CIVILIAN SECRETARIAT FOR THE POLICE SERVICE

NOTICE 276 OF 2016

DRAFT CRITICAL INFRASTRUCTURE PROTECTION BILL, 2016

NOTICE CALLING FOR PUBLIC COMMENTS

The Civilian Secretariat for Police Service is consulting on the Draft Critical Infrastructure Protection Bill, 2016 with a view of submitting it to Cabinet for approval for its introduction in Parliament.

The Draft Critical Infrastructure Protection Bill, 2016 is hereby published for public comments. An invitation is hereby extended to members of the public wishing to comment on the Draft Critical Infrastructure Protection Bill, 2016 to provide written comments by not later than 15 June 2016. Comments received after the closing date will not be considered.

Copies of the Draft Critical Infrastructure Protection Bill, 2016 may be obtained from the WEB: www.policesecretariat.gov.za or collected in person from Van Erkom Building, Van Erkom Arcade, 7th Floor, 217 Pretorius Street, Pretoria.

The written comments inputs must be directed to:

Postal Address

The Civilian Secretariat for Police Service

Attention: Adv. Dawn Bell – Chief Director: Legislation

Private Bag X922

PRETORIA

0001

Physical Address

The Civilian Secretariat for Police Service (Attention: Mr. Milton Ntwana)

7th Floor, Van Erkom Building

Van Erkom Arcade

217Pretorius Street

PRETORIA

0001

Enquiries: (012) 393 4658 (Ms. Noluthando Xuba)

E-mail Address: dawn.bell@csp.gov.za

REPUBLIC OF SOUTH AFRICA

CRITICAL INFRASTRUCTURE PROTECTION BILL

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

(MINISTER OF POLICE)

[B - 2015]

170515ce

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; 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 repeal the National Key Points Act, 1980 (Act No. 102 of 1980); and to provide for matters connected therewith.

PREAMBLE

WHEREAS the Constitution of the Republic 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 essential public services;

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

REALISING that objective criteria need to be followed in the identification and declaration of critical infrastructure;

AND FURTHER REALISING that a process needs to be followed to enhance cooperation between Government and the private sector to secure critical infrastructure against threats;

MINDFUL that the roles, responsibilities and accountability of parties in respect of the securing of critical infrastructure needs to be defined and public confidence and awareness of critical infrastructure protection be enhanced;

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

ARRANGEMENT OF SECTIONS

CHAPTER 1

DEFINITIONS, INTERPRETATIONS, PURPOSE AND APPLICATION OF ACT

CHAPTER 2

CRITICAL INFRASTRUCTURE COUNCIL AND STRUCTURES

Part A

Critical Infrastructure Council

CHAPTER 6

REGULATIONS

CHAPTER 7

GENERAL AND TRANSITIONAL PROVISIONS

CHAPTER 1

DEFINITIONS, PURPOSE AND APPLICATION OF ACT

Definitions

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

"critical infrastructure" means any infrastructure or infrastructure complex which is declared as such in terms of section 20(4);

"critical infrastructure complex" means more than one critical infrastructure grouped together for practical or administrative reasons, which is declared as such in terms of section 20(6);

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

"Cyber Security Centre" means the Cyber Security Centre, established in terms of section 52 of the Cybercrimes and Cybersecurity Act, …….., who is responsible for the identification of critical information infrastructure;

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

"emergency services" includes any provincial or local government emergency medical services, any health services, any fire and any municipal police service or local authority traffic or by-law enforcement department;

"emergency situation" means a situation that has arisen suddenly that poses an imminent and serious threat to the environment, human life or property, including a 'disaster' as defined in section 1 of the Disaster Management Act, 2002 (Act No. 57 of 2002);

"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 103 of 3 June 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;

"Information and communication technology infrastructure" means any data, computer data storage medium, computer device, database, computer network,

electronic communications network, electronic communications infrastructure or any part thereof or any facility or equipment associated therewith;

"infrastructure" means any building, centre, establishment, facility, installation, premises or systems needed for the functioning of society, the government or enterprises of the Republic,

and includes—

(a) 'consumer installation' as defined in the Water Services Act, 1997 (Act No. 108 of 1997);

(b) 'installation' as defined in the Maritime Zones Act, 1994 (Act No. 15 of 1994);

(c) 'major hazard installation' as defined in the Occupational Health and Safety Act, 1993 (Act No. 85 of 1993);

(d) 'nuclear installation' as defined in the National Nuclear Regulator Act, 1999 (Act No. 47 of 1999) and the Nuclear Energy Act, 1993 (Act No. 131 of 1993);

(e) 'offshore installation' as defined in the Marine Traffic Act, 1981 (Act No.2 of 1981); and

