GENERAL NOTICE

NOTICE 888 OF 2012

DEPARTMENT OF COMMUNICATIONS

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS AMENDMENT BILL, 2012

I, Dina Pule, Minister of Communications, hereby publish the proposed Electronic Communications and Transactions Amendment Bill, 2012.

Interested persons are invited to provide written comments on the proposed Bill, within 30 working days of the date of publication of this notice at any of the following addresses:

Post:	For Attention: Ms P Legoze The Director: Cyber Security ICT Infrastructure Development Department of Communications; Private Bag X860 Pretoria 0001;
or deliver to:	First Floor, Block E iParioli Office Park 1166 Park Street Hatfield, Pretoria;
or email to:	palesa@doc.gov.za
or fax to:	0865000562

Please note that comments received after the closing date may be disregarded.

Please contact Palesa Legoze at (012) 427 8036 or Jabu Radebe at (012) 427 8038 for any enquiries.

MS DINA PULE, MP
MINISTER OF COMMUNICATIONS

REPUBLIC OF SOUTH AFRICA

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS AMENDMENT BILL

(As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. XXX of XXX 2012)
(The English text is the official text of the Bill)

(Minister of Communications)

[B -2012]

GENERAL EXPLANATORY NOTE:

[ ] Words in bold type in square brackets indicate omissions from existing enactments.

_____ Words underlined with a solid line indicate insertions in existing enactments.

BILL

To amend the Electronic Communications and Transactions Act, 2002, so as to promote electronic transactions nationally and internationally, recognizing the benefits and efficiency of them; to build confidence in electronic communications by introducing schemes for the accreditation of authentication services and products; to help realize the economic and social benefits that can be derived through the use of authenticated services and products in secure global electronic commerce; to provide further for the use of digital signatures; to prevent abuse of information systems by among other things, cyber crime; to secure the efficient management, issue and protection of South African domain names; to encourage the use of e-government services; and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:-

Amendment of section 1 of Act 36 of 2002

1. Section 1 of the principal Act is hereby amended-

(a) by the insertion of the following definitions prior to the definition of "addressee":

""accreditation" has the meaning set out in section 33;

"Accreditation Authority" means any authority of that name created under Chapter VI;"

(b) by the substitution of the definition of "advanced electronic signature" by the following definition:

""advanced electronic signature" means an electronic signature which [**results from** a **process which**] has been accredited by the Accreditation Authority as provided for in section 37, and which is admissible in legal proceedings;"

(c) by the substitution of the definition of "authentication service provider" by the following definition:

""**authentication service provider**" means a person who or which has been registered and whose authentication products or services have been accredited by the Accreditation Authority under section 37 or recognised under section 40, and who or which may also be a certification service provider;"

(d) by the deletion of the definition of "Authority";

(e) by the insertion of the following definitions after the definition of "certification service provider":

""commercial communication" means a data message sent or received as or as part of or in anticipation of, a commercial electronic transaction;

"commercial electronic transaction" means the sale or purchase of goods or services for consideration, whether between businesses, households, individuals, governments, and/or other public or private organisations, that are conducted over electronic communications networks and/or electronic communications facilities, and include the ordering, payment of consideration for and/or delivery of the goods or service in the same way;

"consideration" shall have the meaning given to it in the Consumer Protection Act;"

(f) by the substitution of the definition of "consumer" by the following definition:

" "consumer" **[means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier]** shall have the meaning given to it in the Consumer Protection Act;"

(g) by the deletion of the definition of "Consumer Affairs Committee";

(h) by the insertion of the definition of "Consumer Protection Act" as follows:

""Consumer Protection Act" means the Consumer Protection Act, 2008 (Act 68 of 2008);"

(i) by the substitution of the definition of "critical information" with the following:

""critical **[data]** information" **[means data that is declared by the Minister in terms of]** shall have the meaning set out in section 53(a) **[to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens]**;"

(j) by the substitution of the definition of "critical information database" with the following:

""critical information **[database]** infrastructure" means a collection of critical **[data]** information that is stored or conveyed in or converted to **[in]** electronic form within an electronic communications network from **[where]** which it may be accessed, reproduced, distributed or extracted;"

(k) by the substitution of the definition of "critical information database administrator" with the following:

""critical information **[database]** infrastructure administrator" means the person responsible for the management and control of **[a critical database]** critical information

infrastructure or national critical information infrastructure;"

(l) by the substitution of the definition of "cryptography product" with the following:

""cryptography product" means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring—
(a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons **[that such data can be accessed only by relevant persons]**;
(b) the authenticity of the data;
(c) the integrity of the data; or
(d) that the source of the data can be correctly ascertained;"

(m) by the substitution of the definition of "cryptography provider" with the following:

""cryptography provider" means any person who provides or who proposes to provide cryptography services or products in the Republic but not end users;"

(n) by the substitution of the definition of "cryptography service" with the following:

""cryptography service" means any service which is provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring—
(a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons;
(b) that the authenticity **[or integrity]** of such data **[or data message is capable of being ascertained]**;
(c) the integrity of the data **[or data measage]**; or
(d) that the source of the data **[or data message]** can be correctly ascertained;"

(o) by the insertion of the following new definitions after the definition of "cryptography service":

""cyber crime" means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them;

"Cyber Security Hub" means the public body formed in terms of section 85A;

"cybersecurity incident" means any event identified as such in terms of the laws and their administration in the Republic, including the National Cyber Security Framework;"

(p) by the deletion of the definition of "data" after the definition of "cyber inspector";

(q) by the substitution of the definition of "data message" with the following:

""data message" means **[data generated, sent, received or stored by electronic means and includes]** electronic communications including—
(a) voice, where the voice is used in an automated transaction; and
(b) any other form of electronic communications stored as a **[stored]** record;"

(r) by the insertion after the definition of "Department" of the following:

""device" means any machine, mechanism, technology or other thing made for electronic communications purposes or for use in electronic communications networks, or both when used together;"

(s) by the substitution of the definition of "electronic agent" with the following:

""electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages, **[or performance in whole or part]** in an automated transaction;"

(t) by the insertion after the definition of "electronic agent" of the following new definitions:

""Electronic Communications Act" means the Electronic Communications Act, 2005 (Act 36 of 2005);

"electronic communications" shall have the meaning given to it in the Electronic Communications Act;

"electronic communications facilities" shall have the meaning given to it in the Electronic Communications Act;

"electronic communications network" shall have the meaning given to it in the Electronic Communications Act;

"electronic communications network services" shall have the meaning given to it in the Electronic Communications Act;"

(u) by the substitution for the definition of "electronic signature" of the following:

""electronic signature" means a sound, symbol or process that is (i) uniquely linked to the signatory; (ii) capable of identifying the signatory; (iii) created using means that the signatory can maintain and which are under his control; (iv) linked to the data to which it relates in such a manner that any subsequent change of the data can be detected; and **[means data attached to, incorporated in, or logically associated with other data and]** (v) **[which is]** intended by the user to serve as a signature;"

(v) by the insertion after the definition of "electronic signature" of the following:

""electronic transaction" shall mean a transaction conducted using electronic communications;"

(w) by the substitution for the definition of "e-mail" of the following:

""e[-]mail" means electronic mail such as a data message used or intended to be used as a **[mail message]** form of correspondence between the originator and addressee **[in an electronic communication]**;"

(x) by the insertion after the definition of "email" the following:

""gTLD" means a generic top level domain as approved by ICANN and in some cases, the Minister as set out in section 64;"

(y) by the insertion after the definition of "ICANN" the following:

""ICASA" means the Independent Communications Authority of South Africa;"

(z) by the substitution for the definition of "information system" the following:

""information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet and electronic communications networks where electronic communications networks are used in the provision of electronic communications network services;"

(aa) by the substitution for the definition of "information system services" of the following:

""information system services" includes the provision of connections, the operation of electronic communications facilities for information systems, the provision of access to information systems and electronic communications networks, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data messages **[at the individual request of the recipient of the services]**;"

(bb) by the substitution for the definition of "Internet" the following:

""Internet" means the **[interconnected system of networks that connects computers around the world using the]** data, communicated through a worldwide network made up of electronic communications facilities using packet-switching technology and communicating through TCP/IP or other identified protocols and includes future versions thereof;"

(cc) by the insertion of new definitions after the definition of "IP address" as follows:

""licensee" shall have the meaning given to it in the Electronic Communications Act;

"JCPS cluster" means the Justice, Crime Prevention and Security cluster or the group of these Ministries by any other name, tasked with the programme of action to make South Africa a safer place for its citizens and in which to do business;"

(dd) by the insertion after the definition of "Minister" the following new definitions:

""national critical information infrastructure" means critical information infrastructure that is fundamental to the effective operation of services that are critical to South Africa such as the national economy, social services, and law enforcement;

"National Cybersecurity Framework" means the National Cybersecurity Policy Framework for South Africa of March 2012, and any legislation, regulations or

guidelines subsequently published in terms of this Policy or by one or more Ministries within the JCPS cluster;"

"non-commercial electronic transaction" means an electronic transaction that does not involve the exchange or payment of consideration;

(ee) by the substitution for the definition of "originator" the following:

""originator" means a person by whom, or on whose behalf, a data message purports to have been sent or generated **[prior to storage, if any]** but does not include a person acting as an intermediary with respect to that data message;"

(ff) by the substitution for the definition of "person" the following:

""person" includes a natural person and any entity recognised as a juristic person and specifically includes a public body;"

(gg) by the substitution for the definition of "personal information" the following:

""personal information" means information **[about]** relating to an identifiable, living, natural person **[individual]**, and where applicable, an identifiable, existing juristic person, including, but not limited to—

(a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person **[individual]**;

(b) information relating to the education or the medical, financial, criminal or employment history of the **[individual or information relating to financial transactions in which the individual has been involved]** person;

(c) any identifying number, symbol, email address, physical address, telephone number or other particular assigned to the person **[individual]**;

(d) the **[address, finger prints or]** blood type or any other biometric information of the person **[individual]**;

(e) the personal opinions, views or preferences of the **[individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual]** person;

(f) correspondence sent by the **[individual]** person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person **[individual]**; and

(h) **[(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and]**

(i) the name of the person **[individual where]** if it appears with other personal information relating to the person **[individual]** or if the disclosure of the name itself would reveal additional information about the person **[individual]**;"

(hh) the substitution for the definition of "**private body**" of the following:

""private body" means—
(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
(b) a partnership which carries or has carried on any trade, business or profession; or
(c) any former or existing juristic person,
but **[not]** excludes a public body;"

(ii) the substitution for the definition of "registrant" of the following:

""registrant" means **[an applicant for or]** a holder of a domain name;"

(jj) by the substitution for the definition of "registrar" of the following:

""registrar" means an entity which is licensed by **[the Authority]** ,zadna to register ,za domain names on behalf of registrants and update [a] the repository with the name of the registrant;"

(kk) by the substitution for the definition of "registry" of the following:

""registry" means **[an]** the central registry which is an entity licensed by the Authority to manage and administer **[a specific]** subdomains and to operate the repository for the domain names;"

(ll) by the substitution of the definition of "repository" with the following:

" "repository" means the primary register of the information maintained by **[a]** the central registry including domain names, registrant name and contact information, registrar name and contact information, zone records, registration and renewal dates and all other data submitted by registrars concerning domain names as may be prescribed in the domain name registration agreement under section 68;"

(mm) by the substitution for the definition of "**second level domain**" of the following:

""second level domain" means the subdomain immediately following the ccTLD as determined by ICANN;"

(nn) by the insertion of a new definition after the definition of "subdomain" as follows:

""supplier" shall have the meaning set out in section 1 of the Consumer Protection Act;"

(oo) by the substitution for the definition of "TCP/IP" of the following:

""TCP/IP" means the **[Transmission]** Transport Control Protocol and/or Internet Protocol used to communicate data by means of **[and to connect to]** the Internet;"

(pp) by the substitution for the definition of "TLD" of the following:

""TLD" means a top level domain of the domain name system as determined by ICANN;"

(qq) by the substitution for the definition of "third party" of the following:

""third party", in relation to a service provider, means a subscriber to the service provider's services or any other user of the service provider's services or a user of information systems or electronic communications network services;"

(rr) by the deletion of "transaction";

(ss) by the insertion after the definition of "transaction" of the following new definition:

