*12. ~~HON. NYAMUDEZA: To ask the Minister of Lands, Agriculture, Fisheries, Water and Rural Resettlement to inform the House the role of Agritex Officials in the management of irrigation schemes.~~

~~*13.~~ ~~HON M.M. MPOFU: To ask the Minister for Mines and Mining Development to inform the House on the status of Jena Mine, in the Silobela Constituency, amid unsubstantiated rumours doing rounds, that the Mine has been sold to Landela Company, sparking fears and despondency that the surrounding communities will not get any benefits from this new Company in terms of its Corporate Social Responsibility.~~

~~*14.~~ ~~HON. NKANI: To ask the Minister of Transport and Infrastructural Development to inform the House when construction of Golden valley – Sanyati road in Chakari Constituency, Mashonaland West will resume.~~

~~NOTICE OF MOTION~~

~~HON. SAMUKANGE~~
~~HON. MATHE~~

~~That this House considers and adopts the Report of the Privileges Committee Investigating Cases~~ of Alleged Misconduct by MDC – Alliance Members of Parliament.

NOTICE OF AMENDMENTS

Cyber Security and Data Protection Bill, (H B 18, 2019)

AMENDMENT OF CLAUSE 1 (SHORT TITLE)

BY THE MINISTER OF INFORMATION COMMUNICATION TECHNOLOGY, POSTAL AND COURIER SERVICES

This is the first of the amendments proposed by the Minister appearing for the first time in the Order Paper for 18th March. His other amendments are to be found on pages 20-21, 22-23 and 25-33 below. Veritas.

On page 3 of the Bill, in line 17 delete the words "Cyber Security and".

AMENDMENT OF CLAUSE 3 (INTERPRETATION)

BY HON. GANDAWA

Clause 3 of the Bill is amended on page 4—

(a) in line 9 by the deletion of the "resources" and the substitution of "processes";

(b) in lines 23 and 24 by the deletion of the definition for "data controller or controller" and the substitution of—

""data controller or controller"—

(a)refers to any natural person or legal person who is licensable by the Authority;

(b)includes public bodies and any other person who determines the purpose and means of processing data;".

AMENDMENT OF CLAUSE 4 (APPLICATION)

BY HON. GANDAWA

Clause 4 of the Bill is amended on page 6 in lines 13, 17, 19 and 21 by the insertion of "and
storage" after the word "processing".

SUBSTITUTION OF CLAUSE 13 (SENSITIVE INFORMATION)

BY THE MINISTER OF INFORMATION COMMUNICATION TECHNOLOGY, POSTAL AND COURIER SERVICES

On page 9 of the Bill, in line 16 delete clause 13 and substitute with —

"**13Sensitive information**

(1) No data controller shall process sensitive data unless the data subject has given consent in writing for such processing;

(2) the consent to the processing of data may be withdrawn by the data subject at any time and without any explanation and free of charge;

(3) the Authority shall determine the circumstances in which the prohibition to process the data referred to in this subsection (1) cannot be lifted even with the data subject's consent "taking into account the factors surrounding the prohibition and the reasons for collecting the data".

(4) The Minister responsible for the Cyber security and Monitoring Centre in consultation with the Minister, may give directions on how to implement this section with respect to sensitive information affecting National security or the interests of the State.

(5) The provisions of subsection (1) shall not apply where—

(a) the processing is necessary to carry out the obligations and specific rights of the controller in the field of employment law; or

(b) the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his or her consent or is not represented by his or her legal, judicial or agreed representative; or

(c) the processing is carried out in the course of its legitimate activities by a foundation, association or any other non-profit organisation with a political, philosophical, religious, health-insurance or trade-union purpose and on condition that the processing relates solely to the members of the organisation or to persons who have regular contact with it in connection with such purposes and that the data is not disclosed to a third party without the data subjects' consent; or

(d) the processing is necessary to comply with national security laws; or

(e) the processing is necessary, with appropriate guarantees, for the establishment, exercise or defence of legal claims; or

(f) the processing relates to data which has been made public by the data subject; or

(g) the processing is necessary for the purposes of scientific research:

Provided the Authority shall be entitled to specify the conditions under which such processing may be carried out; or

(h) the processing of data is authorised by a law or any regulation for any other reason constituting substantial public interest.

