2019-2020

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

SURVEILLANCE LEGISLATION AMENDMENT (IDENTIFY AND DISRUPT) BILL 2020

EXPLANATORY MEMORANDUM

Circulated by authority of the
Minister for Home Affairs, the Honourable Peter Dutton MP
SURVEILLANCE LEGISLATION AMENDMENT (IDENTIFY AND DISRUPT) BILL

GENERAL OUTLINE

1. The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 will amend the Surveillance Devices Act 2004 (SD Act), the Crimes Act 1914 (Crimes Act) and associated legislation to introduce new law enforcement powers to enhance the ability of the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to combat online serious crime.

2. Cyber-enabled serious and organised crime, often enabled by the dark web and other anonymising technologies, such as bespoke encrypted devices for criminal use, present a direct challenge to community safety and the rule of law. For example, on the dark web criminals carry out their activities with a lower risk of identification and apprehension. Many anonymising technologies and criminal methodologies can be combined for cumulative effect, meaning it is technically difficult, and time and resource intensive, for law enforcement to take effective action. Just as online criminals are constantly changing their operations and reacting to new environments, the law must adapt in order to give law enforcement agencies effective powers of response.

3. Existing electronic surveillance powers, while useful for revealing many aspects of online criminality, are not suitably adapted to identifying and disrupting targets where those targets are actively seeking to obscure their identity and the scope of their activities. Without the critical first step of being able to identify potential offenders, investigations into serious and organised criminality can fall at the first hurdle. Being able to understand the networks that criminals are involved in and how they conduct their crimes is also a crucial step toward prosecution.

4. This Bill addresses gaps in the legislative framework to better enable the AFP and the ACIC to collect intelligence, conduct investigations, disrupt and prosecute the most serious of crimes, including child abuse and exploitation, terrorism, the sale of illicit drugs, human trafficking, identity theft and fraud, assassinations, and the distribution of weapons.

5. The Bill contains the necessary safeguards, including oversight mechanisms and controls on the use of information, to ensure that the AFP and the ACIC use these powers in a targeted and proportionate manner to minimise the potential impact on legitimate users of online platforms.

6. The Bill introduces three new powers for the AFP and the ACIC. They are:

   - Data disruption warrants to enable the AFP and the ACIC to disrupt data by modifying, adding, copying or deleting in order to frustrate the commission of serious offences online
• Network activity warrants to allow agencies to collect intelligence on serious criminal activity being conducted by criminal networks, and

• Account takeover warrants to provide the AFP and the ACIC with the ability to take control of a person’s online account for the purposes of gathering evidence to further a criminal investigation.

Schedule 1: Data disruption warrants

7. Schedule 1 amends the SD Act to introduce data disruption warrants. These warrants will allow the AFP and the ACIC to disrupt criminal activity that is being facilitated or conducted online by using computer access techniques.

8. A data disruption warrant will allow the AFP and the ACIC to add, copy, delete or alter data to allow access to and disruption of relevant data in the course of an investigation for the purposes of frustrating the commission of an offence. This will be a covert power also permitting the concealment of those activities. Whilst this power will not be sought for the purposes of evidence gathering, information collected in the course of executing a data disruption warrant will be available to be used in evidence in a prosecution.

9. The purpose of the data disruption warrant is to offer an alternative action to the AFP and the ACIC, where the usual circumstances of investigation leading to prosecution are not necessarily the option guaranteeing the most effective outcome. For example, removing content or altering access to content (such as child exploitation material), could prevent the continuation of criminal activity by participants, and be the safest and most expedient option where those participants are in unknown locations or acting under anonymous or false identities. Under these circumstances, it may be prudent for the AFP or the ACIC to obtain a data disruption warrant.

10. Applications for data disruption warrants must be made to an eligible Judge or nominated Administrative Appeals Tribunal (AAT) member. A data disruption warrant may be sought by a law enforcement officer of the AFP or the ACIC if that officer suspects on reasonable grounds that:

• one or more relevant offences are being, are about to be, or are likely to be, committed, and

• those offences involve, or are likely to involve, data held in a computer, and

• disruption of data held in the target computer is likely to substantially assist in frustrating the commission of one or more of the relevant offences previously specified that involve, or are likely to involve, data held in the target computer.

11. An eligible Judge or nominated AAT member may issue a data disruption warrant if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant and the disruption of data authorised by the warrant is justifiable and
proportionate, having regard to the offences specified in the application. The issuing authority will consider, amongst other things, the nature and gravity of the conduct targeted and the existence of any alternative means of frustrating the commission of the offences.

12. Information obtained under data disruption warrants will be ‘protected information’ under the SD Act and be subject to strict limits for use and disclosure. Consistent with existing warrants in the SD Act, compliance with the data disruption warrant regime will be overseen by the Commonwealth Ombudsman.

**Schedule 2: Network activity warrants**

13. Network activity warrants will allow the AFP and the ACIC to collect intelligence on criminal networks operating online by permitting access to the devices and networks used to facilitate criminal activity.

14. These warrants will be used to target criminal networks about which very little is known, for example where the AFP or the ACIC know that there is a group of persons using a particular online service or other electronic platform to carry out criminal activity but the details of that activity are unknown. Network activity warrants will allow agencies to target the activities of criminal networks to discover the scope of criminal offending and the identities of the people involved. For example, a group of people accessing a website hosting child exploitation material and making that material available for downloading or streaming, will be able to be targeted under a network activity warrant.

15. Intelligence collection under a network activity warrant will allow the AFP and the ACIC to more easily identify those hiding behind anonymising technologies. This will support more targeted investigative powers being deployed, such as computer access warrants, interception warrants or search warrants.

16. Network activity warrants will allow the AFP and the ACIC to access data in computers used, or likely to be used, by a criminal network over the life of the warrant. This means that data does not have to be stored on the devices, but can be temporarily linked, stored, or transited through them. This will ensure data that is unknown or unknowable at the time the warrant is issued can be discovered, including data held on devices that have disconnected from the network once the criminal activity has been carried out (for example, a person who disconnected from a website after downloading child exploitation material).

17. The AFP and the ACIC will be authorised to add, copy, delete or alter data if necessary to access the relevant data to overcome security features like encryption. Data that is subject to some form of electronic protection may need to be copied and analysed before its relevancy or irrelevancy can be determined.

18. Applications for network activity warrants must be made to an eligible Judge or nominated AAT member. A network activity warrant may be sought by the chief officer of the AFP
or the ACIC (or a delegated Senior Executive Service (SES) member of the agency) if there are reasonable grounds for suspecting that:

- a group of individuals are engaging in or facilitating criminal activity constituting the commission of one or more relevant offences, and

- access to data held in computers will substantially assist in the collection of intelligence about those criminal networks of individuals in respect of a matter that is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

19. There are strict prohibitions on the use of information obtained under a network activity warrant. Information obtained under a network activity warrant is for intelligence only, and will not be permitted to be used in evidence in criminal proceedings, other than for a breach of the secrecy provisions of the SD Act. Network activity warrant information may, however, be the subject of derivative use, allowing it to be cited in an affidavit on application for another investigatory power, such as a computer access warrant or telecommunications interception warrant. This will assist agencies in deploying more sensitive capabilities, with confidence that they would not be admissible in court.

20. The Inspector-General of Intelligence and Security (IGIS) will have oversight responsibility for network activity warrants given their nature as an intelligence collection tool. This approach departs from the traditional model of oversight by the Commonwealth Ombudsman of the use of electronic surveillance powers by the AFP and the ACIC. However, the approach is consistent with the oversight arrangements for intelligence collection powers available to other agencies, including the Australian Security Intelligence Organisation (ASIO) and the Australian Signals Directorate (ASD).

21. The Bill also provides that the IGIS and the Commonwealth Ombudsman will be able to share information where it is relevant to exercising powers, or performing functions or duties, as an IGIS or Ombudsman official. This ensures that where a matter may arise during an inspection that would more appropriately be dealt with by the other oversight body, a framework is in place for the transfer of network activity warrant information, allowing efficient and comprehensive oversight to occur.

**Schedule 3: Account takeover warrants**

22. The Bill inserts account takeover warrants into the Crimes Act. These warrants will enable the AFP and the ACIC to take control of a person’s online account for the purposes of gathering evidence about serious offences.

23. Currently, agencies can only take over a person’s account with the person’s consent. An account takeover power will facilitate covert and forced takeovers to add to their investigative powers.
24. An AFP or ACIC officer may apply to a magistrate for an account takeover warrant to take control of an online account, and prevent the person’s continued access to that account. Before issuing the account takeover warrant, the magistrate will need to be satisfied that there are reasonable grounds for suspicion that an account takeover is necessary for the purpose of enabling evidence to be obtained of a serious Commonwealth offence or a serious State offence that has a federal aspect. In making this determination, the nature and extent of the suspected criminal activity must justify the conduct of the account takeover.

25. This power enables the action of taking control of the person’s account and locking the person out of the account. Any other activities, such as accessing data on the account, gathering evidence, or performing undercover activities such as taking on a false identity, must be performed under a separate warrant or authorisation. Those actions are not authorised by an account takeover warrant. The account takeover warrant is designed to support existing powers, such as computer access and controlled operations, and is not designed to be used in isolation. Strict safeguards will be enforced to ensure account takeover warrants are exercised with consideration for a person’s privacy and the property of third parties. There are strong protections on the use of information collected under the power.

26. The Bill will require the agencies to make six-monthly reports to the Commonwealth Ombudsman and the Minister for Home Affairs on the use of account takeover warrants during that period. There are also annual reports to the Minister for Home Affairs that are required to be tabled in Parliament.

**Schedule 4: Controlled operations**

27. Schedule 4 will introduce minor amendments to Part IAB of the Crimes Act to enhance the AFP and the ACIC’s ability to conduct controlled operations online.

28. In particular, the Bill amends the requirement for illicit goods, including content such as child abuse material, to be under the control of the AFP and the ACIC at the conclusion of an online controlled operation.

29. This is intended to address how easy data is to copy and disseminate, and the limited guarantee that all illegal content will be able to be under the control of the AFP and the ACIC at the conclusion of an online controlled operation.

30. This amendment will not change the overall intent of the controlled operations, which is to allow for evidence collection.

**Schedule 5: Minor corrections**

ABBREVIATIONS used in the Explanatory Memorandum

AAT  Administrative Appeals Tribunal
AIC  Australian Intelligence Community (comprising ASIO, ASIS, ASD, AGO, DIO and ONI)
ACIC  Australian Criminal Intelligence Commission (established as the Australian Crime Commission in the ACC Act)
ACC Act  *Australian Crime Commission Act 2002*
ACLEI  Australian Commission for Law Enforcement Integrity
AFP  Australian Federal Police
AFP Act  *Australian Federal Police Act 1979*
AGO  Australian Geospatial-Intelligence Organisation
AHRC  Australian Human Rights Commission
AHRC Act  *Australian Human Rights Commission Act 1986*
ASD  Australian Signals Directorate
ASIO  Australian Security Intelligence Organisation
ASIO Act  *Australian Security Intelligence Organisation Act 1979*
ASIS  Australian Secret Intelligence Service
CEO  Chief Executive Officer
Crimes Act  *Crimes Act 1914*
Criminal Code  Schedule 1, *Criminal Code Act 1995*
DIO  Defence Intelligence Organisation
IGADF  Inspector-General of the Australian Defence Force
IGIS  Office of the Inspector-General of Intelligence and Security
IGIS Act  *Inspector-General of Intelligence and Security Act 1986*
IC Act  *Australian Information Commissioner Act 2010*
Inspector-General  The individual holding the statutory position of Inspector-General of Intelligence and Security, under section 6 of the IGIS Act
<table>
<thead>
<tr>
<th>Integrity bodies</th>
<th>The Ombudsman, the Australian Human Rights Commission, the Information Commissioner, the Integrity Commissioner, and the Inspector-General of the Australian Defence Force</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS Act</td>
<td><em>Intelligence Services Act 2001</em></td>
</tr>
<tr>
<td>LEIC Act</td>
<td><em>Law Enforcement Integrity Commissioner Act 2006</em></td>
</tr>
<tr>
<td>NIC</td>
<td>National Intelligence Community (comprising ASIO, ASIS, ASD, AGO, DIO, ONI, the ACIC, and the intelligence functions of the AFP, AUS TRAC and the Department of Home Affairs)</td>
</tr>
<tr>
<td>Ombudsman</td>
<td>Commonwealth Ombudsman</td>
</tr>
<tr>
<td>Ombudsman Act</td>
<td><em>Ombudsman Act 1976</em></td>
</tr>
<tr>
<td>ONI</td>
<td>Office of National Intelligence</td>
</tr>
<tr>
<td>PJCIS</td>
<td>Parliamentary Joint Committee on Intelligence and Security</td>
</tr>
<tr>
<td>PID</td>
<td>Public interest disclosure</td>
</tr>
<tr>
<td>PID Act</td>
<td><em>Public Interest Disclosure Act 2013</em></td>
</tr>
<tr>
<td>Privacy Act</td>
<td><em>Privacy Act 1988</em></td>
</tr>
<tr>
<td>SD Act</td>
<td><em>Surveillance Devices Act 2004</em></td>
</tr>
<tr>
<td>TIA Act</td>
<td><em>Telecommunications (Interception and Access) Act 1979</em></td>
</tr>
<tr>
<td>TOLA</td>
<td><em>Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018</em></td>
</tr>
</tbody>
</table>

**FINANCIAL IMPACT**

32. Nil, as all financial impacts for the 2020-2021 financial year will be met from existing appropriations. Any ongoing costs will be considered in future budgets.
STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

1. This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the Human Rights (Parliamentary Scrutiny) Act 2011.

Overview of the Bill

2. The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 will amend the Surveillance Devices Act 2004 (SD Act), the Crimes Act 1914 (Crimes Act) and associated legislation to introduce new law enforcement powers and warrants to enhance the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC)’s ability to combat cyber-enabled serious and organised crime, including online child exploitation.

3. The Bill introduces:

   - a data disruption warrant which enables the AFP and the ACIC to access data on one or more computers and perform disruption activities for the purpose of frustrating the commission of criminal activity
   - a network activity warrant to enable the AFP and the ACIC to collect intelligence on criminal networks operating online
   - an account takeover warrant to allow the AFP and the ACIC to takeover a person’s online account the purposes of gathering evidence of criminal activity, and
   - minor amendments to the controlled operations regime, to ensure controlled operations can be conducted effectively in the online environment.

Schedule 1 – Data disruption

Application for a data disruption warrant

4. Data disruption warrants will be issued by an eligible Judge or nominated AAT member acting in his or her personal capacity (persona designata). This is consistent with the existing framework for surveillance device warrants and computer access warrants under the SD Act. AAT members, while not judicial officers, are independent decision makers afforded similar protections to that afforded to judges. Termination of the appointment of an AAT member is only possible if determined by the Governor-General.
Threshold for application for a data disruption warrant

5. The AFP and the ACIC will be able to apply for a data disruption warrant where there is a reasonable suspicion that relevant offences of a particular kind have been, are being, are about to be, or are likely to be, committed, and those offences involve, or are likely to involve, data held in a computer, and the disruption of data held in that computer is likely to substantially assist in frustrating the commission of those offences. Relevant offences are generally those that carry a maximum penalty of imprisonment for at least three years.

Permitted actions under a data disruption warrant

6. The AFP and the ACIC will be permitted to covertly access computers to disrupt data and while doing so, if necessary, add, copy, delete or alter that data in order to frustrate the commission of relevant offences.

Dealing in information about data disruption warrants

7. Information collected under a data disruption warrant is treated as ‘protected information’ under the SD Act, meaning that the Bill prohibits dealing in information collected under a data disruption warrant except in very limited circumstances such as for the purposes of the investigation of a relevant offence, the making of a decision about whether or not to bring a prosecution, or the prevention of serious harm.

Security and destruction of records relating to data disruption warrants

8. The chief officer of the AFP or the ACIC must ensure that information obtained under a data disruption warrant is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. The chief officer must also destroy records or reports as soon as practicable if no civil or criminal proceedings has been, or is likely to be, commenced and the material is not likely to be required in connection with section 45(5A) or (5B), and within 5 years if they are no longer required under the SD Act.

Schedule 2 – Network activity warrants

Application for network activity warrants

9. Network activity warrants will be issued by an eligible Judge or nominated AAT member acting in his or her personal capacity (persona designata). This is consistent with the existing framework for surveillance device warrants and computer access warrants under the SD Act. AAT members, while not judicial officers, are independent decision makers afforded similar protections to that afforded to judges. Termination of the appointment of an AAT member is only possible if determined by the Governor-General.

Threshold for application for a network activity warrant

10. The chief officer of the AFP and the ACIC will be able to apply for a network activity warrant if there is a reasonable suspicion that:
• one or more networks of individuals are participating in, or facilitating or assisting, criminal activity which involves, or is likely to involve, the commission of one or more relevant offences, and

• access to data held in computers will substantially assist in the collection of intelligence about those networks of individuals in respect of a matter that is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

Permitted actions under a network activity warrant

11. Network activity warrants will permit accessing data held in a computer that is used by a criminal network of individuals in order to collect intelligence related to that group, as well as actions necessary to conceal the access.

Dealing in information about network activity warrants

12. The Bill prohibits dealing in information collected under a network activity warrant except in very limited circumstances. Information can only be used for intelligence purposes, and cannot be used in evidence in a criminal proceeding.

Security and destruction of records relating to network activity warrants

13. The chief officer of the AFP or the ACIC must ensure that information obtained under a network activity warrant is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. The chief officer must also destroy records or reports as soon as practicable if no civil or criminal proceeding has been or is likely to be commenced and the material is not likely to be required in connection with section 45(5A) or (5B), and within 5 years if the material is no longer required to be kept under the SD Act.

Schedule 3 – Account takeover warrants

Application for an account takeover warrant

14. Account takeover warrants will be issued under the Crimes Act by a magistrate, to a law enforcement officer of the AFP or the ACIC. Magistrates currently issue section 3E warrants (search warrants), and this issuing authority has been replicated for consistency with other law enforcement powers in the Crimes Act, due to the fact that account takeover warrants will often be applied for at the same time as other warrants in the Crimes Act.

Threshold for application for an account takeover warrant

15. A law enforcement officer may apply for an account takeover warrant on the reasonable suspicion that:
• one or more relevant offences have been, are being, are about to be, or are likely to be committed

• an investigation into those offences is being, will be or is likely to be conducted, and

• taking control of an online account is necessary in the course of that investigation for the purposes of enabling evidence to be obtained.

**Permitted actions under an account takeover warrant**

16. Account takeover warrants permit the taking control of an account through the modification of data. Taking control of an account means taking steps that result in the person having exclusive access to the account.

**Dealing in information about account takeover warrants**

17. Dealing in information about account takeover warrants is prohibited, and is an offence, except in certain limited circumstances, such as using the information for the purposes of the investigation, in connection with the AFP or the ACIC’s functions, and preventing serious harm.

**Security and destruction of records relating to account takeover warrants**

18. The chief officer of the AFP or the ACIC must ensure that information obtained under an account takeover warrant is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. The chief officer must also destroy records or reports as soon as practicable if no civil or criminal proceeding has been or is likely to be commenced and the material is not likely to be required, and within 5 years.

**Human rights implications**

19. The Bill engages the following human rights under the International Covenant on Civil and Political Rights (ICCPR):

• protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR

• protection of the right to freedom of expression contained in Article 19 of the ICCPR

• the right to life contained in Article 6 of the ICCPR

• the right to effective remedy contained in Article 2(3) of the ICCPR, and

• the right to a fair hearing in Article 14(1) of the ICCPR.
Protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR

20. The Bill engages the protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR. Article 17 provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation, and that everyone has the right to the protection of the law against such interference or attacks.

21. The protection against arbitrary or unlawful interference with privacy under Article 17 can be permissibly limited where the limitations are lawful and not arbitrary. The term ‘unlawful’ in Article 17 of the ICCPR means that no interference can take place except as authorised under domestic law. The term ‘arbitrary’ in Article 17(1) of the ICCPR means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted reasonableness to mean that any limitation must be proportionate and necessary in the circumstances to achieve a legitimate objective.

22. The purpose of the Bill is to protect national security, ensure public safety, and to address online crime and particularly the challenges posed by the dark web and anonymising technologies. The Bill aims to protect the rights and freedoms of individuals by providing law enforcement agencies with the tools they need to keep the Australian community safe.

23. To that end, the Bill does place limitations on the right to privacy. Those limitations however, are not arbitrary or unlawful. They are carefully framed and considered in order to ensure public safety and a balanced approach to the intrusion on private individuals’ data with the maximum safeguards.

Mandatory considerations of issuing authorities upon issuing warrants

24. There are mandatory considerations to which the issuing authority must have regard. In determining whether to issue an account takeover warrant, the issuing authority must have regard to the extent to which the privacy of any person is likely to be affected. In determining whether to issue a network activity warrant or a data disruption warrant, the issuing authority must consider whether the warrants are proportionate, having regard to the offences that those warrants are targeting. When considering whether the actions are justified and proportionate, the issuing authority will take into account, for example, the scope of the warrant in terms of who and how many people are affected, the exact nature of the potential intrusion on people’s private information, and whether that intrusion is justified by the serious nature of the criminality that is being targeted. Both these warrants, as well as account takeover warrants, can only be applied for on the basis of a link to serious offending. They target activity of the most serious nature, including terrorism, child exploitation, drug trafficking and firearms trafficking.

25. Central amongst other considerations that issuing authorities must take into account is consideration of the existence of any alternative means of realising the intention of the warrant. In the case of a data disruption warrant, the issuing authority must consider...
alternative means of frustrating the criminal activity. In the case of network activity warrants and account takeover warrants the issuing authority must consider the existence of any alternative or less intrusive means of obtaining the information sought. These provisions are particularly important for ensuring that avenues of investigation, information collection and disruption that are less intrusive on individual privacy are considered. Where there are narrower activities that involve a more targeted approach, for example, this should be taken into account by the issuing authority.

**Limited interference with data and property**

26. There are certain actions that are specifically prohibited on the face of the legislation for each of the three warrants. These provide further protections against unlawful and arbitrary interference with privacy. These warrants do not authorise the doing of any thing that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by another person of a computer, unless doing those things is necessary for carrying out the purpose of the warrant. These warrants also explicitly prohibit the doing of any thing that is likely to cause any other material loss or damage to other persons lawfully using a computer unless that loss or damage is justified and proportionate having regard to the offences covered by the warrant. These are also statutory conditions stating that neither a data disruption warrant nor an account takeover warrant can result in loss or damage to data unless justified and proportionate.

27. These are strong safeguards to ensure that activities carried out under these warrants are justified and proportionate for the purposes of the warrant and are not exercised or issued arbitrarily.

**Protections on information collected under warrants**

28. Information collected under these warrants will have strict protections placed on it. Data disruption warrant information will have the same strong protections as placed on information collected under existing warrants in the SD Act, such as computer access warrants. Data disruption warrant information is ‘protected information’ under the SD Act. Similarly, the Bill inserts a definition of ‘protected information’ into the Crimes Act in respect of account takeover warrants, in order that the information gathered by virtue of conducting an account takeover is governed by the same prohibitions and exceptions as most information under the SD Act, including data disruption warrant information.

29. A person commits an offence if the person uses, records, communicates or publishes protected information except in very limited circumstances. Those circumstances include allowing the use, recording, communication and publication of information, or admittance in evidence where necessary for the investigation of a relevant offence, a relevant proceeding, or the making of a decision as to whether or not to bring a prosecution for a relevant offence.

30. Protected information can only be used, recorded, communicated or published in similarly limited circumstances, such as where that information has been disclosed in proceedings in open court, or where it is necessary to help prevent or reduce the risk of serious violence or damage to property. Information can also be shared with the Australian Security
Intelligence Organisation (ASIO) or any agency within the meaning the *Intelligence Services Act 2001*, if the information relates to the functions of those agencies. Protected information can be shared with a foreign country, the International Criminal Court or a War Crimes Tribunal if relevant to an international assistance authorisation. There are similar allowances for information to be shared under the *Mutual Assistance in Criminal Matters Act 1987* and the *International Criminal Court Act 2002*.

31. The Bill has a different approach to information collected under a network activity warrant. That information is for intelligence purposes, and cannot be used in evidence in a criminal proceeding. There are very limited exceptions to this prohibition, and those exceptions have been made in order either to further investigations into criminal conduct made under other warrants (which will themselves contain protections on information gathered) or to promote the right to a fair trial and facilitate adequate oversight mechanisms. Protected network activity warrant information can be admitted into evidence for, for example, the purpose of making an application for a warrant, for the purpose of an IGIS official exercising powers or performing duties, or for the purposes of an investigation into whether the prohibition on dealing with information has been breached.

*Security and destruction of records*

32. Each of the three warrant frameworks in the Bill contain measures governing security requirements and record keeping for the information gathered. The chief officer of the AFP or the ACIC must ensure that information obtained under these warrants is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. The chief officer must also destroy records or reports as soon as practicable if no civil or criminal proceedings has been or is likely to be commenced and the material is not likely to be required, and within 5 years.

33. Requiring the security and destruction of records ensures that private data of individuals subject to a data disruption warrant is not handled by those without a legitimate need for access, and are not kept in perpetuity where there is not a legitimate reason for doing so.
Summary

34. The provisions that engage Article 17 of the ICCPR do so in a balanced and carefully considered way so as to protect individual privacy whilst enhancing the AFP and the ACIC’s capacity to respond to serious online criminal activity. While the Bill does limit the right to privacy, those limitations are not arbitrary or unlawful. They are accompanied by a range of safeguards, stringent thresholds, proportionality tests, and clear specifications regarding the actions permitted under each warrant. At the same time, the Bill balances privacy with public safety and security. To the extent that there is a limitation on the protection against interference with privacy, statutory safeguards ensure any limitation is reasonable, necessary and proportionate.

Protection of the right to freedom of expression contained in Article 19 of the ICCPR

35. Article 19(2) of the ICCPR provides that everyone shall have the right to freedom of expression, including the right ‘to seek, receive and impart information and ideas of all kinds and regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice’.

36. Furthermore, Article 19(3) of the ICCPR provides that the exercise of the rights provided for in Article 19(2) carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary for the protection of national security or public order, or of public health or morals.

37. As the Bill contains measures which are aimed at combatting the use of the dark web and anonymising technologies, as well as any obfuscating of identities and illegal activities online, the Bill may indirectly have the effect of discouraging the use of such technologies for legitimate purposes. It is plausible that a person concerned about access to private data by government agencies may minimise his or her use of anonymising technologies or other online services.

38. However, this Bill will not permit the AFP or the ACIC to access an individual’s data or device unless under warrant. The measures in this Bill advance a legitimate objective of protecting Australia’s national security and public order by allowing the AFP and the ACIC to respond to the modern communications and cyber environment, and effectively access data to disrupt serious criminal activity and collect intelligence which will inform investigations which may ultimately lead to prosecutions.

39. To the extent that a person refrains from or minimises their legitimate use of anonymising technologies or online services in response to these powers, the additional restrictions on the purposes that the powers may be issued for and the limited things that may be required under these powers complement the protections of a warrant or authorisation and ensure any limitation on the freedom of expression is necessary, reasonable, and proportionate. Any limitation on the right to freedom of expression is consistent with the ICCPR as Article 19(3) allows for limitations for the protection of national security or of public order.
The right to life contained in Article 6 of the ICCPR

40. The right to life in Article 6 of the ICCPR places a positive obligation on states to protect individuals from unwarranted actions by private persons. The obligation to protect life requires the state to take preventative operational measures to protect individuals whose safety may be compromised in particular circumstances, such as by a terrorist act. This includes enhancing the capabilities of law enforcement agencies to respond to a heightened terrorist threat.

41. The Bill promotes the right to life by providing additional tools to manage the risk posed by cyber-enabled serious and organised crime. The Bill is intended to target serious and organised offenders who utilise anonymising technologies to facilitate online criminal activity, including terrorism, child exploitation, and drugs and firearms trafficking.

42. The Bill enhances the capabilities of the AFP and the ACIC to respond to a heightened online threat environment. The Bill extends the ability for the AFP and the ACIC to detect, monitor, identify and disrupt serious online criminal activity.

The right to effective remedy contained in Article 2(3) of the ICCPR

43. Article 2(3) of the ICCPR protects the right to an effective remedy for any violation of rights and freedoms recognised by the ICCPR, including the right to have such a remedy determined by competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the State.

44. The Bill does not provide for merits review of decision making and excludes judicial review under the Administrative Decisions (Judicial Review) Act 1977 (ADJR Act). This approach to review is consistent with similar decisions made for national security and law enforcement purposes, for example those made under the TIA Act. Decisions of a law enforcement nature have been identified by the Administrative Review Council as being unsuitable for merits review.

45. Australian courts will retain jurisdiction for judicial review of a decision of a Judge or nominated AAT member to issue a warrant, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of subsection 39B(1) of the Judiciary Act 1903. This will ensure that an affected person or a provider has an avenue to challenge unlawful decision making.

46. Consistent with other powers in the Crimes Act and the SD Act, the Commonwealth Ombudsman will have oversight of the use of account takeover warrants and data disruption warrants by the ACIC and the AFP.

47. The Bill provides for IGIS oversight of the AFP’s and the ACIC’s activities in relation to network activity warrants. These amendments will enable the Inspector-General to review the activities of the AFP and the ACIC in relation to network activity warrants for legality, propriety and consistency with human rights. The Inspector-General may carry out his or her oversight functions through a combination of inspections, inquiries and investigations into complaints.
The right to a fair trial in Article 14(1) of the ICCPR

48. Article 14(1) of the ICCPR provides that all individuals are equal before a court or tribunal and that all individuals are entitled to a fair and public hearing that allows for a reasonable opportunity for individuals to present their case before a fair, impartial, and competent court.

49. New subsection 47A(7) and section 47B introduced in to the SD Act by the Bill provide that in a proceeding (including a proceeding before a court, tribunal or Royal Commission), a person may object to the disclosure of information on the ground that the information, if disclosed, could reasonably be expected to reveal details of data disruption technologies or methods; and the person conducting or presiding over the proceeding may order that the information is not disclosed in the proceeding. These new subsections engage the right to a fair trial in Article 14(1) of the ICCPR.

50. The impact that new subsection 47A(7) and section 47B of the SD Act has on an individual’s right to a fair trial is mitigated through the requirement that the person conducting or presiding over the proceeding must take into account whether disclosure of the information is necessary for the fair trial of the defendant or is in the public interest (subsection 47B(3)). Therefore the protections on data disruption technologies or methods being disclosed in hearings are reasonable, necessary and proportionate for protecting national security and safeguarding operational capabilities and sensitivities.

Conclusion

51. This Bill is compatible with human rights and promotes a number of human rights. To the extent that the Bill limits a human right, those limitations are reasonable, necessary and proportionate.
NOTES ON CLAUSES

Preliminary

Item 1 – Short title

1. This item provides for the short title of the Act to be the Surveillance Legislation Amendment (Identify and Disrupt) Act 2020.

Item 2 – Commencement

2. This item provides for the commencement of each provision in the Act, as set out in the table. Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table.

3. Sections 1 to 3 and anything in this Act not elsewhere covered by the table is to commence on the day this Act receives the Royal Assent.

4. Schedule 1 is to commence the day after this Act receives the Royal Assent.

5. Schedule 2 is to commence immediately after the commencement of Schedule 1. This is necessary as certain provisions within Schedule 2 amend provisions within Schedule 1.

6. Schedules 3, 4 and 5 are to commence on the day after this Act receives Royal Assent.

7. The note at the end of the table clarifies that this table only relates to the provisions of this Act as enacted. This table will not be amended to deal with any later amendments of this Act.

8. Information may be inserted or edited in column 3 of the table in any published version of the Act. However, this information will not be part of this Act.

Item 3 – Schedules

9. This item provides that legislation that is specified in a Schedule to this Act 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 – Data disruption

Surveillance Devices Act 2004

Item 1 – Title

10. This item amends the long form title of the Act to ‘An Act to set out the powers of Commonwealth law enforcement agencies with respect to surveillance devices and access to, and disruption of, data held in computers, and for related purposes.’ This reflects the new power in the Act for the AFP and the ACIC to disrupt data held in computers.
11. This item does not alter the short title by which it may be cited.

**Item 2 – After paragraph 3(aaa)**

12. This item amends the purposes of the Act to reflect the new power for the AFP and the ACIC to disrupt data held in a computer. It adds as a purpose, the establishment of procedures for certain law enforcement officers of the AFP and the ACIC to obtain warrants (section 27KA) and emergency authorisations (subsection 28(1C)) that authorise disruption of data held in a computer and are likely to assist in frustrating the commission of relevant offences.

**Item 3 – Paragraph 3(ba)**

13. This item amends the purposes of the Act to include restrictions on the use, communication and publication of information that is obtained through accessing or disrupting data held in computers. Access to, and disruption of, data held in computers may be authorised by the new data disruption warrant in Division 5 of Part 2, or emergency authorisations for disruption of data held in a computer in Part 3.

**Item 4 – Paragraph 3(ba)**

14. This item amends the purposes of the Act to restrict the use, communication and publication of information that is otherwise connected with computer data disruption operations. A computer data disruption operation may be an operation conducted under the authority of a data disruption warrant in Division 5 of Part 2 or emergency authorisation for disruption of data held in a computer in Part 3.

15. Information that is obtained through accessing data held in computers, and information that is otherwise connected with computer data disruption operations is subject to the restrictions on the use, communication and publication of information in Division 1 of Part 6.

**Item 5 – Paragraph 3(c)**

16. This item amends the purposes of the Act to include imposing requirements for the secure storage and destruction of records, and the making of reports, in relation to computer data disruption operations.

17. Records and reports in relation to computer data disruption operations must be stored securely and destroyed in accordance with the requirements in Division 1 of Part 6. Records in relation to computer data disruption operations must be kept and reported in accordance with the requirements in Division 2 of Part 6.
Item 6 – At the end of subsection 4(1)

18. This item amends subsection 4(1) to clarify that the Act is not intended to affect any other law of the Commonwealth, a State or any law of a self-governing Territory that prohibits or regulates disruption of data held in computers.

19. The item clarifies this relationship to other laws in respect of disruption of data held in computers, consistent with the position of the use of surveillance devices and access to data held in computers.

Item 7 – After subsection 4(4A)

20. This item inserts new subsection (4B) to clarify that a warrant or an emergency authorisation may be issued or given under the Act for access to, and disruption of, data held in a computer, in relation to a relevant offence. This replicates the clarification in existing subsections 4(4) and 4(4A) relating to warrants and emergency authorisations regarding surveillance devices and access to data held in a computer.

Item 8 – Subsection 6(1)

21. This item provides a definition in section 6(1) for terms that facilitate the operation of the data disruption provisions.

22. **Data disruption intercept information** is defined to have the same meaning as in the TIA Act. Data disruption intercept information in the TIA Act means information obtained under a data disruption warrant by intercepting a communication passing over a telecommunications system. This is distinct from data obtained under a data disruption warrant. This category of information has been created because interception for the purposes of doing things in a data disruption warrant is permitted, in the same way that this is permitted for existing computer access warrants.

23. Intercepting a communication passing over a telecommunications system has the meaning given to it by the TIA Act at section 6. The TIA Act defines interception of a communication passing over a telecommunications system as consisting of, listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

24. The definition of **data disruption warrant** is a warrant issued under section 27KC or subsection 35B(2) or (3). Section 27KC allows an eligible Judge or nominated AAT member to issue a warrant, upon he or she being satisfied of the relevant conditions contained in 27KC(1), including that there are reasonable grounds for the suspicion that the disruption of data held in the target computer is likely to substantially assist in frustrating the commission of one or more relevant offences. Data disruption warrant under subsections 35B(2) and (3) means a warrant issued by an eligible Judge or
nominated AAT member following an emergency authorisation for disruption of data held in a computer.

25. **Digital currency** has the same meaning as in the *A New Tax System (Goods and Services Tax) Act 1999*. In that Act, digital currency means digital units of value that are designed to be fungible, can be provided as consideration for a supply, and are generally available to members of the public without substantial restrictions. Digital units of value are not denominated in any country’s currency, do not have a value that is derived from the value of anything else, and do not give an entitlement to receive, or to direct the supply of things except incidentally to holding or using digital units of value. Digital currency does not include money within the meaning of *A New Tax System (Goods and Services Tax) Act 1999*.

26. **Disrupting data** held in a computer means adding, copying, deleting or altering data held in the computer. Data disruption warrants for the AFP and the ACIC may authorise the disruption of data at any time while the warrant is in force, if doing so is likely to substantially assist in frustrating the commission of one or more relevant offences in relation to which the warrant is sought.

27. The note clarifies that disrupting data by adding, copying, deleting or altering data is understood in relation to data disruption warrants or emergency authorisations for disruption of data held in a computer.

28. The inclusion of this note makes it clear that this is distinct from what may be authorised by a computer access warrant as an evidence gathering power. Computer access warrants may authorise the adding, copying, deleting or altering of data if necessary for the purposes of enabling evidence to be obtained of the commission of relevant offences or the identity or location of offenders (paragraph 27E(2)(e)).

29. The definition of **emergency authorisation for access to data held in a computer** is an emergency authorisation for access to data held in a computer in response to an application under subsection 28(1A), 29(1A) or 30(1A). Law enforcement officers may apply to an appropriate authorising officer (as defined in section 6A) for access to data held in computers where there is an imminent risk of serious violence or substantial damage to property (subsection 28(1A)), where there are urgent circumstances relating to a recovery order (subsection 29(1A)), or where there is a risk of loss of evidence (subsection 30(1A)).

30. The definition of **emergency authorisation for disruption of data held in a computer** is an emergency authorisation for disruption of data held in a computer in response to an application under new subsection 28(1C). A law enforcement officer may apply to an appropriate authorising officer for disruption of data held in computers where there is an imminent risk of serious violence to a person or substantial damage to property (subsection 28(1C)).
31. **IGIS official** is defined to mean the Inspector-General of Intelligence and Security, or another person covered by subsection 32(1) of the IGIS Act. This definition accounts for the fact that the new network activity warrant introduced by Schedule 2 of this Bill will be subject to oversight by the IGIS. The term IGIS official provides a consistent way to refer to the Inspector-General of Intelligence and Security and a member of his or her staff employed to assist in the performance of functions and exercise of powers. This definition is included to differentiate between the two bodies responsible for oversight of powers in the SD Act.

32. **Ombudsman official** is defined to mean the Ombudsman, a Deputy Ombudsman, or a person who is a member of the staff referred to in subsection 31(1) of the Ombudsman Act. This term provides a consistent way to refer to the Ombudsman and a member of his or her staff employed to assist in the performance of functions and exercise of powers. This definition is included to differentiate between the two bodies responsible for oversight of powers in the SD Act.

**Item 9 – Subsection 6(1) (definition of remote application)**

33. This item amends the definition of **remote application** in the SD Act to include reference to new section 27KB of the Act. New section 27KB permits applications for data disruption warrants to be made remotely if it is impractical for the application to be made in person. Remote applications may be made for data disruption warrants in the same way and for the same reasons as for computer access warrants under section 27B, such as time-sensitive situations.

**Item 10 – Subsection 6(1) (definition of unsworn application)**

34. This item includes references to provisions in relation to the new data disruption warrants within the existing definition of **unsworn application** in the SD Act. Applications for data disruptions can be made before an affidavit is prepared or sworn in the circumstances set out in subsections 27KA(4) and (5). Unsworn applications may be made for data disruption warrants in the same way and for the same reasons as for computer access warrants under subsections 27A(13) and (14), such as time-sensitive situations.

35. Unsworn applications for a data disruption warrant can be made in circumstances where an officer of the AFP or the ACIC believes that the immediate disruption of data held in the target computer will substantially assist in frustrating the commission of a relevant offence, and when it is deemed impracticable for the affidavit to be prepared or sworn before the application is made (subsection 27KA(4)). These reasons for unsworn applications replicate those for computer access warrants under subsections 27A(13) and (14).

**Item 11 – Subsection 6(1) (at the end of the definition of warrant)**

36. This item expands the existing definition of **warrant** in the SD Act to include the new data disruption warrant.
Item 12 – At the end of subsection 10(1)

37. This item expands the existing types of warrant that may be issued under Part 2 of the SD Act to include data disruption warrants. This is consequential to the insertion of Division 5 of Part 2 of the SD Act which establishes the framework for the AFP and the ACIC to obtain data disruption warrants.

Item 13 – At the end of Part 2

Division 5 – Data disruption warrants

38. This item introduces Division 5 to Part 2 of the SD Act. Division 5 establishes the framework for the AFP and the ACIC to obtain data disruption warrants. A data disruption warrant enables officers of the AFP and the ACIC to disrupt data held in a computer, if doing so is likely to substantially assist in frustrating the commission of one or more relevant offences. These warrants are in addition to warrants for data surveillance devices, which enable the use of software to monitor inputs and outputs from certain devices, and computer access warrants, which allow law enforcement agencies to search electronic devices remotely and access content on those devices. Surveillance device warrants and computer access warrants may be sought by law enforcement agencies (within meaning of section 6A), whereas data disruption warrants are only available to the AFP and the ACIC.

27KA Application for a data disruption warrant

39. New section 27KA sets out the requirements and processes for applying for a data disruption warrant.

40. An application for a data disruption warrant may be made by a law enforcement officer of the AFP or the ACIC, or another person on the law enforcement officer’s behalf. In subsection 27KA(1), the language ‘law enforcement officer, or another person on the law enforcement officer’s behalf’ has been used to allow support staff engaged in the usual course of an investigation to assist or provide services. These persons are not specified in order to reflect that arrangements may differ between the AFP and the ACIC.

41. A three part test must be satisfied in order to apply for a data disruption warrant.

42. Firstly, the applicant can only apply for the issue of a data disruption warrant if he or she suspects on reasonable grounds that one or more relevant offences of a particular kind have been, are being, are about to be, or are likely to be committed. The meaning of relevant offence is set out in section 6 of the SD Act. A relevant offence includes an offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of 3 years or more or for life.

43. The phrase ‘relevant offences of a particular kind’ has been inserted to allow generality regarding the types of offence in which a data disruption warrant may be obtained. The reason for this is that when performing disruption activity, it will be very difficult for a
law enforcement officer to know exactly which offences have been, are being, or are about to be, or are likely to be committed. Although in some cases there may be an intention to frustrate only one offence, it is highly likely that even when frustrating that one offence, there will be other offending of a similar kind on which that frustration has an impact.

44. For example, if a data disruption warrant were used to re-direct a person away from a child exploitation website, then that person’s access to child exploitation material may be denied, and that person may then be unable to share that particular material with others. In this chain of events, there are multiple offences which have been disrupted in some way by the initial re-direction activity. Hence a data disruption warrant is available for relevant offences of a particular kind in order to ensure that all of this activity is captured by the warrant.

45. The intention with this language is that the potential offences described by ‘relevant offences of a particular kind’ would fall into the same broad category of offending, however described on the warrant. The applicant must have formed a reasonable suspicion that one or more relevant offences of the particular kind that would be disrupted would meet the threshold of offending; that is, the threshold set out by the definition of ‘relevant offence’ in section 6 of the SD Act, for example that the offending punishable by a maximum term of imprisonment of 3 years or more or for life. This threshold will limit the availability of a data disruption warrant to only the most serious offence categories, such as terrorism and child exploitation offences.

46. Secondly, the applicant must suspect on reasonable grounds that the offences involve, or are likely to involve, data held in a computer. Data disruption warrants are only available to combat offences where those offences are conducted online or facilitated by online activities. Furthermore, the only disruption that is available under a data disruption warrant is disruption to data. That data must be held in a computer at some point in time; it cannot be only transiting through a computer or a telecommunication facility.

47. The phrase ‘target computer’ is defined in subsection 27KA(6). The definition of target computer should be read in conjunction with the definition of computer in the SD Act. The existing definition of computer under the SD Act provides that a computer can be a particular computer, a network of computers, or a computer associated with, used by, or likely to be used by a person.

48. While an application for a data disruption warrant must identify a target computer, this does not prevent access to and disruption of data associated with the target computer on another computer (new subsection 27KD). The concept of the target computer is intended to ensure that if an individual has more than one relevant computer, only one warrant will be necessary. For example, individuals generally use a number of online accounts to engage in criminal activity, including web-hosted email, social chat applications, and file-hosting services. Modification of data associated with these accounts (held on separate target computers, but all under the control of the same nominated person) may be required to disrupt the proposed activity. With the variety of computers and electronic devices now
commonly used, it is highly probable that a person may store data on a number of computers (for example, a laptop, a phone and a tablet).

49. There are two limbs to the third test which the law enforcement officer must be satisfied. Firstly, the law enforcement officer must suspect on reasonable grounds that the disruption of data held in the target computer is likely to substantially assist in frustrating the commission of one or more relevant offences that involve, or are likely to involve, data held in the target computer.

50. To frustrate the commission of an offence is to have a negative impact on the plan for that offence to occur. This could involve preventing the offence from ever occurring, or it could involve re-directing the offence so that it occurs in a different, less harmful way, for example by involving fewer participants, or a lesser form of offending. Disruption may also involve stopping the continuation of an offence that is already occurring. In order to satisfy the reasonable suspicion that the disruption of data is likely to substantially assist in frustrating the commission of an offence, the officer does not need to be satisfied that the disruption will stop the offence from occurring altogether. The disruption may delay the offending, cause the offending to be conducted in a controlled environment in which evidence can be collected, or make the offending more difficult for the potential offender to carry out.

51. An example of an offence that could be prevented from occurring under a data disruption warrant is the use of a telecommunications service to access child abuse material, or for grooming persons under 16 years of age, where deletion or modification of contact details would disrupt future offending. Law enforcement may also seek a data disruption warrant to authorise the use of technical tools and capabilities to disable a server hosting a dark web forum that is proliferating child abuse material.