(f) any other installation as may be declared as such for the purposes of this Act;

"Minister" means the Cabinet member responsible for policing as contemplated in section 206 of the Constitution of the Republic of South Africa, 1996;

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

"organ of state" means an 'organ of state' as defined in section 239 of the Constitution, 1996;

"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; or

(iii) operation of law,

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

(c) a 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 administration of a critical infrastructure and includes any employee acting in such post;

"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);

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

"risk category" means a risk category as contemplated in section 20(5);

"Secretary of Police" 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 infrastructures;

(b) information and communication technology infrastructure;

(c) personnel security at critical infrastructures;

(d) contingency plans applicable to critical infrastructures; and

(e) measures aimed at protecting critical infrastructure;

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

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

(a) information security at a critical infrastructure;

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

(c) information and communications technology infrastructure security at or to and from a critical infrastructure;

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

(e) contingency plans for a critical infrastructure; and

(f) administration of, provision of and implementation of security procedures at 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 (Act No. 56 of 2001); and

"this Act" includes the regulations.

Purpose of Act

2. The purpose of this Act is to—

(a) secure critical infrastructure against threats;

(b) ensure that information pertaining to certain critical infrastructure remains confidential;

(c) ensure that objective criteria are developed for the identification, declaration and protection of the 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 essential 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 a 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 absorb and mitigate possible security risks;

(h) ensure that every critical infrastructure complies with regulatory measures aimed at securing such 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. This Act applies to all identification and declaration of critical infrastructures and binds any person in control of critical infrastructure.

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 Critical Infrastructure Council consists of the persons contemplated in subsections (3), appointed by the Minister on such terms and conditions as the Minister may determine.

(3) Subject to subsection (5), the Minister must appoint the following persons as members of the Council, namely—

(a) the Secretary of Police;

(b) officials at the rank of at least Chief Director designated by the head of the following institutions—

(i) State Security Agency;

(ii) Department of Defence;

(iii) South African Police Service;

(iv) Department of Public Works;

(v) Department of International Relations and Cooperation;

(vi) South African Local Government Association;

(vii) Department of Cooperative Governance and Traditional Affairs; and;

(viii) Department of Home Affairs; and

(c) five members appointed in terms of section 5(1)(*a*) from the private sector who are—

(i) not disqualified in terms of section 5(2); and

(ii) appropriately qualified, knowledgeable and experienced in critical infrastructure protection.

(4) In addition to the officials contemplated in subsection (3)*(b)*, the Minister may request the Head of any other Department to designate an appropriately qualified official or person, on an *ad hoc* basis, to assist with a specific application.

(5) The Minister must appoint—

(a) officials referred to in subsection (3)*(b)* after consultation with the Cabinet member responsible for the government department in question; and

(b) members referred to in subsection (3)*(c)* after complying with section 5.

(6) The Secretary of Police is the Chairperson of the Council and the Minister must designate from the officials contemplated in (3)*(b)*, a member as deputy chairperson.

(7) Subject to subsection (9), members of the Council appointed in terms of subsection (3)*(c)* hold office for a period not exceeding five years.

(8) Upon the expiry of an appointed member's first term of office as contemplated in subsection (7), the member may be re-appointed for one further term only.

(9) A member of the Council appointed in terms subsection (3)(*c*) 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.

(10) If a member of the Council appointed in terms subsection (3)(*c*) resigns or vacates office before the expiry of his or her period of office, the Minister must, after complying with subsection 5(*b*), within a period of 90 days, appoint a new member for the unexpired portion of that period after having consulted with Cabinet.

(11) The Minister may, after due process, remove a member of the Council appointed in terms subsection (3)(*c*) from office on account of—

(a) misconduct;

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

(c) becoming disqualified as contemplated in section 5(2); or

(d) any other lawful reason.

(12) The Chairperson may request the Head of a Government Department which is represented on the Council as contemplated in subsection

(3)*(b)* to substitute its representative with another representative on good cause shown.

(13) Members of the Council who are appointed in terms of subsection 3*(c)* and persons outside the public sector who are appointed in terms of section 5(1)*(b)* may be paid for their services such remuneration and allowances as the Minister may determine with the concurrence of the Minister of Finance.

Procedure for appointment of members of Critical Infrastructure Council and disqualification

5. (1) The Minister appoints members of the Critical Infrastructure Council contemplated in section 4(3)(*c*) after—

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

(b) appointing a panel to compile a short-list of not more than 20 persons from—

(i) the applications and nominations referred to in paragraph *(a)*; and

(ii) persons serving on the Council who qualify for a further appointment in terms of section 4(8);

(c) the chairperson of the panel has submitted a short-list of candidates together with their *curriculum vitae* to the Minister; and

(d) the Minister has consulted the Cabinet.

