MEMORANDUM ON THE OBJECTS OF THE CYBERCRIMES AND CYBERSECURITY BILL, 2017

The primary aim of the Bill is to deal with cybercrimes and cybersecurity. There is not a general universal recognised definition of cybercrimes. However, an attempted definition of cybercrimes is crimes which are committed by means of, or which was facilitated by or which involve data, a computer program, a computer data storage medium or a computer system. Cybersecurity on the other hand can more readily be defined as technologies, measures and practices designed to protect data, computer programs, computer data storage mediums or a computer systems against cybercrime, damage or interference.

1. **International position**

Internationally, most countries have cyber-specific legislation, which -

* criminalises conduct which is considered cybercrimes;
* regulates jurisdiction in respect of cybercrimes;
* specifically provides for the investigation of cybercrimes;
* regulates mutual assistance relating to the investigation of cybercrimes;
* regulates the admissibility of electronic evidence; and
* places obligations on certain persons or entities to assist in the investigation of cybercrimes.

Most countries have or are in the process of building cyber capacity to come to terms with the sudden surge of cybercrime, security breaches and attacks on critical information infrastructures, such as information infrastructures responsible for the management of electricity, water and transportation. Most countries are also in the process to put special mechanisms in place to deal with the protection of their critical information infrastructures. Some countries are also establishing a cyber offensive and defensive capacity to protect a country against politically motivated attacks on information and information systems of such a country. Various countries ratified international instruments to facilitate mutual assistance in the investigation of cybercrimes and/or to deal with aspects relevant to cybersecurity.

2. Current position in South Africa

The laws on the Statute Book do not comprehensively and uniformly criminalise conduct which is internationally regarded as cybercrimes. The laws currently on the Statute Book are silo-based, since various Departments enacted legislation to protect their interests in cyberspace, which lead to varying proscriptions of cybercrimes and penalisation of such conduct. The common law is used to prosecute some of the offences but needs to grapple with new concepts such as intangible data. Furthermore, our cybercrime laws are not in line with those of the international community, which is essential for purposes of international cooperation, which is mostly based on reciprocal laws.

Although the Protection of Harassment Act, 2011, was put on the Statute Book to comprehensively deal with harassment in the real and virtual world, many countries have recognised the seriousness of cyber harassment and have enacted specific laws which criminalise such communications. Cyber harassment is currently not recognised as a specific category of conduct in terms of the South African law and should be criminalised.

In general, our laws afford broad jurisdiction to criminal acts which affect national security in the Republic, whilst jurisdiction is significantly narrower in ordinary criminal cases. It is submitted that current jurisdiction should be expanded upon to deal with the transnational dimension of cybercrimes.

Currently, cybercrimes are investigated in terms of the Criminal Procedure Act, 1977. The investigative procedures provided for in Chapter 2 of the Criminal Procedure Act are object based and do not deal with the specialised procedures which are required to investigate cybercrimes, which involve electronic evidence which is of an incorporeal nature. Special procedures are further necessary to ensure the integrity of electronic evidence which is not catered for in the Criminal Procedure Act.

Current procedures for mutual assistance between South Africa and foreign countries in the investigation of cybercrimes do take into account the transient nature of electronic evidence and the need to act expeditiously. The resultant effect is that essential evidence is lost. Various other countries enacted legislation to provide for urgent action to preserve information and to provide expeditious assistance to identify the origin of communications involved in a cybercrime.

The laws dealing with electronic evidence are, in general, sufficient for the purposes of criminal proceedings. However, certain improvements can be made to cater for new technologies.

There is no obligation on electronic communications service providers and financial institutions to report cybercrimes and to preserve evidence of cybercrimes on their systems.

There is no coherent and organised approach in South Africa to deal with cybercrime and cybersecurity. Different Government Departments enacted legislation to protect their own interests. The silo-based approached has the effect that various essential steps which are necessary for the cybersecurity wellness of South Africa are not addressed.

There is inadequate capacity, both in the private and public sector, to deal with cybercrimes and cybersecurity

Information sharing about cyber incidents is limited. Information sharing will ensure that adequate and timeous measures are implemented against a cyber threat and are therefore essential for the cybersecurity wellness of South Africa and to effectively act against cybercrimes.

Critical information infrastructures are not adequately protected. Legislation exists for the protection of physical structures, which cannot be used to protect computer systems. The Electronic Communications and Transactions Act, 2002, narrowly caters only for the protection of databases and not for other information

infrastructures which need to be protected. No provision is currently made for the implementation of minimum security standards which are necessary to protect critical information infrastructures or to monitor compliance with such standards.

As part of Government's Outcome Based Priorities the JCPS Cluster signed the JCPS Delivery Agreement relating to Outcome 3 on 24 October 2010. This agreement focuses on certain areas and activities, clustered around specific outputs, where interventions will make a substantial and a positive impact on the safety of the people of South Africa. One such area relates to Output 8, which requires the development and implementation of a Cyber Security Policy and the development of capacity to combat and investigate cybercrime. In line therewith, the National Cybersecurity Policy Framework (the NCPF) for South Africa, was developed which provides for measures to address national security in cyberspace; measures to combat cyber warfare, cybercrime and other cyber irregularities; the development, review and updating of existing substantive and procedural laws; and measures to build confidence and trust in the secure use of Information Communications Technologies. The NCPF was approved by Cabinet in 2012.

In terms of paragraph 16.1 of the NCPF, the Department of Justice and Constitutional Development (the DOJ&CD) must review and align the cybersecurity laws of the Republic to ensure that these laws are aligned with the NCPF and provide for a coherent and integrated cybersecurity legal framework for the Republic. The Bill gives effect to this mandate of the DOJ&CD.

In terms of the Medium-Term Strategic Framework for Government 2014-2019, the Bill must be enacted and implemented by 2018/19.

3. **Overview of Bill**

The Bill aims to rationalise the laws of the RSA which deals with cybercrime and cybersecurity into a single Bill and to that extent the Bill:

* Creates offences and imposes penalties which have a bearing on cybercrime.