""unsolicited communication" shall, in relation to a data message regarding goods or services, mean that the data message has been transmitted to a consumer by or on behalf of a supplier without the consumer having expressly or implicitly requested that data message;"

(tt) by the deletion of the definitions of "universal service" and "WAP";

(uu) by the substitution for the definition of "web page" of the following:

""web page" means any page or other construct of data available on a web site other than a home page **[a data message on the World Wide Web]**;"

(vv) by the insertion of new definitions after the definition of "website" as follows:

""wireless application service" means applications that use wireless technologies and includes Internet access from a wireless device;

"wireless application service provider" means any person engaged in the provision of a wireless application service to any member or members of the public who concludes an agreement with a licensee authorizing and enabling the provision of such services;"

(ww) by the substitution for the definition of the "World Wide Web" of the following:

""World Wide Web" means an information browsing framework that allows a user to locate and access information stored on a remote **[computer]** device and to follow references from one **[computer]** device to related information on another **[computer]** device;"

(xx) by the insertion of a new definition after the definition of "World Wide Web" as follows:

"".zadna" means the .za Domain Name Authority created under Chapter X to administer the .za domain name space;"

Amendment of section 2 of Act 25 of 2002

2. Section 2 of the principal Act is hereby amended by the substitution for paragraph (1) of the following paragraph:

"(1) The objects of this Act are to enable and facilitate electronic **[communications and]** transactions in the public interest, and for that purpose to—

(a) recognise the importance of the information economy for the economic and social prosperity of the Republic;

[(b) promote universal access primarily in underserviced areas;]

(c) promote the understanding and acceptance of and growth in the number of electronic **[communications and]** transactions in the Republic;

(d) remove and prevent barriers to electronic **[communications and]** transactions in the Republic;

(e) promote legal certainty and confidence in respect of electronic transactions;

[(f) promote technology neutrality in the application of legislation to electronic communications and transactions;]

(f) **[(g)]** promote e-government services and electronic **[communications and]** transactions with public and private bodies, institutions and citizens;

(g) **[(h)]** ensure that electronic transactions in the Republic conform to the highest international standards;

(h) **[(i)]** encourage investment and innovation in respect of electronic transactions in the Republic;

(i) **[(j)]** develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;

(j) **[(k)]** promote the development of electronic transactions services which are responsive to the needs of users and consumers;

[(l) ensure that, in relation to the provision of electronic transactions services, the special needs of particular communities and, areas and the disabled are duly taken into account;]

(k) **[(m)]** ensure compliance with accepted International technical standards in the provision and development of electronic communications and transactions;

(l) **[(n)]** promote the stability of electronic transactions in the Republic;

(m) **[(o)]** promote the development of human resources in the electronic transactions environment;

(n) **[(p)]** promote SMMEs within the electronic transactions environment;

(o) **[(q)]** ensure efficient use and management of the .za domain name space; and

(p) **[(r)]** ensure that the national interest of the Republic is not compromised through the use of electronic **[communications]** transactions."

Amendment of section 5 of Act 25 of 2002

3. Section 5 of the principal Act is hereby amended –

(a) by the substitution for paragraph (1) of the following paragraph:

"(1) The Minister must, within 24 months after the promulgation of this Electronic Communications and Transactions Amendment Act, 2012, develop a three-year national e-strategy for the Republic, which must be submitted to the Cabinet for approval."

(b) by the substitution for paragraph (3)(e) of the following paragraph:

"(e) may conduct research into and keep abreast of developments relevant to electronic **[communications and]** transactions in the Republic **[and internationally]**;"

(c) by the substitution for paragraph (3)(g) of the following:

"(g) may liaise, consult and cooperate with public bodies, the private sector or any other person; **[and]**"

(d) by the addition after subsection (3)(h) of the following additional sub-sections:

"(i) must take account of the nature, scope and impact of electronic transactions;

(j) must take account of international best practice and conformity with the law and guidelines of other jurisdictions and international bodies; and

(k) must take into account existing laws and their administration in the Republic, including the National Cybersecurity Framework."

(e) by the deletion of subsection (ii) of subsection (4)(c) and the renumbering of the remaining subsections.

Deletion of sections 6 and 7 of Act 25 of 2002

4. Sections 6 and 7 of the principal Act are hereby deleted.

Amendment of section 8 of Act 25 of 2002

5. Section 8 of the principal Act is hereby amended:

(a) by the substitution for subsection (1) of the following:

"(1) The Minister, in developing **[the]** national **[e-strategy]** policy in terms of section 10, must provide for ways of promoting development of human resources **[set out in this section]** within the context of the government's integrated human resource development strategies, having regard to structures and programmes that have been established under existing laws, and having regard to the need for technical skills to support the initiatives proposed under the National Cybersecurity Framework."

(b) by the substitution of subsection (3)(g) with the following:

"(g) **[convergence between communication technologies affecting electronic transactions]** cyber security;"

Deletion of section 9 of Act 25 of 2002

6. Section 9 of the principal Act is hereby deleted.

Amendment of section 10 of Act 25 of 2002

7. Section 10 of the principal Act is hereby amended:

(a) by the substitution for section 10 of the following paragraph:

"(1) The Minister **[must]** may, subject to this Act, formulate electronic transactions policy.

(2) In formulating the policy contemplated in subsection (1), the Minister must—

(a) act in consultation with members of the Cabinet directly affected by such policy formulation or the consequences thereof; and
(b) have due regard to [—
(i)] the objects of this Act[;].
[(ii) the nature, scope and impact of electronic transactions;
(iii) international best practice and conformity with the law and guidelines of other jurisdictions and international bodies; and
(iv) existing laws and their administration in the Republic.]

(3) The Minister must publish policy guidelines in the *Gazette* on issues relevant to electronic transactions in the Republic including alignment with any e-identity or public key infrastructure strategy developed in terms of the National Cybersecurity Framework.
(4) In implementing this Chapter, the Minister must encourage the development of innovative information systems and the growth of related industry, the promotion of SMMEs, and the development of human resources to advance electronic transactions and other matters under this Act."

Amendment of section 11 of Act 25 of 2002
8. Section 11 of the principal Act is hereby amended by the substitution for subsection (3) of the following paragraph:

"(3) Information incorporated into an agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is—
(a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and
(b) accessible in a form in which it may be read, stored and retrieved by the other party; and
(c) accessible, whether electronically or as a computer printout, as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it."

Amendment of section 15 of Act 25 of 2002
9. Section 15 of the principal Act is hereby amended by the substitution for subsection (3) of the following paragraphs:

"(3) In assessing the evidential weight of a data message, regard must be had to—
(a) the reliability of the manner in which the data message was generated, stored or communicated;
(b) the reliability of the manner in which the integrity of the data message was maintained;
(c) the manner in which its originator was identified which may include by way of electronic signature; and
(d) any other relevant factor."

Amendment of section 23 of Act 25 of 2002
10. Section 23 of the principal Act is hereby amended by the substitution of subsection (c) by the following paragraph:

"(c) regardless of the device, **[must]** will be regarded as having been sent from the originator's usual place of business or residence and as having been received at the addressee's usual place of business or residence."

Amendment of section 28 of Act 25 of 2002

11. Section 28 of the principal Act is hereby amended:

(a) by the substitution for subsection (1) with the following paragraph:

"(1) In any case where a public body performs any of the functions referred to in section 27, such body may specify by notice in the *Gazette*—
(a) the manner and format in which the data messages must be filed, created, retained or issued;
(b) in cases where the data message has to be signed, the type of electronic signature or advanced electronic signature required;
(c) the manner and format in which such electronic signature or advanced electronic signature must be attached to, incorporated in or otherwise associated with the data message;
(d) the identity of or criteria that must be met by any authentication service provider used by the person filing the data message **[or that such authentication service provider must be a preferred authentication service provider]**;
(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and
(f) any other requirements for data messages or payments.

(b) by the substitution for subsection (2) with the following paragraph:

"(1) For the purposes of subsection (1)(d) the South African Post Office Limited is a preferred authentication service provider and the Minister may designate any other **[authentication service provider]** public body as an **[preferred]** authentication service provider based on such authentication service provider's **[obligations in respect of the provision of universal service]** compliance with the conditions for accreditation set out in section 38."

Insertion of section 28A in Act 25 of 2002

12. The following section is hereby inserted in the principal Act after section 28:

"Objectives of this Chapter

28A. The purpose of this Chapter and the registration of cryptography providers is to-

(a) enable responses to requests for mandatory and lawful access to encrypted real-time communications or encrypted stored data including any data message;

(b) address the challenges posed by the international use of cryptography products when seeking information pursuant to or in anticipation of an investigation in terms of the Regulation of Interception of Communications and Provision of Communications-Related Information Act, 2002 (Act No. 70 of 2002); and
(c) enable liaison with the JCPS cluster in relation to the development of capacity and standards in this regard."

Amendment of section 28 of Act 25 of 2002

13. Section 28 of the principal Act is hereby amended by the substitution of subsection (2) with the following paragraph:

"(2) The Director-General must record the following particulars in respect of a cryptography provider in that register:
(a) the name and address of the cryptography provider;
(b) a description of the type of cryptography service or cryptography product being provided;
(c) a description of the purpose to which that cryptography service or cryptography product or both will be put;
(d) information regarding the country of origin from which the cryptography product is imported and where manufactured or otherwise produced in South Africa, the same details are required in relation to the manufacturer or producer; and
[(c)](e) such other particulars as may be prescribed to identify and locate the cryptography provider or its products or services adequately."

Amendment of section 29 of Act 25 of 2002

14. Section 29 of the principal Act is hereby amended:

(a) by the substitution for subsection (3) of the following paragraph:

"(1) A cryptography provider **[is not required to disclose confidential information or trade secrets in respect of its cryptography services or services]** may, in addition to the provisions of section 32 or otherwise, be de-registered-
(a) for failure to adhere to any provision of this Act; or
(b) if the conduct of the cryptography provider is objectively determined by the Director General to be detrimental to the users of cryptography products and services."

(b) by the insertion of new subsections (4), (5) and (6) as follows:

"(4) A cryptography provider shall comply with the standards prescribed by the Minister in regulations from time to time and shall also comply with any decryption direction, entry warrant or other court order issued under the Regulation of Interception of Communications and Provision of Communication-related information Act, 2002 or any other laws of the Republic.

(5) The Director General shall require each cryptography provider to renew its registration every 2 years, by completing the prescribed forms and adhering to the prescribed renewal procedure which shall be no more onerous than the registration procedure.

(6) The Director General may refuse renewal for reasons of national security or a failure to comply with the renewal procedure."

Amendment of section 30 of Act 25 of 2002

15. Section 30 of the principal Act is hereby amended by the substitution for subsection (3)(a) of the following paragraph:

"(a) to or from premises in the Republic;"

Amendment of section 32 of Act 25 of 2002

16. Section 32 of the principal Act is hereby amended by the substitution for subsection (2) of the following paragraph:

"(2) A person who contravenes or fails to comply with a provision of this Chapter is guilty of an offence and liable on conviction to a fine up to a maximum of R2 million or to imprisonment for a period not exceeding 2 years."

Amendment of section 33 of Act 25 of 2002

17. Section 33 of the principal Act is hereby amended by the substitution for section 33 of the following paragraph:

"33. In this Chapter, unless the context indicates otherwise—
"accreditation" means recognition of an authentication product or service and registration of an authentication service provider or a certification service provider by the Accreditation Authority."

Amendment of section 35 of Act 25 of 2002

18. Section 35 of the principal Act is hereby amended:

(a) by the amendment of the heading in the following way:

"Accreditation [to be voluntary]"

(b) by the substitution for section 35 of the following:

"35.**[Subject to section 30, a]** No person may, without **[the prior authority of any other person]** being registered by the Authentication Authority under section 37, sell or provide authentication products or services in the Republic."

Amendment of section 36 of Act 25 of 2002

19. Section 36 of the principal Act is hereby amended by the substitution for subsection (2) of the following paragraph:

"(2) The Accreditation Authority must maintain a publicly accessible **[database]** register in respect of—
(a) authentication products or services accredited in terms of section 37;
(b) authentication products and services recognised in terms of section 40; **[and]**
(c) revoked accreditations or recognitions; and

(d) an authentication service providers and a certification service providers in terms of section 37 and section 38; and
[d](e) such other information as may be prescribed."