(6) Without prejudice to the application of sections 5 to 8, the processing of data relating to sex life is authorised if—

(a) it is carried out by an association with a legal personality or by an organisation of public interest whose main objective, according to its Memorandum and Articles of Association, is the evaluation, guidance or treatment of persons of such sexual conduct, and who is recognised by a competent public body as being responsible for the welfare of such persons;

(b) the objective of the processing of the data consist of the evaluation, guidance and treatment of the persons referred to in this section, and the processing of data relates only to the aforementioned persons:

Provided that the competent public body referred to in paragraph (a) grants a specific, individualised authorisation, having received the opinion of the Authority.

(7) The authorisation referred to in this section shall specify the duration of the authorisation, the conditions for supervision of the authorised association or organisation by the competent public body, and the way in which the processing must be reported to the Authority."

INSERTION OF NEW CLAUSES 15 AND 16

BY HON. GANDAWA

The bill is amended on page 11 in line 22 by the insertion of the following new clauses and the subsequent clauses shall be accordingly renumbered—

"**15 Duties of Data Controllers**

Every data controller or data processor shall ensure that personal information is—

(a) processed in accordance with the right to privacy of the data subject;

(b) processed lawfully, fairly and in a transparent manner in relation to any data subject;

(c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is

processed;

(e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

(f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; and

(g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected.

16 Rights of Data Subject

A data subject has a right to—

(a) be informed of the use to which their personal information is to be put;

(b) access their personal information in custody of data controller or data processor;

(c) object to the processing of all or part of their personal information;
(d) correction of false or misleading personal information; and
(e) deletion of false or misleading data about them.".

AMENDMENT OF CLAUSE 19 (SECURITY BREACH NOTIFICATION)

BY HON. GANDAWA

Clause 19 of the Bill is amended on page 13 in line 17 by the deletion of "without an undue delay" and the substitution of "within twenty-four (24) hours".

AMENDMENT OF CLAUSE 20 (OBLIGATION OF NOTIFICATION TO AUTHORITY)

BY HON. GANDAWA

Clause 20 of the Bill is amended on page 13 in line 39 by the deletion of sub-clause (6) and the substitution of the following—

"(6) The Authority shall provide guidelines that provide for the qualifications and functions of a data protection officer and such data protection officer's duties shall include—

(a) ensuring compliance by the data controller with the provisions of this Act and regulations made thereunder;
(b) dealing with requests made to the data controller pursuant to this Act;
(c) working with the Authority in relation to the performance of its functions in relation to the data controller.".

AMENDMENT OF CLAUSE 28 (TRANSFER OF PERSONAL INFORMATION OUTSIDE ZIMBABWE)

BY THE MINISTER OF INFORMATION COMMUNICATION TECHNOLOGY, POSTAL AND COURIER SERVICES

On page 16 of the Bill in line 13, insert a new sub-clause (4) as follows—

"(4) The Minister responsible for the Cyber security and Monitoring Centre in consultation with the Minister, may give directions on how to implement this section with respect to transfer of personal information outside of Zimbabwe."

AMENDMENT OF CLAUSE 33 (OFFENCES AND PENALTIES)

BY THE MINISTER OF INFORMATION COMMUNICATION TECHNOLOGY, POSTAL AND COURIER SERVICES

On page 18 of the Bill in line 5, insert after "11" the number "13"

AMENDMENT OF CLAUSE 35 (AMENDMENT OF CHAPTER VIII OF CAP.9:23)

BY THE MINISTER OF INFORMATION COMMUNICATION TECHNOLOGY, POSTAL AND COURIER SERVICES

On page 21 of the Bill, in line 9 insert a new sub paragraph after sub paragraph (d) as follows—

"(e) in an aggravating circumstance certified by the Cyber Security and Monitoring Centre to be a breach of state security to a fine not exceeding level 14 or to imprisonment for a period not exceeding 10 years or to both such fine and such imprisonment."

On page 27 of the Bill, in line 6 delete clauses 165B to 166D.

