REPUBLIC OF SOUTH AFRICA

CYBERCRIMES AND CYBERSECURITY BILL

DRAFT FOR PUBLIC COMMENT

———————

(As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. …….. of …….. 2015) (The English text is the official text of the Bill)

———————

(MINISTER OF JUSTICE AND CORRECTIONAL SERVICES)

[B—2015]

_____

BILL

To create offences and impose penalties which have a bearing on cybercrime; to further regulate jurisdiction of the courts; to further regulate the powers to investigate, search and access or seize; to further regulate aspects of international cooperation in respect of the investigation of cybercrime; to provide for the establishment of a 24/7 Point of Contact; to provide for the establishment of various structures to deal with cyber security; to regulate the identification and declaration of National Critical Information Infrastructures and measures to protect National Critical Information Infrastructures; to further regulate aspects relating to evidence; to impose obligations on electronic communications service providers regarding aspects which may impact on cyber security; to provide that the President may enter into agreements with foreign States to promote cyber security; to delete and amend certain provisions of certain laws; and to provide for matters connected therewith.

PARLIAMENT of the Republic of South Africa enacts as follows:—

ARRANGEMENT OF SECTIONS

CHAPTER 1

DEFINITIONS

CHAPTER 2

OFFENCES

CHAPTER 3

JURISDICTION

CHAPTER 4
POWERS TO INVESTIGATE, SEARCH AND ACCESS OR SEIZE AND INTERNATIONAL COOPERATION

CHAPTER 5
24/7 POINT OF CONTACT

CHAPTER 6
STRUCTURES TO DEAL WITH CYBER SECURITY

CHAPTER 7
NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

CHAPTER 8

EVIDENCE

CHAPTER 9

GENERAL OBLIGATIONS OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND LIABILITY

CHAPTER 10

AGREEMENTS WITH FOREIGN STATE

CHAPTER 11

GENERAL PROVISIONS

Schedule

CHAPTER 1

DEFINITIONS

Definitions and interpretation

1. In this Act, unless the context indicates otherwise—

"**24/7 contact point**" means a designated point of contact, established in terms of section 49;

"**computer data storage medium**" means any article, device or location from which data is capable of being reproduced or on which data is capable of being stored, by a computer device, irrespective of whether the article or device is physically attached to or connected with the computer device;

"**computer device**" means any electronic programmable device used, whether by itself or as part of a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing or storage operations in accordance with set instructions and includes all—

(a) input devices;

(*b*) output devices;

(*c*) processing devices;

(*d*) computer data storage mediums;

(*e*) programs; and

(*f*) other equipment and devices,

that are related to, connected with or used with such a device or any part thereof;

"**computer network**" means two or more inter-connected or related computer devices, which allows these inter-connected or related computer devices to—

(*a*) exchange data or any other function with each other;

(*b*) exchange data or any other function with another computer network; or

(*c*) connect to an electronic communications network;

"**computer program**" means a sequence of instructions which enables a computer device to perform a specified function;

"**critical data**" means data that is of importance for the protection of—

(*a*) the security, defence or international relations of the Republic;

(*b*) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Republic or of a State;

(*c*) the enforcement of a law of the Republic or of a State;

(*d*) the protection of public safety;

(*e*) trade secrets;

(*f*) records of a financial institution; or

(*g*) commercial information, the disclosure of which could cause undue advantage or disadvantage to any person,

and includes data relating to aspects referred to in section 58(2)*(a)* to *(f)* of this Act or any other data which is in possession of or under the control of a National Critical Information Infrastructure;

"**critical database**" means a computer data storage medium or any part thereof which contains critical data;

"**data**" means any representation of facts, information, concepts, elements, or instructions in a form suitable for communications, interpretation, or processing in a computer device, a computer network, a database, an electronic communications network or their accessories or components or any part thereof and includes a computer program and traffic data;

"**database**" means a collection of data in a computer data storage medium;

"**data message**" means data in an intelligible form, in whatever form generated, sent, received, communicated, presented, tendered or stored by electronic means;

"**electronic communications network**" means electronic communications infrastructures and facilities used for the conveyance of data;

"**electronic communications service provider**" means any—

(*a*) person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005;

(*b*) 'financial institution' as defined in section 1 of the Financial Services Board Act, 1990 (Act No. 97 of 1990); or

(*c*) person or entity who or which transmits, receives, processes or stores data—

(i) on behalf of the person contemplated in paragraph (*a*) or (*b*) or the clients of such a person; or

(ii) of any other person;

"foreign State" means any State outside the Republic and includes any territory under the sovereignty or control of such State;

"**National Critical Information Infrastructure**" means means any data, computer data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto—

(*a*) which is specifically declared a National Critical Information Infrastructure in terms of section 58(2) of this Act; or

(*b*) which, for purposes of Chapters 2 and 4 of this Act, are in possession of or under the control of—

(i) any department of State or administration in the national, provincial or local sphere of government; and

(ii) any other functionary or institution exercising a public power or performing a public function in terms of any legislation,

irrespective whether or not it is declared a National Critical Information Infrastructure as contemplated in paragraph (a);

"**National Commissioner**" means the National Commissioner of the South African Police Service, appointed by the President under section 207(1) of the Constitution of the Republic of South Africa, 1996;

"**person**" means a natural or a juristic person;

"**Service**" means the South African Police Service established by section 5(1) of the South African Police Service Act, 1995 (Act No. 68 of 1995); and

"**traffic data**" means data relating to a communication indicating the communication"s origin, destination, route, format, time, date, size, duration or type of the underlying service.

CHAPTER 2

OFFENCES

Definitions and interpretation

2. (1) In this Chapter, unless the context indicates otherwise **"computer related"** means the use of data, a computer device, a computer network, a database or an electronic communications network to commit a prohibited act provided for in sections 11, 12, 13, 14, 15 or 16.

(2) Any act which constitutes an offence in terms of section 3(1), (2) or (3) (in so far as it relates to the acquiring, provision or use of personal information or financial information), 4(1), 5(1), 6(2)(*a*), 7(1), 8(1), 9(1) (in so far as it relates to the use

of malware) or 10(1) (in so far as it relates to the acquiring, provision or use of an access code, password or similar data or devices), which is performed on request of a person who has the lawful authority to consent to such act in order to perform a security audit on data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure —

(*a*) may not be regarded as unlawful if it falls within the written authority which was granted by the person who has the lawfully authority to consent to such act; and

(*b*) must be regarded as unlawful if it exceeds the written authority which was granted by the person who has the lawful authority to consent to such act.

Personal information and financial information related offences

3. (1) Any person who unlawfully and intentionally—

(*a*) acquires by any means;

(*b*) possesses; or

(*c*) provides to another person,

the personal information of another person for purposes of committing an offence under this Act is guilty of an offence.

(2) Any person who unlawfully and intentionally—

(*a*) acquires by any means;

(*b*) possesses; or

(*c*) provides to another person,

the financial information of another person for purposes of committing an offence under this Act is guilty of an offence.

(3) Any person who unlawfully and intentionally uses the personal information or financial information of another person to commit an offence under this Act is guilty of an offence.

(4) Any person who is found in possession of personal information or financial information of another person in regard to which there is a reasonable suspicion that such personal information or financial information—

(*a*) was acquired, is possessed, or is to be provided to another person for purposes of committing an offence under this Act; or

(*b*) was used or may be used to commit an offence under this Act,

and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(5) Any person who contravenes the provisions of subsection (1), (2) or (4) is liable, on conviction to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(6) Any person who contravenes the provisions of subsection (3) is liable, on conviction to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(7) For purposes of this section—

(*a*) "**personal information**" means any „personal information" as defined in section 1 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013); and

(*b*) "**financial information**" means any information or data which can be used to facilitate a financial transaction.

Unlawful access

4. (1) Any person who unlawfully and intentionally accesses the whole or any part of —

(*a*) data;

(*b*) a computer device;

(*c*) a computer network;

(*d*) a database;

(*e*) a critical database;

(*f*) an electronic communications network; or

(*g*) a National Critical Information Infrastructure,

is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), (*b*), (*c*), (*d*) or (*f*), to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*e*) or (*g*) to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(3) For purposes of this section "**access**" includes, without limitation, to make use of, to gain entry to, to view, display, instruct, or communicate with, to store data in or retrieve data from, to copy, move, add, change, or remove data or otherwise to make use of, configure or reconfigure any resources of a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure, whether in whole or in part, including their logical, arithmetical, memory, transmission, data storage, processor, or memory functions, whether by physical, virtual, direct, or indirect means or by electronic, magnetic, audio, optical, or any other means.

(4) For purposes of this section, the actions of a person, to the extent that they exceed his or her lawful authority to access data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure, must be regarded as unlawful.

Unlawful interception of data

5. (1) Any person who unlawfully and intentionally intercepts data to, from or within—

(*a*) a computer device;

(*b*) a computer network;

(*c*) a database;

(*d*) a critical database;

(*e*) an electronic communications network; or

(*f*) a National Critical Information Infrastructure,

or any part thereof, is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), (*b*), (*c*), or (*e*), to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*d*) or (*f*) to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(3) For purposes of this section **"interception of data**" means the acquisition, viewing, capturing or copying of data through the use of a hardware or software tool contemplated in section 6(5) or any other means, so as to make some or all of the data available to a person other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data and includes the—

(*a*) examination or inspection of the contents of the data; and

(*b*) diversion of the data or any part thereof from its intended destination to any other destination.

Unlawful acts in respect of software or hardware tools

6. (1) Any person who unlawfully and intentionally manufactures, assembles, obtains, sells, purchases, makes available or advertises any software or

hardware tool for the purposes of contravening the provisions of section 3(1)(*a*) or (2)(*a*), 4(1), 5(1), 7(1), 8(1), 10(1), 11(1), 12(1) or (2) or 13(1), is guilty of an offence.

(2) Any person who unlawfully and intentionally—

(*a*) uses; or

(*b*) possesses,

any software or hardware tool for purposes of contravening the provisions of section 3(1)(*a*) or (2)(*a*), 4(1), 5(1), 7(1), 8(1), 10(1), 11(1), 12(1) or (2) or 13(1), is guilty of an offence.

(3) Any person who is found in possession of a software or hardware tool in regard to which there is a reasonable suspicion that such software or hardware tool is possessed for the purposes of contravening the provisions of section 3(1)(*a*) or (*c*) or (2)(*a*) or (*c*), 4(1), 5(1), 7(1), 8(1), 10(1), 11(1), 12(1) or (2) or 13(1), and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(4) Any person who contravenes the provisions of subsections (1), (2) or (3) is liable, on conviction to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(5) For purposes of this section " **software or hardware tools**" means any data, electronic, mechanical or other instrument, device, equipment, or apparatus, which is used or can be used, whether by itself or in combination with any other data, instrument, device, equipment or apparatus, in order to—

(*a*) acquire, make available or to provide personal information or financial information as contemplated in section 3(1)(a) or (*c*), or (2)(*a*) or (*c*);

(*b*) access as contemplated in section 4(3);

(*c*) intercept data as contemplated in section 5(3);

(*d*) interfere with data as contemplated in section 7(3);

(*e*) interfere with a computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure as contemplated in section 8(3); or

(*f*) acquire, modify, provide, make available, copy or clone a password, access code or similar data and devices as defined in section 10(4).

Unlawful interference with data

7. (1) Any person who unlawfully and intentionally interferes with—

(*a*) data; or

(*b*) critical data,

is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), to a fine not exceeding R 5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*b*), to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(3) For purposes of this section **"interference with data"** means to—

(*a*) alter data;

(*b*) hinder, block, impede, interrupt or impair the processing of, functioning of, access to, the confidentiality of, the integrity of, or the availability of data; or

(*c*) make vulnerable, suppress, corrupt, damage, delete or deteriorate data.

Unlawful interference with computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure

8. (1) Any person who unlawfully and intentionally interferes with the use of —

(*a*) a computer device;

(*b*) a computer network;

(*c*) a database;

(*d*) a critical database;

(*e*) an electronic communications network; or

(*f*) a National Critical Information Infrastructure,

is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), (*b*), (*c*), or (*e*), to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*d*) or (*f*) to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(3) For purposes of this section "**interference with computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure"** means to hinder, block, impede, interrupt, alter or impair the functioning of, access to, the confidentiality of, the integrity of, or the availability of a computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure.

Unlawful acts in respect of malware

9. (1) Any person who assembles, obtains, sells, purchases, possesses, makes available, advertises or uses malware for the purposes of unlawfully and intentionally causing damage to—

(*a*) data;

(*b*) a computer device;

(*c*) a computer network;

(*d*) a database;

(*e*) a critical database;

(*f*) an electronic communications network; or

(*g*) a National Critical Information Infrastructure,

is guilty of an offence.

(2) Any person who is found in possession of malware in regard to which there is a reasonable suspicion that such malware is possessed for the purposes of unlawfully and intentionally causing damage to—

(*a*) data;

(*b*) a computer device;

(*c*) a computer network;

(*d*) a database;

(*e*) a critical database;

(*f*) an electronic communications network; or

(g) a National Critical Information Infrastructure,

and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(3) Any person who contravenes the provisions of subsection (1) or (2) is liable, on conviction—

(*a*) in the case of a contravention of the provisions of subsection (1)(*a*), (*b*), (*c*), (*d*) or (*f*) or (2), to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment; or

(*b*) in the case of a contravention of the provisions of subsection (1)(*e*) or (*g*) to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(4) For purposes of this section "**malware**" means any data, electronic, mechanical or other instrument, device, equipment, or apparatus that is designed specifically to—

(*a*) create a vulnerability in respect of;

(*b*) modify or impair;

(*c*) compromise the confidentiality, integrity or availability of; or

(*d*) interfere with the ordinary functioning or usage of,

data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure.

Unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices

10. (1) Any person who unlawfully and intentionally—

(*a*) acquires by any means;

(*b*) possesses;

(*c*) provides to another person; or

(*d*) uses,

an access code, password or similar data or device for purposes of contravening the provisions of section 3(1)(*a*) or (*c*) or (2)(*a*) or (*c*), 4(1), 5(1), 7(1), 8(1), 11(1), 12(1) or (2) or 13(1), is guilty of an offence.

(2) Any person who is found in possession of an access code, password or similar data or device in regard to which there is a reasonable suspicion that such access code, password or similar data or device was acquired, is possessed, or is to be provided to another person or was used or may be used for purposes of contravening the provisions of section 3(1)(*a*) or (*c*) or (2)(*a*) or (*c*), 4(1), 5(1), 7(1), 8(1), 11(1), 12(1) or (2) or 13(1), and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(3) Any person who contravenes the provisions of subsection (1) or (2), is liable, on conviction to a fine not exceeding R 5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(4) For purposes of this section **"passwords, access codes or similar data and devices"** means without limitation—

(*a*) a secret code or pin;

(*b*) an image;

(*c*) a security token;

(*d*) an access card or device;

(*e*) a biometric image;

(*f*) a word or a string of characters or numbers; or

(*g*) a password,

used for electronic transactions or user authentication in order to access data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure or any other device or information.

Computer related fraud

11. (1) Any person who unlawfully and intentionally, by means of data or a data message, makes a misrepresentation which—

(*a*) causes actual prejudice; or

(*b*) which is potentially prejudicial,

to another person is guilty of the offence of computer related fraud.

(2) (*a*) A court which convicts a person of an offence in terms of this section, may impose any 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.

(*b*) A court which imposes any sentence in terms of this section must, without excluding other relevant factors, consider as aggravating factors—

(i) the fact that the offence was committed by electronic means;

(ii) the extent of the prejudice and loss suffered by the complainant as a result of the commission of such an offence; and

(iii) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence.

Computer related forgery and uttering

12. (1) Any person who unlawfully and intentionally makes a false data document to the actual or potential prejudice of another person is guilty of the offence of computer related forgery.

(2) Any person who unlawfully and intentionally passes off a false data document to the actual or potential prejudice of another person is guilty of the offence of computer related uttering.

(3) (*a*) A court which convicts a person of an offence in terms of this section, may impose any 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.

(*b*) A court which imposes any sentence in terms of this section must, without excluding other relevant factors, consider as aggravating factors—

(i) the fact that the offence was committed by electronic means;

(ii) the extent of the prejudice and loss suffered by the complainant as a result of the commission of such an offence; and

(iii) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence.

(4) For purposes of this section "**data document**" means a data message containing the depiction of a document which portrays information.

