprisonment, life imprisonment or death, or a fine equivalent to, or greater than 900 penalty units (under section 4AA of the Crimes Act, one penalty unit is currently $110), and

- there are reasonable grounds to believe that a carrier holds stored communications relevant to the investigation or investigative proceeding.

In accordance with section 142A of the TIA Act, which will be inserted by item 18, information obtained pursuant to a stored communications warrant may only be communicated subject to certain conditions on the use and distribution of the information, and any other conditions imposed by the Attorney-General.

The penalty threshold for an application for a stored communications warrant made pursuant to a mutual assistance request is modelled on that required for a stored communications warrant application in relation to a domestic offence, which is a period of at least three years imprisonment or 900 penalty units.

Item 2 will insert a definition of ***investigative proceeding*** which will be defined by reference to paragraphs (a) and (b) only of the existing definition of ***proceeding*** in the MA Act.

The Attorney-General will only be able to authorise Commonwealth and State or Territory police forces to apply for, and execute, a stored communications warrant on behalf of a foreign law enforcement agency. This is appropriate as the other bodies that form part of the definition of ***enforcement agency*** are Commonwealth, State or Territory integrity or anti-corruption bodies and it would not be appropriate for these bodies to be applying for, or executing warrants for the purpose of a foreign criminal investigation.

The decision by the Attorney-General to authorise the AFP, State or Territory police to apply for a stored communications warrant will be subject to the grounds of refusal in the MA Act. The decision by an issuing authority to issue a warrant will be subject to the safeguards contained in the application and decision making process as set out in the TIA Act. These will be amended as necessary (by items 5-16) to ensure that they also apply to the issuing of a warrant in relation to a mutual assistance application.

Telecommunications (Interception and Access) Act 1979

Item 5

Item 5 will insert a definition of ***investigative proceeding*** in subsection 5(1) of the TIA Act. ***Investigative proceeding*** will be defined by the meaning given to the term in the MA Act (which will be inserted by item 2). It will be defined by reference to paragraphs (a) and (b) of the existing definition of ***proceeding*** in the MA Act to ensure that stored communications can be sought at any point where evidence is still being gathered before charges have been laid regardless of the legal system of the requesting country.

Item 6

Currently, under section 116 of the TIA Act, prescribed Australian enforcement agencies may apply to an 'issuing authority' for a warrant to covertly access stored communications to assist in the investigation of domestic offences. The enforcement agency's investigation must relate to a domestic offence that is punishable by imprisonment for at least three years, or a fine of at least 180 penalty units for an individual or 900 penalty units for a corporation (under section 4AA of the Crimes Act, one penalty unit equates to $A110). This law enforcement tool is not currently available for the investigation or prosecution of a foreign offence.

Item 9 will amend section 116 to facilitate the issue of a stored communications warrant in response to a mutual assistance application.

This item will insert a definition of ***mutual assistance application*** in subsection 5(1) of the TIA Act. It will be defined as an application for a stored communications warrant made as a result of an authorisation by the Attorney-General under section 15B of the MA Act. This will enable an application to an issuing authority for a warrant to covertly access stored communications for the investigation or prosecution of a foreign offence.

Item 7

This item will insert new section 5EA into the TIA Act. This new section will define ***serious foreign contravention*** for the purpose of the TIA Act. A stored communication warrant will only be able to be issued by an issuing authority following a mutual assistance application if the application relates to a ***serious foreign contravention***.

A ***serious foreign contravention*** will be defined as a contravention of the law of a foreign country that is punishable by a maximum penalty of:

- three or more years imprisonment, life imprisonment or the death penalty, or
- a fine at least equivalent to 900 penalty units (under section 4AA of the Crimes Act, one penalty unit is currently $110).

This penalty threshold is similar to the threshold for the issue of a stored communications warrant for a domestic offence, which is a period of at least three years imprisonment or 900 penalty units. A similar penalty threshold will ensure that stored communications warrants for foreign offences will only be able to be issued where a warrant for a domestic investigation would also be able to be issued.

Item 8

Section 6H of the TIA Act specifies when an application relates to a particular person. This item will omit 'paragraph 116(1)(d)' in paragraph 6H(c) and replace it with a reference to 'subparagraph 116(1)(d)(i) or (ii), as the case requires'. The reference to paragraph 116(1)(d) will be replaced with 'subparagraph 116(1)(d)(i) or (ii), as the case requires' as a result of the amendment to be made by item 9.

Item 9

Currently, prescribed Australian enforcement agencies may apply to an ***issuing authority*** for a warrant to covertly access stored communications to assist in the investigation of domestic offences. Subsection 116(1) of the TIA Act lists the matters about which an issuing authority must be satisfied when considering an enforcement agency's application for a stored communications warrant.

Paragraph 116(1)(d) states that a warrant can only be issued if information that would be likely to be obtained from accessing those stored communications would be likely to assist in connection with the investigation by the agency of a serious contravention of which the person is involved, including as a victim of the serious contravention. A serious contravention is limited to domestic offences that are punishable by imprisonment for at least three years, or a fine of at least 180 penalty units for an individual or 900 penalty units for a corporation (under section 4AA of the Crimes Act, one penalty unit equates to $A110). As such, there is no scope under section 116 for a stored communications warrant to be issued in relation to the investigation or prosecution of a foreign offence.

This item will replace some of the wording of paragraph 116(1)(d) with two new subparagraphs, the effect of which will be that a stored communications warrant will continue to be able to be issued for a serious contravention, but will also be able to be issued in relation to the investigation or prosecution of a foreign offence.

New subparagraph 116(1)(d)(i) will require an issuing authority to be satisfied, in relation to an application other than a mutual assistance application (that is, for the investigation of a domestic contravention), that information that would be likely to be obtained under the warrant would be likely to assist in the investigation of a serious contravention in which the person in involved, including as a victim of the serious contravention. This retains the current wording of paragraph 116(1)(d).

New subparagraph 116(1)(d)(ii) will require an issuing authority to be satisfied, in relation to a mutual assistance application (that is, for the investigation of a foreign offence on behalf of a foreign country), that information that would be likely to be obtained under the warrant would be likely to assist in the investigation of a serious foreign contravention to which the mutual assistance application relates and in which the person is involved, including as a victim of the serious foreign contravention.

Issuing authority is defined in section 6DB of the TIA Act as:

- a judge of a court created by Parliament who has consented to being appointed an issuing authority
- a federal magistrate who has consented to being appointed an issuing authority
- a magistrate who has consented to being appointed an issuing authority, or
- a member, senior member or Deputy President of the AAT who is enrolled as a legal practitioner and has been enrolled for at least five years.

Although subsection 116(1) references an application by an enforcement agency, under new section 15B (which will be inserted by item 4), only a Commonwealth or State or Territory police force will be able to be authorised to apply for a warrant by the Attorney-General.

Item 10

Section 116 of the TIA Act lists the matters about which an issuing authority must be satisfied when considering an enforcement agency's application for a stored communications warrant. Paragraph 116(1)(e) requires an issuing authority to have regard to certain matters listed in subsection 116(2). The matters listed in subsection 116(2) include:

- how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant
- the gravity of the conduct constituting the serious contravention
- how much the information that would be likely to be obtained through accessing the stored communications would be likely to assist in connection with the investigation
- to what extent methods of investigating the serious contravention that do not involve the use of a stored communications warrant in relation to the person have been used by, or are available to, the agency
- how much the use of such methods would be likely to assist in connection with the investigation by the agency of the serious contravention, and

- how much the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention, whether because of delay or for any other reason.

This item will insert 'or (2A) (as the case requires)' after 'subsection (2)' in paragraph 116(1)(e). It will be consequential upon item 13, which will insert new subsection 116(2A). Subsection 116(2A) will list the factors that will need to be considered if the stored communications warrant application is a mutual assistance application. These factors will include:

- how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant
- the gravity of the conduct constituting the serious foreign contravention, and
- how much the information that would be likely to be obtained through accessing the stored communications would be likely to assist in connection with the investigation.

These matters will be substantially similar to those applicable for a warrant application for a domestic purpose.

As a result, the issuing authority will only be required to have regard to the matters referred to in subsection (2) or subsection (2A) (as the case requires). This will ensure that each warrant application is determined by reference to specific criteria and not irrelevant matters.

Item 11

Subsection 116(2) lists certain matters that an issuing authority must have regard to when determining whether to issue a stored communications warrant.

This item will replace the words '[t]he matters' with 'In the case of an application other than a mutual assistance application, the matters'. This item will be consequential upon item 13 which will insert subsection 116(2A). Subsection 116(2A) will list the matters to which an issuing authority must have regard when determining an application for a stored communications warrant made in response to a mutual assistance request. These matters will be substantially similar to those applicable for a warrant application for a domestic purpose. The difference in factors that need to be considered are important in ensuring that all relevant factors are considered by the issuing authority.

This amendment will ensure that subsection 116(2) will only apply for domestic applications and not for applications relating to a mutual assistance request.

Item 12

Subsection 116(2) lists certain factors that an issuing authority must have regard to when determining whether to issue a stored communications warrant. Paragraph 116(2)(c) requires an issuing authority to have regard to how much the information that would be likely to be obtained by accessing those stored communications would assist the domestic investigation.

This item will replace 'paragraph (1)(d)' with 'subparagraph (1)(d)(i)', so that paragraph 116(2)(c) will read 'how much information referred to in subparagraph (1)(d)(i) will be likely to assist in connection with the investigation...'. This item is consequential upon item 7.

Item 7 will amend paragraph 116(1)(d) to provide that an issuing authority may issue a stored communications warrant if satisfied that information likely to be obtained pursuant to a stored communications warrant will be likely to assist with:

- the investigation of a serious contravention (domestic offence), or
- the investigation by a foreign country of a serious foreign contravention.