Amendment of Part 2 of Chapter VI of Act 25 of 2002
20. Part 2 of Chapter VI of the principal Act is hereby amended:

(a) by the substitution for the heading of it by the following:

"Accreditation and registration"

(b) by the amendment of the heading of section 37 as follows:

"Accreditation and registration of authentication products and services"

(c) by the substitution for section 37(1) by the following paragraph:

"(1) The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures and must then enter the details of the authentication service provider or certification service provider as the case may be, in the register."

(d) by the substitution for section 37(3) by the following paragraph:

"(3) A person falsely holding out its products or services to be accredited and registered by the Accreditation Authority is guilty of an offence and liable on conviction to a fine not exceeding R 2 million or imprisonment for a period not exceeding 2 years."

(e) by the amendment of the heading of section 38 as follows:

"Criteria for accreditation and registration"

(f) by the amendment of section 38 by the substitution for subsections (1) and (2) of the following paragraphs:

"38(1) The Accreditation Authority may not accredit authentication products or services or register an authentication service provider or certification service provider unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate—
(a) is uniquely linked to the user;
(b) is capable of identifying that user;
(c) is created using means that can be maintained under the sole control of that user;
(d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable; and
(e) is based on the face-to-face identification of the user.
(2) For purposes of subsection (1), the Accreditation Authority must have regard to the following factors in respect of an authentication service provider prior to accrediting authentication products or services and registering the provider:

(a) Its financial and human resources, including its assets;
(b) the quality of its hardware and software systems;
(c) its procedures for processing of products or services;
(d) the availability of information to third parties relying on the authentication product or service;
(e) the regularity and extent of audits by an independent body;
(f) the factors referred to in subsection (4) where the products and services are rendered by a certification service provider; and
(g) any other relevant factor which may be prescribed."

(g) by the amendment of section 38 by the substitution for subsection (5) of the following paragraph:

"(5) The Accreditation Authority may impose any conditions or restrictions necessary when accrediting an authentication product or service and registering the authentication service provider or certification service provider."

(h) by the amendment of section 38 by the insertion of a new subsection (6) as follows:

"(6) The Minister may give the Accreditation Authority instructions under the National Cyber Security Framework from time to time, so as to align the activities of the Authority with any guidelines and principles under the Framework."

(i) by the amendment of the heading of section 39 as follows:

"Revocation, renewal or termination of accreditation and registration"

(j) by the substitution for section 39 of the following paragraphs:

"39(1) The Accreditation Authority may suspend or revoke an accreditation and registration if it is satisfied that the authentication or certification service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40.
(2) Subject to the provisions of subsection (3), the Accreditation Authority may not suspend or revoke the accreditation or recognition contemplated in subsection (1) unless it has—
(a) notified the authentication or certification service provider in writing of its intention to do so;
(b) given a description of the alleged breach of any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40; and
(c) afforded the authentication or certification service provider the opportunity to—
(i) respond to the allegations in writing; and
(ii) remedy the alleged breach within a reasonable time.
(3) The Accreditation Authority may suspend accreditation and registration granted under section 38 or recognition given under section 40 with immediate effect for a period not exceeding 90 days, pending implementation of the procedures required by subsection (2), if the continued accreditation or recognition of the authentication or certification service provider is reasonably likely to result in irreparable harm to

consumers or any person involved in an electronic transaction in the Republic.
(4) An authentication or certification service provider whose products or services have been accredited and registered in terms of this Chapter may terminate such accreditation and registration at any time, subject to such conditions as may be agreed to at the time of accreditation or thereafter."

(k) by the insertion of new subsections (5) and (6) in section 39 as follows:

"(5) Each authentication or certification service provider shall renew its own registration and registration of its products and services every 2 years by completing the prescribed forms and adhering to the prescribed renewal procedure which shall be no more onerous than the registration procedure.
(6) The Director General may refuse renewal for reasons of national security or a failure to comply with the renewal procedure."

(l) by substituting the heading of section 40 as follows:

"**Accreditation and registration of foreign products and services**"

(m) by substituting subsection (1) of section 40 with the following paragraph:

"(1) The Minister may, by notice in the *Gazette* and subject to such conditions as may be determined by him or her -
(a) recognise the accreditation or similar recognition granted to any authentication or certification service provider or its authentication products or services in any foreign jurisdiction; and
(b) recognise the electronic signature of any foreign certification service provider provided that such electronic signature is compliant with the requirements for certification or an equivalent procedure, in that foreign jurisdiction which are furthermore equivalent to the requirements for accreditation under this Act. "

(n) by inserting new subsections (2), (3) and (4) in section 40 as follows:

"(2) The Accreditation Authority may conclude agreements with any equivalent institution in a foreign jurisdiction with responsibility for the accreditation and registration of certification service providers or authentication service providers or both, regarding the criteria that may apply for recognition of the electronic signature of a foreign certification service provider by the Minister or the recognition of the electronic signature of a South African certification service provider by a foreign jurisdiction as the case may be.
(3) The Accreditation Authority shall recommend to the Minister the conditions on which he or she may recognise an authentication and certification service provider and the criteria that may apply to registration.
(4) The foreign certification service provider shall nonetheless comply with the other provisions of this Chapter VI."

(o) by renumbering former subsection (2) of section 40 as subsection (5) and substituting it with the following paragraph:

"(5) **[(2)]** An authentication service provider falsely holding out its products or services to have been recognised by the Minister in terms of subsection (1), is guilty of an offence

and liable on conviction to a fine not exceeding R 1 million or imprisonment for a period not exceeding 1 year."

(p) by substituting the heading of section 41 with the following heading:

"Accreditation and registration regulations"

(q) by substituting section 41 with the following paragraph:

"41. The Minister may make regulations in respect of—
(a) the rights and obligations of persons relating to the provision of accredited products and services and authentication and certification service providers;
(b) the manner in which the Accreditation Authority must administer and supervise compliance with those obligations;
(c) the procedure pertaining to the granting, suspension and revocation of accreditation and registration;
(d) fees to be paid;
(e) information security requirements or guidelines; and
(f) any other relevant matter which it is necessary or expedient to prescribe for the proper implementation of this Chapter."

Amendment of section 42 of Act 25 of 2002
21. Section 42 of the principal Act is hereby amended:

(a) by the substitution for subsection (1) of the following paragraph:

"(1) This Chapter applies only to electronic transactions. Unless otherwise indicated, it shall apply in addition to the provisions of any other national law."

(b) by the deletion of subsection (3).

Amendment of section 43 of Act 25 of 2002
22. Section 43 of the principal Act is hereby amended:

(a) by the substitution for subsection (4)(a) of the following paragraph:

"(4) If a transaction is cancelled in terms of subsection (3)—
(a) the consumer must return any goods delivered or other [**the**] performance of the supplier or, where applicable, cease using the services performed; and"

Amendment of section 45 of Act 25 of 2002
23. Section 45 of the principal Act is hereby amended:

(a) by the substitution for section 45 of the following paragraph:

"(1). **[Any person who sends unsolicited commercial communications to consumers, must provide the consumer—**
(a) with the option to cancel his or her subscription to the mailing list of that person; and
(b) with the identifying particulars of the source from which that person obtained

the consumer's personal information, on request of the consumer] No person may send unsolicited communications without the permission of the consumer to whom those unsolicited communications are to be sent or are in fact sent.
(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.
(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to **[the penalties prescribed in section 89(1)]** a fine not exceeding R1 million or imprisonment for a period not exceeding 1 year.
[(4) Any who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).]"

Amendment of section 46 of Act 25 of 2002
24. Section 46 of the principal Act is hereby amended by the substitution for section 46 of the following paragraph:

"(1) The supplier must execute the **[order]** electronic transaction **within** 30 days after the day on which **the [supplier received the order]** transaction is entered into, unless the parties have agreed otherwise.
(2) Where a supplier has failed to execute the **[order]** electronic transaction within 30 days or within the agreed period, the consumer may cancel the agreement with seven days' written notice and the consumer shall be entitled to a full refund of any prior payment, which refund must be made within 30 days of the date of cancellation.
(3) If a supplier is unable to perform the transaction in terms of the agreement on the grounds that the goods or services ordered are unavailable, the supplier must immediately notify the consumer of this fact and refund any payments within 30 days after the date of such notification."

Deletion of section 49 of Act 25 of 2002
25. Section 49 of the principal Act is hereby deleted.

Amendment of section 50 of Act 25 of 2002
26. Section 50 of the principal Act is hereby amended by the substitution for subsection (2) of the following paragraph:

"(2) A data controller **[may voluntarily]** shall subscribe to the principles outlined in section 51 **[by recording]** and must record such fact in an**[y]** agreement with a data subject."

Amendment of Chapter IX of Act 25 of 2002
27. Chapter IX of the principal Act is hereby amended:

(a) by the substitution of the heading of Chapter IX by the following heading:

"PROTECTION OF CRITICAL INFORMATION [DATABASES] AND CRITICAL INFORMATION INFRASTRUCTURE"

(b) by the substitution for the heading of section 52 with the following heading:

"Scope of critical [database] information infrastructure protection"

(c) by the substitution for section 52 with the following paragraph:

"The provisions of this Chapter only apply to a critical [database] information infrastructure administrator and critical [databases] information infrastructure or parts thereof."

(d) by the substitution for the heading of section 53 of the following heading:

"Identification of critical [data] information and national and other critical [databases] information infrastructure"

(e) by the substitution for section 53 of the following paragraph:

"53. The Minister may by notice in the *Gazette*—
(a) declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical [data] information for the purposes of this Chapter; and
(b) establish procedures to be followed in the identification of national critical [databases] information infrastructure for the purposes of this Chapter."

(f) by the substitution for the heading of section 54 the following heading:

"Registration of critical [databases] information infrastructure"

(g) by the substitution for section 54 of the following paragraph:

"54. (1) The Minister may by notice in the *Gazette* determine—
(a) requirements for the registration of national or other critical [databases] information infrastructure with the Department or such other body as the Minister may specify;
(b) procedures to be followed for registration; and
(c) any other matter relating to registration.
(2) For purposes of this Chapter, registration of [a critical database] national or other critical information infrastructure means recording the following information in a register maintained by the Department or by such other body as the Minister may specify:
(a) The full name, address and contact details of the critical [database] information infrastructure administrator;
(b) the location of the [critical database] national or other critical information infrastructure, including the locations of component parts thereof where [a critical database] it is not stored at a single location; and
(c) a general description of the categories or types of information stored in [critical database excluding] the national or other critical information infrastructure but not including the contents of such [critical databases] national or other critical information infrastructure."

(h) by the substitution for the heading of section 55 with the following heading:

"Management of critical [databases] information infrastructure"

(i) by the substitution of section 55(1) and section 55(2) with the following paragraphs:

"55. (1) The Minister may prescribe minimum standards or prohibitions in respect of—

(a) the general management of national or other critical [**databases**] information infrastructure;
(b) access to, transfer and control of national or other critical [**databases**] information infrastructure;
(c) [**infrastructural or**] procedural or other rules and requirements for securing the integrity and authenticity of critical [**data**] information;
(d) procedures and technological methods to be used in the storage or archiving of critical [**databases**] information;
(e) disaster recovery plans in the event of loss of national or critical [**databases**] information infrastructure or parts thereof; and
(f) any other matter required for the adequate protection, management and control of national or other critical [**databases**] information infrastructure.
(2) In respect of national or other critical [**databases**] information infrastructure administered by public bodies, all [**regulations**] standards or prohibitions contemplated in subsection (1) must be made in consultation with all members of the Cabinet affected by the provisions of this Chapter, Provided that the Minister must not record information contemplated in section 54(2) if that information could reasonably compromise—
(a) the security of such [**databases**] national or other critical information infrastructure; or
(b) the physical safety of a person in control of the national or other critical [**databases**] information infrastructure."

(j) by the substitution for subsection (2) of section 56 of the following paragraph:

"(2) Subsection (1) does not apply in respect of information which is disclosed—
(a) to a relevant authority which is investigating a criminal offence or for the purposes of any criminal proceedings;
(b) to government agencies responsible for safety and security in the Republic pursuant to an official request;
(c) to a cyber inspector or independent auditor for purposes of section 57;
(d) pursuant to sections 11 and 30 of the Promotion of Access to Information Act, 2000; or
(e) for the purposes of any civil proceedings which relate to the critical [**data**] information or parts thereof."