* Criminalises the distribution of malicious communications and provides for interim protection measures.
* Regulates jurisdiction to provide for the transnational dimension of cybercrimes.
* Regulates the powers to investigate cybercrimes.
* Regulates mutual assistance to deal with cross-border investigation of cybercrimes.
* Provides for the establishment of a 24/7 Point of Contact to facilitate mutual assistance in the investigation of cybercrime.
* Regulates the proof of certain facts by affidavit.
* Imposes obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes.
* Provides for the establishment structures to promote cybersecurity and capacity building.
* Provides for the identification and declaration of critical information infrastructures and implementation of measures to protect critical information infrastructures.
* Provides that the Executive may enter into agreements with foreign States to promote cybersecurity.
* Provides for the repeal and amendments of certain laws.

4. **Chapter by chapter breakdown of Bill**

4.1 ***Chapter 1 (clause 1)***

This clause contains various definitions aimed at facilitating the interpretation of the Bill

4.2 ***Cybercrimes (Chapter 2***)

This Chapter aims to criminalise unwanted conduct in cyberspace in line with international best practices and can be broken down in the following broad categories of criminal offences:

4.2.1 Offences against the integrity, confidentiality and availability of data, computer programs, data storage mediums and computer systems.

(a) Clause 2 criminalises unlawful securing access without authority. The criminalisation of illegal access represents an important deterrent to many other subsequent acts against the confidentiality, integrity and availability of data, computer programs, data storage mediums or a computer system, and other computer-related offences. The offence criminalises the unauthorised securing of access to data, a computer program, a computer data storage medium or a computer system.

(b) Clause 3 creates the offence of unlawful acquiring of data. The offence aims to protect data which is stored or transmitted over an electronic communications system. The offence criminalises the overcoming of protection measures which are intended to prevent access to data and thereafter acquires data, within or which is transmitted to or from a computer system. The clause further criminalises -

* the possession of data, with the knowledge that such data was acquired unlawfully; and
* possession of data, in regard to which there is a reasonable suspicion that such data was acquired unlawfully where the possessor is unable to give a satisfactory exculpatory account of such possession.

(c) Clause 4 aims to criminalise software or hardware tools which are used in the commission of cybercrimes. The criminalisation of such software and hardware is challenging in light of the fact that most of this software or hardware has dual usages, which may not be unlawful. In order to prevent over-criminalisation the Bill, in accordance with various international and regional benchmarks, requires a specific intent, namely to commit certain offences provided for in the Bill.

(d) Clauses 5 and 6 aim to criminalise unlawful interference with data or a computer program and a computer data storage medium or a computer system, respectively. The availability of the protected interests is vital for users, businesses and public administration, all of which depend on the integrity, workability and

proper functioning of data, computer programs and computer systems. Lack of availability can result in considerable pecuniary damage and may disrupt public administration.

(e) Passwords, access codes and similar data or devices, have a specific function in cyberspace, namely to protect unauthorised access to, the use of, or interference with data, a computer program, a data storage medium or a computer system for criminal purposes. This offence can be the subject of several constitutive acts, namely, the acts of obtaining, possessing, transferring and use of passwords, access codes or similar data or devices to commit an offence. Clause 7 criminalises the afore-mentioned stages to curb the unlawful use of passwords, access codes and similar data or devices to commit an offence. The clause further criminalises -

* the possession of passwords, access codes and similar data or devices, with the knowledge that such data was acquired unlawfully; and
* possession of passwords, access codes and similar data or devices, in regard to which there is a reasonable suspicion that it was acquired unlawfully where the possessor is unable to give a satisfactory exculpatory account of such possession.

4.2.2 Offences committed or facilitated by means of data, computer programs and computer systems

(a) Clause 8 aims to create a statutory offence of cyber fraud to specifically criminalise fraud by means of data or a computer program, or through the interference with data or a computer program.

(b) Clause 9 aims to create statutory offences of cyber forgery and uttering. The elements of the offence of cyber forgery are the making, with the intention to defraud, of false data or a false computer program, to the actual or potential prejudice of another person. The elements of the offence of cyber uttering are the passing off, with the intention to defraud, of false data or a false computer program, to the actual or potential prejudice of another person.

(c) Clause 10 aims to criminalise cyber extortion. The proscription is applicable where a person commits the offence of acquiring protected data, interference with data or a computer program, interference with a computer or computer system or the acquiring or use of a password, access code or related data or devices or threatens another person with the commission of such offences for the purpose of -

- obtaining any advantage from another person; or
- compelling another person to perform or to abstain from performing any act.

4.2.3 Aggravated offences

The objective of this category of offences is to protect essential computer systems and life, limb, property, essential services, the economy or the interests of the Republic, against criminal conduct in cyber space.

(a) In terms of clause 11(1), the offences of acquiring protected data, interfering with data, a computer program, computer data storage medium or a computer system which was committed against a restricted computer system are regarded as aggravated offences which are punishable with a fine or imprisonment of up to 15 years.

(b) In terms of clause 11(2), the offences of interfering with data, a computer program, computer data storage medium or a computer system, or cyber extortion which -

* endangers the life, or violates the physical integrity or physical freedom of, or causes bodily injury to, any person, or any number of persons;
* causes serious risk to the health or safety of the public or any segment of the public;
* causes the destruction of or substantial damage to any property;
* causes a serious interference with, or serious disruption of an essential service, facility or system, or the delivery of any essential service;
* causes any major economic loss; or
* creates a serious public emergency situation; or
* prejudices the security, the defence, law enforcement or international relations of the Republic,

are regarded as aggravated offences which are punishable with a sentence, as provided for in section 276 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), which that court considers appropriate and which is within that court's penal jurisdiction.

4.2.4 Clause 12 provides that the attempt, or conspiring with another person, or the aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring of another person, to commit an offence as contemplated in Chapter 2 of the Bill amounts to an offence.