This item, combined with the amendment in item 11, will provide that, in the case of an application other than a mutual assistance application, the issuing authority must have regard to how much the information will be likely to assist in the investigation of a serious contravention (a domestic contravention).

New subsection 116(2A) will outline the matters to which an issuing authority must have regard in relation to a mutual assistance application for a stored communications warrant.

Item 13

Subsection 116(2) lists certain factors that an issuing authority must have regard to when determining whether to issue a stored communications warrant. These matters include:

- how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant
- the gravity of the conduct constituting the serious contravention
- how much the information that would be likely to be obtained through accessing the stored communications would be likely to assist in connection with the investigation
- to what extent methods of investigating the serious contravention that do not involve the use of a stored communications warrant in relation to the person have been used by, or are available to, the agency
- how much the use of such methods would be likely to assist in connection with the investigation by the agency of the serious contravention, and
- how much the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention, whether because of delay or for any other reason.

However, these factors do not take into account relevant considerations for foreign offences such as how much the information would assist the relevant foreign investigation.

As item 9 will allow an issuing authority to issue a warrant in relation to serious foreign contraventions following a mutual assistance application, it is important that the issuing authority is required to consider matters relevant to the nature of a mutual assistance application.

This item will insert new subsection 116(2A). This subsection will set out the matters to which an issuing authority must have regard (as will be required under paragraph 116(1)(e) as amended by item 10) when determining an application for a stored communications warrant made pursuant to a mutual assistance request.

These matters will be:

- the likely interference with any person's privacy
- the gravity of the conduct constituting the serious foreign contravention, and
- how much the information obtained by accessing the stored communication would assist in connection with the foreign investigation, to the extent this can be determined.

These matters will be substantially similar to those applicable for a warrant application for a domestic purpose under subsection 116(2). The matters currently required to be considered (under subsection 116(2)) in relation to a domestic contravention that will not be mirrored in new subsection 116(2A) relate to knowledge that is only feasible for the enforcement agency making the application to possess in relation to a domestic contravention (such as the extent to which alternative investigative methods have been used or are available). As such, it is not appropriate for these matters to be included as relevant considerations in subsection 116(2A).

Item 14

Subsection 116(3) states that a stored communications warrant may be issued in relation to more than one serious contravention. Item 14 will amend subsection 116(3) so that one warrant may also relate to more than one serious foreign contravention. However, the amendment will prevent a single warrant being issued in relation to both a serious contravention (domestic offence) and a foreign serious contravention.

This is appropriate as there are different considerations that must be taken into account when issuing a warrant and different requirements relating to the use of information that has been obtained under the respective warrants (subsections 139(2), (3) and (4) set out the uses that can be made of information obtained for a domestic offence and new subsection 139(4A) will outline the uses that can be made of information obtained for a foreign offence)

Item 15

Section 118 of the TIA Act sets out what must be included in a stored communications warrant. In particular, subsection 118(3) requires the warrant to include particulars of each serious contravention in relation to which the warrant was issued, as is required to be considered under paragraph 116(1)(d). Item 9 will amend paragraph 116(1)(d) so that an issuing authority may also issue a stored communications warrant if satisfied that information likely to be obtained pursuant to a stored communications warrant will be likely to assist with the investigation by a foreign country of a serious foreign contravention.

This item will insert the words 'or serious foreign contravention' after 'contravention' in subsection 118(3). This will ensure that the particulars of any foreign contravention will need to be included on a stored communications warrant issued as a result of a mutual assistance application.

Item 16

Section 118 of the TIA Act sets out what must be included on a stored communications warrant. In particular, subsection 118(3) requires the warrant to include particulars of each contravention in relation to which the warrant was issued, as is required to be considered under paragraph 116(1)(d).

Item 9 will amend paragraph 116(1)(d) by inserting two subparagraphs so that an issuing authority may issue a stored communications warrant if satisfied that information likely to be obtained pursuant to a stored communications warrant will be likely to assist with the investigation of either a serious contravention (a domestic offence) or a serious foreign contravention.

This item will replace the reference in subsection 118(3) to paragraph 116(1)(d) with a reference to 'subparagraph 116(1)(d)(i) or (ii) as the case may be'. This will ensure that a stored communications warrant that relates to a domestic serious contravention must include the particulars of the domestic offence or offences and a stored communications warrant in relation to a serious foreign contravention must include particulars of the serious foreign contravention or contraventions.

Item 17

Subsection 139(1) of the TIA Act states that lawfully accessed information or stored communications warrant information can only be used or communicated to another person for the purposes listed in subsection 139(2) (which include an investigation into, or proceedings relating to certain offences). Lawfully accessed information is defined in subsection 5(1) of the TIA Act as information obtained by accessing a stored communication. Stored communications warrant information is defined in subsection 5(1) of the TIA Act as information about:

- an application for a stored communications warrant
- the issue of a stored communications warrant
- the existence or non-existence of a stored communications warrant
- the expiry of a stored communications warrant
- any other information that is likely to enable the identification of the telecommunications service to which a stored communications warrant relates, or
- any other information that is likely to enable the identification of a person specified in a stored communications warrant as a person using, or likely to use, the telecommunications service to which the warrant relates.

Item 19 will insert new subsection 139(4A). This new subsection will set out the purposes for which information obtained through the execution of a warrant issued as a result of a mutual assistance application can be used. These purposes will include transmission of information to the foreign country and record keeping requirements.

This item will amend subsection 139(1) to include a reference to new subsection 139(4A) after the reference to subsection 139(2). This will ensure that lawfully accessed information or stored communications warrant information can only be provided to a foreign country where it was obtained for that purpose under a mutual assistance related stored communications warrant.

Item 18

Subsection 139(1) of the TIA Act states that lawfully accessed information or stored communications warrant information can only be used or communicated to another person for the purposes listed in subsection 139(2) (which include an investigation into, or proceedings relating to certain offences).

Item 19 will insert new subsection 139(4A). This new subsection will set out the purposes for which information obtained through the execution of a warrant issued as a result of a mutual assistance application can be used. These purposes will include transmission of information to the foreign country and record keeping requirements.

This item will amend subsection 139(2) to include the words '[I]n the case of information obtained by the agency other than through the execution of a warrant issued as a result of a mutual assistance application.' This amendment will ensure that the purposes for which information may be used or communicated under subsection 139(2) for warrants that were issued in relation to a domestic serious contravention are limited to domestic purposes.

Item 19

Subsection 139(1) of the TIA Act states that lawfully accessed information or stored communications warrant information can only be used or communicated to another person for the purposes listed in subsection 139(2) (which include an investigation into, or proceedings relating to certain offences). Lawfully accessed information is defined in subsection 5(1) of the TIA Act as information obtained by accessing a stored communication. Stored communications warrant information is defined in subsection 5(1) of the TIA Act as information about:

- an application for a stored communications warrant
- the issue of a stored communications warrant
- the existence or non-existence of a stored communications warrant
- the expiry of a stored communications warrant
- any other information that is likely to enable the identification of the telecommunications service to which a stored communications warrant relates, or
- any other information that is likely to enable the identification of a person specified in a stored communications warrant as a person using, or likely to use, the telecommunications service to which the warrant relates.

Item 17 will amend subsection 139(1) to include a reference to new subsection 139(4A) after the reference to subsection 139(2).

This item will insert new subsection 139(4A). This new subsection will set out the purposes for which information obtained through the execution of a mutual assistance related warrant will be able to be used. This subsection will allow information to be used or communicated for the purpose of providing the information to the foreign country or an appropriate authority of the foreign country, or for record keeping requirements.

This new subsection will ensure that following a request from a foreign country, and the execution of a stored communication warrant as a result of that application, the information obtained through accessing the stored communications is able to be provided to the foreign country by the law enforcement agency for its use to investigate the offence or offences to which the mutual assistance request related.

Item 20

Item 19 inserts a new subsection 139(4A) which will set out the purposes for which information obtained through the execution of a warrant issued as a result of a mutual assistance application can be used.

This item will insert new section 142A. This section, notwithstanding new subsection 139(4A), will set out conditions that must be complied with in communicating information obtained under a stored communications warrant to a foreign country. These conditions are:

- that the information will only be used for the purposes for which the foreign country requested the information
- that any document or other thing containing the information will be destroyed when it is no longer required for those purposes, and
- any other condition determined, in writing, by the Attorney-General.

These conditions will ensure that appropriate restrictions are in place when information, particularly personal information, is transferred to a foreign country.

Item 21

Section 161 of the TIA Act requires the Minister to report once every year on the use of stored communications warrants. Subsection 162(1) of the TIA Act sets out that, in relation to each enforcement agency, the report must include statistics about all applications, including telephone applications, for stored communications warrants made during that year.

This item will add two new paragraphs to subsection 162(1). The new paragraphs will require the report to also include, in relation to each enforcement agency:

- the statistics on the number of mutual assistance applications made during that year, and
- for each foreign offence in respect of which a stored communications warrant was issued, the Commonwealth, State or Territory offence that is of the same, or of substantially the same, nature.

Items 22 and 23

Section 161 of the TIA Act requires the Minister to report once every year on the use of stored communications warrants. Subsection 162(2) sets out the overall statistics that must be contained in the report. This includes statistics about all applications, including telephone and renewal applications, for stored communications warrants made during that year and how many warrants included special conditions or restrictions relating to access to stored communications under the warrant.

Items 22 and 23 will insert new matters that must be included in the report. Item 22 will insert new paragraph 162(2)(ba) which will require the report to contain statistics on the number of mutual assistance applications made during that year. Item 23 will insert new paragraph 162(2)(e) which will require the report to include for each foreign offence in respect of which a stored communications warrant was issued, the Commonwealth, State or Territory offence that is of the same, or of substantially the same, nature.

Item 24

This item sets out the application of the amendments by this Part. It will ensure that the amendments made by this Part apply to any requests that are under consideration on or after the commencement of this item, regardless of whether the request was made before or after that commencement.

