REPUBLIC OF SOUTH AFRICA

CRITICAL INFRASTRUCTURE PROTECTION BILL

(As amended by the Portfolio Committee on Police (National Assembly))
(The English text is the official text of the Bill)

(MINISTER OF POLICE)

[B 22B—2017]

ISBN 978-1-4850-0463-9

No. of copies printed 800

BILL

To provide for the identification and declaration of infrastructure as critical infrastructure; to provide for guidelines and factors to be taken into account to ensure transparent identification and declaration of critical infrastructure; to provide for measures to be put in place for the protection, safeguarding and resilience of critical infrastructure; to provide for the establishment of the Critical Infrastructure Council and its functions; to provide for the administration of the Act under the control of the National Commissioner as well as the functions of the National Commissioner in relation to the Act; to provide for the establishment of committees and their functions; to provide for the designation and functions of inspectors; to provide for the powers and duties of persons in control of critical infrastructure; to provide for reporting obligations; to provide for transitional arrangements; to provide for the repeal of the National Key Points Act, 1980, and related laws; and to provide for matters connected therewith.

PREAMBLE

WHEREAS the Constitution of the Republic of South Africa, 1996, provides that all spheres of government and all organs of state must secure the well-being of the people of the Republic;

AND WHEREAS the Constitution of the Republic provides for the right of access to information, subject to the limitations provided for in section 36 of the Constitution;

AND WHEREAS the protection of critical infrastructure is essential for public safety, national security and the continuous provision of basic public services;

AND WHEREAS it is necessary to put in place adequate measures to identify and protect critical infrastructure and the implementation of those measures in order to secure critical infrastructure;

MINDFUL of the need to follow objective criteria with regard to the identification and declaration of critical infrastructure;

AND FURTHER MINDFUL of the need for the roles, responsibilities and accountability of parties with regard to the protection of critical infrastructure to be defined and for the enhancement of public confidence and awareness in respect of the protection of critical infrastructure;

AND REALISING the need to enhance cooperation between Government and the private sector with regard to the protection of critical infrastructure in the interests of the Republic,

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

ARRANGEMENT OF SECTIONS

CHAPTER 1

DEFINITIONS, PURPOSE AND APPLICATION OF ACT

CHAPTER 2

CRITICAL INFRASTRUCTURE COUNCIL AND STRUCTURES

Part A

Critical Infrastructure Council

Part B

Administration of Act

Part C

Committees, exemption and delegations

CHAPTER 3

DECLARATION AS CRITICAL INFRASTRUCTURE AND DETERMINATION OF CRITICAL INFRASTRUCTURE COMPLEX

CHAPTER 1

DEFINITIONS, PURPOSE AND APPLICATION OF ACT

Definitions

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

"basic public service" includes a service, whether provided by the public or private sector, relating to communication, energy, health, sanitation, transport and water, the interference with which may prejudice the livelihood, well-being, daily operations or economic activity of the public;

"critical infrastructure" means any infrastructure which is declared as such in terms of section 20(4) and includes a critical infrastructure complex where required by the context;

"critical infrastructure complex" means more than one critical infrastructure grouped together for practical or administrative reasons, which is determined as such in terms of section 16(3);

"Critical Infrastructure Council" means the Critical Infrastructure Council established in terms of section 4, and ''Council'' has a corresponding meaning;

"cyber response committee" means any cyber response committee established in terms of any cybersecurity legislation;

"disaster management centre" includes the 'National Centre', 'provincial disaster management centre' and 'municipal disaster management centre' as defined in section 1 of the Disaster Management Act, 2002 (Act No. 57 of 2002);

"government infrastructure" for the purposes of section 9(4) and section 19 means infrastructure controlled, owned, occupied or possessed by a government department in the national sphere and in respect of whose operation or administration that department is responsible;

"Head of a Government department" means—

(a) the incumbent of a post mentioned in Column 2 of Schedule 1, 2 or 3 to the Public Service Act, 1994 (Proclamation No. 103 of 1994), and includes any person acting in such post; or

(b) a municipal manager appointed in terms of section 54A of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000), and includes any person acting in such post;

"infrastructure" means any building, centre, establishment, facility, installation, pipeline, premises or systems needed for the functioning of society, the Government or enterprises of the Republic, and includes any transport network or network for the delivery of electricity or water but excludes any information infrastructure as contemplated in any legislation on cybersecurity;

"Minister" means the Cabinet member responsible for policing;

"National Commissioner" means the National Commissioner of the South African Police Service, appointed in accordance with section 207(1) of the Constitution;

"national security" has the meaning ascribed to it in section 198 of the Constitution;

"organ of state" means an 'organ of state' as defined in section 239 of the Constitution;

"person in control of a critical infrastructure" means—

(a) the owner of a critical infrastructure;

(b) the person who, by virtue of—

(i) any right acquired from a person referred to in paragraph *(a)*;

(ii) any other right acquired from any other person whether by way of a public-private partnership or similar agreement; or

(iii) operation of law,

occupies, possesses, is in control of, or is responsible for the operation or administration of such a critical infrastructure; or

(c) the Head of a Government department or the head of any other organ of state who occupies, possesses, is in control of, or is responsible for the operation or administration of a critical infrastructure, and includes any employee acting in such post, and **"person in control of an infrastructure"** shall be construed accordingly;

"police official" means a member of the South African Police Service as defined in section 1 of the South African Police Service Act, 1995 (Act No. 68 of 1995);

"prescribe" means prescribed by regulation;

"PSIRA" means the Private Security Industry Regulatory Authority established in terms of section 2(1) of the Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001);

"regulatory measures" means any security measure that must be implemented as provided for in this Act;

"resilience" means the ability of infrastructure to mitigate, absorb or withstand any damage, disruption, disturbance or interference in order to maintain the functionality, integrity and structural capacity of that infrastructure;

"risk category" means a risk category as contemplated in section 20(4);

"Secretary for the Police Service" means the Secretary for the Police Service appointed in terms of section 7(1) of the Civilian Secretariat for the Police Service Act, 2011 (Act No. 2 of 2011);

"security" includes, but is not limited to—

(a) physical security of critical infrastructure;

(b) personnel security at critical infrastructure;

(c) contingency plans applicable to critical infrastructure; and

(d) measures aimed at protecting critical infrastructure;

"security manager" means the person appointed in terms of section 24(7);

"security measures" means any physical security measure to preserve the availability, integrity or confidentiality of a critical infrastructure, and includes, but is not limited to, physical security measures to protect—

(a) any part or component of a critical infrastructure;

(b) any physical structure that partly consists of, incorporates or houses information infrastructure; or

(c) personnel or other persons at or nearby a critical infrastructure;

"security personnel" means any person registered as a security officer in terms of section 21 of the Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001);

"security service provider" means a security service provider as defined in section 1 of the Private Security Industry Regulation Act, 2001;

"this Act" includes the regulations; and

"threat" includes any action or omission of a criminal, terrorist or accidental nature which may potentially cause damage, harm or loss to critical infrastructure or interfere with the ability or availability of critical infrastructure to deliver basic public services, and may involve any natural hazard which is likely to increase the vulnerability of critical infrastructure to such action or omission.

Purpose of Act

2. The purpose of this Act is to—

(a) secure critical infrastructure against threats;

(b) ensure that information pertaining to security measures applicable to critical infrastructure remains confidential, subject to the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), or any other Act of Parliament that provides for the lawful disclosure of information;

(c) ensure that objective criteria are developed for the identification, declaration and protection of critical infrastructure;

(d) ensure public-private cooperation in the identification and protection of critical infrastructure;

(e) secure critical infrastructure in the Republic by creating an environment in which public safety, public confidence and basic public services are promoted—

(i) through the implementation of measures aimed at securing critical infrastructures; and

(ii) by mitigating risks to critical infrastructures through assessment of vulnerabilities and the implementation of appropriate measures;

(f) promote cooperation and a culture of shared responsibility between various role-players in order to provide for an appropriate multi-disciplinary approach to deal with critical infrastructure protection;

(g) enhance the collective capacity of role-players who are responsible for the protection of critical infrastructure to mitigate possible security risks;

(h) ensure that every critical infrastructure complies with regulatory measures aimed at securing such critical infrastructure against threats;

(i) provide for the powers and duties of persons in control of critical infrastructure; and

(j) support integration and coordination of the functions of various role-players involved in the securing of critical infrastructure.

Application of Act

3. (1) This Act applies to—

(a) the identification and declaration of infrastructure as critical infrastructure;

(b) the determination of critical infrastructure as critical infrastructure complex; and

(c) the protection of critical infrastructure,

and binds any person to whom a function has been assigned in terms of this Act.

(2) This Act does not apply to infrastructure under the control of the Department of Defence.

CHAPTER 2

CRITICAL INFRASTRUCTURE COUNCIL AND STRUCTURES

Part A

Critical Infrastructure Council

Establishment and composition of Critical Infrastructure Council

4. (1) A Critical Infrastructure Council is hereby established.

(2) The Minister appoints members of the Critical Infrastructure Council which must consist of the following persons:

(a) the Secretary for the Police Service;

(b) an official at the level of at least Chief Director or an equivalent level, designated by each of the heads of the following institutions—
(i) Department of Defence;
(ii) Department of Home Affairs;
(iii) Department of Public Works;
(iv) National Disaster Management Centre;
(v) South African Local Government Association;
(vi) South African Police Service; and
(vii) State Security Agency; and

(c) five members appointed in terms of subsection (8) from the private sector and civil society who are—
(i) not disqualified in terms of section 5; and
(ii) preferably appropriately qualified, knowledgeable and experienced in fields that include critical infrastructure protection, risk management, disaster management or basic public services.

(3) The members of the Council must, when viewed collectively, preferably be persons who are suited to serve in the Council by virtue of their qualifications, expertise and experience in fields that include infrastructure protection, engineering, disaster management or security policy.

(4) In the event that—

(a) the functions or functioning of infrastructure that forms the subject of an application for declaration as critical infrastructure may affect or be affected by the functional area of responsibility of a government department or an organ of state not referred to in subsection (2)*(b)*, the Chairperson may request the Head of that Government department or the head of that organ of state to designate an appropriately qualified official to assist with such application; or

(b) the Council is of the opinion that any other person could assist in general or with a specific application for declaration as critical infrastructure, the Council may request the Minister to appoint such person on an *ad hoc* basis to advise or assist the Council.