52. An offence that could be re-directed through a data disruption warrant is a terrorist offence, where the AFP or the ACIC may be authorised to access an email account on a particular computer and modify an email to delay an attack.

53. The continuation of an offence that could be completely disrupted as a result of a data disruption warrant is the presence of child exploitation material on third party computers. A data disruption warrant would allow for this material to be deleted, preventing the continuation of the offence.

54. Secondly, those offences which are aimed to be frustrated, must be of the same kind of offences as the relevant offences that formed the suspicion initiating the warrant. The reason for this specification in subparagraph 27KA(1)(c)(ii) is, as described above, the offences targeted for disruption must be of the same kind. They must be in one category of offending. If there are two categories of offending (for example, the trafficking of both firearms and drugs) then two data disruption warrants should be sought.
Procedure for making applications

55. Subsections 27KA(2) and (3) set out the procedure for making a data disruption warrant application. This procedure replicates the procedure set out in subsections 27A(7) and (8) for computer access warrants. An application for a data disruption warrant under subsection 27KA(1) must be made to an eligible Judge or to a nominated AAT member.

56. An eligible Judge is a person who is a Judge of a court and has consented to be declared an eligible Judge by the Attorney-General, as the Minister responsible for administering the Judiciary Act 1903 (section 12). The functions and powers of Judges are conferred only in a personal capacity and not as a court or a member of a court. A nominated AAT member is a person who is either the Deputy President, senior member or member of the AAT, and has been nominated by the Attorney-General, as the Minister responsible for administering the Administrative Appeals Tribunal Act 1975 (section 13).

57. The application must specify the name of the applicant and the nature and duration for which the warrant is sought. An application must be supported by an affidavit setting out the grounds on which the warrant is sought. An application for a data disruption warrant will have to provide as much information as necessary for the issuing authority to be satisfied that there are reasonable grounds for the suspicion founding the application for the warrant.

Unsworn applications

58. New subsections 27KA(4) and (5) provide for applications for data disruption warrants to be made before an affidavit is prepared or sworn under some circumstances. In those cases, the applicant must send a duly sworn affidavit to a Judge or AAT member no later than 72 hours after the making of the application for the data disruption warrant. This enables an application to be made in circumstances where immediate disruption of data held in the target computer is likely to substantially assist in frustrating the commission of offences. An unsworn application may be sought in circumstances where, for example, credible intelligence is received only shortly before the offending activity is about to occur, and where it is of a very serious nature, or will have substantial impact on potential individuals.

59. Another example might include where the AFP is monitoring the communications of an individual who is suspected to be engaging with an unknown person to sexually abuse a child and live-stream the abuse. An email is received late one evening by the individual agreeing to the illegal activity to occur early the next morning. The AFP may then apply for a data disruption warrant without a sworn affidavit in order to prevent the imminent abuse of a child from occurring. Upon the warrant being issued, the AFP may delete the email from the individual’s inbox, and in doing so, the individual does not receive the email and the abuse does not occur on account of the individual not making contact with the unknown person. The AFP will then be required to provide the eligible Judge or
nominated AAT member with a sworn affidavit within 72 hours of making the unsworn application.

**Target computer**

60. Data disruption warrants are sought for disruption of data held in the target computer. Target computer has the same meaning as in subsection 27A(15) in relation to computer access warrants. This definition has been replicated and included in new subsection 27KA(6). The target computer may be either a particular computer, a computer on a particular premises, or a computer associated with, or used or likely to be used by a person, the identity of whom may or may not be known. The computer does not need to be owned by the suspect. For example, it might be a computer in the suspect’s house that the suspect uses but does not own, or a computer that the suspected offender uses at work.

61. A computer may also be a network of computers. Individuals commonly have multiple devices and access to a variety of networks. For example, a network of computers might be multiple devices owned or used by a particular person, or a group of connected computers owned or used by any number of people.

62. The identity of the person using the target computer does not need to be known. This is because there will be circumstances in which the suspected offender has obfuscated his or her identity through various anonymising techniques and technologies. The offender may be using the dark web in order to hide his or her activities. The law enforcement officer may only know specific identifiers about this activity, such as the IP addresses visited by the computer and the types of material the computer is accessing, or the data that is being transmitted and received. All of these could be indicators of enough criminal activity to meet the threshold in section 27KA(1), without the identity of the offender being known.

63. This also takes into account circumstances in which the AFP or the ACIC seek to frustrate the commission of offences by disrupting data held in a computer belonging to a victim of the suspected offending, or a third party to the offending. This may occur where the perpetrator of an offence may be too well-hidden (for example on the dark web, or through the use of some other anonymising technology) for law enforcement to take any action against that person, or the person may be in a foreign jurisdiction beyond the reach of Australian law enforcement. There may however be a way that law enforcement could disrupt offending by instead interacting with a computer belonging to a victim, with the result that certain information never reaches the victim’s computer, or reaches the computer and then is instantly removed. For example, data could be altered in order to remove offensive material such as that used to groom children online, before any potential victims have access to that material.

64. Another example might involve the AFP or the ACIC applying for a data disruption warrant based on known file and communication attributes that are unique to malware infecting victims’ devices. This will allow the agency to detect and modify the malware to neutralise further infection or further loss of personal information from victims. In this
way, the warrant will be used to frustrate the commission of offending using the malware. In some cases, this could be done without the victim ever being exposed to the harmful material. An example of this type of disruption is where law enforcement have been made aware of certain malware that is infecting victim’s devices for the purpose of a cybercrime offence.

27KB Remote application

65. A remote application for a data disruption warrant may be made in the same way and for the same reasons that a remote application for a computer access warrant may be made under section 27B. New section 27KB permits the application for a data disruption warrant to be made by telephone, fax, email, or by other means of communication where the law enforcement officer of the AFP or the ACIC believes it is impracticable for the application to be made in person.

66. An example of where a remote application may be made is if the AFP or the ACIC uncover evidence that suggests an individual is preparing to upload a cyber crime manual within the next two hours. The time sensitivity in this circumstance may mean that it is too time consuming or impractical for the application to be made in person. In this case, the AFP or the ACIC may apply for a data disruption warrant via other means, including fax, telephone, or email, for the purpose of gaining consent to immediately disrupt data in a target computer. This expedites the application process and allows for a more time-critical response to new and rapidly time-sensitive developments in the course of an investigation or other law enforcement conduct.

27KC Determining the application

67. New section 27KC provides for the conditions under which an eligible Judge or nominated AAT member may issue a data disruption warrant. The condition at paragraph 27KC(1)(a) is modelled on the conditions for the issue of surveillance device warrants (at paragraph 16(1)(a)) and computer access warrants (at paragraph 27C(1)(a)).

68. Before issuing a data disruption warrant, the issuing authority must be satisfied that there are reasonable grounds for the suspicion founding the application for the warrant, and that the disruption of data authorised by the warrant is justifiable and proportionate having regard to the offences in relation to which the warrant is sought. Whether the disruption of data is justifiable and proportionate will be determined by the Judge or AAT member on a case by case basis. The disruption of data would not be justified or proportionate in circumstances where disrupting data would involve loss or damage to the data of third parties that is disproportionately large compared to the benefit that would be gained through the disruption of the data helping to frustrate the commission of offences.

69. The wording ‘having regard to the offences’ is intended to account for consideration of the scale of relevant offences that can be targeted under a data disruption warrant. This may impact the level of data disruption that may be considered justifiable and proportionate.
70. Disruption of data would be justifiable and proportionate in circumstances where it is difficult to undertake traditional law enforcement activity and disrupting data would assist in frustrating the variety of offending and minimising harms to victims.

71. For example, it may be justified and proportionate for an agency to shut down an online site hosting and distributing child exploitation material despite the owner or administrator of that site not necessarily being suspected of this type of criminality. In contrast, it may not be deemed justified or proportionate if an agency were to delete all the data on a third-party computer that was used to access a dark web forum advertising illicit drugs.

72. For unsworn applications (paragraph 27KC(1)(c)), the issuing authority must be satisfied that it was impracticable for an affidavit to have been sworn before the application was made. This allows for external scrutiny of judgments made by officers for an application where an affidavit could not be sworn in time. Similarly, in relation to applications made remotely, the eligible Judge or AAT member must also be satisfied that it was impracticable for the application to have been made in person.

73. Subsection 27KC(2) sets out the mandatory considerations to which an issuing authority must have regard in determining whether a data disruption warrant should be issued. There are four mandatory considerations. These do not preclude the consideration of other things the issuing authority may wish to take into account.

74. The issuing authority must take into account the nature and gravity of the conduct constituting the offences which founded the application for the warrant. This should involve consideration of the seriousness of the offending, and the scope of the relevant offences of a particular kind. As discussed above, the extent to which the disruption of data may be deemed justifiable and proportionate will likely be impacted by the offence being targeted under the data disruption warrant.

75. The issuing authority must have regard to the likelihood that the disruption of data authorised by the warrant will frustrate the commission of the relevant offences specified in the warrant. This may mean weighing up the type of criminal activity, the scope of the activity, and the type of disruption methods sought to combat that activity, in order to determine the likely effect of the relevant disruption activity on the criminal conduct. The issuing authority need not determine through this consideration that any criminal activity will be prevented from occurring, only that there is a likelihood of criminal activity being frustrated by disruption of data. As discussed above, disruption encompasses not only preventing criminal activity from occurring but also re-directing the offence so that it occurs in a different, less harmful way, or stopping the continuation of an offence that is already occurring.

76. The issuing authority must have regard to the existence of any alternative means of frustrating the commission of the offence or offences. This includes, for example, taking into account whether more traditional methods of policing and investigatory powers would have the same effect as the frustration of the offences through disruption of data. For
example, if overt police action, such as the use of a search warrant, would prevent the offending from occurring, this could be taken into account by the issuing authority. On the other hand, if disruption of data would result in a different outcome to a prosecution, for example a significantly more expedient outcome, a more preventative outcome, or a better outcome for the potential victims of a crime, then this also could be taken into account. In having regard to the existence of alternative means of frustrating the commission of offences, the issuing authority may also consider that disruption is appropriate in circumstances where prosecution may not be possible. For example, where there are too many offenders, or where the offender is too well-hidden or inaccessible, due to their use of anonymising technologies, to definitively identify and commence overt police action and prosecution. In these circumstances, disruption would assist law enforcement in managing the threat, as while they may not be able to bring a prosecution, they can interrupt, prevent and frustrate criminal activity.

77. The issuing authority should also take into account whether disruption of data is necessary to frustrate the commission of an offence as opposed to the alternative of accessing data that is available under a computer access warrant in the SD Act. Because data disruption warrants permit the accessing of data, the issuing authority should be careful to ensure that data disruption warrants are not being sought purely to access data, but are sought to achieve purposes that cannot be achieved under other warrant regimes.

78. Lastly, the issuing authority must have regard to any previous warrant sought or issued under this Division in relation to the same alleged relevant offences.

27KD What must a data disruption warrant contain?

79. Subsection 27KD(1) sets out the information a data disruption warrant is required to contain. A data disruption warrant must state that the issuing authority is satisfied of the matters referred to in subsection 27KC(1) and has had regard to the matters referred to in subsection 27KC(2) in determining the application.

80. A data disruption warrant must also specify the name of the person making the application, the offences in relation to which the warrant is sought, the date the warrant is issued, the period for which the warrant is in force and the name of the law enforcement officer primarily responsible for executing the warrant.

81. If the target computer is or includes a particular computer, the data disruption warrant must specify that computer. If the warrant is aimed at a computer located on particular premises, it must specify those premises. If the target computer is or includes a computer associated with, used by or likely to be used by a person, then the warrant must specify that person. The person’s name does not need to be specified, but the person must be able to be specified in some other way.

82. New subparagraph 27KD(1)(b)(ix) states that a data disruption warrant must specify any conditions subject to which things may be done under the warrant.
83. Subsection 27KD(2) provides that a data disruption warrant may only be issued for a period of no more than 90 days. This is in line with the period of effect for surveillance device warrants and computer access warrants. This length of time is intended to allow long-term operations that could be complex, involve multiple linked targets, and involve a combination of warrants as part of the operation, such as the initial period of surveillance with the authority to disrupt data during that time where necessary. The note after subsection 27KD(2) clarifies that disruption can be discontinued earlier than the period stipulated in the warrant, under section 27KH.

84. Subsection 27KD(3) provides that where a warrant authorises access to, or disruption of, data in a target computer located in a vehicle, the warrant need only specify a class of vehicle. This minimises the risk of computer access and disruption being thwarted by frequent vehicle changes. The warrant may specify, for example, a vehicle used by a specific person.

85. Subsection 27KD(4) provides that a warrant must be signed by the person issuing it and include the person’s name.

86. Subsection 27KD(5) provides that, as soon as practicable after a remote application for a data disruption warrant has been completed and signed, the issuing authority must inform the applicant of the terms of the warrant, and the date on which and the time at which the warrant is issued. The issuing authority must also provide the warrant to the applicant, whilst also retaining a copy for their personal records.

27KE What a data disruption warrant authorises

87. Similar to a computer access warrant, subsection 27KE(1) provides that a data disruption warrant must authorise the doing of specified things in relation to the relevant target computer. This is subject to any restrictions or conditions specified in the warrant. This provision ensures that any things authorised under a data disruption warrant must be done in relation to the target computer, as the object of the warrant.

88. Data disruption will often be necessary in circumstances where the use of anonymising technologies has made traditional policing approaches (such as arrest and prosecution) impracticable or even impossible. For example, the dark web offers opportunities for criminals to operate anonymously and across multiple jurisdictions which allows them to evade detection. In these circumstances, targets are often remote, not accessible offline, or too numerous or untenable to pursue for prosecution. Targets may also be located offshore, or their jurisdiction may not be identified, which further complicates law enforcement’s response. In such circumstances, the power to disrupt data held in a computer will often be the most practicable and effective option in preventing the continuation of criminal activity and minimising harms to victims.

89. The things that may be authorised under a data disruption warrant are set out in section 27KE. This will enable law enforcement to use their own sensitive, technical capabilities
to disrupt data in a computer, to effect the desired disruption outcome (for example, ceasing activity on a particular site, redirecting traffic on a site, encouraging user migration to other services or platforms, removing illegal content or otherwise denying access to said content).

90. Subsection 27KE(2) sets out the things that may be specified in a data disruption warrant provided the eligible Judge or nominated AAT member considers it appropriate in the circumstances. The word ‘may’ is used to clarify that all of the following particulars in paragraphs 27KE(2)(a)-(i) are not required in every circumstance.

91. Under paragraph 27KE(2)(a) the eligible Judge or AAT member may specify that premises may be entered for the purposes of doing things mentioned in this subsection. Data disruption may not always be performed remotely, and may require officers to enter premises in order to gain access to a device before disrupting the data held on the device.

92. Paragraph 27KE(2)(b) makes it clear that premises other than the premises specified in a warrant (that is, third party premises) can be entered for the purpose of gaining access to or exiting the subject premises for the purposes of executing the data disruption warrant. This may occur where, upon arriving at a specified premises, there is no other way to gain access to that premises without entering another premises (for example, in an apartment complex where it is necessary to enter the premises through shared or common premises).

93. It may also occur where, for operational reasons, the best means of entry might be through adjacent premises (for example, where entry through the main entrance may involve too great a risk to the safety of executing officers). The need to access third party premises may also arise in emergency and unforeseen circumstances. For example, a person may arrive at the specified premises unexpectedly during the execution of a data disruption warrant it is necessary for the executive officers to exit through the premises of a third party to avoid detection.

94. Under paragraph 27KE(2)(c) the issuing authority may specify in the warrant that the warrant permits using the target computer, a telecommunications facility operated or provided by the Commonwealth or a carrier, any other electronic equipment or a data storage device. There are two purposes for which these things can be used. The first at subparagraph 27KE(2)(c)(v) is to obtain access to data that is held in the target computer, in order to determine whether the relevant data is covered by the warrant. The second at subparagraph 27KE(2)(c)(vi) is to disrupt the relevant data at any time while the warrant is in force, if doing so is likely to assist in frustrating the commission of one or more relevant offences covered by the warrant. Disrupting data means adding, copying, deleting or altering data held in a computer. This power may be used to disrupt or deny service to a computer that is being used for illegal purposes.

95. These provisions are intended to ensure that data can be both accessed and disrupted. In order for law enforcement to disrupt data held in a computer, they must first obtain access
to data. Data can only be accessed under a data disruption warrant in order to assess whether it is the relevant data for the purposes of the activity of disruption.

96. While the activities that may be authorised under a data disruption warrant are similar to those under a computer access warrant (in section 27E), the purposes for which these things may be done under each warrant is distinct. Computer access warrants may authorise access to data held in computers for the purposes of gathering evidence about relevant offences. Data disruption warrants may authorise access to, and disruption of, data held in a computer for the purposes of frustrating the commission of relevant offences. Although evidence may be gathered by virtue of conducting a data disruption exercise, and although that evidence may be gathered using computer access techniques, the data disruption warrant regime is intended to provide for disruption activities. It does not replace the computer access warrants as an evidence gathering regime.

97. Subparagraphs 27KE(2)(c)(v) and (vi) make clear by the words ‘at any time while the warrant is in force’ that data disruption warrants authorise ongoing access to, and disruption of, data held in the target computer over the life of the warrant. Data does not have to be stored on the target computer, but can be passing through it. This is to account for the fact that some relevant data may be unknown or unknowable at the time the warrant has been issued.

98. Some forms of data that may be unknown or unknowable at the time of issue may include, for example, prospective communications, account credentials, access codes, members and content of an illicit forum or service, additional computers linked to the target computer, identifiable information of computers linked to the target computer, and additional content of the target computer that may be relevant for the purposes of the warrant.

99. Paragraph 27KE(2)(d) permits adding, copying, deleting, or altering other data in the target computer if necessary to obtain access to data held in the target computer, in order to determine whether the relevant data is covered by the warrant. Data may need to be copied and analysed before its relevancy or irrelevancy can be determined. The power to add, copy, delete or alter other data can only be used where necessary for the purpose of obtaining access to data held in the target computer. This provision recognises that in some cases direct access to a target computer will be difficult or even impossible.

100. Paragraph 27KE(2)(e) allows using any other computer or a communication in transit to access and disrupt relevant data if it is reasonable in all the circumstances, having regard to other methods of obtaining access to and disrupting the data. This ensures that the AFP and the ACIC can effectively use a third party computer or a communication in transit in order to carry out the disruption activity.

101. Accessing a communication in transit means accessing any communication passing between the target device and the service provider, as long as this access does not amount to interception. Permissible interception is provided for in paragraph 27KE(2)(i).
102. The use of third party computers and communications in transit to add, copy, delete or alter data in the computer or the communication in transit recognises that it may be difficult or even impossible to access a target computer. The ability to use third party computers and communications in transit permits and facilitates access to and disruption of data held in the target computer.

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

104. Paragraph 27KE(2)(g) allows the copying of any data which has been accessed if it either appears relevant for the purposes of determining whether the relevant data is covered by the warrant, or is covered by the warrant. Data that is subject to some form of electronic protection is taken to be relevant for the purposes of determining whether it is relevant data covered by the warrant (subsection 27KE(4)). These provisions ensure that data either accessed and disrupted on a computer remotely, or accessed and disrupted on a computer at the premises specified in the warrant can be copied onto another computer. This will be necessary in order for data to be analysed on a different computer located elsewhere or using different software. It will also allow evidence to be collected.

105. For example, during the course of a data disruption warrant targeting an individual suspected of planning a terrorist attack, the AFP or the ACIC may find blueprints to a building held on the target computer. Under the data disruption warrant, the AFP or the ACIC can copy these blueprints in order to analyse them, determine what building they relate to, and how the blueprints are relevant to the warrant and the individual the warrant is targeting.

106. Paragraph 27KE(2)(h) permits intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing anything specified in the warrant in accordance with 27KE(2).

107. Often it will be necessary for a law enforcement agency to intercept communications for the purpose of executing a data disruption warrant. This subsection ensures that the AFP and the ACIC will be able to do so, but only for those limited purposes of making access to and disruption of data held in a target computer practicable or technically possible. Information obtained under a data disruption warrant by interception is data disruption intercept information. The use of this information is governed by the TIA Act (see new section 64AD).

108. A data disruption warrant cannot authorise the collection of evidence by interception for investigating an offence. If the AFP or the ACIC require interception other than to facilitate a data disruption warrant, they must seek an interception warrant from an eligible issuing authority under the TIA Act.
109. Paragraph 27KE(2)(i) allows a data disruption warrant to authorise the doing of anything reasonably incidental to any of the things specified in paragraphs 27KE(2)(a) to (h).

110. The note at the conclusion of section 27KE(2) clarifies that a person who obtains access to data stored in a computer by using a telecommunication facility will not commit an offence under Part 10.7 of the Criminal Code or equivalent State or Territory laws if the person acts within the authority of the warrant. Part 10.7 of the Criminal Code provides for the Commonwealth computer offences.

111. New subsection 27KE(3) of the SD Act provides for the return of a computer or other thing under a data disruption warrant. Subsection 27KE(3) provides that where a warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph 27KE(2)(f), and the computer or other thing is so removed from the premises, then the computer or thing must be returned to the premises within a reasonable period.

112. Subsection 27KE(4) stipulates that data that is subject to some form of electronic protection is taken to be relevant for the purposes of determining whether it is relevant data covered by the warrant (subsection 27KE(4)) in association with paragraph 27KE(2)(g)).

When data is covered by a warrant and when a relevant offence is covered by a warrant

113. Subsections 27KE(5) and (6) are clarifying provisions to explain that data is taken to be covered by the warrant if disruption of the data is likely to substantially assist in frustrating the commission of one or more relevant offences, and offences are taken to be covered by the warrant if they are the offences to be frustrated by the disruption of data. These provisions reiterate the thresholds in paragraph 27KA(1)(c) which must be met before a law enforcement officer of the AFP or the ACIC may apply for a data disruption warrant.

Certain acts not authorised

114. Subsection 27KE(7) has the same effect as subsection 27E(5) in relation to computer access warrants. A data disruption warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to this limitation has been included so that an agency may undertake such actions where they are otherwise necessary to successfully execute the purpose of the warrant. Similarly, a data disruption warrant can only authorise causing material loss or damage to persons lawfully using a computer if the loss or damage is justified and proportionate with regard to the offences covered by the warrant.

115. Whether loss or damage is justified and proportionate will be a matter to be considered by the issuing authority on a case-by-case basis. For example, it may be justified and proportionate to authorise an activity which causes loss or damage to a third party’s data.
when seeking to frustrate the commission of a particularly serious offence by a large group of criminals.

116. Subsection 27KE(7) recognises that it will often be necessary during the course of a data disruption warrant to interact with third-party data, but this should only be done where necessary for the execution of the warrant (paragraph 27KE(7)(a)) or justified and proportionate with regard to the offences targeted (paragraph 27KE(7)(b)). Prohibiting the ability to interact with a third-party’s data altogether would in many cases critically hinder the ability to frustrate the commission of offences as third-party data can often be inextricably linked or associated to the target computer or the data needing to be accessed.

117. For example, a server is being used to host a child exploitation forum and an innocent-third party is using the same server to store their data. In the event a disruption activity being conducted causes a third party to experience loss of data, then this loss will be limited to their use of the target server, which is being used to commit the relevant offence. While this is not the overall intent of the warrant, the loss may be deemed justifiable and proportionate to the relevant offences (child exploitation offences) that are subject to the data disruption warrant.

Warrant must provide for certain matters

118. At subsection 27KE(8), a data disruption warrant must authorise the use of any force against persons or things that is necessary and reasonable to do the things specified in the warrant. Any unauthorised use of force against a person that does not comply with these requirements may attract criminal and civil liability. If the warrant authorises entry onto premises, then the warrant must state whether entry is authorised to be made at any time, or during a set period of time.

Concealment of access etc.

119. Subsection 27KE(9) provides that a data disruption warrant will also authorise the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to a computer under the warrant. This may include, for example, forcing a device to malfunction, deleting data to obfuscate law enforcement access, or other technical methods that may seek to conceal that things were done under the warrant.

120. Concealment of access is essential for preserving the effectiveness of covert warrants under the SD Act. Paragraphs 27KE(9)(d) and (e) also authorise the entering of premises where the computer that has been accessed is located, or premises for gaining entry or access to where the computer is located, for the purposes of concealing the action that has been taken under a data disruption warrant.

121. At subparagraph 27KE(9)(f), a data disruption warrant may authorise removing the computer or another thing from any place where it is situated, and returning it, for the purposes of concealing access. The ability to temporarily remove a computer from the premises is important in situations where the AFP or the ACIC may have to use specialist
equipment to disrupt data on the computer but cannot, for practical reasons, bring that equipment onto the premises in a covert manner.

122. Paragraph 27KE(9)(g) permits using a third party computer or communication in transit to conceal the fact that anything has been done under a data disruption warrant and, if necessary, the adding, copying, deleting or altering of other data using a third party computer or communication in transit.

123. Paragraph 27KE(9)(h) allows the interception of a communication passing over a telecommunications system for the purposes of doing any thing under subsection 27KE(9) to conceal the fact that any thing has been done under the warrant.

124. Paragraph 27KE(9)(i) allows a data disruption warrant to authorise the doing of any other thing reasonably incidental to do any of the things specified in 27KE(9)(a) to (h).

125. Paragraph 27KE(9)(j) allows concealment activities to be done at any time while the warrant is in force, or within 28 days after it ceases to be in force, or at the earliest time after this period at which it is reasonably practicable to do so. Paragraph 27KE(9)(k) provides that if the concealment activities are not done within the 28-day period, they must be done at the earliest time reasonably practicable after that period.

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

127. Subsection 27KE(10) clarifies that the concealment of access provisions do not authorise the same activities that are not authorised under a data disruption warrant under subsection 27KE(7).

128. Subsection 27KE(11) stipulates that if a computer or thing has been removed from a place in accordance with paragraph 27KE(9)(f), it must be returned to the place within a reasonable period.

Statutory conditions

129. Subsection 27KE(12) sets out the statutory conditions to which a data disruption warrant is subject. These conditions are distinct from the certain acts not authorised by the warrant in subsection 27KE(7). Statutory conditions means that a warrant is invalid if its execution results in any of the things listed in subsection 27KE(12). These conditions must be specified in the data disruption warrant (subsection 27KE(14)).

130. Paragraph 27KE(12)(a) provides that if damage to data occurs during a data disruption warrant, the damage must be justified and proportionate to the serious offence being
targeted by the warrant. As described above, whether damage is justified and proportionate will be a matter to be considered by the issuing authority on a case-by-case basis. A warrant will be invalid if it results in loss or damage to data that is not justified and proportionate.

131. Paragraph 27KE(12) provides that the warrant must not be executed in a manner that causes a person to suffer a permanent loss of money, digital currency, or property (other than data). This provision ensures that money, digital currency and property (other than data) cannot be seized under a data disruption warrant. Seizure of money and property by law enforcement is provided for in the *Proceeds of Crimes Act 2002*. Data disruption warrants are for the purposes of disrupting data, not for the purposes of frustrating criminal activity by depriving a person permanently of funds.

132. However, it is envisaged that under a data disruption warrant the AFP or the ACIC could access and modify data that is associated with a person’s financial accounts, where those modifications do not result in permanent loss.

133. For example, these warrants could be used in investigating money laundering operations in which data associated with the movement of funds could be monitored and potentially re-directed in order to prevent certain activities from occurring. Similarly, interactions with funds flowing in relation to websites hosting illicit material or goods may be necessary to prevent the further spread of, for example, child abuse material. Altering data linked to a person’s bank account credentials is also contemplated under the data disruption warrant.

134. Subsection 27KE(12) has been inserted to ensure that none of these activities can result in seizure and that the seizure of goods such as drugs and firearms, and finances or the proceeds of crimes, remains governed by existing legislation.

135. Subsection 27KE(13) specifies that subsection (12) does not limit the conditions to which a data disruption warrant may be subject. Under subsection 27KE(1), a data disruption warrant must authorise the doing of specified things subject to any restrictions or conditions specified in the warrant.

**27KF Extension and variation of data disruption warrant**

136. Section 27KF allows an officer to apply at any time while the warrant is in force for an extension of the warrant or a variation of its terms. The warrant can only be extended for a period not exceeding 90 days after the day the warrant would otherwise expire but for the extension. This builds flexibility into the warrant process and accounts for extended investigations and unexpected circumstances.

137. The application for an extension or variation must be made to an eligible Judge or nominated AAT member (paragraph 27KF(2)). Paragraph 27KF(4) provides that the Judge or AAT member must consider the same matters required to issue a data disruption warrant.
warrant at first instance (see subsection 27KC(2)) and be satisfied that the grounds on which the application for the warrant was made still exist (see subsection 27KC(1)).

138. Paragraph 27KF(3) specifies that the same provisions which provide for applications for data disruption warrants apply in relation to applications for variations and extensions. This ensures that any varied specifications are within the bounds of what might have been authorised in a data disruption warrant in the first instance. A variation for a warrant cannot authorise the addition, deletion or alteration of data that interferes with a person’s lawful use of a computer, unless it is necessary for the execution of the warrant.

139. This new section does not prevent the issue of further applications for variation or extension.

27KG Revocation of data disruption warrant

140. Section 27KG sets out the provisions for revoking a data disruption warrant. A data disruption warrant may be revoked by an eligible Judge or nominated AAT member on his or her own initiative at any time before the warrant expires. If the warrant is revoked and the officer executing the warrant is already in the process of executing the warrant, the officer does not have any civil or criminal liability for actions done before he or she is made aware of the revocation (subsection 27KG(5)).

141. The chief officer of the agency to which the data disruption warrant was issued must revoke the warrant if satisfied that access to data under the warrant is no longer required for the purposes of disrupting data held in a target computer that is likely to assist in frustrating the commission of one more relevant offences for which the warrant was sought (subsection 27KG(2)).

142. Revocations must be made by instrument in writing, and be signed by the person who revoked the warrant, the Judge or AAT member or chief officer of the agency (subsection 27KG(3)). If the warrant is revoked by the Judge or AAT member, he or she must provide the chief officer of the relevant agency with a copy of the instrument of revocation (subsection 27KG(4)).

27KH Discontinuance of access and disruption under warrant

143. Section 27KH provides for the circumstances in which access to, and disruption of, data under a data disruption warrant must be discontinued.

Scope

144. Subsection 27KH(1) clarifies that the provisions relating to discontinuance of access and disruption under a warrant only apply if a data disruption warrant is issued.
Discontinuance of access and disruption

145. Subsection 27KH(2) places an obligation on the chief officer of the AFP or the ACIC to take steps to discontinue access to and disruption of data where he or she is satisfied that the grounds on which a data disruption warrant was sought have ceased to exist. Access under a data disruption warrant must be discontinued if the chief officer is satisfied that access to data under the warrant is no longer required for the purposes of disrupting data in a target computer that is likely to assist in frustrating the commission of one or more relevant offences.

146. Subsection 27KH(3) complements section 27KG providing that the chief officer of the agency must take steps to discontinue access to, and disruption of, data as soon as practicable after being made aware that an eligible Judge or nominated AAT member has revoked the warrant.

147. Subsections 27KH(4) places an obligation on the law enforcement officer who is primarily responsible for executing the warrant to immediately inform the chief officer if there is a change in circumstances affecting the warrant. Upon being informed of the change in circumstances by the executing officer, the chief officer of the AFP or the ACIC may have obligations under subsection 27KH(2).

148. The person primarily responsible for executing the warrant will be in many cases the officer to whom the warrant was issued under section 27KC and who made the application under section 27KA. However, this may not always be the case as section 27KA enables a person to apply for a warrant on behalf of the law enforcement officer. There may also be staffing and organisational changes during the period the warrant is in place. Subsection 27KH(4) also recognises that there may be multiple people working on the execution of a particular warrant, by placing the obligation on the person who is primarily responsible. This position has not been legislated because agencies frequently structure investigations differently.

27KJ Relationship of this Division to parliamentary privileges and immunities

149. New section 27KJ provides that, to avoid doubt, Division 5 does not affect the law relating to the powers, privileges and immunities of each House of the Parliament, their members, committees of each House of the Parliament and joint committees of both Houses of the Parliament.

150. The purpose of the amendment is to clarify that the provisions relating to data disruption warrants in Division 5 of Part 2 of the SD Act are not intended to intrude on the powers, privileges and immunities of the Parliament.

Item 14 – Subsection 28(1B)

151. This item ensures that the target computer described in existing subsection 28(1B) only refers to target computer in existing subsection 28(1A), being a target computer for the
purposes of an emergency authorisation for access to data held in a computer in the course of an investigation of a relevant offence. This is to narrow this particular mention of target computer to emergency authorisations for computer access activities, as this Bill provides separately for emergency authorisations for disruption offences.

**Item 15 – After subsection 28(1B)**

152. This item amends the emergency authorisation provisions in the SD Act to allow law enforcement officers of the AFP and the ACIC to apply to an appropriate authorising officer (see section 6A) for access to, and disruption of, data held in computers in the course of an investigation of a relevant offence.

153. New subsection 28(1C) provides that in order to apply for an emergency authorisation for disruption of data held in a computer, the law enforcement officer must reasonably suspect that there is an imminent risk of serious violence or substantial property damage, that disruption of data in the target computer is immediately necessary for dealing with that risk, and that the circumstances are so serious and the matter is so urgent that disruption of data held in the target computer is warranted, and that it is not practicable to apply for a data disruption warrant.

154. New subsection 28(1D) provides that target computer that is the subject of the data disruption emergency authorisation may be a particular computer, a computer on a particular premises, or a computer associated with, used by or likely to be used by, a person whose identity may be known or not known. This is the same meaning of target computer for data disruption warrants in subsection 27KA(6).

**Item 16 – Subsections 28(3) and (4)**

155. This item provides for applications for emergency authorisations for disruption of data held in a computer (in subsection 28(1C)) to be made orally, in writing, by telephone, email or fax or any other means of communication.

156. This item also provides that for an emergency authorisation for disruption of data held in a computer, the appropriate authorising officer may give the authorisation if satisfied that there are reasonable grounds for the suspicion founding the application mentioned in subsection 28(1C).

**Item 17 – At the end of section 28**

*Statutory conditions – disruption of data held in a computer*

157. This item inserts an additional subsection under section 28 to provide for the statutory conditions that an emergency authorisation for disruption of data held in a computer is subject to. These are the same statutory conditions to which a data disruption warrant is subject (see subsection 27KE(12)).
158. Paragraph 28(5)(a) provides that if damage to data occurs during an emergency authorisation for a data disruption warrant, the damage must be justified and proportionate to the relevant offence being targeted by the warrant. This will involve the same types of considerations as those for determining whether activity under a data disruption warrant is justified and proportionate, noting the different circumstances that may be presented by an emergency situation.

159. Paragraph 28(5)(b) similarly places a condition on the conduct that can be carried out under an emergency authorisation for a data disruption warrant. The execution of the authorisation must not cause a person to suffer a permanent loss of money, digital currency or property (other than data).

Item 18 – After subsection 32(2A)

160. This item inserts subsection 32(2B) which provides that anything that can be authorised under a data disruption warrant can be authorised under an emergency authorisation for disruption of data.

Item 19 – After subsection 32(3A)

161. This item inserts subsection 32(3B) which provides that a law enforcement officer may only disrupt data held in a computer if he or she is acting in performance of his or her duty.

Item 20 – Subsection 32(4)

162. This item amends subsection 32(4) to provide that the new subsection 32(2B) is not captured by this subsection. Subsection 32(4) provides that nothing in Part 3 of that Act (relating to emergency authorisations) authorises the doing of anything for which a warrant would be required under the TIA Act. The intent of this amendment is to give proper effect to subsection 32(2B) such that an emergency authorisation to disrupt data held in a computer may authorise anything that a data disruption warrant may authorise.

Item 21 – After subsection 33(2A)

163. This item inserts new subsection 33(2B) which provides that an application for an emergency authorisation for disruption of data held in a computer must specify the name of the applicant for the approval, and if a warrant is sought, the nature and duration of the warrant. The authorisation must be supported by an affidavit stating grounds for issue and be accompanied by a copy of the written record made under existing section 31 of the SD Act.

164. Subsection 33(2B) is similar to existing subsections 33(2) and (2A), but will apply to the disruption of data held in a computer under a data disruption warrant rather than a surveillance device or computer access.
Item 22 – After subsection 34(1A)

165. This item sets out the considerations that a Judge or nominated AAT member must take into account before deciding to approve an emergency authorisation for data disruption issued by an appropriate authorising officer under new subsection 28(1C), in circumstances where the law enforcement officer reasonably suspects that there is an imminent risk of serious violence to a person or substantial damage to property.

166. The Judge or nominated AAT member must, being mindful of the intrusive nature of disrupting data held in a computer, turn his or her mind to the following factors including; the nature of the risk of serious violence to a person or substantial damage to property, the extent to which issuing a data disruption warrant would have helped reduce or avoid the risk, the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk, how much the use of such methods would have helped reduce or avoid the risk, how much the use of such methods would have prejudiced the safety of the person or property because of delay or for another reason, and whether or not it was practicable in the circumstances to apply for a data disruption warrant.

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

168. This subsection is similar to existing subsections 34(1) and (1A), which set out the considerations that must be taken into account before a Judge or ATT member may approve an emergency authorisation for the use of a surveillance device and a computer access warrant respectively, in circumstances where the law enforcement officer reasonably suspects that there is an imminent risk of serious violence to a person or substantial damage to property.

Item 23 – After subsection 35A

35B Judge or nominated AAT member may approve giving of an emergency authorisation for disruption of data held in a computer

169. This item inserts new section 35B which sets out the conditions on which an eligible Judge or nominated AAT member may approve an emergency authorisation for disruption of data held in a computer.

170. Before approving an emergency authorisation for disruption of data held in a computer, the eligible Judge or nominated AAT member must be satisfied of the grounds underlying the emergency authorisation. He or she must be satisfied on reasonable grounds that at the time the authorisation was given that there was a risk of serious violence to a person or
substantial damage to property, that disrupting data held in the target computer may have helped reduce the risk, and that it was not practicable in the circumstances to apply for a data disruption warrant.

171. Subsection 35B(2) sets out the options available to an eligible Judge or nominated AAT member when they have approved the giving of an emergency authorisation. Under paragraph 35B(2)(a) the Judge or AAT member may issue a warrant for the continued access to and disruption of data held in the computer as if the application for the emergency authorisation were in fact an application for a data disruption warrant under Division 5 of Part 2, provided that the activity that required disruption continues to exist.

172. Paragraph 35B(2)(b) provides that where the Judge or AAT member is satisfied that, since the application for the authorisation was made, the activity which required computer disruption has ceased, the Judge or AAT member can make an order that the access to, and disruption of, data held in the computer cease.

173. Subsection 35B(3) provides the options where the eligible Judge or nominated AAT member decides not to approve the giving of an emergency authorisation under new subsections 28(1C) and 35B(1). In these circumstances, the Judge or AAT member may order that access to, and disruption of, data held in a computer cease altogether. Where the Judge or AAT member believes that the situation did not warrant an emergency authorisation at the time it was issued but that data disruption under Division 5 of Part 2 has now become necessary, the Judge or AAT member may issue a data disruption warrant for subsequent access and disruption. In this case, the application for the approval of the emergency authorisation shall be treated as if it was an application for data disruption warrant under Division 5 of Part 2.

174. Subsection 35B(4) provides that, in any case, the eligible Judge or nominated AAT member may order that any information obtained from or relating to the exercise of powers under an emergency authorisation or any record of that information be dealt with in a manner specified in the order. However, the Judge or AAT member may not order that such information be destroyed because such information, while improperly obtained, may still be required for a permitted purpose, such as an investigation.

**Item 24 – Section 36**

175. This item makes a consequential amendment to reflect the inclusion of new section 35B, differentiating section 35 and 35A from new section 35B within section 36.

**Item 25 – At the end of Part 3**

36A *Relationship of this Part to parliamentary privileges and immunities*

176. New section 36A provides that, to avoid doubt, Part 3 of the SD Act does not affect the law relating to the powers, privileges and immunities of:
a. each House of Parliament

b. the members of each House of the Parliament

c. the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

177. The purpose of this section is to clarify that the provisions relating to emergency authorisations in Part 3 are not intended to intrude on the powers, privileges and immunities of the Parliament.

**Item 26 – Section 41 (paragraph (b) of the definition of appropriate consenting official)**

178. This item makes an amendment to the definition of appropriate consenting official to ensure that this definition applies in relation to foreign consent for the extraterritorial operation of data disruption warrants.

179. This item reflects the inclusion of new sections 43C and 43D which provide for the extraterritorial operation of data disruption warrants, differentiating sections 43A and 43B from new sections 43C and 43D within section 41.

**Item 27 – At the end of Part 5**

**43C Extraterritorial operation of data disruption warrants**

180. Part 5 of the SD Act provides for how surveillance device warrants and computer access warrants operate extraterritorially. If, in the course of an investigation, a law enforcement agency needs to place a surveillance device or access a computer in a foreign country or on a vessel or aircraft beyond Australia’s territorial waters that is registered under the law of a foreign country, the agency must have the permission of a foreign official of that country.

181. This only applies to federal law enforcement officers. State and Territory officers cannot engage in extraterritorial surveillance (section 42 of the SD Act). In this way, extraterritorial surveillance is carried out under an Australian warrant, with the agreement of the foreign State, which ensures that such surveillance and computer access are subject to appropriate accountability and probity measures under domestic law.

182. The same principle will apply to the disruption of data held in a computer in a foreign country or on a vessel or aircraft that is registered under the law of a foreign country and is in waters beyond Australia’s territorial sea. Subsection 43C(1) provides that an eligible Judge or nominated AAT member must not permit a data disruption warrant to authorise extraterritorial access or disruption unless satisfied that this has been agreed to by an appropriate consenting official of the relevant foreign country. The same applies in relation to approvals for the giving of emergency authorisations for disruption of data held in a computer (subsection 43C(2)).
183. For example, before a data disruption warrant is issued, it may become apparent that a suspect has a computer located in Australia and may have data stored overseas, such as in cloud storage or in an email account for which the server is hosted in a foreign country. In this instance, the law enforcement officer conducting the investigation would have to seek the consent of an appropriate foreign official in order for the warrant to be granted.

184. Subsection 43C(3) provides that if a data disruption warrant has already been issued and during the course of executing that warrant it becomes apparent that there will be a need for access to and disruption of data held in a computer in a foreign country (or on a foreign vessel or aircraft) the warrant is taken to permit that access and disruption only if it has been agreed to by an appropriate consenting official of the foreign country. This means that a law enforcement officer does not need to seek a further warrant, or a change in the warrant conditions from the issuing authority, as long as consent from the foreign official has been granted.

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

186. Subsection 43C(4) provides for the circumstances in which the consent of a foreign official is not required notwithstanding the fact that the data may be held in a computer offshore. Where the person executing the warrant is physically present in Australia and the location of the data is unknown, or cannot reasonably be determined, the consent of a foreign official is not required.

187. Subsection 43C(5) stipulates that consent from a foreign official is not required when a vessel or aircraft beyond Australia’s territorial waters is not beyond the outer limits of the contiguous zones of Australia and the access to and disruption of data is for the purpose of a relevant offence that is related to the customs, fiscal, immigration or sanitary laws of Australia. This subsection safeguards Australia’s right to exercise control necessary to prevent infringement of its customs, fiscal, immigration, or sanitary laws and regulations within its territory or territorial sea.

188. Subsection 43C(6) stipulates that consent from a foreign official is not required when a vessel or aircraft beyond Australia’s territorial waters is not beyond the outer limits of the Australian fishing zone and the access to and disruption of data is required in relation to a relevant offence of a certain kind contained in the Fisheries Management Act 1991 or Torres Strait Fisheries Act 1984. This subsection safeguards Australia’s right to exercise the control necessary to prevent infringement on its management and sustainable use of fisheries resources territorial fishing zone.

189. The chief officer of the law enforcement agency to which the applicant belongs or is seconded must, as soon as practicable, give the Minister written evidence that the access to, and disruption of, data has been agreed to by an appropriate consenting official of the foreign country. The chief officer is to provide this evidence of consent as soon as
practicable after the access to, and disruption of, data has commenced under a warrant in a foreign country or on a foreign vessel or aircraft where such consent is required (subsection 43C(7)).

190. An instrument providing evidence to the Minister is not a legislative instrument (subsection 43C(8)). It is administrative rather than legislative in character. It does not determine or alter the law but instead is an instrument relating to a specific situation and serving a specific operational purpose.

191. In circumstances where access to, and disruption of, data is sought on a vessel or aircraft of a foreign country that is in or above the territorial sea of another country, the law enforcement officer must obtain consent from an appropriate consenting official of each foreign country concerned (subsection 43C(9)).

192. Subsection 43C(10) clarifies that there is no requirement to obtain the consent of a foreign official to access, and disrupt, data held in a computer on a vessel or aircraft of a foreign country that is in Australia or in or above waters within the outer limits of the Australian territorial sea.

**43D Evidence obtained from extraterritorial computer access not to be tendered in evidence unless court is satisfied that the evidence was properly obtained**

193. This item also inserts additional subsection 43D that accounts for information obtained under extraterritorial computer access and disruption being tendered as evidence in court.

194. New subsection 43D provides that information obtained under the extraterritorial execution of a data disruption warrant cannot be tendered in evidence unless the court is satisfied that the evidence was properly obtained through the consent of an appropriate official of the foreign country.

**Item 28 – Subsection 44(1) (after paragraph (aa) of the definition of protected information)**

195. Information obtained under, or relating to, powers in the SD Act is protected by restrictions on use, communication and publication in Part 6. This information, defined as ‘protected information’ in section 44, cannot be used and disclosed, except for in certain circumstances which are provided for in section 45.