Part 2 – Amendments relating to Telecommunications Data

Under the TIA Act, an authorised officer from an Australian enforcement agency can authorise a telecommunications carrier to disclose historical telecommunications data, such as subscriber details and call charge records, if that officer is of the belief that the disclosure is reasonably necessary for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty or protection of the public revenue. Mutual assistance procedures may be used to provide historical telecommunications data to foreign countries for the investigation or prosecution of foreign criminal offences through the use of a search warrant under section 38C of the MA Act following authorisation by the Attorney-General under section 15. However, historical telecommunications data cannot currently be provided to foreign countries on an agency-to-agency basis.

The TIA Act also enables an authorised officer from an Australian criminal law enforcement agency to authorise a telecommunications carrier to disclose prospective telecommunications data – this is, telecommunications data that comes into existence during the period in which the authorisation is in force. However, this type of authorisation can only be made in relation to a domestic offence, not a foreign offence.

Part 2 will amend:

- the TIA Act to allow the AFP to obtain historical telecommunications data from a telecommunications carrier and pass that data on to a foreign law enforcement agency without the need for a request to be made by the foreign country under the MA Act—that is, on an agency to agency basis, and

- the MA Act and the TIA Act to enable the collection of prospective telecommunications data for foreign law enforcement purposes, following a formal request from the foreign country and Attorney-General approval.

Mutual Assistance in Criminal Matters Act 1987

Subsection 3(1) of the MA Act sets out definitions that are relevant to the operation of the Act. Items 25 and 26 will insert new definitions relevant to the changes that will be made by this Part.

Item 25

Item 25 will insert a definition of ***communication*** into the MA Act. It will be defined by its meaning in the TIA Act which includes a conversation and a message in a variety of forms including speech and text.

The term ***communication*** is referred to in new section 15D of the MA Act, which will be inserted by item 27. New section 15D will enable foreign countries to request the disclosure of specified information or documents that relate to a communication passing over a telecommunications system.

Item 26

Item 26 will insert a definition of ***telecommunications system*** into the MA Act. It will be defined by its meaning in the TIA Act which is a telecommunications network that is in, or partly in Australia and includes equipment, a line or other facility that is connected to such a network in Australia.

The term ***telecommunications system*** will be referred to in new section 15D of the MA Act, which will be inserted by item 27. New section 15D will enable foreign countries to request the disclosure of specified information or documents that relate to a communication passing over a telecommunications system.

Item 27

Currently, the TIA Act enables an authorised officer from an Australian criminal law enforcement agency to authorise a telecommunications carrier to disclose prospective telecommunications data – this is, telecommunications data that comes into existence during the period the authorisation is in force. However, this type of authorisation can only be made in relation to a domestic offence, not a foreign offence.

This item will insert new Part IIIB – Assistance in relation to telecommunications data – into the MA Act. This new Part will contain section 15D which will outline how the Attorney-General can respond to a request by a foreign country for assistance in relation to telecommunications data.

Subsection 15D(1) will set out when section 15D will apply. The section will apply if a foreign country requests the disclosure of specified information or documents that come into existence during a specified period (prospective telecommunications data) and the information or documents relate to the fact of a communication passing over a telecommunications system. This subsection is limited to prospective telecommunications data and will not apply to historical telecommunications data, that is, information or documents that already exist and relate to communications that have already taken place. The disclosure of historical telecommunications data to a foreign country for foreign law enforcement purposes will be governed by new sections 180A and 180C of the TIA Act which will be inserted by item 41.

Subsection 15D(2) will set out what information or documents relate to the fact of a communication passing over a telecommunications system. It will state that information or documents **do not** relate to the fact of a communication passing over a telecommunications system if the information is the contents of the communication. Therefore, section 15D will not extend to the contents or substance of a communication. These are 'stored communications' and will be governed by the stored communications regime in the TIA Act (which will be amended by items 5 to 23) and section 15B of the MA Act (which will be inserted by item 4) which establish the means by which Australia may respond to a foreign country's request for material obtained through accessing stored communications.

Subsection 15D(3) will set out when the Attorney-General can authorise the provision of assistance to the foreign country. The Attorney-General will only be able to make an authorisation if satisfied that:

- an investigation relating to a criminal matter involving an offence against the law of the foreign country (the requesting country) has commenced in the requesting country, and

- the offence to which the investigation relates is punishable by a maximum penalty of imprisonment for three or more years, imprisonment for life or the death penalty.

The penalty threshold of three years imprisonment mirrors the threshold that applies to accessing prospective telecommunications data for domestic purposes (see subsection 180(4) of the TIA Act). This will ensure that the use of these powers for foreign purposes does not extend beyond when these powers can be exercised for domestic purposes.

New section 180B of the TIA Act (which will be inserted by item 41) will govern the authorisation process for obtaining and disclosing the specified information or documents, following Attorney-General approval under new section 15D of the MA which will be inserted by item 27.

As the Attorney-General's approval is required prior to consideration under the TIA Act, the disclosure of prospective telecommunications data will be subject to both the safeguards in the TIA Act and the grounds of refusal in the MA Act.

Telecommunications Act 1997

Division 5 of Part 13 of the Telecommunications Act sets out certain record keeping requirements for C/CSPs relating to the disclosure of telecommunications data under the TIA Act. Items 28, 29, 30 and 31 will make various amendments to the record keeping requirements in Division 5 of Part 13 of the Telecommunications Act to reflect the amendments made in this Part requiring disclosure of telecommunications data for foreign law enforcement purposes.

Item 28

Section 305 of the Telecommunications Act requires C/CSPs or number-database operators to retain notification of an authorisation under Division 4 of Part 4-1 of the TIA Act to disclose telecommunications data for three years.

Item 41 will insert new Division 4A into Part 4-1 of the TIA Act. This new Division will outline when telecommunications data can be disclosed for foreign law enforcement purposes. This item will amend subsection 305(1) of the Telecommunications Act to ensure that where a C/CSP or

number-database operator is notified of an authorisation to disclose telecommunications data under new Division 4A of the TIA Act, they will also be required to retain that notification for three years.

Item 29

Section 306 of the Telecommunications Act requires a record of disclosures of historical telecommunications data under, among other provisions, section 177, 178 or 179 or subsection 180(3) of the TIA Act to be made and retained for three years.

Item 41 will insert new Division 4A into Part 4-1 of the TIA Act. This new Division will outline when telecommunications data can be disclosed for foreign law enforcement purposes.

Item 29 will amend subparagraph 306(1)(b)(ii) of the Telecommunications Act to also include section 180A or section 180C. This will ensure that a C/CSP or number-database operator must make and retain a record of disclosures of historical telecommunications data for foreign law enforcement purposes.

Items 30 and 31

Section 306A of the Telecommunications Act requires records of disclosures of prospective telecommunications data under section 180 of the TIA to be made and retained for three years. New section 180B, which will be inserted by item 41, will provide for the disclosure of prospective telecommunications data for foreign law enforcement purposes.

These items will amend paragraph 306A(1)(b) of the Telecommunications Act to also include a reference to section 180B and subsection 180B(2) of the TIA Act respectively. This will ensure that a C/CSP or number-database operator must make and retain a record of disclosures of prospective telecommunications for foreign law enforcement purposes.

Telecommunications (Interception and Access) Act 1979

Subsection 5(1) of the TIA Act sets out definitions that are relevant to the operation of the TIA Act. Items 32 and 33 will insert new, or amend existing, definitions relevant to the changes that will be made by this Schedule.

Item 32

Authorised officer is currently defined in subsection 5(1) of the TIA to be the head or deputy of an enforcement agency or a person who holds a management position covered by an authorisation made by the head of that enforcement agency under subsection 5AB(1) of the TIA Act. ***Enforcement agency*** is also defined in subsection 5(1) and includes the AFP, State and Territory police forces as well as other State and Territory misconduct or integrity bodies such as the Office of Police Integrity and the Corruption and Crime Commission.

This item repeals the current definition and replaces it with a two-part definition. The first part inserts a definition for the purposes of new section 180A, 180B, 180C and 180D, new subsection 184(5) and 185(2) and new paragraph 186(1)(ca) (which will be inserted by items 41, 47, 49 and 50 respectively). The definition of ***authorised officer*** for these purposes is limited to the Commissioner or Deputy Commissioner of Police (the AFP Commissioner or Deputy Commissioner) or a member of the AFP authorised under new subsection 5AB(1A) (which will be inserted by item 35).

The second part of the definition mirrors the current definition of the head or deputy of an enforcement agency or a person who holds a management position in an enforcement agency covered by an authorisation made by the head of that enforcement agency under subsection 5AB(1).

Item 33

This item will insert a new definition of ***foreign law enforcement agency***. This term will be defined as a police force of a foreign country or any other authority or person responsible for the enforcement of the laws of the foreign country.

This definition is required to clearly outline who telecommunications data can be provided to under new sections 180A, 180B and 180C which will be inserted by item 41. These new sections outline when telecommunications data can be obtained and disclosed for a foreign law enforcement purpose.

Item 34

Section 5AB provides that the head of a law enforcement agency may authorise a management position or office for the purposes of paragraph (c) of the definition of ***authorised officer***.

Item 32 amends the definition of authorised officer to give effect to changes made elsewhere in this Part. As such, item 34 will remove the reference to paragraph (c) and replace it with a reference to subparagraph (b)(iii) of the definition of authorised officer as amended by item 32.

Item 35

Subsection 5AB(1) provides that the head of a law enforcement agency may authorise a management position or office for the purposes of paragraph (c) of the definition of ***authorised officer***.

Subsection 5AB(2) requires the head of the law enforcement agency to give a copy of any authorisation made under subsection 5AB(1) to the Communications Access Co-ordinator (as defined by section 6R of the TIA Act).

This item will repeal subsection 5AB(2) and replace it with two new subsections.