(k) by the substitution for subsection (1) of section 57 of the following paragraph:

"(1) The Director-General may, from time to time, cause audits to be performed at the facilities of a critical [**database**] information infrastructure administrator to evaluate compliance with the provisions of this Chapter."

(l) by the substitution for section 58 of the following paragraph:

"(1) Should the audit contemplated in section 57 reveal non-compliance by the critical [**database**] information infrastructure administrator with this Chapter, the Director-General must notify the critical [**database**] information infrastructure administrator thereof in writing, stating—
(a) the finding of the audit report;
(b) the action required to remedy the non-compliance; and
(c) the period within which the remedial action must be performed.
(2) A critical [**database**] information infrastructure administrator that fails to take the remedial action within the period stated in the notice is guilty of an offence and liable, (i)

together with the chief executive officer or equivalent executive on conviction to a maximum fine of R5 million or imprisonment for a maximum period of 3 years, and (ii) together with the accounting officer in the case of national critical information infrastructure, on conviction to a maximum fine of R5 million or imprisonment for a maximum period of 3 years."

Amendment of section 59 of Act 25 of 2002

28. Section 59 of the principal Act is hereby amended by the substitution for section 59 of the following paragraph:

"A juristic person **[to be]** known as the .za Domain Name Authority **[is hereby]** has been established for the purpose of assuming responsibility for the .za domain name space **[as from a date determined by the Minister by notice in the *Gazette* and by notifying all relevant authorities]**."

Amendment of section 60 of Act 25 of 2002

29. Section 60 of the principal Act is hereby amended:

(a) by the substitution of the heading of section 59 by the following heading:

"Incorporation of [the Authority] .zadna"

(b) by the deletion of subsection (1) of section 59 and renumbering of that section;

(c) by the substitution for subsections (2) to (3) with the following paragraphs, renumbered subsections (1) and (2):

"**[(2)]**(1)(a) All citizens and permanent residents of the Republic are eligible for membership of **[the Authority]** .zadna and must be registered as members upon application and on payment of a nominal fee to cover the cost of registration of membership provided that they **[without having to]** comply with any formality determined to be reasonably appropriate by the Minister in regulations from time to time and provided that any applicant for membership shall submit at least his or her full identity and contact information to .zadna.
(b) .zadna may admit as members juristic persons that are registered in South Africa or that carry on a substantial part of their business in South Africa provided that the juristic person shall comply with any formality determined to be reasonably appropriate by the Minister in regulations from time to time.
(2) **[(3)]** For the purpose of the incorporation of **[the Authority]** .zadna a person representing the Minister and the members of Namespace ZA as at the date of application for incorporation must be deemed to be members of **[the Authority]** .zadna."

Amendment of section 61 of Act 25 of 2002

30. Section 61 of the principal Act is hereby amended:

(a) by the substitution of the heading of section 61 by the following heading:

"[Authority's] .zadna memorandum and articles of association"

(b) by the substitution of subsections (1) and (2) with the following paragraphs:

"(1) The memorandum of association and articles of association of **[the Authority]** .zadna must be consistent with national legislation provided that the provisions of this Chapter shall take precedence over any national legislation with a contrary provision. **[and, except where this Chapter provides to the contrary, also with the Companies Act, 1973 (Act No. 61 of 1973).]**
(2) **[Notwithstanding the Companies Act, 1973, an amendment to the memorandum of association or articles of association affecting any arrangement made by any provision of this Chapter, does not have any legal force and effect unless]** [t]The Minister's consent to any amendment to the memorandum or articles of association must be obtained **[has consented]** in writing prior to implementing [to] such an amendment, which consent may not be withheld unreasonably."

(c) by the substitution of subsection (3) with the following paragraph:

"(3) No fee is payable **[in terms of the Companies Act, 1973]** in respect of the reservation of the name of the company, the registration of the said memorandum and articles and the issue of the certificate to commence business."

(d) by the substitution of subsections (4)(a) to (l) with the following paragraph:

"**(4)** The memorandum and articles of association of **[the Authority]** .zadna must, amongst others, and subject to section 62, provide for—
(a) the rules for the convening and conducting of meetings of the Board, including the quorum required for and the minutes to be kept of those meetings;
(b) the manner in which decisions are to be made;
(c) the establishment of any division of **[the Authority]** .zadna to perform specialised functions;
(d) the establishment and functioning of committees, including a management committee which shall comprise only members of the board, a majority of whom should be non-executive directors who shall be independent;
(e) the co-opting by the Board or a committee of any person to assist **[the Authority]** .zadna or a committee in the consideration of any particular matter;
(f) the preparation by the Board of an annual business plan in terms of which the activities of **[the Authority]** .zadna are planned annually;
(g) the banking and investment of funds by the Board;
(h) provisions to regulate the manner in which, and procedures whereby, expertise from any person is obtained in order to further the objects of **[the Authority]** .zadna;
(i) the determination through arbitration of any dispute concerning the interpretation of the memorandum and articles of association of **[the Authority]** .zadna;"

Amendment of Part 2 of Chapter X of Act 25 of 2002
31. Section 62 of the principal Act is hereby amended:

(a) by the substitution for the heading of Part 2 by the following heading:

"Governance and staffing of [Authority] .zadna"

(b) by the substitution for the heading of section 62 by the following heading:

"Board of directors of [the Authority] .zadna"

(c) by the substitution for subsections (1) and (2) of section 62 with the following paragraphs:

"(1) **[The Authority]** .zadna is managed and controlled by a Board of Directors consisting of nine directors, one of whom is the chairperson.
(2) The process of appointment of directors is the following-
(a) The Minister must appoint an independent selection panel consisting of five persons, who command public respect for their fair-mindedness, wisdom and understanding of issues concerning the Internet, culture, language, academia and business, the names of whom must be placed in a notice in the *Gazette*;
(b) the Minister must invite nominations for members of the Board from the public through newspapers which have general circulation throughout the Republic, on-line news services, radio and by notice in the *Gazette*;
(c) nominations must be made to the panel established in terms of paragraph (a);
(d) the panel must recommend to the Minister names of nine persons to be appointed to the Board taking into account the sectors of stakeholders listed in subsection (3)(b);
(e) if the Minister is not satisfied that the recommendations of the panel comply with subsection (3) the Minister may request the panel to review its recommendations and make new ones;
(f) the Minister must appoint the members of the Board, and publish the names of those appointed in the *Gazette*;
(g) the Minister must appoint the Chairperson of the Board from among the names recommended by the panel, who shall hold office for a period of four years. "

(d) by the substitution for subsection (5) of section 62 with the following paragraph:

"(5) All directors serve in a part-time capacity and a majority of the directors shall serve in a non-executive capacity although the chief executive officer and the director responsible for finance shall be executive directors."

(e) by the insertion of new subsections (10), (11) and (12) at the end of section 62 as follows:

"(10) The Board members shall act in good faith in the best interests of .zadna, taking account of the legitimate interests of its stakeholders, and shall exercise the required degree of care, skill and diligence, avoiding conflicts of interest.
(11) Directors shall hold office for a period of three years.
(12) The Board may establish a committee with responsibility for conducting regular and rigorous audits of the business of .zadna, which may include independent third parties, to assess effectiveness of internal controls and risk management within .zadna".

(f) by the substitution of the heading of section 63 with the following heading:

"Staff [of the Authority]"

(g) by the substitution for section 63 of the following paragraph:

"63. (1) The chief executive officer of [the **Authority**].zadna appointed by the Board must perform any work incidental to the functions of **[the Authority]** .zadna.
(2) The chief executive officer must [**be assisted by**] appoint suitable staff [**appointed by the Board**] to assist him or her.

(3) The Board must determine the conditions of service, remuneration and service benefits of the chief executive officer and the staff.
(4) If the chief executive officer is for any reason unable to perform his or her functions, the Board may designate a person in the service of **[the Authority]** .zadna to act as the acting chief executive officer until the chief executive officer is able to resume office."

Amendment of Part 3 of Chapter X of Act 25 of 2002
32. The heading of Part 3 of the principal Act is hereby amended:

(a) by the substitution of the heading of Part 2 by the following heading:

"Functions of [the Authority] .zadna"

(b) by the substitution of the heading of section 64 with the following heading:

"Licensing of registrars [and registries], creation of central registry"

(c) by the substitution of subsections (1), (2) and (3) of section 64 with the following paragraphs:

"(1) No person except .zadna may update a repository or administer a **[second level]** domain unless such person is licensed to do so by **[the Authority]** .zadna.
(2) An application to be licensed as a registrar **[or registry]** must be made in the **[prescribed]** manner and subject to the payment of **[prescribed]** fees as determined by .zadna.
(3) **[The Authority]**.zadna must determine **[apply the prescribed]** conditions and criteria to be used when evaluating an application referred to in subsection (2)."

(d) by the insertion of new subsections (4), (5), (6) and (7) in section 64 as follows:

"(4) There shall be only one central registry of all domain names.
(5) No person may use, license or apply for registration anywhere in the world of a geographic or cultural gTLD that is uniquely South African without the written permission of the Minister, which gTLD may by way of example, include any reference to or be the same as a South African national language, a South African place name, a South African heritage site, a South African historical event, a South African product or service, or a South African national team or national representative of any kind.
(6)The Minister may publish guidelines from time to time regarding the way in which an application may be made and the criteria that will be taken into account in determining whether or not to grant permission under section 64(5), having regard to the public interest.
(7) Failure to comply with the provisions of subsection (5) shall render the person liable on conviction to a fine not exceeding R2 million or imprisonment for period of not more than 2 years."

(e) By the substitution of the heading of section 65 with the following heading:

"[Functions]Powers and duties of [the Authority] .zadna"

(f) by the substitution of section 65 with the following paragraphs:

"(1) **[The Authority]** .zadna must—
(a) administer and manage the .za domain name space;
(b) comply with international best practice in the administration of the .za domain name space;
[(c) license and regulate;]
[(d)] (c) license and regulate registrars for the **[respective registries]** central registry; **[and]**
[(e)] (d) update and maintain the central registry and perform any function necessary to ensure the proper functioning of the .za domain name space, including a second level domain in the event that a licensed entity fails or is unable to perform such functions in relation to that second level domain;
[(f)] (e) develop and publish guidelines or a code of practise on—
(i) the general administration and management of the .za domain name space;
(ii) the requirements and procedures for domain name registration; and
(iii) the maintenance of and public access to a repository,
with due regard to the policy directives which the Minister may make from time to time by notice in the *Gazette*.
(2) **[The Authority]**.zadna must enhance public awareness on the economic and commercial benefits of domain name registration.
(3) **[The Authority]** .zadna—
(a) may conduct such investigations as it may consider necessary;
(b) must conduct research into and keep abreast of developments in the Republic and elsewhere on the domain name system;
(c) must continually survey and evaluate the extent to which the .za domain name space meets the needs of the citizens of the Republic;
(d) shall be the only domain name authority and operate the only registry .za domain names; and
[(d)] (e) may, from time to time, issue information on the registration of domain names in the Republic.
(4) **[The Authority]** .zadna may, and must when so requested by the Minister, make recommendations to the Minister in relation to policy on any matter relating to the .za domain name space.
(5) **[The Authority]**.zadna must continually evaluate the effectiveness of this Act and things done in terms thereof towards the management of the .za domain name space.
(6) **[The Authority]** .zadna may—
(a) liaise, consult and co-operate with any person or other authority; and
(b) appoint experts and other consultants on such conditions as **[the Authority]** .zadna may determine.
[(7) The Authority must respect and uphold the vested rights and interests of parties that were actively involved in the management and administration of the .za domain name space at the date of its establishment: Provided that—
(a) such parties must be granted a period of six months during which they may continue to operate in respect of their existing delegated sub-domains; and
(b) after the expiry of the six-month period, such parties must duly apply to be licensed registrars and registries as provided for in this Part.]"