Computer related appropriation

13. (1) Any person who unlawfully and intentionally appropriates, in any manner—

(*a*) ownership in property, which ownership is vested in another person with the intention to—

(i) permanently; or

(ii) temporarily,

deprive the other person of the ownership in the property to the actual or potential prejudice of the owner of the property; or

(*b*) any other right in property, which right is vested in another person, with the intention to—

(i) permanently; or

(ii) temporarily,

deprive the other person of the right in the property to the actual or potential prejudice of the person in whom the right is vested,

is guilty of the offence of computer related appropriation.

(2) (*a*) A court which convicts a person of an offence in terms of subsection (1), may impose any 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.

(*b*) A court which imposes any sentence in terms of this section must, without excluding other relevant factors, consider as aggravating factors—

(i) the fact that the offence was committed by electronic means;

(ii) the extent of the prejudice and loss suffered by the complainant as a result of the commission of such an offence; and

(iii) the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence.

(3) For purposes of this section—

(*a*) "**property**" means—

(i) money;

(ii) credit; or

(iii) any other movable, immovable, corporeal or incorporeal thing which has a commercial value but excludes any registered patents as defined in the Patents Act, 1978 (Act No. 57 of 1978), any copyright works as defined in the Copyright Act, 1978 (Act No. 98 of 1978), or plant breeders" rights or designs as defined in the Designs Act, 1995 (Act No. 195 of 1993), or trademarks as defined in the Trademark Act, 1993 (Act 194 of 1993); and

(*b*) "**right in property**" means any right, privilege, claim or security in property and any interest therein and all proceeds thereof, and includes any of the foregoing involving any registered patents as defined in the Patents Act, 1978 (Act No. 57 of 1978), any copyright works as defined in the Copyright Act, 1978 (Act No. 98 of 1978), or plant breeders" rights or designs as defined in the Designs Act, 1995 (Act No. 195 of 1993), or trademarks as defined in the Trademark Act, 1993 (Act 194 of 1993).

Computer related extortion

14. (1) Any person who unlawfully and intentionally—

(*a*) threatens to commit any offence under this Act; or

(*b*) commits any offence under this Act,

for the purposes of obtaining any advantage from another person, is guilty of the offence of computer related extortion.

(2) A person who contravenes the provisions of subsection (1) is liable on conviction to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

Computer related terrorist activity and related offences

15. (1) Any person who unlawfully and intentionally engages in a computer related terrorist activity is guilty of an offence.

(2) Any person who unlawfully and intentionally does anything which will, or is likely to, enhance the ability of any person, entity or organisation to engage in a computer related terrorist activity, including—

(*a*) the provision of, or offering to provide, a skill or expertise;

(*b*) entering into any country or remaining therein; or

(*c*) making himself or herself available,

for the benefit of, at the direction of, or in association with any person, entity or organisation engaging in a computer related terrorist activity, and who knows or ought reasonably to have known or suspected, that such act was done for the purpose of enhancing the ability of such person, entity or organisation to engage in a computer related terrorist activity, is guilty of the offence of association with a computer related terrorist activity.

(3) Any person, entity or organisation who unlawfully and intentionally—

(*a*) provides or offers to provide data, any software or hardware tool as contemplated in section 6(5), malware as contemplated in section 9(4), a password, access code or similar data or device as contemplated in section 10(4), a computer device, a computer network, a database, an electronic communications network or any other device or equipment or any part thereof, to any other person for use by or for the benefit of a person, entity or organisation;

(*b*) solicits support for or gives support to a person, entity or organisation;

(*c*) provides, receives or participates in training or instruction, or recruits a person, entity or an organisation to receive training or instruction;

(*d*) recruits any person, entity or organisation; or

(*e*) possesses, receives or makes available data, any software or hardware tool as contemplated in section 6(5), malware as contemplated in section 9(4), a password, access code or similar data and device as contemplated in section 10(4) or a computer device, computer network, a database, an electronic communications network or any other device or equipment or any part thereof,

connected with the engagement in a computer related terrorist activity, and who knows or ought reasonably to have known or suspected that the actions referred to in paragraphs (*a*) to (*e*), are so connected, is guilty of the offence of facilitating a computer-related terrorist activity.

(4) Any person who contravenes the provisions of subsections (1), (2) or (3)) is liable on conviction to imprisonment for a period not exceeding 25 years.

(5) For purposes of this section "**computer related terrorist activity"** means any prohibited act contemplated in section 7(1), 8(1), 9(1) (in so far as it relates to the use of malware) or 14(1) —

(*a*) which—

(i) endangers the life, or violates the physical integrity or physical freedom of, or causes serious bodily injury to or the death of, any person, or any number of persons;

(ii) causes serious risk to the health or safety of the public or any segment of the public;

(iii) causes the destruction of or substantial damage to critical data, a critical database, an electronic communications network or a National Critical Information Infrastructure, whether public or private;

(iv) is designed or calculated to cause serious interference with or serious disruption of an essential service, critical data, a critical database, an

electronic communications network or a National Critical Information Infrastructure;

(v) causes any major economic loss or extensive destabilisation of an economic system or substantial devastation of the national economy of a country; or

(vi) creates a serious public emergency situation or a general insurrection in the Republic,

irrespective whether the harm contemplated in paragraphs (*a*) (i) to (vi) is or may be suffered in or outside the Republic; and

(*b*) which is intended, or by its nature and context, can reasonably be regarded as being intended, in whole or in part, directly or indirectly, to—

(i) threaten the unity and territorial integrity of the Republic;

(ii) intimidate, or to induce or cause feelings of insecurity among members of the public, or a segment of the public, with regard to its security, including its economic security, or to induce, cause or spread feelings of terror, fear or panic in a civilian population; or

(iii) unduly compel, intimidate, force, coerce, induce or cause a person, a government, the general public or a segment of the public, or a domestic or an international organisation or body or intergovernmental organisation or body, to do or to abstain or refrain from doing any act, or to adopt or abandon a particular standpoint, or to act in accordance with certain principles,

whether the public or the person, government, body, or organisation or institution referred to in subparagraphs (ii) or (iii), as the case may be, is inside or outside the Republic.

Computer related espionage and unlawful access to restricted data

16. (1) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to—

(i) gain access, as contemplated in section 4(3), to critical data, a critical database or a National Critical Information Infrastructure; or

(ii) intercept data, as contemplated in section 5(3), to, from or within a critical database or a National Critical Information Infrastructure,

with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data contemplated in subsection (1)(*a*)(ii) or critical data with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(2) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to, or intercept data, as contemplated in section 5(3), which is in the possession of the State and which is classified as confidential, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as confidential, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(3) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to or intercept data, as contemplated in section 5(3), which is in the possession of the State and which is classified as secret, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as secret, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(4) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to or intercept data, as contemplated in section 5(3), which is in the possession of the State and which is classified as top secret, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as top secret, with the intention of directly or indirectly benefiting a foreign state or any person engaged in a terrorist activity against the Republic, is guilty of an offence.

(5) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to, or intercept data, as contemplated in section 5(3), which is in the possession of the State and which is classified as confidential, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as confidential, is guilty of an offence.

(6) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access, as contemplated in section 4(3), to or intercept data which is in the possession of the State and which is classified as secret, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as secret, is guilty of an offence.

(7) (*a*) Any person who unlawfully and intentionally performs or authorises, procures or allows another person to perform a prohibited act contemplated in section 3(1) or (3), in sofar as it relates to the use of personal information, 4(1), 5(1), 6(1) or (2), 7(1), 8(1), 9(1) or 10(1), in order to gain access to or intercept data which is in the possession of the State and which is classified as top secret, is guilty of an offence.

(*b*) Any person who unlawfully and intentionally—

(i) possesses;

(ii) communicates, delivers or makes available; or

(iii) receives,

data which is in the possession of the State and which is classified as top secret, is guilty of an offence.

(8) Any person who contravenes the provisions of —

(*a*) subsection (1) is liable on conviction to imprisonment for a period not exceeding 20 years;

(*b*) subsection (2) is liable on conviction to imprisonment for a period not exceeding 10 years;

(*c*) subsection (3), is liable on conviction to imprisonment for a period not exceeding 15 years;

(*d*) subsection (4) is liable on conviction to imprisonment for a period not exceeding 25 years;

(*e*) subsection (5) is liable on conviction to imprisonment for a period not exceeding 5 years;

(*f*) subsection (6) is liable on conviction to imprisonment for a period not exceeding 10 years; or

(*g*) subsection (7) is liable on conviction to imprisonment for a period not exceeding 15 years.

(8) For purposes of this section "**terrorist activity**" means—

(*a*) a computer related terrorist activity referred to in section 15 of this Act; or

(*b*) any offence referred to in the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act 33 of 2004).

Prohibition on dissemination of data message which advocates, promotes or incites hate, discrimination or violence

17. (1) Any person who unlawfully and intentionally—

(*a*) makes available, broadcasts or distributes;

(*b*) causes to be made available, broadcast or distributed; or

(*c*) assists in making available, broadcasts or distributes,

through a computer network or an electronic communications network, to a specific person or the general public, a data message which advocates, promotes or incites hate, discrimination or violence against a person or a group of persons, is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction to a fine or imprisonment not exceeding 2 years.

(3) For purposes of this section "**data message which advocates, promotes or incites hate, discrimination or violence**" means any data message representing ideas or theories, which advocate, promote or incite hatred, discrimination or violence, against a person or a group of persons, based on—

(*a*) national or social origin;

(*b*) race;

(*c*) colour;

(*d*) ethnicity;

(*e*) religious beliefs;

(*f*) gender;

(*g*) gender identity;

(*h*) sexual orientation;

(*i*) caste; or

(*j*) mental or physical disability.

Prohibition on incitement of violence and damage to property

18. (1) Any person who unlawfully and intentionally—

(*a*) makes available, broadcasts or distributes;

(*b*) causes to be made available, broadcast or distributed;

(*c*) assists in making available, broadcasts or distributes,

to a specific person or the general public, through a computer network or an electronic communications network, a data message which is reasonably likely to incite—

(i) violence against; or

(ii) damage to the property belonging to,

a person or a group of persons, is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction to a fine or imprisonment not exceeding 2 years or to both such fine and imprisonment.

Prohibited financial transactions

19. (1) Any person who unlawfully and intentionally participates in, processes or facilitates a financial transaction through a computer network or an electronic communications network—

(*a*) in order to promote an unlawful activity; or

(*b*) which involves the proceeds of any unlawful activity,

is guilty of the offence of committing a prohibited financial transaction.

(2) Any person who contravenes the provisions of subsection (1) is liable, on conviction to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(3) For purposes of this section "**unlawful activity**" means any conduct which contravenes any law of the Republic.

Infringement of copyright

20. (1) Any person who unlawfully and intentionally, at a time when copyright exists in respect of any work, without the authority of the owner of the copyright, by means of a computer network or an electronic communications network—

(*a*) sells;

(*b*) offers for download;

(*c*) distributes; or

(*d*) otherwise makes available,

any work, which the person knows is subject to copyright and that the actions contemplated in paragraphs (*a*), (*b*), (*c*) or (*d*) will be prejudicial to the owner of the copyright, is guilty of an offence.

(2) Any person who contravenes the provisions of subsection (1), is liable on conviction to a fine or imprisonment not exceeding three years or to both such fine and imprisonment.

(3) For purposes of this section "**work**" means any—

(*a*) literary work;

(*b*) musical work;

(*c*) artistic work;

(*d*) cinematograph film;

(*e*) sound recording;

(*f*) broadcast;

(*g*) programme-carrying signal;

(*h*) published edition; or

(*i*) computer program,

which is eligible for copyright in terms of section 2 of the Copyrights Act, 1978 (Act No. 98 of 1978), or similar legislation of any State designated by the Minister by notice in the *Gazette*.

Harbouring or concealing person who commits offence

21. (1) Any person who unlawfully and intentionally harbours or conceals a person whom he or she knows, or has reasonable grounds to believe or suspect, has committed, or is about to commit, an offence contemplated in—

(*a*) section 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 17, 18, 19 or 20; or

(*b*) any offence contemplated in section 15 or 16,

is guilty of an offence.

(2) Any person who contravenes the provisions of—

(*a*) subsection (1)(*a*), is liable, on conviction to a fine or imprisonment not exceeding two years or to both such fine and imprisonment; and

(*b*) subsection (1)(*b*), is liable, on conviction to imprisonment for a period of 10 years.

Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring to commit offence

22. Any person who unlawfully and intentionally—

(*a*) attempts;

(*b*) conspires with any other person; or

(*c*) aids, abets, induces, incites, instigates, instructs, commands, or procures another person,

to commit an offence in terms of this Chapter, is guilty of an offence and is liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable.

Aggravating circumstances

23. (1) If a person is convicted of any offence in terms of this Chapter, a court which imposes any sentence in terms of this Chapter must, without excluding other relevant factors, consider as an aggravating factor the fact that the offence was committed in concert with one or more persons.

(2) If a person is convicted of any offence provided for in section 3, 4, 5, 7, 8 or 10, a court which imposes any sentence in terms of those sections must, without excluding other relevant factors, consider as an aggravating factor the fact that the offence was committed by a person, or with the collusion or assistance of that person, who as part of his or her duties, functions or lawful authority—

(*a*) is responsible for the processing of personal information or financial information, which personal information or financial information was involved in any offence provided for in section 3;

(*b*) is in charge of, in control of, or has access to data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure or any part thereof which was involved in any offence provided for in section 4, 5, 7 and 8; or

(*c*) is the holder of a password, access code or similar data or device which was used to commit any offence provided for in section 10.

(3) If a person contemplated in subsection (2) is convicted of the offence in question, a court must, unless substantial and compelling circumstances exist which justify the imposition of another sentence as prescribed in paragraphs (*a*) or (*b*) of this subsection, impose, with or without a fine, in the case of—

(*a*) a first contravention of section 3, 4, 5, 7, 8 or 10, a period of direct imprisonment of no less than half of the period of imprisonment prescribed by the section which is contravened; and

(*b*) any second or subsequent contravention of section 3, 4, 5, 7, 8 or 10, the maximum period of imprisonment prescribed by the section which is contravened.

Savings

24. The provisions of this Chapter do not affect criminal liability in terms of the common law or any other legislation.

CHAPTER 3

JURISDICTION

Jurisdiction

25. (1) A court in the Republic trying an offence in terms of this Act has jurisdiction where—

(*a*) the offence was committed in the Republic;

(*b*) any act or omission 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;

(*c*) 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; or

(*d*) 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.

(2) If the act or omission alleged to constitute an offence under this Act occurred outside the Republic, a court of the Republic, regardless of whether or not the

act or omission constitutes an offence at the place of its commission, has jurisdiction in respect of that offence if the person to be charged—

(*a*) is a citizen of the Republic;

(*b*) is ordinarily resident in the Republic;

(*c*) 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;

(*d*) is a company, incorporated or registered as such under any law, in the Republic; or

(*e*) any body of persons, corporate or unincorporated, in the Republic.

(3) Any act or omission alleged to constitute an offence under this Act and which is committed outside the Republic by a person, other than a person contemplated in subsection (2), is, regardless of whether or not the act or omission constitutes an offence or not at the place of its commission, deemed to have also been committed in the Republic if that—

(*a*) act or omission affects or is intended to affect a public body, a business or any other person in the Republic;

(*b*) person is found to be in South Africa; and

(*c*) person is for one or other reason not extradited by South Africa or if there is no application to extradite that person.

(4) 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 or, in case of an omission, should have acted.