New subsection 5AB(1A) will provide that, for the purposes of new paragraph (a) of the definition of ***authorised officer***, which will be inserted by item 32, the Commissioner of Police may authorise *a senior executive AFP employee who is a member of the Australian Federal Police* to be an authorised officer. Therefore, to be authorised by the Commissioner of Police to be an authorised officer, the person would need to be a senior executive employee of the AFP (equivalent of an SES) and a member of the AFP. A member of the AFP is any AFP employee (other than a protective service officer) declared by the Commissioner to be a member of the AFP. A declaration can only be made if the Commissioner is satisfied that the employee meets certain competency and qualification requirements.

As such, new paragraph (a) of the definition of 'authorised officer', which will apply for the purposes of new sections 180A, 180B, 180C and 180D, new subsection 184(5) and 185(2) and new paragraph 186(1)(ca) (which will be inserted by items 41, 47, 49 and 50 respectively), will be limited to the Commissioner or Deputy Commissioner of Police (the AFP Commissioner or Deputy Commissioner) or a *senior executive AFP employee who is a member of the Australian Federal Police* authorised under new subsection 5AB(1A).

New subsection 5AB(2) will replace the requirement currently in subsection 5AB(2). The new subsection will require a copy of an authorisation:

- made under subsection 5AB(1) to be given to the Communications Access Co-ordinator by the head of the law enforcement agency that made the authorisation, or

- made under subsection 5AB(1A) to be given to the Communications Access Co-ordinator by the Commissioner of Police.

Item 36

Sections 276, 277 and 278 of the Telecommunications Act prohibit the disclosure of information or documents relating to communications. Section 171 of the TIA Act provides an outline of Part 4-1 of the TIA Act. This outline sets out certain circumstances when sections 276, 277 and 278 of the Telecommunications Act do not prohibit a disclosure of information or a document.

This item will amend subsection 171(1) of the TIA Act to include a reference to new Division 4A of Part 4-1 of the TIA Act to outline that Division 4A, as well as Divisions 3 and 4, will set out some circumstances when sections 276, 277 and 278 of the Telecommunications Act do not prohibit a disclosure of information or a document.

Item 37

Sections 276, 277 and 278 of the Telecommunications Act prohibit the disclosure of information or documents relating to communications. Section 171 of the TIA Act provides an outline of Part 4-1 of the TIA Act. This outline sets out certain circumstances when sections 276, 277 and 278 of the Telecommunications Act do not prohibit a disclosure of information or a document.

Note 1 at the end of section 171 of the TIA Act sets out what Divisions 3 and 4 of Part 4-1 cover. This item will amend Note 1 so that it will also outline what new Division 4A, which will be inserted by item 41, will cover. New Division 4A will cover disclosures for the purposes of foreign law enforcement.

Item 38

Sections 276, 277 and 278 of the Telecommunications Act prohibit the disclosure of information or documents relating to communications. Section 171 of the TIA Act provides an outline of Part 4-1 of the TIA Act. This outline sets out certain circumstances when sections 276, 277 and 278 of the Telecommunications Act do not prohibit a disclosure of information or a document. Subsection 171(3) of the TIA Act outlines that Division 6 of Part 4-1 creates an offence for the secondary use or disclosure of information or a document disclosed under Division 4.

This item will amend subsection 171(3) of the TIA Act to ensure the outline will clearly state that the offence created in Division 6 also applies to information or a document originally disclosed under new Division 4A, which is inserted by item 41, and will provide for disclosures for the purposes of foreign law enforcement.

Item 39

Section 172 provides that Divisions 3 and 4 of Part 4-1 of the TIA Act do not permit the disclosure of information that is the contents or substance of a communication or a document to the extent that

the document contains the contents or substance of a communication. The disclosure of the contents or substance of a communication is covered separately by the stored communications regime in the TIA Act.

This item will amend section 172 by inserting a reference to new Division 4A. This will confirm that new Division 4A (which will be inserted by item 41) also will not permit the disclosure of information that is, or a document that contains, the contents or substance of a communication.

Item 40

Section 180 outlines when an authorised officer of a criminal law enforcement agency can make an authorisation to disclose specified information or documents that come into existence during the period for which the authorisation will be in force (prospective telecommunications data) for domestic law enforcement purposes. Subsection 180(5) states that prior to making the authorisation, the authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

This item will repeal subsection 180(5). The requirement to consider the privacy of any person or persons will be replaced by new section 180F which will be inserted by item 41. This new section will mirror the requirement currently in subsection 180(5) but will apply to any authorisation to disclose information or documents under existing Division 4 of Part 4-1 or new Division 4A of Part 4-1 of the TIA Act (which will also be inserted by item 41).

Item 41 – Subdivision A – Primary disclosures

Under the TIA Act, an authorised officer from an Australian enforcement agency can authorise a telecommunications carrier to disclose historical telecommunications data, such as subscriber details and call charge records, if that officer is of the belief that the disclosure is reasonably necessary for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty or protection of the public revenue. Mutual assistance procedures may be used to provide historical telecommunications data to foreign countries for the investigation or prosecution of foreign criminal offences through the use of a search warrant under section 38C of the MA Act following authorisation by the Attorney-General under section 15. However, historical telecommunications data cannot currently be provided to foreign countries on an agency-to-agency basis.

The TIA Act also enables an authorised officer from an Australian criminal law enforcement agency to authorise a telecommunications carrier to disclose prospective telecommunications data – this is, telecommunications data that comes into existence during the period in which the authorisation is in force. However, this type of authorisation can only be made in relation to a domestic offence, not a foreign offence.

This item will insert new Division 4A into the TIA Act. This Division will provide the basis for historical and prospective telecommunications data to be provided to a foreign country for foreign law enforcement purposes. The disclosure of the data would be subject to the safeguards in the TIA Act.

Section 180A – Authorisations for access to existing information or documents—enforcement of the criminal law of a foreign country

Under the TIA Act, an authorised officer from an Australian enforcement agency can authorise a telecommunications carrier to disclose existing telecommunications data (historical

telecommunications data), such as subscriber details and call charge records, if that officer is of the belief that the disclosure is reasonably necessary for the enforcement of the criminal law. Mutual assistance procedures may be used to provide telecommunications data to foreign countries for the investigation or prosecution of foreign criminal offences through the use of a search warrant, which has been authorised by the Attorney-General under section 15 of the Mutual Assistance Act. However, this is a time-consuming process.

New Section 180A will provide the basis for the AFP to authorise the disclosure of historical telecommunications data to a foreign country for the purposes of the enforcement of the criminal law of a foreign country. Under section 180A, historical telecommunications data will be able to be provided to a foreign country on a police to police basis—that is, without a mutual assistance request—in accordance with the requirements which will be set out in section 180A.

Subsections 180A(1), (2) and (3) will detail the process for disclosure of information or a document to the AFP. Subsections (4) and (5) will detail the process for disclosure of the information or document to a foreign law enforcement agency.

Subsection 180A(1)

Subsection 180A(1) will outline that sections 276, 277 and 278 of the Telecommunications Act do not prevent a disclosure of information or a document if they are covered by an authorisation that is in force under new subsection 180A(2).

Subsection 180A(2)

Subsection 180A(2) will provide that an authorised officer of the AFP may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

An ***authorised officer*** is defined in subsection 5(1) of the TIA Act, which will be amended by item 32. For the purposes of section 180A, an authorised officer will be limited to the Australian Federal Police (AFP) Commissioner, an AFP Deputy Commissioner or a senior executive AFP officer who has been authorised in writing by the AFP Commissioner (under subsection 5AB(1A) which will be inserted by item 35). Only these people will be able to authorise a telecommunications carrier or other organisation to disclose relevant information or documents to the AFP under subsection 180A(2).

Subsection 180A(3)

Subsection 180A(3) will set out when an authorised officer is able to make an authorisation under subsection 180A(2). Under subsection 180A(3), an authorised officer will only be able to make an authorisation if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country.

This test mirrors the test in subsection 178(3) which provides the test that is applicable to the disclosure of historical telecommunications data for a domestic purpose.

Subsection 180A(4)

Subsection 180A(4) will provide that where specified information or documents have been disclosed because of an authorisation under subsection 180A(2), an authorised officer of the AFP

may authorise the disclosure of that information or those documents to a foreign law enforcement agency.

An ***authorised officer*** is defined in subsection 5(1) of the TIA Act, which will be amended by item 32. For the purposes of section 180A, an authorised officer will be limited to the Australian Federal Police (AFP) Commissioner, an AFP Deputy Commissioner or a senior executive AFP officer who has been authorised in writing by the AFP Commissioner (under subsection 5AB(1A) which will be inserted by item 35). Only these people will be able to disclose information or documents to a foreign law enforcement agency under subsection 180(4).

A ***foreign law enforcement agency*** will be defined as a police force of a foreign country or any other authority or person responsible for the enforcement of the laws of the foreign country. This definition will be inserted into subsection 5(1) of the TIA Act by item 33.

Subsection 180A(5)

Subsection 180A(5) will set out when an authorised officer is able to make an authorisation under subsection 180A(4). Subsection 180A(5) will provide that an authorised officer must not make an authorisation to disclose information or documents to a foreign law enforcement agency unless satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country. An authorised officer would be able to rely on information provided by the foreign law enforcement agency in determining whether the disclosure was reasonably necessary for the enforcement of the criminal law of a foreign country. Further, the disclosure would need to be appropriate in all the circumstances. This will be intended to allow the authorised officer to consider other relevant factors in determining whether it is appropriate to make the disclosure.

Further, new section 180F, which will also be inserted by item 41, will require an authorised officer, prior to making an authorisation, to have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

Section 180B – Authorisations for access to prospective information or documents—enforcement of the criminal law of a foreign country

Currently, the TIA Act enables an authorised officer from an Australian criminal law enforcement agency to authorise a telecommunications carrier to disclose prospective telecommunications data – this is, telecommunications data that comes into existence during the period the authorisation is in force. However, this type of authorisation can only be made in relation to a domestic offence, not a foreign offence.