Amendment of section 66 of Act 25 of 2002
33. Section 66 of the principal Act is hereby amended:

(a) by the substitution for the heading of section 66 by the following heading:

"**Finances [of Authority]**"

(b) by the substitution for section 66 of the following paragraph:

"(1) All money received by **[the Authority]** .zadna must be deposited in a banking account in the name of **[the Authority]** .zadna with a bank established under the Banks Act, 1990 (Act No. 94 of 1990), or a mutual bank established under the Mutual Banks Act, 1993 (Act No. 124 of 1993), or any Act that replaces or amends these Acts.
(2) The chief executive officer is the accounting officer of the Authority and must ensure that—
(a) proper record of all the financial transactions, assets and liabilities of the Authority are kept; and
(b) as soon as possible, but not later than three months after the end of a financial year, accounts reflecting the income and expenditure of **[the Authority]** .zadna and a balance sheet of the assets and liabilities of **[the Authority]** .zadna as at the end of that financial year are prepared and submitted to the Board and Minister.
(3) **[The Authority]** .zadna is funded primarily from domain name fees and then, as applicable, from—
(a) the capital invested in or lent to **[the Authority]** .zadna;
(b) money appropriated by Parliament for that purpose;
(c) income derived from the sale or other commercial exploitation of its licenses, approvals, products, technology, services or expertise in terms of this Act;
(d) loans raised by **[the Authority]** .zadna;
[(e) the proceeds of any sale of assets;]
[(e)] (f) income or interest earned on **[the Authority's]** .zadna's cash balances or on money invested by it; and
[(f)] (g) money received by way of grant, contribution, donation or inheritance from any source inside or outside the Republic.
(4) The funds of **[the Authority]** .zadna must be utilised to meet the expenditure incurred by **[the Authority]** .zadna in connection with its functioning, business and operations in terms of this Act.
(5) **[(a)]** To the extent that .zadna receives funds from any government source, this subsection (5) shall apply.
(a) The money may be so utilised only as provided for in a statement of **[the Authority's]** .zadna's estimated income and expenditure, that has been approved by the Minister.
(b) Money received by way of grant, contribution, donation or inheritance in terms of subsection (3)**[(g)]**(f), must be utilised in accordance with any conditions imposed by the grantor, contributor, donor or testator concerned.
[(6)(a)](c) The Board must in each financial year, at a time determined by the Minister, submit to the Minister for approval a statement of **[the Authority's]** .zadna's estimated income and expenditure for the next financial year.
[(b)] (d) The Board may at any time during the course of a financial year, submit a supplementary statement of estimated income and expenditure of **[the Authority]** .zadna for that financial year, to the Minister for approval.
[(c)] (e) The Minister may grant the approval of the statement referred to in paragraph **[(a)]** (c), with the agreement of the Minister of Finance.
[(d)] (f) **[The Authority]** .zadna may not incur any expenditure in excess of the total amount approved under paragraph **[(c)]** (e).
[(7)] (6) The Board may establish a reserve fund for any purpose that is connected with **[the Authority's]** .zadna's functions under this Act and has been approved by the

Minster, and may allocate to the reserve fund the money that may be made available for the purposes in the statement of estimated income and expenditure or supplementary statement contemplated in subsection **[(6)]** (5).
[(8) To the extent that the Authority is provided with start-up capital by the State, the Authority may, at the election of the Minister of Finance, be made subject to the Public Finance Management Act, (Act No.1 of 1999), until such time as the Authority, to the satisfaction of the Minister of Finance, becomes self-sustaining through the alternative sources of revenue provided for in subsection (3).]"

Amendment of section 68 of Act 25 of 2002
34. Section 68 of the principal Act is hereby amended:

(a) by the substitution for the heading of section 68 by the following heading:

"Regulations regarding [Authority] domain names"

(b) by the substitution for section 68 of the following paragraph:

"(1) [**The Authority**] .zadna may, subject to [**with**] the approval of the Minister make regulations regarding—
(a) the requirements **which [registries and]** registrars must meet in order to be licensed, including objective standards relating to operational accuracy, stability, robustness and efficiency;
(b) the circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked **[by the registries]** with due regard to the express recognition of the right of groups and members of groups within the Republic to identify with, use or communicate cultural, linguistic, geographical, indigenous or any other expressions of heritage including any visual or audible elements or attributes thereof but subject always to section 64(5) and section 64(6);
(c) pricing policy;
(d) provisions for the restoration of a domain name registration and penalties for late payments;
(e) the terms of the domain name registration agreement **which [registries and]** registrars must adopt and use in registering domain names, including issues in respect of privacy, consumer protection and **[alternative]** dispute resolution;
(f) processes and procedures to avoid unfair and anti-competitive practices, including bias to, or preferential treatment of actual or prospective registrants, **[registries or]** registrars, protocols or products;
(g) requirements to ensure that each domain name contains an administrative and technical contact;
[(h) the creation of new sub-domains;]
[(i)] (h) procedures for ensuring monitoring of compliance with the provisions of this Act and the regulations provided for in this Chapter, including regular .za domain name space technical audits; and
[(j)] (i) such other matters relating to the .za domain name space as it may be necessary to prescribe to achieve the objectives of this Chapter**[; and]** .

[(k)] (2) The Minister may make policy **[to be applied]** that shall be taken into account by **[the Authority]** .zadna in making regulations in terms of subsection (1)."

Amendment of section 69 of Act 25 of 2002
35. Section 69 of the principal Act is hereby amended:

(a) by the substitution of subsections (1) and (2) with the following paragraphs:

"69.(1) The Minister, in consultation with the Minister of Trade and Industry, must make, and may amend and withdraw regulations for an alternative mechanism for the resolution of disputes in respect of the .za domain name space.
(2) The regulations must be made, amended and withdrawn with due regard to existing international precedent."

(b) by the substitution of subsection (3)(b) with the following paragraph:

"(b) the role which [**the Authority**] .zadna must fulfill in administering the dispute resolution procedure;"

Amendment of section 70 of Act 25 of 2002
36. Section 70 of the principal Act is hereby amended by the substitution of section 70 with the following paragraph:

"In this Chapter, "service provider" means any person providing information system services or wireless application services."

Amendment of section 71 of Act 25 of 2002
37. Section 71 of the principal Act is hereby amended by the addition of a new subsection (3) as follows:

"(3) A representative body that satisfies the requirements of subsection (2) and that has applied to the Minister for recognition, shall be deemed to be recognised after a period of 12 months has elapsed from the date of application if the Minister has not indicated to the contrary."

Amendment of section 73 of Act 25 of 2002
38. Section 73 of the principal Act is hereby amended:

(a) by the substitution for subsection (1) of the following paragraph:

"(1) A service provider is not liable for providing access to or for operating electronic communications facilities for information systems or electronic communications networks or transmitting, routing or storage of data messages via an information system or electronic communications network under its control, as long as the service provider—"

(b) by the substitution for subsection (2)(a) of the following paragraph:

"(2) The acts of transmission, routing and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place—
(a) for the sole purpose of carrying out the transmission in the information system or electronic communications network;"

Amendment of section 74 of Act 25 of 2002

39. Section 74 of the principal Act is hereby amended by the substitution for subsection (1) of the following paragraph:

"(1) A service provider that transmits data provided by a recipient of the service via an information system or electronic communications network under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider—"

Amendment of section 77 of Act 25 of 2002

40. Section 77 of the principal Act is hereby amended:

(a) by the substitution for the heading of section 77 of the following heading:

"Take-down notifications"

(b) by the substitution for section 77 of the following paragraphs:

"(1) For the purposes of this Chapter but subject to the provisions of section 77A, a first written notification of unlawful activity, defined for purposes of this Chapter XI as a "**first take-down notice**" must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include—
(a) the full names and address of the complainant;
(b) the written or electronic signature of the complainant;
(c) identification of the right that has allegedly been infringed;
(d) identification of the material or activity that is claimed to be the subject of unlawful activity;
(e) the remedial action required to be taken by the service provider in respect of the complaint;
(f) telephonic and electronic contact details, if any, of the complainant;
(g) a statement that the complainant is acting in good faith; and
(h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct.
(2) Any person who lodges a **[notification of unlawful activity]** first take-down notice with a service provider knowing that it materially misrepresents the facts is liable for damages for wrongful take-down.
(3) A service provider is not liable for wrongful take-down in response to a **[notification]** final take-down notice, and for purposes of this Chapter XI, a "**final take-down notice**" shall mean a notice that is issued after a complainant has followed the procedure set out in section 77A, when a complaint has not been resolved to the satisfaction of the complainant or if no response is received within the time period specified in section 77A(2)."

Insertion of a new section 77A in Act 25 of 2002

41. A new section 77A is hereby inserted after section 77 of the principal Act as follows:

"**Right to remedy on receipt of a take-down notice**

77A. (1) Prior to issuing a final take-down notice, a complainant must first give the service provider an opportunity to respond in writing to the first take-down notice.

(2) The service provider shall respond to the first take-down notice within 10 business days in writing and shall address at least the issues set out in section 77(1)(c) to (e) but may also raise any other issues that are in its view, relevant to the complaint and the first take-down notice.

(3) The complainant shall give due consideration to the response from the service provider and may if the complaint has not been resolved to the satisfaction of the complainant, or if no response is received in the time period referred to in subsection (2), issue a final take-down notice to the service provider within a further 10 business days.

(4) A service provider who does not comply with a final take-down notice within a further 10 business days may be liable for a related offence.

(5) The time periods set out in this section 77A may be reduced in cases of urgency where irreparable or substantial harm is anticipated if the complaint is not resolved within a shorter time period than that set out in subsections (2), (3) and (4)."

Amendment of section 79 of Act 25 of 2002

42. Section 79 of the principal Act is hereby amended by the substitution of subsections (c) and (d) of section 79 by the following paragraphs:

"(c) any obligation imposed by law or by a court to remove, block or deny access to any data message or other electronic communications; or
(d) any right to limitation of liability based on the common law or [**the Constitution**] any other laws of the Republic."

Amendment of section 80 of Act 25 of 2002

43. Section 80 of the principal Act is hereby amended by the substitution of subsection (5)(b) of section 80 by the following paragraph:

"(b) falsely holds himself or herself out as a cyber inspector,
is guilty of an offence and liable on conviction to a fine of not more than R1 million or imprisonment for a period of not more than 1 year."

Amendment of section 82 of Act 25 of 2002

44. Section 82 of the principal Act is hereby amended by the substitution of subsection (2) of section 82 by the following paragraph:

"(2) A person who refuses to co-operate or hinders a person conducting a lawful search and seizure in terms of this section is guilty of an offence and liable on conviction to a fine of not more than R1 million or imprisonment for a period of not longer than 1 year."

Amendment of section 84 of Act 25 of 2002

45. Section 84 of the principal Act is hereby amended by the substitution of subsection (2) of section 84 by the following paragraph:

"(2) Any person who contravenes subsection (1) is guilty of an offence and liable on conviction to a fine of not more than R2 million or to imprisonment for a period not exceeding [**six months**] 2 years."

Amendment of section 85 of Act 25 of 2002

46. Section 85 of the principal Act is hereby amended by the substitution of section 85 by the following paragraph:

"In this Chapter, unless the context indicates otherwise—
"access" includes the actions of a person who, after **[taking note of]** obtaining any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access or use that data."

Insertion of new section 85A of Act 25 of 2002

47. A new Section 85A is hereby inserted in the principal Act after section 85 as follows:

"**Cybersecurity Hub**

85A. (1) The Minister shall, in consultation with the JCPS cluster, create a Cybersecurity Hub for the purpose of-

(a) creating awareness about threats to electronic communications networks and electronic communications from cyber crime;
(b) responding to cybersecurity incidents;
(c) creating guidelines to educate persons, private and public bodies about what cybersecurity is and what measures to put in place to protect themselves and their information from cyber crime;
(d) centralising co-ordination of cybersecurity activities;
(e) conducting cybersecurity audits, assessments and readiness exercises for any person on request; and
(f) fostering and promoting co-operation between Government, the private sector, civil society and international communities and businesses in the setting and implementation of cybersecurity standards and other matters.

(2) The Minister may make regulations in respect of—
(a) the types of cybersecurity incidents that should be reported to the Cyber Security Hub;
(b) the manner in which the Cyberscurity Hub shall administer and implement the National Cybersecurity Framework;
(c) cyber security requirements or guidelines that may be generally applicable or recommended;
(d) the provision and sharing of information to and by the Cybersecurity Hub by any person;
(e) compliance with standards, procedures and policies developed in terms of the National Cybersecurity Framework;
(f) the way in which a person may apply for an audit of his or her or its compliance or the way in which such an audit may be carried out at the instance of the Cybersecurity Hub; and
(g) any other relevant matter which it is necessary or expedient to prescribe for the proper implementation of this Chapter."