4.2.5 Clause 13 provides that the common law offence of theft must be interpreted so as to include the theft of an incorporeal.

4.2.6 Clause 14 deals with penalties and prescribes certain factors which must be taken into account as aggravating circumstances.

4.2.7 Clause 14 deals with competent verdicts where a person is charged with an offence provided for in Chapter 2.

4.3 ***Malicious communications (Chapter 3)***

4.3.1 This Chapter aims to criminalise a data message:

(a) Which incites the causing of any damage to any property belonging to, or violence against, a person or a group of persons. (clause 16)

(b) Which is harmful. A data message is considered harmful if -

* it threatens a person with -
  - damage to any property belonging to, or violence against, that person; or
  - damage to any property belonging to, or violence against, any member of the family or household of the person or any other person in a close relationship with the person;
* it threatens a group of persons with damage to any property belonging to, or violence against, the group of persons or any

identified person forming part of the group of persons or who is associated with the group of persons;

* intimidates, encourages or harasses a person to harm himself or herself or any other person; or
* is inherently false in nature and it is aimed at causing mental, psychological, physical or economic harm to a specific person or a group of persons,

and a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful (clause 17)

(c) Which is intimate in nature (person is nude), and which is distributed without the consent of the person involved.

4.3.2 Clause 19 provides for an interim protection order pending finalisation of criminal proceedings. In terms of the protection order a court may -

(a) prohibit any person from further making available, broadcasting or distributing the data message contemplated in section 16, 17 or 18 which relates to the charge; or

(b) order an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question.

A person or electronic communications service provider who contravenes a protection order is guilty of an offence. Provision is made for interim proceedings where the accused person can request the court to set aside or amend the protection order. The order of a court is subject to appeal or review.

4.3.3 Electronic communications service providers are compelled to assist a court during proceedings in terms of clause 19 to make available particulars of a person who distributed the malicious communications in order to ensure that the interim protection order can be served on him or her (clause 20).

4.3.4 Clause 21 provides for orders on completion of criminal proceedings, which includes a prohibition to further distribute, to destroy or to disable access to the malicious communication.

4.3.5 Clause 22 prescribes penalties which a court may impose in respect of malicious communications or offences provided for in terms of clauses 19, 20 or 21.

4.4 ***Jurisdiction (Chapter 4)***

In terms of clause 23, a court will have jurisdiction to try an offence contemplated in Chapter 2 or clauses 16, 17 and 18 if -

* the offence was committed in the Republic;
* any act in preparation for the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;
* the offence was committed in the Republic or outside the Republic by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic;
* the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.
* the offence was committed outside the Republic and the person to be charged -
    - is a citizen of the Republic;
    - ordinarily is resident in the Republic;
    - was arrested in the territory of the Republic, or in its territorial waters or on board a ship or aircraft registered or required to be registered in the Republic at the time the offence was committed;
    - is a company, incorporated or registered under any law, in the Republic; or
    - is any body of persons, corporate or unincorporated, in the Republic; or

* the offence was committed outside the Republic by a person, other than a person provided in the previous paragraph and the offence affects or is intended to affect a public body, a business or any other person in the Republic and the person who committed the offence is found to be in the Republic.

The clause further provides that where a person is charged with attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence or as an accessory after the offence, the offence is deemed to have been committed not only at the place where the act was committed, but also at every place where the person acted.

4.5 ***Powers to investigate, search and access or seize (Chapter 5)***

4.5.1 Clause 24 provides for the issuing of Standard Operating Procedures which must be followed in the investigation of cyber offences or offences which have a cyber element. The Standard Operating Procedures provides for the manner to deal with electronic evidence to maintain the integrity of evidence. This involves five principles namely -

* legality;
* no action taken should change data held on a computer or storage media which may subsequently be relied upon in court;
* persons should be competent to access and be able to give evidence explaining the relevance and the implications of their actions;
* an audit trail should be kept to enable an independent third party to examine those processes and arrive at the same result; and
* any deviation from these principles should be explained..

4.5.2 Clause 25 provides that the Criminal Procedure Act, 1977, applies in addition to the provisions of this Chapter in so far that it is not inconsistent with the provisions of this Chapter.

4.5.3 In terms of clause 26, a police official may, in accordance with the provisions of this Chapter, search for, access or seize any article, within the Republic. An

"article" is widely defined in terms of clause 1 as any data, computer program, computer data storage medium, or computer system which -

* is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;
* may afford evidence of the commission or suspected commission; or
* is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission,

of an offence in terms of Chapter 2 or section 16, 17 or 18 of the Act or any other offence which may be committed by means of or facilitated through the use of such an article, whether within the Republic or elsewhere.

4.5.4 Clause 27 provides that an article can only be searched for, accessed or seized by virtue of a search warrant issued by a judicial officer if it appears to the judicial officer, from information on oath or by way of affirmation that there are reasonable grounds for believing that an article is being used or is involved in the commission of an offence or is required as evidence at criminal proceedings. In terms of a warrant a police official may, amongst others -

* search for any article identified in the warrant to the extent as is set out in the warrant;
* access an article identified in the warrant to the extent as is set out in the warrant;
* seize an article identified in the warrant to the extent as is set out in the warrant; or
* use or obtain and use any instrument, device, equipment, password, decryption key, data, computer program, computer data storage medium or computer system or other information that is believed, on reasonable grounds, to be necessary to search for, access or seize an article identified in the warrant to the extent as is set out in the warrant.

Provision is also made that a search warrant may require an investigator or other person identified in the warrant to assist the police official identified in the warrant, with the search for, access or seizure of the article in question, to the extent set out in the warrant. An “investigator” is defined in clause 1 as a person, who is not a

member of the South African Police Service and who is identified and authorised in terms of a search warrant to, subject to the direction and control of the police official, assist a police official with the search for, access or seizure of an article.

4.5.5 Clause 28 provides for oral applications for search warrants.

4.5.6 Clause 29 provides for search for, access to, or seizure of an article without a search warrant with the consent of a person who has lawful authority to consent.