New Section 180B will provide the basis for the AFP to authorise the disclosure of prospective telecommunications data to a foreign country for the purposes of the enforcement of the criminal law of a foreign country. Under section 180B, prospective telecommunications data will only be able to be provided to a foreign country where the country has made a mutual assistance request and the Attorney-General has authorised provision of the assistance under new section 15D of the MA Act (which will be inserted by item 27).

Subsections 180B(1) to (7) will detail the process for the disclosure of information or a document to the AFP, including the extension of a prospective authorisation. Subsections 180B(8), (9) and (10) will detail the process for disclosure of the information or document to a foreign law enforcement agency.

Subsection 180B(1)

Subsection 180B(1) will outline that sections 276, 277 and 278 of the Telecommunications Act do not prevent a disclosure of information or a document if they are covered by an authorisation that is in force under new subsection 180B(2).

Subsection 180B(2)

Subsection 180B(2) will provide that an authorised officer of the AFP may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force.

An ***authorised officer*** is defined in subsection 5(1) of the TIA Act, which will be amended by item 32. For the purposes of section 180B, an authorised officer will be limited to the Australian Federal Police (AFP) Commissioner, an AFP Deputy Commissioner or a senior executive AFP officer who has been authorised in writing by the AFP Commissioner (under subsection 5AB(1A) which will be inserted by item 35). Only these people will be able to authorise a telecommunications carrier or other organisation to disclose relevant information or documents to the AFP under subsection 180B(2).

Subsection 180B(3)

Subsection 180B(3) will set out when an authorised officer is able to make an authorisation under subsection 180B(2). Under subsection 180B(3), an authorised officer will only be able to make an authorisation if:

- the Attorney-General has authorised the making of the authorisation under section 15D of the MA Act (which will be inserted by item 27), and
- the officer is satisfied that the disclosure is:
    - reasonably necessary for the investigation of an offence against a law of a foreign country that is punishable by imprisonment for three or more years, imprisonment for life or the death penalty, and
    - appropriate in all the circumstances.

An authorised officer would be able to rely on information provided by the foreign law enforcement agency in determining whether the disclosure was reasonably necessary for the enforcement of the criminal law of a foreign country. Further, the disclosure would need to be appropriate in all the circumstances. This will be intended to allow the authorised officer to consider other relevant factors in determining whether it is appropriate to make the disclosure.

The Attorney-General will only be able to make an authorisation under section 15D of the MA Act (which will be inserted by item 27) if satisfied that:

- an investigation relating to a criminal matter involving an offence against the law of the foreign country (the requesting country) has commenced in the requesting country, and
- the offence to which the investigation relates is punishable by a maximum penalty of imprisonment for three or more years, imprisonment for life or the death penalty.

The test in subsection 180B(3) will mirror the test in subsection 180(4) which provides the test that is applicable to the disclosure of prospective telecommunications data for a domestic purpose. Prospective telecommunications data may only be disclosed for a domestic purpose if the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of a domestic offence punishable by at least three years imprisonment.

This ensures that these powers will only be able to be used for foreign law enforcement purposes in circumstances in which they would be able to be used for domestic purposes.

Subsection 180B(4)

Subsection 180B(4) will provide that an authorisation made under subsection 180B(2) must be revoked if the authorised officer is satisfied that the disclosure is no longer required. This mirrors the requirement at a domestic level to revoke a domestic authorisation under subsection 180(7) if the disclosure is no longer required.

Subsection 180B(5)

Subsection 180B(5) will outline the period of time for which an authorisation made under subsection 180B(2) is in force. Paragraph (a) will provide that the authorisation will come into force at the time the person from whom the disclosure is sought (the carrier) receives notification of the authorisation. Paragraph (b) will provide that the authorisation will end at the time specified in the authorisation, which will not be able to be longer than 21 days from the day the authorisation was made, or the period as extended under subsection 180B(6).

These time periods differ from the length of time that a domestic authorisation is able to be in force. Under subsection 180(6), an authorisation is able to be in force for 45 days. The shorter time frame in subsection 180B(5) reflects the need for greater scrutiny and control over an authorisation to access prospective telecommunications data for foreign purposes.

Subsection 180B(6)

Subsection 180B(6) sets out the process for extending an authorisation made under subsection 180B(2). This subsection will allow an authorisation to be extended where the authorised officer is satisfied that the disclosure of the prospective data is still:

- reasonably necessary for the investigation of an offence against a law of a foreign country that is punishable by imprisonment for three or more years, imprisonment for life or the death penalty, and

- appropriate in all the circumstances.

An authorised officer would be able to rely on information provided by the foreign law enforcement agency in determining whether the disclosure was reasonably necessary for the enforcement of the criminal law of a foreign country. Further, the disclosure would need to be appropriate in all the circumstances. This will be intended to allow the authorised officer to consider other relevant factors in determining whether it is appropriate to make the disclosure.

An authorisation will only be able to be extended once.

There is no corresponding power to extend a domestic authorisation. However, domestic authorisations are able to be in force for 45 days. This extension power recognises the possibility of

the need to extend an authorisation in certain circumstances while ensuring appropriate controls and safeguards are in place to control access to, and disclosure of prospective telecommunications data for foreign law enforcement purposes.

Subsection 180B(7)

Subsection 180B(7) will provide that an authorisation may only be extended (under subsection 180B(6)) for a maximum of 21 days (this is still shorter than the 45 days for which a domestic authorisation is allowed to be in force).

Subsection 180B(8)

Subsection 180B(8) will outline when information or documents disclosed to the AFP as a result of an authorisation under subsection 180B(2) will be able to be disclosed to a foreign law enforcement agency. The information or documents will only be able to be disclosed if the authorised officer is satisfied that the disclosure is:

- reasonably necessary for the investigation of an offence against a law of a foreign country that is punishable by imprisonment for three or more years, imprisonment for life or the death penalty, and

- appropriate in all the circumstances.

These are the same factors that need to be considered under new subsection 180B(3) when determining whether the original authorisation is able to be made. This will ensure that at all points in the process, the authorised officer will need to explicitly consider the appropriateness of the proposed disclosure to the foreign country. An authorised officer would be able to rely on information provided by the foreign law enforcement agency in determining whether the disclosure was reasonably necessary for the enforcement of the criminal law of a foreign country. Further, the disclosure would need to be appropriate in all the circumstances. This will be intended to allow the authorised officer to consider other relevant factors in determining whether it is appropriate to make the disclosure.

Further, new section 180F, which will also be inserted by item 41, will require an authorised officer, prior to making an authorisation, to have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

Subsection 180B(9)

This subsection will provide that an authorised officer will not be able to make more than one authorisation each day for the disclosure of prospective telecommunications data to a foreign country. This is designed to ensure the AFP reviews the information or documents disclosed to the AFP each day by the carrier before authorising the disclosure of that information, or those documents, to the foreign country.

Subdivision B – Secondary disclosures

Section 180C – Authorisations to disclose information or documents—enforcement of the criminal law of a foreign country

Sections 178 and 179 enable an authorised officer to authorise the disclosure of existing information or documents for the purposes of enforcing the domestic criminal law, enforcing a domestic law

imposing a pecuniary penalty or protecting the public revenue. Section 180 enables an authorised officer to authorise the disclosure of prospective information or documents for the purpose of investigating a domestic offence punishable by at least three years imprisonment.

New section 180C will allow information or documents disclosed because of an authorisation under Division 4 (sections 178, 179 and 180), except for information disclosed under section 178A, to be disclosed to a foreign law enforcement agency. Subsection 180C(2) will provide that the authorisation to disclose to a foreign law enforcement agency will only be able to be made if the authorised officer is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country and the disclosure is appropriate in all the circumstances. These factors will mirror the requirements in new subsection 180A(5) which must be satisfied when historical telecommunications data that has not been originally disclosed for a domestic purpose, is able to be obtained and then disclosed to a foreign country for foreign law enforcement purposes.

New section 180C does not extend to the secondary disclosure of missing person information, as defined in section 182 of the TIA Act. Section 178A allows disclosures of information to Australia police forces for the purposes of locating a person who has been reported missing. Because this information is collected only for the purposes of locating a missing person, disclosing the information to a foreign law enforcement agency for the purpose of investigating a foreign offence is not appropriate.

Further, new section 180F, which will also be inserted by item 41, will require an authorised officer, prior to making an authorisation under section 180C, to have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

Section 180D – Authorisations to disclose information or documents—enforcement of the criminal law

Section 180A (which will be inserted by item 41) will enable an authorised officer to authorise the disclosure of existing information or documents for foreign law enforcement purposes. Section 180B (which will be inserted by item 41) will enable an authorised officer to authorise the disclosure of prospective information or documents for foreign law enforcement purposes.

New section 180D will allow information or documents disclosed because of an authorisation under new Division 4A to be used by the AFP, or further disclosed to the Organisation or to another enforcement agency for domestic purposes.

Subsection 180D(2) will set out when an authorised officer is able to make an authorisation under subsection 180D(1).

Paragraph 180D(2)(a) will restrict when an authorisation can be made to disclose information or documents to the Organisation to where that disclosure is reasonably necessary for the performance by the Organisation of its function of obtaining intelligence relating to security. This purpose is modelled on the permissible disclosures exempted from the secondary use and disclosure offence in subsection 182(2) of the TIA Act.

Paragraph 180D(2)(b) will restrict when an authorisation can be made to disclose information or documents to an enforcement agency to where the disclosure 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.

These purposes are modelled on the disclosures exempted from the secondary use and disclosure offence in subsection 182(2) of the TIA Act.

Paragraph 180D(2)(c) will restrict when an authorisation can be made to allow the AFP to further use the information or documents to where the use 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.

These uses are modelled on the uses exempted from the secondary use and disclosure offence in subsection 182(3) of the TIA Act.