AMENDMENT OF CLAUSE 35 (AMENDMENT OF CHAPTER VIII of Cap 9:23)

BY HON. GANDAWA

Clause 35 of the Bill is amended—

(a) on page 24 in line 44 by the insertion of "(3) Any person who up skirts and records nude images or videos of a citizen or resident of Zimbabwe without consent shall be guilty of an offence and liable to a fine not exceeding level 10 or imprisonment for a period not exceeding 5 years or both such fine or such imprisonment";

(b) on page 26 in lines 3-10 by the deletion of—

"Any person who unlawfully and intentionally by means of a computer or information system generates and sends any data message to another person, or posts on any material whatsoever on any electronic medium accessible by any person, with the intent to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress, or to degrade, humiliate or demean the person of another or to encourage a person to harm himself or herself, shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.";

and the substitution of—

"(1)Any person who unlawfully and intentionally by means of information and communication technologies generates and sends any data message to another person, or posts on any material whatsoever on any electronic medium accessible by any person, with the intent to coerce, intimidate, harass, threaten, bully or cause substantial emotional distress, or to degrade, humiliate or demean the person of another or to encourage a person to harm himself or herself, shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment.

(2) Special consideration shall be given when a child is found guilty of any of the offences set out in (1), in line with the law of Zimbabwe:

Provided that the penalty shall not give the child a criminal record nor shall the child be imprisoned for this offence.".

(c) on page 26 in lines 34-39 by the deletion of—

"Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes a data message containing any intimate image of an identifiable person without the consent of the person concerned causing the humiliation or embarrassment of such person shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment".

and the substitution of—

"Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes a data message

containing any intimate image or video of an identifiable person without the consent of the person concerned or with recklessness as to the lack of consent of the person concerned, with the aim of causing the humiliation or embarrassment of such person shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.".

(d) on page 27 by the insertion of the following after line 22—

"164F. Recording of genitalia and buttocks beneath closing without consent

(1) Any person who unlawfully and intentionally records an image or video beneath the clothing of another person which depicts this person's genitalia or buttocks, whether covered by underwear or not, without the consent of the depicted person or with recklessness as to the lack of consent of the person concerned, as far as these are to be protected against sight according to the recognizable will of the depicted person, shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

(2) Section 164E shall apply *mutatis mutandis* to any person who makes available, broadcasts or distributes a data message containing an image or video as described in (1).";

(e) on page 27 in lines 25-38 by the deletion of the text headed "Child Pornography" and the substitution of the following—

"165 Child sexual abuse material

(1) In this Act—

"Child sexual abuse material" means any representation through publication, exhibition, cinematography, electronic means or any other means whatsoever, of a child, a person made to appear as a child or realistic material representing a child, engaged in real or simulated explicit sexual activity, or any representation of the sexual parts of a child for primarily sexual purposes.

(2)Any person who unlawfully and intentionally, through a computer or information system—

(a) produces child sexual abuse material;
(b) offers or makes available child sexual abuse material;
(c) distributes or transmits child sexual abuse material;
(d) procures or obtains child sexual abuse material for oneself or for another person;
(e) possesses child sexual abuse material on a computer system or a computer-data storage medium;
(f) knowingly obtains, accesses or procures child sexual abuse material;
(g) baits a child into the production or distribution of child sexual abuse material

shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years, or both such fine and such imprisonment.

(3) Any person of 18 years or above, who unlawfully and intentionally through information and communication technologies, proposes to meet a child who

has not reached the age of consent to sexual activity as set by the Criminal Law (Codification and Reform Act) [*Chapter 9:23*] for the purpose of engaging in sexual activity with him or her, where this proposal has been followed by material acts leading to such a meeting, shall be guilty of an offence and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding ten years, or both such fine and such imprisonment.".

(f) on page 31 by the insertion of the following paragraph after line 37—
"(f) against citizens or permanent residents of Zimbabwe."

INSERTION OF NEW CLAUSE 36 (AMENDMENT OF CAP.9:07)

BY THE MINISTER OF INFORMATION COMMUNICATION TECHNOLOGY, POSTAL AND COURIER SERVICES

On page 27 of the Bill, in line 6 insert a new clause as follows—
" **36 Insertion of New Part in Cap.9:07**

The Criminal Procedure and Evidence Act [*Chapter 9:07*] is amended by the insertion of

after Part XX of the following Part—

"PART XXA

PROVISIONS RELATING TO CYBER CRIME

"379ASearch and seizure

(1) In this section "seize" includes—

(a) taking possession of or securing a computer;

(b) securing a computer system or part thereof or a computer-data storage medium;

(c) taking a printout or output of computer data;

(d) making and retaining a copy of computer data, including through the use of use of onsite equipment;

(e) activating any onsite computer system or computer data storage media;

(f) maintaining the integrity of any stored relevant computer data;

(g) rendering inaccessible or removing computer data in the accessed computer system.