196. This item provides that information obtained under either a data disruption warrant or under an emergency authorisation for disruption of data held in a computer is ‘protected information’ in the same way that information obtained from the use of a surveillance device or computer access is protected information. General data disruption intercept information is not protected information for the purposes of the SD Act. The use and disclosure of this information is governed by the TIA Act.
Item 29 – Subsection 44(1) (subparagraph (d)(iv) of the definition of protected information)

197. This item amends the protected information provisions to ensure that information obtained purportedly under a computer access warrant or an emergency authorisation for access to data held in a computer in a foreign country, or on a vessel or aircraft of a foreign country and that is in or above the Australian territorial sea, is protected information.

198. This amendment separates the restrictions on the use, communication and publication of protected information collected under a computer access warrant or emergency authorisation for access to data held in a computer in a foreign country, or on a vessel or aircraft of a foreign country, from that collected under a data disruption warrant or emergency authorisation for disruption of data. This is necessary given the different purposes for which a computer access warrant can be sought in comparison to a data disruption warrant, which does not include evidence collection.

Item 30 – Subsection 44(1) (at the end of subparagraph (d)(iv) of the definition of protected information)

199. This item is a consequential amendment allowing paragraph 44(1)(d) to continue to subparagraph 44(1)(d)(v).

Item 31 – Subsection 44(1) (after subparagraph (d)(iv) of the definition of protected information)

200. This item inserts an additional subparagraph to provide that information obtained purportedly under a data disruption warrant or an emergency authorisation for disruption of data held in a computer in a foreign country, or on a vessel or aircraft of a foreign country that is in or above the Australian territorial sea, is protected information.

201. This amendment separates the restrictions on the use, communication and publication of protected information collected under a data disruption warrant or emergency authorisation from other warrants or authorisations in the SD Act. This is necessary given the different purposes for which a data disruption warrant can be sought, which does not include evidence collection.

Item 32 – Subsection 44(1) (paragraph (d) of the definition of protected information)

202. This item is a consequential amendment that clarifies that subsection 44(1)(d) applies to all warrants under the SD Act.

Item 33 – Subsection 44(1) (note to the definition of protected information)

203. This item clarifies that the note pointing to Part 2-6 of the TIA Act for the protection of general computer access interception information is now the first of two notes under subsection 44(1).
Item 34 – Subsection 44(1) (note to the definition of protected information)

204. This item adds a note pointing to Part 2-6 of the TIA Act, which is intended to account for the protection of data disruption intercept information.

Item 35 – After subsection 45(6)

205. This item inserts new subsection 45(6A) to provide that protected information may be communicated by an Ombudsman official to an IGIS official for the purposes of exercising his or her powers, or performing functions or duties as an IGIS official. The intent of this provision is to facilitate information sharing and avoid duplication between the two bodies responsible for oversight of powers in the SD Act.

Item 36 – Paragraph 46(1)(a)

206. This item clarifies that in addition to general computer access intercept information, data disruption intercept information, although not protected information, attracts record keeping requirements. The chief officer of a law enforcement agency must ensure that data disruption intercept information is kept in a secure place that is not accessible to people who are not entitled to deal with that information. He or she must also cause the information to be destroyed as soon as practicable once it is no longer required.

Item 37 – At the end of paragraph 46(2)(ab)

207. This item is consequential to the insertion of subparagraph 46(2)(ac).

Item 38 – After paragraph 46(2)(ab)

208. This item provides that if an agency is not a law enforcement agency but under the use and disclosure provisions receives records or reports obtained by disrupting data held in a computer, the officer in charge of that agency must ensure the same record keeping obligations that apply when dealing with records obtained by using a surveillance device or accessing data held in a computer, also apply in this circumstance. Those record keeping obligations are listed in subsection 46(2).

Item 39 – After section 47A

47B Protection of data disruption technologies and methods

209. This item inserts new section 47B to give protection to sensitive information relating to data disruption technologies and methods by preventing its release into the public domain. This provision recognises that the release of such information in the public domain could harm future capabilities and investigations. Section 47B replicates sections 47 and 47A, which provide the same protections for surveillance technologies and methods and computer access technologies and methods. This section is intended to protect technologies as they develop over time and not to limit law enforcement agencies with an exhaustive list.
210. Subsection 47B(1) provides that a person may object to the disclosure of information on the ground that the information could reasonably be expected to reveal details of data disruption technologies or methods if it were disclosed. It is not intended that section 47B would give protection to simple aspects of data disruption, such as the knowledge that a computer was accessed. The section is designed to protect sensitive technologies and methods that need to be closely held. However, less sensitive technologies and methods are not excluded explicitly from section 47B because it is within the discretion of the person conducting or presiding over the proceeding whether information is of sufficient sensitivity (subsection 47B(2)).

211. Subsection 47B(3) requires that the person deciding whether or not to order information not to be disclosed must take into account whether disclosure of the information is necessary for the fair trial of the defendant and whether it is in the public interest. This ensures that the availability of capability protection for law enforcement is not absolute. The public interest in protecting sensitive operational and capability information must be weighed against the defendant’s right to a fair trial and other public interests.

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

213. Subsection 47B(5) requires the person conducting or presiding over the proceeding to make any order they consider necessary to protect data disruption technologies or methods that have been disclosed from being published. In order to do so, the person must be satisfied that the publication of information could reasonably be expected to reveal details of data disruption technologies and methods. However, this does not apply if doing so would conflict with the interests of justice (subsection 47B(6)).

214. It is appropriate to protect this information without a requirement to consider the harms or that the disclosure of the information would be contrary to the public interest as the disclosure of such sensitive information would be inherently harmful. Law enforcement capabilities are fundamental to ongoing investigations and their ability, including over the long-term, to protect essential public interests, including national security and public safety.

215. Subsection 47B(7) provides the definition of data disruption technologies or methods, as technologies or methods relating to using a computer, a telecommunications facility, any other electronic equipment, or a data storage device, for the purposes of either or both the disruption of data held in a computer, or obtaining access to data held in a computer. These activities must have been deployed in giving effect to a data disruption warrant or an emergency authorisation for disruption of data held in a computer.

216. In this section, a proceeding includes a proceeding before a court, tribunal or Royal Commission.
Item 40 – After subsection 49(2C)

217. This item provides the reporting requirements relating to data disruption warrants and emergency authorisations for disruption of data held in a computer. There is no amendment to subsection 49(1) as the current language applies to data disruption warrants and emergency authorisations for disruption of data held in a computer. That subsection states that the chief officer of a law enforcement agency must make a report to the Minister and give a copy of each warrant and authorisation to the Minister.

218. Subsection 49(2D) lists the requirement of the report. The report must state whether the warrant or authorisation was executed, and if so, state the name of the person primarily responsible for the execution, the name of each person involved in accessing or disrupting data, the period during which the data was accessed or disrupted, the name of any known person whose data was accessed and disrupted, and the location at which the computer was located.

219. The report must also give details of the benefit of the warrant or authorisation in frustrating criminal activity, the details of the access to, and disruption of, data, and the details of compliance with the conditions to which the warrant or authorisation was subject.

220. In the event that the warrant or authorisation was extended or varied, the report must also details regarding the number of extensions and variations must be given, along with the reasons for why they were granted.

Item 41 – After subsection 49B

49C Notification to Ombudsman of things done under a data disruption warrant

221. This item inserts new section 49C which stipulates the circumstances for which the Ombudsman must be notified of things done under a data disruption warrant.

222. Section 49C provides that when a data disruption warrant is issued and a thing mentioned in subsection 27KE(2) was carried out during the warrant, the chief officer of the law enforcement agency that the warrant relates to must notify the Ombudsman that the warrant was issued and that the thing (listed under subsection 27KE(2)) was done. This notification must occur within 7 days of the thing being done. This is an important safeguard for the oversight of conduct carried out under a data disruption warrant and ensuring the conduct is compliant with the provisions set out in the SD Act.

Item 42 – After paragraph 50(1)(ea)

223. This item inserts new paragraph 50(1)(eb) to set out the reporting requirements that the AFP and the ACIC have to meet each financial year when reporting about data disruption warrants in their annual report to the Minister.
224. Under this new paragraph, the AFP and the ACIC must detail the kinds of offences targeted by the data disruption warrants during that financial year. Reporting on the number of data disruption warrants and emergency authorisations for disruption of data that were applied for and issued during that year and the number of applications that were refused and the reason why these were refused, is covered under the existing provisions in section 50.

225. Paragraph 50(1)(eb) specifies that the AFP and the ACIC must only report the kinds of offences being targeted by data disruption warrants issued, not the exact offences disrupted by the warrant. This is an important distinction as it accounts for the fact that while data disruption warrants may be sought for a particular offence suspected of being, or likely to be committed, it can be difficult to identify the exact crimes targeted by the warrant. A data disruption warrant may inadvertently target and frustrate prospective crime through preventing the further continuation of criminal activity.

226. For example, a data disruption warrant sought to disrupt a dark web marketplace selling illicit drugs may not only disrupt the forum selling the drugs, but also the trafficking, distribution, and consumption of those drugs. In the reporting of this warrant, the kind of offence targeted by the data disruption warrant would be the sale of illicit drugs, although the offences disrupted by the warrant may be far more than first intended. Therefore, the requirement to report the kind of offences being targeted is a reasonable requirement for reporting on the outcomes of warrants, whilst also not being too arduous in requiring the AFP and the ACIC to report all offences disrupted following the issue of a data disruption warrant.

**Item 43 – Paragraph 51(b)**

227. This item inserts subsection 27KG(4) into paragraph 51(1)(b) to ensure that the AFP and the ACIC must cause a data disruption warrant instrument of revocation given to the chief officer under subsection 27KG(4) to be kept in the agency’s records. This amendment ensures record keeping requirements for data disruption warrants are in line with surveillance device warrants and computer access warrants in the SD Act.

**Item 44 – At the end of subsection 62(1)**

228. This item inserts new paragraph 62(1)(d) to ensure that the AFP and the ACIC will be able to issue evidentiary certificates in respect of data disruption activities and the handling of data disruption information as they are able to with existing surveillance device warrants and computer access warrants. Evidentiary certificates are intended to streamline the court process by reducing the need to contact numerous officers and experts to give evidence on routine matters. Evidentiary certificates also assist agencies to protect sensitive capabilities.

229. Paragraph 62(1)(a) of the SD Act provides that an appropriate authorising officer, or a person assisting him or her, may issue a written certificate setting out the facts of what has been done by the law enforcement officer or a person providing technical expertise in
connection with the execution of the warrant or the emergency authorisation. The inclusion of data disruption warrants and emergency authorisations for the disruption of data held in a computer within the meaning of ‘warrant’ and ‘emergency authorisation’ under section 6 of the SD Act mean that no amendments are required to paragraph 62(1)(a) in order for an evidentiary certificate for data disruption to be issued under that paragraph.

230. The insertion of paragraph 62(1)(d) provides that an evidentiary certificate may also be issued in respect of anything done by a law enforcement officer in connection with the communication by a person to another person, or the making use of, or the making a record of, or the custody of a record of, information obtained from access to, or disruption of, data under a data disruption warrant or an emergency authorisation for disruption of data held in a computer.

**Item 45 – Subsection 62(3)**

231. This item inserts a reference to section 35B into subsection 62(3) as a consequential amendment to the insertion of new section 35B into the SD Act. Section 35B provides that an eligible judge or nominated AAT member must subsequently approve an emergency authorisation for the disruption of data held in a computer.

232. Subsection 62(2) provides that an evidentiary certificate issued under subsection 62(1) is admissible in evidence in any proceeding as prima facie evidence of the matters stated in the certificate.

233. Subsection 62(3) provides that subsection 62(2) does not apply to a certificate to the extent that the certificate sets out facts with respect to anything done in accordance with an emergency authorisation unless the giving of that authorisation has been approved under sections 35 or 35A following the required application to an eligible judge or nominated AAT member. This ensures that if an emergency authorisation has not been subsequently approved by an eligible Judge or nominated AAT member under those sections, an evidentiary certificate is not considered to be admissible in proceedings as prima facie evidence.

234. The insertion of section 35B into subsection 62(3) will ensure an eligible Judge or nominated AAT member must also approve an emergency authorisations for the disruption of data held in a computer before relevant evidentiary certificates can be admitted in proceedings as prime facie evidence.

**Item 46 – Paragraph 64(2)(a)**

235. This item clarifies that if a person suffers loss or injury as a result of the use of a computer, telecommunications facility, any electronic equipment, or a data storage device, for the purpose of disrupting data held in the computer during a data disruption warrant, the Commonwealth is liable to compensate that person.
236. This is in addition to the existing requirement for the Commonwealth to compensate a person who has suffered loss or injury as a result of a computer, telecommunication facility, any electronic equipment, or a data storage device, for the purpose of obtaining access to data held in a computer.

**Item 47 – After section 64A**

**64B Person with knowledge of a computer or a computer system to assist disruption of data etc.**

237. New section 64B will allow a law enforcement officer of the AFP or the ACIC to apply to an eligible Judge or nominated AAT member for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to access and disrupt data held in a computer subject to a data disruption warrant (subsection 64B(1)).

238. This item ensures that should the AFP or the ACIC be issued a data disruption warrant, they will be able to compel assistance in accessing devices, accessing and disrupting data, copying data, and converting documents. The intent of this provision is not to allow law enforcement to compel assistance from industry, but rather from a person with knowledge of a computer to assist in disrupting data (such as a person who uses the computer).

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

240. For example, the AFP or the ACIC may have been issued a data disruption warrant for the purposes of targeting a user of a child exploitation forum hosted on a web service. In the course of executing the warrant, they become aware of a system administrator who has knowledge of how to access the forum but is not necessarily involved in the conduct on the forum. The AFP or the ACIC could use this knowledge by obtaining an assistance order under new section 64B and compelling the administrator to assist them by providing access. This assistance could then be used to facilitate disruption activities such as a data modification.

241. The Judge or AAT member must be satisfied that it is reasonable and necessary to allow the law enforcement officer to do one or more of four things.

242. Firstly, it may be reasonable and necessary to disrupt data held in a computer that is the subject of a data disruption warrant or an emergency authorisation for disruption of data. Assistance orders cannot be requested or granted without being in support of another warrant or authorisation. They are not stand-alone orders.
243. Secondly, it may be reasonable and necessary to access data that is held in a computer which is the subject of the warrant or authorisation. This is where an assistance order may be useful for access to data, because a person may for example have knowledge of a password, but the assistance order is not necessarily required for the disruption activity.

244. Thirdly, it may also be reasonable and necessary to copy data held in the computer to a data storage device, in order to analyse the data for the purposes of disrupting it under a data disruption warrant or an emergency authorisation.

245. Finally, an assistance order can be applied for when it is reasonable and necessary to seek assistance in order to convert into documentary form or another intelligible form, the data held in a computer that is the subject of data disruption warrant or emergency authorisation, or the data that is held in the data storage device, the copying of which was the subject of an assistance order. This provision is necessary in circumstances where information is encrypted and a person can provide assistance in either giving another version of the information or in decrypting the information.

Grant of assistance order

246. In order to grant an assistance order under section 64B, the issuing authority must be satisfied that the disruption of data held in the computer is likely to substantially assist in frustrating the commission of the offences that are covered by the warrant. Offences are taken to be covered by the warrant if the disruption of data held in a computer is likely to substantially assist in frustrating their commission. The issuing authority must also be satisfied that the disruption of data is justifiable and proportionate having regard to those offences (paragraph 64B(2)(a)).

247. If an assistance order is to be granted in respect of an emergency authorisation, the issuing authority must be satisfied that there is imminent risk of serious violence to a person or substantial damage to property and disrupting the data is immediately necessary to deal with that risk (paragraph 64B(2)(b)).

248. If an assistance order requires a person to provide information or assistance to allow the law enforcement officer to disrupt, access, copy or covert data under a data disruption warrant, the issuing authority must be satisfied that this is for the purpose of determining whether the data is covered by the warrant (paragraph 64B(2)(c)). Data is taken to be covered by the warrant if the disruption of which is likely to substantially assist in frustrating the commission of one or more relevant offences.

249. Similarly, if an assistance order requires a person to provide information or assistance in support of an emergency authorisation, the issuing authority must be satisfied that this is for the purpose of determining whether disrupting data is immediately necessary to deal with an imminent risk of serious violence or substantial damage to property (paragraph 64B(2)(d)).
250. Where the assistance order requires a particular person to provide information or assistance, the person who can be compelled to provide assistance must satisfy certain criteria (paragraph 64B(2)(e)). In a case where the computer is the subject of a data disruption warrant or emergency authorisation, the particular person must be either reasonably suspected of having committed a relevant offence, or the owner or lessee of the computer, or an employee or contracted person of the owner or lessee, or a person who uses or has used the computer, or a person who is or was a system administrator for the computer.

251. The issuing authority may only grant the assistance order if satisfied that the person specified in the order has relevant knowledge of the computer or a relevant computer network, or has relevant knowledge of measures applied to protect data held in the computer (paragraph 64B(2)(f)).

**Offence**

252. Subsection 64B(3) provides that a person commits an offence if that person is subject to an assistance order and is capable of complying with the requirements set out in the order, but omits to do an act and the omission does not comply with the requirement of the order.

253. The penalty for not complying with a request compelling assistance under section 64B is a maximum of imprisonment for 10 years. This reflects the penalty for not complying with an assistance order under section 64 or 64A in relation to surveillance devices or computer access.

254. The offence of failure to comply with an assistance order does not currently, and will not under the proposed legislation, abrogate the common law right to freedom from self-incrimination. Assistance orders do not engage the right because they do not compel individuals to provide evidence against their legal interest. Assistance orders only compel individuals, including the target, to provide access to computers or devices to assist in disruption, in the same manner as a search warrant compels individuals to provide access to a premises to assist in a search.

**Item 48 – Paragraph 65(1A)(a)**

255. Section 65 provides that if there is a defect or irregularity in relation to the warrant or emergency authorisation and, but for that defect or irregularity, the warrant or authorisation would be sufficient authority for the use of a surveillance device or computer access in obtaining information or a record, then the use of the device or computer access is to be treated as valid, and the information or record can be given in evidence.

256. This item inserts ‘data disruption warrant’ to ensure that the same is the case for information or a record obtained through a data disruption warrant or an emergency authorisation, were a defect or irregularity to be found.
Item 49 – After subsection 65(1A)

257. This item ensures that if data was disrupted pursuant to a data disruption warrant or an emergency authorisation, and a defect or irregularity to be found, the warrant or authorisation is still taken to be valid if, but for that defect or irregularity, the warrant or authorisation would be sufficient authority for disrupting the data. This ensures that in such circumstances, the disruption of data is taken to be valid as if the warrant or authorisation did not have that defect or irregularity.

Item 50 – Subsection 65(2)

258. This item ensures that subsection 65(2) now applies to defects and irregularities in relation to data disruption warrants and emergency authorisations, in addition to surveillance device warrants and emergency authorisations and also to computer access warrants and emergency authorisations.

Item 51 – After section 65B

65C Evidence obtained from access to, or disruption of, data under a data disruption warrant etc.

259. This item inserts an additional subsection into section 65B which governs the use of information obtained under a data disruption warrant as evidence.

260. This item provides that nothing in the SD Act prevents evidence that has been obtained under a data disruption warrant or emergency authorisation from being deemed admissible as evidence in a proceeding relating to a relevant offence.

Telecommunications (Interception and Access) Act 1979

Item 52 – Subsection 5(1)

261. This item inserts two new definitions into section 5(1) of the TIA Act.

262. Data disruption interception information is the information obtained under a data disruption warrant by means of intercepting a communication in transit over a telecommunications system as permitted by paragraph 27KE(2)(h). The permissible uses of data, information and records obtained through data disruption are governed by the SD Act. This definition is referred to in section 6 of the SD Act.

263. Interception under a data disruption warrant may only occur for the purposes of executing or facilitating the warrant. This is to ensure that where agencies are seeking to obtain intercept material for its own purpose, they must apply for, and be issued with, an interception warrant under Chapter 2 of the TIA Act.

264. Data disruption warrant has the same meaning as in the SD Act. Section 27KC of the SD Act allows an eligible Judge or nominated AAT member to issue a data disruption warrant, upon he or she being satisfied of the relevant conditions, including that there are
reasonable grounds for the suspicion that the disruption of data held in the target computer is likely to substantially assist in frustrating the commission of one or more relevant offences.

Item 53 – Subsection 5(1) (at the end of the definition of restricted record)

265. This item amends the definition of restricted record so that it does not include records of data disruption intercept information, just as it does not include records of general computer access intercept information. This ensures that records of data disruption intercept information are dealt with differently to records otherwise obtained by means of interception.

Item 54 – Subsection 5(1) (paragraph (b) of the definition of warrant)

266. This item expands the definition of warrant in Chapter 2 of the TIA Act to now include data disruption warrants. The effect of this amendment is that interception for the purposes of data disruption warrants is not prohibited by the TIA Act as it constitutes interception under a warrant (paragraph 7(2)(b)).

Item 55 – Paragraph 7(2)(bb)

267. This item amends subsection 7(2)(bb) of the TIA Act to include reference to new subsection 27KE(9) of the SD Act. New subsection 27KE(9) allows a law enforcement officer to do anything reasonably necessary to conceal the fact that anything has been done under a data disruption warrant in the SD Act, including intercepting a communication (paragraph 27KE(9)(h)).

268. This item ensures that the interception of a communication to conceal access under a data disruption warrant pursuant to subsection 27KE(9) of the SD Act is permitted under the TIA Act.

Item 56 – After section 63AC

63AD Dealing in data disruption intercept information etc.

269. Existing subsection 63(1) sets out a general prohibition on the use, recording and communication of lawfully intercepted information. Information is taken to be lawfully intercepted if it was obtained by intercepting a communication passing over a telecommunications system under a warrant. This includes a data disruption warrant.

270. This item inserts new section 63AD to provide two exceptions to the general prohibition on dealing in data disruption intercept information.

271. Subsection 63AD(1) allows a person to communicate to another person, make use of, make a record of, or give in evidence in a proceeding data disruption intercept information for the purposes of doing a thing authorised by the warrant. The intention is that
intercepted information can be used or communicated for a purpose reasonably incidental to the purposes of carrying out data disruption.

272. Subsection 63AD(2) allows a person to communicate to another person, make use of, or make a record of data disruption intercept information if the information relates to the involvement, or likely involvement, of a person in certain activities. Information may be communicated, used or recorded if it relates to the involvement of a person in activities that, generally, are life threatening or emergency situations. These include:

- where there is a significant risk to a person’s safety
- where a person is acting for or on behalf of a foreign power
- where there is a threat to security
- where there is a risk posed to the operational security of intelligence agencies
- where a person is involved in activities related to the proliferation of weapons of mass destruction, or
- where a person is involved in activities related to a contravention of a UN sanction enforcement law.

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

274. New subsection 63AD(3) states that a person may communicate to an Ombudsman official, make use of, or make a record of, data disruption intercept information in connection with the performance by the Ombudsman official of his or her functions or duties or the exercise by an Ombudsman official of his or her powers.

275. Similarly, an Ombudsman official may communicate to another person, make use of, or make a record of, data disruption intercept information in connection with the performance of his or her functions or duties or the exercise of his or her powers (subsection 63AD(4)).

276. New subsection 63AD(5) states that a person may communicate to an IGIS official, make use of, or make a record of, data disruption intercept information in connection with the performance by the IGIS official of his or her functions or duties or the exercise by an IGIS official of his or her powers.

277. Similarly, an IGIS official may communicate to another person, make use of, or make a record of, data disruption intercept information in connection with the performance of his or her functions or duties or the exercise of his or her powers (subsection 63AD(6)).

278. New subsection 63AD(7) provides for the circumstances in which information was obtained by intercepting a communication passing over a telecommunications system, and
the interception was purportedly for the purposes of doing a thing specified in a data disruption warrant, but the interception was not authorised by the warrant. If such circumstances were to exist, then a person may communicate to an Ombudsman or IGIS official, make use of, or make a record of, that information in connection with the respective exercise of powers, or performance of functions or duties, by the Ombudsman or IGIS official. Similarly, an Ombudsman or IGIS official may communicate to another person, make use of, or make a record of, that information in connection with the exercise of his or her respective powers, or performance of his or her respective functions.

279. New subsection 63AD(8) provides that an Ombudsman or IGIS official does not bear an evidential burden in relation to the above matters in a prosecution for an offence against section 63 of the TIA Act despite subsection 13.3(3) of the Criminal Code.

**Item 57 – Paragraph 67(1)(a)**

280. Existing paragraph 67(1)(a) provides that an officer of an agency may communicate, make use of, or make a record of, lawfully intercepted information for a permitted purpose.

281. This item ensures that, just as with general computer access intercept information, data disruption intercept information is not able to be communicated, made use of, or recorded for these purposes.

**Item 58 – Section 68**

282. Under section 68, the chief officer of an agency may communicate lawfully intercepted information under certain circumstances.

283. This item ensures that this does not apply in relation to data disruption intercept information in addition to general computer access intercept information.

**Item 59 – Subsection 74(1)**

284. Under section 74, a person may give lawfully intercepted information in evidence in an exempt proceeding (within meaning of section 5B). An exempt proceeding is a proceeding in which evidence obtained under the powers in the TIA Act may be given.

285. This item ensures that a person may not give data disruption intercept information in evidence in such a proceeding.

**Item 60 – Subsection 75(1)**

286. Under section 75, a person may give information that has been intercepted in contravention of the prohibition in subsection 7(1) in evidence in an exempt proceeding under certain circumstances where there is a defect or irregularity with a warrant.

287. This item ensures that a person may not give data disruption warrant intercept information in evidence in an exempt proceeding in these circumstances.
Item 61 – Paragraphs 77(1)(a) and (b)

288. Section 77 provides that intercepted material is inadmissible in evidence in so far as the relevant exceptions do not apply.

289. This item provides that intercept material is admissible in evidence in so far as new section 63AD permits. New section 63AD permits the dealing of data disruption intercept information where very serious circumstances exist or where there is a purpose reasonably incidental to the purposes of carrying out data disruption.

Item 62 – After paragraph 108(2)(cb)

290. This item inserts new paragraph 108(2)(cc) which provides an exception to the prohibition in subsection 108(1) on accessing a stored communication. The prohibition does not apply to accessing a stored communication under a data disruption warrant.

Schedule 2 – Network activity warrants

Part 1 – Main amendments

Surveillance Devices Act 2004

Item 1 – After paragraph 3(aab)

291. This item amends the purposes of the SD Act to reflect the new power in the Act for the AFP and the ACIC to access data held in computers for intelligence collection purposes, a network activity warrant. It adds as a purpose the establishment of procedures for the AFP and the ACIC to obtain warrants that authorise access to data held in computers where that data will substantially assist in the collection of intelligence that relates to criminal networks of individuals.

Item 2 – After subsection 4(4B)

292. This item inserts new subsection 4(4C) to put beyond doubt that a warrant may be issued under this Act for access to data held in a computer in relation to the collection of intelligence that relates to a criminal network of individuals. This replicates the clarification in existing subsections 4(4) and (4A) relating to warrants and emergency authorisations regarding the use of a surveillance device and access to data held in a computer as authorised by a computer access warrant.

Item 3 – Subsection 6(1)

293. This item inserts definitions for terms that facilitate the operation of the new network activity warrant provisions.

294. Criminal network of individuals is defined to have the meaning given by section 7A. Section 7A provides that a criminal network of individuals is a group of individuals who
are an electronically linked group of individuals. One or more individuals in the group must have either engaged, are engaging, or are likely to engage, in conduct that constitutes a relevant offence, or have facilitated, are facilitating, or are likely to facilitate another person’s engagement, in conduct that constitutes a relevant offence.

295. The person whose engagement in criminal activity was facilitated by an individual in the group, may or may not be an individual in the group themselves. Relevant offence retains its existing meaning as set out in section 6 of the Act, being an offence punishable by a maximum term of imprisonment of 3 years or more, or certain other offences as listed.

296. A key consideration in applying for a network activity warrant is suspicion on reasonable grounds that a group of individuals is a criminal network of individuals. The meaning of a criminal network of individuals is described in further detail below.

297. An *electronically linked group of individuals* is a group of at least two individuals. Each individual in the group must either use the same electronic service or communicate electronically, or do both, with at least one other individual in the group. The individuals in the group may also be likely to do one or both of these things. The terms ‘electronic service’ and ‘electronic communication’ are defined separately in the SD Act.

298. An electronically linked group of individuals is an important concept in the meaning of a criminal network of individuals. In applying for a network activity warrant, a group of individuals may be a criminal network of individuals if the individuals are electronically linked (see section 7A).

299. An electronically linked group of individuals may be using a shared internet service in common, or may have established their own secure communications networks in order to communicate and conduct their activities. Whilst the number and identity of the group of individuals may not be known, there must be a link between two or more people who meet or communicate electronically.

300. *Electronic communication* is defined broadly to mean a communication of information by means of guided and/or unguided electromagnetic energy. The communication may be in the form of text, data, speech, music or other sounds, visual images (animated or otherwise), or in any other form or combination of forms. This term has the same meaning as in Part 9.9 of the Criminal Code.

301. An electronically linked group of individuals may mean a group of at least two individuals who communicate with at least one other individual in the group by electronic communication. This could include, for example, a group of individuals engaging with one another by exchanging text messages or images on a messaging platform, such as WhatsApp or Telegram.

302. *Electronic service* has the same meaning as in the *Telecommunications Act 1997*. In that Act, electronic service means a service that either allows end-users to access material using a carriage service, or, a service that delivers material to persons having equipment.
appropriate for receiving that material, where the delivery of the service is by means of a carriage service. This does not include a broadcasting service, or a datacasting service (as defined in the *Broadcasting Services Act 1992*).

303. This definition is intended to account for the online platforms and databases that provide online delivery or access to materials via a carriage service. Examples of an electronic service would be a website, social media platform or online gaming service as it relies on carriage services to enable access to, and delivery of, content.

304. An electronically linked group of individuals may mean a group of at least two individuals, where each individual uses the same electronic service. This would capture situations where a person accesses a website at a particular time, but does not necessarily interact or communicate with other people who have accessed the website. For example, this might involve logging in to a chat room and viewing the conversations without actively participating.

305. The definition of *network activity warrant* is a warrant issued under section 27KM. Section 27KM allows an eligible Judge or nominated AAT member to issue a warrant, upon being satisfied of the relevant conditions set out in subsection 27KM(1), including that there are reasonable grounds for the suspicion that access to data will substantially assist in the collection of intelligence that relates to a criminal networks of individuals and is relevant for the prevention, detection or frustration of a relevant offence.

306. *Network activity warrant intercept information* is defined to have the same meaning as in the TIA Act. A definition of this new term has been inserted into the TIA Act to mean information obtained under a network activity warrant by intercepting a communication passing over a telecommunications system. This is distinct from data obtained under a network activity warrant.

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

308. Information may be intercepted under a network activity warrant if authorised by an eligible Judge or nominated AAT member and only for the purpose of doing any thing specified in the network activity warrant (paragraph 27KP(2)(h)). The definition of ‘network activity warrant intercept information’ has been included to differentiate this information from protected network activity warrant information.

309. Protected network activity warrant information means information obtained under, or relating to, a network activity warrant that is not network activity warrant intercept information. Network activity warrant intercept information is not protected information for the purposes of the SD Act. Consistent with other information obtained by interception, the provisions for dealing with network activity warrant intercept information
are in the TIA Act.

310. **Protected network activity warrant information** is defined to have the meaning given by section 44A. Section 44A provides that protected network activity warrant information means any information (other than network activity warrant intercept information) obtained under, or relating to, a network activity warrant. This includes any information that is likely to enable the identification of a person, object or premises specified in a network activity warrant.

311. Protected information in the SD Act is subject to the restrictions on the use, communication and publication of information in Division 1 of Part 6. The inclusion of this definition is necessary to distinguish protected network activity warrant information from other protected information in the SD Act. This ensures that protected network activity warrant is subject to different requirements to other protected information. Given that this information was obtained via intelligence collection it is important that this information is dealt with differently to information obtained under a traditional evidence gathering power.

**Item 4 – Subsection 6(1) (definition of remote application)**

312. This item amends the definition of **remote application** in the SD Act to include a reference to new section 27KL. New section 27KL allows applications for network activity warrants to be made remotely if it is impractical for the application to be made in person. Remote applications for network activity warrants may be made in the same way and for the same reasons as for computer access warrants under section 27B.

**Item 5 – Subsection 6(1) (definition of unsworn application)**

313. This item includes references to provisions in relation to new network activity warrants within the existing definition of **unsworn application** in the SD Act. Subsections 27KK(5) and (6) allow applications for network activity warrants to be made before an affidavit is prepared or sworn in certain circumstances. Unsworn applications for network activity warrants may be made in the same way and for the same reasons as for computer access warrants under subsections 27A(13) and (14).

**Item 6 – Subsection 6(1) (at the end of the definition of warrant)**

314. This item expands the existing definition of **warrant** in the SD Act to include the new network activity warrant.

**Item 7 – At the end of subsection 10(1)**

315. This item expands the existing types of warrant that may be issued under Part 2 of the SD Act to include network activity warrants. This is consequential to the insertion to
Division 6 of Part 2 of the SD Act which establishes the framework for the AFP and the ACIC to obtain network activity warrants.

Item 8 – After section 7

7A Criminal network of individuals

316. This item inserts new section 7A which sets out the meaning of a criminal network of individuals. The meaning of a criminal network of individuals is relevant for the purposes of obtaining a network activity warrant under new Division 6 of Part 2. A key consideration in applying for a network activity warrant under new section 27KK is suspicion on reasonable grounds that a group of individuals is a criminal network of individuals.

317. Subsection 7A(1) provides that a criminal network of individuals is a group of individuals who are linked electronically (the meaning of this term is defined at subsection 6(1)). One or more individuals in the group must have engaged, are engaging, or are likely to engage in conduct that constitutes a relevant offence, or have facilitated, are facilitating, or are likely to facilitate, another person’s engagement in conduct that constitutes a relevant offence. The person whose engagement in criminal activity was facilitated by an individual in the group, may or may not be an individual in the group themselves.

318. There is no requirement that every individual who is part of the criminal network is himself or herself committing, or intending to commit, a relevant offence. The word ‘facilitating’ is used to capture those individuals who are, knowingly or unknowingly, facilitating engagement by another person in conduct constituting a relevant offence as defined in section 6 of the SD Act.

319. For example, a criminal network of individuals may include an individual who owns an IT platform that is, without the knowledge of that person, being exploited by a criminal organisation for illegal purposes. It will sometimes be necessary for agencies to collect intelligence on the devices used by unwitting or incidental participants in the criminal network in order to determine the full scope of offending and the identities of offenders. However, this does not include accessing the devices of third parties who are not connected to the criminal network in any way.

320. The definition of a criminal network of individuals does not require that individuals within the group consider themselves members, or that the group is formalised sufficiently to have a membership. This ensures that organised groups will be captured by the definition, as well as circumstances where individuals are not coordinated in any way, and do not have knowledge of each other’s activities or existences, but are still electronically linked (as per the definition in section 6) and engaging in or facilitating conduct that constitutes a relevant offence. For example, a criminal network of individuals may be persons accessing an illicit dark web marketplace where they are unlikely to consider themselves as members, but rather customers, such as people who are paying to view the live streaming
of child exploitation material. In this case, what is providing the link that makes these people a ‘criminal network’ is the shared electronic service, the dark web marketplace that each person has accessed or signed up to.

321. The effect of paragraphs 7A(2)(a) and (b) is that the identities of the individuals in the group or the details of relevant offences likely to be engaged in or facilitated do not have to be known for a group of individuals to be considered a criminal network of individuals. This makes clear that, in applying for a network activity warrant, the agency does not need to know the identities of the individuals of the group, or the details of a relevant offence that is taking place or likely to take place. This reflects the purpose of the network activity warrant in enabling intelligence to be collected about offences and offenders, before there is enough specific information to obtain an evidence-gathering warrant such as a surveillance device warrant or computer access warrant.

322. For example, a criminal network of individuals might involve a group of individuals engaging in or facilitating in terrorist activity constituting offences punishable by 3 years imprisonment or more. Terrorist activity may involve, for example, recruiting for a terrorist organisation, advocating terrorism, associating with a terrorist organisation and financing terrorism. There is no requirement to know exactly what offences are occurring, or by whom. This is because a network activity warrant is intended to allow for the collection of intelligence about the commission of such offences at the initial stages of an investigation or without an investigation, rather than to gather evidence to prove the exact nature of the offending.

323. Paragraph 7A(2)(c) provides that it is immaterial whether there are likely to be changes, from time to time, in the composition of the group. The effect of this provision is that the composition of the group that makes up the criminal network of individuals may fluctuate over time and the total number of individuals in the group may also increase and decrease. Any individual who joins, remains or leaves the network is still considered to form part of the criminal network of individuals. This is intended to account for the changeable nature of criminal networks, and the likelihood that individuals will enter and exit the group to evade detection.

Item 9 – At the end of Part 2

Division 6 – Network activity warrants

324. This item introduces Division 6 to Part 2 of the SD Act. Division 6 establishes the framework for the AFP and the ACIC to obtain network activity warrants. A network activity warrant enables the AFP and the ACIC to collect intelligence against groups suspected on reasonable grounds of being a criminal network of individuals – for example, where individuals are exchanging child abuse material over a common platform, or they are an organised syndicate engaged in a variety of criminal offences. A network activity warrant will authorise access to data held in computers used by the individuals in the
criminal network, even if agencies have not ascertained the precise identities or locations of individuals or target computers.

325. These warrants are in addition to warrants for data surveillance devices and computer access warrants, which allow for certain activities for the purpose of enabling evidence to be obtained of the commission of relevant offences or the identity or location of the offenders.

27KK Application for a network activity warrant

326. New section 27KK sets out the threshold tests for making an application for a network activity warrant. As network activity warrants are an intelligence collection power, this test borrows from the test for issue of a computer access warrant under section 25A of the ASIO Act. Section 25A of the ASIO Act provides that the Attorney-General can only issue a computer access warrant if he or she is satisfied that there are reasonable grounds for believing that access to data held in a computer by ASIO will substantially assist the collection of intelligence in respect of a matter that is important in relation to security.

327. The chief officer of the AFP or the ACIC, may apply for the issue of a network activity warrant. In the case of the AFP, this will be the AFP Commissioner. In the case of the ACIC, this will be the CEO of the ACIC. This is distinct from the level of officer able to apply for the issue of surveillance device warrants and computer access warrants in the SD Act. The senior level of officer able to apply for a network activity warrants reflects the purpose of the warrant as an intelligence collection power.

328. Section 63 of the SD Act provides that the chief officer of a law enforcement agency may, by writing, delegate to a member of the staff of the agency who is an SES employee or a person of equivalent rank, all or any of the chief officer’s powers or functions. Should a chief officer delegate his or her power to apply for a network activity warrant in accordance with section 63, the delegate SES employee, or person of an equivalent rank, may apply for the issue of a network activity warrant.

329. New section 27KK contains a two part test that must be satisfied in order to apply for a network activity warrant.

330. First, the chief officer of the AFP or the ACIC must suspect on reasonable grounds that a group of individuals is a criminal network of individuals (within meaning of section 7A). A group of individuals must be electronically linked (as per the definition in section 6). One or more individuals in the group must have either engaged, are engaging, or are likely to engage, in conduct that constitutes a relevant offence, or have facilitated, are facilitating, or are likely to facilitate another person’s engagement, in conduct that constitutes a relevant offence. Relevant offence retains its existing meaning as set out in section 6 of the Act, being an offence punishable by a maximum term of imprisonment of 3 years or more, or certain other offences as listed. The meaning of a criminal network of individuals is described in further detail at section 7A.
331. There are two limbs of the second test which the applicant must be satisfied. Firstly, the applicant must suspect on reasonable grounds that access to data held in the target computer that is, from time to time, used or likely to be used, by any of the individuals in the group will substantially assist in the collection of intelligence that relates to the group or any of the individuals in the group.

332. The term ‘target computer’ is defined in subsection 27KK(7). In this context, the concept of the target computer is intended to capture the computers used, or likely to be used, by the criminal network of individuals in relation to which the warrant is sought. This will capture multiple linked computers, a number of which may be used by an individual, given the variety of computers and electronically devices commonly used. While a network activity warrant will be sought for access to data held in the target computer, the target computer or its location does not need to be identified at the time of application (subsection 27KK(2)(b) and (d)).

333. The language ‘from time to time’ is intended to capture the computers used, or likely to be used, by individuals in the group at any time while the warrant is in force. This phrase recognises that criminals will often use multiple computers to conduct their illegal activity. Criminals will often continually interchange the devices used or abandon a used device and start using a new one, as a means to conceal their criminal activities. The inclusion of ‘from time to time’ ensures that a network activity warrant can be used to target computers used, or likely to be used, by a criminal network of individuals as these computers change over time.

334. Secondly, the collection of intelligence, must be relevant to the prevention, detection or frustration of one or more kinds of relevant offences. The reason for this specification in subparagraph 27KK(1)(b)(ii) is that the collection of intelligence must be relevant for the purposes of agencies’ existing functions in responding to relevant offences. The effect of this provision is that the collection of intelligence must be linked to the prevention, detection or frustration of relevant offences, it cannot be for any other purposes that would constitute a ‘fishing expedition’ or otherwise fall within the remit of the ASIO or an intelligence agency empowered under the IS Act. For example, the collection of intelligence under a network activity warrant could not be in relation to a matter that is prejudicial to security as this would fall within the remit of the ASIO.

335. Subsection 27KK(2) accounts for the fact that, at the time of seeking the warrant, the number of individuals (and computers) making up the criminal network of individuals will likely be unknown, as will likely be the identity of future participants. As such, in applying for a network activity warrant, the agency does not have to know the identities of each person (paragraph 27KK(2)(a)), or be able to identify or locate the computers (paragraphs 27KK(2)(b) and (c)) from which access to data is sought. These warrants will be used to target the computers used by the individuals in the criminal network as they change from time to time, as opposed to the group being determined at the time of application (paragraph 27KK(2)(d)). Over the life of the warrant, new persons may join
the network by accessing the same electronic service or communicating electronically with the existing participants. These associates will also be covered by the original warrant.

336. For example, an agency may be aware that a number of people are using a bespoke encrypted device that is frequently, or exclusively, used by organised crime members to facilitate criminal activity and has very few, if any, legitimate purposes. The agency is unlikely to know in advance of seeking a warrant the identities of all the individuals making up the criminal network of individuals. However, the use of a network activity warrant will enable agencies to target these devices and collect intelligence about offences and offenders, before there is enough specific information to seek an evidence-gathering warrant, such as a surveillance device warrant or computer access warrant.

337. At the time of applying for a network activity warrant, the individuals’ identities, the target computers and their location, and the composition of the group, do not have to be known. However, the application must provide clear characteristics or identifiers that permit the eligible Judge or nominated AAT member to discern (and include in the warrant discernible parameters around) the criminal network of individuals, and that access to data will substantially assist in the collection of intelligence.

Procedure for making applications

338. New subsections 27KK(3) and (4) set out the procedure for making an application for a network activity warrant. An application for a network activity warrant may be made to an eligible Judge or nominated AAT member.

339. An eligible Judge is a person who is a Judge of a court and has consented to be declared an eligible Judge by the Attorney-General, as the Minister responsible for administering the Judiciary Act 1903 (section 12). The functions and powers of Judges are conferred only in a personal capacity and not as a court or a member of a court. A nominated AAT member is a person who is either the Deputy President, senior member or member of the AAT, and has been nominated by the Attorney-General, as the Minister responsible for administering the Administrative Appeals Tribunal Act 1975 (section 13).

340. The application must specify the name of the applicant and the nature and duration of the warrant sought, and be supported by an affidavit setting out the grounds on which the warrant is sought. This procedure is identical to the procedure for making an application for a computer access warrant under section 27A.

341. An application for a network activity warrant should seek to provide as much information as necessary for the issuing authority to be satisfied that there are reasonable grounds for the suspicion founding the application for the warrant while keeping sensitive capabilities and operational matters appropriately protected. The affidavit could include, for example, the category of offences to which the information sought to be obtained under the warrant relates (for example, terrorism offences, without needing to specify particular terrorism offences), the reason for suspecting that criminal activity is being conducted by the
criminal network of individuals, the value of the information expected to be revealed by the data acquired under the warrant, and the procedures the agency has in place to minimise the likelihood that the data of innocent third parties will be affected.

342. The application may also specify the criminal network of individuals that is the subject of the warrant, and the expected boundaries of the criminal network. This could include, for example, information about the geographical boundaries over which the network will extend, and the suspected size of the network. The network activity warrant must specify the criminal network of individuals to which the warrant relates (see subparagraph 27KN(1)(b)(iii)).

343. As network activity warrants will be used to target a network of unknown persons engaging in or facilitating criminal activity, an application may be sought by reference to the communications methodology employed that forms the link in the network. Network activity warrant applications may be used to target, for example, “persons suspected of participating in criminal activity ‘X’ using communications service ‘Y’”. This could include people using a particular messaging platform to participate in the sharing or live streaming of child abuse material, or plan to import a particular drug consignment. Associates conducting criminal activity through use of an online discussion forum or chatroom, a file hosting service or a command and control service would also be captured. Another example is a bitcoin network, where people are suspected of using a digital currency account to finance terrorism or launder money.

Unsworn applications

344. Subsections 27K(5) and (6) provide for applications for network activity warrants to be made before an affidavit is prepared or sworn in circumstances where the chief officer believes that immediate access to data is necessary, and it is impracticable for an affidavit to be prepared or sworn before an application is made. This allows for external scrutiny of judgements made by chief officers that an application could not be made in person or that an affidavit could not be sworn in time. In such circumstances, the applicant must send a duly sworn affidavit to a Judge or AAT member no later than 72 hours after the making of the application.