Further, new section 180F, which will also be inserted by item 41, will require an authorised officer, prior to making an authorisation under section 180D, to have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

Subdivision C – Conditions of disclosure to foreign country

Section 180E

Sections 180A, 180B and 180C which will be inserted by this item, will allow information or documents to be disclosed to a foreign law enforcement agency in certain circumstances if specified conditions are met.

New section 180E will impose further restrictions on when information or documents can be disclosed to a foreign country under section 180A, 180B or 180C.

Subsection 180E(1) will set out conditions that must be complied with prior to communicating information or documents to a foreign country. These conditions are:

- that the information will only be used for the purposes for which the foreign country requested the information
- that any document or other thing containing the information will be destroyed when it is no longer required for those purposes, and
- any other condition determined, in writing, by the Attorney-General.

The Attorney-General will only be able to impose conditions on information or documents disclosed under 180B as information provided under 180A or 180C is done so on a police-to-police basis without Attorney-General approval or oversight.

These conditions will ensure that appropriate restrictions are in place when information, particularly personal information, is transferred to a foreign country.

Subsection 180E(2) will state that any conditions determined by the Attorney-General under paragraph 180E(1)(c) will not be a legislative instrument.

Section 180F

New section 180F will also impose further restrictions on when information or documents are able to be disclosed. Section 180F will require an authorised officer, prior to making any authorisation under Division 4 or 4A, to have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

This requirement will mirror the current requirement in subsection 180(5) which applies to an authorisation for the disclosure of prospective telecommunications data for domestic purposes (subsection 180(5) will be repealed by item 40).

This new section will ensure that privacy considerations are taken into account for every disclosure of historical and prospective telecommunications data under Division 4 and 4A of Part 4-1 of the TIA Act.

For the purposes of the Bill, privacy is intended to be interpreted more broadly than is considered by the *Privacy Act 1988*, which regulates the collection, use, disclosure and storage of personal information, as defined in that Act. The Bill's intent is for wider considerations to be made prior to making an authorisation, including the amount of information that making the authorisation will give the agency, the relevance of the accessed information to the investigation in question, as well as how third parties' privacy may be impacted by accessing this information.

Item 42

Section 181 of the TIA Act states that section 276, 277 or 278 of the Telecommunications Act do not prohibit the use by a person of information or documents if that use is connected with the disclosure of the information or documents for the purposes of Division 3 or 4 of Part 4-1 of the TIA Act.

This item will amend section 181 to ensure that sections 276, 277 or 278 also do not prohibit the use by a person of information or documents if that use is connected with the disclosure of the information or documents for the purposes of Division 4A of Part 4-1 of the TIA Act which will be inserted by item 41.

Item 43

Subsection 182(1) of the TIA Act makes it an offence to further use or disclose information originally disclosed as permitted by Division 4 of Part 4-1. This item will insert a reference to new Division 4A (which will be inserted by item 41) into paragraph 182(1)(a). This will ensure that the offence provision in subsection 182(1) also applies to information or documents originally disclosed as permitted by new Division 4A.

Item 44

Subsection 182(1) of the TIA Act makes it an offence to further use or disclose information originally disclosed as permitted by Division 4 of Part 4-1. Further, item 43 will amend subsection 182(1) so that it also applies to the further use or disclosure of information originally disclosed as permitted by Division 4A of Part 4-1.

However, new sections 180C and 180D, which will be inserted by item 41, provide for the further use or disclosure of information or documents. Section 180C will allow information or documents

disclosed because of an authorisation under Division 4 (sections 178, 179 and 180), except for information disclosed under section 178A, to be disclosed to a foreign law enforcement agency. Section 180D will allow information or documents disclosed because of an authorisation under new Division 4A to be used by the AFP, or further disclosed to the Organisation or to another enforcement agency for domestic purposes.

This item will insert a new subsection into section 182 to clarify that the offence in subsection 182(1) will not apply to a disclosure or use of information if that disclosure or use is permitted by section 180C or 180D.

Item 45

Missing persons information is defined by the TIA Act, in relation to a missing person, as information or a document that is disclosed under section 178A. Section 178A allows an authorising officer of the AFP or a Police Force of a State to authorise a carrier to disclose information if it is relevant to locating a missing person. Non-missing person information is currently defined as information or a document that is disclosed as permitted by Division 4, but not under section 178A. That is, it does not include information disclosed for the purpose of locating a missing person.

This item will amend the definition of non-missing person information to include a reference to Division 4A after Division 4. This will ensure that non-missing person information is defined as information or documents disclosed as permitted by Division 4 or 4A, but not under section 178A

Item 46

Section 183 sets out the requirements that apply to authorisations and notifications. In particular, they must be in writing or in electronic form and comply with any requirements determined by the Communications Access Co-ordinator under subsection 183(2).

This item will amend paragraph 183(1)(a) to include a reference to new Division 4A (which will be inserted by item 41). This will ensure that the requirements in the section will also apply to an authorisation under Division 4A, notification of such an authorisation, revocation of an authorisation or notification of the revocation of an authorisation.

Item 47

Section 184 of the TIA Act outlines who is responsible for providing notification to the person from whom the disclosure is sought following an authorisation or revocation under Division 3 or 4 of Part 4-1 of the TIA Act.

This item will insert two new subsections to the end of section 184. New subsection 184(5) will provide that where an authorised officer makes an authorisation under new subsection 180A(2) or 180B(2), or extends the period for which an authorisation is in force under subsection 180B(6), a relevant staff member of the AFP must notify the person from whom the disclosure of information or documents is sought.

Similarly, new subsection 184(6) will require, following a revocation under subsection 180B(4), a relevant staff member of the AFP to notify the person from whom the disclosure of information or documents was originally sought of the revocation.

Items 48 and 49

Section 185 of the TIA Act requires the head of an enforcement agency to retain each authorisation made by an authorised officer of that enforcement agency under Division 4 of Part 4-1 for three years from the day the authorisation is made.

Items 48 and 49 will add a second subsection to section 185. Item 48 will insert '(1)' before the commencement of the current section so that will become the first subsection of section 185.

Item 49 will insert a new subsection (2). The new subsection will provide that the Commissioner of the AFP must retain each authorisation made under new Division 4A of Part 4-1, which will be inserted by item 41, for three years from the day on which the authorisation was made.

Item 50

Subsection 186(1) of the TIA Act requires enforcement agencies to report to the Minister once a year on their use of the powers under Part 4-1 of Chapter 4 of the TIA Act relating to telecommunications data. This includes reporting on the number of authorisations made under sections 178, 179 and 180 in that year as well as any other matter requested by the Minister in relation to those authorisations.

This item will insert a new paragraph into subsection 186(1). The new paragraph will require the AFP to include in their report to the Minister the number of authorisations made under new sections 180A, 180B, 180C and 180D (which will be inserted by item 41 in that year.

Item 51 – application of amendments made by this part – authorisations

This item will set out the application of the amendments made by this Part on authorisations. It will ensure that the amendments apply only in relation to an authorisation made on or after the commencement of this item. However, this item will also note that an authorisation made under new section 180C will be able to disclose information originally disclosed under a Division 4 authorisation prior to the commencement of this item.

Item 52 – application of amendments made by this part – requests by foreign countries

This item will set out the application of the amendments made by this Part on requests by foreign countries. It will ensure that the amendments made by this Part apply to any requests that are under consideration on or after the commencement of this item, regardless of whether the request was made before or after that commencement.

Item 53 – savings of existing authorisations

This item will ensure that any authorisation by the head of an enforcement agency under subsection 5AB(1) will continue to operate despite the amendments made by this Part to that subsection.

Division 4 – Recovery of costs by carriage service provides etc. for providing assistance to Australian law enforcement authorities

Items 54 and 55

Section 313 of the Telecommunications Act sets out various obligations of C/CSPs in connection with the operation of telecommunications networks or facilities or the supply of carriage services. In particular, subsections 313(3) and (4) require C/CSPs to provide officers and authorities of the Commonwealth and States and Territories such help as is reasonably necessary for:

- enforcing the criminal law and laws imposing pecuniary penalties
- protecting the public revenue, and
- safeguarding national security.

Section 314 sets out the terms and conditions on which help is to be provided as required under subsection 313(3) or (4). In particular, subsection 314(2) states that providing help is on a no profit, no cost basis.

Items 54 and 55 will insert new paragraphs into subsections 313(3) and (4). The new paragraphs will require C/CSPs to also provide assistance to officers and authorities of the Commonwealth and the States and Territories for the purpose of assisting the enforcement of the criminal laws in force in a foreign country.

These new paragraphs will ensure that carriers are required to provide assistance where requested to do so by law enforcement agencies under the new provisions inserted by item 41 in relation to providing telecommunications data to a foreign country for the purposes of enforcing the criminal law of the foreign country. Further, due to the operation of subsection 314(2), this assistance will be able to be provided on a no profit, no loss basis.

Item 114

This item will ensure that the amendments made by items 54 and 55 only apply in relation to help provided by C/CSPs or carriage service intermediaries on or after the commencement of this item.

Schedule 3 – Criminal Code Amendments

Criminal Code Act 1995

The amendments in this Schedule will ensure the computer offences in Part 10.7 of the *Criminal Code Act 1995* (Cth) are consistent with the obligations contained in Articles 2, 4 and 5 of the Council of Europe Convention on Cybercrime. These articles require parties to adopt legislative and other measures to establish as criminal offences:

- access to a computer system without right (Article 2)
- interference with data without right (Article 4), and
- interference with the functioning of a computer system without right (Article 5).

The offences in Part 10.7, which are based on model laws developed by the Model Criminal Code Officers Committee in 2001, cover acts relating to illegal access, modification and impairment of computer data.