(2) A magistrate may, on an application by a police officer in the prescribed form, that specified computer data or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, order that—

(a) a person in Zimbabwe in control of the relevant computer system produce from the system specified computer data or a printout or other intelligible output of that data; or

(b) an electronic communications service provider in Zimbabwe produce information about persons who subscribe to or otherwise use the service.

(3) An application referred to in subsection (1) shall be supported by an affidavit in which the police officer shall set out the offence being investigated, the computer system in which it is suspected to be stored,

the reasonable grounds upon which the belief is based, the measures that will be taken in pursuance of the investigation and the period over which those measures will the taken.

(4) A police officer granted a warrant in terms of this section may—

(a) if there are reasonable grounds to believe that computer data concerned is susceptible to loss, alteration, deletion, impairment or modification, by written notice given to a person in control of the computer data, require the person in control of the data to ensure that the data specified in the notice is preserved for a period not exceeding seven days as may be specified in the notice which period may be extended, on an application to a magistrate, for such period as the magistrate may grant;

(b) by written notice to a person in control of the computer system or information system concerned, require the person in control thereof to disclose relevant traffic data concerning specified communications in order to identify—

(i) the service providers; or

(ii) (ii) the path through which the communication was transmitted.

(5) Any person who does not comply with the order given in terms of this section shall be guilty of an offence and liable to a fine.

379B Expedited preservation

(1) A magistrate may, on an application by a police officer in the prescribed form, that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is required for the purposes of a criminal investigation—

(a) order any person in control of such data to—

(i) collect, record or preserve the traffic data associated with a specified communication during a specified period; or

(ii) permit and assist a specified police officer to collect or record that data.

(b) authorise the police officer to collect or record traffic data associated with a specified communication during a specified period through the use of any appropriate technological means.

(2) Section 33(3) of the Data Protection Act [*Chapter 11:22*] shall apply *mutatis mutandis* to an application in terms of this section.

379C Obligations and immunity of service providers

(1) An electronic communications network or access service provider shall not be criminally liable for providing access or transmitting information through its system if such service provider has not—

(a) initiated the transmission; or

(b) selected the receiver of the transmission; or

(c) (c)selected or modified the information contained in the transmission.

(2) The provision of access or the transmission referred to in subsection (1) shall include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and the information is not stored for any period longer than is reasonably necessary for the transmission.

(3) A hosting provider shall not be criminally liable for the information stored at the request of a user of the service if the hosting provider—

(a) promptly removes or disables access to the information after receiving an order from any court of law to remove specific stored illegal information; or

(b) (b) in any other manner, obtains knowledge or becomes aware of any illegal information stored, promptly informs the appropriate authority to enable it to evaluate the nature of the information and if necessary, issue an order for its removal.

(4) Subsection (3) shall not apply where the user of the service is acting under the authority or the control of the hosting provider.

(5) Where the hosting provider removes the content after receiving an order pursuant to sub-section (3), no liability shall arise from the contractual obligations with the user with regard to the availability of the service.

(6) A hosting provider who fails to remove or disable access to information in terms of subsection (3) shall be guilty of an offence and liable to a fine not exceeding level 8 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(7) A caching provider shall not be criminally liable for the automatic, intermediate or temporary storage of information where the caching was performed for the sole purpose of making the onward transmission of the information to other users of the service upon their request more efficient if the caching provider—

(a) does not modify the information;

(b) complies with conditions of access to the information;

(c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(d) (d)does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) (e)acts promptly to remove or to disable access to the information it has stored upon obtaining knowledge that the information has been removed from the network at the initial source of the transmission, or that access to it has been disabled, or that a court or an appropriate public authority has ordered such removal or disablement.