4.5.7 Clause 30 provides that a police official may without a search warrant search any person or container or premises for the purposes of seizing a computer data storage medium or any part of a computer system involved in the commission of an offence, if the police official on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and that the delay in obtaining such warrant would defeat the object of the search and seizure. A police official may only access or seize data in respect of the computer data storage medium or a computer system in terms of a search warrant. Provision is further made that a police official may if he or she on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant he or she may access the device and search for and seize data on such a device.

4.5.8 Clause 31 provides that a police official may without a warrant, as contemplated in section 40 of the Criminal Procedure Act, 1977, arrest any person who commits or whom he or she reasonably suspects of having committed any offence or against whom a reasonable complaint has been made or credible information has been received or a reasonable suspicion exists that the person has committed an offence, contemplated in Chapter 2 or section 16, 17 or 18 of the Bill or any other offence substantially similar to an offence recognised in the Republic; which is or was committed by means of, or facilitated by the use of an article, in a foreign State and for which he or she is, under any law relating to

extradition or fugitive offenders, liable to be arrested or detained in custody in the Republic. The clause further provides that on the arrest of such a person, or where any person is arrested in terms of a warrant issued in terms of section40 or section 43 of the Criminal Procedure Act, 1977, a police official may search the person and seize a computer data storage medium or any part of a computer system which is found in the possession of or in the custody or under the control of the person. A police official may, however, only access or seize data in respect of the computer data storage medium or a computer system in terms of a search warrant. Provision is further made that a police official may if he or she on reasonable grounds believes that a search warrant will be issued to him or her if he or she applies for such warrant and it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written or oral application for a search warrant to access the article and seize data, he or she may perform these actions without a search warrant.

4.5.9 Clause 32 imposes obligations on an electronic communications service provider, financial institution and other persons, who are in control of data, a computer program, a computer data storage medium or a computer system to provide technical assistance and other assistance to a police official who is authorised in terms of a warrant to conduct an investigation, in order to search for, access and seize an article.

4.5.10 Clause 33 criminalises the obstruction or hindering of a police official or investigator to conduct an investigation in terms of this Chapter and authorises a police official to use such force as may be reasonably necessary to overcome any resistance.

4.5.11 Clause 34 provides that the powers to search, access and seize must be conducted with strict regard to decency and order and with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.

4.5.12 Clause 35 criminalises wrongful -

* searches, access and seizures; and
* obtaining or using of any instrument, device, password, decryption key or other information that is necessary to access data, a computer program, a computer data storage medium or any part of a computer system.

The clause also regulates the retention of passwords, decryption keys, data or other information. The clause further provides for civil liability which may result from a contravention of the clause.

4.5.13 Clause 36 criminalises the giving of false information which results in -

* the issuing of a search warrant;
* a search and seizure in terms of the Bill; or
* the issuing of a preservation of data direction, a preservation of evidence direction or a disclosure of data direction.

The clause further provides for civil liability which may result from a contravention of the clause.

4.5.14 Clause 37 prohibits the disclosure of any information which a person has obtained in the exercise of his or her powers or the performance of his or her functions in terms of Chapter 5 or 6 of the Bill. The clause further regulates the instances where the disclosure of information will not amount to a contravention of the clause.

4.5.15 Clause 38 clarifies the operation of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (RICA), *vis-à-vis* the Bill. In terms of the clause the interception of an indirect communication and obtaining of any real-time communication-related information on an ongoing basis, as it becomes available, must take place in terms of the RICA. Since not all electronic communications service providers are required in terms of a Government Notice No. 1325 of 2005, to be interceptable or to store communication-related information, specific obligations are imposed on these electronic communications service provider to -

(i) provide real-time communication-related information, on an ongoing basis, as it becomes available;

(ii) implement an expedited preservation of data direction;

(iii) implement a preservation of evidence direction; and

(iv) implement a disclosure of data direction;

(v) to provide archived communication-related information in respect of a customer that was stored by the electronic communications service provider; or

(vi) any order of the designated judge in terms of clause 46 of the Bill (which deals with mutual assistance (Chapter 6)).

4.5.16 Clause 39 provides for expedited preservation of data. In terms of this clause a specifically designated police official may issue, with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question, an expedited preservation of data direction to such a person, electronic communications service provider or financial institution to preserve data which is on reasonable grounds believed to be involved in an offence provided for in Chapter 2 or clause 16, 17 or 18 of the Bill. In terms of the expedited preservation of data direction a person, electronic communications service provider or financial institution must, from the time of service of the direction and for a period of 21 days, preserve the data in order to preserve the availability and integrity of the data. However, no data may be disclosed to a police official on the strength of an expedited preservation of data direction unless it is authorised in terms of clause 42 (disclosure of data direction). A person, electronic communications service provider or financial institution to whom an expedited preservation of data direction is addressed may apply to a magistrate for an amendment or the cancellation of the direction concerned on the ground that he, she or it cannot timeously or in a reasonable fashion, comply with the direction. Non-compliance with a preservation of data direction is criminalised.

4.5.17 Clause 40 provides that a judicial officer may, on the written application of a police official with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence in question, issue a preservation of evidence direction, if it appears to the judicial officer that there are reasonable grounds for believing that any person, electronic communications

service provider or financial institution may receive, is in possession of, or is in control of an article involved in the commission of an offence referred to in Chapter 2 or clause 16, 17 or 18 of the Bill. This is a procedure which is less invasive than seizure of an article and can be resorted to where it is not necessary to seize the article in question. In terms of a preservation of evidence direction a person, electronic communications service provider or financial institution must, for a time period specified in the direction (which may not exceed 90 days), preserve the article in question in order to preserve the availability of or integrity of the article. A person, electronic communications service provider or financial institution to whom a preservation of evidence direction is addressed may apply to a judicial officer for an amendment or the cancellation of the direction concerned on the ground that he, she or it cannot timeously or in a reasonable fashion, comply with the direction. Non-compliance with the direction is criminalised. Clause 41 provides for the oral application for a preservation of evidence direction.