(5) The Minister must appoint—

(a) officials referred to in subsection (2)*(b)* after consultation with the Cabinet member responsible for the institution in question;

(b) members referred to in subsection (2)*(c)* in terms of subsection (8); and

(c) persons referred to in subsection (4)*(b)* on advice of the Council.

(6) In the event that it is necessary to appoint a member referred to in subsection 2*(c)*, the Minister must request the National Assembly to submit a list of candidates for appointment.

(7) The Speaker must refer the matter to the relevant committee of the National Assembly to—

(a) publish a notice in the Gazette and in at least two national newspapers circulating in the Republic, inviting applications from interested persons and members of the public to nominate persons;

(b) compile a shortlist of not less than 20 persons who are not disqualified in terms of section 5*(a)*, *(c)*, *(d)*, *(e)*, or *(f)*, from the applications and nominations referred to in paragraph *(a)* or persons serving on the Council who qualify for a further appointment in terms of subsection (10);

(c) submit the list referred to in paragraph *(b)* to the State Security Agency for consideration and issuing of a top secret security clearance;

(d) conduct interviews with the persons referred to in paragraph *(b)* who are not disqualified in terms of section 5*(b)* for purposes of compiling a list of 10 recommended candidates in order of preference;

(e) submit the list of names referred to in paragraph *(d)* to the National Assembly for approval; and

(f) submit the approved list of names contemplated in paragraph *(e)* together with their résumés to the Minister.

(8) The Minister must appoint five members to the Council from the list referred to in subsection (7)*(f)* and publish the names of the members in the *Gazette*.

(9) Subject to subsection (12), a member of the Council appointed in terms of subsection (8) holds office for a period not exceeding five years.

(10) Upon the expiry of an appointed member's first term of office as contemplated in subsection (9), the member may be re-appointed for one further term only.

(11) The Secretary for the Police Service is the Chairperson of the Council and the Minister must designate, from the persons contemplated in subsection (2)*(c)*, a member as deputy chairperson.

(12) A member of the Council appointed in terms of subsection (8) must vacate office if that member—

(a) resigns by giving at least 30 days written notice addressed to the Minister; or

(b) is removed from office by the Minister as contemplated in subsection (14).

(13) If a member of the Council appointed in terms subsection (8) resigns or vacates office before the expiry of his or her period of office, the Minister must request the National Assembly to follow the procedure in subsection (7). Provided that the Minister may appoint a new member from the list contemplated in subsection (7)*(d)* where candidates on that list are still available for appointment.

(14) The Minister may, after due process by the National Assembly, remove a member of the Council appointed in terms of subsection (8) from office on account of—

(a) absence from three consecutive meetings without good cause;

(b) misconduct, incapacity or incompetence;

(c) becoming disqualified as contemplated in section 5; or

(d) any other lawful reason.

(15) The Minister may suspend a member where there are reasonable grounds to do so, until the process contemplated in subsection (14) is finalised.

(16) The Minister may request the Cabinet member responsible for an institution which is represented on the Council, as contemplated in subsection (2)*(b)*, to nominate another representative for appointment to substitute the institution's representative in the Council.

(17) Members of the Council who are appointed in terms of subsection (8) may be paid such remuneration and allowances as the Minister may, with the written concurrence of the Minister of Finance, determine.

(18) The deputy chairperson referred to in subsection (11) must, when the chairperson is absent or unable to perform his or her duties, act in his or her stead and when so acting, exercise or perform any function of the chairperson.

Disqualification from appointment as member of Critical Infrastructure Council

5. A person is disqualified from being appointed or continuing to serve as a member of the Critical Infrastructure Council contemplated in section 4(2)*(b)* and *(c)*, if he or she—

(a) is not a South African citizen;

(b) does not have a valid top secret security clearance certificate issued to him or her by the State Security Agency;

(c) is an unrehabilitated insolvent;

(d) has, in the preceding 20 years, been sentenced in the Republic or elsewhere, to imprisonment without the option of a fine;

(e) has a direct or indirect financial or personal interest in any critical infrastructure; or

(f) has been removed from a position or an office of trust; or

(g) is by virtue of any other law, disqualified from being appointed.

Funding and remuneration

6. The expenses incurred in connection with the exercise of the powers, the carrying out of the duties and the performance of the functions of the Critical Infrastructure Council, including the remuneration and expenses contemplated in section 4(17), must be defrayed from the budget allocation of the Civilian Secretariat for the Police Service established in terms of section 4(1) of the Civilian Secretariat for Police Service Act, 2011 (Act No. 2 of 2011) as voted in terms of the annual Division of Revenue Act.

Functions of Critical Infrastructure Council

7. (1) The functions of the Critical Infrastructure Council are to—

(a) subject to subsection (2), consider any application for declaration of infrastructure as critical infrastructure referred to in Chapter 3 and make recommendations on such application to the Minister;

(b) subject to subsection (3), approve guidelines regarding—
(i) the assessment of an application contemplated in sections 18 and 19;
(ii) the implementation of the prescribed system for categorisation of critical infrastructure in a low-risk, medium-risk or high-risk category referred to in section 20(7);
(iii) policies, protocols and standards regarding any matter necessary to achieve the purpose of this Act; and
(iv) the promotion of public-private sector cooperation in the protection of critical infrastructure; and

(c) perform any other functions which may be assigned to the Council by the Minister.

(2) When making a recommendation to the Minister on an application referred to in subsection (1)*(a)*, the Council must consider the following before making such a recommendation—

(a) the requirements referred to in section 16(2)*(a)*;
(b) any factor contemplated in section 17;
(c) any report or submission that must accompany such application;
(d) an appropriate risk categorisation of the infrastructure in question in accordance with the prescribed system of categorisation referred to in section 20(7); and
(e) any conditions for such declaration as contemplated in section 21(1)*(c)*.

(3) When approving guidelines referred to in section (1)*(b)*, the Council must consider the following:

(a) any submission by the National Commissioner as contemplated in section 9(2);
(b) any relevant submission by any other person having an interest in the protection of critical infrastructure;
(c) any budgetary implications related to critical infrastructure protection;
(d) any other matter that may promote the purpose of this Act or affect the implementation thereof.

(4) The guidelines referred to in subsection (1)*(b)* must include guidelines regarding—

(a) the identification and management of risks relating to critical infrastructure;
(b) the establishment and maintenance of a legitimate, effective and transparent process for identifying and declaring infrastructure as critical infrastructure; and
(c) the procedures to coordinate the functions and activities of Government departments and the private sector insofar as those functions and activities are performed to achieve the purpose of this Act.

(5) In addition to any function contemplated in this section, the Council may—

(a) advise the Minister on evaluation, monitoring and reviewing of the implementation of policy, protocols, standards and legislation related to the protection of critical infrastructure; and
(b) make recommendations to the Minister on any function of the Minister contemplated in section 22 or section 23.

(6) The Council must submit a report to the Minister within three months after the end of each financial year regarding—

(a) the activities of the Council during the preceding financial year;
(b) particulars pertaining to the number of declarations as critical infrastructure, including the names of the critical infrastructure;
(c) particulars pertaining to any limitations or revocation as critical infrastructure;
(d) the level and extent of public-private sector cooperation; and
(e) any other matter that may impact on the protection of critical infrastructure or the functioning of the Council.

Meetings of Critical Infrastructure Council

8. (1) The Critical Infrastructure Council must meet at least quarterly.

(2) The Secretary for the Police Service must ensure that secretarial services are provided to the Critical Infrastructure Council.

(3) The chairperson may at any time convene a special meeting of the Council and must also convene such a meeting at the written request of the Minister.

(4) If at least three members of the Council request a special meeting in writing, the chairperson must convene such a meeting within seven days after receiving the request.

(5) Seven members of the Council, which must include the chairperson or deputy chairperson, will constitute a quorum at any meeting of the Council.

(6) Decisions of the Council must be taken by majority of votes, and in the case of an equality of votes the chairperson has a casting vote in addition to his or her deliberate vote.

Part B

Administration of Act

Functions of National Commissioner

9. (1) The National Commissioner must—

(a) establish and maintain the administrative systems and procedures necessary for the implementation and enforcement of this Act;

(b) support the Critical Infrastructure Council and the Minister in the administration of this Act; and

(c) effect cooperation between the South African Police Service, other organs of state and the private sector insofar as it relates to the protection of critical infrastructure.

(2) The functions of the National Commissioner are to develop uniform standards, guidelines and protocols for approval by the Council regarding—

(a) the manner in which—

(i) infrastructure must be identified, categorised and declared critical infrastructure;

(ii) any physical security assessment of critical infrastructure and potential critical infrastructure is conducted and coordinated between Government departments;

(iii) information which may be relevant to critical infrastructure protection is shared between the relevant stakeholders;

(iv) any prescribed committee or forum must function and report; and

(b) structures and mechanisms to facilitate coordination in and management of the protection of critical infrastructure.

(3) The National Commissioner must—

(a) consider applications from a person in control of an infrastructure for declaring that infrastructure as critical infrastructure;

(b) conduct or facilitate any physical security assessment of critical infrastructure or potential critical infrastructure;

(c) make recommendations to the Council on the declaration and risk categorisation of such critical infrastructure or potential critical infrastructure;

(d) evaluate, monitor and review the application and operational effectiveness of policy, guidelines or legislation related to the protection of critical infrastructure, and advise the Council accordingly;

(e) evaluate and review physical security assessments, resilience reports and any designation as critical infrastructure and advise the Council accordingly;

(f) consider any draft of a prescribed security policy or plan submitted to his or her office;

(g) issue directives regarding the procedures to be followed at the meetings of any prescribed committee or forum; and

(h) compile and submit quarterly reports to the Council, which must at least include—

(i) particulars of the related activities of the South African Police Service during the preceding quarter;

(ii) particulars of the number of applications for declaration of infrastructure as critical infrastructure;

(iii) particulars of the level and extent of Government department participation in the functioning of the committee or forum; and

(iv) the level and extent of public-private sector cooperation in the functioning of the committee or forum.