Target computer

345. Network activity warrants are sought for access to data held in the target computer. The definition of target computer should be read in conjunction with the definition of ‘computer’ in the SD Act. Section 6 of the SD Act provides that a computer may be one or more, or any combination of, computers, computer systems, or computer networks.

346. The target computer must be a computer that is from time to time used by, or likely to be used by, an individual, the identity of whom may or may not be known. Pursuant to paragraph 27KK(1)(b), the computer must be used by, or likely to be used by, one or more of the individuals in the criminal network. The word ‘must’ is used to clarify that
use by an individual is a requirement for the target computer, in contrast with ‘may’ which indicates that the following particulars are not required in every circumstance. The target computer may, in addition to being used by an individual, be a particular computer or a computer that is from time to time on a particular premises. For example, the target computer may also be ‘an iPhone 8, serial number ‘X’ used by suspected criminal ‘Y’’, or ‘all computers used by criminal organisation ‘X’ at location ‘Y’.’

347. The concept of the target computer in relation to network activity warrants is intended to capture the computers used, or likely to be used, by the criminal network of individuals in relation to which the warrant is sought. This will capture multiple linked computers, a number of which may be used by an individual, given the variety of computers and electronically devices commonly used. While a network activity warrant will be sought for access to data held in the target computer, the target computer or its location does not need to be identified at the time of application (subsection 27KK(2)(b) and (d)).

27KL Remote application

348. A remote application for a network activity warrant may be made in the same way and for the same reasons that a remote application for a computer access warrant may be made under section 27B. New section 27KL permits the application for a network activity warrant to be made under section 27KK by telephone, fax, email or by other means of communication where the chief officer believes that it is impracticable for the application to be made in person. For remote applications, the issuing authority must also be satisfied that it was impracticable for the application to have been made in person.

27KM Determining the application

349. New section 27KM makes provision for the conditions under which an eligible Judge or nominated AAT member may issue a network activity warrant. New section 27KM is modelled on the current section 27C for computer access warrants.

350. Before issuing a network activity warrant, the eligible Judge or nominated AAT member must be satisfied that there are reasonable grounds for the suspicion founding the application for the warrant. This will provide for external scrutiny of the same matters in relation to which the chief officer had a reasonable suspicion in applying for the warrant (see subsection 27KK(1)). It is important to ensure judicial oversight for the issuing of a network activity warrant as the information obtained under the network activity warrant may be used to make out the grounds for suspicion for an application for another warrant. Judicial oversight will provide for external scrutiny of the warrant application and satisfaction of reasonableness and proportionality.

351. For unsworn applications, the eligible Judge or nominated AAT member must be satisfied that it would have been impractical for an affidavit to have been sworn or prepared before the application was made. Similarly, in relation to applications made remotely, the eligible Judge or nominated AAT member must be satisfied that it would have been
impractical for the application to have been made in person. This allows for external scrutiny of judgments made by officers that an affidavit could not be sworn in time or an application could not be made in person.

352. Subsection 27KM(2) sets out the considerations which an issuing authority must have regard to in determining whether a network activity warrant should be issued. Consideration of the below matters ensures that a network activity warrant may only be issued where an issuing authority finds it reasonable, proportionate and necessary.

353. The issuing authority must have regard to the nature and gravity of the conduct constituting the kinds of offences targeted (paragraph 27KM(2)(a)). This should involve consideration of the seriousness of the offences targeted, and the scope of the conduct constituting the kinds of offences targeted.

354. The issuing authority must take into account the extent to which access to data will assist in the collection of intelligence that relates to the criminal network of individuals and is relevant to the prevention, detection or frustration of one or more kinds of offences (paragraph 27KM(2)(b)). This will require the issuing authority to make an assessment on the extent to which the warrant is necessary for purposes in which it was sought (see paragraph 27KK(1)(b)).

355. The issuing authority must also consider the likely intelligence value of any information sought to be obtained under the warrant (paragraph 27KM(2)(c)). This should involve consideration of the likely utility of the information to be obtained under the warrant in forming an intelligence picture of the operation of criminal networks online.

356. The issuing authority must also have regard to whether the things authorised by the warrant are proportionate to the likely intelligence value of the information sought to be obtained (paragraph 27KM(2)(d)). For example, the issuing authority may weigh the seriousness of the offending that the applicant has set out as being the relevant offence, against the scope and size of the network sought to be uncovered.

357. As the purpose of the network activity warrant is target discovery, agencies are unlikely to know in advance the identity or location of the offenders involved in the commission of offences to which the warrant sought relates. Accordingly, the applicant may not be able to assess in advance the extent to which privacy is likely to be impacted as a result of the warrant. This will make it difficult for the issuing authority to assess the privacy impact in determining the application for a warrant to a sufficient degree.

358. The issuing authority must also consider the existence of any alternative or less intrusive means of obtaining the information sought to be obtained (paragraph 27KM(2)(e)). This will involve consideration of whether a network activity warrant is the most appropriate power for achieving the intent of the warrant. If there is another less intrusive power available, for example a computer access warrant or surveillance device warrant may under the circumstances be considered less intrusive as they may be more narrowly
targeted, the agency should seek this warrant instead. Network activity warrants should only be sought if they are the most appropriate means available in the circumstances.

359. The issuing authority must take into account the extent to which the execution of the warrant is likely to result in access to data of persons who are lawfully using a computer. Consideration of this matter ensures that an application for a network activity warrant must meet a test of proportionality. Access to the data refers to any actions whereby data can be viewed or collected. Data of persons will include access codes, downloadable or shareable content, usernames or credentials, location identifiers, and device specifics (like electronic code). However, encrypted and anonymised data does not constitute data of persons as it is unable to be identified as directly relating or belonging to that person.

360. During the execution of a network activity warrant, it is possible that access to the data of persons not likely to be members of the criminal network or those that are lawfully using a computer may occur. For example, if an innocent third party is using a server to store data and that same server is being used by a criminal network to sell illicit drugs, the data of persons not likely to be members of the criminal network may be accessed during the life of the warrant. The issuing authority must have regard for the risk that data of persons not subject to the warrant may be accessed, and be of the view that should access to data belonging to persons not connected with a criminal network occur, this is proportionate and necessary for the purpose of executing the warrant.

361. The issuing authority must also have regard to any previous warrant sought or issued in relation to the criminal network that is the subject of the warrant.

362. These considerations are modelled on the conditions for issue of a computer access warrant (subsection 27C(2)), but take into account the fact that when executing a network activity warrant, an agency may need to access a large number of unknown devices used by a criminal network. For network activity warrants, the privacy considerations and their proportionality to the relevant offending need to differ from those taken into account when issuing other warrants under the SD Act. This is due to the nature of a network activity warrant as an intelligence collection tool, unlike the other warrants available in the SD Act.

363. Subsection 27KM(3) provides that where a network activity warrant is issued, the chief officer of the relevant agency must notify the IGIS within 7 days of the warrant is issued. This provision is important to assist oversight by the IGIS by making a requirement to notify the body when network activity warrants have been issued or exercised. The chief officer is also required to notify the IGIS if a network activity has been extended or varied (see subsection 27KQ(7)) or revoked (see subsections 27KR(6) and (7)). Similar notification provisions can be found in relation to the ASIO’s use of the industry assistance provisions in Part 15 of the Telecommunications Act 1997.
27KN What must a network activity warrant contain?

364. Subsection 27KN(1) sets out the information a network activity warrant is to contain. A network activity warrant must state that the eligible Judge or nominated AAT member is satisfied that there are reasonable grounds for the suspicion founding the application for the warrant (subsection 27KM(1)) and has had regard to the considerations for issue at subsection 27KM(2).

365. Network activity warrants must also contain the name of the applicant, the kinds of relevant offences in respect of which the warrant is issued, the criminal network of individuals to which the warrant relates, the date the warrant is issued, the period during which the warrant is in force, and the name of the law enforcement officer primarily responsibility for executing the warrant. A network activity warrant must also specify any conditions subject to which things may be done under the warrant.

366. Paragraph 27KN(1)(c) provides for certain additional matters that must be specified in the warrant if the warrant authorises the use of a surveillance device. In these circumstances, the warrant must also specify the surveillance device authorised to be used and the purpose for which the surveillance device may be used under the warrant. The surveillance device authorised to be used may be a data surveillance device, listening device, optical surveillance device or tracking device. A surveillance device may only be used for the purposes of doing any thing authorised by the network activity warrant, for example, entering premises to obtain access to a computer (paragraph 27KP(2)(a)). These purposes must be specified in the warrant.

367. A network activity warrant may only be issued for a period of no more than 90 days (subsection 27KN(2)). This is consistent with the period in which a computer access warrant may be in effect (subsection 27D(3)). The warrant must also be signed by the person issuing it, and include the person issuing the warrant’s name (subsection 27KN(3)).

368. Subsection 27KN(4) clarifies that a criminal network of individuals may be specified by identifying one or more matters or things that are sufficient to identify the criminal network of individuals. For example, a criminal network of individuals may be specified in the warrant as “persons suspected of participating in criminal activity ‘X’ using communications service ‘Y’”. This could include people participating in the sharing of child abuse material on a particular forum, or people participating in a plan to import a drug consignment using a particular messaging platform. This description will be sufficient to identify the criminal network of individuals, while also being sufficiently broad enough to capture individuals in the group as they change over time.

369. Subsection 27KN(5) provides that the issuing authority must, as soon as practicable after completing and signing a warrant issued on a remote application, inform the applicant of the terms of the warrant, and the date and time at which the warrant was issued. The
issuing authority must also give the warrant to the applicant while retaining a copy of the warrant for his or her own record.

27KP What a network activity warrant authorises

370. A network activity warrant authorises the doing of specified things in relation to the relevant target computer or computers subject to any conditions or restrictions specified in the warrant. This ensures that any things authorised under the warrant must be done in relation to the target computer (or computers), as the object of the warrant. This is modelled on the provisions for what a computer access warrant authorises under section 27E.

371. Subsection 27KP(2) sets out the things that may be specified provided that the eligible Judge or nominated AAT member considers it appropriate in the circumstances. The word ‘may’ is used to clarify that all of the particulars in paragraphs 27KP(2)(a)-(j) are not required in every circumstance.

372. Under paragraph 27KP(2)(a) the issuing authority may specify premises that may be entered for the purpose of doing things mentioned in this subsection. Installation and retrieval of a device to access networks and computers may not always be performed remotely, and may involve some entry onto property. Paragraph 27KP(2)(b) makes it clear that premises other than the premises specified in a warrant (that is, third party premises) can be entered for the purpose of gaining access to or exiting the subject premises for the purposes of executing the network activity warrant. This may occur where there is no other way to gain access to the subject premises (for example, in an apartment complex where it is necessary to enter the premises through shared or common areas). In line with the covert nature of surveillance, it would in many circumstances not be appropriate to notify a third party before the execution of a network activity warrant could take place as there may be significant risks to capabilities and methodology, and risks to operations if third parties were required to be notified.

373. Under paragraph 27KP(2)(c) the issuing authority may specify in the warrant that the warrant permits using the target computer, using a telecommunications facility operated or provided by the Commonwealth or a carrier, using any other electronic equipment or using a data storage device, for the purpose of obtaining access to data that is held in the target computer, in order to determine whether the relevant data is covered by the warrant. Data is covered by the warrant if access to the data will substantially assist in the collection of intelligence that relates to a criminal network of individuals and is relevant to the prevention, detection or frustration of one or more kinds of offences (subsection 27KP(5)).

374. The intent of this provision is to ensure that data that is unknown or unknowable at the time the warrant has been issued can be discovered by using other means, in order to determine whether it is covered by the warrant. Access to a secondary device, such as a USB key, for example, may be necessary in order to determine whether any data relevant
to an investigation is held in any of the target computers. This would include access to any external storage devices, such as cloud-based data or any back-ups on other devices. Other electronic equipment might also include specialist communications equipment used within telecommunications transmittal devices.

375. Network activity warrants may authorise access to multiple connected devices that are used by the criminal network of individuals for the purposes of engaging in criminal activity at any point during the life of the warrant. Paragraph 27KP(2)(c) makes clear by the words ‘held in the target computer at any time while the warrant is in force’ that networks activity warrants authorise ongoing access to data held in any of the target computers over the life of the warrant. Data does not have to be stored on any of the target computers, but can be passing through them.

376. This allows the AFP and the ACIC to access any devices that are, or have been, connected to the criminal network of individuals, even after they have disconnected, provided that the issuing authority considers it appropriate in the circumstances. It will often be the case that individuals, after having downloaded child exploitation material on their device, will disconnect from other participants including by ceasing interaction and communication, as a means of masking their activity. This inclusion of this provision ensures that the AFP and the ACIC will continue to be able to access these devices, despite them having disconnected from the criminal network, for the duration of the warrant.

377. Paragraph 27KP(2)(d) permits adding, coping, deleting or altering other data if necessary to obtain access to data held in any of the target computers in order to determine whether the data is covered by the warrant. Data may need to be copied and analysed before its relevancy or irrelevancy to the warrant can be determined.

378. Paragraph 27KP(2)(e) allows the use of any other computer or a communication in transit to access relevant data if it is reasonable in all the circumstances, having regard to other methods of obtaining access to the data. This ensures that the AFP and the ACIC can use a third party computer or a communication in transit to access relevant data. In recognition of the potential privacy implications for third parties, the eligible Judge or nominated AAT member must have regard to any other method of obtaining access to the relevant data which is likely to be as effective. The eligible Judge or nominated AAT member must consider this before authorising the use of a third party’s computer under a network activity warrant. This consideration does not require agencies to have exhausted all other methods of access but rather ensures that the issuing authority must take into account the circumstances before him or her and balance the impact on privacy against the benefit to the intelligence operation.

379. Using a communication in transit means accessing any communication passing between the target device and the service provided, as long as this access does not amount to interception. Permissible incidental interception is provided for in paragraph 27KP(2)(h).
380. A network activity warrant may also authorise adding, copying, deleting or altering other data in the computer or communication in transit. The power to add, copy, delete or alter other data can only be used where necessary for the purpose of obtaining access to relevant data held in any of the target computers. This provision recognises that in some cases direct access to any of the target computers will be difficult or even impossible. The use of third party computers and communications in transit to add, copy, delete or alter data in the computer or the communication in transit may facilitate that access (subparagraph 27KP(e)(ii)).

381. The ability to copy information, including third-party data, is essential to be able to conceal the execution of a network activity warrant. The IGIS will be a key oversight mechanism in the use of this power. It will be within the purview of the IGIS to examine agencies’ copying of any third-party data and subsequent use. The ability to copy third-party data acknowledges the operational realities of executing highly technical capabilities such as those deployed under a network activity warrant.

382. Paragraph 27KP(2)(f) allows the removal of a computer or other thing from the premises for the purposes of executing the warrant, and returning the computer or other thing once it is no longer required. A computer may need to be removed from premises to allow law enforcement to analyse, or obtain access to, the data held on it. This provision also permits the removal, for example, of a USB key, a remote access token, or a password written on a piece of paper, from the premises, along with the computer.

383. Paragraph 27KP(2)(g) allows for the copying of any data which has been accessed if it either appears relevant for the purposes of determining whether the relevant data is covered by the warrant or is covered by the warrant. Data that is subject to some form of electronic protection is taken to be relevant for the purposes of determining whether it is relevant data covered by the warrant (subsection 27KP(4)). Data is covered by the warrant if access to the data will substantially assist in the collection of intelligence that relates to a criminal network of individuals and is relevant to the prevention, detection or frustration of one or more kinds of offences (subsection 27KP(5)). This provision ensures that data either accessed on a computer remotely or accessed on a computer at the premises specified in the warrant can be copied onto another computer. This will allow data to be analysed on a different computer located elsewhere or using different software. This provision will also be necessary to enable the collection of intelligence.

384. Paragraph 27KP(2)(h) permits intercepting a communication passing over a telecommunication system, if the interception is for the purposes of doing anything specified in the warrant in accordance with subsection 27KP(2). Often it will be necessary for the AFP or the ACIC to intercept communications for the purpose of executing a network activity warrant. This subsection ensures that they will be able to do so, but only for those limited purposes of making a network activity warrant practicable or technically possible.
385. A network activity warrant cannot authorise the collection of evidence or intelligence by interception. If agencies require interception other than to facilitate a network activity warrant, they must seek an interception warrant from an eligible Judge or nominated AAT member under the TIA Act.

386. Paragraph 27KP(2)(i) allows a network activity warrant to authorise the use of a surveillance device for the purposes of doing any thing specified in the warrant. It will often be necessary for law enforcement to use a surveillance device while executing a network activity warrant in order to make the things authorised by the warrant possible or to maintain the covert nature of the warrant. For example, the use of an optical surveillance device may be necessary in order to surveil a premises before entering under paragraph 27KP(2)(a) to ensure that the warrant may be executed covertly.

387. The inclusion of this provision is necessary as it may not always be possible for law enforcement to seek a surveillance device warrant and network activity warrant concurrently as the threshold tests for application are not aligned. Similar to permissible interception under paragraph 27KP(2)(h), a network activity warrant cannot authorise the collection of evidence or intelligence by using a surveillance device.

388. Paragraph 27KP(2)(j) allows a network activity warrant to authorise the doing of anything reasonably incidental to any of the things specified in paragraphs 27KP(2)(a) to (i).

389. The note after 27KP(2)(j) clarifies that a person who obtains access to data stored in a computer by using a telecommunication facility will not commit an offence under Part 10.7 of the Criminal Code or equivalent State or Territory laws if the person acts within the authority of the warrant. Part 10.7 of the Criminal Code provides for the Commonwealth computer offences.

390. Subsection 27KP(3) provides for the return of a computer or other thing that was removed under a network activity warrant in accordance with paragraph 27KP(2)(f). Subsection 27KP(3) provides that where a warrant authorised the removal of a computer or other thing from premises, and the computer or other thing is so removed from the premises, then the computer or thing must be returned to the premises within a reasonable period.

391. Subsection 27KP(4) stipulates that data that is subject to some form of electronic protection is taken to be relevant for the purposes of determining whether it is relevant data covered by the warrant (subsection 27KP(5) in association with paragraph 27KP(2)(g)). This is to provide for circumstances where there is a form of encryption or other form of electronic protection on data and because of that protection the data is not immediately in a readable format, and cannot be assessed for relevance.

When data is covered by a warrant

392. Subsection 27KP(5) clarifies that data is covered by the warrant if access to the data will substantially assist in the collection of intelligence that relates to a criminal network of individuals and is relevant to the prevention, detection or frustration of one or more kinds
of relevant offences. Many of the things that may be authorised by a network activity warrant may be done in order to determine whether data is covered by the warrant, and so would assist in the collection of intelligence. This provision also replicates paragraph 27KK(2) to clarify that the composition of the criminal network of individuals that is the subject of the warrant may change during the period in which the warrant is in force.

Certain acts not authorised

393. Subsection 27KP(6) has the same effect as subsection 27E(5) in relation to computer access warrants which was modelled on the provisions in subsection 25A(5) of the ASIO Act. A network activity warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to the limitation has been included so that an agency may undertake such actions where they are otherwise necessary to execute the warrant.

394. Paragraph 27KP(6)(b) clarifies that a network activity warrant does not authorise the doing of such things if it is likely to cause any other material loss or damage to other persons lawfully using a computer.

395. A network activity warrant cannot be used to disrupt or deny a service to a computer, even where that computer is being used for illegal purposes. Network activity warrants are intelligence collection tools and are not intended to enable agencies to engage in disruption without the requisite warrant or authority in place.

Warrant must provide for certain matters

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

Concealment of access etc.

397. Subsection 27KP(8) provides that a network activity warrant will also authorise the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to a computer under a network activity warrant. Subsection 27E(7) makes the same provision in relation to computer access warrants. Likewise, under paragraph 25A(4)(c) of the ASIO Act, an ASIO computer access warrant authorises the doing of anything reasonably necessary to conceal the fact that anything has been done under the warrant.

398. Concealment of access is essential for preserving the effectiveness of covert warrants like the network activity warrant. Paragraphs 27KP(8)(d) and (e) also authorise the entering of
premises where the computer that has been accessed is located, or premises for gaining entry or access to where the computer is located, for the purposes of concealing the action that has been taken.

399. A network activity warrant may also authorise removing the computer or another thing from a place where it is situated, and returning it, for the purpose of concealing access (paragraph 27KP(8)(f)). The ability to temporarily remove a computer from the premises is important in situations where an agency may have to use specialist equipment to access the computer but cannot for practical reasons bring that equipment onto the premises in a covert manner.

400. In some instances it will be necessary to retrieve a physically implanted computer access device from a computer in order for the access to be concealed. Doing anything reasonably necessary for concealment as envisaged by paragraph 27KP(8)(c) includes retrieving such a device.

401. This structure acknowledges the importance of ensuring that agencies have the ability to determine when access to premises or to a planted device will best ensure the operation remains covert. It will not always be possible to predict when safe retrieval of a device can be performed without compromising an intelligence operation.

402. Paragraph 27KP(8)(g) authorises the use of a third party computer or communication in transit to conceal access under a network activity warrant, including, if necessary, adding, copying, deleting or altering of other data in the computer or communication in transit. This is important in maintaining the covert nature of a network activity warrant as indications that access has been enabled may need to be deleted or disguised by further data modification.

403. Paragraph 27KP(8)(h) permits the interception of a communication passing over a telecommunication system for the purpose of doing any thing to conceal access to data under a network activity warrant.

404. Similarly, paragraph 27KP(8)(i) allows the use of a surveillance device for the purpose of doing any thing to conceal access to data under a network activity warrant.

405. Paragraph 27KP(8)(j) allows a network activity warrant to authorise any other thing reasonably incidental to any of the things specified in 27KP(8)(a) to (i).

406. Paragraphs 27KP(8)(k) and (l) provide that concealment activities may be done at any time while the warrant is in force, or within 28 days after it ceases to be in force, or at the earliest time after this period at which it is reasonably practicable to do so.

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

408. Subsection 27KP(9) clarifies that the concealment of access provisions do not authorise the same activities that are not authorised under a network activity warrant in subsection 27KP(6).

409. Subsection 27KP(9) does not authorise for the material interference with, interruption or obstruction of a communication in transit, or the lawful use by other persons of a computer for the purpose of concealing access. An exception to the limitation has been included so that an agency may undertake such actions in 27KP(9) where they are otherwise necessary to execute the warrant and conceal access. Paragraph 27KP(9)(b) does not authorise the doing of such things if it is likely to cause any other material loss or damage to other persons lawfully using a computer.

410. Subsection 27KP(10) specifies that if a computer or another thing is removed from a place, it must be returned within a reasonable period.

27KQ Extension and variation of network activity warrant

411. Section 27KQ allows the AFP Commissioner or CEO of the ACIC to apply at any time while the warrant is in force for an extension of the warrant or a variation of any of its terms. The warrant can only be extended for a period not exceeding 90 days after the day the warrant would otherwise expire but for the extension. This builds flexibility into the warrant process and accounts for extended investigations and unexpected circumstances.

412. The application must be made to an eligible Judge or nominated AAT member (paragraph 27KQ(2)). Paragraph 27KQ(4) provides that the issuing authority must consider the same matters required to issue a network activity warrant at first instance (see subsection 27KM(2)) and be satisfied that the grounds on which the application for the warrant was made still exist (see subsection 27KM(1)).

413. Paragraph 27KQ(3) specifies that the same provisions which provide for applications for network activity warrants apply in relation to applications for variations and extensions. This ensures that any varied specifications are within the bounds of what might have been authorised in a network activity warrant in the first instance. The warrant cannot authorise the addition, deletion or alteration of data that interferes with a person’s use of a computer unless it is necessary for the purposes of the warrant.

414. Subsection 27KQ(7) provides that, if a network activity warrant is extended or varied, the chief officer of the relevant agency must notify the IGIS within 7 days after the extension or variation is issued. This provision is important to assist oversight by the IGIS by making a requirement to notify the body when network activity warrants have been extended or varied. This requirement is in addition to the requirement to notify the IGIS that a network activity warrant has been issued (subsection 27KM(3)) or revoked (subsections 27KR(6) and (7)).
This section does not prevent the issue of a further applications for variation or extension (subsection 27KQ(6)).

27KR Revocation of network activity warrant

Section 27KR sets out the provisions for revoking a network activity warrant. A network activity warrant may be revoked by an eligible Judge or nominated AAT member, by instrument in writing. The Judge or AAT member may revoke the warrant on their own initiative at any time before the warrant expires. If the warrant is revoked and the officer executing the warrant is already in the process of executing the warrant, the officer does not have any civil or criminal liability for actions done before he or she is made aware of the revocation (subsection 27KR(5)).

The chief officer of the agency to which the network activity warrant was issued must revoke the warrant if satisfied that access to data under the warrant is no longer required for the purpose for which the warrant was sought (subsection 27KR(2) in accordance with subsection 27KS(2)).

The instrument of revocation must be signed by the person revoking the warrant, either the eligible Judge or nominated AAT member of the chief officer of the AFP or the ACIC (subsection 27KR(3)). If the warrant is revoked by an eligible Judge or nominated AAT member he or she must give a copy of the revocation instrument to the chief officer of the relevant agency to which the warrant was issued (subsection 27KR(4)).

Subsections 27KR(6) and (7) provides that, the IGIS must be notified within 7 days of a warrant being revoked. This provision is important to assist oversight by the IGIS by making a requirement to notify the body when network activity warrants have been revoked. The chief officer is also required to notify the IGIS if a network activity has been issued (see subsection 27KM(3)) or extended or varied (see subsection 27KQ(7)). Similar notification provisions can be found in relation to ASIO’s use of the industry assistance provisions in Part 15 of the Telecommunications Act 1997.

27KS Discontinuance of access under warrant

Section 27KS provides for the circumstances in which access under a network activity warrant must be discontinued.

Scope

Subsection 27KS(1) provides that this section relating to discontinuance of access under a warrant only applies if a network activity warrant is issued.

Discontinuance of access

Subsection 27KS(2) places an obligation on the chief officer of the AFP or the ACIC to take steps to discontinue access to data under a network activity warrant where he or she
is satisfied that the grounds on which the warrant was issued (as set out in paragraph 27KK(1)(b)) cease to exist. Access to data under a network activity warrant must be discontinued if the chief officer of the relevant agency is no longer satisfied that access to data will substantially assist in the collection of intelligence that relates to the criminal network of individuals and is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

423. Subsection 27KS(3) complements section 27KR in that the chief officer must, as soon as practicable after being made aware that an issuing authority has revoked the network activity warrant, take steps to discontinue access to data authorised by that warrant. This does not include discontinuing access to the data that has already been collected by virtue of the warrant. Further access to data after the revocation must be discontinued, but the agency will still be able to use the existing holdings that that agency has obtained under the warrant whilst it was in force.

424. Subsection 27KS(4) places an obligation on the law enforcement officer who is primarily responsible for executing the warrant to immediately inform the chief officer if there is a change in circumstances affecting the warrant. Upon being informed of the change in circumstances by the executing officer, the chief officer of the relevant agency may have obligations under section 27KS(2) to revoke the warrant and take steps to ensure that access to data authorised by the warrant is discontinued.

27KT Relationship of this Division to parliamentary privileges and immunities

425. New section 27KT provides that, to avoid doubt, Division 6 does not affect the law relating to the powers, privileges and immunities of:

   a. each House of Parliament

   b. the members of each House of the Parliament

   c. the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

426. The purpose of this section is to clarify that the provisions relating to network activity warrants in Division 6 of Part 2 are not intended to intrude on the powers, privileges and immunities of the Parliament.

Item 10 – Section 41 (paragraph (b) of the definition of appropriate consenting official)

427. This item amends the definition of appropriate consenting official in section 41 to reflect the inclusion of new section 43E. An appropriate consenting official is an official of a foreign country with the authority to give consent to either use surveillance devices in that country or on a vessel or aircraft of that country, or to access data held in computers in that country or on a vessel or aircraft. The effect of this provision is to ensure that the
The concept of an appropriate consenting official applies in relation to the extraterritorial operation of network activity warrants in new section 43E.

**Item 11 – At the end of Part 5**

**43E Extraterritorial operation of network activity warrants**

428. Before the issue of a network activity warrant, it may become apparent that an agency needs to access data held in a computer in a foreign country or on a vessel or aircraft that is registered under the law of a foreign country and is in waters beyond Australia’s territorial sea. For example, a group of individuals may be using a number of computers in Australia with data stored overseas, such as in cloud storage or in an email account for which the server is hosted in a foreign country. Subsection 43E(1) provides that in such circumstances the applicant must seek the consent of an appropriate foreign official in order for the warrant to be granted.

429. Subsection 43E(2) provides that if a network activity warrant has already been issued and during the course of executing that warrant it becomes apparent that there will be a need for access to data held in a computer in a foreign country (or on a foreign vessel or aircraft) the warrant is taken to permit that access only if it has been agreed to by an appropriate consenting official of the foreign country. This means that the chief officer does not need to seek a further warrant, or a variation of the warrant conditions from the issuing authority, as long as consent from the foreign official has been granted.

430. Subsection 43E(3) provides for the circumstances in which the consent of a foreign official is not required notwithstanding the fact that the data may be held in a computer offshore. Where the person executing the warrant is physically present in Australia and the location of the data is known, or cannot reasonably be determined, the consent of a foreign official is not required.

431. Subsection 43E(4) stipulates that consent from a foreign official is not required when a vessel or aircraft beyond Australia’s territorial waters is not beyond the outer limits of the contiguous zones of Australia and the access to data is for the purpose of a relevant offence that is related to the customs, fiscal, immigration or sanitary laws of Australia. The intent of this provision is to safeguard Australia’s right to exercise control necessary to prevent the infringement of its customs, fiscal, immigration or sanitary laws and regulations within its territory or territorial sea.

432. Subsection 43E(5) stipulates that consent from a foreign official is not required when a vessel or aircraft beyond Australia’s territorial waters is not beyond the outer limits of the Australian fishing zone and the access to data is required in relation to a relevant offence of a certain kind contained in the *Fisheries Management Act 1991* or *Torres Strait Fisheries Act 1984*. The intent of this provision is to safeguard Australia’s right to exercise the control necessary to prevent infringement and sustainable use of fisheries resources territorial fishing zone.
433. The chief officer of the agency to which the applicant belongs or is seconded must, as soon as practicable, give the Minister written evidence that the access to data has been agreed to by an appropriate consenting official of the foreign country. The chief officer is to provide this evidence of consent as soon as practicable after the access to data has commenced under a warrant in a foreign country or on a vessel or aircraft where such consent is required (subsection 43E(6)).

434. An instrument providing evidence to the Minister is not a legislative instrument (subsection 43E(7)). It is administrative rather than legislative in character. It does not determine or alter the law but instead is an instrument relating to a specific situation and serving a specific operational purpose.

435. In circumstances where access to data is sought on a vessel or aircraft of a foreign country that is in or above the territorial sea of another country, the chief officer must obtain consent from an appropriate consenting official of each foreign country concerned (subsection 43E(8)).

436. Subsection 43E(9) clarifies that there is no requirement to obtain the consent of a foreign official to access data held in a computer on a vessel or aircraft of a foreign country that is in Australia or in or above waters within the outer limits of the Australian territorial sea.

Item 12 – Subsection 44(1) (paragraph (a) of the definition of protected information)

437. Information obtained pursuant to evidence gathering powers in the SD Act is protected by restrictions on use, communication and publication in Part 6. The Act operates by first defining that information as ‘protected information’ under section 44, prohibiting the use and disclosure of that information in certain circumstances under section 45, and providing for some exceptions.

438. This item amends paragraph 44(1)(a) to provide that information obtained from the use of a surveillance device under a network activity warrant (as permitted by paragraph 27KP(2)(i)) does not constitute ‘protected information’ for the purposes of the SD Act. This ensures that information obtained under a surveillance device in the execution of a network activity warrant is dealt with differently to information obtained under a surveillance device warrant. The inclusion of this provision is necessary as the use of a surveillance device under a network activity warrant cannot be used to circumvent the need to obtain the appropriate warrant under section 14.

Item 13 – Subsection 44(1) (subparagraph (b)(i) of the definition of protected information)

439. This item amends subparagraph 44(1)(b)(i) to provide that any information obtained from access to data under a network activity warrant does not constitute ‘protected information’ for the purposes of the SD Act. The inclusion of this provision is necessary because the information obtained under a network activity warrant is intelligence and therefore must be subject to different use and disclosure rules to other information obtained under evidence gathering powers in the SD Act. Information obtained from
access to data under a network activity warrant is governed by the use and disclosure provisions in new section 45B.

Item 14 – Subsection 44(1) (paragraph (c) of the definition of protected information)

440. This item amends paragraph 44(1)(c) to provide that any information that is likely to enable the identification of a person, object or premises specified in a network activity warrant does not constitute ‘protected information’ for the purposes of the SD Act. This ensures that this type of information is dealt with differently for network activity warrants than it is for surveillance device warrants and computer access warrants. Information that is likely to enable the identification of a person, object or premises specified in a network activity warrant is governed by the use and disclosure provisions in new section 45B.

Item 15 – Subsection 44(1) (subparagraph (d)(i) of the definition of protected information)

441. This item amends subparagraph 44(1)(d)(i) to provide that any other information obtained by a law enforcement officer without the authority of a network activity warrant does not constitute ‘protected information’ for the purposes of the SD Act. This ensures that this type of information is dealt with differently for network activity warrants than it is for surveillance device warrants and computer access warrants. Information obtained without the authority of a network activity warrant is governed by the use and disclosure provisions in new section 45B.

Item 16 – Subsection 44(1) (subparagraph (d)(iii) of the definition of protected information)

442. This item amends subparagraph 44(1)(d)(iii) to provide that any information obtained by a law enforcement officer by using of a surveillance device in a foreign country (or vessel or aircraft of a foreign country) under a network activity warrant without the consent of a foreign official does not constitute ‘protected information’ for the purposes of the SD Act. This ensures that information obtained under a surveillance device in the execution of a network activity warrant is dealt with differently to information obtained under a surveillance device warrant.

Item 17 – Subsection 44(1) (paragraph (d) of the definition of protected information)

443. This item amends paragraph 44(1)(d) to provide that any other information obtained by a law enforcement officer in contravention of a network activity warrant does not constitute ‘protected information’ for the purposes of the SD Act. This ensures that this type of information is dealt with differently for network activity warrants than it is for surveillance device warrants and computer access warrants. Information obtained by a law enforcement officer in contravention of a network activity warrant is governed by the use and disclosure provisions in new section 45B.
Item 18 – After section 44

44A What is protected network activity warrant information?

444. This item inserts new section 44A which provides for the meaning of protected network activity warrant information. This item is required in order to distinguish protected network activity warrant information from protected information (such as that obtained under a computer access warrant) as already provided for in the Act. New section 44A replicates the structure of section 44 which sets out the meaning of protected information but in relation to computer access warrants. Protected network activity warrant information is subject to a different use and disclosure framework (set out in new section 45B), as it is information obtained under an intelligence collection power rather than the evidence gathering powers for investigations that already exist in the SD Act.

445. Protected network activity warrant information includes any information, that is not network activity warrant intercept information, obtained under a network activity warrant, information obtained from the use of a surveillance device under a network activity warrant, and information relating to a network activity warrant, including the application, issue, existence or expiration of the warrant.

446. The meaning of protected network activity warrant information also includes any information that is likely to enable the identification of a criminal network of individuals, an individual in a criminal network of individuals, or a computer or premises specified in the network activity warrant.

447. This definition also includes any other information obtained by a law enforcement officer without the authority of a network activity warrant, or where information was obtained extraterritorially without a foreign official’s consent, in contravention of the requirement for a network activity warrant.

448. Such information will be subject to the prohibitions on the use, recording, communication or publication of information in subsections 45B(1) and (2).

449. The note at the end of section 44A clarifies that network activity warrant intercept information is governed by Part 2-6 of the TIA Act (see Part 2 of Schedule 2).

Item 19 – After section 45A

45B Prohibition on use, recording, communication of publication of protected network activity warrant information or its admission in evidence

450. New section 45B creates two offences with respect to the unlawful use, recording, communication, publication or admission of evidence of protected network activity warrant.
451. Subsection 45B(1) makes it an offence if a person uses, records, communicates or publishes protected network activity warrant information in a manner that is not permitted by one of the exceptions in this section. The penalty for this offence is two years imprisonment. This offence is in line with the offence for the unlawful use, recording, communication or publication of protected information under existing subsection 45(1).

452. Subsection 45B(2) makes it an offence if a person uses, records, communicates or publishes protected network activity warrant information in a manner that is not permitted by one of the exceptions in this section, and the use, recording, communication or publication endangers the health or safety of any person, or prejudices the effective conduct of an investigation into a relevant offence. The penalty for this offence is ten years imprisonment. A higher penalty is applicable with respect to this offence because it is an aggravated offence. This offence is in line with the offence for the unlawful use, recording, communication or publication of protected information under existing subsection 45(2).

453. Protected network activity warrant information may not be admitted in evidence unless permitted by one of the relevant exceptions in this section (subsection 45B(3)). Further, the prohibitions on the use, recording, communication or publication of protected network activity warrant information, or its admission in evidence, do not apply if there is a relevant exception that applies.

454. Subsection 45B(4) provides for a set of circumstances, not directly related to law enforcement, for which protected network activity warrant information may be lawfully used, recorded, communicated or published. These provisions are an exception to the prohibition of the use, recording communication or publication of protected network activity warrant information, or its admission in evidence in subsections 45B(1), (2) and (3).

455. Paragraph 45B(4)(a) provides that protected network activity warrant information may be used, recorded, communicated or published in connection with the administration or execution of the SD Act. This allows for the effective administration and execution of the network activity warrant provisions.

456. Paragraph 45B(4)(b) provides that where protected network activity warrant information has been disclosed in proceedings in open court, the subsequent use, recording, communication or publication will not constitute an offence provided that the disclosure in court was lawful in the first place.

457. Paragraph 45B(4)(c) provides that the use or communication of protected network activity warrant information is permitted, if the use or communication is by a person who believes on reasonable grounds that it is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property. Such a person need not necessarily be a law enforcement officer.
458. The communication of protected network activity warrant information to the Director-General of Security (paragraph 45B(4)(d)) or an agency head of an agency empowered under the *Intelligence Services Act 2001* (paragraph 45B(4)(e)) will not constitute an offence if the information relates or appears to relate to the functions of the relevant organisation. In the case of ASIO, the information must relate or appear to relate to activities prejudicial to security (within meaning of the ASIO Act.)

459. Protected network activity warrant information that relates or appears to relate to the functions of ASIO may be used, recorded or communicated by the Director-General of Security, an ASIO employee or an ASIO affiliate in the performance of their official functions (subparagraph 45B(4)(f)(i)). Similarly, protected network activity warrant information that relates or appears to relate to the functions of an intelligence agency may also be used, recorded or communicated by the agency head or a member of staff of the intelligence agency in the performance of their official functions (subparagraph 45B(4)(f)(ii)).

460. To clarify, where paragraph 45B(4)(f) refers to protected network activity warrant information referred to in paragraphs 45B(4)(d) and (e), this means information that relates or appears to relate to any matter within the functions of the relevant agency, not to information communicated to the agency head under those paragraphs. This is an important distinction as information may be communicated to ASIO or an intelligence agency through a provision other than paragraphs 45B(4)(d) and (e). For example, this information may be communicated to ASIO or an intelligence agency if necessary to help or prevent the risk of serious violence to a person under paragraph 45B(4)(b).

461. Subsection 45B(5) provides for a set of circumstances, more closely related to law enforcement activities, for which protected network activity warrant information (other than information that was obtained under a surveillance device) may be lawfully used, recorded, communicated, published or admitted in evidence. Information that was obtained by use of a surveillance device under a network activity warrant may only be used, recorded, communicated or published for the purposes set out in subsection 45B(7). This information cannot be used for intelligence purposes, or for making an application for another warrant.

462. Protected network activity warrant information may be lawfully used, recorded, communicated or published if necessary for collecting, correlating, analysing or disseminating criminal intelligence in the performance of the AFP’s functions set out in section 8 of the AFP Act (paragraph 45B(5)(a)). The AFP’s functions include providing police services to assist or cooperate with a foreign law enforcement or intelligence agency (paragraph 8(1)(bf) of the AFP Act). This provision will allow protected network activity warrant information to be used or disclosed if necessary for this purpose.

463. Similarly, this information may be used, recorded, communicated or published for the purposes of the ACIC collecting, correlating, analysing or disseminating criminal
intelligence in the performance of the functions set out in section 7A of the ACC Act (paragraph 45B(5)(b)).

464. This information may also be used, recorded, communicated or published for the purposes of the AFP and the ACIC making reports in relation to criminal intelligence (paragraph 45B(5)(c)).

465. Paragraphs 45B(5)(d), (e) and (f) allow for the use, recording, communication or publication of protected network activity warrant information for the making of an application for a warrant, variation of a warrant or extension of a warrant. This is intended to include the deliberation process for making a warrant, such as the gathering of materials to support that warrant. These provisions allow protected network activity warrant information to have derivative use by permitting this information to be cited in an affidavit on application for another investigatory power, such as a computer access warrant.

466. In these provisions, the term ‘warrant’ is taken to have its ordinary meaning and is not taken to mean a surveillance device warrant, retrieval warrant or computer access warrant (as defined in subsection 6(1)) (see subsection 45B(6)). The effect of this provision is to allow protected network activity warrant information to be used, recorded, communicated or published for the purposes of making an application for any warrant, not only the warrants contained in the SD Act.

467. Paragraph 45B(5)(g) provides that protected network activity warrant information may be used, recorded, communicated or published for the purposes of the keeping of records and the making of reports by the AFP and the ACIC in accordance with the obligations imposed by Division 2 of Part 6. The inclusion of this provision is necessary to ensure that the AFP and the ACIC are able to comply with the reporting and record-keeping requirements set out in Division 2 of Part 6.

468. Protected network activity warrant information may be used, recorded, communicated or published for the purposes of an IGIS official exercising powers or performing functions or duties as an IGIS official (within the meaning of subsection 6(1)) (paragraph 45B(5)(h)). The inclusion of this provision is necessary in order to facilitate the IGIS exercising powers and performing functions or duties in relation to the agency’s oversight of network activity warrants.

469. Paragraphs 45B(5)(i) and (j) ensure that protected network activity warrant information may be used, recorded, communicated or published in an investigation or proceeding relating to an offence against the prohibition on the use, recording, communication or publication of protected network activity warrant information in subsections 45B(1) and (2). This provision ensures that where a person has unlawfully used or disclosed protected network activity warrant information, he or she may be effectively investigated and prosecuted for the offence. The effect of this provision is that the penalties for the
unauthorised use, recording, communication or publication of protected network activity warrant information can be properly enforced.

470. Subsection 45B(7) provides for the purposes in which information obtained from the use of a surveillance device under a network activity warrant may be used, recorded, communicated or published. It is important that information obtained by using a surveillance device under a network activity warrant must be dealt with differently to other information obtained under a network activity warrant. Paragraph 27KP(2)(i) provides that a network activity warrant may permit the use of a surveillance device but only for the purposes of doing a thing authorised by the warrant. The purpose of this power is to facilitate the execution of the warrant, not to collect intelligence.

471. Information obtained from the use of a surveillance device may be used for the purposes of doing a thing authorised by a network activity warrant (paragraph 45B(7)(a)). This provision ensures that a surveillance device may be used to facilitate the execution of a network activity warrant.

472. Paragraph 45B(7)(b) provides that protected network activity warrant information may be used, recorded, communicated or published for the purposes of an IGIS official exercising powers or performing functions or duties as an IGIS official. This provision is necessary to facilitate IGIS oversight of network activity warrants, including oversight of the use of a surveillance device under a network activity warrant. This ensures that the IGIS will be able to assess the legality and propriety of using a surveillance device under a network activity warrant.

473. Paragraphs 45B(7)(c) and (d) ensure that information obtained by using a surveillance device may be used, recorded, communicated or published in an investigation or proceeding relating to an offence against the prohibition on the use, recording, communication or publication of protected network activity warrant information in subsections 45B(1) and (2). This provision ensures that where a person has unlawfully used or disclosed information obtained by using a surveillance device, he or she may be effectively investigated and prosecuted for the offence. This is an important safeguard in ensuring that information obtained by using a surveillance device under a network activity warrant is used appropriately.

474. Subsection 45B(8) provides for the circumstances in which protected network activity warrant information can be communicated by an Ombudsman official to an IGIS official. This may be done for the purposes of the IGIS official exercising their powers, or performing functions or duties. Similarly, an IGIS official can communicate this information to an Ombudsman official for the purposes of the Ombudsman official exercising powers, or performing functions or duties as an Ombudsman official under subsection 45B(9). The purpose of this provision is to manage oversight of the activities of the AFP and the ACIC by the Ombudsman and the IGIS. The intent of this provision is facilitate information sharing between integrity bodies and avoid duplication in the oversight of these agencies.
475. Under subsection 45B(10), protected network activity warrant information may be admitted into evidence in a proceeding for an offence against the unauthorised use or disclosure of protected network activity warrant information in subsections 45B(1) and (2), or proceedings that are not a criminal proceeding. The intent of allowing network activity warrant information to be admitted into evidence in a proceeding that is not a criminal proceeding is to allow for protected network activity warrant information to be admitted into other hearings, such as those that question the validity of the warrant.

476. Subsection 45B(11) provides that information obtained under a network activity warrant that is communicated to another law enforcement agency, or an agency that is not a law enforcement agency (other than the IGIS, ASIO or an agency empowered under the IS Act), may only be communicated within that second agency for the purpose for which it was communicated. This information must also not be communicated to any person who is not an officer of that second agency. The effect of this provision is that protected network activity warrant information may not be on-disclosed for a purpose beyond that for which it was originally communicated. This is intended to protect the security of sensitive information obtained under a network activity warrant.