CHAPTER 4

POWERS TO INVESTIGATE, SEARCH AND ACCESS OR SEIZE AND INTERNATIONAL COOPERATION

Definitions and interpretation

26. For purposes of this Chapter, unless the context indicates otherwise—

"**access**" means to make use of, to gain entry to, to view, display, to retrieve, to copy data, or otherwise make use of a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or their accessories or components or any part thereof;

"**article**" means any data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or any part thereof or any other information, instrument, device or equipment which—

(*a*) is concerned in, connected with or is, on reasonable grounds, believed to be concerned in or connected with the commission or suspected commission;

(*b*) may afford evidence of the commission or suspected commission; or

(*c*) 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 this Act or any other offence which may be committed by means of or facilitated through, the use of an article, whether within the Republic or elsewhere;

"**investigator**" means an appropriately qualified, fit and proper person, who is not a member of a law enforcement agency, and who is appointed by the National Commissioner or the Director-General: State Security, on the strength of his or her expertise in order to, subject to the control and directions of a member of a law enforcement agency, assist a law enforcement agency in an investigation in terms of this Act;

"**designated judge**" means a designated judge as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002);

"law enforcement agency" means—

(*a*) the South African Police Service referred to in section 5 of the South African Police Service Act, 1995 (Act No. 68 of 1995); and

(b) the State Security Agency referred to in section 3(1) of the Intelligence Services Act, 2002 (Act No. 65 of 2002);

"magistrate" includes a regional court magistrate;

"**public available data**" means data which is accessible in the public domain without restriction; and

"specifically designated member of a law enforcement agency" means—

(*a*) a commissioned officer referred to in section 33 of the South African Police Service Act, 1995 (Act No. 68 of 1995), who has been designated in writing by the National Commissioner; or

(*b*) a member as defined in section 1 of the Intelligence Services Act, 2002 (Act No. 65 of 2002), who has has been designated in writing by the Director-General: State Security;

to—

(i) make oral applications for a search warrant or an amendment of a warrant contemplated in section 30;

(ii) issue expedited preservation of data directions contemplated in section 40; or

(iii) serve a disclosure of data direction from the designated judge on a person or electronic communications service provider contemplated in section 41(7).

Application of provisions in this Chapter

27. The provisions of this Chapter apply in addition to—

(*a*) Chapter 2 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), or any other applicable law which regulates the search and accessing or seizure of articles connected with offences; and

(*b*) Chapter 2 of the International Co-operation in Criminal Matters Act, 1996 (Act No. 75 of 1996), which regulates the mutual provision of evidence in criminal matters.

Search for and access to or seizure of, certain articles

28. Any member of a law enforcement agency or an investigator accompanied by a member of a law enforcement agency may, in accordance with the provisions of this Chapter, access or seize any article, whether within the Republic or elsewhere.

Article to be accessed or seized under search warrant

29. (1) Subject to the provisions of sections 31, an article referred to in section 28 can only be accessed or seized by virtue of a search warrant issued—

(*a*) by a magistrate or judge of the High Court, on written application by a member of a law enforcement agency, if it appears to the magistrate or judge, from information on oath or by way of affirmation that there are reasonable grounds for believing that an article is—

(i) within his or her area of jurisdiction; or

(ii) being used or is involved in the commission of an offence—

(*aa*) within his or her area of jurisdiction; or

(*bb*) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved in the commission of an offence; or

(*b*) by a magistrate or judge presiding at criminal proceedings, if it appears to such magistrate or judge that an article is required in evidence at such proceedings.

(2) A search warrant issued under subsection (1) must require a member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency to access or seize the article in question and, to that end, must authorize the member of a law enforcement agency or an investigator who is accompanied by a member of the law enforcement agency to—

(*a*) search any person identified in the warrant;

(*b*) enter and search any container, premises, vehicle, facility, ship or aircraft identified in the warrant;

(*c*) search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who is found near such container, on or at such premises, vehicle, facility, ship or aircraft;

(*d*) search any person who is believed, on reasonable grounds, to be able to furnish any information of material importance concerning the matter under investigation and who—

(i) is nearby;

(ii) uses; or

(ii) is in possession of or in direct control of,

any data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;

(*e*) access and search any data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;

(*f*) obtain and use any instrument, device, equipment, password, decryption key, data or other information that is believed, on reasonable grounds, to be necessary to access or use any part of any data, computer device, computer network, database, critical database, electronic communications network or

National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;

(*g*) copy any data or other information to the extent as is set out in the warrant; or

(*h*) seize an article identified in the warrant to the extent as is set out in the warrant.

(3) For purposes of subsection (2), whenever a search warrant issued under subsection (1), authorises an investigator who is accompanied by a member of the law enforcement agency to search any person, the search of such a person must, subject to section 35(2), be carried out by a member of the law enforcement agency accompanying the investigator.

(4) (*a*) A search warrant may be executed at any time, unless the person issuing the warrant in writing specifies otherwise.

(*b*) A search warrant may be issued on any day and is of force until it is executed or is cancelled by the person who issued it or, if such person is not available, by a person with like authority.

(5) A member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency who executes a warrant under this section must, upon demand by any person whose rights in respect of any search or article accessed or seized under the warrant have been affected, hand to him or her a copy of the warrant.

Oral application for search warrant or amendment of warrant

30. (1) An application referred to in section 29(1)(*a*), or an application for the amendment of a warrant issued in terms of section 29(1)(*a*), may be made orally by a specifically designated member of a law enforcement agency, if it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

(2) An oral application referred to in subsection (1) must—

(*a*) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the member of the law enforcement agency, justify the making of an oral application; and

(*b*) comply with any supplementary directives relating to oral applications issued by the Judges President of the respective Divisions of the High Court.

(3) A magistrate or judge of the High Court may, upon an oral application made to him or her in terms of subsection (1) and subject to subsection (4), issue a warrant.

(4) A warrant may only be issued under subsection (3)—

(*a*) if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that—

(i) there are reasonable grounds to believe that a warrant applied for could be issued;

(ii) a warrant is necessary immediately in order to access or seize or search for an article within his or her area of jurisdiction or an article which is being used or is involved in the commission of an offence—

(*aa*) within his or her area of jurisdiction; or

(*bb*) within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved in the commission of an offence; and

(iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of a warrant; and

(*b*) on condition that the member of the law enforcement agency concerned must submit a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the warrant under subsection (3).

(5) A warrant issued under subsection (3) must be in writing and must be transmitted electronically to the member of the law enforcement agency.

(6) A magistrate or judge of the High Court who has issued a warrant under subsection (3) or, if he or she is not available, any other magistrate or judge of the High Court must, upon receipt of a written application submitted to him or her in terms of subsection (4)(*b*), reconsider that application whereupon he or she may confirm, amend or cancel that warrant.

Search and access or seizure without search warrant

31. Any member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency may, without a search warrant, execute the powers referred to in section 29(2) of this Act, subject to any other law if the person who has the lawful authority to consent to the—

(*a*) search for and access to or seizure of the article in question; or

(*b*) search of a container, premises, vehicle, facility, ship, aircraft, data, computer device, computer network, database, critical database, electronic communications network or a National Critical Information Infrastructure,

consents, in writing, to such search and access to or seizure of the article in question.

Search and seizure for and access to article on arrest of person

32. (1) On the arrest of any person on suspicion that he or she has committed—

(*a*) an offence under this Act; or

(*b*) any other offence,

a member of a law enforcement agency may search the arrested person and seize any article referred to in section 28 which is in the possession of, in the custody of or under the direct control of, the arrested person.

(2) A member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency may access and search any article referred to in subsection (1).

Assisting member of law enforcement agency or investigator

33. (1) An electronic communications service provider or person, other than the person who is suspected of having committed an offence under this Act, who is in control of any container, premises, vehicle, facility, ship, aircraft, data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure or any other information, instrument, device or equipment that is subject to a search authorised in terms of section 29(1) or 30(3) or which takes place in terms of section 31 must, if required, provide—

(*a*) technical assistance; and

(*b*) such other assistance as may be necessary,

to the member of the law enforcement agency or investigator who is accompanied by a member of a law enforcement agency in order to—

(i) access or use any data, computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure or any other information, instrument, device or equipment;

(ii) copy data or other information;

(iii) obtain an intelligible output of data; or

(iv) remove a computer device, any part of a computer network, database, critical database, electronic communications network or National Critical Information Infrastructure.

(2) An electronic communications service provider or person who fails to comply with the provisions of subsection (1) is guilty of an offence and is liable on

conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Obstructing or hindering member of law enforcement agency or investigator who is accompanied by member of law enforcement agency and authority to overcome resistance

34. (1) Any person who obstructs or hinders a member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency in the exercise of his or her powers or the performance of his or her duties or functions in terms of this Chapter or who refuses or fails to comply with a search warrant issued in terms of section 29(1), section 30(3) or which takes place in terms of section 31, is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

(2) (*a*) A member of a law enforcement agency or a member of a law enforcement agency who accompanies an investigator who may lawfully execute any power conferred upon him or her in terms of section 29(2) of this Act, may use such force as may be reasonably necessary, proportional to all the circumstances relating to the execution of such powers.

(*b*) No member of a law enforcement agency may enter upon or search any premises, vehicle, facility, ship or aircraft unless he or she has audibly demanded admission to the premises, vehicle, facility, ship or aircraft and has notified the purpose of his or her entry.

(*c*) The provisions of paragraph (*b*) do not apply where the member of a law enforcement agency is, on reasonable grounds, of the opinion that an article which is the subject of the search may be destroyed, disposed of or tampered with if the provisions of paragraph (*b*) are complied with.

Powers conferred upon member of law enforcement agency or investigator who is accompanied by member of law enforcement agency to be conducted in decent and orderly manner with due regard to rights of other persons

35. (1) The powers conferred upon member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency in terms of section 29(2) of this Act, must be conducted —

(*a*) with strict regard to decency and order; and

(*b*) with due regard to the the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.

(2) If a female needs to be searched physically in terms of section 29(2)(*a*), (*c*) or (*d*) or section 32 of this Act, such search must be carried out by a member of a law enforcement agency who is also a female: Provided that if no female member of a law enforcement agency is available, the search must be carried out by any female designated for that purpose by a member of a law enforcement agency.

Wrongful search and access or seizure and restriction on use of instrument, device, password or decryption key or information to gain access

36. (1) A member of a law enforcement agency or an investigator—

(*a*) who acts contrary to the authority of a search warrant issued under section 29(1) or section 30(3); or

(*b*) who, without being authorized thereto under this Chapter or the provision of any other law which affords similar powers to a member of a law enforcement agency or investigator—

(i) accesses, searches, copies or seizes data, a computer device, any part of a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or any other information, instrument, device or equipment; or

(ii) obtains any instrument, device, password, decryption key or other information that is necessary to access or uses data, a computer device, any part of a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure,

is guilty of an offence and is liable on conviction to a fine not exceeding R300 000 or imprisonment for a period not exceeding 3 years or to both such fine and imprisonment.

(2) A member of a law enforcement agency or an investigator who obtains or uses any instrument, device, equipment, password, decryption key, data or other information contemplated in section 29(2)(*f*)—

(*a*) must use the instrument, device, equipment, password, decryption key, data or information only in respect of and to the extent specified in the warrant to gain access to or use data, a program, a computer data storage medium, a computer device, any part of a computer network, a database, any part of an electronic communications network or any part of an electronic communications infrastructure in the manner and for the purposes, specified in the search warrant concerned; and

(*b*) must destroy all information if—

(i) it will not be required for purposes of any criminal or civil proceedings contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act or for purposes of evidence or for purposes of an order of court; or

(ii) no criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, are to be instituted in connection with such information.

(3) The provisions of subsection (2) apply with the necessary changes required by the context to a search and access or seizure without a search warrant contemplated in section 31 or access to and search of an article contemplated in section 32(2).

(4) A member of a law enforcement agency or an investigator who fails to comply with subsections (2) or (3), is guilty of an offence and is liable on conviction to a fine not exceeding R300 000 or imprisonment for a period not exceeding 3 years or to both such fine and imprisonment.

(5) Where a member of a law enforcement agency or an investigator is convicted of an offence referred to in subsection (1) or (4), the court convicting such a person, may upon application of any person who has suffered damage, or upon the application of the prosecutor acting on the instructions of that person, award compensation in respect of such damage, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), apply with the necessary changes, with reference to such award.

False information under oath or by way of affirmation

37. (1) Any person who gives false information under oath or by way of affirmation knowing it to be false or not knowing it to be true, with the result that a search warrant is issued, or is issued and executed, or a search contemplated in section 31 took place on the basis of such information, is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(2) Where a person is convicted of an offence referred to in subsection (1), the court convicting such a person, may upon application of any person who has suffered damage, or upon the application of the prosecutor acting on the instructions of that person, award compensation in respect of such damage, whereupon the provisions of section 300 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), apply with the necessary changes, with reference to such award.

Prohibition on disclosure of information

38. (1) No person, investigator, member of a law enforcement agency, electronic communications service provider or an employee of an electronic communications service provider may disclose any information which he, she or it has obtained in the exercise of his, her or its powers or the performance of his, her or its duties in terms of this Act, except—

(*a*) to any other person who of necessity requires it for the performance of his or her functions in terms of this Act;

(*b*) if he or she is a person who of necessity supplies such information in the performance of his or her functions in terms of this Act;

(*c*) if it is information which is required in terms of any law or as evidence in any court of law;

(*d*) if it constitutes information-sharing—

(i) contemplated in Chapter 6 of this Act; or

(ii) between electronic communications service providers, the South African Police Service or any other person or entity which is aimed at preventing, investigating or mitigating cybercrime or relating to aspects of cyber security:

Provided that such information-sharing may not prejudice any criminal investigation or criminal proceedings;

(*e*) to any competent authority which requires it for the institution of criminal proceedings or an investigation with a view to instituting criminal proceedings.

(2) A person, investigator, member of a law enforcement agency, electronic communications service provider or an employee of an electronic communications service provider who contravenes the provisions of subsection (1) is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Interception of data

39. (1) The interception of data which is an indirect communication as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), must take place in terms of an interception direction issued in terms of section 16 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), and must, subject to subsection (3), be dealt with further in the manner provided for in that Act.

(2) If no interception direction has been issued, the interception of data on an ongoing basis, which is real-time communication-related information as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), must take place in terms of a real-time communication-related direction issued in terms of section 17 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002), and must, subject to subsection (3), be dealt with further in the manner provided for in that Act.

(3) Data referred to in subsection (1) or (2), which is intercepted at the request of an authority, court or tribunal exercising jurisdiction in a foreign State must, after the interception, be dealt with in the manner provided in an order referred to in section 46(6), which is issued by the designated judge.

Expedited preservation of data direction

40. (1) A specifically designated member of a law enforcement agency may, if he or she on reasonable grounds believes that any person or an electronic communications service provider, which is not required to provide an electronic communications service which has the capability to be intercepted or to store communication-related information, as contemplated in section 30 of the Regulation of Interception of Communications and Provision of Communication-related Information

Act, 2002 (Act No. 70 of 2002), may receive, is in possession of, or is in control of data—

(*a*) which is relevant to;

(*b*) which was used or may be used in;

(*c*) for the purposes of or in connection with;

(*d*) which has facilitated or may facilitate; or

(*e*) which may afford evidence of,

the commission or intended commission of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by, the use of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) 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,

issue an expedited preservation of data direction to such a person or electronic communications service provider.

(2) An expedited preservation of data direction must be in the prescribed form and must be served on the person or electronic communications service provider affected thereby, in the prescribed manner by a member of a law enforcement agency.

(3) An expedited preservation of data direction must direct the person or electronic communications service provider affected thereby, from the time of service of the direction, and for a period of 120 days—

(*a*) to preserve the current status of;

(*b*) not to deal in any manner with; or

(*c*) to deal in a certain manner with,

the data referred to in the direction in order to preserve the availability and integrity of the data.

(4) No data may be disclosed to a law enforcement agency on the strength of an expedited preservation of data direction unless it is authorised in terms of section 41.

(5) The 120 day period referred to in subsection (3), may only be extended by way of a preservation of evidence direction contemplated in section 42 of this Act.

(6) A person or electronic communications service provider to whom an expedited preservation of data direction referred to in subsection (1) is addressed, may, in writing, apply to a magistrate in whose area of jurisdiction the person or electronic communications service provider is situated, 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.

(7) The magistrate to whom an application is made in terms of subsection (6) must, as soon as possible after receipt thereof—

(*a*) consider the application and may for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(*b*) give a decision in respect of the application; and

(*c*) inform the applicant and member of the law enforcement agency referred to in subsection (1) of the outcome of the application.

(8) A person or an electronic communications service provider referred to in subsection (1) who—

(*a*) fails to comply with an expedited preservation of data direction or contravenes the provisions of subsection (4); or

(*b*) makes a false statement in an application referred to in subsection (6),

is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Disclosure of data direction

41. (1) Subject to sections 15(2), 16 and 17 of the Regulation of Interception of Communications and Provision of Communication-related information Act, 2002 (Act No. 70 of 2002), and subsection (4), a magistrate or judge of the High Court, may on written application by a member of a law enforcement agency, if it appears to the magistrate or judge, from information on oath or by way of affirmation that there are reasonable grounds for believing that a person or electronic communications service provider may receive, is in possession of, or is in control of data which is relevant to or which may afford evidence of, the commission or intended commission of—

(*a*) an offence under Chapter 2 of this Act; or

(*b*) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article,

issue a disclosure of data direction.