(4) The National Commissioner may, in the prescribed manner, apply for the declaration of government infrastructure as critical infrastructure.

Designation of inspectors

10. (1) The National Commissioner may designate police officials who are in possession of an appropriate security clearance certificate, experienced in infrastructure protection, on at least the rank level of a warrant officer, as inspectors.

(2) The National Commissioner must issue each inspector designated in terms of subsection (1) with a certificate in the prescribed form, stating that the police official has been designated as an inspector in terms of this Act.

Functions of inspectors

11. (1) An inspector may, at any reasonable time, conduct an inspection at a critical infrastructure to—

(a) verify whether the person in control of that critical infrastructure took the steps to secure the critical infrastructure contemplated in section 24(1);

(b) verify any information relating to the declaration as critical infrastructure as well as the physical security report contemplated in section 18;

(c) review the physical security assessment and evaluate the status of the physical security of the critical infrastructure;

(d) verify compliance with this Act; and

(e) compile a report on the matters referred to in paragraphs *(a)* to *(d)* for the National Commissioner and the person in control of the critical infrastructure.

(2) An inspector must—

(a) preserve, or aid in preserving, confidentiality with regard to all matters concerning the operational activities of the critical infrastructure that may come to his or her knowledge in the performance of his or her duties and may not communicate any such matter to any person except the National Commissioner, or unless a court of law orders such communication, or insofar as such communication is necessary to properly carry out the inspection;

(b) carry out his or her duties and exercise his or her powers—

(i) subject to any prescribed procedure;

(ii) in accordance with any directives issued by the Minister;

(iii) in a manner that does not hamper or endanger the operational activities of the critical infrastructure where an inspection is being conducted; and

(iv) with strict regard to decency and order.

(3) Where the person in control of a critical infrastructure fails or refuses to allow an inspector access to the critical infrastructure concerned, the inspector may issue the prescribed compliance notice in the prescribed manner to the person in control of the critical infrastructure, requiring of that person to provide the inspector with access to the critical infrastructure within seven days, for the purpose of conducting the inspection.

(4) If an inspector has reasonable grounds to believe that any method or practice of safeguarding or securing the critical infrastructure in question or any failure or refusal to comply with this Act, may negatively affect the physical security measures of that critical infrastructure, the inspector may, by written notice in the prescribed form and manner, order the person in control of that critical infrastructure to take, within a period specified in the notice, such steps in respect of the security of the critical infrastructure as may be specified in the notice.

(5) Despite subsection (4), the Minister may take or cause steps to be taken in respect of the security of any critical infrastructure, when credible information on oath is brought to his or her attention to the effect that—

(a) the person in control of critical infrastructure fails or refuses to—

(i) comply with the provisions of this Act; or

(ii) take the steps contemplated in the notice referred to in subsection (4);

(b) the failure or refusal contemplated in paragraph *(a)* creates a substantial risk that the critical infrastructure in question cannot be secured in the event of a threat; and

(c) in the event of a threat, a failure to secure the critical infrastructure in question is likely to cause an imminent disruption of—

(i) the functioning or stability of the economy of the Republic;

(ii) the maintenance of law and order;

(iii) the provision of basic public services; or

(iv) national security.

(6) Despite the power of the Minister to take or cause steps to be taken in respect of the security of any critical infrastructure as contemplated in subsection (5), the Minister, when exigent circumstances dictate that the provisions of subsection (3) or (4) be dispensed with, may apply to a court having jurisdiction for—

(a) an order compelling the person in control of critical infrastructure—

(i) to comply with any provision of this Act or to cease contravening a provision of this Act;

(ii) to comply with any notice issued under subsection (3) or take any other reasonable steps necessary to secure the critical infrastructure in question; or

(iii) to cease any method or practice of safeguarding or securing the critical infrastructure in question that may cause a serious breach of the physical security measures of that critical infrastructure; or

(b) any other order the court considers appropriate.

(7) A notice referred to in subsections (3) and (4) must be given to the person in control of the infrastructure or a person designated by the person in control of the critical infrastructure or, in their absence, the most senior employee available at the critical infrastructure to whom the notice can be issued.

(8) The Minister may, by notice in the *Gazette*, in consultation with the head of a public entity or statutory body, either generally or subject to such conditions as may be specified in the notice, extend the powers provided for in this section to any competent person employed by a public entity contemplated in section 1 of the Public Finance Management Act, 1999 (Act No. 1 of 1999), or any other statutory body if that person is a peace officer contemplated in section 1(1) of the Criminal Procedure Act, 1977 (Act No. 51 of 1977).

(9) The notice referred to in subsection (8) must set out—

(a) the extent to, and the conditions under, which such powers are extended to such person; and

(b) the extent to which the directives contemplated in subsection (2)(*b*)(ii) are applicable to such person in the exercise of such powers.

(10) An inspector, prior to exercising any power in terms of this Chapter, must identify himself or herself to the person in control or the security manager of the critical infrastructure in question and must produce the certificate issued by the National Commissioner referred to in section 10(2).

Part C

Committees, exemption and delegations

Ad hoc and standing committees

12. (1) The National Commissioner may, when he or she deems it necessary or expedient to obtain advice or assistance in order to perform any function contemplated in section 9(2) and (3), establish any *ad hoc* or standing committee to assist him or her.

(2) A committee established under subsection (1) may establish *ad hoc* working groups to assist it in the performance of its functions.

(3) Any committee or working group established under subsections (1) and (2) may include persons who are not police officials.

(4) The National Commissioner must designate a police official who is a member of a committee or working group, as chairperson thereof.

(5) A committee is accountable to the National Commissioner.

(6) The advice contemplated in subsection (1) does not bind the National Commissioner or absolve him or her from his or her responsibility under this Act.

(7) A member of a committee is disqualified from being appointed or continuing to serve as a member of the committee, if he or she—

(a) has, in the preceding 20 years, been sentenced in the Republic or elsewhere, to imprisonment without the option of a fine;

(b) does not have a valid security clearance certificate issued to him or her by the State Security Agency;

(c) is an unrehabilitated insolvent;

(d) is not a South African citizen; or

(e) is by virtue of any other law disqualified from being appointed.

(8) The cyber response committee must function as a standing committee to advise the Council on any matter relating to information infrastructure.

Exemption of certain persons

13. (1) The restrictions on entry contemplated in section 25(2) do not apply in respect of a member of the security services established in terms of section 199 of the Constitution, who is required in the performance of his or her functions and the carrying out of his or her duties, to enter any critical infrastructure.

(2) Section 25(2) must not be interpreted so as to restrict powers of entry assigned by law on any functionary in the employ of an organ of state.

(3) Any member or functionary referred to in subsections (1) or (2) must produce proof of his or her appointment and identity to the satisfaction of the person in control of the critical infrastructure or an appointed security manager.

Delegation of powers

14. (1) The Minister may, by notice in the *Gazette*, delegate any of his or her powers under this Act to the National Commissioner, except—

(a) the power conferred on the Minister by sections 22, 23 and 27; and

(b) the duty imposed on the Minister by sections 4, 11, 16, 19, 20 and 21.

(2) The Minister must regularly review and, if necessary, amend or withdraw a delegation under subsection (1).

(3) A delegation to the National Commissioner under subsection (1)—

(a) is subject to such limitation and conditions as the Minister may impose;

(b) may authorise the National Commissioner to sub-delegate, in writing, the power or duty to another police official of a rank not less than that of level 13;

(c) does not prevent the exercise of that power or the performance of that duty by the Minister; and

(d) does not divest the Minister of the responsibility concerning the exercise of the delegated power.

(4) The Minister may confirm, vary or revoke any decision taken by a police official as a result of a delegation or sub-delegation under this section, subject to any rights that may have become vested as a consequence of that decision.

(5) The National Commissioner may, in writing, delegate any function conferred upon him or her by this Act to any police official of a rank not less than that of level 13.

(6) A delegation in terms of subsection (5)—

(a) is subject to such limitation and conditions as the National Commissioner may impose;

(b) does not prevent the exercise of that power or the performance of that duty by the National Commissioner; and

(c) does not divest the National Commissioner of the responsibility concerning the exercise of the delegated power.

(7) The National Commissioner may confirm, vary or revoke any decision taken by a police official as a result of a delegation under this section, subject to any rights that may have become vested as a consequence of that decision.

Reporting by Minister

15. The Minister must, on a bi-annual basis, table a report in Parliament on the activities of the Critical Infrastructure Council, substantially corresponding with the format of the report in section 7(6).

CHAPTER 3

DECLARATION AS CRITICAL INFRASTRUCTURE AND DETERMINATION OF CRITICAL INFRASTRUCTURE COMPLEX

Power of Minister to declare critical infrastructure and determine critical infrastructure complex

16. (1) Subject to the provisions of this Chapter, the Minister may declare any infrastructure as critical infrastructure on application by—

(a) a person in control of that infrastructure; or

(b) in the case of government infrastructure, the National Commissioner.

(2) When considering an application contemplated in subsection (1), the Minister must have regard to—

(a) whether the loss, damage, unlawful disruption or immobilisation of such infrastructure may severely prejudice—

(i) the functioning or stability of the economy of the Republic;

(ii) the public interest with regard to safety and the maintenance of law and order;

(iii) the provision of basic public services; or

(iv) national security;

(b) factors set out in section 17;

(c) any prescribed guidelines for the identification and declaration of infrastructure as critical infrastructure; and

(d) recommendations of the Critical Infrastructure Council.

(3) The Minister may, on the recommendation of the Council, determine that a critical infrastructure is part of a critical infrastructure complex where it is necessary to achieve the objects of this Act.

(4) The Minister must, in consultation with the Cabinet member responsible for State security, determine the procedure that the National Commissioner and the State Security Agency must follow when dealing with an application contemplated in section 18(4).

(5) Where an application contemplated in section 18(4) is referred to the Cabinet member responsible for State security in terms of any legislation on cybersecurity, the Cabinet member responsible for State security must, within 60 days or such further period as agreed upon between the Ministers, decide whether the infrastructure in question, or any part thereof must be dealt with in terms of any legislation on cybersecurity or not, and inform the Minister in writing of the decision.