Item 20 – After section 46

46AA Dealing with records obtained by accessing data under a network activity warrant

477. New section 46AA imposes a duty upon the chief officer of the AFP or the ACIC to ensure that every record or report containing protected network activity warrant information or network activity warrant intercept information is kept securely and is not accessible to those who are not authorised to deal with that information (paragraph 46AA(1)(a)). The inclusion of network activity warrant intercept information ensures that this type of information, while not protected network activity warrant information, has record keeping requirements.

478. Paragraph 46AA(1)(b) further imposes an obligation upon the chief officer to destroy or cause to be destroyed any record or report as soon as practicable, and within a period of five years, after the making of the record or report. Before destroying the record or report, the chief officer must first be satisfied that the record or report is not likely to be required for a civil or criminal proceeding, in connected with an activity listed in subsection 45B(4), or a purpose listed in subsection 45B(5) or (7).

479. Subsection 46AA(2) imposes the same duties that the chief officer of the AFP or the ACIC has under subsection 46AA(1) on the officers in charge of an agency that is not a law enforcement agency. However, this obligation does not apply to the IGIS (subsection 46AA(3)).
Item 21 – Subsection 47A(7) (after paragraph (c) of the definition of computer access technologies or methods)

480. Subsection 47A(7) provides that computer access technologies or methods means technologies or methods relating to using a computer, telecommunications facility, any other electronic equipment, or data storage device, for the purposes of obtaining access to data, or for adding, copying, deleting or altering other data in a computer. This item ensures that where such activities have been deployed in giving effect to a network activity warrant, those activities are captured under the definition of computer access technologies or methods.

481. The effect of this amendment is to ensure that section 47A also applies in relation to network activity warrants. Section 47A gives protection to sensitive information relating to computer access technologies or methods in order to prevent its release into the public domain. This is because there is a significant risk that releasing such information could harm future capabilities and investigations.

482. Section 47A now provides the same protection to information that, if disclosed, could reveal details of computer access technologies or methods that have been deployed in giving effect to a network activity warrant. This is an important protection for law enforcement capabilities which are fundamental to ongoing investigations and agencies’ ability to protect essential public interests, including national security and public safety.

Item 22 – After subsection 49(2D)

483. This item provides the reporting requirements relating to network activity warrants. There is no amendment to subsection 49(1) as the current language would apply to network activity warrants. That subsection states that the chief officer of a law enforcement agency must make a report and give a copy of each warrant to the Minister.

484. New subsection 49(2E) lists the requirements of the report as it relates to network activity warrants. The report must state whether the warrant was executed, the name of the person primarily responsible for the execution, the name of each person involved in accessing the data, the name (if known) of any person whose data was accessed and the location (if known) of the computers.

485. The report must also give details of the extent to which the execution of the warrant has contributed to the prevention, detection or frustration of one or more kinds of relevant offences, the extent to which the execution of the warrant assisted the agency in carrying out its functions, the communication of information obtained under the warrant to persons other than officers of the agency and compliance with the conditions (if any) to which the warrant was subject.

486. The report must also give details of the information that was obtained from access to data under the warrant, how that information was used, and how that information was destroyed or retained if required.
The report must also detail any premises accessed, telecommunications intercepted, or computers removed, as well as any concealment activities undertaken or assistance orders made in relation to the warrant.

If a network activity warrant was extended or varied, the report must also state the number of extensions or variations made and the reasons for making them.

Item 23 – After section 49C

49D Notification to Inspector-General of Intelligence and Security of things done under a network activity warrant

This item imposes an obligation on the chief officer of the AFP or the ACIC to notify the IGIS if a network activity warrant was issued and a concealment activity (see subsection 27KP(8)) was undertaken after a 28 day period. The chief officer must make this notification within 7 days of the concealment activity being undertaken.

Item 24 – After paragraph 50(1)(eb)

Section 50 sets out the reporting requirements agencies have to meet each financial year in their annual report to the Minister on their use of powers in the SD Act. The report is to be submitted to the Minister as soon as practicable, and within a three month period, following the end of each financial year (subsection 50(3)).

This item sets out the reporting obligations for the AFP and the ACIC in relation to their use of network activity warrants. The AFP and the ACIC must report on the kinds of offences in relation to which information was obtained under network activity warrants issued during that year.

Item 25 – Paragraph 51(b)

This item amends the record keeping requirement at paragraph 51(b) to account for network activity warrants. This amendment ensures that each instrument of revocation in relation to network activity warrants under new subsection 27KR(4) must be kept by the agency.

Item 26 – After paragraph 52(1)(h)

Under existing subsection 52(1), the chief officer of a law enforcement agency must cause to be kept details of each occasion when information obtained by the use of a surveillance device or computer access was used for certain purposes. New paragraph 52(1)(ha) provides that the AFP and the ACIC must cause to be kept the details of things done under a network activity warrant.
Item 27 – Paragraph 52(1)(j)

494. This item amends paragraph 52(1)(j) to ensure that the AFP and the ACIC must cause to be kept the details of the destruction of records or reports in relation to network activity warrants under paragraph 46AA(1)(b).

Item 28 – After subsection 55(1)

495. Division 3 of Part 6 provides for inspections by the Ombudsman into the execution of the powers granted under the Act. This item carves network activity warrants out of subsection 55(1) as the Ombudsman does not have oversight of network activity warrants. The IGIS has oversight responsibility for network activity warrants. The relevant provisions are in Part 2 of Schedule 2 of this Bill.

Item 29 – At the end of subsection 62(1)

496. Under section 62, an appropriate authorising officer (within meaning of subsection 6A) may issue a written certificate setting out the facts of what has been done by a law enforcement officer or a person providing technical expertise in connection with the execution of a warrant. Evidentiary certificates are intended to streamline the court process by reducing the need to contact numerous officers and experts to give evidence on routine matters.

497. This item amends section 62 to ensure that an evidentiary certificate may be issued with respect to anything done by a law enforcement officer in connection with the use, recording or communication of information obtained from access to data under a network activity warrant. This is appropriate given that information obtained under a network activity warrant may be used in evidence in a proceeding for an offence in relation to the unauthorised use, recording or communication of protected network activity warrant information (see subsection 45B(10)).

Item 30 – After subparagraph 64A(1)(a)(i)

498. Section 64A provides that a law enforcement officer may apply to an eligible Judge or nominated AAT member for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do the things set out in paragraphs 64A(1)(a)-(c). Paragraph 64A(1)(a) provides that an assistance order may be sought for the purposes of allowing the officer to access data held in a computer subject to a computer access warrant. The penalty for not complying with an order compelling assistance under section 64A is a maximum term of imprisonment for 10 years (subsection 64A(8)).

499. This item amends section 64A to provide that a law enforcement officer may apply for an assistance order (under section 64A) to allow them to access data held in a computer that is the subject of a network activity warrant. This ensures that the AFP or the ACIC, with a network activity warrant, will be able to compel assistance in accessing devices. The
intent of this provision is not to allow law enforcement to compel assistance from industry, but rather from a person with knowledge of a computer to assist access (such as a person who uses the computer).

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

Item 31 – After subsection 64A(6)

501. This item inserts new subsection 64(6A) which sets out the matters to which an eligible Judge or nominated AAT member must be satisfied of in order to grant an assistance order in relation to a network activity warrant. The Judge or AAT member must be satisfied that there are reasonable grounds for suspecting that access to data held in the computer will substantially assist in the collection of intelligence in relation to criminal networks of individuals. The issuing authority must also be satisfied that there are reasonable grounds for suspecting that access to data held in the computer will substantially assist in the collection of intelligence that is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

502. The Judge or AAT member must also be satisfied that the person specified in the order is either reasonably suspected of having committed any of the offences in relation to which information will be obtained under the warrant, is the owner or lessee of the computer, is an employee of the owner or lessee of the computer, is a person engaged under a contract for services by the owner or lessee of the computer, is a person who uses or has used the computer, or is a person who is or was a system administrator for the system including the computer.

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

Item 32 – Paragraph 65(1A)(a)

504. Section 65 provides that if there is a defect or irregularity in relation to a warrant or emergency authorisation and but for that defect or irregularity the warrant or authorisation would be sufficient authority for the use of a surveillance device or accessing data held in a computer in obtaining information or a record, then the use of the device is to be treated as valid, and the information or record can be given in evidence.

505. This item ensures that the same is the case for information or a record obtained pursuant to a network activity warrant, were a defect or irregularity to be found.
Part 2 – Consequential amendments

Australian Crime Commission Act 2002

Item 33 – Subsection 51(4) (at the end of the definition of relevant Act)

506. This item amends the ACC Act to include within the definition of relevant Act in section 51, the IGIS Act, and any other Act, or instrument made under an Act that confers functions, duties or powers on the IGIS. This enables members of the ACIC to communicate information acquired by reason of, or in the course of, the performance of duties under the ACC Act to carry out a purpose under the IGIS Act, or in connection with the performance of their duties under the IGIS Act without committing an offence under subsections 51(2) or (3).

Item 34 – After paragraph 59AA(1B)(f)

507. This item inserts new paragraph 59AA(1B)(fa) to provide that the ACIC CEO is able to disclose national policing information to the IGIS without seeking the approval of the ACIC Board.

508. Section 59AA(1B) provides that the ACIC CEO must obtain the ACIC Board’s approval before he or she can release national policing information, noting that national policing information can only be released in accordance with policies or directions issued by the Board, as per subsection 59AA(1A), unless they are disclosing it to an entity that is listed in paragraphs (a)-(g) of subsection 59AA(1B). Currently, listed entities include the AFP, ASIO, and Home Affairs (captured as “the Department administered by the Minister who administers the Australian Border Force Act 2015”).

509. New paragraph 59AA(1B)(fa) specifies that the ACIC CEO can disclose national policing information to the IGIS without the approval of the ACIC Board. This amendment reflects the expansion of the IGIS’s oversight functions to the ACIC’s use of network activity warrants, and ensures that the IGIS is able to access the information required to fulfil its oversight functions.

Australian Federal Police Act 1979

Item 35 – Subsection 4(1)

510. This item inserts a definition of IGIS official into the AFP Act, meaning the Inspector-General of Intelligence and Security or any other person covered by subsection 32(1) of the IGIS Act. The Bill inserts this definition into a number of Acts and provides a consistent way to refer to both the IGIS, and any other person covered by subsection 32(1) of the IGIS Act. This definition is necessary as the IGIS will have oversight of the AFP’s use of and compliance with network activity warrants, as opposed to other powers exercised by the AFP for which the Commonwealth Ombudsman has responsibility for oversight.
**Item 36 – Subsection 40ZA(3)**

511. This item amends subsection 40ZA(3) to ensure that the secrecy offences in section 40ZA will not prevent a person from divulging information to an IGIS official where that information is relevant to the IGIS’s powers, functions or duties.

512. Section 40ZA(2) prohibits a person (other than an AFP appointee or the Ombudsman) from making a record of, or disclosing information that he or she obtained as a result of an investigation or inquiry into:

- category 3 conduct, which is defined in section 40RP of the AFP Act as serious misconduct by an AFP appointee that raises the issue of whether the appointee ought to be terminated (but is not corruption)

- a corruption issue under Subdivision D of Division 3 of the AFP Act, or

- a ministerially directed inquiry under Division 4 of Part V of the AFP Act.

513. If a person discloses such information, he or she is liable to a penalty of 30 penalty units.

514. Subsection 40ZA(3) notes that the offence in subsection 40ZA(2) has effect subject to subsections (4)-(6). These provisions allow the disclosure of the information for the purposes of the inquiry or investigation (section 40ZA(4)), with the consent of the Minister or Commissioner who directed the inquiry or investigation (section 40ZA(5)) and as evidence in a court (section 40ZA(6)).

515. This item amends subsection 40ZA(3) by omitting “and (6)” and substituting “, (6) and (6A)”. This is consequential to the proposed insertion of subsection 40ZA(6A) by item 32.

**Item 37 – after subsection 40ZA(6)**

516. This item inserts a new subsection 40ZA(6A) which provides that the secrecy offences under subsection 40ZA(2) do not prevent a person from making a record of, or divulging or communicating, information for the purpose of an IGIS official exercising powers, or performing functions or duties, as an IGIS official.

517. This amendment ensures that the secrecy offences in subsection 40ZA(2) would not prevent a person from divulging information that is relevant to the IGIS’s powers, functions or duties. This reflects the expansion of the IGIS’s oversight function to include the AFP’s use of network activity warrants.

518. Further, the amendment ensures that it is clear, on the face of agencies’ governing legislation, that individuals can share information and records with IGIS officials (including voluntarily) for the purpose of the IGIS performing oversight functions. The amendment clarifies when officials are able to disclose information to the IGIS.
Item 38 – After paragraph 60A(2)(f)

519. This item amends section 60A to ensure that the secrecy offences in subsection 60A(2) will not stop a person from divulging information that is relevant to the IGIS’s powers, functions or duties.

520. Section 60A contains general secrecy provisions that apply to members of the AFP, including the Commissioner, Deputy Commissioner, employees, contractors or consultants and secondees amongst others. Paragraphs 60A(2)(a)-(b) make it an offence for persons to whom the section applies to make a record of any prescribed information or divulge or communicate any prescribed information. Paragraphs 60A(2)(c)-(f) contains exceptions to that offence. Current exceptions include for the purposes of the LEIC Act and regulations and the Parliamentary Joint Committee on Law Enforcement Act 2010 and regulations.

521. This item inserts paragraph 60A(2)(g) which creates an additional exception so that the offence does not apply for the purposes of an IGIS official exercising powers, or performing functions or duties, as an IGIS official.

522. This item reflects the expansion of the IGIS’s oversight function to include the AFP’s use of network activity warrants. The amendment ensures that it is clear, on the face of agencies’ governing legislation, that individuals can share information and records with IGIS officials (including voluntarily) for the purpose of the IGIS performing oversight functions. The amendment clarifies when officials are able to disclose information to the IGIS.

Australian Human Rights Commission Act 1986

523. The Bill introduces new oversight arrangements for the AFP and the ACIC by the IGIS in relation to network activity warrants. The AHRC may currently inquire into an act or practice of the AFP or the ACIC if that act or practice is not consistent with, or contrary to, any human right. In the event that a complaint is made to, or a matter brought to the attention of, the AHRC that may be more appropriately dealt with by the IGIS, amendments to the AHRC Act are required to facilitate the transfer of that complaint and associated information to IGIS officials.

Item 39 – Subsection 3(1)

524. This item amends subsection 3(1) by inserting new definitions.

525. ACIC means the agency known as the Australian Criminal Intelligence Commission established by the Australian Crime Commission Act 2002.

526. Examiner of ACIC means an examiner within the meaning of the ACC Act. An examiner of the ACIC is a person appointed under subsection 46B(1) of the ACC Act by the Governor-General.
IGIS official means the Inspector-General of Intelligence and Security or any other person covered by subsection 32(1) of the IGIS Act, namely, persons engaged under the Public Service Act 1999 or persons the Inspector-General has employed to perform functions and exercise powers under Division 3 or 4 of Part II of the IGIS Act for the purposes of a particular inquiry.

Item 40 – At the end of subsection 11(3)

This item adds a note after subsection 11(3) to clarify the operation of the section in relation to the duplication in oversight between the AHRC and the IGIS in relation to the ACIC and the AFP that is created by the Bill.

Subsection 11(1) provides that the functions of the AHRC include, among others, such functions as are conferred on the Commission by the Age Discrimination Act 2004, the Disability Discrimination Act 1992, the Racial Discrimination Act 1975, the Sex Discrimination Act 1984 or any other enactment (paragraph 11(1)(a)), to inquire into, and attempt to conciliate, complaints of unlawful discrimination (paragraph 11(1)(aa)), and to inquire into any act or practice that may be inconsistent with or contrary to any human right; and attempt to effect a settlement to the matter (paragraph 11(1)(f)).

Subsection 11(3) specifies that where a complaint relates to an AIC agency (ASIO, ASIS, ASD, AGO, DIO and ONI), the AHRC must not inquire into a matter and must transfer it to the IGIS.

The Bill creates overlapping jurisdiction between the IGIS and the AHRC in relation to the ACIC and the AFP. The IGIS will have jurisdiction in relation to agencies’ compliance with human rights and anti-discrimination law only as it relates to network activity warrants, while the AHRC would have oversight of the agencies’ compliance with these matters in all other functions. Due to this intersection, it is not appropriate to require the AHRC to automatically transfer all matters relating to these agencies to the IGIS.

The note highlights this overlap and notes that the IGIS and AHRC may transfer matters between each other and share information in relation to actions taken by any of these agencies as appropriate for their respective oversight responsibilities. This clarifies the interrelation between the AHRC Act and the IGIS Act, and how complaints relating to the ACIC and AFP may be managed by these integrity bodies.

Item 41 – At the end of subsection 20(1)

This item adds a note after subsection 20(1) to clarify that complaints are deemed to have been made to the AHRC where they have been transferred to the AHRC by the IGIS.

Subsection 20(1) provides that the AHRC must inquire into any act or practice that may be inconsistent with or contrary to any human right, and, if appropriate, attempt to effect a settlement to the matter (a function of the AHRC set out in paragraph 11(1)(f)) in
response to a direction from the Minister, a complaint (made in writing), or where the Commission determines it is desirable to do so.

535. This item inserts a note after subsection (1) to note that, where the IGIS transfers a complaint to the AHRC (as it is able to do under new section 32AD), the transferred complaint is taken to have been made to the AHRC for the purposes of the AHRC’s functions. This streamlines the complaints process for complainants, as it removes the need to re-submit complaints to the AHRC.

**Item 42 – After subsection 20(4B)**

536. This item inserts new subsections 20(4C) and (4D). Section 20 deals with the AHRC’s performance of its functions relating to human rights. New subsections 20(4C) and (4D) would facilitate the transfer of a complaint from the AHRC to the IGIS.

537. New paragraphs 20(4C)(a)-(b) allow the AHRC to decide not to inquire into a complaint or part of a complaint about acts or practices of the ACIC (except for complaints about examiners) or the AFP, on the basis that the complaint could be more effectively or conveniently dealt with by the IGIS under the IGIS Act.

538. Where the AHRC makes a decision not to inquire into a matter based on new paragraphs 20(4C)(a)-(b), they must consult the IGIS (per new paragraph 20(4C)(c), and if the IGIS agrees to receive the complaint, transfer that complaint to the IGIS as soon as is reasonably practicable (per new paragraph 20(4C)(d)). Under subsection 20(4C)(f) the AHRC would have to give to the IGIS any information or documents that relate to the complaint, and are in the possession or under the control, of the AHRC.

539. Finally, under new paragraph 20(4C)(e) the AHRC must also take reasonable steps to give the complainant written notification that the complaint has been transferred to the IGIS.

540. These amendments will assist with the management of the overlapping oversight responsibilities of the AHRC and the IGIS relating to the ACIC and AFP, by allowing cases to be transferred from the AHRC to the IGIS when it is appropriate to do so. Provisions in new Part IIIA of the IGIS Act allow the IGIS to transfer complaints to the AHRC.

541. New subsection 20(4D) allows the AHRC and the IGIS to enter into a standing agreement relating to the transfer of cases, although such agreements cannot limit subsection 20(4C). Subsection 20(4D) is not intended to affect any existing standing arrangements between the AHRC and the IGIS.
Item 43 – Subsection 46P(1) (note)

542. This item amends the note after subsection 46P(1) by omitting “Note” and substituting “Note 1”. This amendment is a consequence of inserting a second note after subsection 46P(1).

Item 44 – At the end of subsection 46P(1)

543. This item inserts a second note after subsection 46P(1). Section 46P(1) provides that a written complaint may be lodged with the AHRC for conciliation by the President of the AHRC.

544. The proposed note highlights that in addition to a person lodging a complaint under section 46P, a complaint may be deemed to have been lodged with the AHRC if transferred from IGIS under new section 32AD of the IGIS Act. This note would clarify that the means by which a complaint may come to the AHRC, noting that a transferred complaint has the same effect as a written notification directly to the AHRC.

Item 45 - Before section 47

46PZ Transfer of complaints from the Inspector-General of Intelligence and Security

545. This item inserts section 46PZ. Subsection 46PZ(1) allows the AHRC to determine whether certain complaints transferred by the IGIS under section 32AD of the IGIS Act should be deemed to be made as referred to in paragraph 20(1)(b) of the AHRC Act (for human rights complaints), or lodged under section 46P of the AHRC Act (for unlawful discrimination complaints).

546. When a complaint is transferred from the IGIS to the AHRC under section 32AD of the IGIS Act, it is intended that the date it is transferred is the date the complaint is taken to be to be made to the AHRC.

547. Both types of complaint are subject to a different set of procedures, and a decision by the AHRC under section 46PZ would effectively determine which set of procedures to apply. It is intended that the AHRC would base its determination on which set of procedures is most appropriate to the specifics of each transferred matter.

548. Subsection 46PZ(2) provides that such a determination would be effective in deeming the provision to have been made or lodged. Subsection 46PZ(3) provides that such a determination (under 46PZ(2)) is not a legislative instrument, and as such is not subject to disallowance under section 42 of the Legislation Act 2003 (Legislation Act) or sunsetting under section 50 of the Legislation Act. This characterisation is appropriate as these determinations would not meet the definition of legislative instrument in section 8 of the Legislation Act. Specifically, it would not meet subparagraph 8(4)(b)(i) as the declaration would be determining particular cases rather than determining the law or altering the
contents of the law. As such subsection 46PZ(3) is declaratory of the law and intended to remove any ambiguity as to the status of a declaration made under subsection 46PZ(3).

549. Overall, the new section is intended to facilitate the transfer between the IGIS and the AHRC, and to minimise disruption or administrative delay for complainants.

**Item 46 - Subsection 49(4A)**

550. This item ensures that provisions regulating the disclosure of private information obtained by an AHRC staff member in section 49 can be disclosed to IGIS officials without penalty.

551. Section 49 creates an offence for the inappropriate disclosure of private information by AHRC officials. Subsection 49(4A) provides that the offence in subsection 49(1) does not prevent the AHRC from giving information or documents in accordance with paragraph 20(4A)(e) (which allows the AHRC to give documents and information to the Information Commissioner when transferring complaints from the AHRC to the Information Commissioner).

552. This item inserts “or (4C)(f)” after “20(4A)(e)” in subsection 49(4A). This amendment reflects the insertion of new paragraph 20(4C)(f). New subsection 20(4C)(f) is analogous to existing 20(4A)(e), the only difference being that it permits information and documents to be transferred to the IGIS where a complaint is transferred. It is appropriate that these provisions are treated in a like manner, to ensure that AHRC officials are not subject to penalties depending on which agency they transfer a complaint to.

553. It is intended that this item ensures that the offence in subsection 49(1) would not stop a person from divulging information that is relevant to the IGIS’s powers, functions or duties.

**Item 47 – after subsection 49(4B)**

554. This item ensures that provisions regulating the disclosure of private information obtained by an AHRC staff member in section 49 can be disclosed to IGIS officials without penalty.

555. This item inserts new subsection 49(4C). Subsection 49(4C) would provide that the offence in subsection 49(1) does not prevent the AHRC, or a person acting for or on behalf of the AHRC, from giving information or documents to an IGIS official for the purpose of the IGIS official exercising a power, or performing a function or duty, as an IGIS official. This would ensure that IGIS officials are able to access any information required to perform their duties, functions or powers as IGIS officials.

556. A note at the end of subsection 49(4C) highlights that a defendant (being the person who disclosed information to an IGIS official) bears an evidential burden in relation to a matter in subsection 49(4C), which refers to the action of subsection 13.3(3) of the
Criminal Code. The effect of this provision is that, in a prosecution under section 49(1), the AHRC official would have to lead evidence that would point to the reasonable possibility that they gave the information or documents to an IGIS official for the purpose of the IGIS official exercising a power, or performing a function or duty, as an IGIS official.

557. This item also inserts a provision to clarify that the Commission may give information or documents to an IGIS official whether or not the Commission is transferring a complaint or just part of a complaint to the IGIS.

558. It is intended that this item ensures that the offence in subsection 49(1) would not stop a person from divulging information that is relevant to the IGIS’s powers, functions or duties.

**Australian Information Commissioner Act 2010**

559. The Bill introduces new oversight arrangements for the AFP and the ACIC by the IGIS in relation to network activity warrants. Currently, the Information and Privacy Commissioner may inquire into certain matters relating to the AFP and the ACIC if it is within their functions outlined in the AIC Act or the Privacy Act. In the event that a complaint is made to, or a matter brought to the attention of, the Information and Privacy Commissioner that may be more appropriately dealt with by the IGIS, amendments to the AIC Act are required to facilitate the transfer of that complaint and associated information to IGIS officials.

**Item 48 – Section 3**

560. This item inserts a new definition of IGIS official into section 3 of the AIC Act. This definition would give IGIS official the meaning given subsection 29(6) of that Act (which is inserted below).

**Item 49 – After Paragraph 29(2)(c)**

561. This item inserts new paragraph 29(2)(d), which provides a defence for disclosing information to an IGIS official.

562. Subsection 29(1) of the AIC Act criminalises the recording or disclosing of information acquired by a person in the course of performing functions or exercising powers conferred for the purposes of an Information Commissioner function, a freedom of information function or a privacy function.

563. Subsection 29(2) contains circumstances in which the offence in subsection 29(1) does not apply. New paragraph 29(2)(d) would provide that the offence does not apply when the record, use or disclosure relates to an IGIS official performing a function or duty as an IGIS official. This item is intended to ensure that the secrecy offences in section 60A will
not stop a person from divulging information that is relevant to the IGIS’s powers, functions or duties.

**Item 50 – At the end of section 29**

564. This item inserts new subsection 29(6) to provide the definition for the defined term *IGIS official* inserted in section 3 of the Act. The definition is included here rather than in section 3 as it is only relevant to section 29 of the Act. The definition provided by subsection 29(6) matches the definition of IGIS official inserted into a number of Acts by the Bill and provides a consistent way to refer to both the IGIS, and any other person covered by subsection 32(1) of the IGIS Act.

*Inspector-General of Intelligence and Security Act 1986*

**Item 51 – Subsection 3(1)**

565. This item provides for two new definitions in the IGIS Act.

566. *ACIC* means the agency known as the Australian Criminal Intelligence Commission established by the ACC Act 2002.

567. *CEO of ACIC* means the Chief Executive Officer of the Australian Crime Commission. The insertion of this definition is necessary to give effect to provisions allowing for IGIS oversight of the ACIC in relation to network activity warrants as the ACIC has not previously been subject to oversight by the IGIS.

**Item 52 – Subsection 3(1) (after paragraph (d) of the definition of head)**

568. This item amends the definition of “head” (referring to agency heads) in subsection 3(1) of the IGIS Act to capture the heads of the new agencies subject to IGIS oversight. The definition includes the CEO of the Australian Crime Commission and the Commissioner of Police. These new definitions are in addition to the existing definitions of ‘head’, which apply to AIC agencies.

**Item 53 – Subsection 3(1)**

569. This item amends subsection 3(1) of the IGIS Act by inserting several definitions.

570. *Information Commissioner* refers to section 3A of the AIC Act, which contains a definition of Information Commissioner that applies in all Acts. The Information Commissioner means the person appointed under section 14 of that Act as the Australian Information Commissioner.

572. **Integrity body means** the Ombudsman, the AHRC, the Information Commissioner, the Integrity Commissioner, or the Inspector-General ADF. An **integrity body** for a complaint has the meaning given by paragraph 11(4A)(a) which is the integrity body for which a complaint in respect of action taken by an intelligence agency has been, or could have been, made to by the complainant instead of the Inspector-General.

573. **Integrity Commissioner** has the meaning given by section 5 of the LEIC Act. Section 5 of the LEIC Act provides that ‘Integrity Commissioner’ means the Integrity Commissioner appointed under section 175 of the LEIC Act.

574. The inclusion of the IGADF reflects the potential for the ASD to provide Commonwealth and State Authorities assistance under section 7 of the IS Act. In the context of the Bill, ASD may provide assistance to the ACIC or AFP under subsection 7(e) in relation to:

- cryptography, and communication and computer technologies, and
- other specialised technologies acquired in connection with the performance of its other functions.

575. ASD providing assistance of this kind may be useful to the ACIC or AFP during the execution of, or analysis of information obtained under, network activity warrants. ASD currently may provide assistance under section 7(1)(e) to Commonwealth and State authorities, including when those agencies are exercising their powers, for example, under the TIA Act or SD Act.

576. As ASD’s functions also enable it to provide assistance to the Defence Force in support of military operations, it is appropriate that the amendments to the IGIS Act, for example, relating to complaints transfer, sharing of information and avoiding duplication of oversight, also apply to the IGADF.

**Item 54 – Subsection 3(1) (definition of intelligence agency)**

577. This item amends subsection 3(1) by repealing the current definition of **intelligence agency**. Intelligence agency now means ASIO, ASIS, AGO, DIO, ASD, or ONI; or the AFP and the ACIC to the extent that they have intelligence functions.

578. Paragraph (b) of the new definition is intended to capture the intelligence functions of the AFP and the ACIC. The AFP and the ACIC are defined separately as they will only have limited oversight by IGIS relating to network activity warrants. Although paragraph (b) describes these agencies generally, it is not intended that the non-intelligence functions of these agencies would be subject to IGIS oversight. The definition of ‘intelligence function’ and subsections 8(3A)-(3B) provide the extent to which the functions of these agencies would be overseen by the IGIS.
Item 55 – Subsection 3(1)

579. This item amends subsection 3(1) by inserting a new definition for intelligence function.

580. **Intelligence function** in relation to the ACIC means the collection, correlation, analysis, production and dissemination of intelligence obtained by the ACIC from the execution of a network activity warrant; or the performance of a function, or the exercise of a power, conferred on a law enforcement officer of the ACIC by the network activity warrant provisions of the SD Act 2004.

581. Intelligence function in relation to the AFP means the collection, correlation, analysis, production and dissemination of intelligence obtained by the AFP from the execution of a network activity warrant; or the performance of a function, or the exercise of a power, conferred on a law enforcement officer of the AFP by the network activity warrant provisions of the SD Act.

582. This definition is intended to enable the IGIS to oversee all aspects of the network activity warrant life cycle. For example the IGIS will be able to oversee the initial collection of intelligence by the AFP and the ACIC through the execution of the warrant, the correlation of intelligence, the analysis of that intelligence, the production of intelligence and the dissemination of intelligence, where all of these relate to the warrant or the execution of the warrant.

583. This definition also covers the performance of a function, or the exercise of a power, conferred on a law enforcement officer by the network activity warrant provisions of the SD Act. This ensures that where aspects of the network activity warrant regime are not strictly connected with the execution of the warrant, the IGIS will be able to oversee their operation. For example, compliance with the SD Act where a network activity warrant application is made and subsequently issued but revoked before it is executed, compliance with the record-keeping and reporting provisions so far as they relate to network activity warrants, or ensuring delegations made under the Act are correctly made and complied with so far as they relate to network activity warrants.

584. **Law enforcement officer**, when used in relation to the AFP has the same meaning as in the SD Act. This means the Commissioner of Police, the Deputy Commissioner of Police, an AFP employee, a special member; or person seconded to the AFP.

585. Law enforcement officer when used in relation to the ACIC means the CEO, or a person covered by a paragraph of the definition of member of the staff of the ACC in section 4 of the ACC Act.

586. **Network activity warrant** has the same meaning as in the SD Act. The SD Act provides that a network activity warrant is a warrant issued under section 27KM of that Act.
Item 56 – After subsection 8(3)

587. This item inserts new subsections 8(3A) and 8(3B).

588. New subsection 8(3A) sets out the potential inquiry functions of the IGIS in relation to the intelligence functions of the ACIC and the AFP as defined by the IGIS Act, while subsection (3B) sets out matters that are outside of IGIS jurisdiction. Subsections (3C)-(3D) outline how inquiries into the matters in subsection (3A) may be initiated.

589. These provisions are modelled on the existing provisions in subsections 8(1) to (3) that outline the IGIS’s functions in relation to ASIO, ASIS, ASD, AGO, ONI and DIO, but with amendments to reflect that the ACIC and AFP have functions outside their intelligence functions as defined by the IGIS Act, and, in the case of the ACIC, a different governance structure. The main divergence from other subsections in section 8 is specification that the IGIS would only have functions ‘to the extent that the matter relates to an intelligence function of the agency’. This caveat is intended to reflect that IGIS oversight does not extend to the parts of the agencies that are unrelated to network activity warrants.

590. New paragraphs 8(3A)(a)-(c) provide that the Attorney-General or relevant Minister (the Minister responsible for the intelligence functions of the AFP and the ACIC) may request the IGIS to inquire into any of the matters in paragraphs 8(3A)(d)-(i). The IGIS is also able to commence an inquiry based on its own-motion or in response to a complaint made to the IGIS in relation to any of the matters in paragraphs 8(3A)(d)-(i). This is consistent with how inquiries may be commenced in relation to any of the agencies currently subject to IGIS oversight.

591. New paragraphs 8(3A)(d)-(i) provide that the functions of the IGIS in relation to the ACIC and the AFP are to inquire into the following matters provided that the IGIS’s inquiry relates to an intelligence function of the agency:

- compliance by that agency of Commonwealth, State and Territory laws
- compliance by that agency with directions or guidelines given to that agency by the responsible Minister
- propriety of particular activities by that agency, and
- the effectiveness and appropriateness of the procedures of the ACIC and AFP relating to the legality or propriety of the activities of the agency.

592. New paragraph 8(3A)(h) provides that a function of the IGIS in relation to the intelligence functions of the ACIC and the AFP is to inquire into a matter referred to the IGIS by the AHRC, provided that the matters relates to an intelligence function of the agency as defined by the IGIS Act. These matters must also relate to an act or practice of
the agency which may be inconsistent with a human right, constitute discrimination, or be unlawful under Australian anti-discrimination legislation.

593. New paragraph 8(3A)(i) provides that a function of the IGIS in relation to the ACIC is to inquire into its compliance with directions, guidelines, policies or decisions made by the board of the ACIC or the Inter-Governmental Committee established under the ACC Act so far as those directions, guidelines, policies or decisions relate to the intelligence function of the ACIC as defined by the IGIS Act. This extension reflects that under the governance structure of the ACIC, the board and Inter-Governmental Committee can direct the agency in a similar manner to both the CEO of the ACIC and the responsible Minister. This paragraph is necessary to ensure that there is not an arbitrary limit on the IGIS’s jurisdiction based on the origin of directions, guidelines, policies or decisions.

594. New subsection 8(3B) excludes the actions taken by an ACIC examiner performing functions or exercising powers as an examiner, such as an examination, under the ACC Act, from IGIS oversight. This is appropriate, as the IGIS does not have jurisdiction over matters that could be heard in a court or tribunal (sections 9AA and 11(3)-(4) IGIS Act). The conduct of the ACIC examiners may be reviewed by the Ombudsman, the Law Enforcement Integrity Commissioner, and ultimately, a court of law. As such, it is not necessary for the IGIS to oversee these aspects of the ACIC’s activities.

Item 57 – Subsection 8(5)

595. This item amends subsection 8(5) to omit “and (3)” and substitute “, (3) and (3A)”. This item is consequential to the proposed insertion of subsection 8(3A).

Item 58 – Subsection 8(5)

596. Subsection 8(5) outlines that the IGIS’s jurisdiction does not include complaints regarding promotion, termination, discipline, remuneration or any other matter relating to intelligence agencies’ employment of individuals in relation to AGO, DIO and ONI. This item amends subsection 8(5) to ensure this exception also applies to employees of the ACIC and the AFP.

597. This exclusion is consistent with the existing treatment of those agencies currently overseen by the IGIS whose staff are engaged under the Public Service Act. This exclusion is appropriate because employees of the ACIC and the AFP are able to avail themselves of other avenues to address employment concerns (including the Fair Work Ombudsman), and as such, it is unnecessary for the IGIS to provide an additional layer of oversight to these matters.

Item 59 – Paragraph 8A(1)(b)

598. This item amends paragraph 8A(1)(b) by inserting “(within the meaning of this Act)” after “intelligence agency”. This amendment is intended to modernise and improve the clarity of paragraph 8A(1)(b) by clarifying that the reference to “intelligence agency” in
this paragraph refers to the agencies defined in this Act, rather than the definition within the PID Act.

**Item 60 – After paragraph 8A(1)(b)**

599. This item amends subsection 8A(1) by inserting new paragraph 8A(1)(c). Subsection 8A(1) provides that if a disclosure of information has been, or is required to be, allocated under section 43 of the PID Act and some or all of the disclosable conduct with which the information is concerned relates (within the meaning of that Act) to an intelligence agency, then to the extent that the conduct so relates, it is taken, for the purposes of the IGIS Act, to be action that relates to the propriety of particular activities of the intelligence agency.

600. This item ensures that this disclosable conduct, where it relates to the ACIC and AFP, must relate to their intelligence functions to be action that relates to the propriety of particular activities of the ACIC and the AFP. This is so it is in harmony with the rest of IGIS’ jurisdiction over the ACIC and the AFP’s use of network activity warrants provided for by the Bill.

**Item 61 – Subsection 8A(1)**

601. This item inserts the words “as described in paragraph (b)” after “so relates” in subsection 8A(1). This is necessary because the inclusion of new paragraph 8A(1)(c) could make it ambiguous as to what conduct is being referred to.

**Item 62 – Paragraph 9AA(b)**

602. This item omits “paragraph 8(1)(d)” from paragraph 9AA(b) and substitute “paragraphs 8(1)(d) and (3A)(b)”. This item is consequential to the insertion of paragraph 8(3A)(b).

603. Paragraph 9AA(b) prohibits the IGIS from inquiring into actions taken by a Minister, except to the extent necessary for the IGIS to perform the functions referred to in subparagraphs 8(1)(a)(ii) and 8(2)(a)(ii), and paragraphs 8(1)(d) and 8(3A)(b). The specified subparagraphs each relate to circumstances where the IGIS can inquire into whether the relevant agency has complied with directions and guidelines provided by the Minister. Each of these inquiries would necessarily involve the IGIS considering the actions of the Minister.

604. Paragraph 8(3A)(b) relates to IGIS inquiries into compliance with Ministerial guidelines or directions by the ACIC and the AFP. It is appropriate, and consistent with oversight arrangements for other intelligence agencies, that the general prohibition in paragraph 9AA(b) is extended to these agencies.
Item 63 – After paragraph 9AA(b)

605. This item inserts new paragraph (ba) after paragraph 9AA(b). The effect of this item is to limit the IGIS’s ability to inquire into the actions taken by the Board of the ACIC or the Inter-Governmental Committee established by the ACC Act, except where necessary to perform functions of the IGIS referred to in paragraph 8(3A)(i).

606. This prohibition is similar to existing paragraph 9AA(b), which limits the IGIS’s ability to inquire into actions taken by Ministers. This provision takes into account that the roles of the ACIC Board and the Inter-Governmental Committee are analogous to the role played by the Minister. For example, under subsections 46A(6) and 59AA(1A) ACC Act, the ACIC CEO is required to act in accordance with any policy determined or directions given by the Board in relation to certain decisions.

607. Given the similarities in these roles, it is appropriate that Board and Inter-Governmental Committee actions are excluded from IGIS oversight to the same extent as Ministerial actions.

Item 64 – Section 9A

608. This item amends section 9A by inserting “(1)” before “The functions”. This item is consequential to the insertion of an additional subsection into section 9A.

Item 65 – At the end of section 9A

609. This item amends section 9A by inserting new subsection (2). New subsection (2) clarifies that when conducting an inspection of the ACIC or the AFP, the IGIS, or a member of staff assisting the IGIS, are entitled to enter and remain on any premises at all reasonable times, are entitled to all reasonable facilities and assistance that the head of the agency is capable of providing, to full and free access at all reasonable times to any information, documents or other property of the agency, and the ability to examine, make copies or take extracts from any information or documents.

610. As the ACIC and the AFP are not presently subject to oversight by the IGIS, and as a result have no existing relationship or arrangements with the IGIS, these amendments are required to make clear what the IGIS is entitled to during inspections of the ACIC and the AFP as part of their oversight of network activity warrants.

Item 66 – At the end of subsection 10(1)

611. This item inserts two notes at the end of subsection (1) to highlight other relevant parts of the IGIS Act.

612. Note 1 would advise that, under new section 32AE, a complaint that has been transferred to the IGIS by another integrity body is taken to a complaint made directly to the IGIS.
This provision makes clear that the protections for IGIS complaints also apply to complainants in transferred matters.

613. Note 2 would direct the reader to the new Part IIIA of the Act. This is intended to signpost that in addition to the provisions in section 10, which provides that complaints to the IGIS must be made in writing, the IGIS may consider their overarching duty avoid duplication with other agencies (the principles of which are set out in new Part IIIA).

**Item 67 – Before subsection 11(2)**

614. This item inserts a heading before subsection 11(2): “When inquiry or further inquiry into complaints is not required”. This will improve accessibility and comprehension of the complaints provisions in section 11 of IGIS Act.

**Item 68 – After subsection 11(4)**

615. This item amends section 11 by inserting new subsection 11(4A) after subsection 11(4). Subsection 11(4A) allows the IGIS to decide not to consider (or consider further) a complaint where it considers that the complaint could be more effectively or conveniently dealt with by another integrity body. Those integrity bodies are:

- the Ombudsman
- the AHRC (for human rights complaints under Division 3 of Part II AHRC Act, or unlawful discrimination complaints under Part IIB AHRC Act)
- the Information Commissioner (for complaints or investigations about acts or practices that may be an interference with the privacy of an individual under Part V of the Privacy Act)
- the Integrity Commissioner, or
- the Inspector-General ADF.

616. The IGIS must also consider whether a complaint has, or could have, been made to the other integrity body.

617. This provision reflects that multiple integrity bodies have oversight jurisdiction in relation to the ACIC and the AFP, and as such, it is likely that complaints to the IGIS may be more appropriately dealt with by another integrity body. This will most obviously arise in situations where a complaint is made to the IGIS about a function unrelated to network activity warrants of these agencies, or in relation to a matter which is specifically excluded from IGIS oversight under subsection 8(3B). The provision is intended to reduce duplication of oversight by integrity bodies and ensure that complaints are directed to the most appropriate integrity body.
618. This item also inserts a note at the end of subsection (4A) to draw readers’ attention to section 32AD, which would allow the IGIS to transfer complaints, or parts of complaints, to another integrity body.

619. This item also amends section 11 by inserting a new subheading ‘Inquiries into complaints about employment, contracts and related matters’ before subsection 11(5). This heading clarifies the structure of the section.

**Item 69 – Paragraph 15(3)(a)**

620. This item amends paragraph 15(3)(a) by inserting “, the Australian Crime Commission, the Australian Federal Police” after “ASD”, wherever it occurs in the paragraph.

621. Subsection 15(3) requires IGIS to notify the Minister responsible for an agency where its inquiry relates to the head of an intelligence agency, and not to notify the agency head. This is to ensure that an IGIS inquiry is performed without interference, and with appropriate discretion. The amendment is consequential to the expansion of the IGIS’s oversight powers to the ACIC and the AFP to their intelligence functions (within the meaning of the IGIS Act).

**Item 70 – Paragraph 21(1B)(a)**

622. This item inserts “, the Australian Crime Commission, the Australian Federal Police” after “ASD”, wherever it occurs in paragraph 21(1B)(a). This amendment reflects the expanded remit of the IGIS in relation to the oversight of the intelligence functions (within the meaning of the IGIS Act) of the ACIC and the AFP.

623. Under existing subsection 21(1B), where the IGIS does not give a draft report to the head of an agency, on the basis that the conclusions and recommendations of the report relate directly to the head of the agency, the IGIS must give the draft report to the responsible Minister for that agency. The amendment would ensure that where the report relates to the head of the ACIC or the AFP, the IGIS must provide the report to the responsible Minister for the relevant agency. The amendment is not intended to change existing law, as each of those agencies would otherwise be subject to paragraph 21(1B)(c) which provides that where the IGIS prepares reports about the head of a Commonwealth agency, it must provide the draft report to the responsible Minister.

**Item 71 – After Part III**

624. The Bill introduces new oversight arrangements for the AFP and the ACIC by the IGIS in relation to network activity warrants. The IGIS will be able to conduct inspections and inquire into the intelligence functions of the AFP and the ACIC as defined by the IGIS Act. A complaint may be made to, or a matter brought to the attention of, the IGIS, that may be more appropriately dealt with by another integrity body with jurisdiction over the ACIC or AFP. As such, Part IIIA establishes arrangements for the IGIS to transfer
complaints and information to other integrity bodies, as well as to receive complaints transferred to it. It contains sections 32AC, 32AD and 32AE.

Part IIIA – Relationships with other agencies and information sharing

Section 32AC Information sharing with integrity bodies

625. Section 32AC allows the IGIS to share information or documents with other integrity bodies. This is necessary to manage concurrent jurisdiction between the IGIS and other integrity bodies who have oversight over the ACIC and the AFP unrelated to network activity warrants. This clause is not intended to limit the Inspector-General’s existing powers, functions and duties in relation to the sharing of information.

626. It is intended that the provision would reduce the potential for duplication of individual oversight activities by integrity bodies through the sharing of information and cooperation. For example, if the IGIS were to share information with another integrity body it may enable that integrity body to satisfy itself that there are no further issues arising in respect of its specific statutory functions that would require it to undertake separate oversight activity in relation to that matter. For example, this could arise in relation to the AFP where both the IGIS and Ombudsman could have jurisdiction over a matter, and allowing the IGIS to share contextual information with the Ombudsman could assist that body to determine that the IGIS is the appropriate oversight agency. Sharing information to avoid duplication reduces administrative burdens on both overseen agencies and integrity bodies.