(2) An application contemplated in subsection (1) must—

(*a*) contain the identity of the member of the law enforcement agency who applies for the disclosure of data direction;

(*b*) identify the customer, if known, or the service or communication in respect of whom data is to be provided;

(*c*) identify the person or electronic communications service provider to whom the disclosure of data direction must be addressed;

(*d*) contain a description of the data which must be provided;

(*e*) contain a description of the offence which has been or is being or will probably be committed; and

(*f*) comply with any supplementary directives relating to applications for expedited disclosure of data issued by the Judges President of the respective Divisions of the High Court.

(3) Upon receipt of an application in terms of subsection (1), a magistrate or judge, must satisfy himself or herself—

(*a*) that there are reasonable grounds for believing that—

(i) an offence in terms of Chapter 2 of this Act; or

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article,

has been, is being or will probably be committed or that it is necessary to determine whether such an offence has been so committed; and

(*b*) that it will be in the interests of justice if a disclosure of data direction is issued.

(4) (*a*) The designated judge, may on request of an authority, court or tribunal of a foreign State, if it appears to the designated judge, from information on oath or by way of affirmation that there are reasonable grounds for believing that any person or electronic communications service provider in the Republic may receive, is in possession of, or is in control of data which is relevant to, or which may afford evidence of, the commission or intended commission of an offence—

(i) similar to those contemplated in Chapter 2 of this Act; or

(ii) 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, issue, subject to paragraph (*b*), a disclosure of data direction.

(*b*) The designated judge must, before a disclosure of data direction as contemplated in paragraph (*a*) is issued, inform the Cabinet member responsible for the administration of justice, in writing of the—

(i) fact that he or she intends to issue a disclosure of data direction; and

(ii) reasons for such decision.

(5) A request contemplated in subsection (4) must—

(*a*) identify the customer, if known, or the service or communication in respect of whom data is to be provided;

(*b*) identify the person or electronic communications service provider to whom the disclosure of data direction must be addressed;

(*c*) contain a description of the data which must be provided;

(*d*) contain a description of the offence which has been or is being or will probably be committed; and

(*e*) comply with any supplementary directives relating to applications for disclosure of data issued by the designated judge.

(6) Upon receipt of a request in terms of subsections (4), the designated judge must satisfy himself or herself—

(*a*) that there are reasonable grounds for believing that an offence—

(i) similar to those contemplated in Chapter 2 of this Act; or

(ii) 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 the requesting foreign State, has been committed or that it is necessary to determine whether such an offence has been so committed and that an investigation in respect thereof is being conducted in the requesting foreign State;

(*b*) that the request, where applicable, is in accordance with—

(i) any treaty, convention or other international agreement to which that foreign state and the Republic are parties; or

(ii) any agreement with any foreign State entered into in terms of section 65 of this Act; and

(*c*) that it will be in the interests of justice if a disclosure of data direction is issued.

(7) A disclosure of data direction must be in the prescribed form and must be served on the person or electronic communications service provider affected thereby, in the prescribed manner by a member of a law enforcement agency or in the case of subsection (4), a specifically designated member of a law enforcement agency.

(8) The disclosure of data direction—

(*a*) must direct the person or electronic communications service provider to provide data identified in the direction to the extent as is set out in the direction to an identified member of the law enforcement agency;

(*b*) must set out the period within which the data identified in paragraph (*a*) must be provided; and

(*c*) may specify conditions or restrictions relating to the provision of data authorised therein.

(9) A person or electronic communications service provider to whom a disclosure of data direction referred to in subsection (7) is addressed, may in writing apply to the magistrate or judge or the designated judge 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.

(10) The magistrate or judge or the designated judge to whom an application is made in terms of subsection (9) must, as soon as possible after receipt thereof—

(*a*) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(*b*) give a decision in respect of the application; and

(*c*) if the application is successful, inform the law enforcement agency or authority, court or tribunal of a foreign State, of the outcome of the application.

(11) A person or an electronic communications service provider who—

(*a*) fails to comply with a disclosure of data direction; or

(*b*) makes a false statement in an application referred to in subsection (9),

is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Preservation of evidence direction

42. (1) A magistrate or judge of the High Court, may on written application by a member of a law enforcement agency, if it appears to the magistrate or judge, from information on oath or by way of affirmation that there are reasonable grounds for

believing that any person or electronic communications service provider may receive, is in possession of, or is in control of an article—

(*a*) relevant to;

(*b*) which was used or may be used in;

(*c*) for the purpose of or in connection with;

(*d*) which has facilitated or may facilitate; or

(*e*) may afford evidence of,

the commission or intended commission of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) 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,

issue a preservation of evidence direction.

(2) A preservation of evidence direction must be in the prescribed form and must be served on the person or electronic communications service provider affected thereby, in the prescribed manner by a member of a law enforcement agency.

(3) The preservation of evidence direction must direct the person or electronic communications service provider, from the time of service of the direction, and for the time period specified in the direction, immediately—

(*a*) to preserve the current status of;

(*b*) not to deal in any manner with; or

(*c*) to deal in a certain manner with,

an article in order to preserve the integrity of the evidence.

(4) Any person or electronic communications service provider who fails to comply with a preservation of evidence direction is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(5) A person or electronic communications service provider to whom a preservation of evidence direction referred to in subsection (1) is addressed, may in writing apply to a magistrate or judge of the High Court in whose area of jurisdiction the person or electronic communications service provider is situated 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 order.

(6) The magistrate or judge of the High Court to whom an application is made in terms of subsection (5) must, as soon as possible after receipt thereof—

(*a*) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(*b*) give a decision in respect of the application; and

(*c*) inform the applicant and law enforcement agency of the outcome of the application.

Oral application for preservation of evidence direction

43. (1) An application referred to in section 42(1), may be made orally by a member of a law enforcement agency, if he or she is of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application.

(2) An oral application referred to in subsection (1) must—

(*a*) indicate the particulars of the urgency of the case or the other exceptional circumstances which, in the opinion of the member of the law enforcement agency, justify the making of an oral application; and

(*b*) comply with any supplementary directives relating to oral applications issued by the Judges President of the respective Divisions of the High Court.

(3) A magistrate or judge of the High Court may, upon an oral application made to him or her in terms of subsection (1), issue the preservation of evidence direction applied for.

(4) A preservation of evidence direction may only be issued under subsection (3) —

(a) if the magistrate or judge of the High Court concerned is satisfied, on the facts alleged in the oral application concerned, that—

(i) there are reasonable grounds to believe that a preservation of evidence direction applied for could be issued;

(ii) a preservation of evidence direction is necessary immediately in order to preserve the integrity of the evidence; and

(iii) it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuing of the preservation of evidence direction applied for; and

(*b*) on condition that the member of the law enforcement agency concerned must submit a written application to the magistrate or judge of the High Court concerned within 48 hours after the issuing of the preservation of evidence direction under subsection (3).

(5) A preservation of evidence direction issued under subsection (3) must be in writing and must be transmitted electronically to the member of the law enforcement agency.

(6) A magistrate or judge of the High Court who issued a direction under subsection (3) or, if he or she is not available, any other magistrate or judge of the High Court must, upon receipt of a written application submitted to him or her in terms of subsection (4)(*b*), reconsider that application whereupon he or she may confirm, amend or cancel that preservation of evidence direction.

Access to data and receipt and forwarding of unsolicited information

44. (1) Any member of a law enforcement agency or an investigator may, without being specifically authorised thereto in terms of this Chapter—

(*a*) access public available data regardless of where the data is located geographically;

(*b*) access 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—

(i) in writing, consents to such accessing of data; or

(ii) provides the data to a member of a law enforcement agency or an investigator; or

(c) access any data, regardless of where the data is located geographically, if such data is lawfully—

(i) accessible from; or

(ii) available to,

a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure which is being accessed or seized in terms of section 29, 30, 31 or 32.

(2) The head of a law enforcement agency may, after obtaining the written approval of the National Director of Public Prosecutions as contemplated in subsection (3), forward any information obtained during any investigation to a law enforcement agency of a foreign State when that head of a law enforcement agency is of the opinion that the disclosure of such information may—

(*a*) assist the foreign State in the initiation or carrying out of investigations regarding an offence committed within the jurisdiction of a foreign State; or

(*b*) lead to further cooperation with a foreign State to carry out an investigation regarding the commission or intended commission of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which may be committed or facilitated by means of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) 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.

(3) The National Director of Public Prosecutions must consider a request by a head of a law enforcement agency in terms of subsection (2) and may only grant approval referred to in subsection (2) if he or she is satisfied that the forwarding of information —

(*a*) will not affect any pending criminal proceedings or investigations adversely regarding criminal offences committed within the Republic; and

(*b*) is in accordance with any applicable law of the Republic.

(4) A law enforcement agency may receive any information from a foreign State which will—

(*a*) assist the law enforcement agency in the initiation or carrying out of investigations regarding an offence committed within the Republic; or

(*b*) lead to further cooperation with a foreign State to carry out an investigation regarding the commission or intended commission of—

(i) an offence under Chapter 2 of this Act; or

(ii) any other offence in terms of the laws of the Republic which may be committed by means of or facilitated by, an article.

Issuing of direction requesting foreign assistance and cooperation

45. (1) If it appears to a magistrate or judge of the High Court from information on oath or by way of affirmation that there are reasonable grounds for believing that an article necessary for the investigation or prosecution of—

(*a*) an offence under Chapter 2 of this Act; or

(*b*) any other offence in terms of the laws of the Republic which may be committed or facilitated by means of an article,

is in the possession of, under the control of or upon any person or in a container, upon or at any premises, vehicle, facility, ship, aircraft, computer device, computer network, database or any part of an electronic communications network within the area of jurisdiction of a foreign State, the magistrate or the judge may issue a direction in the prescribed form, in which assistance from that foreign State is sought in order to—

(i) preserve an article; or

(ii) intercept or obtain and provide data,

as is stated in the direction.

(2) A direction contemplated in subsection (1) must specify that—

(*a*) there are reasonable grounds for believing that an offence contemplated in this Act has been committed in the Republic or that it is necessary to determine whether an offence has been committed;

(*b*) an investigation in respect thereof is being conducted; and

(*c*) for purposes of the investigation, it is necessary, in the interests of justice, that the article be preserved, or that data be intercepted or obtained and be provided by a person or authority in a foreign State.

(3) Subject to subsection (4), a direction must be sent to the National Director of Public Prosecutions for transmission to—

(*a*) the court or tribunal specified in the direction;

(*b*) the appropriate authority in the foreign State which is requested to provide assistance and cooperation; or

(*c*) a designated 24/7 contact point in the foreign State which is requested to provide assistance and cooperation.

(4) (*a*) In a case of urgency a direction may be transmitted directly to the court or tribunal referred to in subsection (3)(*a*), exercising jurisdiction in the place where the article is to be preserved, or the data is to be intercepted or obtained and be provided, or to the appropriate government authority referred to in subsection (3)(*b*) or designated 24/7 contact point referred to in subsection (3)(*c*).

(*b*) The National Director of Public Prosecutions must, as soon as practicable, be notified that a direction has been sent in the manner referred to in paragraph (*a*) and he or she must be furnished with a copy of such direction.

(5) The Cabinet member responsible for the administration of justice must be notified that a direction has been sent as contemplated in subsection (3) or (4) and must be furnished with a copy of such direction.

Foreign requests for assistance and cooperation

46. (1) A request by an authority, court or tribunal exercising jurisdiction in a foreign State for assistance in preserving an article or the interception or the obtaining and providing of data in the Republic for use by such foreign State must be submitted—

(*a*) to the 24/7 point of contact established in terms of section 49 of this Act, which must submit it—

(i) to the National Director of Public Prosecutions; or

(ii) in a case of urgency, to the designated judge;

(*b*) to the National Director of Public Prosecutions; or

(*c*) in a case of urgency, to the designated judge.

(2) Upon receipt of a request in terms of subsection (1)(*a*)(i) or (*b*), the National Director of Public Prosecutions must satisfy himself or herself—

(*a*) that proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting foreign State; or

(*b*) that there are reasonable grounds for believing that an offence has been committed in the requesting 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 requesting foreign State.

(3) Upon receipt of a request in terms of subsection (1)(*a*)(ii) or (*c*), the designated judge, must—

(*a*) satisfy himself or herself—

(i) that proceedings have been instituted in a court or tribunal exercising jurisdiction in the requesting foreign State; or

(ii) that there are reasonable grounds for believing that an offence has been committed in the requesting 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 requesting foreign State; and

(*b*) obtain the recommendations of the National Director of Public Prosecutions on the request.

(4) For purposes of subsection (2) and (3)(*a*), the National Director of Public Prosecutions or the designated judge may rely on a certificate purported to be issued by a competent authority in the foreign State concerned, stating the facts contemplated in the said subsections.

(5) (*a*) The National Director of Public Prosecutions must, if satisfied as contemplated in subsection (2), submit the request for assistance in preserving an article or intercepting or obtaining and providing data, together with his or her recommendations, to the Cabinet member responsible for the administration of justice, for his or her approval.

(*b*) Upon being notified of the Cabinet member"s approval the National Director of Public Prosecutions must forward the request contemplated in subsection (1)(*a*) or (*b*) to the designated judge, for consideration.

(6) (*a*) Subject to subsection (7), the designated judge may on receipt of a request referred to—

(i) in subsection (1)(*a*)(ii) or (*c*), subject to paragraph (*b*); or

(ii) in subsection (5)(*b*),

issue any order which he or she deems appropriate to ensure that the requested—

(*aa*) article is preserved for a period; or

(*bb*) data is intercepted or obtained and provided,

as is specified in the request.

(*b*) The designated judge must, before any order as contemplated in paragraph (*a*) is issued, inform the Cabinet member responsible for the administration of justice, in writing of the—

(i) fact that he or she intends to issue an order; and

(ii) reasons for such decision.

(7) The designated judge may only issue an order contemplated in subsection (6)(*a*), if—

(*a*) on the facts alleged in the request, there are reasonable grounds to believe that—

(i) an offence substantially similar to the offences contemplated in Chapter 2 of this Act, has been or is being or will probably be committed; or

(ii) 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

(iii) that for purposes of the investigation it is necessary in the interests of justice that an article be preserve for a period or that data be intercepted or obtained and provided;

(*b*) the request clearly identifies—

(i) the article that must be preserved;

(ii) the data which must be intercepted or obtained and be provided; and

(iii) the person, entity or electronic communications service provider—

(*aa*) who or which is in possession of the article that must be preserved;

(*bb*) from whose facilities the data must be intercepted and provided; or

(cc) from whom the data must be obtained or provided;

(*c*) the request is, where applicable, in accordance with—

(i) any treaty, convention or other international agreement to which that foreign state and the Republic are parties; or

(ii) any agreement with any foreign State entered into in terms of section 65 of this Act;

(*d*) the order contemplated in subsection (6)(*a*) is in accordance with any applicable law of the Republic; and

(*e*) that it will be in the interests of justice if the order contemplated in subsection 6(*a*) is made.

(8) An order contemplated in subsection (6)(*a*) must be executed by a member of the South African Police Service referred to in section 33 of the South African Police Service Act, 1995 (Act No. 68 of 1995), who is specifically designated in writing by the National Commissioner to execute such orders.

Complying with order of designated judge

47. (1) A person or electronic communications service provider must immediately comply with an order of the designated judge issued in terms of section 46(6).

(2) A person or electronic communications service provider to whom an order referred to in section 46(6) is addressed, 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.

(3) The designated judge to whom an application is made in terms of subsection (2) must, as soon as possible after receipt thereof—

(*a*) consider the application and may, for this purpose, order oral or written evidence to be adduced regarding any fact alleged in the application;

(*b*) give a decision in respect of the application; and

(*c*) if the application is successful, inform the National Director of Public Prosecutions of the outcome of the application.

(4) A person or an electronic communications service provider who—

(*a*) fails to comply with an order referred to in section 46(6); or

(*b*) makes a false statement in an application referred to in subsection (2),

is guilty of an offence and is liable on conviction to a fine not exceeding R5 million or imprisonment not exceeding 5 years or to both such fine and imprisonment.

Informing foreign State of outcome of request for assistance and cooperation and furnishing of data to foreign State

48. (1) The National Director of Public Prosecutions must inform a foreign State of the outcome of its request for assistance and cooperation.