4.5.18 In terms of clause 42, where -

* an expedited preservation of data direction or a preservation of evidence direction is in place; or
* where it is otherwise expedient to obtain data without issuing a search warrant contemplated in clause 27,

a judicial officer may, on written application by a police official, if it appears to the judicial officer from information on oath that data which is relevant to an offence contemplated in Chapter 2 or clause 16, 17 or 18 is in possession of, is in control of, may be received by a person, electronic communications service provider or financial institution, issue a disclosure of data direction. Similar to clause 40, this is a procedure which can be resorted to where it is not necessary to utilize the more invasive procedure to seize the article in question. A person, electronic communications service provider or financial institution to whom a direction is addressed may apply to a judicial officer for an amendment or the cancellation of the direction concerned on the ground that he, she or it cannot timeously or in a reasonable fashion, comply with the direction. Non-compliance with the direction is criminalised.

4.5.19 In terms of clause 43 a police official may -

* search for, access or seize publicly available data regardless of where the data is located geographically, without any specific authorisation; or
* receive non-public available data, regardless of where the data is located geographically if the person, who has the lawful authority to disclose the data voluntarily and on such conditions regarding confidentiality and limitation of use which he or she deems necessary, discloses the data to a police official.

4.6 ***Mutual assistance (Chapter 6)***

4.6.1 The provisions of clauses 46 to 49 apply in addition to Chapter 2 of the International Co-operation in Criminal Matters Act, 1996, and relate, unless specified otherwise, to the preservation of evidence, pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act (clause 44).

4.6.2 In terms of clause 44, the National Commissioner of the South African Police Service may, after obtaining the written approval of the National Director of Public Prosecutions (NDPP) and on such conditions regarding confidentiality and limitation of use, forward any information obtained during any investigation to a law enforcement agency of a foreign State when the National Commissioner is of the opinion that the disclosure of such information may assist the foreign State in the initiation or carrying out of investigations regarding an offence committed within the jurisdiction of that foreign state or lead to further cooperation with a foreign State to carry out an investigation regarding cybercrimes or offences contemplated in clause 16, 17 or 18. The South African Police Service may similarly receive any information from a foreign state, subject to such conditions regarding confidentiality and limitation of use as may be agreed upon, which will assist the South African Police Service in the investigation of a cybercrime or offences contemplated in clause 16, 17 or 18.

4.6.3 Clauses 46 to 48 of the Bill deal with requests for assistance and cooperation received from a foreign State and provide as follows:

(a) In terms of clause 46, a mutual assistance request from a foreign State must in general be submitted to the 24/7 Point of Contact contemplated in Chapter 7 of the Bill. The 24/7 point of contact must submit the request to the NDPP for consideration. Upon receipt of a request, the NDPP must satisfy himself or herself that -

* proceedings have been instituted in the foreign State; or
* there are reasonable grounds for believing that an offence has been committed in the foreign State or that it is necessary to determine whether an offence has been so committed and that an investigation in respect thereof is being conducted in the foreign State;
* the offence in question is similar to those contemplated in Chapter 2 or section 16, 17 or 18 of the Bill or other offence recognised in South Africa; and
* the State intends to submit a request in terms of section 7 of the International Co-operation in Criminal Matters Act, for obtaining the data, communication or article in the Republic for use in such proceeding or investigation in the foreign State.

The NDPP must submit the request for assistance, together with his or her recommendations, to the Cabinet member responsible for the administration of justice, for his or her approval. On receipt of the approval of the Cabinet Member, the request must be submitted to the designated judge for consideration. Where the request relates to the expedited disclosure of traffic data, the NDPP must submit the request for assistance, together with his or her recommendations, to the designated judge. The designated judge may issue any order which he or she deems appropriate to ensure that the requested -

* data or other article is preserved in accordance with clause 40;
* data is seized on an expedited basis in accordance with clause 27 and preserved;
* traffic data (which is data relating to a communication indicating the communication's origin, destination, route, format, time, date, size, duration or type of the underlying service), in so far as it may indicate that a person, electronic communications service provider or financial institution in another

state was involved in the transmission of the communication, is disclosed on an expedited basis in accordance with clause 42;

* data, which is a real-time communication-related information, is obtained and preserved; or
* data which is an indirect communication is intercepted and preserved,

as is specified in the request.

The designated judge may only issue an order if the facts alleged in the request -

* substantiate the fact that -
  - an offence substantially similar to the offences contemplated in Chapter 2 or section 16, 17 or 18 has been or is being or will probably be committed or any other offence substantially similar to an offence recognised in the Republic was committed by means of, or facilitated through the use of an article; and
  - it is necessary, in the interests of justice, to give the order;
* clearly identifies the person, electronic communications service provider or financial institution that will receive, is in possession of, or is in control of the data or other article that must be preserved, or from whose facilities the data or traffic data must be obtained or intercepted; the data or other article which must be preserved; the data which must be seized on an expedited basis; the traffic data which must be disclosed on an expedited basis; the data, which is real-time communication-related information, which is to be obtained; or the data, which is an indirect communication, which is to be intercepted;
* the request is, where applicable, in accordance with any treaty, convention or other agreement to which that foreign state and the Republic are parties or which can be used as a basis for mutual assistance; and
* the order is in accordance with any applicable law of the Republic.

Where a request relates to the expedited disclosure of traffic data, the designated judge may -

* specify conditions or restrictions relating to the disclosure of traffic data as he or she deems appropriate; or

* refuse to issue an order if he disclosure of the traffic data will or is likely to prejudice the sovereignty, security, public safety, or other essential interests of the Republic.

In the case of urgency, a request by any authority, court or tribunal exercising jurisdiction in a foreign State may be submitted directly to the designated judge who must deal with the request in accordance with this clause.