In their current form, the computer offences in the Criminal Code are restricted to conduct involving Commonwealth computers, Commonwealth data or the use of a carriage service. These limitations are not consistent with the obligations in the Convention. Although State and Territory offences provide some coverage for conduct which is excluded from the Commonwealth offences, some gaps remain. To ensure that Australia can meet the obligations under the Convention, this Schedule will remove the current restrictions on the computer offences in Part 10.7.

Ensuring that Commonwealth laws meet the obligations under Articles 2, 4 and 5 of the Convention, without reliance on State and Territory laws, will also ensure that the jurisdictional obligations in Article 22 of the Convention are fulfilled in respect of those offences. Article 22 of the Convention requires that parties adopt legislative or other measures to establish jurisdiction over the offences in Articles 2 to 11 of the Convention, when the offence is committed:

- in its territory
- on board a ship flying the flag of that party
- on board an aircraft registered under the laws of that party, or
- by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

State and Territory laws do not meet the jurisdictional obligations in Article 22 of the Convention.

Section 476.3 of the Criminal Code extends the jurisdiction of Part 10.7 to conduct which occurs wholly or partly in Australia, on board an Australian aircraft or Australian ship, and to the conduct of Australian nationals abroad in certain circumstances, thereby meeting the obligations in Article 22 of the Convention.

Item 1 – Subsection 476.1(1)

This item will repeal the definition of Commonwealth computer in subsection 476.1(1). As a result of the amendments in this Schedule, there will no longer be any reference to Commonwealth computers in Part 10.7 of the Criminal Code. The definition is therefore no longer required.

Items 2 and 3 – Subsections 477.1(1) and (2)

Subsection 477.1(1) provides that it is an offence to cause unauthorised access to data held within a computer, unauthorised modification of data held in a computer, or unauthorised impairment of electronic communication to or from a computer with intent to commit a serious offence (defined in section 477.1(9) to mean an offence that is punishable by imprisonment for life or a period of five or more years). However, paragraph 477.1(1)(b) currently limits the offence to situations where the unauthorised access, modification or impairment is caused by means of a carriage service. Subsection 477.1(2) applies absolute liability to paragraph 477.1(1)(b).

Item 2 will repeal paragraph 477.1(1)(b) to remove the existing requirement for a carriage service to have been used in the commission of the offence.

Item 3 will repeal subsection 477.1(2). Following the repeal of paragraph 477.1(1)(b) by item 2 of this Schedule, subsection 477.1(2) will be obsolete.

These amendments will ensure section 477.1 meets the obligations in Articles 2, 4 and 5 of the Convention relating to illegal access, data interference and system interference respectively, which are not limited to the interference caused by means of a carriage service.

Following the commencement of this Schedule, section 477.1 will capture a broader range of illegal conduct, such as the unauthorised access to data by means of a local network with an intent to commit a serious offence.

Item 4 – Subsections 477.1(4) and (5)

Subsection 477.1(4) provides that it is an offence to cause unauthorised access to data held within a computer, unauthorised modification of data held in a computer, or unauthorised impairment of electronic communication to or from a computer with intent to commit a serious Commonwealth offence. Subsection 477.1(5) provides that in a prosecution for an offence under subsection (3) (this is an error as the reference should be to subsection (4)), it is not necessary to prove that the defendant knew that the offence was an offence against a law of the Commonwealth or a serious offence.

Subsection 477.1(4) was necessary to capture situations where a carriage service was not used, but a person intended to, without authorisation, access, modify or impair data held in a computer with an intention to commit a serious Commonwealth offence.

This item will repeal subsections 477.1(4) and 477.1(5). These provisions concerning Commonwealth computers are no longer required as subsection 477.1(1), as amended in item 2, will now capture any unauthorised access, modification or impairment of data held in any computer with intent to commit a serious offence.

Items 5, 6 and 7 – Section 477.2

Subsection 477.2(1) provides that it is an offence to cause unauthorised modification of data held in a computer in order to impair access to that or any other data or to impair the reliability, security or operation of any such data. However, paragraph 477.2(1)(d) currently limits the offence to situations involving or affecting a carriage service, a Commonwealth computer or data held on behalf of the Commonwealth in a computer. Subsection 477.2(2) applies absolute liability to paragraph 477.2(1)(d).

Item 5 will omit the 'and' from subparagraph 477.2(1)(c)(ii) as it refers to paragraph 477.2(1)(d), which will be repealed by Item 6.

Item 6 will repeal paragraph 477.2(1)(d) to remove the existing requirement for a carriage service to have been used, a Commonwealth computer to have been involved or affected, or data held on behalf of the Commonwealth in a computer to have been affected, in the commission of the offence.

Item 7 will repeal subsection 477.2(2). Following the repeal of paragraph 477.2(1)(d) by item 6 of this Schedule, subsection 477.2(2) will be obsolete.

These amendments will ensure that section 477.2 meets the obligations in Articles 4 and 5 of the Convention relating to data interference and system interference respectively, which are not limited to interference involving or affecting a carriage service, computers owned by particular persons or entities, or data held on behalf of particular persons or entities.

Following the commencement of this Schedule, section 477.2 will capture a broader range of illegal conduct, such as the unauthorised modification of data by means of a local network with an intent to impair the operation of the data.

Items 8, 9 and 10 – Section 477.3

Subsection 477.3(1) provides that it is an offence to cause unauthorised impairment of electronic communication to or from a computer (such as an email). However, paragraph 477.3(1)(c) currently limits the offence to electronic communications which are either sent over a carriage service or sent to or from a Commonwealth computer. Subsection 477.3(2) applies absolute liability to paragraph 477.3(1)(c).

Item 8 will omit the 'and' from paragraph 477.3(1)(b) as it refers to paragraph 477.3(1)(c), which will be repealed by Item 9.

Item 9 will repeal paragraph 477.3(1)(c) to remove the existing requirement for electronic communications to have been either sent over a carriage service or sent to or from a Commonwealth computer in the commission of the offence.

Item 10 will repeal subsection 477.3(2). Following the repeal of paragraph 477.3(1)(c) by item 9 of this Schedule, subsection 477.3(2) will be obsolete.

These amendments will ensure that section 477.3 meets the obligations in Articles 4 and 5 of the Convention relating to data interference and system interference respectively, which apply to interference with any electronic communication, not just those sent over a carriage service or to or from computers owned by particular persons or entities.

Following the commencement of this Schedule, section 477.3 will capture a broader range of illegal conduct, such as the impairment of electronic communication sent over a local network or between computers that do not belong to the Commonwealth.

Items 11, 12 and 13 – Section 478.1

Subsection 478.1(1) provides that it is an offence to cause unauthorised access to, or modification of, restricted data. However, paragraph 478.1(1)(d) currently limits the offence to situations where the restricted data is held in a Commonwealth computer or held on behalf of the Commonwealth, or where the access to or modification of the restricted data is caused by means of a carriage service. Subsection 478.1(2) applies absolute liability to paragraph 478.1(1)(d).

Item 11 will omit the 'and' from paragraph 478.1(1)(c) as it refers to paragraph 478.1(1)(d), which will be repealed by Item 12.

Item 12 will repeal paragraph 478.1(1)(d) to remove the existing requirement for restricted data to have been held in a Commonwealth computer or held on behalf of the Commonwealth or for a carriage service to have been used in the commission of the offence.

Item 13 will repeal subsection 478.1(2). Following the repeal of paragraph 487.1(1)(c) by item 12 of this Schedule, subsection 478.1(2) will be obsolete.

These amendments will ensure that section 478.1 meets the obligations in Articles 2, 4 and 5 of the Convention relating to illegal access, data interference and system interference respectively, which are not limited to interference or access caused by means of a carriage service, or affecting data held in particular computers or on behalf of particular persons or entities.

Following the commencement of this Schedule, section 478.1 will capture a broader range of illegal conduct, such as causing unauthorised modification of restricted data by means of a local network.

Items 14, 15, 16 and 17 – Section 478.2

Subsection 478.2(1) provides that it is an offence to cause unauthorised impairment of the reliability, security or operation of data held on a computer disk, credit card or another electronic storage device. However, paragraph 478.2(1)(d) currently limits this offence to situations where the device whose data is impaired is owned or leased by a Commonwealth entity. Subsection 478.2(2) applies absolute liability to paragraph 478.2(1)(d).

Item 14 will omit the '(1)' from subsection 478.2. Following the repeal of subsection 478.2(2) by item 17, this reference will no longer be required.

Item 15 will omit the 'and' from paragraph 478.2(1)(c) as it refers to paragraph 478.2(1)(d), which will be repealed by item 16 of this Schedule.

Item 16 will repeal paragraph 478.2(1)(d) to remove the existing requirement for the device that holds the data impaired in the commission of the offence to have been owned or leased by a Commonwealth entity.

Item 17 will repeal subsection 478.2(2). Following the repeal of subsection 478.2(1)(d) by item 16 of this Schedule, subsection 478.2(2) will be obsolete.

These amendments will ensure section 478.2 meets the obligations in Article 4 of the Convention relating to data interference, which applies to data on any device.

Following the commencement of this Schedule, section 478.2 will capture a broader range of illegal conduct, such as causing unauthorised impairment of data on devices which are owned by individuals or private entities.

Item 18

This item is an application provision that makes it clear that the offences in Part 10.7 of the Criminal Code as amended by this Schedule apply only to acts or omissions that take place after the Schedule commences. The current offences will continue to apply to acts or omissions that take place prior to the commencement of this Schedule.

Schedule 4 – Telecommunications data confidentiality

Telecommunications (Interception and Access) Act 1979

Schedule 4 amends the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to protect the existence of authorisations for the disclosure of information or documents made under Chapter 4, access to telecommunications data, of the TIA Act.

The Council of Europe Convention on Cybercrime places requirements on Parties to adopt legislative and other measures to keep confidential the execution of powers provided for by the Convention, as well as the information obtained from the use of those powers, for example clause 20(3).