(2) Any data which is intercepted or obtained in terms of an order referred to in section 46(6) of this Act, must be—

(*a*) provided to the 24/7 Point of Contact, established in terms of section 49 of this Act, for submission to an authority, court or tribunal of a foreign State, in an industry-standard format which ensures ease of access to the information and which guarantees the authenticity, integrity and reliability of the information; and

(*b*) accompanied by—

(i) a copy of the order referred to in section 46(6); and

(ii) an affidavit in the prescribed form by the person or authorised representative of an electronic communications service provider, verifying the authenticity, integrity and reliability of the information that is furnished.

(3) A person or electronic communications service provider must keep copies of any the information which is furnished to the 24/7 Point of Contact in terms of subsection (2)(*a*), for a period of three years, in a manner which will ensure the authenticity, integrity and reliability of the information.

(4) The information referred to in subsection (2)(*a*), together with the copy of the order and affidavit referred to in subsection (2)(*b*), must be provided to the authority, court or tribunal exercising jurisdiction in a foreign State which requested the assistance in terms of section 46(1), in the manner agreed upon.

(5) A person or electronic communications service provider who—

(*a*) fails to comply with subsections (2) or (3);

(*b*) makes a false statement in an affidavit referred to in subsection (2)*(b)*(ii),

is guilty of an offence and is liable on conviction to a fine or imprisonment not exceeding 3 years or to both such fine and imprisonment.

CHAPTER 5

24/7 POINT OF CONTACT

Establishment of 24/7 Point of Contact

49. (1) The Cabinet member responsible for policing must, in consultation with the Cabinet member responsible for national financial matters—

(a) establish an office to be known as the 24/7 Point of Contact for the Republic; and

(*b*) equip, operate and maintain the 24/7 Point of Contact.

(2) The Cabinet member responsible for policing exercises final responsibility over the administration and functioning of the 24/7 Point of Contact.

(3) (*a*) The National Commissioner must appoint a member of the Service—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39

of 1994), to the satisfaction of the Cabinet member responsible for State security,

as Director of the 24/7 Point of Contact.

(*b*) The Director must exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, subject to the control and directions of the National Commissioner.

(*c*) Whenever the Director is for any reason temporarily unable to exercise, perform and carry out his or her powers, functions and duties, the National Commissioner must appoint a member of the Service—

(i) who on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Director.

(*d*) The Director must, in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, be assisted, subject to his or her control and directions, by—

(i) appropriately qualified members of the Service designated to the 24/7 Point of Contact and to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security;

(ii) a member of the National Prosecuting Authority at the rank of at least Deputy-Director of Public Prosecutions—

(*aa*) who has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who is seconded to the 24/7 Point of Contact to assist the Director; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State Security; and

(iii) any person or entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is appointed to assist the Director from time to time; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State Security.

(*e*) In order to achieve the objects of this Act, the Director must—

(i) carry out the administrative duties relating to the functioning of the 24/7 Point of Contact;

(ii) exercise control over the persons contemplated in subsection (3)(*d*);

(iii) manage and exercise administrative and technical control over the 24/7 Point of Contact;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by the 24/7 Point of Contact; and

(v) co-ordinate the activities of the 24/7 Point of Contact with those of the Cyber Security Centre, the Government Security Incident Response teams, the Cyber Crime Response Centre, the Cyber Command, the Cyber Security Hub and the Private Sector Security Incident Response Teams.

(*f*) The Director is, for the purposes of the exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this

Act, accountable to the National Commissioner regarding any matter relevant to, incidental to or which may impact on the objects and functions of the 24/7 Point of Contact as set out in subsection (4).

(*g*) The Director must, on a monthly basis, or as the National Commissioner requires, submit a written report to the National Commissioner regarding any matter relevant to, incidental to or which may impact on the objects and functions of the 24/7 Point of Contact as set out in subsection (4).

(*h*) The Director must, on a quarterly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for policing and the Chairperson of the Cyber Response Committee regarding any matter relating to this Act which the Director wishes to or may want to bring to the attention of the Cyber Response Committee.

(4) (*a*) 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 for the purpose of proceedings or investigations regarding the commission or intended commission of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which may be committed or facilitated by means of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) 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.

(*b*) The assistance contemplated in subsection (4)(*a*), includes—

(i) the provision of technical advice and assistance;

(ii) the facilitation or provision of assistance regarding anything which is authorised under Chapter 4 of this Act;

(iii) the provision of legal information;

(iv) the identification and location of an article;

(v) the identification and location of a suspect; and

(vi) cooperation with appropriate authorities of a foreign State.

(5) The Cabinet member responsible for policing may, after consultation with the Cyber Response Committee, make regulations to further—

(*a*) regulate any aspect provided for in subsection (4);

(*b*) impose additional duties on the 24/7 Point of Contact; and

(*c*) regulate any aspect which is necessary or expedient for the proper implementation of this section.

(6) (*a*) The Cabinet member responsible for policing must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act 40 of 1994), on the functions and activities of the 24/7 Point of Contact.

(*b*) The report contemplated in paragraph (*a*) must include—

(i) the number of matters in which technical advice and assistance were provided to a foreign State; and

(ii) the number of matters in which technical advice and assistance were received from a foreign State.

CHAPTER 6

STRUCTURES TO DEAL WITH CYBER SECURITY

Definitions and interpretation

50. For purposes of this Chapter, unless the context indicates otherwise—

(*a*) **"Head of a Department"** means the incumbent of a post mentioned in Column 2 of Schedule 1, 2 or 3 to the Public Service Act, 1994 (Proclamation 103 of 3 June 1994), and includes any employee acting in such post; and

(*b*) "**representative Department**" means—

(i) the Department of Correctional Services;

(ii) the Department of Defence;

(iii) the Department of Home Affairs;

(iv) the Department of Justice and Constitutional Development;

(v*)* the National Prosecuting Authority;

(vi*)* the South African Police Service;

(vii) the State Security Agency;

(viii) the Department of Finance;

(ix) the Financial Intelligence Centre, established by section 2 of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001);

(x) the State Information Technology Agency, established in terms of section 2 of the State Information Technology Agency Act, 1998 (Act No. 88 of 1998);

(xi) the Department of Science and Technology; and

(xii) any other Department or public entity which is requested, in writing, by the Chairperson of the Cyber Response Committee to assist the Committee.

Cyber Response Committee

51. (1) The Cyber Response Committee is hereby established.

(2) The Cyber Response Committee consists of—

(*a*) a chairperson who is the Director-General: State Security;

(*b*) members who are the Heads of the representative Departments and their nominees who must be officials—

(i) at the rank of at least a chief director or equivalent, of a representative Department, who are specifically nominated by a Head of that representative Department to serve on the Cyber Response Committee; and

(ii) to whom a security clearance certificate has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994); and

(*c*) any person who has particular knowledge and skills in respect of any aspect dealt with in this Act and who is, from time to time, requested, in writing, by the Chairperson of the Cyber Response Committee to assist the Committee.

(3) The Cabinet member responsible for State security must appoint a member to act as chairperson whenever the chairperson is absent from the Republic or from duty, or for any reason, is temporarily unable to carry out the responsibilities as chairperson.

(4) The work incidental to the performance of the functions of the Cyber Response Committee must be performed by a secretariat, consisting of designated administrative personnel of the State Security Agency allocated to the Cyber Security Centre established in terms of section 52 of this Act.

(5) The chairperson of the Cyber Response Committee must determine the scheduled time and place of meetings of the Committee and make this known to the other members of the Committee.

(6) The objects and functions of the Cyber Response Committee are to—

(*a*) implement Government policy relating to cybersecurity;

(*b*) identify and prioritise areas of intervention;

(*c*) coordinate cybersecurity activities and be a central point of contact on all cybersecurity matters pertinent to national security;

(*d*) identify and prioritise areas of intervention and promote focussed attention and guidance where required regarding cybersecurity related threats and incidents;

(*e*) promote, guide and coordinate activities aimed at improving cybersecurity measures by all role players, which includes the strengthening of intelligence collection and improved State capacity to investigate, prosecute and combat cybercrime and to deal with cyber threats;

(*f*) oversee and guide the functioning of the 24/7 Point of Contact, the Cyber Security Centre, the Government Security Incident Response Teams, the Cyber Crime Response Centre, the Cyber Command, the Cyber Security Hub and the Private Sector Security Incident Response Teams established in the Republic;

(*g*) promote and provide guidance in respect of the development and implementation of—

(i) the National Critical Information Infrastructure Plan;

(ii) any situational analysis and awareness campaigns concerning the risk environment of South African cyberspace;

(iii) a cybersecurity culture and compliance with minimum security standards;

(iv) public-private partnerships and national and regional action plans in line with Government policy;

(v) appropriate technical and operational cybersecurity standards;

(vi) cybersecurity training, education, research and development and skills development programmes; and

(vii) international cooperation initiatives;

(*h*) facilitate interaction on cyber security, both nationally and internationally and to develop policy guidelines in order to give effect to such interaction;

(*i*) facilitate the establishment of sector, regional and continental Computer Security Incident Response Teams; and

(*j*) establish and promote a comprehensive legal framework governing cyber-related matters.

(7) (*a*) No person referred to in subsection (2), may disclose any confidential information or document obtained by that person in the performance of his or her functions in terms of this Act, except—

(i) to the extent to which it may be necessary for the proper administration of any provision of this Act;

(ii) to any person who of necessity requires it for the performance of any function in terms of this Act;

(iii) when required to do so by order of a court of law; or

(iv) with the written permission of the Cyber Response Committee.

(*b*) Any person who contravenes a provision of paragraph (*a*) is guilty of an offence and is liable on conviction to a fine, or to imprisonment for a period not exceeding 2 years or to both such fine and imprisonment.

(*c*) Any person referred to in subsection (2)(*c),* must, before assisting the Cyber Security Committee, make and subscribe to an affirmation of secrecy in the following form:

'I, ... solemnly declare:

(i) I have taken cognizance of the provisions of section 51(7) of the Cyber Crimes and Cybersecurity Act, ... (Act No. of .....).

(ii) I understand that I may not disclose any information or document, or the contents thereof, of whatever nature that comes to my knowledge or into my possession in consequence of my performance of any function in terms of the Cyber Crimes and Cybersecurity Act, ... (Act No. of .....), whether verbal or in writing, to any unauthorized person without the prior written approval of the Chairperson of the Cyber Security Committee.

(iii) I am fully aware of the serious consequences which may follow any breach or contravention of the above-mentioned provisions.

.....

(Signature)'.

(8) The Cabinet member responsible for State security may, in consultation with the Cabinet member responsible for national financial matters, make

regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person referred to in subsection (2)(*c*).

(9) The Cabinet member responsible for State security must oversee and exercise control over the performance of the functions of the Cyber Response Committee.

(10) The Cabinet member responsible for State security must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act 40 of 1994), regarding progress that has been made towards achieving the objects and functions of the Cyber Response Committee.

Cyber Security Centre

52. (1) The Cabinet member responsible for State security must, in consultation with the Cabinet member responsible for national financial matters—

(*a*) establish a Cyber Security Centre; and

(*b*) equip, operate and maintain the Cyber Security Centre.

(2) The Cabinet member responsible for State security exercises final responsibility over the administration and functioning of the Cyber Security Centre.

(3) The Cabinet member responsible for State security must enter into service level agreements with—

(*a*) the Head of a department; and

(*b*) any entity or institution,

in respect of the provision of services by the Cyber Security Centre.

(4) (*a*) The Cabinet member responsible for State security must appoint a person from the State Security Agency—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as Director of the Cyber Security Centre.

(*b*) The Director must exercise the powers and must perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member responsible for State security or under this Act, subject to the control and directions of the Cabinet member.

(*c*) Whenever the Director is for any reason temporarily unable to exercise, perform or carry out his or her powers, functions and duties, the Cabinet member responsible for State security must appoint a person from the State Security Agency—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Director.

(*d*) The Director must, in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member or under this Act, be assisted, subject to his or her control and directions, by—

(i) members of the State Security Agency allocated to the Cyber Security Centre to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security;

(ii) any person or a entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is, from time to time, appointed to assist the Director; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the Cabinet member responsible for State Security.

(*e*) In order to achieve the objects of this Act, the Director must—

(i) carry out the administrative duties relating to the functioning of the Cyber Security Centre;

(ii) exercise control over the members of the State Security Agency allocated to the Cyber Security Centre, Government Security Incident Response Teams or persons or entities contemplated in subsection (4)(*d*)(ii);

(iii) manage, and exercise administrative and technical control over the Cyber Security Centre and Government Security Incident Response Teams;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by Cyber Security Centre and Government Security Incident Response Teams; and

(v) co-ordinate the activities of the Cyber Security Centre and Government Security Incident Response teams with those of the 24/7 Point of Contact, the National Cybercrime Centre, the Cyber Command, the Cyber Security Hub and the Private Sector Security Incident Response Teams.

(*f*) The Director is, for the purposes of exercising the powers, performing the functions and carrying out the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member responsible for State Security or under this Act, accountable to the Cabinet member.

(*g*) The Director must, on a quarterly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for State security and the Chairperson of the Cyber Response Committee regarding—

(i) cyber security-related threats, any measures implemented to address such cyber security-related threats and shortcomings in addressing such cyber security related threats;

(ii) any matter relevant to, incidental to or which may impact on the objects and functions of the Cyber Security Centre as set out in subsection (5); and

(iii) any other matter relating to this Act which the Director wishes to or may want to bring to the attention of the Cyber Response Committee.

(5) The objects and functions of the Cyber Security Centre are to—

(*a*) facilitate the operational coordination of cyber security incident response activities regarding national intelligence;

(*b*) develop measures to deal with cyber security matters impacting on national security;

(*c*) facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange on national security and threats in order to improve technical response coordination;

(*d*) provide guidance to and facilitate the identification, protection and securing of National Critical Information Infrastructures;

(*e*) ensure the assessment and testing of National Critical Information Infrastructures, including vulnerability assessments, threat and risk assessments and penetration testing, on the written request of the Director-General: State Security;

(*f*) provide coordination and guidance regarding corporate security and policy development, governance, risk management and compliance, identity and security management, security information and event management and cyber forensics;

(*g*) develop response protocols in order to guide coordinated responses to cyber security incidents and interaction with the various stakeholders;

(*h*) ensure the conducting of cyber security audits, assessments and readiness exercises and provide advice on the development of national response plans;

(*i*) act as a point of contact regarding matters relating to State security; and

(*j*) provide the secretarial services required in relation to the Cyber Response Committee.

(6) The Cabinet Member responsible for State security may make regulations to further—

(*a*) regulate any aspect provided for in subsection (5);

(*b*) impose additional duties upon the Cyber Security Centre; and

(*c*) regulate any aspect which is necessary or expedient for the proper implementation of this section.

(7) The Cabinet member responsible for State security may, in consultation with the Cabinet member responsible for national financial matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (4)(*d*)(ii).

(8) The Cabinet member responsible for State security must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act 40 of 1994), on the functions of the Cyber Security Centre.

Government Security Incident Response Teams

53. (1) The Cabinet member responsible for State security must, in consultation with the Cabinet member responsible for national financial matters—

(*a*) establish one or more Government Security Incident Response Teams; and

(*b*) equip, operate and maintain the Government Security Incident Response Teams.

(2) The Cabinet member responsible for State security exercises final responsibility over the administration and functioning of the Government Security Incident Response Teams.

(3) The Cabinet member responsible for State security must enter into service level agreements with—

(*a*) the Head of a department; and

(*b*) any entity or institution,

in respect of the provision of services by the Government Security Incident Response Teams.

(4) (*a*) The Director-General: State Security must, in consultation with the Cabinet member responsible for State security, appoint a person from the State Security Agency—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as head for each Government Security Incident Response Team established under this section.

(*b*) The Head referred to in this section must exercise the powers and perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Director: Cyber Security Centre or under this Act, subject to the control and directions of the Director: Cyber Security Centre.

(*c*) Whenever a Head of a Government Security Incident Response Team is, for any reason, temporarily unable to exercise, perform or carry out his or her powers, functions and duties, the Director-General: State Security must, in consultation with the Cabinet member responsible for State security, appoint a person from the State Security Agency—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Head.

(*d*) The Head of a Government Security Incident Response Team must, in the exercise of the powers, performance of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Director: Cyber Security Centre or under this Act, be assisted, subject to his or her control and directions, by—

(i) members of the State Security Agency, to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, allocated to the Government Security Incident Response Team;

(ii) any person or a entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is, from time to time, appointed to assist the Head; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the Cabinet member responsible for State security.