An order contemplated by the designated judge must be executed by a specially designated police official, who must inform the designated judge and the NDPP, of the fact that an order has been executed. The NDPP must inform a foreign State of the fact that an order was issued and executed or not issued.

(b) Clause 47 imposes obligations on a person, electronic communications service provider or financial institution to comply with an order of the designated judge issued in terms of clause 46. A person, electronic communications service provider or financial institution may, in writing, apply to the designated judge for an amendment or the cancellation of the order concerned on the ground that he, she or it cannot timeously or in a reasonable fashion, comply with the order. Non-compliance with an order of the designated judge or the giving of false information is criminalised.

(c) Clause 48 provides that the NDPP must inform the designated judge and a foreign State of the outcome of its request for assistance and cooperation. The clause further provides that any traffic data which is made available on an expedited basis, in terms of an order in terms of clause 46, must be provided to the 24/7 Point of Contact for submission to a foreign State.

4.6.4 Clause 49 deals with the requests for mutual assistance by South Africa to a foreign State. In terms of the clause if there is reasonable grounds for believing that an offence, contemplated in Chapter 2 or clause 16, 17 or 18, or any other offence in terms of the laws of the Republic which may be committed or facilitated by means of an article, has been committed and that it is necessary pending the issuing of a letter of request in terms of section 2(2) of the International Co-operation in Criminal Matters Act, 1996, to -

* preserve data or other articles;
* seize data or other articles on an expedited basis;
* disclose traffic data on an expedited basis;
* obtain data which is real-time communication-related information or archived communication-related information; or
* intercept data which is an indirect communication,

within the area of jurisdiction of a foreign State, a magistrate may issue a direction in the prescribed form in which assistance from that foreign State is sought as is stated in the direction. The direction must specify -

* that there are reasonable grounds for believing that an offence contemplated in the Bill has been committed in the Republic or that it is necessary to determine whether an offence has been committed;
* that an investigation in respect thereof is being conducted; and
* the nature of the mutual assistance that is required within the area of jurisdiction of a foreign State.

The NDPP is responsible for the transmission of the direction to the foreign State which is requested to provide assistance and cooperation.

4.7 ***24/7 Point of Contact (Chapter 7)***

Clause 50 provides for the establishment and functions of the 24/7 Point of Contact as part of the South African Police Service. The 24/7 Point of Contact must operate on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate expedited assistance, which includes -

* technical advice and assistance;
* anything which is authorised under Chapters 5 and 6;
* legal assistance;
* identification and location of an article;
* the identification and location of a suspect; and
* cooperation with appropriate authorities of a foreign State,

for the purpose of proceedings or investigations regarding the commission or intended commission of an offence under Chapter 2 or section 16, 17 or 18 or any

other offence which may be committed or facilitated by means of an article within the Republic or in a foreign State.

The Cabinet member responsible for policing may make regulations to further regulate any aspect which is necessary or expedient for the proper implementation of this clause. The NDPP must make available members of the National Prosecuting Authority to provide legal assistance to the 24/7 Point of Contact as may be necessary or expedient for the effective operation of the 24/7 Point of Contact.

4.8 ***Evidence (Chapter 8)***

Clause 51 aims to regulate the proof of certain facts by affidavit. In terms of the clause, whenever any fact established by any examination or process requiring any skill in the interpretation of data; the design of, or functioning of data, a computer program, a computer data storage medium or a computer system; computer science; electronic communications networks and technology; software engineering; or computer programming, is relevant to criminal proceedings, an affidavit made by a person who, in that affidavit, states that he or she -

* is in the service of a body in the Republic or a foreign State designated by the Cabinet member responsible for the administration of justice, by notice in the Gazette;
* possesses relevant qualifications, expertise and experience which make him or her competent to make the affidavit; and
* has established such fact by means of an examination or process,

is, upon its mere production at such proceedings, prima facie proof of such fact.

Any person who makes such an affidavit wilfully states anything which is false, is guilty of an offence. The clause further provides that any court before which an affidavit is produced as *prima facie* proof of the relevant contents thereof may, in its discretion, cause the person who made the affidavit to be subpoenaed to give oral evidence in the proceedings in question or may cause written interrogatories to be submitted to such person for reply and such interrogatories and any reply thereto purporting to be a reply from such person are likewise admissible in evidence at such proceedings. The clause also prescribes specific requirements

which must be adhered to if the person who has made the affidavit alleges that he or she is in the service of a body in the Republic or foreign State designated by the Cabinet member responsible for the administration of justice.

4.9 ***Obligations of electronic communications service providers and financial institutions (Chapter 9)***

Clause 52 imposes obligations on electronic communications service providers and financial institutions who are aware of, or becomes aware of the fact that their computer systems are involved in the commission of any category or class of offences provided for in Chapter 2 which is determined by the Cabinet member responsible for policing, to report such offences to the South African Police Service and to preserve any information which may be of assistance to the South African Police Service to investigate such offences. Non-compliance with the clause is criminalised. The clause is not applicable to a financial sector regulator or any function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act, 1989.

4.10 ***Structures to deal with cybersecurity (Chapter 10)***

4.10.1 Clause 53 establishes the Cyber Response Committee (CRC) as the overseeing body to implement the cyber initiative of the Republic. The CRC consists of a chairperson who is the Director-General: State Security and members who are the Heads of the representative Departments and one of their nominees. The Cabinet member responsible for State security must -

* oversee and exercise control over the performance of the functions of the CRC; and
* at the end of each financial year, submit a report to the Chairperson of the Joint Standing Committee on Intelligence, regarding progress that has been made towards achieving the objects and functions of the Cyber Response Committee.