(6) Where the Cabinet member responsible for State security decides that an application must not be dealt with in terms of legislation on cybersecurity, the Cabinet member responsible for State security must return the application to the Minister, whereafter the application must be dealt with in terms of this Act.

Factors to be taken into account in declaration of critical infrastructure

17. The following factors must be taken into account when an application for declaration as critical infrastructure is considered:

(a) The sector in which the primary functions of such an infrastructure take place;

(b) the strategic importance, including the potential impact of destruction, disruption, failure or degradation of such an infrastructure or the interruption of a service which might affect the Republic's ability to function, deliver basic public services or maintain law and order;

(c) the risk category of such an infrastructure or parts thereof;

(d) the resources available to the person in control of the infrastructure to—

(i) safeguard such an infrastructure against destruction, disruption, failure or degradation;

(ii) repair or replace such infrastructure, including its equipment, materials or service; or

(iii) ensure that the infrastructure recovers from any destruction, disruption, failure or degradation;

(e) the effects or the risk of a destruction, disruption, failure or degradation of such an infrastructure on—

(i) the environment;

(ii) the health or safety of the public or any segment of the public; or

(iii) any other infrastructure that may negatively affect the functions and functioning of the infrastructure in question;

(f) the size and location of any population at risk;

(g) historic incidents of destruction, failure or degradation of such infrastructure;

(h) the level of risk or threats to which such an infrastructure is exposed;

(i) special characteristics or attributes of such an infrastructure which enhance the resilience of that infrastructure;

(j) the extent to which the declaration as critical infrastructure will affect the interests of the public; and

(k) any other factor which may, from time to time, be determined by the Minister by notice in the *Gazette*, after consultation with the Critical Infrastructure Council.

Application for declaration as critical infrastructure by person in control

18. (1) A person in control of an infrastructure may, in the prescribed manner and format, lodge with the National Commissioner an application contemplated in section 16(1) to have such infrastructure declared as critical infrastructure.

(2) The National Commissioner must require of the person in control of that infrastructure to—

(a) submit a report by the head of a government department or head of an organ of state who has functional control over the sector in which the activities of the infrastructure falls regarding the application; and

(b) disclose—

(i) particulars of any person other than the applicant who has a right or interest in the infrastructure in question;

(ii) particulars of any agreement with a person contemplated in paragraph *(a)* regarding the application for declaration as critical infrastructure;

(iii) particulars of any person other than the applicant who will be responsible for the costs of securing the infrastructure in question;

(iv) particulars of any agreement with a person contemplated in paragraph (iii) regarding the costs of securing the infrastructure in question; or

(v) any other information necessary for the proper consideration of the application.

(3) Subject to subsections (4) and (5), the National Commissioner must—

(a) upon receipt of an application, publish a notice of the application in the Gazette—

(i) stating the name of the applicant and the address of the premises in respect of which the application is made; and

(ii) inviting interested persons to submit written comments in relation to the application;

(b) within 30 days of receipt of an application and where applicable, the information contemplated in subsection (2), conduct a physical security assessment of the infrastructure in order to—

(i) verify the information in the application;

(ii) assess the risk category in which such infrastructure or parts thereof may be categorised;

(iii) confirm whether the physical security measures proposed by the person in control of the infrastructure in response to the outcome of the physical security assessment, comply with the prescribed measures and standards for the protection of the infrastructure; and

(c) within 60 days after the physical security assessment has been conducted, submit—

(i) a written inspection report together with the application made in terms of subsection (1);

(ii) any comments contemplated in paragraph *(a)*(ii); and

(iii) any written submissions in terms of subsection (5) or, where applicable, subsection (8), to the Critical Infrastructure Council for consideration.

(4) Where it appears from the application that the infrastructure contemplated in subsection (1) partly consists of, incorporates or houses, any information infrastructure as contemplated in any legislation on cybersecurity, the National Commissioner must follow the procedure contemplated in section 16(4).

(5) In the event that the applicant shows good cause why the procedure in subsection (3)*(a)* should not be followed, the National Commissioner must refer the request to the Council who may dispense with the publication as referred to in subsection 3*(a)* after considering the factors in subsection (5).

(6) For purposes of subsection (5), the applicant must show that a departure from the procedure in subsection (3)*(a)* is reasonable and justifiable in the circumstances and that a departure from the process referred to in subsection (3)*(a)* is justified, taking into account all relevant factors, including—

(a) the objects of declaration as critical infrastructure;

(b) the nature, purpose and likely effect of the declaration as critical infrastructure;
(c) the nature and the extent of the departure from subsection (3)*(a)*;
(d) the relation between the departure and its purpose;
(e) the importance of the purpose of the departure; and
(f) the need to promote an efficient administration and good governance.

(7) The National Commissioner must provide the person in control of that infrastructure with an opportunity to make written submissions regarding any physical security assessment which is conducted as contemplated in subsection (3)*(b)*.

(8) In the event that the Council decides that the procedure contemplated in subsection (3)*(a)*—

(a) must be followed, the Council may direct the National Commissioner to publish the notice contemplated in subsection (3)*(a)* with directions on the information that must be contained in the notice, whereafter the National Commissioner will deal with the application; or
(b) may be departed from, the Council may direct the National Commissioner to depart from the provisions of subsection (3)*(a)* and proceed to deal with the application.

(9) The National Commissioner may request the Head of a Government department which is a security service established under section 199 of the Constitution, to designate a suitably experienced member of that security service to assist with the physical security assessment contemplated in subsection (3)*(b)*, when required.

(10) Where the National Commissioner is unable to comply with the timeframe contemplated in subsection (3)*(c)*, the National Commissioner must, in writing, apply to the Council in the prescribed form and manner for an extension not exceeding 30 days or such other period as the Council may determine.

(11) The Council must at its meeting consider the application, the physical security assessment report and any other documentation referred to in this section.

(12) Subject to section 20(2), the Council must within seven days of its last meeting submit the application and its recommendations to the Minister for a decision within 30 days of receipt thereof.

(13) Where the Council is unable to comply with the timeframes as contemplated in subsection (12), the Council must in writing request the Minister for an extension not exceeding 30 days or such other period as the Minister may determine.

(14) If the infrastructure relevant to the application consists of multiple structures, services or facilities, the person in control of those infrastructures must apply for declaration in respect of all such infrastructure as critical infrastructure.''

(15) Where an extension of time is granted as contemplated in subsection (10) or (13), the Council must inform the person in control of that infrastructure in writing.

Application for declaration as critical infrastructure by National Commissioner

19. (1) Where the National Commissioner identifies for possible declaration—

(a) infrastructure under the control of or occupied by a provincial government department, he or she must advise the relevant head of the department in the province to lodge an application in terms of section 18; or
(b) government infrastructure, he or she must lodge an application in accordance with subsection (2)

(2) Where the National Commissioner makes an application for the declaration of government infrastructure as critical infrastructure, the application must, subject to section 18(4) and subsection (4), be made in the prescribed form and manner and submitted to the Critical Infrastructure Council for consideration.

(3) After consideration of the application in terms of subsection (2), the Council must submit the application to the Minister for his or her decision.

(4) Where the National Commissioner intends to make an application referred to in subsection (1)*(b)*, the National Commissioner must—

(a) notify the relevant head of a Government department who is the person in control of the infrastructure, in the prescribed form and manner, of the intention of the National Commissioner;
(b) afford the person referred to in paragraph *(a)* an opportunity to submit written representations within 60 days on any aspect relating to the intended application of the National Commissioner;
(c) consider the representations referred to in paragraph *(b)*; and

(d) within seven days of taking a decision on whether or not to proceed with the application, notify the person referred to in paragraph *(a)* in writing of such decision and his or her reasons.

(5) In the event that the National Commissioner decides to proceed with the application, he or she must ensure that the written representations referred to in subsection (4)*(b)* as well as his or written reasons referred to in subsection 4*(d)* forms part of the application that is submitted to the Council.

Declaration as critical infrastructure

20. (1) The Critical Infrastructure Council must, after considering the report from the National Commissioner and all other facts pertaining to the matter, make recommendations to the Minister regarding—

(a) whether or not to declare an infrastructure as critical infrastructure; and

(b) any risk categorisation, with reference to the prescribed guidelines, which must be assigned to the infrastructure.

(2) Before the Council makes a recommendation to the Minister to declare or not to declare the infrastructure as critical infrastructure, the Council must—

(a) notify the person in control of that critical infrastructure of such recommendation and the reasons for such recommendation; and

(b) afford the person in control of that infrastructure a period of no less than 60 days to make representations.

(3) The Council must consider any representations received in terms of subsection (2) before making a recommendation to the Minister on whether or not to declare an infrastructure as a critical infrastructure.

(4) The Minister may—

(a) declare an infrastructure as critical infrastructure after considering—

(i) the application;

(ii) the factors referred to in sections 16(2) and 17;

(iii) the recommendation of the Critical Infrastructure Council; and

(iv) any other information which the Minister deems appropriate;

(b) subject to subsection (7), categorise a critical infrastructure or certain parts of such critical infrastructure that is declared in terms of paragraph *(a)* in either a low-risk, medium-risk or high-risk category, as may be prescribed; and

(c) impose such conditions as may be prescribed regarding any steps and measures the person in control of the critical infrastructure must implement to safeguard the critical infrastructure in question.

(5) The Minister must notify the Council, the National Commissioner and the person in control of that critical infrastructure of—

(a) the declaration of the infrastructure as a critical infrastructure;

(b) the risk categorisation of such declaration;

(c) the conditions contemplated in subsection (4)*(c)*;

(d) any implications of the Income Tax Act, 1962 (Act No. 58 of 1962); and

(e) the period within which the person in control of that critical infrastructure must take the steps contemplated in section 24(1).

(6) When infrastructure has been declared as critical infrastructure, the Minister may, in consultation with the person in control of the infrastructure, taking into account the probability of compromising the security of the critical infrastructure in question, determine that the publication of information regarding the security measures which must be implemented at such critical infrastructure be restricted.

(7) When considering the categorisation of infrastructure, the Minister must have regard to—

(a) the prescribed system of categorising infrastructure in a low-risk, medium-risk or high-risk category;

(b) the probability of failure, disruption or destruction of the infrastructure in question or threat thereof; and

(c) the impact and consequence of failure, disruption or destruction of infrastructure or threat thereof.