(*e*) In order to achieve the objects of this Act, a Head referred to in this section must—

(i) carry out the administrative duties relating to the functioning of the Government Security Incident Response Team;

(ii) exercise control over the members of the State Security Agency allocated to the Government Security Incident Response Team or persons or entities contemplated in subsection (4)(*d*)(ii);

(iii) manage and exercise administrative and technical control over the Government Security Incident Response Team;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by the Government Security Incident Response Team; and

(v) co-ordinate the activities of the Government Security Incident Response Team with those of the 24/7 Point of Contact, other Government Security Incident Response Teams, the Cyber Security Centre, the National Cybercrime Centre, the Cyber Command, the Cyber Security Hub and Private Sector Security Incident Response Teams.

(*f*) The Head referred to in this section is, for the purposes of exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Director: Cyber Security Centre or under this Act, accountable to the Director: Cyber Security Centre.

(*g*) The Head referred to in this section must, on a monthly basis, or as the Director: Cyber Security Centre requires, submit a written report to the Director: Cyber Security Centre regarding —

(i) cyber security-related threats and measures implemented in order to address such cyber security-related threats and shortcomings in addressing such cyber security-related threats;

(ii) any matter relevant to, incidental to or which may impact on the objects and functions of the Government Security Incident Response Team as set out in subsection (5); and

(iii) any other matter relating to this Act which the Head wishes to or may want to bring to the attention of the Director: Cyber Security Centre or Cyber Response Committee.

(5) The objects and functions of a Government Security Incident Response Team are to—

(*a*) develop or acquire and implement measures to deal with cyber security matters impacting on national intelligence and national security;

(*b*) protect and secure National Critical Information Infrastructures;

(*c*) implement measures, on the written request of the Director-General: State Security, in order to assess and test National Critical Information Infrastructures, including vulnerability assessments, threat and risk assessments and penetration testing;

(*d*) provide a reactive service to the State which includes—

(i) responding to alerts and warnings;

(ii) handling incidents by—

(*aa*) incident analysis;

(*bb*) providing incident responses on site;

(*cc*) providing incident response support; and

(*dd*) incident response coordination;

(iii) vulnerability handling by—

(*aa*) analysing vulnerabilities;

(*bb*) mitigating the effect of a vulnerability or repairing a vulnerability; and

(*cc*) coordinating responses to vulnerabilities; and

(iv) artifact handling by—

(*aa*) analysing artifacts;

(*bb*) responding to artifacts; and

(*cc*) artifact response coordination;

(*e*) provide a proactive service to the State which includes—

(i) intrusion alerts, vulnerability warnings, security advice and other similar announcements;

(ii) technical analysis of software, malware, intruder activities and related trends in order to help identify future threats and vulnerabilities;

(iii) the furnishing of security audits and assessments;

(iv) the configuration and maintenance of equipment, software, hardware, configurations and infrastructure;

(v) the development of security tools;

(vi) the provision of an intrusion detection service; and

(vii) the dissemination of security-related information to Government Departments; and

(*f*) provide security quality management services to the State which includes—

(i) a risk analysis service;

(ii) a continuity of service and disaster recovery planning service;

(iii) a security consulting service; and

(iv) a product certification service.

(6) The Cabinet Member responsible for State security may, after consultation with the Cyber Response Committee, make regulations to further—

(*a*) regulate any aspect provided for in subsection (5);

(*b*) impose additional duties upon Government Security Incident Response Teams; and

(*c*) regulate any aspect which is necessary or expedient for the proper implementation of this section.

(7) The Cabinet member responsible for State security may, in consultation with the Cabinet member responsible for national financial matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (4)(*d*)(ii).

(8) The Cabinet member responsible for State security must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Intelligence established by section 2 of the Intelligence Services Control Act, 1994 (Act 40 of 1994), on the functions of the Government Security Incident Response Teams.

National Cybercrime Centre

54. (1) The Cabinet member responsible for policing must, in consultation with the Cabinet member responsible for national financial matters—

(*a*) establish a National Cybercrime Centre; and

(*b*) equip, operate and maintain the National Cybercrime Centre.

(2) The Cabinet member responsible for policing exercises final responsibility over the administration and functioning of the National Cybercrime Centre.

(3) (*a*) The National Commissioner must appoint a member from the Service—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as Director of the National Cybercrime Centre.

(*b*) The Director must exercise the powers and perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, subject to the control and directions of the National Commissioner.

(*c*) Whenever the Director is, for any reason, temporarily unable to exercise, perform or carry out his or her powers, functions and duties, the National Commissioner must appoint a person from the Service—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Director.

(*d*) The Director must, in exercising the powers and performing the functions and carrying out the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, be assisted, subject to his or her control and directions, by—

(i) appropriately qualified members of the Service, to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, allocated to the National Cybercrime Centre;

(ii) any person or an entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is, from time to time, appointed to assist the Director; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the Cabinet member responsible for State security.

(*e*) In order to achieve the objects of this Act, the Director must—

(i) carry out the administrative duties relating to the functioning of the National Cybercrime Centre;

(ii) exercise control over the members of the Service allocated to the National Cybercrime Centre or persons or entities contemplated in paragraph (*d*)(ii);

(iii) manage and exercise administrative and technical control over the National Cybercrime Centre;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by the National Cybercrime Centre;

(v) co-ordinate the activities of the National Cybercrime Centre with those of the 24/7 Point of Contact, the Cyber Security Centre, the Government Security Incident Response Teams, the Cyber Command, the Cybersecurity Hub and the Private Sector Security Incident Response Teams; and

(vi) develop and implement cyber security policies and strategies to investigate and combat cybercrime.

(*f*) The Director is, for the purposes of exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the National Commissioner or under this Act, accountable to the National Commissioner.

(*g*) The Director must, on a monthly basis, or as the National Commissioner requires, submit a written report to the National Commissioner regarding any matter relevant to, incidental to or which may impact on the objects and functions of the National Cybercrime Centre as are set out in subsection (4).

(*h*) The Director must, on a quarterly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for policing and the Chairperson of the Cyber Response Committee regarding—

(i) cyber security-related threats impacting on law enforcement, any measures implemented to address such cyber security-related threats and shortcomings in addressing such cyber security-related threats;

(ii) cyber crime trends;

(iii) successes and shortcomings in investigative measures in order to investigate cybercrime;

(iv) successes and shortcomings in international cooperation in the investigation of cybercrime;

(v) any matter relevant to, incidental to or which may impact on the objects and functions of the National Cybercrime Centre as set out in subsection (4); and

(vi) any other matter relating to this Act which the Director wishes to or may want to bring to the attention of the Cyber Response Committee.

(4) The objects and functions of the National Cybercrime Centre are to—

(*a*) facilitate the operational coordination of cyber security incident response activities with reference to the prevention, combating and investigation of crime in

order to maintain public order, to secure the inhabitants of the Republic and their property and to uphold and enforce the laws of the Republic;

(*b*) develop measures in order to deal with cyber security matters impacting on law enforcement;

(*c*) facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange on law enforcement and threats in order to improve technical response coordination;

(*d*) provide coordination and guidance regarding corporate security and policy development, governance, risk management and compliance, identity and security management, security information and events management;

(*e*) establish, develop and maintain an adequate cyber forensics capacity;

(*f*) develop response protocols in order to guide coordinated responses to cyber security incidents and interact with the various stakeholders;

(*g*) develop and maintain cross-border law enforcement cooperation in respect of cybercrime;

(*h*) promote, establish and maintain public-private cooperation in order to fight cybercrime;

(*i*) promote, establish and maintain international cooperation in order to fight cybercrime; and

(*j*) develop capacity and implement measures in order to impede and neutralize cyber security-related incidents and threats.

(5) The Cabinet Member responsible for policing may, after consultation with the Cyber Response Committee, make regulations to further—

(*a*) regulate any aspect provided for in subsection (4);

(*b*) impose additional duties upon the National Cybercrime Centre; and

(*c*) regulate any aspect which is necessary or expedient for the proper implementation of this section.

(6) The Cabinet member responsible for policing may, in consultation with the Cabinet member responsible for national financial matters, make regulations

regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (3)(*d*)(ii).

(7) The Cabinet member responsible for policing must, at the end of each financial year, submit a report to Parliament regarding progress that has been made towards achieving the objects and functions of the National Cybercrime Centre.

Cyber Command

55. (1) The Cabinet member responsible for defence must, in consultation with the Cabinet member responsible for national financial matters—

(*a*) establish a Cyber Command as part of the Intelligence Division of the South African National Defence Force contemplated in section 33 of the Defence Act, 2002 (Act 42 of 2002); and

(*b*) equip, operate and maintain the Cyber Command.

(2) The Cabinet member responsible for defence exercises final responsibility over the administration and functioning of the Cyber Command.

(3) (*a*) The Chief of the South African National Defence Force must appoint a member or employee from the South African National Defence Force—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002),

as General Officer Commanding of the Cyber Command.

(*b*) The General Officer Commanding must exercise the powers and perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Chief of the South African National Defence Force or under this Act, subject to the control and directions of the Chief of the South African National Defence Force.

(*c*) Whenever the General Officer Commanding is for any reason temporarily unable to exercise, perform and carry out his or her powers, functions and duties, the Chief of the South African National Defence Force must appoint a member or employee from the South African National Defence Force—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002),

as acting General Officer Commanding.

(*d*) The General Officer Commanding must, in exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Chief of the South African National Defence Force or under this Act, be assisted, subject to his or her control and directions, by—

(i) members and employees of the South African National Defence Force, to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002);

(ii) any person or an entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act;

(*bb*) who or which is, from time to time, appointed to assist the General Officer Commanding; and

(*cc*) to whom a security clearance has been issued in terms of section 37 of the Defence Act, 2002 (Act No. 42 of 2002).

(*e*) In order to achieve the objects of this Act, the General Officer Commanding must—

(i) carry out the administrative duties relating to the functioning of the Cyber Command;

(ii) exercise control over the members and employees of the Defence Force or persons or entities contemplated in subsection (3)(*d*)(ii);

(iii) manage and exercise administrative and technical control over the Cyber Command;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by Cyber Command;

(v) co-ordinate the activities of the Cyber Command with those of the 24/7 Point of Contact, the Cyber Security Centre, the Government Security Incident Response Teams, the National Cybercrime Centre, the Cyber Security Hub and the Private Sector Security Incident Response Teams.

(*f*) The General Officer Commanding is, for the purposes of exercising the powers, performing of the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the the Chief of the South African National Defence Force or under this Act, accountable to the Chief of the South African National Defence Force.

(*g*) The General Officer Commanding must, on a monthly basis, or as the Chief of the South African National Defence Force requires, submit a written report to the Chief of the South African National Defence Force regarding any matter relevant to, incidental to, or which may impact on the objects and functions of the Cyber Command as set out in subsection (4).

(*h*) The General Officer Commanding must, on a quarterly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for defence and the Chairperson of the Cyber Response Committee regarding—

(i) cyber security-related threats, any measures implemented to address such cyber security-related threats and shortcomings in addressing such cyber security-related threats which may impact on the defence of the Republic;

(ii) any matter relevant to, incidental to or which may impact on the objects and functions of the Cyber Command as set out in subsection (4); or

(iii) any other matter relating to this Act which the General Officer Commanding wishes to or may want to bring to the attention of the Cyber Response Committee.

(4) The objects and functions of the Cyber Command are to—

(*a*) facilitate the operational coordination of cyber security incident response activities regarding national defence;

(*b*) develop measures to deal with cyber security matters impacting on national defence;

(*c*) facilitate the analysis of cyber security incidents, trends, vulnerabilities, information-sharing, technology exchange and threats on national defence in order to improve technical response coordination;

(*d*) provide guidance to and facilitate the identification, protection and securing of National Critical Information Infrastructures relevant to national defence;

(*e*) ensure, on the written command of the Chief of the South African National Defence Force, regular assessments and testing of National Critical Information Infrastructures relevant to national defence, including vulnerability assessments, threat and risk assessments and penetration testing;

(*f*) ensure the conducting of cyber security audits, assessments and readiness exercises and provide advice on the development of national response plans in so far as they relate to national defence;

(*g*) act as a point of contact regarding matters relating to national defence; and

(*h*) coordinate and implement cyber offensive and defensive measures as part of its defence mandate.

(5) The Cabinet Member responsible for defence may, after consultation with the Cyber Response Committee, make regulations to further—

(a) regulate any aspect provided for in subsection (4);

(*b*) impose additional duties upon the Cyber Command; and

(*c*) regulate any aspect which it is necessary or expedient for the proper implementation of this section.

(6) The Cabinet member responsible for defence may, in consultation with the Cabinet member responsible for national finance matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (3)(*d*)(ii).

(7) The Cabinet member responsible for defence must, at the end of each financial year, submit a report to Chairperson of the Joint Standing Committee on Defence of Parliament, on the functions of the Cyber Command.

Cyber Security Hub

56. (1) The Cabinet member responsible for telecommunications and postal services must, in consultation with the Cabinet member responsible for national financial matters, —

(*a*) establish a Cyber Security Hub; and

(*b*) equip, operate and maintain the Cyber Security Hub.

(2) The Cabinet member responsible for telecommunications and postal services exercises final responsibility over the administration and functioning of the Cyber Security Hub.

(3) The Cabinet member responsible for telecommunications and postal services must enter into service level agreements with—

(*a*) the Heads of departments; and

(*b*) any public or private entity or institution,

in respect of the provision of services by the Cyber Security Hub.

(4) (*a*) The Cabinet member responsible for telecommunications and postal services must appoint a person—

(i) who, on the grounds of his or her technical knowledge and experience, is a suitable and qualified person,

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as Director of the Cyber Security Hub.

(*b*) The Director must exercise the powers and perform the functions and carry out the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member responsible for telecommunications and postal services or under this Act, subject to the control and directions of the Cabinet member.

(*c*) Whenever the Director is for any reason temporarily unable to exercise, perform or carry out his or her powers, functions and duties, the Cabinet member responsible for telecommunications and postal services must, appoint a person—

(i) who, on the grounds of his or her knowledge and experience, is a suitable and qualified person; and

(ii) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security,

as acting Director.

(*d*) The Director must, in exercising the powers, performing the functions and carrying out the duties conferred upon, assigned to or imposed upon him or her by the Minister or under this Act, be assisted, subject to his or her control and directions, by—

(i) officials or employees of the Department of Telecommunications and Postal Services, to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, allocated to the Cyber Security Hub;

(ii) members of the law enforcement agencies, to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National

Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, seconded to the Cyber Security Hub; and

(iii) any person or a entity—

(*aa*) who or which has particular knowledge and skills in respect of any aspect dealt with in this Act; and

(*bb*) who or which is, from time to time, appointed to assist the Director; and

(*cc*) to whom a security clearance has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994, to the satisfaction of the Cabinet member responsible for State security.

(*e*) In order to achieve the objects of this Act, the Director must—

(i) carry out the administrative duties relating to the functioning of the Cyber Security Hub;

(ii) exercise control over the officials or employees, members and persons and entities contemplated in subsection (4)(*d*);

(iii) manage, and exercise administrative and technical control over the Cyber Security Hub and Private Sector Security Incident Response Teams;

(iv) regulate the procedure and determine the manner in which the provisions of this Act must be carried out by Cyber Security Hub and Private Sector Security Incident Response Teams;

(v) co-ordinate the activities of the Cyber Security Hub and Private Sector Security Incident Response Teams;

(vi) co-ordinate the activities of the Cyber Security Hub and Private Sector Security Incident Response Teams with those of the 24/7 Point of Contact, the Cyber Security Centre, the Government Security Incident Response Teams, the National Cybercrime Centre and the Cyber Command; and

(viii) ensure implementation of any national security guidelines which are issued by the Cabinet member responsible for State security, in consultation with the Cabinet member responsible for telecommunications and postal services and after consultation with the Cyber Response Committee.

(*f*) The Director is, for the purposes of exercising the powers, performing the functions and carrying out of the duties conferred upon, assigned to or imposed upon him or her by the Cabinet member responsible for telecommunications and postal services or under this Act, accountable to the Cabinet member.

(*g*) The Director must, on a monthly basis, or as the Cabinet member responsible for telecommunications and postal services requires, submit a written report to the Cabinet member regarding any matter relevant to, incidental to, or which may impact on the objects and functions of the Cyber Security Hub and Private Sector Security Incident Response Teams.