627. The provision also supports cooperation and coordination across integrity bodies, by allowing the IGIS to share information about its investigative processes and methodologies, as well as trends they have identified through its oversight.

628. It is also intended that this provision supports the IGIS to manage concurrent jurisdiction that may arise in relation to Commonwealth agencies other than intelligence agencies, if the IGIS is directed by the Prime Minister to inquire into an intelligence or a security matter relating to one or more of those agencies under section 9 of the IGIS Act.

629. The IGIS’s information sharing function would be subject to the following safeguards. Firstly, the IGIS may only share information it has obtained by exercising its duties, functions or powers (as an IGIS official). Secondly, the IGIS may only share information that is relevant to the receiving agency’s functions. Finally, the IGIS must be satisfied, on reasonable grounds, that the receiving agency has appropriate arrangements in place to protect the shared information.

630. Finally, the IGIS, like all agencies, is bound by the Protective Security Policy Framework (PSPF), as well as the offences that govern the unauthorised sharing of classified information in the Criminal Code. Additionally, section 34 of the IGIS Act provides that the IGIS may only disclose information in the performance of legislated functions, powers or duties. Improper disclosure of information by an IGIS official is a criminal
offence, punishable by 2 years imprisonment, a fine of 50 penalty units, or both. These provisions provide a substantial protection mechanism against improper disclosure.

**Section 32AD Transferring complaints to other integrity bodies**

631. New section 32AD provides that where the IGIS determines that a complaint could be more effectively or conveniently dealt with by another integrity body (under new subsection 11(4A)), the IGIS may transfer all, or part, of that complaint to that integrity body.

632. Currently, the IGIS does not have any capacity to transfer complaints to other integrity bodies. This creates additional administration for both integrity bodies and complainants where complaints must be re-made to the appropriate integrity body. The complaints transfer scheme is intended to assist complainants, by removing the need for them to re-submit their complaints to other integrity body. Complaints-transfer provisions are common within the legislation of integrity bodies (including the AHRC Act, Privacy Act, Ombudsman Act and Defence Act 1903 (Defence Act)), and support cooperation between integrity bodies.

633. This item would also insert a note following section 32AD, to draw readers’ attention to the corresponding ‘deeming provisions’ in the governing legislation of the integrity body to which the IGIS transfers a complaint. These deeming provisions state that a complaint that is transferred by the IGIS to another integrity body is taken to be a complaint made to that body for the purposes of its governing legislation. This note signposts where the IGIS Act interacts with other integrity bodies’ primary legislation and is intended to assist with interpreting the Act.

634. This item does not include a specific reference to the IGADF in the note to s32AG. Under the IGADF’s functions (as outlined in section 110C of the Defence Act), the IGADF is able to do anything incidental or conducive to the performance of its functions. The functions of the IGADF include to “inquire into or investigate matters concerning the military justice system” as well as any functions conferred on the IGADF by the Defence Act, other Commonwealth laws, or regulations. Relevantly, the Inspector-General of the Australian Defence Force Regulation 2016 allows the IGADF to consider complaints in particular circumstances. These provisions, read together, clearly allow the IGADF receive transferred complaints as being incidental to their functions. As such, it was not necessary to draft a specific deeming provision in the Defence Act, and the IGADF was not included in the note. This should not be read to infer that the IGIS cannot transfer complaints to the IGADF.

**Section 32AE Complaints transferred by integrity bodies**

635. Section 32AE would provide that where an integrity body has transferred a complaint to the IGIS, that complaint is deemed to have been made to the IGIS under the IGIS Act. This will ensure that the complainant does not need to re-submit the original complaint to
the IGIS, and that the IGIS has a legal basis to handle transferred complaints. It also ensures that the complainant is protected under the IGIS Act for any disclosure of information.

636. The item also inserts a note following new section 32AE, to draw readers’ attention to the provisions in other integrity bodies’ legislation that permits the transfer of complaints to the IGIS. This note would signpost where the IGIS Act interacts with other integrity bodies’ primary legislation and is intended to assist with interpreting the Act.

637. It is noted that there is no ‘transfer provision’ in the LEIC Act. This is due to the broad information-sharing powers available to the Integrity Commissioner under which complaints may be transferred to another integrity body. However, as these powers are not specific to transferring complaints, they have not been listed in the note to section 32AE. The absence of a reference to the LEIC Act here does not infer that the IGIS may not receive complaints transferred to it by ACLEI.

Item 72 – At the end of subsection 32A(1)

638. This item inserts new paragraphs 32A(1)(e) and (f). Section 32A(2) allows the IGIS to request intelligence agencies’ reports, providing an avenue for agency heads to voluntarily provide information to the IGIS. Subsection 32A(1) provides that the IGIS may request access to annual or periodic reports prepared by intelligence agencies and provided to Ministers or the Secretary of the Defence Department (depending on the specific intelligence agency).

639. New paragraph 32A(1)(e) would extend the powers in subsection 32A(2) to cover documents which relate to the ACIC and the AFP. These documents would include those issued by the ACIC and the AFP under section 46 of the Public Governance, Performance and Accountability Act 2013, and any other report that the IGIS believes relates to one of these agencies’ intelligence functions (as defined in the IGIS Act), provided that such a report is prepared on a periodic basis and is given to the responsible Minister.

640. New paragraph 32A(1)(f) applies specifically to the ACIC. It would allow the IGIS to request copies of a report that relates to the ACIC’s intelligence function that is provided to the Board of the ACIC or the Inter-Governmental Committee (so long as that report was prepared by the ACIC CEO or the Chair of the Board). This provision reflects the organisational structure of the ACIC, and that there may be reports that are provided to the Board or Inter-Governmental Committee rather than the Minister. As the Board and Inter-Governmental Committee serve analogous roles to that of a Minister, it is appropriate that the IGIS is able to access reports to these entities where they relate to the performance of the ACIC’s intelligence functions under the IGIS Act.

641. This item is necessary to give effect to the IGIS’s expanded jurisdiction over the ACIC and the AFP, and to ensure that oversight of intelligence agencies is consistent across the National Intelligence Community.
Item 73 – After paragraph 32A(5)(a)

642. This item inserts new paragraph 32A(5)(aa). Subsection 32A(5)(a) provides that where the head of ASIO, ASIS, ASD and ONI have not provided the responsible Minister with a copy of report outlined in section 32A(1), the agency head need not give a copy of the report to the IGIS until the head has given the report to the responsible Minister.

643. New paragraph 32A(5)(aa) ensures this also applies to ACIC and AFP reports at paragraphs 32A(1)(e) and (f).

Item 74 – At the end of section 32A

644. This item inserts subsection 32A(6), which deals specifically with ACIC reports to the Board or Inter-Governmental Committee. It provides that where the IGIS requests a report from the ACIC, and that report is provided to the Board or Inter-Governmental Committee (rather than the Minister), that the ACIC CEO is not required to provide a copy of the report to the IGIS until the report has been given to the Board of Inter-Governmental Committee (as appropriate).

645. This provision reflects the organisational structure of the ACIC, and that there may be reports that are provided to the Board or Inter-Governmental Committee rather than the Minister. As the Board and Inter-Governmental Committee serve similar roles to that of a Minister, it is appropriate that the IGIS is able to access reports that are for these entities on similar terms to Ministerial reports.

Item 75 – Subsections 32B(2) and (4)

646. This item repeals subsections 32B(2) and 32B(4) and substitute new subsections 32B(1A) and 32B(2).

647. Subsection 32B(1A) would extend the existing provisions of section 32B to apply to the ACIC and AFP (in relation to their intelligence functions under the IGIS Act). That is, section 32AB also applies to guidelines or directions issued by the responsible Minister to the ACIC and the AFP, and to guidelines and directions issued to the ACIC by the ACIC Board or Inter-Governmental Committee.

648. New subsection 32B(2) would reproduce the provisions in existing subsection 32AB(2), but would also require the CEO of the ACIC to give a copy of the direction or guideline to the IGIS as soon as practicable, where the decisions are given to the ACIC by the Board of ACIC or by the Inter-Governmental Committee.

649. This amendment is necessary to give effect to the IGIS’s new jurisdiction over the ACIC and the AFP’s use of network activity warrants, and to ensure its oversight of these agencies’ use of the power is consistent with other NIC agencies.
650. The repeal of 32B(4) is consequential to the insertion of new subsection 32B(2), as this subsection defined a term that is no longer used in the section.

**Item 76 – After section 34B**

**34C No evidential burden for IGIS officials in relation to defences to secrecy offences**

651. New section 34C would provide that in any prosecution against an IGIS official for the disclosure of information, that IGIS official will not bear any evidential burden as to whether the disclosure of information is for the purposes of, or in connection with, that or any other IGIS official exercising a power, or performing a function or duty, as an IGIS official.

652. Under section 13.3 of the Criminal Code, the default position is that a person seeking to raise a defence or exception to an offence will bear an evidential burden in relation to that defence. A person bearing an evidential burden is required to lead evidence that points to the reasonable possibility that a matter exists.

653. IGIS officials are subject to strict secrecy offences under section 34 of the IGIS Act which prevent IGIS officials from disclosing ‘any information’ obtained in the course of their duties to any person, including to a court. As such, an IGIS official is not permitted to adduce any evidence in a court hearing without breaching the secrecy offences in their primary legislation. Given the importance of ensuring the security of information provided to, or obtained by, the IGIS in the course of its duties, it is appropriate to shift the evidential burden to the prosecution.

654. This provision is intended to cover the field in terms of secrecy offences. It is intended that this provision would cover offences with physical elements such as: “communicat[ing]”, “deal[ing] with” (e.g. section 18B of the ASIO Act). It is also intended to apply in situations such as section 3ZQT of the Crimes Act or section 29B of the ACC Act (which are about disclosing the existence of a notice).

**Law Enforcement Integrity Commission Act 2006**

655. The Bill introduces new oversight arrangements for the AFP and the ACIC by the IGIS in relation to network activity warrants. The Law Enforcement Integrity Commissioner currently has jurisdiction over AFP and the ACIC where it is within their functions outlined in section 15 of the LEIC Act. In the event that a complaint is made to, or a matter brought to the attention of, the Integrity Commissioner that may be more appropriately dealt with by the IGIS, amendments to the LEIC Act are required to facilitate the transfer of that complaint and associated information to IGIS officials.
Item 77 – Subsection 5(1)

656. This item inserts a new definition of *IGIS official* in subsection 5(1) of the LEIC Act. This definition would be inserted into a number of Acts and provides a consistent way to refer to both the IGIS, and any other person covered by subsection 32(1) of the IGIS Act.

Item 78 – Subsection 5(1) (paragraph (b) of the definition of law enforcement secrecy provision)

657. This item amends the definition of ‘law enforcement secrecy provision’ in the LEIC Act to include section 45B of the SD Act in addition to section 45. This amendment ensures that information obtained under network activity warrants (*protected network activity warrant information*) is afforded the same protections for use and disclosure under the LEIC Act as information obtained under the existing SD Act framework.

Item 79 – After section 23

23A Transfer of complaints from the Inspector-General of Intelligence and Security

658. This item inserts new section 23A. New section 23A would ensure that when the IGIS transfers a complaint to the Integrity Commissioner under proposed section 32AG of the IGIS Act, that complaint is deemed to have been referred under subsection 23(1) of the LEIC Act. This is intended to ensure that there is a clear pathway for the IGIS to transfer a case to the Integrity Commissioner where it is appropriate to do so and resolve any ambiguities between the transfer provisions in the IGIS Act and the referral provisions in the LEIC Act.

Item 80 - After subsection 90(3A)

659. This item inserts new subsections 90(3B), (3C) and (3D).

Disclosure to IGIS officials

660. Subsection 90(1) of the LEIC Act allows the Integrity Commissioner to issue directions limiting the use and disclosure of hearing material (within the meaning of that Act), subsection 90(6) makes it an offence to contravene such a direction (unless the use or disclosure is under subsection 90(4) or (5).

661. New subsection 90(3B) would provide that nothing in such a direction would prevent the disclosure of hearing material to an IGIS official, or the IGIS official using the hearing material for the exercise of the IGIS official’s powers or functions. This would create a default position which supports the ability of the IGIS to obtain all necessary information to support its oversight functions.

662. New subsection 90(3C) would provide that the Integrity Commissioner may direct (under subsection 90(1)), in the circumstances where the use or disclosure of the hearing
information would be reasonably likely to prejudice the performance of functions or exercise of powers of the Integrity Commissioner, that subsection 90(3B) does not apply.

663. New subsection 90(3D) would require the Integrity Commissioner to inform the IGIS as soon as practicable after giving a direction in accordance with subsection 90(3C).

664. This item is intended to provide an appropriate balance between the IGIS’s need to access information for an inquiry, and the secrecy necessary to avoid compromising the Integrity Commissioner’s powers and functions. It is important to note that while a person would be prevented from disclosing information that is subject to a section 90(1) direction voluntarily to the IGIS, the IGIS would be able to obtain this information through its powers at section 18 of the IGIS Act.

Item 81 – After paragraph 208(3)(a)

665. Subsection 207(1) of the LEIC Act contains a secrecy offence that limits the circumstance in which ACLEI staff can record, communicate or divulge information certain information disclosed or obtained under, or for the purposes of, the LEIC Act.

666. Section 208 contains exceptions to that offence. Subsection 208(3) provides that the Integrity Commissioner may disclose information to the heads of specified agencies. Subsection 208(6) provides that the Integrity Commissioner may disclose information where they are satisfied that it is necessary to do so to protect a person’s life or physical safety. Subsection 208(7) limits subsections 208(3) and (6) providing that information cannot be disclosed under those subsections where the information is section 149 certified information and doing so would contravene a section 149 certificate.

667. This item adds the IGIS to the list of specified agencies in subsection 208(3), ensuring that the Integrity Commissioner could provide relevant information to the IGIS.

668. This item is intended to ensure that the IGIS would have access to information relevant to an inquiry despite any bar under subsection 207(1) or section 149.

Items 82 – Subsection 208(7)

669. This item provides that disclosure under subsection 208(3) and (6) would be possible, regardless of whether the information is certified under section 149, when the information is disclosed to the IGIS for the purposes of the IGIS’s functions.

670. This item is intended to ensure that the IGIS would have access to information relevant to an inquiry despite any bar under subsection 207(1) or section 149.

671. A disclosure authorised under subsection 208(3) would still be subject to any directions under section 90 (i.e. the Integrity Commissioner would be able to direct that the information not be voluntarily provided to IGIS where doing so would be reasonably likely to prejudice the Integrity Commissioner’s functions).
Items 83 – At the end of section 208

672. This item inserts new subsection 208(8) which would require the Integrity Commissioner to notify the Attorney-General where they intend to provide section 149 certified information to the IGIS. This is intended to allow the Attorney-General to have visibility of where information that they have certified as being of a highly sensitive nature is being made available to the IGIS, but will not prevent the disclosure of that information. This protects the independence of the IGIS, while maintaining the security of information.

Ombudsman Act 1976

673. The Bill introduces new oversight arrangements for the AFP and the ACIC by the IGIS in relation to network activity warrants. The Ombudsman currently has jurisdiction over the AFP and the ACIC where it is within their functions outlined in section 5 of the Ombudsman Act Ombudsman Act, or where the Ombudsman is responsible for oversight of specific powers such as in the SD Act or TIA Act. In the event that a complaint is made to, or a matter brought to the attention of, the Ombudsman that may be more appropriately dealt with by the IGIS, amendments to the Ombudsman Act are required to facilitate the transfer of that complaint and associated information to IGIS officials.

Item 84 – Subsection 3(1)

674. This item provides that examiner of ACC has the meaning given by the ACC Act. An examiner of the ACIC is a person appointed under subsection 46B(1) of the ACC Act by the Governor-General.

Item 85 – After section 5A

5B Transfer of complaints from the Inspector-General of Intelligence and Security

675. This item inserts new section 5B. New section 5B would ensure that when the IGIS transfers a complaint relating to action taken by the ACIC (except action taken by an examiner) or the AFP to the Ombudsman under new section 32AD of the IGIS Act that complaint is deemed to have been made under the Ombudsman Act. This is intended to ensure that there is a clear pathway for the IGIS to transfer a complaint to the Ombudsman where it is appropriate to do so.

676. This item also inserts a note following this section, to draw the readers’ attention to the operation of new section 6F which allows the Ombudsman to transfer complaints to the IGIS. This is intended to signpost how complaints may be transferred between the IGIS and the Ombudsman, and their respective legislative bases.

Item 86 – Subsection 6A(1)

677. Section 6A of the Ombudsman Act provides the Ombudsman with the power to transfer complaints relating to the ACIC to other relevant integrity bodies.
678. This item would amend subsection 6A(1) to provide that the Ombudsman’s ability to transfer complaints about the ACIC is subject to new subsection 6A(3).

**Items 87 – At the end of section 6A**

679. This item inserts new subsection 6A(3) which would bar the Ombudsman from transferring a complaint or part of a complaint under section 6A that relates to action taken by the ACIC to the IGIS. This is intended to ensure that any transfer of complaints relating to the ACIC to the IGIS is done through new section 6F. As compared with section 6A, new section 6F would require the agreement of the IGIS before the Ombudsman could transfer a complaint.

680. New subsection 6A(3) is not intended to limit the transfer of complaints via new section 6F.

**Item 88 – After section 6E**

**6F Transfer of complaints to the Inspector-General of Intelligence and Security**

681. This item inserts new section 6F, which allows the Ombudsman to transfer complaints to the IGIS. This section is intended to manage duplication between oversight bodies by ensuring that the most appropriate integrity body is able to consider each specific complaint.

682. Subsection 6F(1) provides for when section 6F applies. This subsection is intended to ensure that the Ombudsman can only exercise the power to transfer complaints (or parts of complaints) to the IGIS in the appropriate circumstances. Specifically, the Ombudsman needs to be of the opinion that the complainant could or has complained to the IGIS under the IGIS Act in relation to action taken by the ACIC (except where that action is not taken by an examiner performing functions and exercising powers as an examiner as these matters are outside of the IGIS’s jurisdiction under new subsection 8A(3B), or the AFP, and that complaint would be more appropriately or effectively dealt with by the IGIS.

**Requirement to consult with Inspector-General of Intelligence and Security**

683. New paragraph 6F(2)(a) requires the Ombudsman to consult the IGIS about the complaint or part of the complaint that relates to the action.

684. New paragraph 6F(2)(b), provides the Ombudsman with the discretion to not investigate, or cease investigating the complaint (in which case subsection 6F(3) would apply, provided that the IGIS agrees to the transfer the complaint or the part of the complaint).
Transfer to Inspector-General of Intelligence and Security

685. New subsection 6F(3) provides that where the Ombudsman has decided to not investigate or not continue investigating the complaint, the Ombudsman must, with the consent of the IGIS:

- transfer the complaint (or part) to the IGIS
- give written notice to the complainant of the transfer, and
- give any related information or documents in the possession or control of the Ombudsman to the IGIS.

686. Notice to the complainant is required to be given ‘as soon as reasonably practicable’, however it is possible (for example if the complainant does not provide up to date contact details) that it may never be practicable to respond.

Relationship with other provisions

687. New subsection 6F(4) is intended to clarify that the requirements of section 6F do not apply to other powers to transfer complaints to the IGIS that the Ombudsman may have. For example, under section 43 of the PID Act, the Ombudsman could allocate the handling of a PID disclosure to the IGIS. Such an allocation would not need to meet the requirements of section 6F.

688. New subsection 6F(5) is intended to resolve any ambiguity between the action of new paragraph 6F(3)(c) and subsection 35(2) of the Ombudsman Act, ensuring that the secrecy provision located in section 35(2) does not apply when the Ombudsman officer is transferring information as part of the transfer of a complaint to the IGIS.

Item 89 – At the end of subsection 35(6)

689. Subsection 35(5) of the Ombudsman Act creates a secrecy offence that restricts officers (as defined in that Act) from divulging, communicating or furnishing certain information or documents that are the subject of certificate made by the Attorney-General made under that subsection. Subsection 35(6) creates exceptions to that offence.

690. This item inserts new paragraph 35(6)(d) creating a new exception to an offence under subsection 35(5). Specifically, new paragraph 35(6)(d) provides that subsection 35(5) would not prevent an officer from giving information or a document to the IGIS in accordance with section 35AB.

691. This item is intended to ensure that the IGIS could access information relevant to an inquiry.
Item 90 – After section 35AA

692. This item inserts new section 35AB, which relates to the disclosure of information and documents by the Ombudsman to the IGIS. The section applies if the Ombudsman:

- either obtained information or documents relating to Commonwealth agency performing functions under any Act; or when the Ombudsman prepares a report or other information in relation to a Commonwealth agency performing a function under any Act; and
- the Ombudsman is of the opinion that the information, document or report may be relevant to a function of the IGIS that relates to an intelligence agency the IGIS oversees, or an intelligence security matter relating to a Commonwealth agency.

693. New subsection 35AB(2) provides that nothing in the Ombudsman Act precludes the Ombudsman disclosing information, making a statement that includes information, or giving documents to the IGIS. ‘Information’ and ‘document’ in this case relate to the information or document that would cause section 35AB to apply due to the action of subsection 35AB(1).

694. Section 35AB is intended to ensure that the Ombudsman can provide the IGIS with information that is relevant to an inquiry despite any provisions of the Ombudsman Act which may otherwise restrict the release of relevant information or documents. This is necessary to reduce duplication in oversight between integrity bodies.

Item 91 – At the end of subsections 35B(1) and 35C(1)

695. Sections 35B and 35C relate to the disclosure of ACIC or ACLEI information (respectively) by the Ombudsman when the Attorney-General has certified that the disclosure of the information would be contrary to the public interest.

696. This item inserts an exception to the prohibition on the Ombudsman sharing such information. That exception would be where the information is provided to the IGIS in accordance with section 35AB of the Ombudsman Act. This is intended to clarify the interaction of sections 35B and 35C with section 35AB.

Privacy Act 1988

697. The Bill introduces new oversight arrangements for the AFP and the ACIC by the IGIS in relation to network activity warrants. The Information and Privacy Commissioner may currently inquire into certain matters relating to the AFP and the ACIC if it is within their functions outlined in the AIC Act or the Privacy Act. In the event that a complaint is made to, or a matter brought to the attention of, the Information and Privacy Commissioner that may be more appropriately dealt with by the IGIS, amendments to the Privacy Act are required to facilitate the transfer of that complaint and associated information to IGIS officials.
Item 92 – After section 49A

698. This item inserts new section 49B into the Privacy Act. New section 49B would provide that when a complaint or part of a complaint in respect of action taken by the ACIC or the AFP is transferred to the Information Commissioner under section 32AD of the IGIS Act that the complainant is deemed to have made a complaint to the Information Commissioner under subsection 36(1) of the Privacy Act.

699. This is intended to ensure that a complaint transferred to the Information Commissioner by the IGIS in respect of the ACIC or the AFP receives equivalent treatment to a complaint made directly to the Information Commissioner. For example, without this amendment the various circumstances in which the commissioner may or must not investigate under section 41 of the Privacy Act would not apply to a transferred complaint, as each subsection refers to ‘a complaint [that] has been made under section 36’.

Items 93 - Subsection 50(1) (after paragraph (e) of the definition of alternative complaint body)

700. This item facilitates the Information Commissioner transferring complaints to the IGIS.

701. Section 50 of the Privacy Act provides for the referral of complaints made to the Privacy Commissioner to other relevant bodies. This item expands the definition of ‘alternative complaint body’ to include the IGIS.

702. Subsection 50(2) of the Privacy Act includes a number of references to an ‘alternative complaint body’ including the ability under paragraph 50(2)(c), subject to certain conditions, to transfer a complaint to an alternative complaint body.

703. This item intended to provide the Information Commissioner with the ability to transfer cases to the IGIS when it is appropriate to do so, and to ensure that IGIS can investigate those complaints when it receives them.

Item 94 - After subparagraph 50(2)(a)(iv)

704. This item facilitates the Information Commissioner transferring complaints to the IGIS.

705. Paragraph 50(2)(a) provides the requirements for a complaint to the transferred to an ‘alternative complaint body’ under the Privacy Act. It provides that the complaint relating to the matter must have also been made, or could have been made, to one of the bodies listed at paragraph 50(2)(a).

706. This item inserts a new subparagraph 50(2)(a)(iva) to include the IGIS as a listed body. This means that the Information Commissioner may transfer all or part of a complaint to the IGIS if they consider that the complaint could be more conveniently or effectively dealt with by the IGIS.
707. This item is intended to provide the Information Commissioner with the ability to transfer cases to the IGIS when it is appropriate to do so, and to ensure that IGIS can investigate those complaints when it receives them.

**Item 95 - After subparagraph 50(3)(a)(iv)**

708. This item facilitates the Information Commissioner transferring complaints to the IGIS.

709. Paragraph 50(3)(a) deems a complaint that is transferred under subsection 50(2) to be a complaint that was made directly to the relevant body, as listed in the subparagraphs to paragraph 50(3)(a).

710. This item inserts new subparagraph (50)(3)(a)(iva) that would ensure that when a complaint is transferred to the IGIS under subsection 50(2) it can be treated the same way as a complaint made under the IGIS Act.

711. This item is intended to provide the Information Commissioner with the ability to transfer cases to the IGIS when it is appropriate to do so, and to ensure that IGIS can investigate those complaints when it receives them.

**Public Interest Disclosure Act 2013**

**Item 96 – Section 8**

712. This item amends section 8 of the PID Act by inserting new definitions.

713. *ACIC* means the Australian Criminal Intelligence Commission as established by the Australian Crime Commission Act 2002.

714. *Examiner* of the Australian Crime Commission has the meaning given by the ACC Act. An examiner of the ACIC is a person appointed under subsection 46B(1) of the ACC Act by the Governor-General.

715. *Intelligence function*, in relation to the ACIC or the AFP, has the meaning given by the Inspector-General of Intelligence and Security Act 1986.

**Item 97 – Section 34 (table item 1, column 2, after paragraph (c))**

716. Section 34 of the PID Act contains a table which sets out who is to be considered an authorised internal recipient of a disclosure, which varies based on the agency to which the conduct to be disclosed relates. Generally, an authorised internal recipient is a person to whom a PID must be made in the first instance (other than in the case of an emergency disclosure).

717. Item 1 of the table provides the potential authorised internal recipients of a disclosure, where the conduct with which the disclosure is concerned relates to an agency other than an intelligence agency, are the Ombudsman or the IGIS.
718. This item inserts paragraph (ca) in Column 2 of item 1. Paragraph (ca) provides that in the circumstance where the discloser believes on reasonable grounds that where their disclosure relates to action taken by the ACIC and the AFP in relation to that agency’s intelligence functions, and it is appropriate for the disclosure to be investigated by the IGIS then the IGIS would be an authorised internal recipient.

719. This is intended to mirror the arrangements for intelligence agencies found in paragraph (b) of item 2 of the same table.

**Item 98 – Section 42 (note 2)**

720. Note 2 of section 42 currently informs the reader that the way a disclosure is allocated may be the subject of a complaint to the Ombudsman under the Ombudsman Act, or, in the case of an intelligence agency, to the IGIS under the IGIS Act.

721. This item amends note 2 of section 42 to clarify that a disclosure may be the subject of complaint to the IGIS under the IGIS Act, where a disclosure relates to the intelligence functions of the ACIC and the AFP. This amendment reflects the IGIS’s expanded jurisdiction to oversee the intelligence functions (under the IGIS Act) of these agencies.

**Item 99 – Subparagraph 43(3)(a)(iii)**

722. Section 43 outlines the responsibilities of an authorised officer who has received a PID, and how they are to allocate that PID.

723. Section 43 provides that where a PID is made, the recipient of that PID must allocate that PID to one or more agencies for consideration. The recipient is not required to allocate the PID where the recipient is satisfied, on reasonable grounds, that there is no reasonable basis that the disclosure could be considered to be an internal disclosure (subsection 43(2)).

724. Subsection 43(3) provides the matters to which an authorised officer must have regard when determining which agency to refer the disclosure to. Paragraph 43(3)(a) requires the officer to have regard to the principle that an agency should not handle a disclosure unless certain conditions, specified in the subparagraphs, apply.

725. Existing subparagraph 43(3)(a)(iii) provides that IGIS should not handle a disclosure unless some or all of the suspected disclosable conduct relates to an intelligence agency.

726. This item amends subparagraph 43(3)(a)(iii) to instead require an authorised officer not to allocate the handling of a disclosure to the IGIS unless some or all of the suspected disclosable conduct relates to an intelligence agency, or the ACIC and the AFP in relation to their intelligence function (as defined in the IGIS Act). This is intended to reflect that IGIS oversight would now extend to the ACIC and the AFP in relation to network activity warrants.
**Item 100 – After subsection 43(3)**

727. This item inserts new subsection 43(3A). New subsection 43(3A) would provide that the authorised officer must not allocate the handling of the disclosure to IGIS where the disclosure relates to action taken by an ACIC examiner performing functions and exercising powers as an examiner. This is intended to reflect that the IGIS does not have any jurisdiction to consider the actions of ACIC examiners, as noted by new paragraph 8(3B)(a) of the IGIS Act.

**Item 101 – Paragraphs 44(1A)(a) and (b)**

728. Section 44 relates to the information that an authorised officer must share with the principal officer of the agency which has been allocated the disclosure.

729. Subsection 44(1) requires an authorised officer to provide to the principal officer of each agency which has been allocated the disclosure:

- the allocation itself
- the information that was disclosed, the suspected disclosable conduct, and
- the discloser’s name and contact details if they are available, and the discloser consents to the sharing of this information.

730. In addition to the agency which has been allocated the disclosure, subsection 44(1A) requires the authorised officer originally in receipt of the disclosure to provide the same information as provided in subsection 44(1) to other agencies in certain circumstances. Specifically:

- paragraph 44(1A)(a) requires the authorised officer to inform the Ombudsman where the disclosure is not allocated to the Ombudsman, the IGIS or an intelligence agency, and
- paragraph 44(1A)(b) requires the authorised officer to inform the IGIS where the disclosure is allocated to an intelligence agency.

731. This item amends paragraphs 44(1A)(a) and (b) so that the reference to “intelligence agencies” are extended to “intelligence agency or the Australian Crime Commission or the Australian Federal Police in relation to that agency’s intelligence functions”. As result, where a disclosure does relate to those agencies, the authorised officer will need to inform IGIS, and otherwise, if the issue has not been reported to the Ombudsman or the IGIS, to the Ombudsman. This is intended to reflect the extension of the IGIS’s oversight to include the ACIC and the AFP in relation to network activity warrants.

**Item 102 – Section 46 (note)**

732. Section 46 sets out a simplified outline of Division 2 of Part 3 of the PID Act, which relates to the obligations of the principal officer of the allocated agency to investigate and
report on the disclosure. A note to section 46 signposts that the way a disclosure is investigated (or refused) may be subject to a complaint to the Ombudsman under the Ombudsman Act, or in the case of an intelligence agency, to the IGIS under the IGIS Act.

733. This item updates the note in section 46 to clarify that the way a disclosure is investigated (or refused) may also be subject to a complaint to the Ombudsman under the Ombudsman Act, or, in the case of an intelligence agency, the ACIC or the AFP in relation to their intelligence functions, to the IGIS under the IGIS Act. This is intended to reflect the extension of the IGIS’s oversight to include these agencies as it relates to network activity warrants.

Item 103 – At the end of paragraph 50A(1)(b)

734. This item is a consequential amendment, adding the word “and”, to reflect the addition of new paragraph 50A(1)(c).

Items 104 – After paragraph 50A(1)(b)

735. Section 50A requires the principal officer of an agency which has been allocated a disclosure to notify the Ombudsman or IGIS of a decision under section 48 or 49 of the PID Act to not investigate the disclosure, or to not investigate the disclosure further.

736. Under existing section 50A, the principal officer is required to notify the Ombudsman where the agency is not the Ombudsman, the IGIS or an intelligence agency, and must notify the IGIS when the agency is an intelligence agency.

737. This item inserts paragraph 50A(1)(c) to the effect that the principal officer is required to notify the Ombudsman where the agency is the ACIC or the AFP and the disclosure does not relate to the intelligence functions of that agency.

738. This amendments is intended to reflect the expansion of the IGIS’s oversight to include the intelligence functions of the ACIC and the AFP.

Item 105 – Paragraph 50A(2)(b)

739. This item replaces existing paragraph 50A(2)(b) to the effect that the principal officer is required to notify IGIS when the agency is an intelligence agency, or where the agency is the ACIC or the AFP and the disclosure relates to the intelligence functions of that agency.

740. This amendment is intended to reflect the expansion of the IGIS’s oversight to include the intelligence functions of the ACIC and the AFP.

Item 106 – Subsection 52(4)

741. Section 52 requires investigations to be completed within 90 days after allocation of the disclosure, unless an extension is granted.
Subsection 52(4) provides the IGIS with the power to provide an extension where the agency is the IGIS or an intelligence agency, either under its own power, on application of the principal officer of the agency (where the agency is not IGIS) or on application by the discloser.

This item would amend subsection 52(4) to also permit the IGIS to extend the time limit for investigations undertaken by the ACIC or the AFP, where the disclosure relates to the intelligence functions of the agency.

This amendment is intended to reflect the expansion of the IGIS’s oversight to include the intelligence functions of these agencies.

**Item 107 – Section 58 (note)**

Section 58 provides a simplified outline of Division 1 of Part 4 of the PID Act. Division 1 of Part 4 relates to additional obligations placed on persons involved in the PID process, as well as providing additional functions to the Ombudsman and the IGIS.

The note to section 58 signposts that the way these additional obligations are complied with may be subject to a complaint to the Ombudsman under the Ombudsman Act, or, where the obligations relate to an intelligence agency, to the IGIS under the IGIS Act.

This item would amend the note to section 58 to clarify that the complaint may be to the IGIS in circumstances where the complaint relates to the actions of an intelligence agency, or where the complaint relates to the ACIC or the AFP in relation to the intelligence functions of that agency. This amendment is consequential to the expanded oversight of the IGIS to cover the intelligence functions under the IGIS Act of these agencies.

**Items 108 - After paragraph 63(a)**

Section 63 of the PID Act provides additional functions to the IGIS. Each of the paragraphs to section 63 specifies a new function or functions of the IGIS under the PID Act.

This item inserts new paragraph 63(aa) providing the IGIS with an additional functions of assisting principal officers, authorised officers, public officials, and former public officials in relation to the operation of the PID Act where it relates to the intelligence functions of the ACIC or the AFP.

New paragraph 63(aa) is intended to provide the IGIS with functions in relation to these agencies similar in scope to the existing powers provided by paragraph 63(a) in relation to the intelligence agencies already subject to IGIS oversight.
Item 109 – After paragraph 63(b)

751. This item would insert new paragraph 63(ba) providing the IGIS with additional functions of conducting educational and awareness programs concerning the PID Act, relating to the intelligence functions of the ACIC and the AFP, but only to the extent that the PID Act relates to one of those agencies, public officials who belong to that agency, or public officials who belonged to that agency.

752. New paragraph 63(ba) is intended to provide the IGIS with functions in relation to the ACIC and the AFP similar in scope to the existing powers provided by paragraph 63(b) in relation to the intelligence agencies already subject to IGIS oversight.

Item 110 – Section 63 (note)

753. This item would replace and substitute the existing note to section 63 of the PID Act. The new note is the same in substance as the existing note, except that it includes reference to the IGIS’s functions under section 8A of the IGIS Act regarding the intelligence functions of the ACIC and the AFP. This amendment is consequential to the expansion of the IGIS’s functions by new section 8A of the IGIS Act to include these agencies.

Item 111 – Transitional – Section 52 of the Public Interest Disclosure Act 2013

754. This item is a transitional provision to clarify that the amendment of section 52 of the PID Act made by this Part does not affect the continuity of a period that was extended, or further extended, under subsection 52(4) of that Act before the commencement of this item. This ensures that the amendment of section 52 by this Part is not taken to effect the continuity of any existing investigations under Part 3 of the PID Act.

Telecommunications (Interception and Access) Act 1979

755. Amendments to the TIA Act are provided for in the Bill as a result of the creation of the concept of network activity warrant intercept information. How network activity warrant intercept information can be used and disclosed is governed by the TIA Act, not the SD Act. These provisions replicate those provided for Schedule 1 in respect of data disruption intercept information.

Item 112 – Subsection 5(1)

756. This item inserts two new definitions into section 5(1) of the TIA Act.

757. Network activity warrant has the same meaning as in the SD Act. The SD Act provides that a network activity warrant is a warrant issued under section 27KM of that Act.

758. Network activity warrant interception information is the information obtained under a data disruption warrant through the means of intercepting a communication that is in transit over a telecommunications system.
759. Interception under a network activity warrant may only occur for the purposes of executing or facilitating the warrant. This is to ensure that where agencies are seeking to obtain intercept material for its own purpose, they must apply for, and be issued with, an interception warrant under Chapter 2 of the TIA Act.

**Item 113 – Subsection 5(1) (definition of restricted record)**

760. This item expands the definition of restricted record to now include records of data disruption intercept information and network activity warrant information.

**Item 114 – Subsection 5(1) (paragraph (b) of the definition of warrant)**

761. This item expands the definition of warrant to include network activity warrants. The effect of this amendment is that interception for the purposes of network activity warrants is not prohibited by the TIA Act as it constitutes interception under a warrant (paragraph 7(2)(b)).

**Item 115 – Paragraph 7(2)(bb)**

762. This item amends subsection 7(2)(bb) of the TIA Act to include reference to new subsection 27KP(9) of the SD Act. New subsection 27KP(9) governs the concealment of access under network activity warrants in the SD Act.

763. This item allows for, under paragraph 7(2)(bb), the interception of a communication under subsection 27KP(9) of the SD Act is permitted.

**Item 116 – After section 63AD**

**63AE Dealing in network activity warrant intercept information etc.**

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

765. Existing subsection 63(1) sets out a general prohibition on the use, recording and communication of lawfully intercepted information. Information is taken to be lawfully intercepted if it was obtained by intercepting a communication passing over a telecommunications system under a warrant.

766. This item inserts new section 63AE to provide exceptions to the general prohibition on dealing in network activity warrant intercept information.

767. Section 63AE allows a person, for the purposes of doing a thing authorised by a network activity warrant, to communicate to another person, make use of, make a record or, or give in evidence in a proceeding network activity warrant intercept information. The
intention is that intercepted information can be used or communicated for a purpose reasonably incidental to the purposes of carrying out computer access.

768. Section 63AE also allows a person to communicate network activity warrant intercept information to another person or make use or a record of that information if the information relates to involvement of a person in activities that, generally, exist in life threatening or emergency situations. These include:

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

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

770. New subsection 63AE(3) states that a person may, in connection with the performance by an IGIS official of the IGIS official’s functions or duties or the exercise by an IGIS official of the IGIS official’s powers communicate to the IGIS official, make use of, or make a record of, network activity warrant intercept information.

771. New subsection 63AE(4) states that an IGIS official may, in connection with the performance by the IGIS official of the IGIS official’s functions or duties or the exercise by the IGIS official of the IGIS official’s powers communicate to another person, make use of, or make a record of, network activity warrant intercept information.

772. New subsection 63AE(5) states that if information was obtained by intercepting a communication passing over a telecommunications system and the interception was purportedly for the purposes of doing a thing specified in a network activity warrant and the interception was not authorised by the network activity warrant then a person may, in connection with the performance by an IGIS official of the IGIS official’s functions or duties or the exercise by an IGIS official of the IGIS official’s powers communicate to the IGIS official, make use of, or make a record of, that information and an IGIS official may, in connection with the performance by the IGIS official of the IGIS official’s functions or duties or the exercise by the IGIS official of the IGIS official’s powers communicate to another person, make use of, or make a record of, that information.
New subsection 63AE(6) states that despite subsection 13.3(3) of the Criminal Code, in a prosecution for an offence against section 63 of this Act, an IGIS official does not bear an evidential burden in relation to the matters in subsection (4) or (5).

**Item 117 – Paragraph 67(1)(a)**

This item is a consequential amendment to clarify that subsection 67(1)(a) applies to network activity warrant intercept information.

Section 67(1)(a) deals with the permitted purposes for communicating information to another person only when in relation to the agency.

**Item 118 – Section 68**

Under section 68, the chief officer of an agency may communicate lawfully intercepted information under certain circumstances. This item will exclude network activity warrant interception information from being communicated under section 68.

**Item 119 – Subsection 74(1)**

Under section 74, a person may give lawfully intercepted information in evidence in an exempt proceeding.

This item ensures that a person may not give network activity warrant intercept information in evidence in an exempt proceeding.

**Item 120 – Subsection 75(1)**

Under section 75, a person may give information that has been intercepted in contravention of the prohibition in subsection 7(1) in evidence in an exempt proceeding under certain circumstances where there is a defect or irregularity with a warrant.

This item ensures that a person may not give network activity warrant intercept information in evidence in an exempt proceeding where there is a defect or irregularity in connection with the warrant.

**Item 121 – Paragraphs 77(1)(a) and (b)**

This item provides that intercept material is admissible in evidence in so far as new sections 63AE permits. This section permits the dealing of data disruption intercept information where very serious circumstances exist or where there is a purpose reasonably incidental to the purposes of carrying out computer access.

**Item 122 – After paragraph 108(2)(cc)**

This item inserts new paragraph 108(2)(cd) which provides an exception to the prohibition in subsection 108(1) on accessing a stored communication. The prohibition does not apply to accessing a stored communication under a network activity warrant.
Schedule 3 – Account takeover warrants

Crimes Act 1914

Item 1 – Subsection 3(1) (definition of law enforcement officer)

783. This item amends the definition of law enforcement officer in subsection 3(1) to provide that the meaning of this term does not apply in relation to the account takeover warrant provisions in new Part IAAC of the Crimes Act. Part IAAC introduces a new meaning of ‘law enforcement officer’ as it relates to account takeover warrants. A law enforcement officer may apply for the issue of an account takeover warrant.

784. In this new Part, a law enforcement officer means the AFP Commissioner, the Chief Executive Officer of the ACIC or a member of each of their staff. The definition of this term in Part IAAC is narrower than the definition provided for in subsection 3(1) which includes a member of a State or Territory police force, a staff member of ACLEI, a Customs officer, or a member of a foreign law enforcement agency.

Item 2 – Subsection 3LA(6) (penalty)

785. This item makes a correction to subsection 3LA(6) by removing the words ‘for contravention of this subsection’ from the penalty for the aggravated offence for not complying with an order to provide information or assistance under section 3LA. The words ‘for contravention of this subsection’ are extraneous to the effect of this provision. The omission has been made for consistency with subsection 3LA(5).

Item 3 – At the end of section 3LA

Additional use of information etc.

786. Existing section 3LA allows a constable to make an application to a magistrate for an order requiring certain persons (such as owners or users of a device) to provide any information or assistance to allow law enforcement to access data held in, or accessible from, a computer that has been seized, moved or found in the course of a section 3E search warrant. For example, a section 3LA order may be used to compel a person to provide their password to assist law enforcement in obtaining access to data held in a computer found or seized under a search warrant.

787. This item inserts new subsection 3LA(7) which provides for the additional use of information or assistance provided as a result of an order made under section 3LA. Information or assistance provided under section 3LA for an investigation into an alleged offence under a search warrant may be used in the execution of an account takeover warrant that relates to that same investigation.

788. The inclusion of this provision overrides the principle that information obtained under a power conferred by statute can only be used or disclosed for the purpose for which it was
obtained. In the case of a section 3LA assistance order, this would be for the purposes of executing a search warrant under section 3E. The intent of this amendment is to ensure that information obtained under a section 3LA assistance order can be used in the execution of an account takeover warrant. Account takeover warrants are designed to complement the use of other investigatory powers, including search warrants, to authorise the taking control of a person’s online account in the investigation of serious offences.

789. Often, it will be the case that an account takeover warrant will be sought in the context of executing a section 3E search warrant. While seeking to obtain access to data held in a computer under a search warrant, law enforcement may obtain a person’s password or account credentials through the provision of assistance under section 3LA. This amendment ensures that such information could also be used for the purposes of taking control of an online account under an account takeover warrant but only where the matter relates to the same investigation.

Item 4 – After Part IAAB

Part IAAC – Account takeover warrants

790. This item inserts new ‘Part IAAC – Account takeover warrants’ into the Crimes Act. This new Part provides for the application and issuance of account takeover warrants, as well as the associated use and disclosure provisions, reporting obligations and oversight mechanisms.

Division 1 – Introduction

791. New Division 1 of Part IAAC is the first of eight divisions which set out the new account takeover warrant framework in the Crimes Act. This Division introduces and defines key concepts with respect to the account takeover warrant provisions.

3ZZUJ Simplified outline of this Part

792. Section 3ZZUJ provides a simplified outline of new Part IAAC. This outline summarises the key elements of the new account takeover warrant framework in Part IAAC for ease of reference in the Crimes Act.

793. An account takeover warrant may be issued by a magistrate to authorise the AFP or the ACIC to take control of one or more online accounts. In order to apply for an account takeover warrant, there must be reasonable grounds to suspect that a relevant offence is being, or is likely to be, committed and investigated, and taking control of an online account is necessary for the purposes of enabling evidence to be obtained of the commission of those offences in the course of that investigation (see section 3ZZUN). An emergency authorisation for taking control of an online account may also be given by an appropriate authorising officer (see section 3ZZUX). Such an authorisation is subject to approval by a magistrate (see sections 3ZZVA, 3ZZVB and 3ZZVC).
The magistrate may make an order requiring a person to provide any information or assistance that is reasonable and necessary to allow law enforcement to take control of the online account (see section 3ZZVG).

Information obtained under, or relating to, an account takeover warrant or emergency authorisation must not be used or disclosed by any person unless a relevant exception applies (see Division 4). Reporting and record-keeping requirements apply to the AFP and the ACIC in relation to account takeover warrants and emergency authorisations (see Division 5). The Commonwealth Ombudsman is empowered to inspect the records of the AFP and the ACIC to determine the extent of their compliance with the account takeover warrant provisions (see Division 6).