(8) A caching provider who contravenes the conditions set out in subsection (7) shall be guilty of an offence and liable to a fine not exceeding level 8 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(9) An internet service provider who enables access to information provided by a third person by providing an electronic hyperlink shall not be criminally liable with respect to the information if the internet service provider—

(a) promptly removes or disables access to the information after receiving an order from an appropriate public authority or court to remove the link; or

(b) (b)through other means, obtains knowledge or becomes aware of stored specific illegal information promptly informs the appropriate authority to enable it to evaluate the nature of the information and if necessary issue an order for its removal.

(10) An internet service provider who fails to promptly remove or disable access to information in terms of subsection (9) shall be guilty of an offence and liable to a fine not exceeding level 8 or to imprisonment for a period not exceeding two years or both such fine and such imprisonment.

(11) Any service provider who knowingly enables access to, stores, transmits or provides an electronic hyperlink to, any information with knowledge of the unlawfulness of the content of any such information

shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment not exceeding a period of ten years or to both such fine and such imprisonment.

379D Jurisdiction

(1) A court in Zimbabwe shall have jurisdiction to try any offence under this Act where the offence was committed wholly or in part—

(a) within Zimbabwe or by any person in or outside Zimbabwe using a computer or information system or device, software or data located in Zimbabwe; or

(b) on a ship or aircraft registered in Zimbabwe; or

(c) by a national or permanent resident of Zimbabwe or a person carrying on business in Zimbabwe, whether or not the offence is committed in Zimbabwe; or

(d) by a national or permanent resident of Zimbabwe or a person carrying on business in Zimbabwe and the offence is committed outside Zimbabwe, if the person's conduct also constitutes an offence under the law of the country where the offence was committed and harmful effects were caused in Zimbabwe; or

(e) by any person, regardless of the location, nationality or citizenship of the person—

(i) using a computer or information system or device, software, or data located within Zimbabwe; or directed against a computer or information system or

(ii) device, software or data located in Zimbabwe.

379E Admissibility of electronic evidence

(1) In any criminal proceedings for an offence in terms of this Act, evidence generated from a computer system or by means of information and communications technologies or electronic communications systems shall be admissible in court.

(2) In assessing the admissibility or evidential weight of the evidence, regard shall be given to—

(a) the reliability of the manner in which the evidence was generated, stored or communicated

(b) the integrity of the manner in which the evidence was maintained;

(c) the manner in which the originator or recipient of the evidence was identified; and

(d) any other relevant factors.

(3) The authentication of electronically generated documents shall be as prescribed in rules of evidence regulating the integrity and correctness of any other documents presented as evidence in a court of law.

(4) This section shall apply in addition to and not in substitution of any other law in terms of which evidence generated by computer systems or information and communications technologies or electronic communications systems or devices may be admissible in evidence.

379F Forfeiture

A court convicting any person of an offence under this Act may order the forfeiture to the State of—

(a) any money, asset or property constituting or traceable to the gross proceeds of such offence; and

(b) any computer or information system, software or other devices used or intended to be used to commit or to facilitate the commission of such offence."

INSERTION OF NEW CLAUSE 37 (AMENDMENT OF CAP.11:22)

BY THE MINISTER OF INFORMATION COMMUNICATION TECHNOLOGY, POSTAL AND COURIER SERVICES

On page 31 of the Bill, insert after clause 36 a new clause as follows—

"37 Amendment of Cap.11:22

(1) The Interception of Communications Act [*Chapter 11:20*] (hereinafter called the "principal Act") is amended in section 2 —

(a)by the repeal of the definition of "monitoring centre" and substitution of—

""cyber security and monitoring centre" means the Cyber Security and Monitoring of Interception of Communications Centre being unit central monitoring apparatus designated to be the monitoring facility through which all the intercepted communications and call-related information of a particular interception target are forwarded to an authorised person;"

(2) The principal Act is amended in by the repeal of section 4 and the following is substituted—

"4 Cyber Security and Monitoring of Interceptions of Communications Centre

(1) There shall be established a unit in the Office of the President, which shall be called the Cyber Security and Monitoring of Interception of Communications Centre.

(3) The cyber security and monitoring centre shall be advised by a committee which shall give advice to the director of the centre on whether or not a warrant should be issued.

The cyber security and monitoring centre shall be manned, controlled and operated by technical experts designated by the agency.

(4) The cyber security and monitoring centre shall give technical advice to—

(a) authorised persons; and

(b) service providers;

on cyber security and the interception of communications in terms of this Act.