(*h*) The Director must, on a monthly basis, or as the Chairperson of the Cyber Response Committee requires, submit a written report to the Cabinet member responsible for telecommunications and postal services and Chairperson of the Cyber Response Committee regarding—

(i) cyber security-related threats, any measures implemented to address such cyber security-related threats and shortcomings in addressing such cyber security-related threats;

(ii) any matter relevant to, incidental to or which impacts on the objects and functions of the Cyber Security Hub as set out in subsection (5); and

(iii) any other matter relating to this Act which the Director wishes to or may want to bring to the attention of the Cabinet member responsible for telecommunications and postal services or the Cyber Response Committee.

(5) The objects and functions of the Cyber Security Hub are to—

(*a*) coordinate general cyber security activities in the private sector;

(*b*) inform Private Sector Security Incident Response Teams, electronic communications service providers, vendors and other persons or entities who may have an interest in cyber security, of cyber security developments;

(*c*) provide best practice guidance on Information and Communications Technology security to Government, electronic communications service providers and the private sector;

(*d*) initiate cyber security awareness campaigns;

(*e*) promote compliance with standards, procedures and policy developed by the Cybersecurity Response Committee regarding cyber security which have a bearing on national security and cybercrime;

(*f*) encourage and facilitate the development of Private Sector Security Incident Response Teams;

(*g*) centralise co-ordination of cyber security activities in the private sector;

(*h*) respond to cyber security incidents;

(*i*) act as a point of contact regarding cyber security activities in the private sector;

(*j*) investigate the activities of cryptography service providers in relation to their compliance or non-compliance with relevant legislation and issue orders to cryptography service providers in order to ensure compliance;

(*k*) conduct cyber security audits, assessments and readiness exercises on request;

(*l*) assist the National Cybercrime Centre, subject to the provisions of subsection (3), in investigations relating to cyber crime; and

(*m*) assist the Cyber Security Centre, the Government Security Incident Response Teams, the National Cybercrime Centre, subject to subsection (3), with any aspect which may impact on their objects and functions.

(6) The Cabinet member responsible for telecommunications and postal services may—

(*a*) after consultation with the Cyber Response Committee and the electronic communications service providers, make regulations to—

(i) further regulate any aspect provided for in subsection (5); or

(ii) impose additional duties on the Cyber Security Hub, not inconsistent with this Act;

(*b*) in consultation with the Cabinet member responsible for national financial matters, make regulations regarding travelling, subsistence, remuneration and other expenses and allowances payable to a person or entity referred to in subsection (4)(*d*)(iii); and

(*c*) make regulations regarding any other relevant matter which is necessary or expedient to prescribe for the proper implementation of this section.

(7) The Cabinet member responsible for telecommunications and postal services must, at the end of each financial year, submit a report to Parliament regarding progress that has been made towards achieving the objects and functions of the Cyber Security Hub.

Private Sector Security Incident Response Teams

57. (1) (*a*) The Cabinet member responsible for telecommunications and postal services must, by notice in the *Gazette*, declare different sectors which provide an electronic communications service for which Private Sector Security Incident Response Teams must be established.

(*b*) The declaration of different sectors referred to in paragraph (*a*) must be done in consultation with the Cabinet member responsible for the functional area of the sector and after consultation with the Cyber Response Committee.

(2) (*a*) Each sector must, within six months from the date of the publication of a notice referred to in subsection (1)(*a*) at own cost establish one or more Private Sector Security Incident Response Teams for that sector.

(*b*) The Cabinet member responsible for telecommunications and postal services must, by notice in the *Gazette*, recognise any Private Sector Security Incident Response Team which is established in terms of paragraph (*a*), for a sector.

(3) (*a*) If a sector fails to establish a Private Sector Security Incident Response Team, contemplated in subsection (2), the Cabinet member responsible for telecommunications and postal services may, after consultation with the sector, establish a Private Sector Security Incident Response Team for that sector on such terms and conditions as he or she deems fit to give effect to the objects of this Act.

(*b*) The particular sector is responsible for the operational costs of a Private Sector Security Incident Response Team which is established in terms of paragraph (*a*).

(4) A Private Sector Security Incident Response Team recognised in terms of subsection (2)(*b*) or established under subsection (3)(*a*), must—

(*a*) act as a point of contact between the sector entities in the sector for which it is established and the Cyber Security Hub;

(*b*) be a contact point for that specific sector on cyber security matters;

(*c*) coordinate cyber security incident response activities within that sector;

(*d*) facilitate information-sharing and technology-sharing within the sector;

(*e*) facilitate information-sharing and technology-exchange with other Private Sector Security Incident Response Teams established for other sectors and the Cyber Security Hub;

(*f*) establish minimum security standards and best practices for the sector for which it is established in consultation with the Cyber Security Hub;

(*g*) report all cyber security threats in the sector for which it is established and measures which have been implemented to address such threats to the Cyber Security Hub and Private Sector Security Incident Response Teams established for other sectors;

(*h*) immediately report new cybercrime trends which come to its attention to the Cyber Security Hub, Private Sector Security Incident Response Teams established for other sectors and the National Cybercrime Centre;

(*i*) provide sector entities within the sector for which it is established with best practice guidance on cyber security; and

(*j*) perform any other function conferred on or assigned to it by the Cabinet member responsible for telecommunications and postal services by notice in the *Gazette*.

(5) (*a*) The Cabinet member responsible for telecommunications and postal services may make regulations after consultation with the relevant sector and the Cyber Security Hub, and after consultation with the Cyber Response Committee—

(i) to further regulate any aspect provided for in subsection (4);

(ii) regarding different grades of security clearances to be issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), to the satisfaction of the Cabinet member responsible for State security, to persons involved in the Private Sector Security Incident Response Teams; and

(ii) regarding any other relevant matter which is necessary or expedient to prescribe for the proper implementation of this section.

(*b*) The regulations contemplated in paragraph (*a*), may provide that any person or entity who contravenes or fails to comply with a regulation is guilty of an offence and is liable on conviction to a fine or to imprisonment not exceeding one year or to both such fine and imprisonment.

CHAPTER 7

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Identification and declaring National Critical Information Infrastructures

58. (1) The Cyber Security Centre—

(*a*) in consultation with the Cyber Response Committee; and

(b) after consultation with any information infrastructure which is identified as a potential National Critical Information Infrastructure,

must within 12 months of the date of commencement of this Act, submit to the Cabinet member responsible for State security, information and recommendations regarding information infrastructures which need to be declared as National Critical Information Infrastructures.

(2) The Cabinet member responsible for State security may, subject to subsection (3), after considering any information and recommendations made to him or her in terms of subsection (1) or at any time, by notice in the *Gazette*, declare any information infrastructure, or category or class of information infrastructures or any part thereof, as National Critical Information Infrastructures if it appears to the Cabinet member that such information infrastructure or information infrastructures are of such a strategic nature that any interference with them or their loss, damage, disruption or immobilization may—

(*a*) prejudice the security, the defence, law enforcement or international relations of the Republic;

(*b*) prejudice the health or safety of the public;

(*c*) cause interference with or disruption of, an essential service;

(*d*) causes any major economic loss;

(*e*) cause destabilization of the economy of the Republic; or

(*f*) create a public emergency situation.

(3) (*a*) Before the Cabinet member responsible for State security declares an information infrastructure to be a National Critical Information Infrastructure as contemplated in subsection (2), he or she must—

(i) with the exception of the State Security Agency, as referred to in section 3(1) of the Intelligence Services Act, 2002 (Act No. 65 of 2002), where the information infrastructure, or any part thereof, belongs to a Department of State, consult with the Cabinet member responsible for that Department;

(ii) where the information infrastructure, or any part thereof belongs to a company or entity that is not a state-owned or a person—

(*aa*) consult with the company, entity or person;

(*bb*) afford the company, entity or person the opportunity to make written representations on any aspect relating to the Cabinet member‟s intention to declare the information infrastructure, as a National Critical Information Infrastructure;

(*cc*) consider the representations of the company, entity or person; and

(*dd*) give a written decision to the company, entity or person; or

(iii) where the information infrastructure, or any part thereof, belongs to a bank as defined in section 1(1) of the Banks Act, 1990 (Act No. 94 of 1990), a mutual bank as defined in section 1(1) of the Mutual Banks Act, 1993 (Act No. 124 of 1993), a co-operative bank as defined in section 1(1) of the Co-operative Banks Act, 2007 (Act No. 40 of 2007) or the South African Reserve Bank as contemplated in the South African Reserve Bank Act, 1989 (Act No. 90 of 1989)—

(*aa*) consult with the Cabinet member responsible for finance, the South African Reserve Bank as contemplated in the South African Reserve Bank Act, 1989 (Act No. 90 of 1989), and the Financial Services Board established by section 2 of the Financial Services Board Act, 1990 (Act 97 of 1990);

(*bb*) consult with the bank in question;

(*cc*) afford the bank the opportunity to make written representations on any aspect relating to the Cabinet member‟s intention to declare the information structure, as a National Critical Information Infrastructure;

(*dd*) consider the representations of the bank; and

(*ee*) give a written decision to the bank.

(*b*) (i) A company, entity, person or bank may appeal against any decision of the Cabinet member in terms of paragraph (*a*)(ii)(*dd*) or (*a*)(iii)(*ee*) to the High Court.

(ii) An appeal in terms of paragraph (*b*)(i) must—

(*aa*) be lodged within 180 days from the date on which the decision was made known by the Cabinet member or such later date as the High Court permits; and

(*bb*) set out the grounds for the appeal.

(iii) The appeal must be proceeded with as if it were an appeal from a magistrate's court to the High Court.

(4) Any information infrastructure declared to be a National Critical Information Infrastructure must, notwithstanding any other law, comply with the regulations made in terms of subsection (5).

(5) The Cabinet member responsible for State security, in consultation with the relevant Cabinet members and the Cyber Response Committee must, within six months of the declaration of any information infrastructure, or category or class of information infrastructures or any part thereof, as National Critical Information Infrastructure, make regulations regulating—

(*a*) the classification of information on National Critical Information Infrastructures;

(*b*) security policies and procedures to be applied to National Critical Information Infrastructures;

(*c*) access to National Critical Information Infrastructures;

(*d*) the storing and archiving of information on National Critical Information Infrastructures;

(*e*) cyber security incident management and continuation with service provision;

(*f*) minimum physical and technical security measures that must be implemented in order to protect National Critical Information Infrastructures;

(*g*) the period within which the owner of, or person in control of a National Critical Information Infrastructure must comply with the regulations; and

(*h*) any other relevant matter which is necessary or expedient to prescribe for the proper implementation of this section.

(6) The owner of, or person in control of, a National Critical Information Infrastructure, which includes National Critical Information Structures under control of a Department of State, must in consultation with the Cabinet member responsible for

State security, at own cost, take steps to the satisfaction of the Cabinet member for purposes of complying with the regulations contemplated in subsection (5).

(7) If the owner of, or person in control of, the National Critical Information Infrastructure, which includes a National Critical Information Structure under control of a Department of State, fails to take the steps referred to in subsection (6), the Minister may, by written notice, order him or her to take such steps in respect of the National Critical Information Infrastructure as may be specified in the notice, within the period specified in the notice.

(8) If the owner of, or person in control of, the National Critical Information Infrastructure, which includes a National Critical Information Structure under control of a Department of State, without reasonable cause refuses or fails to take the steps specified in the notice within the period specified therein he or she is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(9) If the owner of, or person in control of, the National Critical Information Infrastructure fails or refuses to take the steps specified in the notice within the period specified therein, 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, irrespective of whether the owner or person has been charged or convicted in connection with that failure or refusal, and the Cabinet may recover the costs of those steps from the owner or person on whose behalf they were taken.

(10) For purposes of this section—

(*a*) "**information infrastructure**" means any data, computer data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto; and

(*b*) **"relevant Cabinet members"** means the Cabinet members responsible for defence, telecommunications and postal services, justice and correctional

services, policing, State security and includes the National Director of Public Prosecutions.

Establishment and control of National Critical Information Infrastructure Fund

59. (1) There is hereby established a fund to be known as the National Critical Information Infrastructure Fund.

(2) The Fund must be credited with—

(*a*) moneys appropriated by Parliament for the National Critical Information Structure Fund;

(*b*) interest derived from the investment of money in the Fund;

(c) any costs recovered in terms of section 58(9); and

(*d*) money accruing to the Fund from any other source.

(3) (*a*) The money in the Fund must be utilised—

(i) for purposes of section 58(9) on behalf of the owner or person who fails or refuses to take steps referred to in section 58; or

(ii) to implement disaster management measures in respect of National Critical Information Infrastructures in disaster situations.

(*b*) The Cabinet member responsible for State security must, before the Fund can be utilised for the purposes contemplated in paragraph (*a*)(ii), obtain the permission of the Cabinet member responsible for national financial matters.

(4) The Director-General: State Security is the accounting officer of the Fund in terms of the Public Finance Management Act, 1999 (Act No. 1 of 1999).

(5) The Fund is, subject to the directions of the Cabinet member responsible for State security, after consultation with the Cyber Response Committee, under the control and management of the Director-General: State Security, who—

(*a*) must utilise the money in the Fund in accordance with subsection (3);

(*b*) is charged with the responsibility of accounting for money received in, and payments made from, the Fund; and

(c) must cause the necessary accounting and other related records to be kept.

(6) Any money in the Fund which is not required for immediate use must be invested by the Director-General: State Security with a banking institution approved by the Cabinet member responsible for State security, in consultation with the Cabinet member responsible for national financial matters, and may be withdrawn when required.

(7) Any unexpended balance of the money in the Fund at the end of any financial year must be carried forward as a credit in the Fund to the next financial year.

(8) The Fund and the records referred to in subsection (5)(*c*) must be audited by the Auditor-General.

(9) For purposes of this section—

(*a*) **"disaster management measure"** means any measure aimed at—

(i) preventing or reducing the risk of a disaster;

(ii) mitigating the severity or consequences of a disaster;

(iii) emergency preparedness;

(iv) rapid and effective responses to a disaster; and

(v) post-disaster recovery and rehabilitation; and

(*b*) "**disaster situation**" means a progressive or sudden, widespread or localised occurrence, which takes place or is imminent and which causes or may cause substantial damage to a National Critical Information Infrastructure or any part thereof and which is of such a magnitude that it exceeds the ability of such a National Critical Information Infrastructure affected by the disaster to cope with its effects using its own resources only.

Auditing of National Critical Information Infrastructures to ensure compliance

60. (1) The owner of, or person in control of, a National Critical Information Infrastructure must, at least once a year, cause an audit to be performed on the

National Critical Information Infrastructure in order to evaluate compliance with the provisions of section 58(6) of this Act.

(2) Before an audit referred to in subsection (1) is performed on a National Critical Information Infrastructure, the owner of, or person in control of, a National Critical Information Infrastructure must, at least 30 days in advance of the date of the audit, notify the Director-General: State Security, in writing of—

(*a*) the date on which an audit is to be performed; and

(*b*) the particulars and contact details of the person who is responsible for the overall management and control of the audit.

(3) The Director-General: State Security may designate any member, person or entity, referred to in section 52(4) of this Act, to monitor, evaluate and report on the adequacy and effectiveness of any audit referred to in subsection (1).

(4) The owner of, or person in control of, a National Critical Information Infrastructure must, within 30 days after an audit referred to in subsection (1) has been completed, report in the prescribed form and manner to the Director-General: State Security regarding the outcome of the audit referred to in subsection (1).

(5) The Director-General: State Security may request the owner of, or person in control of, a National Critical Information Infrastructure to provide such additional information as may be necessary within a specified period, in order to evaluate the report referred to in subsection (4).

(6) If the owner of, or person in control of, a National Critical Information Infrastructure—

(*a*) fails to cause an audit to be performed on a National Critical Information Infrastructure in order to evaluate compliance with the provisions of section 58(6) of this Act as contemplated in subsection (1);

(*b*) fails to give a report referred to in subsection (3) to the satisfaction of the Director-General: State Security after he or she has been requested to do so in terms of subsection (5), to provide additional information; or

(*c*) requests the Director-General: State Security to perform an audit referred to in subsection (1),

the Director-General: State Security must cause an audit to be performed on the National Critical Information Infrastructure in order to evaluate compliance with the provisions of section 58(6) of this Act.

(7) No person may perform an audit on a National Critical Information Structure pursuant to the provisions of subsection (6) unless he or she—

(*a*) has been authorised in writing by the Director-General: State Security to perform such audit;

(*b*) is in possession of a certificate of appointment, in the prescribed form, issued by the Director-General: State Security, which certificate must be produced on demand; and

(*c*) is accompanied by a person in control of the National Critical Information Infrastructure or a person designated by such a person.