Amendment of section 86 of Act 25 of 2002

48. Section 86 of the principal Act is hereby amended as follows:

(a) by the substitution of subsection (1) by the following paragraph:

"(1) Subject to the **[Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992]** Regulation of Interception of Communications and Provision of

Communications-Related Information Act, 2002 (Act No. 70 of 2002), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence."

(b) by the insertion of a new subsection (6) in section 86 as follows:

"(6) Any person who is convicted of an offence referred to in this section 86 shall be liable on conviction to a fine of up to R10 million or imprisonment of up to 10 years."

Amendment of section 87 of Act 25 of 2002
49. Section 87 of the principal Act is hereby amended by the insertion of a new subsection (3) in section 87 as follows:

"(3) Any person who is convicted of an offence referred to in this section 87 shall be liable on conviction to a fine of up to R10 million or imprisonment of up to 10 years."

Amendment of section 88 of Act 25 of 2002
50. Section 88 of the principal Act is hereby amended by the substitution for section 88 by the following paragraphs:

"(1) A person who attempts to commit any of the offences referred to in **[subsections (1) or (2)]** sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in sections 86 or 87, as the case may be.
(2) Any person who aids and abets someone to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to **[the penalties set out in (1) or (2), as the case may be]** a fine of up to R5 million or imprisonment of up to 5 years."

Deletion of section 89 of Act 25 of 2002
51. Section 89 of the principal Act is hereby deleted.

Amendment of section 90 of Act 25 of 2002
52. Section 90 of the principal Act is hereby amended by the substitution of section 90(d) by the following paragraph:

"(d) the offence was committed on board any ship or aircraft or other craft capable of electronic communications registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed."

Deletion of section 92 of Act 25 of 2002
53. Section 92 of the principal Act is hereby deleted.

Amendment of section 94 of Act 25 of 2002
54. Section 94 of the principal Act is hereby amended by the substitution for section 94 by the following paragraph:

"(1) The Minister may make regulations regarding any matter that may or must be prescribed in terms of this Act or any matter which it is necessary or expedient to prescribe for the proper implementation or administration of this Act except where that function is expressly reserved or delegated to another entity under this Act.

(2) The Minister shall make such regulations available in draft form by notice in the *Gazette* for public comment for a period of no less than 30 days and shall consider written or oral representations from the public prior to publishing the regulations in final form."

Deletion of section 95 of Act 25 of 2002

55. Section 95 of the principal Act is hereby deleted.

Short title

56. *(a)* This Act is called the Electronic Communications and Transactions Amendment Act, 2012 and comes into operation on a date determined by the Minister by Notice in the Gazette.
(b) Different dates may be fixed for the coming into operation of different sections of this Act by Notice in the Gazette.

MEMORANDUM ON THE OBJECTS OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS AMENDMENT ACT

1. Background to this consultation

1.1 The Electronic Communications and Transactions Act, 2002, or ECT Act as it has become known, has been in place for a decade. During this time, the ECT Act has functioned well in all areas, providing for consumer protection ahead of the introduction of the Consumer Protection Act, 2008, and heralding the important notions of privacy and data protection. In addition, this Act has enabled the creation of the .za Domain Name Authority and so provided for the protection of level one and two domain names, and the resolution of disputes regarding registration of competing domain names. This Act has also enabled the creation of our first authentication service providers, LawTrust, to accredit electronic signature providers and cryptography providers.

1.2 However, in the decade since its introduction, the world has seen significant changes in the electronic communications sector, affecting our use of the internet. Social media over the internet and other forms of communications have revolutionized the way we communicate with one another and our fellow man, removing physical barriers to communications and the sharing of information. At the same time and as a consequence of the exponential growth in electronic transactions and our dependence on the internet, we have experienced a significant increase in hacking, security breaches, data mining for economic purposes, misuse of personal information, cyber security threats and cyber crime.

1.3 In response to these changes, the international community is seeking to harmonise their approach to a communications system that traverses borders, and to the sort of threats that are nameless and faceless but that can destroy or harm these otherwise beneficial systems. South Africa is a participant in many international initiatives and is a party to associated agreements and therefore has agreed to certain reforms. These reforms have some effect on the way in which electronic transactions and the internet and associated activities including cryptography and cyber security are carried out. As a result it is appropriate to review the ECT Act to ensure that South Africa meesures up to the international benchmark in these areas.

1.4 Amendments are also proposed to this Act to take account of industry needs and recommendations that have been brought to the Minister's attention. The original version of the Act was based largely and still is consistent with the UNCITRAL model for e-commerce legislation. Where the South African law of contract and/or sale provides rules for the conclusion of transactions, whether electronically or not, which are entrenched in our law, those rules have been preferred.

1.5 The Minister is grateful to the South African Law Reform Commission (SALRC) for certain suggestions in key areas affecting communications sector, namely, the institutional framework, the regulation of electronic communications, e-commerce, and interception and monitoring.

1.6 The Minister welcomes your views on these proposed amendments.

2. CHAPTER I: Interpretation, Objects and Application

2.1 Several definitions now refer simply to the definition given to that term or word in another Act. Although we recognise that requires cross-referencing as between Acts, if the other Acts change then this one would have to change every time to reflect the exact definition if we were to copy the existing definition into this Act. For reasons of flexibility and accuracy we consider this to be a more sensible approach.

2.2 The International Telecommunications Union (ITU) has identified the following categories of e-commerce:

- Subscription and usage-based telephony, online, and Internet access services
- Subscription or transaction-based information services and software sales
- Consumer retail sales
- Business-to-business wholesale and retail services and sales
- Advertising and marketing services
- Financial services and transactions
- Government services and information; and
- Ancillary functions contributing to business/commercial activities.

With this in mind we have proposed a new definition of "electronic transactions" which includes commercial and non-commercial transactions. This definition is based largely on the definitions of "consideration", "supplier" and "transaction" from the Consumer Protection Act, 2008 (CPA), for consistency. These definitions are important when it comes to unsolicited communications, dealt with in Chapter VII.

2.3 We have also had regard to the definitions advanced by the OECD, other jurisdictions, and the ITU. In particular we note the ITU's guidelines in the context of a review of e-commerce in Caribbean countries in 2011[1], which are generally applicable. The guidelines feature eight categories of general principles which are:

(i) Transparent and Effective Protection for Consumers which is not less than the level of protection afforded in other forms of commerce.

(ii) Fair Business, Advertising and Marketing Practices by businesses engaged in electronic commerce.

(iii) Online Disclosures – Clear and obvious disclosures.

[1] http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-1-A_Assessment_Electronic_Transactios_V2-E.pdf

(iv) Confirmation Process included in the electronic transaction affording the consumer an opportunity to express an informed and deliberate consent to the purchase; and retain a complete and accurate record of the transaction.

(v) Secure Payment mechanisms, including information on the level of security such mechanisms afford.

(vi) Dispute Resolution alternatives accessible in a timely manner without undue cost or burden

(vii) Privacy in accordance with the recognized privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980) to provide appropriate and effective protection for consumers.

(viii) Education and Awareness to educate consumers about electronic commerce, to foster informed decision-making by consumers and to increase business and consumer awareness of the consumer protection framework that applies to their online activities.

2.4 We have noted these principles in proposing other changes to the Act.

2.5 To remove confusion regarding the different "authorities" in the Act, we have defined the Authority responsible for accreditation of authentication products as the "Accreditation Authority" and the Domain Name Authority is simply called ".zadna".

2.6 The definition of a "cryptography provider" is broad and can be construed to mean that even a person who installs software in a computer could be a cryptography provider. This clause in the Act was meant to refer only to people or entities that develop cryptography products and services. The phrase has been reviewed to define "cryptography providers" as entities or individuals that develop cryptography products and service and not end users.

2.7 "critical information databases" are now being referred to as "critical information infrastructure" in terms of both international texts and conventions on cyber security, and our own National Cyber Security Policy Framework of March 2012 (the Framework). We have therefore replaced "database" in this term with "infrastructure". In addition, the Framework distinguishes between "national" and other critical information infrastructure, "national" having reference to information that is of national importance, such as security information. We have amended both the definitions and Chapter IX in this regard.

2.8 The ECT Act contains a definition of the 'Internet' which the SALRC suggests has been superseded by technical revisions determined by engineers and developers, and case law. The suggested amendment describes the internet as binary code, or data, communicated through a network made up of electronic communications facilities using packet switching technology and communicating through TCP/IP, and as including future versions.

2.9 New entities such as the "National Consumer Commission" have been inserted to refer to the regulatory authority established by the CPA. The "JCPS cluster" refers to the cluster of Ministries tasked with Justice, Crime Prevention and Security, which Ministries are important in relation to the protection of South African networks and information, specifically in relation to cyber security. The Bill refers to this Cluster and to the Framework throughout – this is important to enable co-operation and joined up working to ensure that our information and communications systems are protected in a uniform way.

2.10 Although some changes have been made to the definition of "personal information", these have been made in the hope that this particular definition will not change in the final version of the Protection of Personal Information Bill when it is finally approved. However, other clauses and provisions of that Bill have not been included because we understand that the Bill, when passed, will take precedence over any provisions pertaining to personal information in the ECT Act in any event. The definition of "personal information" has proved to be relatively uncontroversial and is not likely to change. It remains valid and important to the operation of the remainder of the ECT Act however, even if no other changes are made.

2.11 The ECT Act contains definitions of 'registry' and 'registrar' that do not include the .za Domain Name Authority (.zaDNA) as a registrar and registry or registry operator, as they are known in practice. We agree that the relevant authority or the country code top-level domain (ccTLD) administrator, like .zaDNA, should have the same responsibilities as registries or registrars operators with respect to updating repositories and the second-level domain administration. We have made consequential amendments to Chapter X and amendments to these definitions to address this. Furthermore we agree that an applicant for a domain name should remain an applicant until their application is approved and we have amended the definition of "registrant" accordingly. Finally, changes are also proposed to "repository" to reflect its nature as more accurately a registry databasa.

2.12 New definitions have been proposed including to define domain data as being data specifically used in and with relevance to the domain name registration process and the holding of a domain name. We propose to refer here to "registry data" including domain names, registrant names and contact details, zone records, registration and renewal dates, and any other data as may be prescribed.

2.13 The definition of 'Universal Access' differs in the ECT Act and ECA. In addition, section 82(3) of the ECA empowers the Minister of Communications (Minister) to further determine what constitutes universal service and access, upon the recommendations of the Universal Service and Access Agency of South Africa

(USAASA). We propose to remove the definition from the ECT Act which should focus more on transactions, security and use of the internet, than policy goals such as universal service. This belongs more properly in the ECA.

2.14 "Unsolicited communications" are now unlawful unless the recipient has consented to receiving them – the so-called "opt-in" regime now applies. The definition of this term has been guided by the provisions of the CPA. The dti has been consulted in this regard. No consequential changes need to be made to the CPA.

2.15 Because service providers now include not only internet service providers but also wireless application service providers (WASPs), we have included definitions that allow for the recognition of these WASPs and their representative organization.

2.16 As a general matter we note that our review of the legislation has led us to review the penalty and remedy clauses within the Act. Throughout the Act we have replaced reference to a general or specific offence and associated cross-reference to section 85, with specific penalties or remedies for each Chapter. The loss of civil liberty should be a greater deterrent to potential wrongdoers than a financial penalty, therefore we have suggested either a fine up to a maximum or imprisonment with a maximum term, and in the case of service providers, a notice and take down procedure with a notice period. The severity of each offence will be judged on its merits and the adjudicating body or judge as the case may be, will be able to apply the remedy or the fine or imprisonment (as the case may be) to the maximum, in their discretion.

3. **CHAPTER II: Maximising Benefit and Policy Framework**

3.1 This chapter is intended to enable use of the internet (among other things) to help to bridge the digital divide. The Act currently requires the development of a National e-Strategy by the Minister of Communications, in consultation with other Ministers. The national e-Strategy must include detailed plans and programmes, with clear deliverables and timeframes, and must address the development of an e-transactions policy, the promotion of universal access and e-readiness, SMME development, empowerment of previously disadvantaged persons and communities, human resource development, education and training in the ICT sector.

3.2 This strategy has not yet been developed, however the Minister considers that it is necessary and will prioritise the development of such a strategy within 24 months after the promulgation of this Amendment Act. The strategy must deal with those matters that are globally being addressed, and in which endeavours South Africa is participating. These matters will include e-commerce for businesses, e-government, and security issues. The reference to the e-strategy has been amended in this regard. The strategy

should address a 3-year period and should be approved by Cabinet. Some of the issues previously forming part of the content of policy should form part of the e-strategy including the need to take account of international best practice. In the same vein, certain of the human resource issues provided for in relation to the e-strategy can be situated within the ambit of the policy that the Minister may make for the sector.