4.10.2 Clause 54 deals with the establishment of structures which supports cybersecurity and capacity building. In terms of the clause:

* The Cabinet member responsible for State security must—
  - establish, equip, operate and maintain a Computer Security Incident Response Team for Government;
  - establish and maintain sufficient human and operational capacity to give effect to cybersecurity measures falling within the Constitutional mandate of the State Security Agency and to deal with critical information infrastructure protection.
* The Cabinet member responsible for policing must establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes and ensure that members of the South African Police Service receive basic training in aspects relating to the detection, prevention and investigation of cybercrimes.
* The Cabinet member responsible for defence must establish and maintain a cyber offensive and defensive capacity as part of the defence mandate of the South African National Defence Force.
* The Cabinet member responsible for telecommunications and postal services must -
  - establish and maintain a Cybersecurity Hub as part of the Department of Telecommunications and Postal Services to promote cybersecurity in the private sector; and
  - encourage and facilitate the establishment of nodal points and private sector computer security incident response teams in the private sector.
* The clause further provides that the respective Cabinet members -
  - may make regulations to regulate any aspect which is necessary or expedient for the proper implementation of this subsection; and
  - must report to Parliament regarding progress that has been made towards achieving the objects and functions as is provided in the clause.

4.10.3 Clause 55 deals with the establishment of nodal points (structures which receive and distribute information regarding cybersecurity incidents) and the recognition of private sector computer security incident response teams (expert groups that handle cybersecurity incidents). In terms of the clause the Cabinet member responsible for telecommunications and postal services must, by notice in the Gazette, after following a consultation process with the persons or entities in a sector, declare different sectors which provide an electronic communications service for which a nodal point must be established.

Each sector must, within 6 months from the date of the publication of a notice identify and establish a nodal point, which will be responsible for -

* distributing information regarding cyber incidents to other entities within the sector;
* receiving and distributing information about cybersecurity incidents to the nodal points established for other sectors or any computer security incident response team;
* reporting cybersecurity incidents to the Cybersecurity Hub; and
* receiving information about cybersecurity incidents from the Cybersecurity Hub.

If a sector fails to identify or establish a nodal point, the Cabinet member responsible for telecommunications and postal services may, after consultation with the sector, identify and establish a nodal point for that sector on such terms and conditions as he or she deems fit. The different sectors are responsible for the establishment and operating costs of nodal points. The clause empowers the Cabinet member to make regulations regarding the funding of nodal points and to further regulate any aspect relating to the establishment, operation or functioning of a nodal point. The clause further provides that the Cabinet member may recognise any computer security incident response team which is established for a sector and provide for the making of regulations to further facilitate the effective functioning of such a computer security incident response team.

4.10.4 Clause 56 empowers the Cabinet member responsible for the administration of justice to make regulations to regulate information sharing, for purposes of Chapter 10.

4.11 ***Critical information infrastructure protection (Chapter 11)***

4.11.1 Clause 57 deals with the protection of critical information infrastructures. In terms of the clause:

* The Cabinet member responsible for State security is empowered to declare information infrastructures which are of such a strategic nature that any interference with them or their loss, damage, disruption or immobilisation may -
  - substantially prejudice the security, the defence, law enforcement or international relations of the Republic;
  - substantially prejudice the health or safety of the public;
  - cause a major interference with or disruption of, an essential service;
  - cause any major economic loss;
  - cause destabilisation of the economy of the Republic; or
  - create a major public emergency situation,

  as critical information infrastructures.
* The clause provides for an extensive consultation process with the various parties involved before an information infrastructure may be declared a critical information infrastructure.
* The Cabinet member responsible for State security must, within six months of the declaration of any information infrastructure as a critical information infrastructure, in consultation with the relevant Cabinet members (Cabinet members responsible for defence, telecommunications and postal services, justice and correctional services, policing and State security) and other specified persons, issue directives to the critical information infrastructure in order to regulate minimum standards relating to -
  - the classification of data held by the critical information infrastructure;
  - the protection of, the storing of, and archiving of data held by the critical information infrastructure;
  - cybersecurity incident management by the critical information infrastructure;
  - disaster contingency and recovery measures which must be put in place by the critical information infrastructure;

- minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure;
- the period within which the owner of, or person in control of a critical information infrastructure must comply with the directives; and
- any other relevant matter which is necessary or expedient in order to promote cybersecurity in respect of the critical information infrastructure.

The clause provides for a dispute mechanism, in terms of which an information infrastructure may dispute the decision by the Cabinet member responsible for State security to declare it a critical information infrastructure as well as the measures which the infrastructure needs to implement in terms of a direction which was issued to it.

* A critical information infrastructure must at own cost, take steps to the satisfaction of the Cabinet member responsible for State security, to comply with a directive. If a critical information infrastructure fails to comply with a direction, the Cabinet member responsible for State security may, by written notice, order him or her to take such steps in respect of the critical information infrastructure as may be specified in the notice, within the period specified in the notice. A critical information infrastructure which without reasonable cause refuses or fails to take the steps specified in the notice within the period specified therein, is guilty of an offence. The Cabinet member responsible for State security may take or cause to be taken those steps which the owner or person failed or refused to take, and the Cabinet member may recover the costs of those steps from the owner or person on whose behalf they were taken.

4.11.2 Clause 58 provides for the auditing of critical information infrastructures to ensure compliance with a directive which is issued by the Cabinet member responsible for State security in terms of clause 57. In terms of the clause:

* The owner or person in control of a critical information infrastructure must, once every 24 months, at own cost, cause an audit to be performed on the critical information infrastructure by an independent auditor in order to evaluate compliance with the directive. The critical information infrastructure must notify the Director-General: State Security of the date on which an audit is to be performed whereupon the Director-General: State Security may designate any member of the

State Security Agency or any other person to monitor, evaluate and report on the adequacy and effectiveness of the audit.

* The owner or person in control of a critical information infrastructure must, upon completion of the audit, report in the prescribed form and manner to the Director-General: State Security regarding the outcome of the audit in order to enable the Director-General to evaluate compliance with the directive.

* The failure to perform an audit or to comply with the various regulatory provisions of the clause is criminalised.

* The Cabinet member responsible for State security must, by notice in the *Gazette*, prescribe the persons or the category or class of persons who are competent to be appointed to perform an audit as contemplated in the clause.