(3) The principal Act is amended by the insertion after section 4 of the following sections—

" 4A Functions of Cyber Security and Monitoring of Interceptions of Communications Centre

The functions of the Cyber Security and Monitoring Centre shall be to—

(a) be the sole facility through which authorised interceptions shall be effected;

(b) advise Government and implement Government policy on cybercrime and cyber security;

(c) identify areas for intervention to prevent cybercrime;

(d) coordinate cyber security and establish a national contact point available daily around-the-clock;

(e) establish and operate a protection-assured whistle-blower system that will enable members of the public to confidentially report to the Committee cases of alleged cybercrime;

(f) promote and coordinate activities focused on improving cyber security and preventing cybercrime by all interested parties in the public and private sectors;

(g) provide guidelines to public and private sector interested parties on matters relating to awareness, training, enhancement, investigation, prosecution and combating cybercrime and managing cyber security threats;

(h) oversee the enforcement of the Act to ensure that it is enforced reasonably and with due regard to fundamental human rights and freedoms;

(i) provide technical and policy advice to the Minister;

(j) advise the Minister on the establishment and development of a comprehensive legal framework governing cyber security matters.

4B Establishment of Cybersecurity Committee

(1) There is hereby established a committee to be known as the Cybersecurity Committee which will shall be an ad hoc advisory body to the Minister.

(2) The Cyber Security Committee shall consist of eleven members appointed by the Minister for their knowledge in computer and telecommunications, law and policy and skills in respect of any aspect dealt with in this Act as follows—

(a) one representative nominated by each of the following—

(i) the Postal and Telecommunications Regulatory Authority of Zimbabwe;

(ii) the ministry responsible for information and communications technologies;

(ii) the ministry responsible for science and technology;

(iii) the ministry responsible for justice;

(iv) the Zimbabwe Republic Police;

(v) the National Prosecution Authority;

(vi) the ministry responsible for defence;

(vii) the Central Intelligence Organisation;

(viii) the Prisons and Correctional Service;

(b) one representative from the cyber security and monitoring centre;

(c) any representative from any sector of the economy or any other person who may be necessary to the deliberations in respect of a particular warrant, appointed on an ad hoc basis.

(4) From among the appointed members, the Minister shall appoint the Chairperson of the Cybersecurity Committee.

(5) The Committee shall, at its first meeting, elect a Vice-Chairperson of the Board from among its members:

Provided that the Chairperson and the Vice Chairperson shall be of different genders.

(6) The provisions of the Schedule apply to the Cybersecurity Committee.

(7) The Cyber Security Committee may, with the approval of the Minister, issue such guidelines as may be necessary for the carrying out of the provisions of this Act as it relates to its functions under this Act."

(4) The principal Act is amended in section 5 by the insertion after subsection 3 of the following subsection—

"(4) The Minister, upon receiving an application for a warrant in terms of this section, shall refer the application to the Cyber security committee, who shall advise the Minister on whether or not any of the reasonable grounds to issue a warrant referred to in section 6 are present:

Provided that Minister may issue a provisional warrant if in his or her opinion any of the reasonable grounds referred to in section 6 are present.

(5) The Minister may withdraw a warrant issued provisionally upon the advice of the Committee that no reasonable grounds to issue to the warrant existed, without prejudice to anything that may be done by virtue of the warrant issued by the Minister between the time he or she issued it provisionally and the time it was referred to the committee and withdrawn."

(5) The principal Act is amended by the insertion of the following Schedule —

"**SCHEDULE (4B (6))**

PROVISIONS APPLICABLE TO CYBERSECURITY COMMITTEE

Terms and conditions of office of members

1. (1) Subject to this Schedule, a member shall hold office for such period, not exceeding five years, as the Minister may fix on his or her appointment.

(2) Subject to paragraph 8, a member shall hold office on such conditions as the Minister may fix in relation to members generally.

(3) A retiring member shall be eligible for re-appointment as a member.