3.3 The Minister therefore considers it appropriate to also provide for the making of policy in this Act, in the same way as the Minister makes policy under the ECA. However, the 2 Acts need to deal with different policies – this Amendment Act should address policy that is necessary in relation to e-readiness, SMME development, human resource development, education and training in the ICT sector. The current references to matters that are related in part or whole to universal service and access are proposed to be deleted in this Amendment Act. Although SMME development may be considered to fall within the ambit of the ECA and particularly section 9 of the ECA, given that the Minister may in terms of section 3(1)(g) make policy in relation to the mechanisms to promote SMME participation in the ICT sector, the Minister considers this objective to be so important as to provide for it in the context of both electronic communications (within the ECA) and transactions using electronic communications (within this Act).

3.4 In making policy the Minister should have regard to the Framework for Cyber Security and issues that arise under Chapter XIII (cyber crime).

4. CHAPTER III: Facilitating Electronic Transactions

4.1 This chapter deals with removal of social and legal barriers to electronic transacting.

4.2 Part 1 provides for the legal recognition to data messeges and records. Data messages are regarded as the functional equivalent of traditional "writing". Provision is made for the legal recognition of electronic signatures and "advanced electronic signatures" – a secure form of electronic signing. It is necessary to refer to the e-strategy and public key infrastructure strategy that may be developed by the committee to be established pursuant to the Framework, as this will have to be taken into account when regulating electronic transactions.

4.3 Part 2 deals with the rights and obligations that follow from the communication of data messages, namely contract formation. The time and place of sending and receiving data messages, as well as the time and place where a contract is deemed to be formed by means of data messages are provided for. The Act also provides for the validity of sending notices and other declarations of intent through data messages. In summary, this chapter addresses the admissibility of online communication as evidence in the court of law and what constitutes a contract. It introduces the concept of the advanced electronic signature, which subject to certain conditions, will have the same commercial weight as the traditional signature.

4.4 This chapter was reviewed by the SALRC with a view to determining how to ensure that electronic signatures can also have evidentiary weight. Very few changes are recommended to this chapter, as it is broadly in line with UNICTRAL rules and the position in the international community.

4.5 In general therefore, this chapter is considered to have taken account of international trends in adopting electronic signatures for the purpose of creating binding documents that can be relied upon in court.

5. CHAPTER IV: e-Government Service

5.1 This chapter facilitates e-filing, the requirements for the production of electronic documents and the integrity of information. Provision is made for any Department or Ministry to accept and transmit documents in the form of electronic data messages, to issue permits or licences in the form of a data message or make or receive payment in electronic form.

5.2 *The Minister has noted that the Department of Public Service and Administration (DPSA) is already acting in terms of this chapter and is consulting with the DPSA.*

6. CHAPTER V: Cryptography Providers

6.1 This chapter creates a framework for the registration of cryptography products and service, and for cryptography providers by the establishment and maintenance of a Cryptography Provider Register by the Department. The objective is to assist law enforcement in their investigations. This chapter should be read with Chapter 11 of the Regulation of Interception of Communications and Provision of Communications-Related Information Act, 2002 (as amended) (RICA).

6.2 However the chapter did not go far enough to require cryptography providers to provide information that will or could enable the Director General to determine whether or not that provider or those products and services as the case may be, could pose a threat to national security or prejudice the public interest.

6.3 The chapter has been amended to introduce specific objectives in relation to cryptography providers and their services and products, and obligations on those providers to renew their registration every 2 years. Other changes have been made to bring the chapter in line with international trends and requirements in relation to cryptography. This is unfortunately, one of the ways in which cyber criminals can access and destroy or interference or remove information stored or transmitted electronically and it is therefore receiving more attention and being made subject to stronger controls.

6.4 The objectives are to:

6.4.1 enable responses to requests for mandatory and lawful access to encrypted real-time communications or encrypted stored data;

6.4.2 address the challenges posed by the international use of cryptography products when seeking to gather security-related information of national importance; and

6.4.3 enable liaison with the JCPS cluster in relation to the development of capacity and standards in this regard.

6.5 The register must now record the country of origin of products of this sort.

6.6 Additional obligations may be imposed on cryptography service providers under regulations and these persons are reminded that they may have to comply with an order under RICA.

6.7 Because of the significance of the products that will be provided within the Republic, registration must be renewed every 2 years and application for renewal may be refused for example, for reasons of national security or poor or inadequate performance.

7. **CHAPTER VI: Authentication Service Providers**

7.1 This chapter provides for the establishment of an Accreditation Authority within the Department, to accredit certain types of electronic transaction service providers. The Accreditation Authority should also monitor compliance. The Accreditation Authority may temporarily suspend or revoke accreditations of an authentication product or service. Several of the provisions in this Chapter are now aligned with the preceding chapter on cryptography providers, such as registration of products and providers and renewal of registration.

7.2 The mandatory registration of these entities, products and services is new to this chapter. We consider that the significance of providing services and/or producing products requires mandatory registration. The tracking of manufacturers as well as providers will be possible through central registration.

7.3 The current definition of "authentication products and services" means any product or service designed to identify the holder of an electronic signature to other persons. The creation of an electronic signature is the result of a process involving a digital certificate (confirming the identity of the holder). The Accreditation Authority should also, in our view, create a register of products and services as well as service providers.

7.4 Registration should be mandatory in our view, not voluntary as is currently the case, because of the importance of the use of the products and services and the implications of their use by providers. We consider that registration of products and authentication service providers should extend to certification service providers, who may form a subset of authentication service providers, but may also simply provide certificates and not authentication products or services. They should therefore be obliged to register separately as well as where they are also authentication service providers.

7.5 Section 37 (3) provides for penalizing any person who falsely holds out its products or services. The extent of the penalty is not presently defined. The penalty should be such

that it deters such behavior, and we have made amendments in this regard. A person falsely holding out its products or service to have been accredited by the Accreditation Authority should be guilty of an offence and fined or jailed in order to discourage falsification of products and services and the resulting prejudice to consumers.

7.6 Currently, only a South African accredited certification service provider can issue advanced electronic signatures. It is proposed that an electronic signature which is accredited in a foreign jurisdiction will only be recognised in South Africa and therefore eligible for registration, if there is an agreement of mutual recognition with that jurisdiction.

8. CHAPTER VII: Consumer Protection

8.1 This chapter deals with consumer rights and issues pertaining to electronic transactions.

8.2 The CPA came into effect on 1 April 2011. The CPA clauses do not cover issues addressed by sections 43, 44 and 46 of this Act. Unless the CPA is amended so as to incorporate these provisions, they should be retained as is in the Act. The amendments proposed to this Act will however, replace the Consumer Affair Committee with the National Consumer Commission.

8.3 We have also given consideration to certain principles previously advanced by members of the public in relation to this Act. These have included suggestions to minimize the transmission of spam or prevent it altogether. The Minister is aware of the Code of Conduct prepared and enforced by the Wireless Application Services Provider Association (more about WASPA later). Having considered the provisions of the Act and the concerns, the Minister is of the view that certain changes will be useful:

8.3.1 The definition of "unsolicited communications" has been amended, taking into account the provisions of section 21 of the CPA, which section sets out in detail when a transaction or communication shall be considered to be "unsolicited". Unsolicited communications are not permitted without the specific and prior permission of the recipient, under section 45.

8.3.2 The Act now affords protection to both natural and legal persons.

8.4 The balance of the provisions of the chapter deal with the reception of messages, confidentiality, security and protection of the consumer, and should be read with the relevant provisions of the CPA.

9. CHAPTER VIII: Protection of Personal Information

9.1 This chapter deals with the protection of personal information. However much work has been done in relation to new legislation to deal with personal information and privacy and the protection of state information. As a result, except as set out below, we have not amended this chapter and await the new legislation.

9.2 Section 50(2) of the Act provides that the principles governing the processing of electronically collected personal information[2] are voluntary. We have amended this section in order to make the principles obligatory because the voluntary principles do not give effect to the right to privacy provided for in the Constitution.

9.3 As indicated in relation to definitions, "personal information" has been amended to reflect the proposed definition in the new Bill on personal information.

10. CHAPTER IX: Protection of Critical Information Infrastructure

10.1 This chapter makes provision for the Minister to prescribe minimum standards on how to manage and maintain critical databases.

10.2 Information and network infrastructure for example the electricity grid, the management of dams and so on and all security information is stored on what are now going to be classified as critical information infrastructure or "national" critical information infrastructure – databases that hold information that is important and even critical to the country, or certain sectors.

10.3 This trend in nomenclature is being adopted by the Department, along with other changes to reflect the importance of the infrastructure and the responsibility that is shouldered by the infrastructure administrator, as indicated by the level of fines and length of term of imprisonment proposed for contraventions or failures to comply with this chapter.

11. CHAPTER X: Domain Name Authority and Administration

11.1 This chapter established a .za domain name authority as a section 21 company. The objects, powers and matters incidental to the incorporation of the company are already provided for in the Act. The Minister is empowered to establish a national policy on the .za domain name space. The Authority's role and function is described and provision is also made for alternate dispute resolution in the event of disputes arising from abusive domain name registrations or other issues related to domain name registrations.

11.2 The Act was previously silent on the removal of a board member from the board. The amendments address the removal in section 62. The Minister appoints members therefore the Minister should remove board directors subject to the list of circumstances that may apply in this regard.

11.3 Several other changes are proposed in relation to the board composition, appointment and changes. These are in part to improve transparency and efficiency in administration, having regard to best practise in corporate governance and specifically the requirements of King III.

[2] Section 51 of the ECT Act.

11.4 Additional changes to the staffing provisions of the chapter are also proposed, including that the chief executive officer should appoint suitable staff and because of this s/he can be held accountable for staff's performance and actions. Members of the board should be appointed for 3 years but the chairperson will be appointed for 4 years which we hope will ensure that because they will be appointed at different times, continuity will result.

11.5 Several wide-ranging changes have been proposed over the years by zadna. The Minister has considered these and presents a number of them for consultation where they are in line with international approaches to domain name management and administration.

11.6 The Minister recognises too that there are a number of registry operators administering second-level domain names, such as UNIFORUM South Africa (.co.za), the state-owned State Information Technology Agency (.gov.za) and privately-owned Internet Solutions (Proprietary) Limited (.org.za). In addition to these entities, the Internet Corporation for Assigned Names and Numbers (ICANN) has overall responsibility for managing the Domain Naming System (DNS). It administers the root domain, delegating control over each Top Level Domain (TLD) to a ccTLD administrator, such as .za Domain Name Authority (DNA). Because the DNS is not centralized, the administration of the second-level domain is further delegated to above-mentioned registry operators who administer the DNS with a great degree of independence. Some countries have third and fourth level domain administrators.

11.7 To ensure the stability of the system, .zaDNA must take the final and overall responsibility of the DNS in its territory, therefore it must be able to perform the functions of the registrars and registry operators, as and when required.

11.8 Additional changes have been made to definitions as set out in the initial section of this note.

11.9 Section 60 requires zadna to accept any citizen as a member without the member complying with any formality. For a number of reasons of an administrative nature, and for purposes of security and accountability, we propose to require members or applicants to submit more detailed information prior to registration. There is no good reason why members could not be juristic or natural persons and changes have been made in this regard as well.

11.10 The funding of .zadna has been reconsidered. To the extent that .zadna does receive funds from National Revenue Fund or other government sources it should be required to report on them to Cabinet in the ordinary course, but this is an obligation that need not apply to funds that .zadna receives from other sources. The usual reporting and accounting obligations continue to apply, as these would to any other section 21 company.

11.11 Section 68 provided that .zadna could make regulations with the approval of the Minister. This provoked some discomfort in that section 94 authorises the Minister specifically to make regulations. It was felt that .zadna ought not to have power to make regulations. However, it is our view that section 94 is not an exclusive provision but an authorizing provision – it does not say that only the Minister may make regulations. To allay any concerns about the appropriateness of .zadna making regulations we have reviewed the types of regulations that may be made and the content of them within section 68 and also provided that regulations must be made "subject to" the approval of the Minister. If the Minister has any concerns, then he or she will not approve the regulations. In this way the Minister retains the right to make regulations, whilst not having to propose their content which .zadna is better-placed to do in any event.