Certificate of declaration as critical infrastructure

21. (1) Where an infrastructure is declared a critical infrastructure, the Minister must issue a certificate of declaration, in the prescribed form and manner, to the person in control of that critical infrastructure, setting out—

(a) the risk categorisation as determined by the Minister;

(b) the premises or complex where the critical infrastructure is located;

(c) the conditions which the Minister may deem necessary to impose for purposes of securing the critical infrastructure; and

(d) whether information regarding security measures will be restricted.

(2) The Minister must issue a certificate for each of the premises on which any such critical infrastructure, forming part of a complex, is located.

(3) The certificate must be issued in the designation of the person in control of that critical infrastructure.

(4) Declaration as critical infrastructure does not exempt a person in control of critical infrastructure from having to comply with the provisions of any other law applicable to the critical infrastructure in question.

(5) The National Commissioner must enter the particulars of any declaration as critical infrastructure or the termination of such declaration, into the prescribed register, which must be accessible to the public in the prescribed manner or form.

(6) The Minister must, by notice in the *Gazette*, publish such particulars as may be prescribed regarding infrastructure which has been declared as critical infrastructure and when such declaration is terminated.

Amendment or variation of information or conditions by Minister

22. (1) If there is a change in the circumstances of any critical infrastructure, the Minister may, on the recommendation of the Critical Infrastructure Council or upon a request in writing by the person in control of a critical infrastructure or the National Commissioner—

(a) amend the risk categorisation determined in terms of section 20(4)*(b)*; or

(b) vary any or all of the information or conditions on a certificate of declaration as critical infrastructure referred to in section 21.

(2) Before acting on the advice or the request contemplated in subsection (1) to amend or vary the risk categorisation, or any of the information or conditions, the Minister must give the person in control of the critical infrastructure—

(a) written notice of his or her intention to amend or vary the risk categorisation, information or conditions on the certificate of declaration as critical infrastructure; and

(b) no less than 30 days to submit written representations to the Minister as to why the Minister must not amend or vary the risk categorisation, information or conditions on the certificate of declaration.

(3) The Minister must consider the written representations referred to in subsection (2)*(b)* and notify the person in control of the critical infrastructure in writing—

(a) of any decision taken under this section;

(b) the reasons for the decision; and

(c) the date on which the decision takes effect.

Termination and revocation of declaration

23. (1) A declaration as critical infrastructure in terms of this Chapter terminates—

(a) where the person in control of a critical infrastructure ceases the activities which formed the basis upon which the Minister declared the infrastructure as a critical infrastructure; or

(b) upon revocation in terms of subsection (4).

(2) The person in control of a critical infrastructure must notify the National Commissioner in writing within 30 days if—

(a) there is any change with regard to any information that was submitted in respect of the application for declaration as a critical infrastructure;

(b) there is a change in the control or ownership of the critical infrastructure; or

(c) there is any change that impacts on the ability of the critical infrastructure or the person in control of a critical infrastructure to comply with all or any of the obligations under this Act.

(3) The National Commissioner may, after having considered any notification contemplated in subsection (2), recommend to the Minister to revoke the declaration as critical infrastructure if—

(a) there is any change contemplated in subsection (2);

(b) the infrastructure in question was declared as critical infrastructure on the basis of incorrect or false information; or

(c) the person in control of the critical infrastructure fails to comply with any—

(i) condition of declaration; or

(ii) of the provisions of this Act.

(4) The Minister may, after having considered the recommendation of the National Commissioner, revoke the declaration as critical infrastructure based on any factor referred to in subsection (3).

(5) Before revoking the declaration as critical infrastructure in terms of subsection (4), the Minister must—

(a) give the person in control of that critical infrastructure written notice of the intention to revoke;

(b) give the person in control of that critical infrastructure an opportunity to submit written representations within a period of 30 days as to why the declaration as critical infrastructure must not be revoked; and

(c) duly consider any such representations and the facts pertaining to the matter.

(6) *(a)* The Minister must notify the person in control of that critical infrastructure, in writing, of any decision taken under this section and, if the declaration is revoked, state the reasons for the revocation and the date on which the revocation takes effect, in such notice.

(b) A notification contemplated in paragraph *(a)* must be served on the person in control of the critical infrastructure by a police official, in the prescribed manner.

(7) In the event where a declaration as a critical infrastructure is revoked as contemplated in subsection (4), the person in control of that critical infrastructure must—

(a) hand all certificates relating to such declaration to the police official serving the notice contemplated in subsection (6) immediately upon such service; or

(b) return all certificates to the Minister in the event of a termination contemplated in subsection (1)*(a)*, within seven days after termination.

(8) The police official referred to in subsection (6)*(b)* must deliver the certificates contemplated in subsection (7)*(a)* to the Minister.

CHAPTER 4

POWERS AND DUTIES OF PERSONS IN CONTROL OF CRITICAL INFRASTRUCTURE

Powers and duties of person in control of critical infrastructure

24. (1) On receipt of a notice referred to in section 20(5)*(e)*, the person in control of a critical infrastructure must, subject to subsection (4), take such steps as may be prescribed to secure such critical infrastructure at that person's own expense.

(2) The person in control of critical infrastructure that is under the control of a Government department or any other organ of state, must take steps to ensure that such critical infrastructure is protected by the employees of that government department or organ of state.

(3) Where the Government department or organ of state referred to in subsection (2) is unable to protect a critical infrastructure as contemplated in subsection (2), the person in control of that critical infrastructure must take steps to ensure that a security service provider is appointed to protect the critical infrastructure: Provided that such security service provider may only be appointed after the successful completion of security vetting by the State Security Agency.

(4) *(a)* Subject to paragraphs *(b)* and *(c)*, the Minister may, if the person in control of critical infrastructure shows good cause in the application contemplated in section 18(1) or 19(1), determine that the Head of a Government department is responsible for all or some of the expenses necessary to implement the steps contemplated in subsection (1).

(b) For purposes of determining the extent to which the Head of a Government department contemplated in paragraph *(a)* is responsible for the expenses, the Minister must—

(i) in the case of a national department, consult the Minister of Finance and the Minister responsible for the affected department;

(ii) in the case of a provincial department, consult the relevant Member of the Executive Council responsible for finance and the relevant Member of the Executive Council responsible for the affected department;

(iii) in the case of a municipality, consult the relevant Municipal Council; and

(iv) where applicable, take into account any policy of the Cabinet, the relevant Executive Council or Municipal Council regarding the standards of any security measures and the reasonable costs that may be incurred by the State.

(c) The Minister must, in writing, inform the Head of the Government department and the person in control of that critical infrastructure of the decision, setting out the extent to which—

(i) the Head of the Government department contemplated in paragraph *(b)*; and

(ii) the person in control of the critical infrastructure,

is responsible for expenses necessary to implement the steps contemplated in subsection (1).

(5) In the event that a person in control of a critical infrastructure fails to take the steps contemplated in subsection (1), the Minister may, by written notice in the prescribed form and manner, order him or her to take, within a period specified in the notice and at his or her own expense, such steps in respect of the security of the critical infrastructure as may be specified in the notice.

(6) If the person in control of a critical infrastructure refuses or fails to take the steps specified in the notice within the period specified therein, the Minister must take or cause steps to be taken in respect of the security of that critical infrastructure and the Minister must recover the reasonable cost thereof from the person in control of that critical infrastructure to such extent as the Minister may determine.

(7) A person in control of a critical infrastructure must appoint a person in the employ of the critical infrastructure as security manager to—

(a) implement and monitor, on behalf of the person in control of the critical infrastructure, the prescribed security policy and plan compiled for that critical infrastructure;

(b) authorise access to critical infrastructure or oversee the authorisation of such access by security personnel working under his or her direction;

(c) liaise with any security service provider appointed by the person in control of that critical infrastructure;

(d) implement the directions contemplated in section 25(1)*(b)*;

(e) provide monthly reports to the person in control of that critical infrastructure on the functions contemplated in paragraphs *(a)*, *(b)* and *(c)*; and

(f) perform such other functions related to the securing of that critical infrastructure as may be assigned to him or her by the person in control of that critical infrastructure:

Provided that such security manager may only be appointed after successful completion of security vetting by the State Security Agency.

(8) A person in control of a critical infrastructure must as far as practically possible demarcate and place a notice, in the prescribed format and manner, on premises constituting a critical infrastructure, in order to notify persons that the premises are declared a critical infrastructure.

(9) A person to whom functions are assigned in terms of this Chapter must exercise such powers and perform such duties subject to the Constitution and with due regard to the fundamental rights of every person.

Access to critical infrastructure

25. (1) Subject to section 24, the person in control of a critical infrastructure must—

(a) take such lawful steps as he or she may consider necessary, for the securing of a critical infrastructure and the contents thereof, as well as for the protection of the persons present at the critical infrastructure;

(b) issue a notification in the prescribed form that the critical infrastructure may only be entered upon in accordance with the provisions of subsection (2) and that persons or vehicles may be searched upon entering or leaving the premises in terms of subsection (5); and

(c) ensure that a notification as contemplated in paragraph *(b)* is placed at the entrance to that critical infrastructure.

(2) *(a)* No person may, without the permission of the security manager, or the security personnel under the direction of the security manager enter into or upon any critical infrastructure in respect of which a direction has been issued in terms of subsection (1)*(b)*.

(b) For the purpose of granting permission, the security manager or the security personnel under the direction of the security manager, may require of a person to—

(i) furnish his or her name, address and any other relevant information required by the authorised person;

(ii) produce proof of his or her identity;

(iii) declare whether he or she has any dangerous object in his or her possession or under his or her control;

(iv) declare the contents of any vehicle, suitcase, bag, handbag, folder, envelope, parcel or container of any nature, which he or she has in his or her possession, custody or control, and show the content to the security manager;

(v) subject himself or herself and anything in his or her possession or under his or her control to an examination by an electronic or other apparatus, in order to determine the presence of any dangerous or prohibited object; and

(vi) subject to subsection (6) be searched by a security manager or security personnel under the direction of the security manager.