The note at the end of the simplified outline provides that Part IAAC confers non-judicial functions and powers on magistrates. This note points to section 4AAA which should be read in conjunction with these provisions. Section 4AAA deals with the conferral of non-judicial functions and powers on magistrates. A magistrate is defined in section 16C of the Acts Interpretation Act 1901 to mean any magistrate in respect of whose office an annual salary is payable. A magistrate may also refer to a chief, police, stipendiary, resident or special magistrate, or any other magistrate.

Under section 4AAA, a function or power conferred on a magistrate under a law of the Commonwealth relating to criminal matters is so conferred only in a personal capacity, not as a court or a member of a court (subsection 4AAA(2)). Further, a magistrate has the same protection and immunity as if he or she were performing such a function or exercising such a power as, or as a member of, a court (subsection 4AAA(4)). The inclusion of this note clarifies that these provisions apply in relation to magistrates due to their functions and powers in relation to the issue of account takeover warrants in Part IAAC.

3ZZUK Definitions

This section inserts definitions for terms that facilitate the operation of the new account takeover warrant provisions.

An account has the same meaning as in the Enhancing Online Safety Act 2015. The definition is not exhaustive, and it includes a free account, a pre-paid account and anything that may reasonably be regarded as the equivalent of an account. For the purposes of the account takeover warrant provisions, an account is an online account.

The purpose of including this definition is to ensure that an account takeover warrant may be sought by the AFP or the ACIC in order to take control of an online account if doing so is necessary for enabling evidence to be obtained of the commission of relevant offences. The account that may be taken control of by law enforcement under this warrant must be an online account, this may be a free account, a pre-paid account or anything that may reasonably be regarded as the equivalent of an account.
801. **Account-based data** has the same meaning as in Part IAA. Existing section 3CAA provides that account-based data includes data associated with an account for an electronic service with end-users that is either held by a person or is used, or likely to be used, by a person. Account-based data includes data that is accessible from the online account, such as messages and posts, and data that is otherwise associated with the account. The meaning of account-based data also applies in relation to deceased persons who, prior to their death, either held or used the account.

802. A person is taken to hold an account with the electronic service if they use, pay or manage an account, whether or not the account is in a particular name of a person or whether the person created the account. A person who inherits an account, establishes an account in a false name, shares an account, has an account established in his or her name, or attempts to anonymise an account, is still taken to hold the account. An account that is used, or likely to be used, by a person could include an account held by a person (such as a family member, friend or business associate) but utilised by the first-mentioned person.

803. The inclusion of this definition ensures that the AFP or the ACIC will be able to access account-based data for the purposes of taking control of an online account under an account takeover warrant.

804. **Account credentials** is defined to mean information that a user of an online account requires in order to access or operate the account. Some examples of account credentials include a username, password, PIN, security question and answer, and a biometric form of identification (such as facial recognition or fingerprint scanner). The definition of account credential is not exhaustive.

805. This definition is included to ensure that the AFP or the ACIC will be able to add, copy, delete or alter account credentials for the purposes of taking control of the online account. It will often be necessary to deny the account holder or user access to the account to ensure that law enforcement is able to obtain exclusive access to that account. This will most often be achieved by, for example, changing the passwords to the account and locking the person out in order for law enforcement to take control of the account under the account takeover warrant.

806. An **account takeover warrant** is a warrant issued under section 3ZZUP or subsections 3ZZVC(2) or (3). Section 3ZZUP allows a magistrate to issue a warrant, upon he or she being satisfied that there are reasonable grounds for the suspicion that taking control of an online account is necessary in an investigation for the purposes of enabling evidence to be obtained of the commission of relevant offences. Subsections 3ZZVC(2) and (3) allow a magistrate to issue an account takeover warrant as if an application for the approval of the giving of an emergency authorisation were an application for an account takeover warrant under 3ZZUN.

807. An **appropriate authorising officer** is a term used in Division 3 with respect to emergency authorisations. This term has the meaning given to it by section 3ZZUM. An
appropriate authorising officer means an officer authorised to give an emergency authorisation for taking control of one or more online accounts under section 3ZZUX. An appropriate authorising officer means, in relation to the AFP, the Commissioner of the AFP, the Deputy Commissioner of the AFP or an authorised senior executive service employee of the AFP. In relation to the ACIC, an authorising officer means the Chief Executive Officer of the ACIC or an authorised executive level member of the staff of the ACIC. The inclusion of this definition is necessary to facilitate the operation of the emergency authorisation provisions in Division 3.

808. **Carrier** means a carrier or carriage service provider within the meaning of the *Telecommunications Act 1997*. This Act defines carrier to mean the holder of a carrier license granted under that Act. A carriage service provider means a person who supplies, or proposes to supply, certain carriage services. A carrier operates telecommunications networks and infrastructure, whereas a carriage service provider uses the carrier networks to provide services such as phone and internet. This definition is inserted to facilitate provisions that allow the use of a telecommunications facility operated or provided by a carrier for the purposes of taking control of an online account under the warrant.

809. A **chief officer** means, in relation to the AFP, the Commissioner of the AFP and, in relation to the ACIC, the Chief Executive Officer of the ACIC. The chief officer of the agency to which an account takeover warrant is issued has certain obligations, including record-keeping and reporting requirements, under this Part. The inclusion of this definition allows these provisions to operate as intended.

810. A **communication in transit** means a communication passing over a telecommunications network within meaning of the *Telecommunications Act 1997*. The communication may be between persons and persons, things and things or persons and things, and may be in the form of speech, music or other sounds, data, text, visual images (animated or otherwise), signals or any other form or combination of forms. The communication must be passing over a system or series of systems that carries communications by means of guided or unguided electromagnetic energy.

811. This term has been inserted to facilitate provisions that allow the use of a communication in transit, and the adding, copying, deleting or altering of data in the communication transit if necessary for the purposes of taking control of an online account. Paragraph 3ZZUR(2)(d) provides that a magistrate may authorise these activities under an account takeover warrant if it is reasonable in the circumstances after having regard to the effectiveness of any other methods of taking control of the account.

812. **Computer** means all or part, or any combination, of one or more computers, computer systems or computer networks. This term is defined as such in the *Australian Security Intelligence Organisation Act 1979* and *Surveillance Devices Act 2004*. The inclusion of this definition ensures consistency in references to computer in related powers conferred under those Acts. This definition is inserted to facilitate the provisions that allow for the use of a computer for the purposes of taking control an online account under the warrant.
Electronic service has the same meaning as in the Enhancing Online Safety Act 2015. In that Act, electronic service means a service that either allows end-users to access material using a carriage service, or, a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service. This does not include a broadcasting service, or a datacasting service (as defined in the Broadcasting Services Act 1992).

The purpose of including this definition is to clarify the meaning of key terms that facilitate the operation of the account takeover warrant provisions. An account takeover warrant can be sought in order to take control an online account. An online account is an account that an electronic service has for end-users, and taking control of an online account involves taking steps that result in obtaining exclusive access to that account (including by altering account credentials).

For the purposes of the account takeover warrant provisions, examples of an electronic service may include a website, social media platform or online gaming service which people can have account-based membership or subscription to, as these services on carriage services to enable access to, and delivery of, content.

Emergency authorisation is defined to mean an emergency authorisation given under section 3ZZZURA. Under this section, an emergency authorisation may be given for taking control of one or more online accounts in response given in response to an application under section 3ZZUX. Law enforcement officers may apply to an appropriate authorising officer for an emergency authorisation for taking control of one or more online accounts where there is an imminent risk of serious violence or substantial damage to property and taking control of an online account is immediately necessary to deal with that risk. This definition is included to ensure that law enforcement officers are able to take control of one or more online accounts in emergency situations without first having to apply to a magistrate.

Executing officer is defined to mean one of three things in relation to account takeover warrants.

Firstly, an executing officer may be a law enforcement officer named in the warrant by the magistrate as being responsible for executing the warrant.

Secondly, an executing officer may be another officer whose name has been written in the warrant by the officer who was originally named in the warrant, if that officer does not intend to execute the warrant themselves.

Thirdly, an executing officer may be another officer whose name has been written by the last named officer in the warrant. The inclusion of this definition builds flexibility into the account takeover warrant by allowing the officer responsible for executing an account takeover warrant to change flexibly over time to meet the operational need. For example, where upon executing the warrant, it becomes apparent that the responsible officer named
in the warrant does not have the relevant technical capability to access an account, that officer may name another officer with the technical expertise to execute the warrant.

821. A **formal application** is an application for an account takeover warrant made by means of a written document signed by the applicant (paragraph 3ZZUN(2)(a)). An application for an account takeover warrant must provide sufficient information to enable the issuing authority to decide whether or not to issue the warrant.

822. An application for an account takeover warrant must be made formally, in writing, unless he or she has reason to believe that the delay caused by making a written application may affect the success of the investigation. In such urgent circumstances, the applicant may apply for an account takeover warrant orally or remotely.

823. **IGIS official** is defined to mean the Inspector-General of Intelligence and Security, or another person covered by subsection 32(1) of the Inspector-General of Intelligence and Security Act 1986. The term IGIS official provides a consistent way to refer to the Inspector-General of Intelligence and Security and a member of his or her staff employed to assist in the performance of functions and exercise of powers.

824. This definition is included to ensure that information obtained under, or relating to, an account takeover warrant may be disclosed to an IGIS official for the purposes of exercising powers or performing functions or duties as an IGIS official. While the account takeover warrant will be subject to oversight by the Commonwealth Ombudsman, it may be necessary in some circumstances to disclose information to the Inspector-General of Intelligence and Security if the matter is relevant to his or her functions, duties or powers.

825. A **law enforcement agency** means the AFP or the ACIC. This definition is inserted to ensure that account takeover warrants may only be sought by the AFP or the ACIC as law enforcement agencies. These warrants are not available to any other agency.

826. A **law enforcement officer** means, in relation to the AFP, the Commissioner of the AFP, a Deputy Commissioner of the AFP, an AFP employee, or a special member of the AFP (within meanings of the terms in the Australian Federal Police Act 1979). In relation to the ACIC, a law enforcement officer means the Chief Executive Officer of the ACIC or a member of the staff of the ACIC (within meaning of the Australian Crime Commission Act 2002).

827. This definition is included to differentiate the meaning of law enforcement officer in the account takeover warrant provisions in Part IAAC from the rest of the Crimes Act. Subsection 3(1) includes a broader definition of the term that applies to the Crimes Act except for Part IAAC. This term is defined to ensure that a law enforcement officer of the AFP or the ACIC may apply for the issue of an account takeover warrant under section 3ZZUN.
828. An Ombudsman official is defined to mean the Ombudsman, a Deputy Ombudsman, or a person who is a member of the staff referred to in subsection 31(1) of the Ombudsman Act 1976. This term provides a consistent way to refer to the Ombudsman and a member of his or her staff employed to assist in the performance of functions and exercise of powers by the Ombudsman. This definition is included to ensure that the restrictions on the use or disclosure of information obtained under, or relating to, an account takeover warrant do not apply if the disclosure was made by an Ombudsman official.

829. An online account is an account that an electronic service has for an end-user. This definition should be read in conjunction with the definition of account which includes a free account, a pre-paid account, or anything that may reasonably be considered an account. An online account may include, for example, an email service, Facebook account, Reddit subscription, Twitter profile, a log-in to a commentary section on a news website, a user of a messaging service such as WhatsApp or an account on a dark web forum or marketplace.

830. An online account is an important concept for the account takeover warrant provisions in Part IAAC. Account takeover warrants enable the AFP or the ACIC to take control an online account in an investigation to enable evidence to be obtained of relevant offences. This will allow law enforcement to use the trusted relationships and networks which have been built between criminal associates against those same criminals. In many cases, taking control of an online account will, when used in conjunction with other investigatory powers, be an efficient method for law enforcement to penetrate online networks, uncover the identities of criminal actors and gather evidence on the commission of serious offences online.

831. Protected information means any information obtained under, or relating to, an account takeover warrant or emergency authorisation. This includes information relating to an application for, the issue of, the existence of, or the expiration of, an account takeover warrant or emergency authorisation or an application for approval of the giving of an emergency authorisation. Information obtained under, or relating to, an account takeover warrant or emergency authorisation is protected by restrictions on use and disclosure in Division 4. This information cannot be used or disclosed, except in certain circumstances which are provided for in section 3ZZVH. A person will commit an offence for unlawfully using or disclosing protected information.

832. Including this definition facilitates the operation of the restrictions on the use and disclosure of information in Division 4. This Division ensures that information obtained under, or relating to, an account takeover warrant or emergency authorisation cannot be used or disclosed unless a relevant exception applies.

833. A relevant offence is a serious Commonwealth offence or a serious State offence that has a federal aspect. A serious Commonwealth offence and a serious State offence have the same meanings as in section 15GE of Part IAB, that is, offences against the...
A relevant offence is the kind of offence in respect of which an account takeover warrant must be sought. An account takeover warrant may be sought for the purposes of enabling evidence to be obtained of the commission of relevant offences. This definition is included to provide a simplified and consistent way to refer to the kinds of offences in respect of which an account takeover warrant may be sought.

A serious Commonwealth offence has the same meaning as in section 15GE of Part IAB. A serious Commonwealth offence is punishable on conviction by imprisonment for a period of three years or more, and involves a matter listed in this section. These matters include, but are not limited to, money laundering, threats to national security, dealings in child abuse material, importation of prohibited imports and violence.

This definition is included as serious Commonwealth offences, as well as serious State offences that have a federal aspect, are offences in relation to which an account takeover warrant may be sought. The offences in relation to which an account takeover warrant is sought are referred to as relevant offences in Part IAAC for simplicity and consistency.

A serious State offence that has a federal aspect has the same meaning as in section 15GE of Part IAB. A serious State offence that has a federal aspect is a State offence that has a federal aspect and would be a serious Commonwealth offence if it were a Commonwealth offence. A State offence may have a federal aspect where the offence affects the interests of the Commonwealth or relates to a matter outside Australia (see section 3AA).

State offences with a federal aspect may fall within Commonwealth legislative power, and the jurisdiction of the AFP or the ACIC, because of the elements of the offence, the circumstances in which it was committed, or a federal agency is investigating the offence because it is incidental to the investigation of a Commonwealth offence.

This definition is included as serious State offences that have a federal aspect, as well as serious Commonwealth offences, are offences in relation to which an account takeover warrant may be sought. The offences in relation to which an account takeover warrant is sought are referred to as relevant offences in Part IAAC for simplicity and consistency.

To take control of an online account has the meaning given by section 3ZZUL. Taking control of an online account involves a person taking one or more steps that result in that person having exclusive access to the account.

The steps that may be taken to ensure exclusive access to an account could include using existing account credentials to alter one or more account credentials (such as by changing a password to an account), removing a requirement for two-factor authentication, or altering the kinds of account credentials that are required to access or operate the account.
842. A key consideration in applying for an account takeover warrant is suspicion on reasonable grounds that taking control of an online account is necessary in the course of an investigation for the purposes of enabling evidence to be obtained of the commission of relevant offences. The meaning of when a person takes control of an online account is described in further detail at section 3ZZUL.

843. **Telecommunications facility** is defined to mean a facility within the meaning of the *Telecommunications Act 1997*. Under this Act, a facility means any part of the infrastructure of a telecommunications network. It also means any line, equipment, apparatus, tower, mast, antenna, tunnel, duct, hole, pit, pole or other structure or thing used in or in connection with a telecommunications network. This definition is inserted to facilitate provisions that allow the use of a telecommunications facility operated or provided by a carrier for the purposes of taking control of an online account under the warrant.

844. An **urgent application** means an application for an account takeover warrant made orally in person, or remotely by telephone, email, fax or any other means of communication (paragraph 3ZZUN(2)(b)). An application may only be made orally or remotely if the applicant has reason to believe that the delay caused by making a formal application, in writing, may affect the success of the investigation. Regardless of whether the application is made in writing, orally or remotely the application must provide sufficient information to enable the issuing authority to decide whether or not to issue the warrant.

**3ZZUL When a person takes control of an online account**

845. Section 3ZZUL provides for when a person takes control of an online account for the purposes of the account takeover warrant provisions in Part IAAC.

846. A person takes control of an online account if he or she takes one or more steps that result in him or her having exclusive access to the account. To take steps means to carry out a course of action with a view to achieving a certain objective. In this context, to take steps involves adopting certain measures to facilitate obtaining exclusive access to the account. This section is not intended to impose an obligation on the law enforcement officer to guarantee that he or she does or will have exclusive access. Positively confirming that no-one else has access to the account is not required, as this could be difficult or impractical to guarantee, depending on the circumstances of the case. The officer must however take steps to gain control of the account, with the intent to achieve exclusive access.

847. Having exclusive access to the account involves access to the account being restricted to the law enforcement officer so that he or she is the sole person in control of the account. Having exclusive access to the account will mean that the law enforcement officer can operate that account fully, without interaction or interference from other people who may have been given the account credentials or otherwise be accessing the account. It is important the law enforcement officers have exclusive access because of the activities
that they may seek to undertake in conjunction with an account takeover, such as activities permitted by a controlled operation.

848. Subsection 3ZZUL(2) provides some examples of steps that law enforcement may take to ensure they are able to have exclusive access to an account. This is not, however, an exhaustive list of the actions that can be undertaken to ensure exclusive access to an account. It does not preclude law enforcement from taking any other such steps that result in them having exclusive access to the account.

849. A person may use existing account credentials to alter one or more account credentials to take control of an online account. In most cases, taking control of an online account will involve law enforcement taking the steps necessary to deprive the account holder or a user of their access to the account. Officers will be able to use account credentials to change passwords, or other log-in credentials, associated with an account to lock out the account holder or user to gain exclusive access to the account.

850. Obtaining exclusive access to an account may also involve removing a requirement for two-factor authentication. Two-factor authentication is a security feature in which a user may be granted access to a website or application only after successfully presenting two pieces of evidence to an authentication mechanism. The intent of two-factor authentication is to protect the user from an unknown person trying to access the data held on their online accounts. When executing an account takeover warrant, it may be necessary to remove the requirement for two-factor authentication to remove the security features restricting access to an account. This will ensure that the account is more readily accessible when law enforcement is seeking to take control of the account.

851. Taking control of an online account may also require altering the kinds of account credentials required to access or operate the account. Law enforcement may seek to alter the kinds of account credentials associated with an account to other kinds that may be easier to overcome when seeking to take control of the account. For example, if an account required a biometric form of identification (such as facial recognition) for the user to access and operate, law enforcement may alter this requirement to a written password which is more likely to be able to be exploited in the taking over of an account. Alternatively, law enforcement may change the biometrics required from the account holder, to the law enforcement officer’s biometrics to facilitate access.

3ZZUM Appropriate authorising officer

852. Section 3ZZUM provides that an appropriate authorising officer means an officer authorised to give an emergency authorisation for taking control of one or more online accounts under section 3ZZUX.

853. An appropriate authorising officer means, in relation to the AFP, the Commissioner of the AFP, the Deputy Commissioner of the AFP or an authorised senior executive service employee of the AFP. In relation to the ACIC, an authorising officer means the Chief
Executive Officer of the ACIC or an authorised executive level member of the staff of the ACIC.

854. The Commissioner of the AFP or the Chief Executive Officer of the ACIC may authorise a person within their agency to be an appropriate authorising officer for purposes of giving emergency authorisations under section 3ZZUX. The Commissioner of the AFP may authorise a senior executive service employee, and the Chief Executive Officer of the ACIC may authorise an executive level member of staff of the ACIC, to be an appropriate authorising officer. This provision ensures that a senior executive service employee or an executive level member of the ACIC may give an emergency authorisation for taking control of one or more online accounts if they are authorised to do so by the chief officers of their respective agencies.

855. The senior level of officer that may give an emergency authorisation reflects the intrusive nature of the use of emergency authorisations for taking control of one or more online accounts.

Division 2 – Account takeover warrants

856. New Division 2 of Part IAAC establishes the framework for the AFP and the ACIC to obtain account takeover warrants. This Division provides for the application, issuance and authorisation of account takeover warrants. Account takeover warrants will enable the AFP and the ACIC to take control of an online account for the purposes of gathering evidence about serious offences. An account takeover warrant will facilitate covert and compelled (without consent of the account holder) account takeovers to add to the investigatory powers of the AFP and the ACIC. This power will support the exercise of other evidence-gathering powers, such as search warrants, computer access warrants and controlled operations being conducted online.

3ZZUN Application for account takeover warrant

857. New section 3ZZUN sets out the circumstances in which an account takeover warrant may be sought and the procedures for applying for an account takeover warrant. As account takeover warrants are a covert evidence-gathering power that may be executed remotely, the threshold tests for applying for an account takeover warrant borrow from the test for the issue of a computer access warrant under section 27A of the SD Act. Section 27A of that Act provides that a computer access warrant may be sought if there are reasonable grounds for suspecting that access to data held in the target computer will be necessary for the purposes of enabling evidence to be obtained of the commission of relevant offences and the identity and location of offenders.

858. The threshold tests in section 3ZZUN are in line with the tests for making an application for a surveillance device warrant or computer access warrant in the SD Act. It will often be necessary for an agency to obtain multiple warrants during the course of a single investigation.
For example, during the course of executing a computer access warrant, a law enforcement officer may obtain account credentials for an online account. The officer will then be able to seek an account takeover warrant to authorise the officer to take control of that online account in order to gather further evidence about a person’s online criminality and the activity of their associates. Equally, an officer may obtain an account takeover warrant to authorise the taking control of an online account and then seek a computer access warrant to enable the officer to search an associated electronic device remotely and access and modify data on those devices.

A law enforcement officer of the AFP or the ACIC may apply for the issue of an account takeover warrant to a magistrate. In the case of the AFP, this will be the Commissioner of the AFP, the Deputy Commissioner of the AFP, an AFP employee, special member or person seconded to the AFP. In the case of the ACIC, this is the Chief Executive Officer of the ACIC or a member of staff of the ACIC.

Section 3ZZUN contains a three part test that must be satisfied in order to apply for an account takeover warrant.

First, the law enforcement officer of the AFP or the ACIC must suspect on reasonable grounds that a relevant offence (or relevant offences) has been, is being, is about to be, or is likely to be committed and, secondly that an investigation into that offence (or those offences) is being, will be or is likely to be conducted.

A relevant offence is an offence against the Commonwealth or a State punishable on conviction by imprisonment of three years or more. Relevant offences include the same types of offences in respect of which a controlled operation under Part IAB may be sought. The alignment of thresholds ensures that a law enforcement officer will be able to seek an account takeover warrant and controlled operation concurrently during the course of a single investigation.

These powers are likely to be sought in conjunction as the account takeover warrant may be used to authorise taking control of an online account, and a controlled operation may be used to authorise any otherwise criminal conduct undertaken while in control of the account. This could include, for example, authorising assuming the account holder’s identity and making false representations as that person.

The third part of the test in paragraph 3ZZUN(1)(c) provides that there must be a reasonable suspicion that taking control of a one or more online accounts is necessary in the conduct of that investigation for evidence-gathering purposes in relation to the relevant offence or offences.

The words ‘one or more online accounts’ are included in recognition of the likelihood that it will often be necessary to take control of more than one online account during the course of executing an account takeover warrant. For example, where law enforcement is seeking to take control of a social media account used to procure and disseminate child
abuse material, it may also be necessary to take control of the account for the email service associated with that particular social media account. Taking control of multiple online accounts will often be required for maintaining the covert nature of the investigation and ensuring the successful execution of the warrant. A warrant authorising the taking control of multiple online accounts may only be sought where there is a reasonable suspicion that taking control of each of those accounts is necessary in the course of the same investigation into a relevant offence. In deciding whether or not to issue an account takeover warrant, the magistrate will need to consider whether the taking control of more than one online account is reasonable, necessary and proportionate in all the circumstances. Each online account sought to be taken control of must also be specified in the warrant.

867. The word ‘necessary’ is used to ensure that an account takeover warrant may only be sought where the applicant considers it essential for the investigation in all the circumstances, not just likely to substantially assist. Necessary is used as a threshold for account takeover warrants as this warrant may only be sought for targeted investigatory purposes. This reflects the threshold for similar powers such as surveillance device warrants and computer access warrants in the SD Act.

868. The evidence sought to be obtained must be of the commission of the relevant offences or offences of the kind that are reasonably suspected as having been, being or going to be committed and investigated. Evidence may also be gathered under another evidence-gathering power used in conjunction with an account takeover warrant (such as a computer access warrant or controlled operation) provided that taking control of online account is necessary in order to enable that evidence to be obtained. For example, evidence may be gathered under these subsequent powers while law enforcement is in control of the online account.

869. The phrase ‘target accounts’ is used in section 3ZZUN to refer to the online accounts in relation to which an account takeover warrant is sought. The target account is the particular online account that law enforcement may be authorised to take control of under the account takeover warrant. The target accounts must be specified in the account takeover warrant. This may be specified by identifying one or more matters sufficient to identify the account, for example, by specifying a particular username connected with an account with a particular electronic service.

870. Account takeover warrants are only available to take control of online accounts that an end-user has with an electronic service. This could include a free account, a pre-paid account, or anything that may reasonably considered an account. These warrants cannot be used to allow law enforcement to take control of an account that is not accessible via the internet. The target account may include any online account, including, an email service, Facebook account, Reddit subscription, Twitter profile, a log-in to a commentary section on a news website or a user of a messaging service such as WhatsApp, or an account on a dark web forum or marketplace.
871. Taking control of an online account under an account takeover warrant will involve law enforcement taking steps that result in them having exclusive access to the account. This is further described above at the clause relating to section 3ZZUL.

872. In most circumstances, an application for an account takeover warrant will be made in writing and signed by the applicant (subsection 3ZZUN(2)). An application for an account takeover warrant made in writing is a formal application. However, if the applicant believes that the delay caused by making an application in writing may affect the success of the investigation, the application may also be made orally or remotely. Where these circumstances apply, and an account takeover warrant may be applied for orally or remotely, this is an urgent application. Urgent applications may be made orally in person, by telephone, email, and fax or by any other means of communication.

873. As soon as practicable after an urgent application is made, the applicant must make a written record of the application and provide a copy of the record to the magistrate that the application was made to (subsection 3ZZUN(5)).

874. Applications for account takeover warrants must provide sufficient information to enable the magistrate to decide whether or not to issue the account takeover warrant (subsection 3ZZUN(3)). This requirement applies regardless of whether a formal or urgent application was made.

875. An application could include, for example, the category of offences in relation to which the warrant is sought, the reason for suspecting that taking control of an online account is necessary in the course of an investigation into those offences, the procedures the agency has in place to minimise the likelihood that the privacy of innocent third parties would be impacted, and the value of information expected to be revealed or enabled to be obtained by executing the warrant.

876. In addition, the magistrate may require the applicant to provide any additional information as he or she finds to be necessary to allow for the proper consideration of applications for account takeover warrants (subsection 3ZZUN(4)).

3ZZUP Determining the application

877. New section 3ZZUP provides for the conditions under which a magistrate may issue an account takeover warrant. These conditions are modelled on the conditions for issuing a computer access warrant in the SD Act as an account takeover warrant is also a remote and covert evidence-gathering power.

878. Before issuing an account takeover warrant, the magistrate must be satisfied that there are reasonable grounds for the suspicion founding the application for the warrant. This includes being satisfied that there are reasonable grounds for suspecting that taking control of the target account is necessary to enable evidence to be obtained in the investigation of a relevant offence. Satisfaction of the issuing criteria is reliant on the
application for the warrant providing sufficient information to enable the magistrate to make their determination.

879. Subsection 3ZZUP(2) sets out the matters to which a magistrate must have regard to in determining whether an account takeover warrant should be issued. Consideration of these matters does not preclude the consideration of other things the magistrate may wish to take into account in assessing the application for an account takeover warrant.

880. The magistrate must have regard to the nature and gravity of the alleged offence or offences which founded the application for the warrant. This may involve consideration of the seriousness of the offence and the scale at which the offence or offences has been or is likely to be committed. Consideration of this matter ensures that the issuing authority will be able to assess the reasonableness and proportionality of executing an account takeover warrant in the circumstances. If the offence in relation to which the warrant is sought is not sufficiently serious to justify the conduct of an account takeover warrant, the issuing authority may decide not to issue the warrant.

881. The existence of any alternative means of obtaining the evidence sought to be obtained must also be taken into account. This includes, for example, taking into account whether other less intrusive methods of investigation would have the same effect as taking control of an online account to facilitate evidence gathering. An account takeover warrant should only be issued if it is the most appropriate power to enable evidence to be obtained in the circumstances. If there is another less intrusive power available that is likely to be successful in enabling evidence to be obtained, this should be sought rather than the account takeover warrant.

882. The magistrate must consider the extent to which the privacy of any person is likely to be affected. A privacy consideration is appropriate for the issue of account takeover warrants as this is a targeted evidence gathering power similar to computer access warrants. In assessing the likely impact on privacy, the issuing authority may wish to consider the type of account that the agency is seeking to take control of under the warrant. For example, taking control of an online banking account may have a more significant impact on privacy than taking control of an online shopping account. In addition, taking control of an account with an electronic service with a large number of diverse end-users may impact privacy more than taking control of an account with an electronic service for a closed group with fewer end-users.

883. The likely evidentiary value of any evidence sought to be obtained must also be considered. The purpose of an account takeover warrant is to enable evidence to be obtained of the commission of relevant offences. As such, having regard to this matter ensures that the magistrate has turned their mind to the likely effectiveness of the warrant in achieving its objective. If the issuing authority were to consider that the evidence sought to be obtained would be of little evidentiary value, he or she may decide that a warrant should not be issued as the intrusive nature of the warrant would not be balanced against the benefit to the investigation.
Finally, the magistrate must also have regard to any previous account takeover warrant sought or issued in connection with the same online account and any previous account takeover warrant sought or issued in connection with the same alleged relevant offences.

**3ZZUQ What must an account takeover warrant contain?**

Section 3ZZUQ sets out the information an account takeover warrant is required to contain. An account takeover warrant must state that the issuing authority is satisfied that there are reasonable grounds for the suspicion founding the application for the warrant, and has had regard to the issuing criteria in section 3ZZUP (subsection 3ZZUQ(1)). The warrant must also be signed by the issuing authority and include their name (subsection 3ZZUQ(5)).

An account takeover warrant must specify the name of the person making the application, the name of the law enforcement officer who, unless he or she inserts the name of another officer, is to be responsible for executing the warrant, the alleged relevant offence in relation to which the warrant is sought, the date the warrant is issued and the period for which the warrant is in force. An account takeover warrant may only be issued for a period of no more than 90 days (subsection 3ZZUQ(3)). However, the note at the end of subsection 3ZZUQ(3) clarifies that the control of the target account under the warrant may be discontinued earlier if circumstances apply (see section 3ZZUU).

The target accounts must also be specified in the warrant. Subsection 3ZZUQ(2) provides that the target account may be specified by identifying one or more matters or things that are sufficient to identify the target account. This could include specifying the account by identifying a particular username connected to an account with a particular electronic service.

If the applicant knows the holder of the account, this too must be specified in the warrant. A person is taken to hold an account with the electronic service if they use, pay or manage an account, whether or not the account is in a particular name of a person or whether the person created the account. A person who inherits an account, establishes an account in a false name, shares an account, has an account established in his or her name, or attempts to anonymise an account, is still taken to hold the account. The account holder’s name does not need to be specified, but the person must be specified in some way, such as by an alias.

Similarly, if the applicant knows one or more users of the account (other than the known holder of the account), those users must be specified in the warrant. The user of an account does not need to be the holder of the account. An account that is used by a person could include an account held by a person (such as a family member, friend or business associate) but utilised by the first-mentioned person. The account user’s name does not need to be specified, but the person must be specified in some way, such as by an alias.
890. The warrant must also specify any conditions subject to which things may be done under the warrant. The magistrate may authorise things to be done under the warrant subject to any conditions or restrictions he or she so decides.

891. The warrant must also provide an outline of the investigation to which the warrant relates. An outline of the investigation in the warrant does not need give specific details of the investigation, but must set out the key features of the investigation, including whether other investigatory powers have been or are being sought. This provision has been included in recognition of the likelihood that an account takeover warrant will be used as part of a broader criminal investigation. Setting out an outline of the investigation to which he warrant relates also ensures that the issuing authority has all relevant information before them when issuing an account takeover warrant.

892. It will often be necessary for law enforcement to execute an account takeover warrant and controlled operation concurrently. An account takeover warrant will authorise the AFP and the ACIC to take control of an online account if doing so is necessary in the investigation of a relevant offence. Once the account is under the control of law enforcement, the officer may wish to seek a controlled operation authority under Part IAB to allow them to engage in otherwise criminal conduct, including by making false representations to others and assuming a person’s identity, while in control of the account.

3ZZUR What an account takeover warrant authorises

893. Subsection 3ZZUR(1) provides that an account takeover warrant must authorise the doing of specified things in relation to the relevant target account. This is subject to any restrictions or conditions specified in the warrant. This provision ensures that any things authorised under an account takeover warrant must only be done in relation to each target account, as the object of the warrant.

894. Subsection 3ZZUR(2) sets out the things that may be specified in the account takeover warrant. Not all the things listed in subsection 3ZZUR(2) will be required in every circumstance. An account takeover warrant will need to, however, specify at least one of these listed things in order to facilitate the execution of the warrant. The things that are able to be authorised by an account takeover warrant are only things that can be conducted online, as they are limited to online accounts. The actions permitted under 3ZZUR are somewhat borrowed from the actions permitted under computer access warrants in the SD Act. They do not contemplate taking control of an account by any physical means, such as use of physical force against a person. They only contemplate using access to devices and data to take control.

895. Paragraph 3ZZUR(2)(a) provides that an account takeover warrant may authorise the taking control of the target account at any time while the warrant is in force. This activity may only be authorised if it is necessary in the course of the investigation into a relevant offence in respect of which the warrant was issued.
896. This paragraph makes clear by the words ‘at any time while the warrant is in force’ that an account takeover warrant authorises law enforcement to take control of the target account, by taking steps to ensure exclusive access to that account, at any point over the life of the warrant.

897. This power only enables the action of taking control of an online account. Any other activities, such as accessing or modifying data on the account (other than that required to access the account) or performing undercover activities such as assuming a false identity, must be performed under a separate warrant or authorisation. These actions are not authorised by an account takeover warrant. This warrant is designed to support existing powers, such as computer access warrants and controlled operations, not to be used in isolation.

898. For example, a law enforcement officer may execute a section 3E search warrant on a person suspected of using a dark web forum to distribute child abuse material. During the course of executing the warrant, the law enforcement officer recovers a laptop and other devices used by the person that is the subject of the warrant. The person complies with a section 3LA assistance order, and provides the officer with the password to their forum account, but does not consent to the officer taking control their account. The law enforcement officer may then apply for an account takeover warrant to permit them to take control of the account.

899. This enables the law enforcement officer to use the password obtained using the section 3LA assistance order to take control of the person’s account which prevents the person’s continued access to the forum and the continuation of their offending. The law enforcement officer may then seek a controlled operation under Part IAB to assume the person’s identity on the forum and engage in ongoing interactions with other members to elicit information to assist in the identification of offenders and collection of evidence on other participants on the dark web forum. By enabling the taking control of the account, the account takeover warrant will facilitate evidence-gathering against other forum members, mapping of the criminal network and potential identification of victims.

900. Under paragraph 3ZZUR(2)(b), the issuing authority may specify that the warrant permits using a computer, telecommunications facility operated or provided by the Commonwealth or a carrier, any other electronic equipment or a data storage device. The only purpose for which these things can be used is to take control of the target account. This provision will allow the AFP or the ACIC to take control of an online account without having to be physically present at the computer in which the electronic service hosting the account is held. This provision is important in ensuring that an account takeover warrant can be carried out remotely and covertly.

901. In the context of account takeover warrants, taking control of an account involves taking steps that result in law enforcement obtaining exclusive access to the account. Allowing law enforcement officers the ability to use a computer, telecommunications facility or other device assists in cases where an account takeover warrant could be used without the
consent of the account holder. This may include the computer on which the account is held or used, or any other computer that enables access to the account.

902. Paragraph 3ZZUR(2)(c) permits an account takeover warrant to authorise three specific things in order to take control of the target account. These things may only be authorised if considered by the issuing authority to be necessary for the limited purpose of taking control of the target account, and for no other purposes. The following things cannot be used for the purposes of accessing data once law enforcement is in control of the account. This type of activity may only be authorised under a subsequent warrant or authorisation, such as a computer access warrant or controlled operation.

903. Firstly, an account takeover warrant may authorise accessing account-based data for the purposes of taking control of the target account. Account-based data includes data associated with an account for an electronic service with end-users that is either held by a person or is used, or likely to be used, by a person. This could be data associated with an email service, a social media account or any other type of account with an electronic service. Account-based data may be held on a particular device, or within another computer such as an external server or cloud.

904. The mobile nature of communications requires law enforcement to access data associated with the use of an account for the purposes of taking control of the account under an account takeover warrant. For example, it is feasible that a broad range of people may be using an account to conduct illegal activity, or a person of interest is using the accounts of others to conduct illegal activity. It will often be necessary to access account-based data when seeking to take control of an account to, for example, determine when an account is being used and by whom. The ability to access account-based data is important in facilitating the effective execution of an account takeover warrant.

905. Secondly, adding, copying, deleting or altering of account credentials may be authorised for the purposes of taking control of the target account. Account credentials, such as usernames and passwords, will often need to be modified to enable law enforcement to take control of an online account. Passwords associated with an account will often need to be altered in order to prevent the account holder or user from being able to access and operate the account and ensure that law enforcement have exclusive access to the account.

906. Thirdly, the issuing authority may authorise the adding, copying, deleting or altering data in a computer for the purposes of taking control of the target account. The ability to modify any data to take control of an account may be used to alter or delete data or methods of authentication that are used to provide others with access to the account. For example, law enforcement may add, copy, delete or alter data to degrade the service providing access to the account or temporarily disable a person’s access to an account to allow law enforcement to access it exclusively. This power may also be used to remove a requirement for two-factor authentication to degrade the security features restricting access to an account.
907. Subparagraph 3ZZUR(2)(d)(i) allows using a communication in transit to take control of the target account if it is reasonable in all the circumstances, having regard to any other methods of taking control of the target account. Consideration of other available methods before authorising the use of a communication in transit does not require all other methods to be exhausted, but rather allows the issuing authority to take into account the circumstances before him or her and balance the impact on privacy with the risk of detection. This ensures that this type of communication will only be used where it is the most reasonable and appropriate method of taking control of the target account in the circumstances.

908. Using a communication in transit involves accessing a communication passing over a telecommunications network, as long as this use does not amount to interception. An account takeover warrant also does not authorise the material interference, interruption or obstruction of a communication in transit unless necessary to successfully execute the warrant (subsection 3ZZUR(5)).

909. During the course of executing an account takeover warrant, it may be necessary to use a communication in transit to determine whether an account or electronic service is being used or accessed by a person at a particular time, or a person is attempting to access the account or electronic service while the account is under the control of law enforcement. Where necessary for the purpose of using a communication in transit to take control of the target account, the warrant may also authorise the adding, copying, deleting or altering of data in a communication in transit (subparagraph 3ZZUR(2)(d)(ii)).

910. Paragraph 3ZZUR(2)(e) allows a warrant to authorise the copying of any account-based data which has been accessed under the warrant if it either appears relevant for the purposes of determining whether the data is covered by the warrant, or is covered by the warrant. Data that is subject to some form of electronic protection is taken to be relevant for the purposes of determining whether it is relevant data covered by the warrant (subsection 3ZZZO(3)). This provision ensures that account-based data accessed for the purposes of taking control of the target account can be copied onto a computer. This will be necessary in order for data to be analysed or for evidence to be collected.

911. While the purpose of the account takeover warrant is to facilitate access to data and evidence-gathering under a subsequent investigatory power, it is important to ensure that any data accessed under the account takeover warrant can also be copied and used in evidence for investigations into serious offences.

912. The information obtained through access to account-based data under an account takeover warrant is likely to pertain to an individual’s identity and their use of a particular account. Such information may make valuable evidence for investigations into serious offences, particularly those in relation to crimes perpetrated on the dark web. Evidence relating to the commission of a specific offence is more likely to be obtained under the subsequent investigatory power, such as a computer access warrant or controlled operation.
Paragraph 3ZZUR(2)(f) allows copying any account credentials to which the target account relates. As with account-based data, account credentials used or obtained under an account takeover warrant may need to be copied to enable its use in evidence.

An account takeover warrant may also authorise any other thing reasonably incidental to any of the other activities listed in subsection 3ZZUR(2).

When account-based data is covered by a warrant

Subsection 3ZZUR(4) is a clarifying provision to explain that account-based data is taken to be covered by the warrant if access to the data is necessary for enabling evidence to be obtained of the commission of the relevant offences in respect of which the warrant was issued. This provision reiterates the thresholds in paragraph 3ZZUN(1)(c) which must be met before a law enforcement officer of the AFP or the ACIC may apply for an account takeover warrant.

Certain acts not authorised

Subsection 3ZZUR(5) provides that an account takeover warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to this limitation has been included so that the AFP or the ACIC may undertake such actions but only where necessary to carry out the activities authorised by the warrant. An account takeover warrant also does not authorise causing material loss or damage to persons lawfully using a computer. This provision has the same effect as subsection 27E(5) in the Sd Act in relation to computer access warrants.

The inclusion of this provision recognises that, in some circumstances, it may be necessary for law enforcement to take control of the account used by a third party not suspected of committing an offence (such as a family member) in order to enable evidence to be obtained of the commission of serious offence by their associates. This provision ensures that law enforcement will be able to do so but only if it is necessary for the successful execution of the warrant. Prior to authorising the taking control of the account used by a third party, the issuing authority will have regard to all the relevant matters before them and determine that this type of activity would be reasonable and proportionate in the circumstances.

Concealment of access etc.

Subsection 3ZZUR(6) provides that an account takeover warrant will also authorise the doing of anything reasonably necessary to conceal the fact that anything has been done under the warrant. Concealment of access is important for maintaining the effectiveness of covert warrants. Similar provisions exist in relation to other covert powers, such as computer access warrants in subsection 27E(7) of the SD Act.
919. Paragraph 3ZZUR(6)(d) authorises the use of a computer or communication in transit to conceal access under an account takeover warrant, including, if necessary, adding, copying, deleting or altering data in the computer or communication in transit. This is important in maintaining the covert nature of an account takeover warrant as indications that access to an account by law enforcement has been enabled may need to be deleted or disguised by further data modification.

920. Paragraph 3ZZUR(6)(e) allows an account takeover warrant to authorise any other things reasonably incidental to do any of the things authorised by subsection 3ZZUR(6).

921. Concealment activities must be performed at any time while the warrant is in force, or within 28 days after it ceases to be in force, or at the earliest time after this period at which it is reasonably practicable to do so (paragraphs 3ZZUR(6)(f) and (g)).

922. Paragraph 3ZZUR(6)(g) recognises that it may not be possible to conceal access under an account takeover warrant within 28 days of the warrant expiring. If such circumstances exist, concealment activities must be performed ‘at the earliest time after the 28-day period at which it is reasonably practicable to do so.’ This acknowledges that the authority to conceal access under an account takeover warrant should not extend indefinitely, but only until when it is practical operationally.

923. Subsection 3ZZUR(7) clarifies that the concealment of access provisions in subsection 3ZZUR(6) do not authorise the same activities that are not authorised under an account takeover warrant as set out in subsection 3ZZUR(5).

Statutory conditions

924. Subsection 3ZZUR(8) sets out the statutory conditions to which an account takeover warrant is subject. These conditions are distinct from the certain acts that are not authorised by the warrant in subsection 3ZZUR(5). Failure to comply with the statutory conditions will impact the validity of an account takeover warrant. These conditions must be specified in the account takeover warrant (subsection 3ZZUR(10)).

925. Paragraph 3ZZUR(8)(a) provides that if damage to data occurs during an account takeover warrant, the damage must be justified and proportionate to the serious offence being targeted by the warrant. Whether damage is justified and proportionate will need to be a matter considered by the issuing authority on a case-by-case basis.

926. Paragraph 3ZZUR(8)(b) provides that a warrant must not be executed in a manner that causes a person to suffer a permanent loss of money, digital currency or property (other than data). This provision is intended to provide an abundance of clarity about the scope of an account takeover warrant. The account takeover warrant is for the purposes of taking control of an account, meaning to gain exclusive access and lock a person out of his or her account. Interference with account data beyond what is required to take control of the account is not permitted by this warrant.
However, subsection 3ZZUR(8)(b) acknowledges that there may be some circumstances in which gaining exclusive access to an account (such as a bank account) may result in some interference with a person’s finances. For example, if a PIN is changed, the person will not be able to withdraw cash from the account.

This alteration to a person’s finances cannot result in a permanent loss. The account takeover warrant is not a power to seize property or finances. Seizure of money and property by law enforcement is provided for in the *Proceeds of Crimes Act 2002*.

Subsection 3ZZUR(9) clarifies that subsection 3ZZUR(8) does not limit the conditions to which an account takeover warrant may be subject. Under subsection 3ZZUR(1), an account takeover warrant must authorise the doing of specified things subject to any restrictions or conditions the issuing authority so decides.

### 3ZZUS Variation of account takeover warrant

Section 3ZZUS allows a law enforcement officer to apply at any time while the warrant is in force for an extension of the warrant or a variation of its terms. The warrant can only be extended for a period not exceeding 90 days after the day the warrant would otherwise expire but for the extension. This section builds flexibility into the warrant process by accounting for extended investigations and unexpected circumstances.