Disqualification for appointment as member

2. (1) The Minister shall not appoint a person as a member and no person shall be qualified to hold office as a member if he or she—

(a) is married to a person who is engaged in any activity connected with any business, if in the opinion of the Minister such financial interest or activity is likely to interfere with the impartial discharge by that person of his or her duties as a member; or

(b) has, in terms of a law in force in any country—

(i) been adjudged or otherwise declared insolvent or bankrupt and has not been rehabilitated or discharged; or

(ii) made an assignment to, or arrangement or composition with, his or her creditors which has not been rescinded or set aside;or

(c) has, within the period of five years immediately preceding the date of his or her proposed appointment, been convicted—

(i) in Zimbabwe, of an offence; or

(ii) outside Zimbabwe, in respect of conduct which if committed in Zimbabwe would constitute an offence; and sentenced to a term of imprisonment imposed without the option of a fine, whether or not any portion has been suspended, and has not received a free pardon.

(2) A person who is—

(a) a member of Parliament; or

(b) a member of two or more other statutory bodies;

shall not be appointed as a member, nor shall he or she be qualified to hold office as a member.

(3) For the purpose of subparagraph (2)(b)—

(a) a person who is appointed to a council, board or other authority which is a statutory body or which is responsible for the administration of the affairs of a statutory body, shall be regarded as a member of that statutory body;

(b) "statutory body" means—

(i) any Commission established by the Constitution; or

(ii) any body corporate established-directly by or under an Act for special purposes specified in that Act, the membership of which consists wholly or mainly of persons appointed by the President, Vice President, a Minister or a statutory body or by a Commission established by the Constitution

Vacation of office by member

3. A member shall vacate his or her office and the member's office shall become vacant—

(a) one month after the date upon which he or she gives notice in writing to the Minister of his or her intention to resign or on the expiry of such other period of notice as the member and the Minister may agree; or

(b) on the date he or she begins to serve a sentence of imprisonment imposed in Zimbabwe without the option of a fine—

(i) in Zimbabwe, in respect of an offence; or

(ii) outside Zimbabwe, in respect of conduct which if committed in Zimbabwe, would constitute an offence; or

(c) if he or she becomes disqualified in terms of paragraph 2(1)(a), (b) or (c) to hold office as a member; or

(d) if he or she is required in terms of paragraph 4 to vacate his or her office.

Dismissal or suspension of members

4. (1) The Minister may require a member to vacate his or her office if the member—

(a) has been guilty of any conduct that renders him or her unsuitable as a member; or

(b) has failed to comply with the conditions of his or her office fixed by the Minister in terms of paragraph 1(2); or

(c) is mentally or physically incapable of efficiently carrying out his or her functions as a member.

(2) The Minister, on the recommendation of the Board, may require a member to vacate his or her office if the member has been absent without the permission of the Board from two consecutive meetings of the Board of which he or she was given at least seven days' notice and there was no just cause for the member's absence.

(3) The Minister may suspend a member—

(a) whom he or she suspects on reasonable grounds of having been guilty of conduct referred to in subparagraph (1)(a); or

(b) against whom criminal proceedings have been instituted for an offence in respect of which a sentence of imprisonment without the option of a fine may be imposed; and while that member is so suspended he or she shall not carry out any functions as a member.

Filling of vacancies in Board

5. On the death of or the vacation of office by a member the Minister shall appoint a person to fill the vacancy.

Meetings and procedure of Board

6. (1) The Cybersecurity Committee shall hold its meetings on an ad hoc basis on such date and at such place as the Minister may fix.

(2) The chairperson or, in his or her absence, the vice-chairperson shall preside at all meetings of the Committee:

Provided that, if the chairperson and the vice-chairperson are absent from a meeting of the Committee, the members present may elect one of their number to preside at that meeting as chairperson.

(3) Five members shall form a quorum at any meeting of the Committee.

(4) All acts, matters or things authorised or required to be done by the Committee may be decided by a majority vote at a meeting of the Committee at which a quorum is present.

(8) Subject to subparagraph (9), at all meetings of the Committee each member present shall have one vote on each question before the Committee and, in the event of an equality of votes, the chairperson shall have a casting vote in addition to a deliberative vote.

Validity of decisions and acts of Board

7. No decision or act of the Committee or act done under the authority of the Committee shall be invalid by reason only of the fact that a disqualified person acted as a member of the Committee at the time the decision was taken or act was done or authorised.

Minutes of proceedings of Board and committees

8. (1) The Committee shall cause minutes of all proceedings of and decisions taken at every meeting of the Committee to be entered in books kept for the purpose in a confidential manner."