(3) Where the security manager or the security personnel under the direction of the security manager grants permission to a person in terms of subsection (2), the person may enter subject to conditions regarding—

(a) the carrying or displaying of proof that the necessary permission has been granted;

(b) restrictions relating to persons with whom he or she may come into contact in or on the critical infrastructure;

(c) restriction of access to certain parts of the critical infrastructure;

(d) the duration of his or her presence on or in the critical infrastructure;

(e) being escorted while he or she is on or in the critical infrastructure; and

(f) other requirements as the security manager or the security personnel may consider necessary.

(4) Without derogating from the provisions of the Trespass Act, 1959 (Act No. 6 of 1959), a security manager or the security personnel under the direction of the security manager may, at any time, remove any person from any critical infrastructure if—

(a) that person enters the critical infrastructure or any part of the critical infrastructure concerned, without the required permission contemplated in subsection (2);

(b) that person refuses or fails to observe a condition contemplated in subsection (3); or

(c) it is necessary for the securing of the critical infrastructure concerned or the contents thereof or for the protection of the people therein or thereon.

(5) The person in control of a critical infrastructure may determine that persons and vehicles leaving that critical infrastructure must be searched subject to subsection (6).

(6) *(a)* Any search of a person's body conducted under subsections (2)*(b)*(vi) or (5) must be carried out by a person of the same gender, or as preferred in terms of paragraph *(d)*(iii), with strict regard to the right to privacy and dignity and must be in accordance with the provisions of this section and any other prescribed directive.

(b) When conducting a search of a person's body under subsections (2)*(b)*(vi) and (5), the manner of search is restricted to a pat-down of the person's outer garments to establish whether that person is in possession or control of a prohibited or dangerous object.

(c) A search of a person's body under subsections (2)*(b)*(vi) or (5) may only be performed if—

(i) a reasonable suspicion exists that such a person did not declare a dangerous or prohibited object in his or her possession or under his or her control; and

(ii) the manner of or place where the search is performed does not infringe upon the privacy and dignity of the person to be searched.

(d) Before a security manager or security personnel under the direction of the security manager may search a person referred to in paragraph *(c)*(i), the person to be searched must be—

(i) informed of the gender of the person who will conduct the search, the manner of search and the place where the search will be performed;

(ii) provided with an opportunity to express a preference regarding the gender of the member of the security personnel who must conduct the search.

(7) If it is not practicable to examine or keep in custody on or in the critical infrastructure concerned, anything which may be examined or kept in custody under subsection (2), it may be removed to a suitable place for that purpose.

(8) The person in control of a critical infrastructure must indicate in a notice, in the prescribed form and manner, at every entry point of a critical infrastructure that the critical infrastructure may only be entered upon in accordance with the provisions of subsection (2) and the conditions determined by the security manager.

CHAPTER 5

OFFENCES AND PENALTIES

Offences and penalties

26. (1) Any person who unlawfully—

(a) furnishes, disseminates or publishes in any manner whatsoever information relating to the security measures applicable at or in respect of a critical infrastructure other than in accordance with the Protected Disclosures Act, 2000 (Act No. 26 of 2000), Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004) or any other Act of Parliament that provides for the lawful disclosure of information.

(b) takes or records, or causes to take or record, an analog or digital photographic image, video or film of the security measures at a critical infrastructure or critical infrastructure complex;

(c) takes or records, or causes to take or record, an analog or digital photographic image, video or film of the security measures at a critical infrastructure or critical infrastructure complex in contravention of the notice contemplated in section 24(8) or 25(8);

(d) hinders, obstructs or disobeys a person in control of a critical infrastructure in taking any steps required or ordered in terms of this Act in relation to the security of any critical infrastructure;

(e) hinders, obstructs or disobeys any person while performing a function or in doing anything required to be done in terms of this Act;

(f) enters or gains access to critical infrastructure without the consent of the security manager or person in control of that critical infrastructure;

(g) enters or gains access to critical infrastructure in contravention of the notice contemplated in section 24(8) or 25(8);

(h) damages, endangers or disrupts a critical infrastructure or threatens the safety or security at a critical infrastructure or part thereof;

(i) threatens to damage critical infrastructure; or

(j) colludes with or assists another person in the commission, performance or carrying out of an activity referred to in paragraphs *(a)* to *(i)*,

commits an offence and is, subject to subsection (2) and (3), liable on conviction to a fine or to imprisonment for a period not exceeding three years, or to both a fine and imprisonment.

(2) If the evidence on a charge for any offence in subsection (1)*(a)* to *(j)* proves that the activity referred to was carried out with the intention to cause damage or substantial harm to critical infrastructure, a court may, in the case of critical infrastructure categorised as—

(a) low-risk, impose a fine or imprisonment for a period not exceeding three years or both a fine and imprisonment;

(b) medium-risk, impose a fine or imprisonment for a period not exceeding five years, or both a fine and imprisonment; or

(c) high-risk, impose a fine or imprisonment for a period not exceeding seven years, or both a fine and imprisonment.

(3) If the evidence on a charge for any offence in subsection (1)*(a)* to *(j)* proves that the activity referred to in fact caused damage, substantial harm or loss of property to the critical infrastructure in question, the court may in the case of critical infrastructure categorised as—

(a) low-risk, a court may impose a fine or imprisonment for a period not exceeding 10 years, or both a fine and imprisonment;

(b) medium-risk, a court may impose a fine or imprisonment for a period not exceeding 15 years, or both a fine and imprisonment;

(c) high-risk, a court may impose a fine or imprisonment for a period not exceeding 20 years, or both a fine and imprisonment.

(4) If the evidence on a charge for any offence in subsection (1)*(a)*, *(b)* or *(c)*, proves that the security measures at the critical infrastructure in question were clearly visible to the public or in the public domain, the court may have regard to such evidence as a mitigating factor in the determination of any penalty that may be imposed in terms of subsection (3).

(5) Any person in control of a critical infrastructure who—

(a) knowingly furnishes false or incorrect information on an application for declaration as critical infrastructure;

(b) refuses or fails to comply with a notice issued in terms of section 11(3) or 11(4);

(c) refuses or fails to take the steps specified in the notice contemplated in section 24(1);

(d) refuses or fails to take the steps specified in the notice contemplated in section 24(1) within the period specified in the notice;

(e) refuses or fails to comply with section 24(8) in circumstances where compliance would not severely threaten the security at the critical infrastructure concerned; or

(f) refuses or fails to comply with section 25(8),

commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding five years, or to both a fine and imprisonment or, in the case of a corporate body as contemplated in section 332(2) of the Criminal Procedure Act, 1977, a fine not exceeding R10 million.

(6) Whenever a court convicts any person of an offence in terms of this Act where damage to or loss of property related to a critical infrastructure was caused, the prosecutor must direct the attention of the person in control of that critical infrastructure to the provisions of section 300 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), and inform the court accordingly.

CHAPTER 6

REGULATIONS

Regulations

27. (1) The Minister may, by notice in the *Gazette*, make regulations regarding—

(a) factors to be taken into account in making any recommendation in terms of section 7*(c)* or 9(3)*(c)* regarding identification, categorisation or declaration of critical infrastructure;

(b) the functioning and meeting procedure of the Critical Infrastructure Council;

(c) the establishment, functions, functioning, meeting and reporting procedure of any committee or forum contemplated in section 9(2) or (3);

(d) the manner in which—

(i) the National Commissioner must apply for the declaration of any infrastructure as critical infrastructure as contemplated in section 9(4);

(ii) the physical security assessment and evaluation contemplated in section 11(1)*(c)* must be carried out; and

(iii) a notification contemplated in section 23(5)*(b)* must be issued;

(e) the form and content of—

(i) a compliance notice contemplated in section 11(3) and the manner in which an inspector must issue such a compliance notice;

(ii) a written notice contemplated in section 11(4) and the manner in which such a notice must be issued;

(iii) an application for declaration of critical infrastructure contemplated in section 18(1) or 19(1) and the manner in which such an application must be lodged;

(iv) a notice contemplated in section 18(3)*(a)*;

(v) an application for an extension contemplated in section 18(6) or (9) and the manner in which such an application must be lodged;

(vi) a notice contemplated in section 19(3)*(a)* and the manner in which such a notice must be issued;

(vii) a certificate contemplated in section 21(1) and the manner in which such a certificate must be issued;

(viii) the register contemplated in section 21(5) and the manner in which such a register must be made accessible to the public;

(ix) the written notice, to order a person to take steps in respect of the security of critical infrastructure, as contemplated in section 24(5), and the manner in which such a notice must be issued;

(x) any notification contemplated in section 25(1)*(b)* and the manner in which such notification must be issued; and

(xi) any notice or sign that must be placed as contemplated in section 24(8) or 25(8), including the size of the notice or sign and the manner in which it must be placed;

(f) the form of any certificate contemplated in section 10(2);

(g) the procedure, contemplated in section 11(2)*(b)*, that must be followed by inspectors when carrying out duties or exercising powers;

(h) guidelines for the identification and declaration of infrastructure as critical infrastructure, as contemplated in section 16(2)*(c)*;

(i) guidelines and standards to establish a system to categorise critical infrastructure or parts thereof in a low-risk, medium-risk or high-risk category, as contemplated in section 20(4)*(b)*;

(j) any conditions regarding the steps and measures the person in control of critical infrastructure must implement to safeguard the critical infrastructure, as contemplated in section 20(4)*(c)*;

(k) the particulars that must be published where infrastructure has been declared as critical infrastructure or where such declaration has been terminated, as contemplated in section 21(6);

(l) the steps that must be taken by the person in control of critical infrastructure to secure such critical infrastructure as contemplated in section 24(1);

(m) in respect of security personnel including a security manager—

(i) the administration, provisioning and functioning of security service providers at a critical infrastructure;

(ii) such standards and training courses as may be determined and recognised by PSIRA that security personnel who render a security service at a critical infrastructure must comply with;

(iii) the requirements, qualification, security clearance level and procedure of appointment of security personnel at a critical infrastructure;

(iv) grounds which disqualify persons from appointment as security personnel or from continued employment at a critical infrastructure; and

(v) the role and responsibilities of security service providers at a critical infrastructure;

(n) in respect of the physical security measures at a critical infrastructure—

(i) the standards of physical security measures;

(ii) access and egress control at a critical infrastructure; and

(iii) emergency and evacuation procedures at a critical infrastructure; and

(o) any other ancillary or administrative matter that it is necessary or expedient to prescribe for the proper implementation or administration of this Act.