An application for an extension or variation must be made to a magistrate and be accompanied by the original warrant (subsection 3ZZUS(2)). Subsection 3ZZUS(3) provides that the magistrate must be satisfied that the grounds on which the application for the warrant was made still exist (see subsection 3ZZUP(1)), and be satisfied of the same matters required to issue the warrant in the first instance (see subsection 3ZZUP(2)). This ensures that any varied specifications of the warrant are within the bounds of what might have been authorised in an account takeover warrant in the first instance.

If an application of variation is granted, the magistrate must endorse the new expiry data or other varied term on the original warrant (subsection 3ZZUS(4)).

This new section does not prevent the issue of further applications for extensions or variations (subsection 3ZZUS(5)).

### 3ZZUT Revocation of account takeover warrant

Section 3ZZUT sets out the provisions for revoking an account takeover warrant. This provision ensures that if it becomes apparent that an account takeover warrant is no longer necessary for the purpose in which it was sought, it must cease to be in force.

An account takeover warrant may be revoked by a magistrate if he or she is satisfied that taking control of the target account is no longer necessary in order to enable evidence to be obtained of the commission of a relevant offence.
936. The chief officer of the agency to which an account takeover warrant was issued must revoke the warrant if satisfied that the warrant is no longer required for the purpose for which it was sought (subsections 3ZZUT(2) and 3ZZUU(2)).

937. Revocations for account takeover warrants must be made by instrument in writing (subsection 3ZZUT(1)). If a warrant is revoked, the magistrate must give a copy of the instrument of revocation to the chief officer of the agency to which the warrant was issued (subsection 3ZZUT(4)).

938. If the warrant is revoked and the officer executing the warrant is already in the process of executing the warrant, the officer does not have any civil or criminal liability for actions done before he or she is made aware of the revocation (subsection 3ZZUT(5)).

3ZZUU Discontinuance of execution of account takeover warrant

939. Section 3ZZUU provides for the circumstances in which the taking control of the account under an account takeover warrant, must be discontinued.

Scope

940. Subsection 3ZZUU(1) clarifies that the provisions relating to discontinuance of operation under a warrant only apply if an account takeover warrant is issued.

Discontinuance of execution of account takeover warrant

941. Subsection 3ZZUU(2) places an obligation on the chief officer of the AFP or the ACIC to take steps to discontinue execution of an account takeover warrant where he or she is satisfied that the grounds on which the warrant was sought cease to exist. Control of the target account must be discontinued if the chief officer is satisfied that taking control of the account is no longer required for the purpose of enabling evidence to be obtained of the commission of one or more relevant offences.

942. Subsection 3ZZUU(3) complements section 3ZZUT providing that the chief officer of the agency must take steps to ensure the discontinuance of the execution of an account takeover warrant as soon as practicable after being made aware that a magistrate has revoked the warrant.

943. Subsection 3ZZUU(4) places an obligation on the executing officer to immediately inform the chief officer if there is a change in circumstances affecting the warrant. Upon being informed of the change in circumstances by the executing officer, the chief officer of the agency may have obligations to discontinue the operation of the account under subsection 3ZZUU(2)).

3ZZUV Restoration of online account

944. Section 3ZZUV provides for the circumstances in which the access to the target account must be restored to the account holder.
945. If an account takeover warrant ceases to be in force (either by expiry or revocation), it is lawful for the account holder to operate the account, and as a result of the warrant, the account holder is not able to operate the account, the executing officer must take all reasonable steps to ensure that the account holder is able to operate the account. For example, restoration of an account may be effected by changing the account credentials back to what they originally were before the account was taken over.

3ZZUW Relationship of this Division to parliamentary privileges and immunities

946. New section 3ZZUW provides that, to avoid doubt, Division 2 does not affect the law relating to the powers, privileges and immunities of each House of the Parliament, their members, committees of each House of the Parliament and joint committees of both Houses of the Parliament.

947. The purpose of this provision is to clarify that the provisions relating to account takeover warrants in Division 2 of Part IAAC are not intended to intrude on the powers, privileges and immunities of Parliament.

Division 3 – Emergency authorisations

948. Division 3 provides for the taking control of one or more online accounts without a warrant in emergency situations where it is not practicable to obtain an account takeover warrant from a magistrate. This Division sets out the procedures for the giving of emergency authorisations where there is a serious immediate risk to person or property which justifies the taking control of an online account without prior magistrate authorisation.

3ZZUX Emergency authorisation – serious risks to person or property

949. Section 3ZZUX provides that a law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for taking control of one or more online accounts if he or she has a reasonable suspicion that four circumstances exist. Firstly, that there is an imminent risk of serious violence to a person or substantial damage to property, and secondly, that taking control of one or more online accounts is immediately necessary for dealing with that risk. Thirdly, the circumstances must be so serious and the matter must be of such urgency that taking control of one or more online accounts is warranted. Finally, it must not be practicable to apply for an account takeover warrant in the circumstances.

950. This provision establishes a high threshold, characterised by urgency, immediacy and seriousness, for an emergency authorisation to be issued. However, in the emergency situations in which these circumstances exist, emergency authorisations will allow law enforcement officer to respond quickly and effectively to criminal activity.

951. An application for an emergency authorisation may be made orally, in writing, by telephone, email or fax or any other means of communication.
952. An appropriate authorising officer may give an emergency authorisation if he or she is satisfied that there are reasonable grounds for the law enforcement officer’s suspicion of the matters which founded the application.

Statutory conditions

953. Subsection 3ZZUX(4) provides that an emergency authorisation for taking control of an online account is subject to the same statutory conditions as an account takeover warrant.

954. Paragraph 3ZZUX(4)(a) provides that if damage to data occurs during an account takeover warrant, the damage must be justified and proportionate to the serious offence being targeted by the warrant. Whether damage is justified and proportionate will need to considered on a case-by-case basis.

955. Paragraph 3ZZUX(4)(b) provides that an emergency authorisation must not be executed in a manner that causes a person to suffer a permanent loss of money, digital currency or property (other than data).

3ZZUY Record of emergency authorisation to be made

956. Section 3ZZUY requires the appropriate authorising officer, as soon as practicable after having issued the emergency authorisation, to make a written record of the giving of that emergency authorisation. The record is to name the applicant, the date and time the authorisation was given and the nature of the authorisation. This record is later to accompany the application for approval of the emergency authorisation by a magistrate.

3ZZUZ Attributes of emergency authorisations

957. Section 3ZZUZ provides that emergency authorisations may permit the law enforcement officer to whom it was issued to do anything that an account takeover warrant may authorise a law enforcement officer to do. A law enforcement officer may only take control of one or more accounts under an emergency authorisation if he or she is acting in the performance of his or her duty.

3ZZVA Application for approval of emergency authorisation

958. Section 3ZZVA provides that where an emergency authorisation for taking control of one or more online accounts has been given by an appropriate authorising officer, approval of the emergency authorisation must then be sought from a magistrate within 48 hours from when the authorisation was given.

959. The appropriate authorising officer must apply for approval of the giving of an emergency authorisation to a magistrate. This application must provide sufficient information to enable the magistrate to decide whether or not to approve the giving of the emergency authorisation. The application must also be accompanied by a copy of the
written record made by the appropriate authorising officer in relation to the emergency authorisation under 3ZZUY.

3ZZVB Consideration of application

960. Section 3ZZVB provides that when deciding whether to approve an emergency authorisation given by an appropriate authorising officer, the magistrate must take into account a number of considerations.

961. The magistrate must consider the nature of the risk of serious violence to a person or substantial damage to property which the law enforcement officer suspected at the time of applying for the authorisation. The magistrate must also consider the extent to which issuing an account takeover warrant would have helped reduce or avoid that risk.

962. The extent to which law enforcement officers could have used alternative methods to help reduce or avoid the risk to a person or property must also be considered, balance with how much the use of alternative methods of investigation could have helped reduce or avoid the risk. The magistrate must also consider how much the use of alternative methods of investigation would have prejudiced the safety of the person or property because of delay or for another reason.

963. An important consideration for the magistrate in deciding whether to approve an emergency authorisation is whether, in the circumstances, it was indeed impracticable for the law enforcement officer to apply for an account takeover warrant in the normal manner. This will involve having regard to whether the urgency and seriousness of the risk justified the use of an emergency authorisation.

3ZZVC Magistrate may approve giving of an emergency authorisation for the taking control of an online account

964. Section 3ZZVC sets out what a magistrate must be satisfied of in order to approve an emergency authorisation. A magistrate may approve the taking control of an online account under an emergency authorisation if he or she is satisfied of three matters.

965. Firstly, that there are reasonable grounds to suspect that a risk of serious violence to a person or substantial damage to property did exist, and secondly, that taking control of the account may have helped reduce that risk. Finally, that it was not practicable in the circumstances for an application to be made for an account takeover warrant.

966. There are two options available to the magistrate when they have approved the giving of an emergency authorisation. The first option is that the a magistrate may issue an account takeover warrant for the continued taking control of the online account as if the application for the approval of the emergency authorisation were in fact an application for an account takeover warrant under section 3ZZUN. This option is available provided that the activity required the account takeover continues to exist. This will ensure that the
duration of the account takeover is then subject to the 90 day period of effect and the magistrate may impose conditions or restrictions on the warrant.

967. The second option available to the magistrate is to be used in circumstances where the magistrate is satisfied that since the application for the emergency authorisation was made, the activity which required the account takeover has ceased. In such circumstances, the magistrate may order that the exercise of powers under the emergency authorisation cease.

968. Similarly, there are a couple of options available where the magistrate chooses not to approve the giving of an emergency authorisation for taking control of an online account. In these circumstances, the magistrate may order that the exercise of powers under the emergency authorisation cease altogether.

969. However, where the magistrate believes that the situation did not warrant an emergency authorisation at the time it was given but that the taking control of one or more online accounts has now become necessary, he or she may issue an account takeover warrant for the future taking control of online accounts. In this case, the application for the approval of the giving of an emergency authorisation shall be treated as if it was an application for an account takeover warrant in section 3ZZUN.

970. Whether or not the magistrate approves the giving of an emergency authorisation, he or she may order that any information obtained from or relating to the exercise of powers under the emergency authorisation, or any record of that information, be dealt with in a manner specified in the order. The magistrate may not order that such information be destroyed because such information, while improperly obtained, may still be required for a permitted purpose in section 3ZZVH.

**3ZZVD Admissibility of evidence**

971. Section 3ZZVD provides that evidence obtained under an emergency authorisation which has been subsequently approved by a magistrate will be admissible in any proceedings. The fact that the evidence was obtained under the authorisation prior to receiving approval does not render such evidence inadmissible.

**3ZZVE Restoration of online account**

972. Section 3ZZVE provides for the circumstances in which the access to the target account must be restored to the account holder. This provision reflects section 3ZZUV in relation to account takeover warrants.

973. If a magistrate orders the cessation of taking control of an online account under emergency authorisation, and it is lawful for the account holder to operate the account, and as a result of the authorisation, the account holder is not able to operate the account, the executing officer must take all reasonable steps to ensure that that the account holder is able to operate the account. For example, restoration of an account may be effected by
changing the account credentials back to what they originally were before the account was taken over.

3ZZVF Relationship of this Division to parliamentary privileges and immunities

974. Section 3ZZVF provides that, to avoid doubt, Division 3 does not affect the law relating to the powers, privileges and immunities of:

a. each House of Parliament

b. the members of each House of the Parliament

c. the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

975. The purpose of this section is to clarify that the provisions relating to emergency authorisations in Division 3 are not intended to intrude on the powers, privileges and immunities of the Parliament.

Division 4 – Assistance orders

3ZZVG Person with knowledge of an online account to provide assistance

976. New section 3ZZVG will allow a law enforcement officer to apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to take control of the target account. For example, an assistance order may be used to enable the taking control of an online account because a person may have knowledge of a password.

977. New section 3ZZVG ensures that when an account takeover warrant or emergency authorisation is in place, a law enforcement officer will be able to compel assistance to take control of the online account that is the subject of the warrant or authorisation. The intent of this provision is not to allow law enforcement to compel assistance from industry, but rather from a person with knowledge of an online account, such as a person holds or uses the account. Assistance provided by industry is governed by the Telecommunications Act 1997.

978. Although the account takeover warrant permits covert activity, there may be circumstances in the course of an investigation where a person who is not the suspect or target will have knowledge of a computer system and be able to assist law enforcement in taking control of the account, without compromising the covert nature of the investigation. Alternatively, there may be a point in the investigation where the benefits of compelling information from a person in order to assist in the taking control of an account may outweigh the disadvantages of maintaining the secrecy of the investigation. For example, where the person who holds the account has been detained and law
enforcement is now seeking to gather evidence on the person’s criminal associates by taking control of their account.

Grant of an assistance order

979. In order to grant an assistance order, the magistrate must be satisfied of three things.

980. Firstly, the magistrate must be satisfied that there are reasonable grounds for suspecting that taking control of the target account is necessary for enabling evidence to be obtained of the commission of an alleged relevant offence. This must be the offence in respect of which the warrant is issued. The assistance must be in the course of the investigation to which the warrant relates. Assistance orders cannot be requested or granted without being in support of the account takeover warrant or emergency authorisation. They are not stand-alone orders.

981. Secondly, the magistrate must be satisfied that the person from whom assistance is sought is either the person suspected of having committed the relevant offence, or is a holder of the target account, an employee of the holder, a person engaged in a contract for services by the holder, a person who uses or has used the account, or a person who is or was a system administrator for the service to which the account relates.

982. Finally, a magistrate may only grant the assistance order if he or she is satisfied that the specified person from whom assistance is requested is a person who has relevant knowledge of either the target account, the electronic service to which the target account relates, or of measures applied to protect account-based data to which the target account relates.

Offence

983. Subsection 3ZZVG(3) provides that a person commits an offence if that person is subject to an assistance order and is capable of complying with the requirements set out in the order, but omits to do an act and the omission does not comply with the requirement of the order.

984. The penalty for not complying with a request compelling assistance under section 3ZZVG is a maximum of imprisonment for 10 years. This reflects the penalty for not complying with an assistance order under section 64 or 64A in relation to surveillance devices or computer access.

985. The offence of failure to comply with an assistance order does not currently, and will not under the proposed legislation, abrogate the common law right to freedom from self-incrimination. Assistance orders do not engage the right because they do not compel individuals to provide evidence against their legal interest. Assistance orders only compel individuals to provide access to computers or devices to assist in disruption, in the same manner as a search warrant compels individuals to provide access to a premises to assist in a search.
Additional use of information etc.

986. Subsection 3ZZVG(4) provides for the additional use of information or assistance provided as a result of an order made under this section. Information or assistance provided under section 3ZZVG for an investigation into an alleged offence under an account takeover warrant may be used in the execution of a search warrant but only where the matter relates to the same investigation into the same alleged offences. This provision reflects the amendment made to section 3LA at item 3 of this Schedule to promote interoperability between the search warrant and account takeover warrant frameworks.

987. The intent of this provision is to ensure that information obtained under a section 3ZZVG assistance order can be used in the execution of a search warrant. Account takeover warrants are designed to complement the use of other investigatory powers, including search warrants, by authorising the taking control of a person’s online account in the investigation of serious offences. This investigation will be furthered by a subsequent investigatory power, such as a search warrant, to enable access to data and collection of evidence.

Division 5 – Restrictions on use and disclosure of information

988. Division 4 sets out the restrictions on the use and disclosure of information associated with account takeover warrants and emergency authorisations. Information obtained pursuant to an account takeover warrant or emergency authorisation is protected by restrictions on use and disclosure. These provisions operate by setting out what information is ‘protected information’, prohibiting the use and disclosure of that information, and providing several exceptions to that prohibition.

3ZZVH Unauthorised use or disclosure of protected information

989. Under subsection 3ZZVH(1) it is an offence to use or disclose protected information. For the purposes of new Part IAAC, protected information means any information obtained under an account takeover warrant or emergency authorisation, or any information relating to an application for, the issue of, the existence of, or the expiration of an account takeover warrant or emergency authorisation, or an application for the approval of the giving of an emergency authorisation.

990. The penalty for disclosing protected information is two years’ imprisonment. This offence is in line with the offence for the unlawful use, recording, communication or publication of protected information under the SD Act.

991. Subsection 3ZZVH(2) provides an aggravated offence for disclosing protected information. If a person discloses protected information and the use or disclosure of the information endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence, the penalty for disclosing that information is imprisonment for 10 years.
Exceptions

992. Under subsection 3ZZVH(3), there are several exceptions to the general prohibition on disclosing protected information relating to account takeovers.

993. Protected information can be used or disclosed in connection with the administration or execution of Part IAAC of the Crimes Act. This allows for the effective administration and execution of the account takeover warrant provisions.

994. Under paragraph 3ZZVH(3)(b) protected information can be used and disclosed in connection with the functions of the AFP under section 8 of the *Australian Federal Police Act 1979*. The AFP’s functions include providing police services to assist or cooperate with a foreign law enforcement or intelligence agency (paragraph 8(1)(bf) of the AFP Act). This provision will allow protected information to be used or disclosed if necessary for this purpose.

995. Similarly, under paragraph 3ZZVH(3)(c) protected information can be used and disclosed in connection with the functions of the ACIC under section 7A of the *Australian Crime Commission Act 2002*. The ACIC’s functions under that section include to collect, correlate, analyse and disseminate criminal information and intelligence and to undertake special ACC operations and investigations. Protected information can be used or disclosed in connection with this purpose.

996. Protected information may be used or disclosed under paragraph 3ZZVH(3)(d) in connection with preventing, investigation or prosecuting an offence. This is the central purpose for which information obtained under, or relating to, an account takeover warrant is intended to be used.

997. The use or disclosure of protected information by a person who believes on reasonable grounds that the use or disclosure is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property is permitted under paragraph 3ZZVH(3)(e). Such a person need not necessarily be a law enforcement officer of the AFP or the ACIC but may be a person to whom protected information was disclosed originally.

998. Under paragraph 3ZZVH(3)(f), protected information may be used or disclosed for the purposes of any legal proceedings arising out of or otherwise related to Part IAAC or of any report of any such proceedings. This provision will allow protected information to be used as evidence in court.

999. Paragraph 3ZZVH(3)(g) allows protected information to be used and disclosed for the purposes of obtaining legal advice in relation to Part IAAC. Legal advice may need to be sought on the interpretation of the account takeover warrant provisions to ensure that the AFP and the ACIC are acting in accordance with the law when exercising this power.
1000. Protected information can be used and disclosed in accordance with any requirement imposed by law under paragraph 3ZZVH(3)(h). For example, where a court has ordered certain documents containing protected information to be produced.

1001. The use and disclosure of protected information is permitted in connection with the performance of functions or duties, or the exercise of powers, under Part IAAC (paragraph 3ZZVH(3)(i)).

1002. Under paragraph 3ZZVH(3)(j), protected information may be used or disclosed in connection with the performance of functions or duties, or the exercise of powers by a law enforcement officer. Under this subsection, the use and disclosure of protected information in connection with the performance of functions or duties or the exercise of powers by the Director-General (within the meaning of the Australian Security Intelligence Organisation Act 1979), an ASIO employee (within the meaning of that Act) or an ASIO affiliate (within the meaning of that Act) will not constitute an offence. Similarly, protected information in connection with the performance of functions or duties, or the exercise of powers, by the agency head or a staff member of an agency empowered under the Intelligence Services Act 2001 can be used and disclosed without constituting an offence.

1003. Paragraph 3ZZVH(3)(k) permits the use and disclosure of protected information for the purposes of admission of evidence in a proceeding that is not a criminal proceeding. This provision allows the use and disclosure of protected information as evidence in judicial review proceedings.

1004. Subsection 3ZZVH(4) provides that the prohibition on using and disclosing protected information does not apply if the disclosure was made by a person to an Ombudsman official (whether in connection with a complaint made to the Ombudsman or in any other circumstances). This is to facilitate oversight of account takeover warrants by the Commonwealth Ombudsman.

1005. Similarly, subsection 3ZZVH(5) provides that the prohibition on using and disclosing protected information does not apply if the disclosure was made by a person to an IGIS official for the purposes of that official exercising their powers, or performing their functions or duties.

1006. The notes after subsections 3ZZVH(3), (4) and (5) clarify that a defendant bears an evidential burden in relation to the matters in these subsections. This refers to the operation of subsection 13.3(3) of the Criminal Code Act 1995.

**3ZZVJ Dealing with records obtained under, or relating to, account takeover warrants etc.**

1007. The Bill inserts section 3ZZVJ in order to provide for the record keeping obligations that are associated with records obtained under, or relating to, account takeover warrants or emergency authorisations.
1008. The chief officer of the AFP or the ACIC must ensure that every record or report comprising protected information is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. This is an important security mechanism that ensures that the information obtained by virtue of conducting an account take over will be adequately protected.

1009. The chief officer of the AFP or the ACIC must also cause records or reports comprising protected information to be destroyed either as soon as practicable or within a period of 5 years. The chief officer must cause the record to be destroyed as soon as practicable if he or she is satisfied that no civil or criminal proceeding to which the material contained in the record or report relates has been, or is likely to be, commenced and that the material is not likely to be required for the purposes for which protected information can be disclosed, that is, the exceptions to the prohibition in subsections 3ZZVH(2) and (3).

1010. Under subparagraph 3ZZVJ(b)(ii) records and reports must be destroyed within 5 years, unless the chief officer certifies that the records are still necessary for the purposes of subparagraph 3ZZVJ(b)(i).

3ZZVK Protection of account takeover technologies and methods

1011. This provision is based on section 47A of the Surveillance Devices Act, and applies the same protections for computer access technologies and methods to technologies and methods that may be used by agencies to conduct account takeovers under an account takeover warrant or emergency authorisation in court proceedings.

1012. Section 3ZZVK gives protection to sensitive information relating to account takeover technologies and methods by preventing its release into the public domain. This recognises that the release of such information in the public domain could harm future capabilities and investigations. This section is intended to protect technologies as they develop over time and not to limit law enforcement agencies with an exhaustive list.

1013. Subsection 3ZZVK(1) provides that, in a proceeding, a person may object to the disclosure of information on the ground that the information could reasonably be expected to reveal details of account takeover technologies or methods if it were disclosed. It is not intended that section 3ZZVK would give protection to simple aspects of account takeovers, such as the knowledge that an account was accessed. The section is designed to protect sensitive technologies and methods that need to be closely held. However, less sensitive technologies and methods are not excluded explicitly from section 3ZZVK because it is within the discretion of the person conducting or presiding over the proceeding whether information is of sufficient sensitivity (subsection 3ZZVK(2)).

1014. Subsection 3ZZVK(3) requires that the person deciding whether or not to order information not to be disclosed must take into account whether disclosure of the information is necessary for the fair trial of the defendant and whether it is in the public
interest. This ensures that the availability of capability protection for law enforcement is not absolute. The public interest in protecting sensitive operational and capability information must be weighed against the defendant’s right to a fair trial and other public interests.

1015. Subsection 3ZZVK(4) is a saving provision which provides that this section does not affect any other law under which a law enforcement officer cannot be compelled to disclose information or make statements in relation to the information.

1016. Subsection 3ZZVK(5) requires the person conducting or presiding over the proceeding to make any order they consider necessary to protect account takeover technologies or methods that have been disclosed from being published. In order to do so, the person must be satisfied that the publication of information could reasonably be expected to reveal details of account takeover technologies and methods. However, this does not apply if doing so would conflict with the interests of justice (subsection 3ZZVK(6)).

1017. It is appropriate to protect this information without a requirement to consider the harms or that the disclosure of the information would be contrary to the public interest as the disclosure of such sensitive information would be inherently harmful. Law enforcement capabilities are fundamental to ongoing investigations and their ability, including over the long-term, to protect essential public interests, including national security and public safety.

1018. Subsection 3ZZVK(7) provides the definition of account takeover technologies or methods. Account takeover technologies or methods means one of three things where those technologies or methods have been, or are being, deployed in giving effect to an account takeover warrant or emergency authorisation. Firstly, these are technologies or methods relating to using a computer, a telecommunications facility, any other electronic equipment, or a data storage device, for the purposes of taking control of an online account. Secondly, account takeover technologies and methods are technologies and methods relating to adding, copying, deleting or altering account-based data, if doing so is necessary to take control of an online account. Finally, they can be technologies or methods relating to adding, copying, deleting or altering account credentials to which an online account relates, if doing so is necessary to take control of the online account.

1019. In this section, a proceeding includes a proceeding before a court, tribunal or Royal Commission.

Division 6—Reporting and record keeping

1020. Division 6 contains the reporting and record keeping obligations relating to account takeover warrants. These are important safeguards in ensuring accountability and compliance with the account takeover warrant provisions.
3ZZVL Chief officers’ 6 monthly reports to the Minister and the Ombudsman

1021. Section 3ZZVL sets out the reporting requirements that the chief officers of the AFP and the ACIC must comply with in relation to their agencies’ use of account takeover warrants over a six month period. Subsection 3ZZVL(1) provides that the chief officer must submit a report to the Minister for Home Affairs and the Ombudsman as soon as practicable after 30 June and 31 December each year. The report must include certain information in relation to the previous six month period from the last report made.

1022. A six monthly report on the use of account takeover warrants is more appropriate than a report on each warrant, as the Ombudsman is empowered to inspect the records of the AFP and the ACIC to assess their compliance with the account takeover warrant provisions on a six monthly basis. The requirement to report to both the Minister for Home Affairs and the Ombudsman every six months supports Ministerial and independent oversight of the use of account takeover warrants.

1023. The six monthly report to the Minister and Ombudsman must include the number of applications for account takeover warrants made, and the dates on which those applications were made and the number of account takeover warrants issued, and the dates on which those warrants were issued. If any applications for account takeover warrants were refused, the report must specify the number of applications that were refused, and the date on which those applications were refused.

1024. If any applications for variations were made, the report must include the number of applications for variations made, the number of variations made, the number of applications for variations refused, and the dates on which each variation was applied for, granted or refused.

1025. The report must also specify the number of revocations made, if any account takeover warrants were revoked at all, and the date on which those warrants were revoked.

1026. In relation to each account takeover warrant issued to the AFP or the ACIC that ceased to be in force during the previous six months, the report must also specify the date the warrant ceased to be in force, whether the warrant expired or was revoked and whether the warrant was executed. If the warrant was not executed, the report must also explain the reason why the warrant was not executed.

1027. The report must also include the number of applications for emergency authorisations made, and the dates on which those applications were made, and the number of emergency authorisations given, and the dates on which those authorisations were given. If any applications were refused, the report must specify the number of applications that were refused, and the date on which those applications were refused.

1028. If the giving of any emergency authorisations were approved, the report must include the number of those approvals, and the date on which those approvals were given. If any applications for the approval of the giving of an emergency authorisation were refused,
the report also include the number of those refusals, and the date on which those applications were refused.

1029. If the warrant was executed, the report must also include the following additional information: the name of the executing officer; the names of any law enforcement officers involved in executing the warrant; the period during which the warrant was executed; the target account to which the warrant relates and the account holder or user of the account if this person is known to the officer responsible for executing the warrant.

1030. The report must also give details of the benefit of the execution of the warrant to the investigation of a relevant offence, how information obtained under the warrant was used, details of the communication of information under the warrant to persons outside the agency to which the warrant was issued and details of the compliance with any conditions to which the warrant was subject.

1031. In the report, the target account may be specified by identifying one or more matters and things that are sufficient to identify the account. For example, an account may be specified by identifying a particular username associated with an account for a particular electronic service.

3ZZVM Chief officers’ annual reports to the Minister

1032. Section 3ZZVM provides that, within three months after the end of each financial year, the chief officer of the AFP and the ACIC must submit a report to the Minister for Home Affairs setting out relevant statistical information in relation their use of account takeover warrants over the previous financial year.

1033. The annual report to the Minister must include the number of account takeover warrants applied for, issued and refused. This includes the number of urgent applications made, the number of warrants issued in response to an urgent application and the number of urgent applications refused.

1034. If any account takeover warrants were varied, the report must include the number of variations made. If any variations of account takeover warrants were refused, the report must also include the number of those refusals.

1035. The report must also include the number of emergency authorisations applied for, given and refused, as well as the number of approvals for the giving of emergency authorisations applied for, given, and refused.

1036. The report must specify the types of offences in respect of which account takeover warrants and emergency authorisations were sought, the number of arrests made on the basis of information obtained under account takeover warrants or emergency authorisations, the number of prosecutions for relevant offences commenced in which information obtained under an account takeover warrant or emergency authorisation was
given in evidence, and the number of those prosecutions in which a person was found guilty.

1037. The Minister is to cause a copy of the report to be tabled before both Houses of Parliament within 15 sittings days after the Minister receives the report from the chief officer. A copy of a report given to the Minister must be given to the Ombudsman at the same time as it is given to the Minister.

3ZZVN Keeping documents connected with account takeover warrants

1038. Section 3ZZVN provides that the chief officers of the AFP and the ACIC must keep certain documents associated with their use of account takeover warrants. Documents to be kept include a copy of each warrant, section 3ZZVG assistance order and instrument of variation granted, and the applications on which they were based. If an account takeover warrant was revoked, a copy of each revocation must also be retained.

1039. A copy of each application for an emergency authorisation made, emergency authorisation given, and application for approval of the giving of an emergency authorisation must also be kept.

1040. The chief officer must also cause to be kept a copy of each written record of an urgent application made under section 3ZZUN(5), as well as a copy of each report given to the Minister and the Ombudsman under section 3ZZVL.

3ZZVP Register of applications for account takeover warrants and emergency authorisations

1041. Section 3ZZVP requires the chief officers of the AFP and the ACIC to cause a register of each application for account takeover warrants and emergency authorisations sought by their agency to be kept. The register is intended to provide an overview for the Ombudsman who is empowered to inspect such records under Division 7.

1042. Subsection 3ZZVP(2) states that the register is to include, for each account takeover warrant sought, the date the warrant was issued or refused, the date the warrant was applied for, whether the application was a formal or urgent application, the name of the magistrate who issued or refused the issue of the warrant and the name of the applicant. If the warrant was issued, the register must also include the name of the executing officer, the alleged relevant offences in respect of which the warrant was issued, the period during which the warrant is in force, details of any variations or extensions of the warrant, and whether the warrant has expired or been revoked.

1043. The register must also include the date the emergency authorisation was given or refused and the name of the appropriate authorising officer who gave or refused to give the authorisation. If the authorisation was given, the register must also include the name of the law enforcement officer to whom the authorisation was given, the alleged relevant offences in respect of which the authorisation was made, and whether that application for approval of the giving of the authorisation was successful or not.
1044. Subsection 3ZZVP(3) clarifies that a register kept under section 3ZZVP is not a legislative instrument. This subsection is merely declaratory of the law and does not prescribe a substantive exemption from the requirements relating to legislative instruments under the *Legislation Act 2003*.

**Division 7 – Inspections**

3ZZVQ Appointment of inspecting officers

1045. This item provides that the Ombudsman may, by writing, appoint members of the Ombudsman’s staff to be inspecting officers for the purposes of this Part. This is to ensure that the Ombudsman can carry out the function of overseeing agencies’ exercise of account takeover warrants.

3ZZVR Inspection of records by the Ombudsman

1046. This provision ensures that the Ombudsman must inspect the records of the AFP and the ACIC at least once every 6 months to determine compliance.

1047. Subsection 3ZZVR(2) specifies the actions that the Ombudsman may take in conducting an inspection. These actions include:

- Entering, at any reasonable time, the premises of the AFP or the ACIC, after notifying the relevant chief officer
- Having full and free access at all reasonable times to relevant records of the AFP and the ACIC
- Requiring a member of staff of the AFP or the ACIC to give necessary information to the Ombudsman where that information is in the staff member’s possession and the information is relevant to an inspection, and
- Making copies of and taking extracts from records of the AFP and the ACIC.

1048. These actions that are available to the Ombudsman are core activities enabling the Ombudsman to have effective oversight of the exercise of account takeover warrants.

1049. Subsection 3ZZVR(3) provides that the chief officer of the AFP and the ACIC must ensure that their members of staff give the Ombudsman any assistance that is reasonably required to enable the Ombudsman to perform his or her functions.

3ZZVS Power to obtain relevant information

1050. This section sets out the process by which the Ombudsman may obtain the information relevant to performing an oversight function in relation to account takeover warrants. The section only applies if the Ombudsman has reasonable grounds to believe that a law
enforcement officer of the AFP or the ACIC is in a position to give information relevant to an inspection under this Division (subsection 3ZZVS(1)).

1051. Under subsection 3ZZVS(2) the Ombudsman can request information in writing, from a law enforcement officer, to be given at a specified place and within a specified period.

1052. Under subsection 3ZZVS(3), the Ombudsman can require a law enforcement officer to attend a specified place within a specified period or at a specified time or day, in order to answer questions relevant to the inspection before a specified inspecting officer.

1053. Under subsection 3ZZVS(4), if the Ombudsman believes that a law enforcement officer has relevant information but the Ombudsman does not know that particular officer’s identity, the Ombudsman may require that the chief officer or a person nominated by the chief officer attend a specified place, at a time or date, instead of the aforementioned officer.

1054. There is a requirement under subsection 3ZZVS(5) that the place, period, time and day specified by the Ombudsman under this section has to be reasonable having regard to the circumstances in which the requirement is made.

**3ZZVT Offence**

1055. This section supports the power of the Ombudsman to compel assistance from law enforcement officers with inspections by making it an offence to fail to attend an inspection or to give information or answer questions, if a person has been requested to do so under section 3ZZVS. The penalty for this offence is imprisonment for 6 months.

**3ZZVU Ombudsman to be given information and access despite other laws**

1056. This section clarifies that there are circumstances under which a person is not excused from giving information, answering a question, or giving access to a document if requested to do so by the Ombudsman. This section explicitly overrides any other law that would otherwise contravene the request from the Ombudsman.

1057. A person is not excused from giving information, answering a question, or giving access to a document as when required by the Ombudsman under this Division and in relation to account takeover warrants on the grounds that meeting that requirement:

- would contravene a law
- would be contrary to the public interest
- might tend to incriminate the person
- would disclose legal advice given to a Minister, a Department or a prescribed authority
would disclose a communication between an officer of a Department or a prescribed authority and another person or body, being a communication protected against disclosure by legal professional privilege.

1058. **Prescribed authority** has the meaning given to it by subsection 3ZZVU(7), which is the same as the meaning of prescribed authority in the Ombudsman Act.

1059. A person who gives information to the Ombudsman is protected from prosecution by subsection 3ZZVU(2). This provision ensures that any information given to the Ombudsman is not admissible in evidence against the person who has given that information except in a proceeding by way of a prosecution for an offence against section 3ZZVH, or Part 7.4 or 7.7 of the Criminal Code.

1060. Subsection 3ZZVU(3) provides that a person is not excused from giving information, answering a question, or giving access to a document on the grounds that the person would otherwise be able to claim the privilege against self-exposure to a penalty.

1061. Subsection 3ZZVU(4) provides additional clarity about the giving of information to the Ombudsman by a law enforcement of the AFP and the ACIC. Although information collected by virtue of exercising an account takeover warrant is protected information and is subject to the prohibition on use and disclosure provided in section 3ZZVH, law enforcement officers can still share this information with the Ombudsman. Nothing in section 3ZZVH or in any other law prevents a law enforcement officer of the AFP or the ACIC from giving information to an inspecting officer or giving access to a relevant record, for the purposes of an inspection by the Ombudsman related to account takeover warrants.

1062. Similarly, under subsection 3ZZVU(5), the use and disclosure provisions relating to account takeovers do not prevent a law enforcement officer from making a record of information, causing a record to be made, or giving information to a person, if it is for the purposes of an inspection by the Ombudsman related to account takeover warrants.

1063. These provisions do not affect claims of legal professional privilege (subsection 3ZZVU(6)).

**3ZZVV Delegation by Ombudsman**

1064. These provisions ensures that the Ombudsman can delegate to an Australian Public Service employee who is responsible to the Ombudsman any or all of the Ombudsman’s functions under this Division. This exception to this broad delegation power is the power to make reports on inspections under section 3ZZVX. This cannot be delegated.

1065. This delegation power is purposefully broad. This is consistent with other delegations that relate to the Ombudsman’s inspection functions, for example in section 91 of the TIA Act. The reason for such a broad delegation is that it allows the Ombudsman to determine the most efficient, effective and appropriate means of operationalising the Ombudsman’s
functions as between the Ombudsman and staff members, whilst taking into account the powers involved and the expertise required to exercise them.

1066. A delegate must produce the instrument of delegation, or a copy of the instrument, upon the request of any person affected by the exercise of the power that has been delegated (subsection 3ZZVV(2)).

3ZZVW Ombudsman not to be sued

1067. This section ensures that whilst performing certain functions, the Ombudsman, or an inspecting officer, or anyone acting under the inspecting officer’s direction or authority, is immune from suit. They are not liable to an action, suit or proceeding for, or in relation to an act done, or omitted to be done in the exercise of a function or power conferred by this Division. To be exempt from this liability, the person must have carried out his or her actions in good faith.

3ZZVX Report on inspection

1068. This section sets out the reporting obligations that the Ombudsman has in respect of account takeover warrants.

1069. The Ombudsman must make a written report to the Minister every 6 months on the results of each inspection in regard to account takeover warrants. This is consistent with the reporting requirements under the controlled operations framework in the Crimes Act.

1070. The report given to the Minister must not include information that would prejudice an investigation or prosecution were it to be made public. Neither can the report to the Minister include information that could reasonably be expected to compromise any law enforcement agency’s operational activities or methodologies. This is because these reports will be made public as they must be tabled in Parliament under subsection 3ZZVX(3), and there needs to be consideration applied as to whether this type of information should be available to the public.

Division 8—Miscellaneous

3ZZVY Minor defects in connection with account takeover warrant

1071. Section 3ZZVY provides that if there is a defect or irregularity in relation to an account takeover warrant, and but for that defect or irregularity, the warrant would be sufficient authority to take control of the online account, then the taking control of the account is to be treated as valid, and any information obtaining by taking control of the account can be dealt with, or given in evidence in any proceeding.

1072. Subsection 3ZZVY(2) provides that a defect or irregularity in relation an account takeover warrant is any defect or irregularity other than a substantial defect or irregularity. The defect or irregularity may be in, or in connection with the issuing of, a
document purporting to be that warrant, or in connection with the execution of that warrant or the purported execution of a document purporting to be that warrant.

3ZZVZ Evidentiary certificates

1073. Section 3ZZVZ allows a law enforcement officer to issue an evidentiary certificate. Such a certificate is intended to streamline the court process by reducing the need to call numerous law enforcement officers and expert technical witnesses to give evidence about routine matters concerning the execution of warrants and the use of information obtained from taking control of an online account.

1074. The certificate may contain facts the issuer considers relevant, including anything done by the law enforcement officer or by a person assisting or providing technical expertise in connection with the warrant’s execution (paragraph 3ZZVZ(1)(a)).

1075. The certificate may also set out relevant facts with respect to anything done by the law enforcement officer relating to the communication of information obtained under a warrant by a person to another person (paragraph 3ZZVZ(1)(b)). A certificate can also set out anything done by a law enforcement officer concerning the making use of, or the making of, a record or the custody of a record of information obtained from taking control of an online account.

1076. Under subsection 3ZZVZ(2), a certificate issued under subsection 3ZZVZ(1) is admissible in evidence in any proceeding as prima facie evidence of the matters stated in the certificate.

3ZZWA Compensation for property loss or serious damage

1077. Section 3ZZWA provides that if a person suffers loss of or serious damage to property or personal injury in the course of, or as a direct result of, the execution of an account takeover warrant, the Commonwealth is liable to compensate that person. Compensation may be agreed to between the Commonwealth and the person, or, in the absence of such agreement determined by the Federal Court of Australian or Supreme Court of a State or Territory in action against the Commonwealth.

1078. Subsection 3ZZWA(2) clarifies that this provision does not apply if the person who suffered the loss, damage or injury in the course of, or as a result of, engaging in any criminal activity.

Schedule 4 – Controlled operations

Crimes Act 1914

Item 1 – Paragraph 15GI(2)(d)

1079. This item amends the controlled operations framework in the Crimes Act to enhance the ability of the AFP and the ACIC to conduct controlled operations online.
1080. In determining an application for a controlled operation, the authorising officer must be satisfied on reasonable grounds of the matters set out in subsection 15GI(2). Existing paragraph 15GI(2)(d) provides that the authorising officer must be satisfied on reasonable grounds that the operation will be conducted in a way that ensures that, to the maximum extent possible, any illicit goods involved in the controlled operation will be under the control of an Australian law enforcement officer at the end of the controlled operation. This item ensures that this matter only has to be satisfied so far as the controlled operation is not conducted online.

1081. The effect of this provision is that this consideration does not need to be given to the extent that a controlled operation is conducted online. This ensures that illicit goods or content involved in a controlled operation conducted online do not have to be under the control of law enforcement at the completion of the operation. While law enforcement will always ensure that illicit content is controlled, to the best of their ability, this provision acknowledges how easy data is to copy and disseminate, and that there may be limited guarantee that all illegal content (the illicit goods) will be under law enforcement’s control at the end of an operation conducted online.

Item 2 – Paragraph 15GQ(2)(d)

1082. This item replicates the amendment made at item 1 for the consideration of the control of illicit goods in relation to the requirements for variation of a controlled operation authority. Existing paragraph 15GQ(2)(d) provides that the authorising officer must be satisfied of the same matters in determining whether to grant a controlled operations authority. This item ensures that the illicit goods consideration only has to be satisfied so far as the controlled operation does not involve using the internet.

Item 3 – Paragraph 15GV(2)(d)

1083. This item replicates the amendments made at items 1 and 2 for the consideration of the control of illicit goods in relation to determining an application to vary an authority beyond three months. Existing paragraph 15GV(2)(d) provides that the nominated AAT member must be satisfied of the same matters in determining whether to grant a controlled operations authority. This item ensures that the illicit goods consideration only has to be satisfied so far as the controlled operation does not involve using the internet.

Schedule 5 – Minor amendments

Surveillance Devices Act 2004

Item 1 – Subsection 43A(10)

1084. The Bill provides an opportunity to make a technical correction to existing subsection 43A(10) of the SD Act.
1085. This item omits ‘of a vessel’ and substitutes it with ‘on a vessel’, which clarifies that in regards to the extraterritorial operation of computer access warrants, consent of an appropriate consenting foreign official is not required when the computer access warrant relates to a target computer that is on a vessel or aircraft of a foreign country that is Australia or in or above waters within the outer limits of the territorial sea of Australia.

**Item 2 – Before paragraph 45(4)(a)**

1086. This item makes a clarification required due to some risk associated with the ambiguity in the present drafting of section 45 of the SD Act.

1087. Section 45 contains the prohibition on the use, recording, communication or publication of protected information or its admission in evidence. It is an offence to use, record, communicate or publish protected information, otherwise than in accordance with the exception set out in subsection 45(4).

1088. The Bill adds to the list of exceptions in subsection 45(4) paragraph 45(4)(aa) which has the effect of allowing that protected information may be used, recorded, communicated or published in connection with the administration or execution of the SD Act. The effect of this amendment is that the Department and the Minister responsible for administering and executing the SD Act can receive and share information for administrative purposes. For example, information regarding how each warrant has been used can be provided to the Minister outside of the preparation of the annual reports.

**Item 3 – Subparagraph 45(4)(e)(i)**

1089. This amendment clarifies that once protected information has been communicated to the Director-General (within the meaning of the ASIO Act) under paragraph 45(4)(c), the Director-General (along with ASIO employees and ASIO affiliates) can use, record or communicate that information in the performance of their official functions.

**Item 4 – Subparagraph 45(4)(e)(i)**

1090. This amendment replaces the reference to the *Australian Security Intelligence Organisation Act 1979* to a reference to ‘that Act’, as that Act is mentioned in paragraph 45(4)(c).

**Item 5 – Subparagraph 45(4)(e)(ii)**

1091. This amendment clarifies that once protected information has been communicated to the agency head (within the meaning of the IS Act) under paragraph 45(4)(d), the agency head (along with staff members of the agencies under the IS Act) can use, record or communicate that information in the performance of their official functions.
Item 6 – Subparagraph 45(4)(e)(ii)

1092. This amendment replaces the reference to the *Intelligence Services Act 2001* to a reference to ‘that Act’, as that Act is mentioned in paragraph 45(4)(d).

*Telecommunications (Interception and Access) Act 1979*

Item 7 – Paragraph 63AB(2)(g)

1093. This item corrects an error brought to light by the drafting of this Bill, created in the process of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018*. The item repeals existing paragraph 63AB(2)(g) as it refers to ‘operational security (within the meaning of the *Intelligence Services Act 2001*) of the Organisation or of ASIS, AGO or ASD. The phrase ‘operational security’ only exists as a legislated term in the Intelligence Services Act in reference to ASIS, not in reference to the other listed bodies in the existing section.

1094. The amendment separates the paragraph into (g) and (ga), so that the phrase ‘operational security’ of ASIS is read within the meaning of the Intelligence Services Act, and the phrase ‘operational security’ in relation to the other listed bodies is taken to be the ordinary meaning of the term ‘operational security’.

Item 8 – Paragraph 63AC(2)(g)

1095. As with the above item, this item corrects an error brought to light by the drafting of this Bill, created in the process of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018*. The item repeals existing paragraph 63AC(2)(g) as it refers to ‘operational security (within the meaning of the *Intelligence Services Act 2001*) of the Organisation or of ASIS, AGO or ASD. The phrase ‘operational security’ only exists as a legislated term in the Intelligence Services Act in reference to ASIS, not in reference to the other listed bodies in the existing section.

1096. The amendment separates the paragraph into (g) and (ga), so that the phrase ‘operational security’ of ASIS is read within the meaning of the Intelligence Services Act, and the phrase ‘operational security’ in relation to the other listed bodies is taken to be the ordinary meaning of the term ‘operational security’.