4.12 ***Agreements with foreign states (Chapter 12)***

In terms of clause 59, the National Executive may enter into agreements with any foreign State regarding -

* mutual assistance and cooperation relating to the investigation and prosecution of offences contemplated in the Bill;
* research, information and technology-sharing and the development and exchange of information on cybersecurity-related matters;
* the establishment of 24/7 contact points; and
* the implementation of measures to address cyber threats.

4.13 ***General provisions (Chapter 13)***

4.13.1 In terms of clause 60, the NDPP is obliged to keep statistics of the number of prosecutions instituted in terms of Chapter 2 or clause 16, 17 or 18 of the Bill, the outcome of such prosecution and any other information relating to such prosecutions, which is determined by the Cabinet member responsible for the administration of justice. These statistics must be included in the report of the NDPP, referred to in section 22(4)(*g*) of the National Prosecuting Authority Act, 1998, and on the written request of the Chairperson of the CRC be made available to the CRC.

4.13.2 Clause 61 repeals or amends the following laws:

	Law	Extent of repeal or amendment
(a)	South African Police Service Act, 1995 (Act 68 of 1995)	Section 71, which criminalises conduct which is now criminalised in terms of the Bill, is deleted.
(b)	Criminal Procedure Act, 1977 (Act 51 of 1977)	Schedule 5 is amended to further regulate bail proceedings in respect of offences contemplated in - * clauses 8, 9 or 10 which exceed R500 000 or involve aggravating circumstances; or * clause 11(2).
(c)	Criminal Law Amendment Act, 1997 (Act 105 of 1997)	Part II of Schedule 2 is amended in order to make the minimum sentence regime applicable to the offences contemplated in - * clauses 8, 9 or 10 involving amounts of more than R500 000, or involve aggravating circumstances; or * clause 11(2).
(d)	National Prosecuting Authority Act, 1998 (Act 32 of 1998)	Sections 40A and 41(4), which criminalise conduct which is criminalised in terms of the Bill, are deleted.
(e)	Correctional Services Act, 1998 (Act 111 of 1998)	Section 128, which criminalises conduct which is criminalised in terms of the Bill, is deleted.
(f)	Financial Intelligence Centre Act, 2001 (Act 38 of 2001)	Sections 65, 66 and 67, which criminalise conduct which is criminalised in terms of the Bill, are deleted.
(g)	Electronic Communications and Transactions Act, 2002 (Act 25 of 2002)	* The definitions of “critical data”, “critical database” and “critical database administrator” (section 1) and Chapter IX, are deleted/ * Sections 85, 86, 87, 88 and 90, which criminalise conduct which is criminalised in terms of the Bill, are deleted and section 89 is substituted to effect consequential amendments.
(h)	Disaster Management Act, 2002 (Act 57 of 2002)	The definition of “disaster”, in section 1 is substituted to include damage to or disruption of critical information infrastructure as contemplated in section 51(2) of the Bill.
(i)	Regulation of Interception of Communications and Provision of Communication related Information Act, 2002 (Act 70 of 2002)	(i) Section 17(4) is substituted to provide for the issuing of a direction for the provision of real-time communication-related information on an ongoing basis if it is necessary for purposes of investigating an offence contemplated in the newly inserted Schedule 2.

	Law	Extent of repeal or amendment
		(ii) The Schedule to the Act is renamed to "Schedule I" and the following items are added to the Schedule: * The offence contemplated in sections 17, 18, 19A or 20 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007). * The offence contemplated in - - clause 8, 9(1) or (2) or 10 of the Bill which involves an amount of R200 000 or more; and - section 11(1) or (2) or 12 (in so far as the section relates to the offences referred to in section 11(1) or (2)) of the Bill. (iii) A new Schedule II is included to further regulate the provision of real-time communication-related information on an ongoing basis in respect of offences contemplated in sections 3(1), 4(2), 5, 6, 7(1), 8, 9(1) or (2), 10 of the Bill, which involves an amount in excess of R50 000. (iv) A consequential amendment is affected to the definition of a "serious offence".
(j)	Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act 33 of 2004)	(i) A definition of "critical information infrastructure" is inserted in section 1. (ii) The definition of "terrorist activity" is amended to include "the destruction of or substantial damage to, or interference with, a critical information infrastructure or any part thereof". (iii) Section 3(2) is amended to expand the offence connected with a terrorist activity to the provision or offering of a "software or hardware tool as defined in clause 4(3)" of the Bill, connected with the engagement in a terrorist activity, and who knows or ought reasonably to have known or suspected that such "software or hardware tool" so connected.
(k)	Films and Publications Act, 1996 (Act 65 of 1996)	Section 24B of the Act, which deals with child pornography and the sexual exploitation of children, is repealed.
(l)	Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007)	(i) The definition of "child pornography" is amended to extend its application to "presentations". (ii) A definition of "electronic communications service provider" is inserted in section 1.

	Law	Extent of repeal or amendment
		(iii) The proposed section 10A aims to criminalise the disclosure of pornography, threats to disclose pornography and disclosure or threats childpornography for the purposes of obtaining any advantage from a person. The proposed amendments further provides for interim court orders and orders on completion of criminal proceedings to protect a victim against the offences in question. (iv) The proposed clause 19A aims to comprehensively criminalise child pornography and the sexual exploitation of children in line with international instruments. (v) The current section 20 is amended to criminalise conduct which relates to live performance involving child pornography and the recruiting of a child for purposes of creating, making or producing child pornography or participating in a live performance involving child pornography. (vi) Section 56A is amended to provide for penalties which a court may impose in respect of the proposed offences.
(m)	Child Justice Act, 2008 (Act 75 of 2008)	Schedules 2 and 3 are amended to provide for the sentencing of child offenders who commit cyber offences.

4.13.3 Clause 62 provides for the making of regulations to further regulate aspects provided for in the Bill.

4.13.4 Clause 63 deals with the Short Title and commencement.