(2) Regulations made under this section may provide for a penalty of a fine or imprisonment for a period not exceeding 12 months or both a fine and such imprisonment, for any contravention thereof or for a failure to comply therewith.

(3) The Minister may make different regulations for different categories of critical infrastructure.

(4) The Minister may issue such practice directives regarding the identification, assessment and management of critical infrastructure as may be required to ensure consistent application of this Act.

(5) The Minister must table any proposed regulations in Parliament for scrutiny before promulgation.

(6) Any regulation necessary for the immediate implementation of the Act must be promulgated to coincide with the coming into operation of the Act.

(7) Before making any regulation in terms of this section, the Minister must—

(a) publish a notice in the *Gazette*—

(i) setting out the draft regulations; and

(ii) inviting written comments to be submitted on the proposed regulations within a specified period; and

(b) consider any comments received.

(8) The Minister may, after complying with subsection (7), and whether or not he or she has amended the regulations referred to in subsection (1), after complying with subsection (5), publish the regulations in final form in the *Gazette*.

CHAPTER 7

GENERAL AND TRANSITIONAL PROVISIONS

Administrative justice

28. Any administrative process conducted, or decision taken, in terms of this Act must be conducted or taken in accordance with the Promotion of Administrative Justice Act, 2000 (Act No. 3 of 2000), unless provided for in this Act.

Repeal of legislation

29. The laws mentioned in Schedule A are hereby repealed to the extent indicated in the third column thereof.

Transitional arrangements

30. (1) Any National Key Point or National Key Point Complex declared under any of the laws referred to in the Schedule (''the previous Acts''), must be deemed to be a critical infrastructure until the Minister has decided whether or not to declare such National Key Point or National Key Point Complex as a critical infrastructure in terms of section 20(4).

(2) Within a period of 60 months after the coming into operation of this Act, the National Commissioner must, after consultation with a person in control of a National Key Point, compile a report regarding the suitability of each National Key Point or National Key Point complex to be declared as a critical infrastructure or determined to be a critical infrastructure complex, as the case may be, and submit such report, together with a recommendation, to the Critical Infrastructure Council who must deal with the report in the manner contemplated in section 20.

(3) Within a period of three months after the coming into operation of this Act, the person in control of a critical infrastructure contemplated in subsection (1) must ensure that the process of vetting any security service provider, including any security officer employed at the critical infrastructure, has been initiated.

(4) Subject to subsection (5), this Act does not affect any proceedings instituted in terms of any of the previous Acts which were pending in a court immediately before the date of commencement of this Act and such proceedings must be disposed of in the court in question as if this Act had not been passed.

(5) *(a)* Proceedings contemplated in subsection (4) must be regarded as having been pending if the person concerned has pleaded to the charge in question.

(b) No proceedings may continue against any person in respect of any contravention of a provision of any of the previous Acts if the alleged act or omission constituting the offence would not have constituted an offence if this Act had been in force at the time when the act or omission took place.

(6) *(a)* Despite the repeal of the previous Acts, any person who, before such repeal, committed an act or omission which constituted an offence under that Act and which constitutes an offence under this Act may, after this Act takes effect, be prosecuted under the relevant provisions of this Act.

(b) Despite the retrospective application of this Act as contemplated in paragraph *(a)*, any penalty imposed in terms of this Act in respect of an act or omission which took place before this Act came into operation, may not exceed the maximum penalty which could have been imposed on the date when the act or omission took place.

(7) The functions, powers and duties assigned in terms of sections 3, 8 and 12 of the National Key Points Act, 1980 (Act No. 102 of 1980), and the regulations related to those sections shall remain in force for the period contemplated in subsection (2) insofar as they are not in conflict with the provisions of this Act.

(8) The Minister must, by notice in the *Gazette* and within a period of 60 days after the coming into operation of this Act, publish a list containing the names of National Key Points or National Key Point Complexes which are deemed to be critical infrastructure in terms of subsection (1).

(9) In the event that no legislation on cybersecurity is in operation when this Act comes into operation, the Minister must, in consultation with the Cabinet member responsible for State Security, determine interim guidelines on the manner in which an application contemplated in section 18(4) must be dealt with by any person performing a function in terms of this Act.

Indemnity against loss or damage

31. Neither the Minister nor any person in the service of the State is liable for anything done in good faith in terms of or in furthering the objectives of this Act.

Short title and commencement

32. This Act is called the Critical Infrastructure Protection Act, 2017, and comes into operation on a date determined by the President by proclamation in the *Gazette*.

SCHEDULE

LAWS

(Section 29, Section 30)

No. and year of law	Short title	Extent of repeal
Act No. 102 of 1980	National Key Points Act, 1980	The whole
Act No. 9 of 1984 (Bophuthatswana)	National Key Points Act, 1984	The whole
Act No. 26 of 1985 (Transkei)	National Key Points Act, 1985	The whole
Act No. 9 of 1986 (Venda)	National Key Points Act, 1986	The whole
Act No. 16 of 1986 (Ciskei)	National Key Points Act, 1986	The whole

MEMORANDUM ON THE OBJECTS OF THE CRITICAL INFRASTRUCTURE PROTECTION BILL, 2017

1. BACKGROUND AND PURPOSE

1.1 The Critical Infrastructure Protection Bill, 2017 (''the Bill''), seeks to replace the National Key Points Act, 1980 (Act No. 102 of 1980) (''the Act''), and corresponding laws of the former TBVC States. The Act was initially administered by the Minister of Defence. However, the administration of the Act was transferred to the Minister of Police.

1.2 The Act was passed in 1980 and has become outdated and is not aligned with the constitutional imperatives. The Act has not been amended since it was put into operation and has been criticised as ''old order'' legislation.

1.3 The Bill responds to international developments relating to the protection of Critical Infrastructure. The modern definition of Critical Infrastructure is wider than ''safeguarding'' which was an objective of the Act. It is increasingly accepted that the protection of critical infrastructure has become a much broader concept with a distinctly new focus in that the concept increasingly refers to preventative security measures as well.

1.4 Countries have different approaches to protection of critical infrastructure. The Chinese approach to critical infrastructure is viewed as an attempt to reconcile the internal security endeavours of the state with the necessity of economic modernisation with regard to information technology. India drew up a definitive action plan that statutorily mandated the establishment of dedicated organisations and guidelines for the area of IT security. In the United States of America, the Department of Homeland Security is coordinating all the US government's critical infrastructure protection initiatives at governmental level. Canada has incorporated information and communication technology (ICT) protection in its ''Total Defence'' overall concept and follows the All Hazards approach.

1.5 A common thread running through the approaches of these nations is the adoption of an all-hazards approach aimed at improving their ability to anticipate vulnerabilities to current and future threats.

1.6 In recent times, the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), was used to request information relating to declared national key points. The High Court in the matter of the Right2Know Campaign alluded to certain aspects of the Act that require review relating to provisions that do not prohibit the disclosure of national key points, the public interest that national key points should be disclosed, and the constitutional rights to freedom of expression, movement and access to information.

1.7 It is also necessary that the Bill is harmonised with other legislation such as the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994), the Regulation of Gatherings Act, 1993 (Act No. 205 of 1993), the Disaster Management Act, 2002 (Act No. 57 of 2002), the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), the Promotion of Administrative Justice Act, 2000 (Act No. 3 of 2000), and the Firearms Control Act, 2000 (Act No. 60 of 2000).

1.8 In order to improve the statutory framework regarding the protection of critical infrastructure, the Act is to be repealed by a constitutionally friendly Bill to provide for all security issues related to critical infrastructure.

2. CLAUSE-BY-CLAUSE ANALYSIS

2.1 Clause 1

Clause 1 of the Bill provides for definitions that include key definitions such as ‘‘critical infrastructure’’, ‘‘critical infrastructure complex’’, ‘‘cyber response committee’’, ‘‘person in control of a critical infrastructure’’, ‘‘secretary for the police service’’, ‘‘security manager’’ and ‘‘security measures’’.

2.2 Clause 2

Clause 2 provides for the purpose of the Bill. The primary purpose of the Bill is to secure critical infrastructure against threats. This clause also provides for the confidentiality of information pertaining to certain critical infrastructure subject to the Promotion of Access to Information Act, 2000.

2.3 Clause 3

Clause 3 provides that the Bill applies to the identification and declaration of infrastructure as critical infrastructures and it excludes infrastructure under the control of the Department of Defence.

2.4 Clause 4

Clause 4 provides for the establishment and composition of a Critical Infrastructure Council that must consist of 16 members appointed by the Minister of Police. The Council will consist of a mix of 11 State officials and five persons from the private sector. The clause also deals with the transparent procedure for appointment of the private sector experts by the Minister, for a period not exceeding four years on such terms and conditions as the Minister may determine. The role of the Portfolio Committee on Police is provided for.

2.5 Clause 5

This clause provides for the criteria that these members must comply with. All members must be South African citizens and must have or be issued with top security clearance certificates by the State Security Agency.

2.6 Clause 6

Clause 6 deals with funding and remuneration of the five private sector experts of the Critical Infrastructure Council as well as the interviewing panel for the shortlisting of the private sector experts.

2.7 Clause 7

Clause 7 provides for the functions of the Council. The functions include advising the Minister on the establishment and maintenance of an effective and transparent process of identifying and declaring infrastructure as critical infrastructure. The Council further provides advice to the Minister on guidelines for the identification of critical infrastructure and monitoring the implementation of policy and legislation. It also evaluates and reviews physical security assessments and any other relevant information received from the National Commissioner. The Council submits an annual report to the Minister, within three months after the end of each financial year, on its activities and specified matters.

2.8 Clause 8

Clause 8 provides for matters relating to the meetings of the Council and secretarial services to the Council.

2.9 Clause 9

Clause 9 provides for the administration of the legislation whereby the National Commissioner must establish and maintain the administrative systems and procedures necessary for its implementation and enforcement. This clause further provides functions of the National Commissioner such as the development of uniform standards, guidelines and protocols for consideration by the Council. The National Commissioner must also consider and process the applications for identification and declaration of infrastructure as critical infrastructure as well as conduct physical security assessment of critical infrastructure and make recommendations to the Council on the declaration and categorisation of critical infrastructure.