The TIA Act currently contains prohibitions on the use and disclosure of information obtained via telecommunications interception or access to stored communications under Chapters 2 and 3 of the TIA Act respectively. These prohibitions also relate to the use or disclosure of information relating to warrants which authorise such powers.

However, whilst the TIA Act limits what can be done with information obtained under an authorisation under Chapter 4 of the TIA Act, the limitation does not relate to the information contained in the actual instruments authorising the access to that information.

To achieve consistency throughout the legislation and fulfil Convention obligations, the below clauses will create offences for the use and disclosure of information about:

- whether an authorisation has been, or is being, sought
- the making of such an authorisation
- the existence or non-existence of such an authorisation
- the revocation of such an authorisation, or
- the notification of such a revocation.

In addition to facilitating accession to the Convention, these provisions will increase the operational security provided by the TIA Act. Given that the use of authorisations is one of the main methods of identifying relevant services related to telecommunications interception and stored communications warrants, it is important to ensure that protections are in place across the life of an operation.

The changes will also provide mechanisms to address misuse of authorisation information by employees of enforcement agencies, as well as carriers.

The offences will not relate to authorisations made under section 178A, as introduced by the *Telecommunications Interception and Intelligence Services Amendment Act 2011* relating to locating a person subject to a missing person report. These authorisations relate to the protection of public safety and so it is not necessary to protect operational actions in the same way. Information obtained from a section 178A authorisation is subject to specific protections set out in new subsection 182(2A), created by the same Act.

Telecommunications (Interception and Access) Act 1979

Item 1 – Subsection 171(3)

Section 171 currently provides an outline of Chapter 4 of the TIA Act The current section separates Chapter 4 into three parts:

- circumstances where the prohibition in section 276, 277 and 278 of the *Telecommunications Act 1997*, relating to the **disclosure** of documents, does not apply
- circumstances where the prohibition in section 276, 277 and 278 of the *Telecommunications Act 1997*, relating to the **use** of documents, does not apply, and
- the creation of a general prohibition to use or disclose information obtained by way of Chapter 4.

Item 1 will amend the outline of Chapter 4 of the TIA Act to include that Chapter 4 also includes an offence in relation to other disclosures and uses of information, being those set out in the provisions below.

Item 2 – Division 6 of Part 4-1 (heading)

Item 2 of the Schedule amends the existing heading to Division 6 of Part 4-1 of the TIA Act. The current heading is 'Secondary disclosure/use offence'. Division 6 currently sets out an offence of making a secondary use or disclosure of information obtained by way of an authorisation compliant with either Division 3 or 4 of the TIA Act. Uses and disclosures relevant to why the information was originally disclosed are considered primary, whereas subsequent or unrelated uses and disclosures are secondary disclosures.

As item 3 introduces a general offence in dealing with authorisations, they are dealing with uses and disclosures which are not technically 'secondary'. Therefore, item 2 of this Schedule removes the reference to secondary in the current text of the Act, relying on the general description of offences.

Item 3 – Before section 182

Item 3 inserts new sections 181A and 181B into the TIA Act. These new section create offences relating to the use or disclosure of information that relates to authorisations. Exception are provided to allow information or documents about communications (but not the content or substance of the communications) to be disclosed for the purposes related to the performance by the Organisation of its function of obtaining intelligence relating to security, the enforcement of the criminal law, a law imposing a pecuniary penalty or for the protection of the public revenue.

New section 181A relates to authorisations made under Division 3 of Chapter 4 of the TIA Act, which are authorisations made by the Organisation for the disclosure of documents that relate to the performance by the Organisation of its function of obtaining intelligence relating to security.

New subsection 181A(1) creates an offence if a person discloses information which is about:

- whether an authorisation under Division 3 (other than under section 178A) has been, or is being, sought
- the making of such an authorisation
- the existence or non-existence of such an authorisation
- the revocation of such an authorisation, or
- the notification of such a revocation.

New subsection 181A(2) creates an offence if a person discloses a document to a person and the document consists (wholly or partly) of any of the following:

- an authorisation under Division 3
- the revocation of such an authorisation or
- the notification of such a revocation.

New subsection 181A(3) provides exemptions for these offences. It states that the offences do not apply to disclosures when:

- the disclosure is for the purposes of the authorisation, revocation or notification concerned, or
- the disclosure is reasonably necessary:
    - to enable the Organisation to perform its function of obtaining intelligence relating to security.
    - to enforce the criminal law
    - to enforce a law imposing a pecuniary penalty, or
    - to protect the public revenue.

These exemptions are necessary to ensure carriers have the lawful ability to use and disclose information when actioning an authorisation.

The remaining exemptions facilitate the effect of section 182, which enables the Organisation to disclose the contents of information that it receives by way of an authorisation to other agencies if that information is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or for the protection of the public revenue.

New subsections 181A(4) and 181A(5) create offences relating to the use of the same information and documents set out in new subsections 181A(1) and (2).

New subsection 181A(6) creates exemptions to these offences, so that the Organisation can make use of the authorisations that they have made.

Item 3 also inserts new section 181B. New section 181B follows the same structure as section 181A, except that it deals with authorisations made under Division 4 of the TIA Act, which are authorisations made by enforcement agencies for the purposes of:

- enforcing the criminal law
- enforcing a law imposing a pecuniary penalty, or
- protecting the public revenue.

The offences relate to the same activities set out in new section 181A. However, the offences do not relate to authorisations made under section 178A of the TIA Act. Section 178A was introduced in the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* and relate to making authorisations to assist in the location of a person who has been reported missing. These authorisations are based on a public safety, rather than investigation function of police and so therefore their confidentiality is not needed.

The exemptions to these offences mostly mirror those contained in new section 181A. However, to reflect the fact that these authorisations are not made by the Organisation, there is no requirement to provide an exemption for use of authorisations under new subsection 181B(5) made under this Division for the Organisation to perform its function of obtaining intelligence relating to security.

This reflects the current provisions of section 182 of the TIA Act, whereby an agency can disclose the information obtained via an authorisation in connection with the Organisation's function of obtaining intelligence relating to security, but no such use is permitted.

New sections 181A and 181B include notes that the defendant bears an evidential burden in relation to the matters in subsections (3) or (6) – being that any disclosure or use was valid. These notes are consistent with current offences in the TIA Act, including sections 132, 133 and 182.

The evidential burden means the burden of adducing, or pointing to, evidence that suggests a reasonable possibility that the matter – being that a particular instance of use or disclosure was lawful pursuant to section 181A or 181B – exists. If such evidence is pointed to, the prosecution must refute the defence beyond reasonable doubt.

The evidential burden is distinct from the legal burden, which means proving the existence of the matter. In the case of a legal burden defence, the defendant bears the burden of establishing the defence on the balance of probabilities. If the defendant establishes the matter on the balance of probabilities, the prosecution must refute the defence beyond reasonable doubt.

New subsections 181A(3) and (6) and 181B(3) and (6) put a burden on the defendant to indicate which use or disclosure exemption they relied upon when making the use or disclosure. The subsections do not shift the legal burden.

There are two reasons the defendant is required to indicate which provision they made the disclosure pursuant to. First, the fact a defendant believed that a use or disclosure was reasonably necessary for a certain purpose under the TIA Act is a state of belief held by the defendant. Other than by the defendant indicating which state of belief detailed in section 181A or 181B they held, it would be difficult for the prosecution to raise and disprove every possible state of belief. Secondly, the states of belief, in many circumstances, will go to the operational procedures of enforcement agencies.

Narrowing the extent to which the operational procedures of law enforcement agencies, including when and how information or documents are disclosed to the Organisation, are subject to court proceeding helps protect the capability of these agencies.

Item 4 – Application

Item 4 is an application provision. It does not retrospectively criminalise any act. Item 4 sets out that a person commits an offence if they disclose or use information, regardless of when that information came into existence. However, the actual disclosure or use must occur after this provision comes into force.

Schedule 5 – Miscellaneous

Telecommunications (Interception and Access) Act 1979

Schedule 5 amends the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to expand the geographical jurisdiction of offences against subsection 7(1) and section 63 of the TIA Act. These sections relate to unlawful interception and dealing with intercept related information respectively.

The amendment to jurisdiction implements a requirement of the Council of Europe Convention on Cybercrime (the Convention) in Article 22 that offences established under the Convention must cover circumstances where the conduct occurred on board a ship flying the flag of that party, on board an aircraft registered under the laws of that party and by one of the Party's nationals, if the offence is punishable under a criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

Schedule 5 also amends the TIA Act to expand the offences for which authorisations for access to prospective information or documents are available. This amendment implements a requirement in Article 14 of the Convention. Article 14 requires that the range of offences or categories of offences for which real-time access to traffic data is available is not more restrictive than the range of offences or categories of offences for which interception of content data is available.

Item 1 – At the end of section 105

New subsection 105(5) adds a reference to Section15.1 (standard geographical jurisdiction – Category A) of the Criminal Code. The change implements a requirement under Article 22 of the Convention on Cybercrime.

Extended geographical jurisdiction means that a person does not commit the offence unless the relevant conduct occurs wholly or partly in Australia or wholly or partly on board an Australian aircraft or an Australian ship or, if the relevant conduct occurs wholly outside Australia, the person is an Australian citizen or a body corporate incorporated under Australian law.

Item 2 – Application of amendment

Item 2 clarifies that the change to the offences in subsection 7(1) and section 63 or apply after Schedule 5 comes into force. Schedule 5 does not retrospectively criminalise any activity.

Item 3 – Subsection 180(4)

Item 3 amends subsection 180(4) to include ***serious offence*** in addition to 'an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years'. ***Serious offence*** is defined in section 5D of the TIA Act and details the offences for which interception agencies can obtain warrants for the interception of communications.

Inserting a reference to ***serious offence*** into section 180(4) of the TIA Act ensures that real-time access to traffic data is available at least in all circumstances where inception of content data is available. The change guarantees compliance with Article 14 of the Convention.