(8) The person contemplated in subsection (7)(*c*) and any other employee of the National Critical Information Structure must assist and provide technical assistance and support to a person who is authorised to carry out an audit in terms of subsection (7)(*a*).

(9) The National Critical Information Structure which is audited pursuant to the provisions of subsection (6) is responsible for the cost of the audit.

(10) The owner of, or person in control of, a National Critical Information Infrastructure who—

(*a*) fails to cause an audit to be performed on a National Critical Information Infrastructure in order to evaluate compliance with the provisions of section 58(6) of this Act as contemplated in subsection (1);

(*b*) fails to notify the Director-General: State Security, in writing of an audit to be performed as contemplated in subsection (2);

(*c*) fails to—

(i) report on the outcome of the audit within 30 days; or

(ii) report in the prescribed form and manner to the Director-General: State Security regarding the outcome of the audit,

as contemplated in subsection (4);

(*d*) furnishes—

(i) a report referred to in subsection (4); or

(ii) any additional information referred to in subsection (5),

to the Director-General: State Security which he or she knows to be false or which he or she does not know or believe to be true; or

(*e*) fails to provide, within the specified time period the additional information requested by the Director-General: State Security as contemplated in subsection (5),

is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding three years, or to both such fine and such imprisonment.

(11) Any person who—

(*a*) hinders or obstructs any member, person or entity to monitor, evaluate and report on the adequacy and effectiveness of an audit as contemplated in subsection (3);

(*b*) hinders or obstructs a person authorised to carry out an audit in the exercise of his or her powers or the performance of his or her functions or duties in terms of subsection (6);

(*c*) fails to accompany a person authorised to carry out an audit as contemplated in subsection (7)(*c*); or

(*d*) fails to assist or provide technical assistance and support to a person authorised to carry out an audit as contemplated in subsection (8),

is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years, or to both such fine and such imprisonment.

CHAPTER 8

EVIDENCE

Admissibility of affidavits

61. (1) Whenever any fact established by any examination or process requiring any skill in—

(*a*) the interpretation of data;

(*b*) the design of, or functioning of data, a computer device, a computer network, a database, an electronic communications network;

(*c*) computer science;

(*d*) electronic communications networks and technology;

(*e*) software engineering; or

(*f*) computer programming,

is or may become relevant to an issue at criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998), a document purporting to be an affidavit made by a person who, in that affidavit, states that he or she—

(i) 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*;

(ii) possesses relevant qualifications, expertise and experience which make him or her competent to make the affidavit; and

(ii) 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.

(2) Any person who makes an affidavit under subsection (1) and who in such affidavit wilfully states anything which is false, is guilty of an offence and is liable on conviction to a fine or imprisonment not exceeding two years.

(3) The 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.

(4) No provision of this section affects any other law under which any certificate or other document is admissible in evidence and the provisions of this section are deemed to be additional to and not in substitution of any such law.

(5) (a) For the purposes of subsection (1), a document purporting to be an affidavit made by a person who in that 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, by notice in the *Gazette,* have no effect unless—

(i) it is obtained in terms of an order of a competent court or on the authority of a government institution of the foreign State concerned, as the case may be; and

(ii) it is authenticated—

(*aa*) in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic; or

(*bb*) by a person and in the manner contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act No. 16 of 1963).

(*b*) The admissibility and evidentiary value of an affidavit contemplated in paragraph (*a*) are not affected by the fact that the form of the oath, confirmation or attestation thereof differs from the form of the oath, confirmation or attestation prescribed in the Republic.

(*c*) A court before which an affidavit contemplated in paragraph (*a*) is placed may, in order to clarify any obscurities in the said affidavit and at the request of a party to the proceedings, order that a supplementary affidavit be submitted or that oral evidence be heard: Provided that oral evidence may only be heard if the

court is of the opinion that it is in the interests of the administration of justice and that a party to the proceedings would be prejudiced materially if oral evidence is not heard.

Admissibility of evidence obtained as result of direction requesting foreign assistance and cooperation

62. (1) Evidence which is provided in response to a direction contemplated in section 45 of this Act from a foreign State is deemed to be evidence under oath if—

(*a*) it is obtained in terms of an order of a competent court of a foreign State; or

(*b*) it is accompanied by a statement in which it appears that the witness was, in terms of the law of the foreign State, warned to tell the truth and which is authenticated —

(i) in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic; or

(ii) by a person and in the manner contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act No. 16 of 1963); or

(iii) in terms of the laws of the foreign State,

which verifies the correctness of any evidence which has been furnished; and

(*c*) the person, according to the law of the foreign State, would be guilty of an offence for which he or she could be prosecuted if he or she makes a false statement or representation, or furnishes false information, knowing it to be false.

(2) Any evidence received in response to a direction, together with the statement contemplated in subsection (1)(*b)* and the direction issued in terms of section 45(1) must be open to inspection by the parties to any proceedings.

(3) Evidence obtained in terms of subsection (1) must be admitted as evidence at any proceedings and forms part of the record of such proceedings if—

(*a*) the party against whom the evidence is to be adduced agrees to the admission thereof as evidence at such proceedings; or

(*b*) the court, having regard to—

(i) the nature of the proceedings;

(ii) the nature of the evidence;

(iii) the purpose for which the evidence is adduced;

(iv) any prejudice to any party which the admission of such evidence might entail; and

(v) any other factor which in the opinion of the court should be taken into account,

is of the opinion that such evidence should be admitted in the interests of justice.

(4) The provisions of subsection (2) do not render admissible any evidence which would be inadmissible had such evidence been given at the subsequent proceedings by the witness from whom it was obtained.

(5) The court before which evidence is produced as *prima facie* proof of the relevant contents thereof may, in its discretion—

(*a*) cause the person who made the statement to be subpoenaed to give oral evidence in the proceedings in question; or

(*b*) 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.

(6) The provisions of this section do not affect any other law in terms of which evidence may be admitted as evidence at any proceedings and the provisions of this section are additional to and not in substitution for, any such law.

Admissibility of evidence

63. (1) In any criminal proceedings under this Act, the rules of evidence do not apply in a manner so as to preclude the admissibility of data, a data message or data document in evidence—

(*a*) merely on the grounds that it is data or a data message; or

(*b*) if it is the best evidence that the person adducing it could reasonably be expected to obtain on the grounds that it is not in its original form.

(2) Evidence in the form of data or a data message must, subject to subsection (3), be given due evidential weight.

(3) In assessing the admissibility or evidential weight of data or a data message regard must be had to—

(*a*) the reliability of the manner in which the data or data message was generated, stored or communicated;

(*b*) the reliability of the manner in which the integrity of the data or data message was maintained;

(*c*) the manner in which the originator or recipient of the data or data message was identified; and

(*d*) any other relevant factor.

(4) A copy or printout of data or a data message is rebuttable proof of the contents of such data or data message if it is accompanied by a declaration that is authenticated—

(a) in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic;

(*b*) by a person, and in the manner, contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act No. 16 of 1963); or

(*c*) in terms of the laws of the foreign State regulating the integrity and correctness of the data or data message and the correctness of the copy or printout.

(5) The provisions of this section do not affect any other law in terms of which data or a data message may be admitted as evidence at any proceedings and the provisions of this section are additional to and not in substitution for, any such law.

CHAPTER 9

GENERAL OBLIGATIONS OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND LIABILITY

General obligations of electronic communications service providers and liability

64. (1) An electronic communications service provider must—

(*a*) take reasonable steps to inform its clients of cybercrime trends which affect or may affect the clients of such an electronic communications service provider;

(*b*) establish procedures for its clients to report cybercrimes with the electronic communications service provider; and

(*c*) inform its clients of measures which a client may take in order to safeguard himself or herself against cybercrime.

(2) An electronic communications service provider that is aware or becomes aware that its computer network or electronic communications network is being used to commit an offence provided for in this Act must—

(*a*) immediately report the matter to the National Cybercrime Centre; and

(*b*) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence, including information which shows the communication‟s origin, destination, route, time date, size, duration and the type of the underlying services.

(3) An electronic communications service provider which fails to comply with subsection (1) or (2), is guilty of an offence and is liable on conviction to a fine of R10 000, for each day on which such failure to comply, continues.

(4) The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice, must make regulations regulating the manner in which an electronic communications service provider must report the use of its computer network or electronic communications network to commit an offence, to the National Cybercrime Centre.

CHAPTER 10

AGREEMENTS WITH FOREIGN STATE

President may enter into agreements

65. (1) The President may, on such conditions as he or she may deem fit, enter into any agreement with any foreign State regarding—

(*a*) the provision of mutual assistance and cooperation relating to the investigation and prosecution of—

(i) an offence under Chapter 2 of this Act;

(ii) any other offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article; or

(iii) an offence—

(*aa*) similar to those contemplated in Chapter 2 of this Act; or

(*bb*) 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 that foreign State;

(*b*) the implementation of cyber threat response activities;

(*c*) research, information and technology-sharing and the development and exchange on cyber security related matters;

(*d*) the protection and securing of National Critical Information Infrastructures;

(*e*) the establishment of 24/7 contact points;

(*f*) the implementation of emergency cross-border response mechanisms to address cyber threats;

(*g*) the reciprocal implementation of measures to curb cybercrime; and

(*h*) the establishment of emergency centres to deal with cyber-related threats.

(2) The Cabinet member responsible for the administration of justice must, as soon as practical after Parliament has agreed to the ratification of, accession to or amendment or revocation of an agreement referred to in subsection (1), give notice thereof in the *Gazette*.

CHAPTER 11

GENERAL PROVISIONS

Repeal or amendment of laws

66. The laws mentioned in the Schedule are hereby repealed or amended to the extent reflected in the third column of the Schedule.

Regulations

67. (1) The Cabinet member responsible for the administration of justice must make regulations, prescribing the—

(*a*) form of the expedited preservation of data direction and the manner in which it must be served by a member of a law enforcement agency as contemplated in section 40(2);

(*b*) form of the disclosure of data direction and the manner in which it must be served by a member of a law enforcement agency as contemplated in section 41(7);

(*c*) form of the preservation of evidence direction and the manner in which it must be served by a member of a law enforcement agency as contemplated in section 42(2);

(*d*) form of the direction as contemplated in section 45(1); and

(*e*) form of the affidavit which must accompany the information furnished to the 24/7 Point of Contact as contemplated in section 48(2)(*b*)(ii).

(2) The Cabinet member responsible for State security must, in consultation with the Cabinet member responsible for the administration of justice, make regulations, prescribing the—

(*a*) form of the report and manner of reporting to the Director-General: State Security as contemplated in section 60(4); and

(*b*) form of the certificate as contemplated in section 60(7).

(3) The Cabinet member responsible for State security must make regulations as contemplated in section 58(5).

Short title and commencement

68. (1) This Act is called the Cybercrimes and Cybersecurity Act, 20..... (Act No. ..... of .....), and comes into operation on a date fixed by the State President by proclamation in the *Gazette*.

(2) Different dates may be fixed under subsection (1) in respect of different provisions of this Act.

Schedule

LAWS REPEALED OR AMENDED

Number and year of law	Short title	Extent of repeal or amendment
Act No. 68 of 1995	South African Police Service Act, 1995	The deletion of section 71.
Act No. 32 of 1998	National Prosecuting Authority Act, 1998	The deletion of sections 40A and 41(4).
Act No. 111 of 1998	Correctional Services Act, 1998	The deletion of section 128.
Act No. 38 of 2001	Financial Intelligence Centre Act, 2001	The deletion of sections 65, 66 and 67.
Act No. 25 of 2002	Electronic Communications and Transactions Act, 2002	(*a*) The amendment of section 1 by the deletion of the definitions of "critical data", "'critical database" and "critical database administrator". (*b*) The deletion of Chapter IX. (*c*) The deletion of sections 85, 86, 87, 88 and 90. (*d*) The substitution for section 89 of the following section: "Penalties **89. [(1)]** A person convicted of an offence referred to in sections 37 (3), 40 (2), 58 (2), 80 (5)**[,]** or 82 (2) **[or 86 (1), (2) or (3)]** is liable to a fine or imprisonment for a period not exceeding 12 months. **[(2) A person convicted of an offence referred to in section 86 (4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.]**.
Act No. 70 of 2002	Regulation of Interception	The addition of the following items

Number and year of law	Short title	Extent of repeal or amendment
	of Communications and Provision of Communication related Information Act, 2002	to the Schedule to the Act: "15 any offence referred to in section 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21(2)(*b*) or 22 (in so far as the attempt, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring to commit offence relates to any of the aforementioned offences) of the Cybercrimes and Cybersecurity Act, 20… (Act …… of ….); and 16 any offence which is substantially similar to an offence referred to in item 15 which is or was committed in a foreign State.".
Act No. 32 of 2007	Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007	(**a**) The insertion of the following section after section 16, in Part 2 of Chapter 3 of the Act: **"Definitions** **16A**. For the purposes of this Part and unless the context indicates otherwise— (*a*) "computer data storage medium" means any article, device or location from which data is capable of being reproduced or on which data is capable of being stored, by a computer device, irrespective of whether the article or

Number and year of law	Short title	Extent of repeal or amendment
		device is physically attached to or connected with the computer device; (*b*) "computer device" means any electronic programmable device used, whether by itself or as part of a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure or any other device or equipment or any part thereof, to perform predetermined arithmetic, logical, routing or storage operations in accordance with set instructions and includes all— (i) input devices; (ii) output devices; (iii) processing devices; (iv) computer data storage mediums; (v) programs; and (vi) other equipment and devices, that are related to, connected with or used with such a device or any part thereof; (*c*) "computer network" means two or more inter-connected or related computer devices, which allows these inter-connected or related computer devices to— (i) exchange data or

Number and year of law	Short title	Extent of repeal or amendment
		any other function with each other; (ii) exchange data or any other function with another computer network; or (iii) connect to an electronic communications network; (*d*) "database" means a collection of data in a computer data storage medium; (*e*) "electronic communications network" means electronic communications infrastructures and facilities used for the conveyance of data; (*f*) "electronic communications service provider" means any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005.". (*b*) The insertion of the

Number and year of law	Short title	Extent of repeal or amendment
		following section after section 20: "**Cybercrimes involving child pornography** **20A.** (1) Any person who unlawfully and intentionally takes steps to procure, obtain or access or in any way, knowingly assists in, or facilitates the procurement, obtaining or accessing of child pornography through a computer network or electronic communications network, is guilty of an offence. (2) Any person who unlawfully and intentionally possesses child pornography on a computer data storage medium, a computer device, a computer network, a database or an electronic communications network, is guilty of an offence. (3) Any person who unlawfully and intentionally produces child pornography for the purpose of making it available, distributing it or broadcasting it by means of a computer network or an electronic communications network, is guilty of an offence. (4) Any person who unlawfully and intentionally— (*a*) makes available, distributes or broadcasts; (*b*) causes to be made available, broadcast or distributed; (*c*) assists in making available, broadcasting or distributing, child pornography by means of a

Number and year of law	Short title	Extent of repeal or amendment
		computer network or an electronic communications network, is guilty of an offence. (5) Any person who unlawfully and intentionally advocates, advertises, encourages or promotes— (*a*) child pornography; or (*b*) the sexual exploitation of children, by means of a computer network or an electronic communications network, is guilty of an offence. (6) Any electronic communications service provider who unlawfully and intentionally— (a) makes available, distributes or broadcasts; (b) causes to be made available, broadcast or distributed; (c) assists in making available, broadcasting or distributing, child pornography through a computer network or an electronic communications network, is guilty of an offence. (7) Any electronic communications service provider who unlawfully and intentionally advocates, advertises, encourages or promotes child pornography or the sexual exploitation of children, is guilty of an offence. (8) Any person who unlawfully and intentionally processes or facilitates a financial transaction, knowing that such transaction will facilitate access to, or the distribution or possession

Number and year of law	Short title	Extent of repeal or amendment
		of, child pornography, by means of a computer network or an electronic communications network, is guilty of an offence. (9) Any person or electronic communications service provider who, having knowledge of the commission of any offence referred to in subsections (1) to (8), or having reason to suspect that such an offence has been or is being committed and unlawfully and intentionally fails to— (*a*) report such knowledge or suspicion as soon as possible to a police official; or (*b*) furnish, at the request of the South African Police Service, all particulars of such knowledge or suspicion, is guilty of an offence. (*c*) The amendment of section 56A of the Act, by the addition of the following subsection: "(3) Any person or electronic communications service provider who contravenes the provisions of section 20A(9), is liable, on conviction to a fine not exceeding R 5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.".