2.10 Clause 10

Clause 10 of the Bill provides that the National Commissioner may designate, as an inspector, a person from the South African Police Service experienced in infrastructure protection, on at least the rank level of a warrant officer.

2.11 Clause 11

Clause 11 provides for the functions of inspectors. These include the power to enter any critical infrastructure to conduct inspections and to verify information. The clause empowers the inspectors to issue compliance notices to provide them with access.

2.12 Clause 12

Clause 12 provides for the establishment of *ad hoc* committees or standing committees by the National Commissioner to assist him or her in the performance of his or her functions. The clause also provides for the cyber response committee, which shall function as a standing committee in advising the Council on any matter relating to national critical information infrastructure.

2.13 Clause 13

Clause 13 provides for the exemption of any member of the security services established in terms of section 199 of the Constitution, from a restriction contemplated in section 25 in the performance of his or her functions to enter any critical infrastructure.

2.14 Clause 14

Clause 14 provides for the Minister to delegate certain powers to the National Commissioner, who in turn can delegate any function conferred upon him or her to any police official of a rank not less than that of level 13.

2.15 Clause 15

Clause 15 provides that the Minister must on an annual basis table a report on the activities of the Critical Infrastructure Council in Parliament.

2.16 Clause 16

Clause 16 provides for the power of the Minister to declare critical infrastructure and critical infrastructure complex on application by a person in control of an infrastructure or by the National Commissioner. The Minister of Police must consult with the Minister responsible for State Security should an infrastructure partly consists of any information and communication infrastructure.

2.17 Clause 17

Clause 17 provides for factors to be taken into account when application for declaration as critical infrastructure is considered. These include the sector, strategic importance, risk category, resources available, environment, health, safety and interest of the public or any other infrastructure dependent on the functions and functioning of the critical infrastructure in question.

2.18 Clause 18

Clause 18 provides that a person in control of a critical infrastructure may lodge with the National Commissioner an application in the prescribed manner for the declaration of an infrastructure as critical infrastructure. It also provides for the procedures to be followed after an application for declaration has been made. The National Commissioner must conduct a physical security assessment of such infrastructure to determine the level of its importance and the sector in which such infrastructure may be categorised and to advise the Council of such physical security assessment. These processes must be conducted within specified timeframes and condonation is provided for late submission.

2.19 Clause 19

Clause 19 provides for the procedures to be followed where the National Commissioner makes an application for declaration of an infrastructure as a Critical Infrastructure.

2.20 Clause 20

Clause 20 provides for the declaration of an infrastructure as a critical infrastructure after recommendation by the Council. It provides for risk categorisation, with reference to the prescribed guidelines, which must be assigned to the infrastructure.

2.21 Clause 21

Clause 21 provides that where an infrastructure is declared a critical infrastructure, the Minister must issue a prescribed certificate of declaration indicating the category, the location of such infrastructure and the conditions imposed. The Minister must by notice in the *Gazette* publish such particulars regarding infrastructure which has been declared or when the declaration as critical infrastructure is terminated.

2.22 Clause 22

Clause 22 provides for the power of the Minister on the advice of the Critical Infrastructure Council or at the request of the National Commissioner to amend or vary information or conditions on a certificate of declaration of a critical infrastructure. The Minister must notify the person in control of a critical infrastructure of the intention to amend or vary information and must give the person in control of a critical infrastructure an opportunity to make representations.

2.23 Clause 23

Clause 23 provides for the power of the Minister to terminate and revoke a declaration as critical infrastructure and the procedures to be followed for such revocation and termination.

2.24 Clauses 24

Clause 24 provides for the powers and duties of persons in control of critical infrastructure to ensure the protection of critical infrastructure. This clause

provides for a consultation process as a safeguard for unnecessary expenditure. Expenses relating to security measures where the person in control shows good cause on why government should co-finance some of the expenses is provided for. It provides for the appointment of a security manager. The clause further provides that a person in control must demarcate and place a notice on premises constituting a critical infrastructure in order to notify persons that the premises have been declared critical infrastructure.

2.25 Clause 25

Clause 25 provides for matters relating to access to critical infrastructures. No person may enter upon any critical infrastructure without the permission of a security manager, or the security personnel under the direction of the security manager. The security manager or the security personnel under the direction of the security manager may request the person wishing to enter the premises to provide specific information and may require the person to be searched. Such search must be carried out by a person of the same gender with strict regard to decency and order. This clause further provides that persons or vehicles may be searched upon leaving the premises.

2.26 Clause 26

Clause 26 provides for offences and penalties. The offences are categorised in order of severity and discretion of the courts is provided for**.**

2.27 Clause 27

Clause 27 provides for the Minister to make regulations. The clause further provides for the establishment, functioning, meeting and reporting procedure of any committee or the Critical Infrastructure Council. Before the Minister promulgates any regulation, the proposed regulations must be published in the *Gazette* for public comment. The Minister must also table draft regulations in Parliament for notification before promulgation.

2.28 Clause 28

Clause 28 provides for administrative justice processes.

2.29 Clause 29

Clause 29 provides for the repeal of the Act and corresponding laws that were applicable in the former TBVC states.

2.30 Clause 30

Clause 30 provides for transitional arrangements. The National Key Points that have been declared national key points or national key point complexes in terms of the Act and the laws applicable to the former TBVC states are deemed to be critical infrastructure and critical infrastructure complexes until such time that the Minister decides whether or not to declare such infrastructure as critical infrastructure. The National Commissioner must compile a report regarding the suitability of each National Key Point to be declared as critical infrastructure within 60 months after the provisions of the Bill have been operationalised.

2.31 Clause 31

Clause 31 provides that the Minister or any person in the service of the State is indemnified against claim for damages for anything done in good faith in terms of furthering the objectives of this Act.

2.32 Clause 32

Clause 32 provides for the short title and commencement.

3. DEPARTMENTS/BODIES/PERSONS CONSULTED

The Bill was drafted by a Task Team consisting of officials of both the South African Police Service and the Civilian Secretariat for the Police Service. The draft Bill was consulted with interested parties that included the Presidency, the Department of Communications, the State Security Agency, the National Treasury, the Department of Defence, the Department of Justice and Constitutional Development, the Department of Health, the South African National Roads Agency, Department of Agriculture, Forestry and Fisheries, the Department of Water and Sanitation, the National Prosecuting Authority, the South African Local Government Association, the National Disaster Management Centre and the National Economic Development and Labour Council (NEDLAC).

4. IMPLICATIONS FOR PROVINCES

None.

5. CONSTITUTIONAL IMPLICATIONS

None.

6. ORGANISATIONAL AND PERSONNEL IMPLICATIONS

The Critical Infrastructure Council will need to be established.

7. FINANCIAL IMPLICATIONS FOR THE STATE

The Civilian Secretariat for the Police Service will be responsible for any remuneration of members of the Council who are not members of the public service. The relevant government departments and institutions will be responsible for the remuneration and costs of participation at meetings of their employees who serve on the Council. The South African Police Service will be responsible for the expenses relating to the activities of the National Commissioner.

8. PARLIAMENTARY PROCEDURE

8.1 The State Law Advisers and the Civilian Secretariat for Police Service are of the opinion that the Bill should be dealt with in accordance with procedure set out in section 75 of the Constitution, since it contains no provisions to which the procedure set out in sections 74 or 76 of the Constitution applies.

8.2 The Constitution distinguishes between four categories of bills as follows: Bills amending the Constitution (section 74); Ordinary Bills not affecting provinces (section 75); Ordinary Bills affecting provinces (section 76); and Money Bills (section 77). A Bill must be correctly classified or tagged, otherwise it would be constitutionally invalid.

8.3 The Bill has been considered against the provisions of the Constitution relating to the tagging of Bills, and against the functional areas listed in Schedule 4[1] to the Constitution.

8.4 The crux of tagging has been explained by the courts especially the Constitutional Court in the case of *Tongoane and Others v Minister of Agriculture and Land Affairs and Others 2010 (8) BCLR 741 (CC)*. The court in its judgment stated as follows:

---

[1] Functional areas of concurrent national and provincial legislative competence

> ‘‘**[58]** What matters for the purpose of tagging is not the substance or the true purpose and effect of the Bill, rather, what matters is whether the provisions of the Bill ‘‘in substantial measure fall within a functional area listed in schedule 4’’. This statement refers to the test to be adopted when tagging Bills. This test for classification or tagging is different from that used by this court to characterise a Bill in order to determine legislative competence. This ‘‘involves the determination of the subject matter or the substance of the legislation, its essence, or true purpose and effect, that is, what the [legislation] is about’’. (footnote omitted)
>
> **[59]** . . .
>
> **[60]** The test for tagging must be informed by its purpose. Tagging is not concerned with determining the sphere of government that has the competence to legislate on a matter. Nor is the process concerned with preventing interference in the legislative competence of another sphere of government. The process is concerned with the question of how the Bill should be considered by the provinces and in the NCOP, and how a Bill must be considered by the provincial legislatures depends on whether it affects the provinces. The more it affects the interests, concerns and capacities of the provinces, the more say the provinces should have on its content.’’

8.5 In light of what the Constitutional Court stated in the abovementioned case, the test essentially entails that ‘‘any Bill whose provisions in substantial measure’’ affect the provinces must be classified to follow the section 76 procedure.

8.6 The Bill seeks to repeal the Act and corresponding laws of the former TBVC States and to provide afresh for the protection of critical infrastructure in the Republic. In our view the provisions of the Bill do not fall within any of the functional areas listed in Schedule 4 to the Constitution. Consequently, we are of the opinion that this Bill is an ordinary Bill not affecting provinces and that it must be dealt with in accordance with the procedure set out in section 75 of the Constitution.

9. REFERRAL TO NATIONAL HOUSE OF TRADITIONAL LEADERS

The opinion is held that it is not necessary to refer this Bill to the National House of Traditional Leaders in terms of section 18(1)*(a)* of the Traditional Leadership and Governance Framework Act, 2003 (Act No. 41 of 2003), since it does not contain provisions pertaining to customary law or customs of traditional communities.