11.12 We understand that the regulations on alternative dispute resolution under section 69 have enabled the establishment of a successful mechanism in this regard, and we do not consider that any changes are required to this section.

11.13 Finally but importantly we have introduced new provisions in section 64 to address the registration by ICANN in the last few months of this year, of new generic domain names. This is for several reasons:

11.13.1 Domain names are beginning to take on importance that was previously not foreseen.

11.13.2 South African names that are intrinsically of national importance or relevance should be treated differently than corporate or brand names for reasons of public interest.

11.13.3 We propose that geographic or cultural gTLDs that are uniquely South African should not be registered without the permission of the Minister. These names might include for example, any reference to a South African national language, a South African place name, a South African heritage site, a South African historical event, a South African product or service, or a South African national team or national representative of any kind.

11.13.4 The registration of a South African language domain name such as .zulu by a non-South African for example, is innately wrong. The Minister wishes to promote the registration of this sort of domain name by entities associated with the protection and promotion of it or what it stands for and to prevent the arbitrary registration of important names or phrases which may be associated with our unique national heritage, by persons without an appropriate or justifiable reason.

11.14 Offenders under this chapter are liable for fines or imprisonment.

12. CHAPTER XI: Limitation of Liability for Service Providers

12.1 This chapter creates a safe harbour for service providers who may be exposed to a wide variety of potential liability by virtue only of fulfilling their basic technical functions. The service providers may seek to limit their liability where they have acted as mere conduits for the transmission of data messages, provided the technical means for system caching, hosted data on an information system or where they have linked or referred users to an on-line location by the use of information location tools.

12.2 Chapter XI of ECTA deals with conditions under which the liability of service providers will be limited. One of the conditions is the membership of a service provider to an industry representative body recognised by the Minister. In the past applications have been made without response from the Department. We have recognised this as being an obstacle to the application of the Act. Once a representative body has requested recognition and received no response from the Minister within a period of 12 months, the industry body will be deemed to be recognised.

12.3 This chapter provided initially for the Internet Service Provider and at the time did not take into consideration Wireless Application Service Providers (WASPs). Amendments to the section now enable the application of it to WASPs as well. We have amended the section to refer to "information systems" and amended that definition as well. Although on the face of it the section may not apply to licensees under the ECA who are not "service providers", they should not be liable simply because they are categorized as licensees. Amendments are made in this regard so that any person providing service of the type that these service providers may or do provide, should fall within the section. This will require licensees wishing to benefit from the provisions to register with an industry body that is recognised by the Minister.

12.4 Liability will accrue nonetheless if any of the conditions set out in this chapter are not adhered to.

12.5 After further consideration, the Minister considers that any notice or take-down procedure should allow for the right of reply in accordance with the principle of administrative justice and the *audi alteram partem* rule. Changes have been proposed in this regard to section 77 and a new section 77A is proposed.

13. CHAPTER XII: Cyber Inspectors

13.1 This chapter makes provision for the Director-General to appoint cyber inspectors.

13.2 The cyber inspectors may monitor websites in the public domain. Cyber inspectors may also investigate whether cryptography service providers,

authentication service providers and data controllers or information officers comply with the relevant provisions of this Act.

13.3 The power to inspect, search and seize has been granted to cyber inspectors, provided they obtain a warrant.

13.4 Section 84 (2) stipulates that "Any person who contravenes subsection (1) is guilty of an offence and liable conviction to a fine or to imprisonment for a period not exceeding six months". The clause does not currently stipulate how much the fine should be and the prison sentence of six months is not a deterrent. The amendments propose revisions here to increase the penalties that are possible in the event of a contravention of the section, for example, obstructing a cyber inspector or pretending to be one.

13.5 In addition, using information obtained pursuant to this section in contravention of its intended use or where confidentiality restrictions apply, will also render the offender liable to a penalty. This penalty is greater than the penalty referred to above, because the nature of the information may be of considerable importance, and In the case where it is of a personal nature, may expose the person to harm or prejudice. We have set out in a table attached to this note, an explanation of the existing and proposed penalty regime.

14. CHAPTER VIII: Cyber Crime

14.1 This chapter introduces into the South African law statutory criminal offences relating to information systems. These crimes relate to the unauthorised access to, interception of or interference with data, and computer-related extortion, fraud or forgery. Any person aiding or abetting another to perform any of these crimes will be guilty as an accessory to the commission of that crime.

14.2 The provisions of this chapter have been aligned to moves internationally and particularly those anticipated in the Framework.

14.2.1 The Framework envisages that the JCPS cluster will take action in different ways to implement that policy, such as by criminalizing certain types of content (eg child pornography), making possession of certain types of malware an offence, introducing new measures to combat crime in general and cyber crime in particular, and requiring certain types of entities to adhere to a prescribed set of security parameters.

14.2.2 The Department is required to establish a Cyber Security Hub, which will have certain duties and powers. Its main function will be to co-ordinate the various activities and institutions involved in cyber security, and to educate the public and private sector about cyber security and cyber threats.

14.2.3 It will also publish guidelines on the steps that can be taken to protect electronic systems from cyber threats and cyber warfare, and if a "cyber incident" should occur, then this Hub will allocate resources to deal with it.

14.2.4 The Hub will also liaise with international counterparts on international trends and standards in cyber security and make these known within South Africa and within all Ministries with an interest in cyber security.

14.2.5 This is a crucially important role. For this purpose the Department will create a new unit and this will need to be staffed. Technical skill will be a priority for this Hub and the policy to be produced by the Minister will outline the steps that we will take to prioritise skills development in this area.

14.2.6 The establishment of the Hub will begin immediately but will need to be developed alongside the development of other and related measures by the JCPS cluster. These endeavours will be ongoing. Information flows will be critical and the Department will focus on information-sharing and education as a first priority.

14.3 The ECT Act prescribes the penalties if a person is convicted of an offence in section 89 read with other sections of the Act.

14.3.1 In our view none of the current penalties are substantive and will not serve as a deterrent to criminals or potential wrongdoers. In the information society more emphasis needs to be placed on doing things correctly because of the reliance of us all on electronic communications and networks. Unfortunately deterrents are usually of a negative nature, and in South African law may take the form of specific remedies, or administrative fines, or prison terms, or more than one form of remedy.

14.3.2 *Annexure A* indicates what offences are identified under the Act as it stands, and what is proposed as a result of the changes and because more than a decade has passed since the offences and penalty regime under this Act was considered.

October 2012

ANNEXURE A: THE CURRENT OFFENCES, PENALTIES AND REMEDIES REGIME UNDER THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002 AND SUGGESTED CHANGES

Current provision	Contravention	Current sanction	Suggested change
Chapter VI: cryptography providers	s30: Providing cryptography products or services without registering with the Department	s32: contravention or failure to comply with this Chapter means the person is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding 2 years	New s29(3): in addition to or separately from s32, a cryptography provider can be de-registered for failure to adhere to any provision of the Act, or if his/her conduct is objectively determined by the DG to be detrimental to the users of cryptography providers and services in any way
	s30: Not providing the required information [implied that if the information is false this also applies] and/or not paying the fee	As above	Amend s32 to remove the prison term unless the information provided is false, but also impose a fine. It is difficult to prescribe a fine in this instance because the nature of the transgression could be minor (an omission of information) or major (a fraudulent representation). Leave the fine wording as is with a maximum fine of R2 million
	s31: Disclosing information to any person other than employees of the Department responsible for keeping the register (unless to a relevant authority in relation to investigation of an offence or for purposes of criminal proceedings, national safety and security agencies, cyber inspectors, in terms of PAIA, or for civil proceedings relating to cryptography products or services to which a provider is a party)	As above	Again the fine could be large if the disclosure is material and not as large if the disclosure is not material. Remove the prison term in this case as well and leave the fine wording as is with a maximum of R2 million

Chapter VI: authentication service providers	s37: Holding out products or services as being accredited by Authentication Authority	s89: Fine or imprisonment not exceeding 12 months	New penalty provision introduced to s37(3) – fine of not more than R2 million or prison term of not more than 2 years
	s39: Authentication service provider fails to meet or ceases to meet requirements, conditions or restrictions under which accreditation was given	s39: Suspend or revoke the accreditation	Leave as is. Applicants for renewal must adhere to the procedure and complete the forms or no renewal will take place
	s40: Foreign person falsely holding out products or services as having been accredited	s89: Fine or imprisonment not exceeding 12 months	Amend s40 to reflect fine of not more than R1 million or prison term of not more than 12 months, amend s89 to delete reference to s40
Chapter VII: consumer protection	s45: Failure to comply with subsection (1)	s89: Penalties include a fine or imprisonment for a period not exceeding 12 months	Amendment to section 45 to prohibit unsolicited communications and include a fine not exceeding R1 million or a prison term not exceeding 12 months, amend s89 to delete reference to s45
	s48: Provisions that exclude any rights provided for in this Chapter	s48: Those provisions are null and void	-
Chapter IX: critical information infrastructure	s56: disclosure of certain information except as specified in exceptions (subject to audit of compliance with the Chapter under s57)	s58: notice to be given to remedy but if not remedied, then s89 applies and fine or imprisonment for maximum period of 12 months	Amend s58 to apply fine of maximum R5 million or imprisonment of 3 years, amend s89 to delete reference to s58(2)
Chapter X: domain name registration			New 64(5) and (6) regarding gTLDs and new (7) for failure to comply meaning a fine up to R2 million and imprisonment up to 2 years

Chapter XI: liability of service providers	s71-77 – no liability if conditions are followed as set out in law	Implication that liability for damages or other remedies may apply (contractually) if conditions are not followed	
Chapter XII: cyber inspectors	s80: person holding themselves out as cyber inspect or obstructing a cyber inspector in the course of his duties	s89: fine or imprisonment not longer than 12 months	Amend s80 to provide for a fine not more than R1 million or imprisonment not more than 12 months, amend s89 to delete reference to s80
	s82: refusal to co-operate or obstruction during a search and seizure	s89: fine or imprisonment not longer than 12 months	Amend s82 to provide for a fine not more than R1 million or imprisonment not more than 12 months, amend s89 to delete reference to s82
	s84: disclosure of information obtained pursuant to exercising power under the Act	s84: a fine or imprisonment up to 6 months	Amend s84 to refer to R2million and 2 years (in line with others)

Chapter XIII: cyber crime	s86(1), (2) or (3): unauthorised access to, interception of or interference with data	s89: fine or imprisonment up to 12 months	Amend s86 to introduce new (6) to provide for any offence under this section (subsections (1) to (5)) is liable on conviction to a fine not exceeding R10 million or imprisonment of up to 10 years (following RICA examples), delete reference in s89 to s86
	s87: computer-related extortion, fraud and forgery	s89: fine or imprisonment up to 5 years	Amend s87 to introduce new (3) to provide for any offence under subsections (1) or (2) to be liable on conviction to a fine not exceeding R10 million or imprisonment up to 10 years, delete reference in s89 to s87
	s88: attempt, and aiding and abetting	s88(1): liable under s89(1) or (2) as the case may be s88(2): same	Amend s88(1) to refer to penalties set out in s86 or 87 as the case may be and amend 88(2) to refer to penalties up to R5million or imprisonment up to 5 years
	s89: penalties to apply to named sections by cross-reference	Fine not specified or imprisonment up to 12 months (subsection (1) or 5 years (subsection (2))	Delete entire section [not appropriate to have in cyber crime chapter anyway]

Printed by and obtainable from the Government Printer, Bosman Street, Private Bag X85, Pretoria, 0001
Publications: Tel: (012) 334-4508, 334-4509, 334-4510
Advertisements: Tel: (012) 334-4673, 334-4674, 334-4504
Subscriptions: Tel: (012) 334-4735, 334-4736, 334-4737
Cape Town Branch: Tel: (021) 465-7531

Gedruk deur en verkrygbaar by die Staatsdrukker, Bosmanstraat, Privaatsak X85, Pretoria, 0001
Publikasies: Tel: (012) 334-4508, 334-4509, 334-4510
Advertensies: Tel: (012) 334-4673, 334-4674, 334-4504
Subskripsies: Tel: (012) 334-4735, 334-4736, 334-4737
Kaapstad-tak: Tel: (021) 465-7531