(2) A person is disqualified from being appointed or continuing to serve as a member of the Critical Infrastructure Council contemplated in section 4(3)(c) if he or she—

(a) is not a South African citizen;

(b) does not have a valid security clearance certificate issued to him or her by an intelligence service established in terms of the Constitution, on the level as determined by the Minister;

(c) is an unrehabilitated insolvent;

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

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

(f) 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(13), must be defrayed from the budget of the Civilian Secretariat for Police established in terms the Civilian Secretariat for Police Service Act, 2011 (Act No. 2 of 2011).

Functions of Critical Infrastructure Council

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

(a) advise the Minister —

(i) on guidelines for the identification of potential critical infrastructure;

(ii) on guidelines for the assessment of an application for declaration as critical infrastructure;

(iii) on guidelines for the identification and management of risks relating to critical infrastructures;

(iv) on the establishment and maintenance of a legitimate, effective and transparent process for identifying and declaring infrastructure as critical infrastructure;

(v) in developing policies and standards regarding identifying, declaring and protecting critical infrastructure;

(vi) budgetary implications relating to critical infrastructure protection; and

(vii) any other aspect relevant to the protection of critical infrastructure.

(b) receive and consider applications for the declaration as critical infrastructure, as well as any evaluation or resilience report or physical security risk assessment and any other relevant information received from the National Commissioner;

(c) make recommendations to the Minister on—

(i) applications for declaration as critical infrastructures, including any conditions, after considering the application contemplated in paragraph *(b)*; or

(ii) any limitation or variation of conditions and revocation of any declaration as critical infrastructure;

(d) evaluate, monitor and review the implementation of policy and legislation related to the protection of critical infrastructure, and advise the Minister accordingly;

(e) evaluate and review security risk assessments, resilience reports and any recommendations from the National Commissioner or the Cyber Security Centre on the declaration of any infrastructure as critical infrastructure and advise the Minister accordingly;

(f) establish procedures to coordinate the activities of Government departments and the private sector insofar as it relates to critical infrastructure protection;

(g) compile and submit a report to the Minister at the end of each financial year regarding—

(i) the activities of the Council during the preceding financial year;

(ii) particulars pertaining to the number of declarations as critical infrastructure;

(iii) particulars pertaining to any limitations or revocation as critical infrastructure;

(iv) financial statements;

(v) the level and extent of public-private sector cooperation; and

(vi) any other matter that may impact on the functioning of the Council;

(h) promote public-private sector cooperation in the protection of critical infrastructure; and

(i) perform such duties and functions which are assigned to it by the Minister.

Meetings of Critical Infrastructure Council

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

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

(3) *(a)* 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.

(b) 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.

Part B

Administration of the 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 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 in so far 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 consideration by the Council regarding—

(a) the manner in which—

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

(ii) any national risk assessment of critical infrastructure and potential critical infrastructure is conducted and co-ordinated between government departments;

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

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

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

(3) The National Commissioner must—

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

(b) conduct or facilitate a national security risk assessment or other risk assessments of critical infrastructure or potential critical infrastructure;

(c) make recommendations to the Council on the declaring and categorisation of such critical infrastructure;

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

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

(f) consider any draft security policy and plan submitted to the National Commissioner;

(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 as critical infrastructure;

(iii) particulars of the level and extent of Government Department participation; and

(iv) the level and extent of public-private sector cooperation.

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

DESIGNATION AND FUNCTIONS OF INSPECTORS

Designation of inspectors

10. (1) The National Commissioner may designate any police official as an inspector.

(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, with the consent of the person in control of a critical infrastructure, enter upon that critical infrastructure dealt with in this Act, so as to—

(a) conduct an inspection of the critical infrastructure to evaluate or verify any information relating to the physical security assessment;

(b) verify any information relating to the security status of the critical infrastructure; and

(c) conduct evaluations as prescribed.

(2) An inspector must, in the carrying out of an evaluation –

(a) exercise his or her powers in accordance with strict regard to decency and order;

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

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

(ii) subject to any limitations and in accordance with any procedures that may be prescribed; and

(c) use any applicable equipment or device necessary to perform his or her functions during an evaluation.

(3) (*a*) Where a person in control of a critical infrastructure refuses entrance to the inspector or cannot be found, the inspector may, in the prescribed form and manner, apply to a magistrate in chambers for a warrant, in the prescribed form, authorising the inspector to enter the infrastructure for purposes of an inspection.

(*b*) An inspector who is in possession of a warrant contemplated in paragraph (*a*), may use such force as may be reasonably necessary, proportional to all the circumstances relating to enter the for purposes of an inspection .

(4) If an inspector discovers that any method of safeguarding or securing critical infrastructure or any other non-compliance with this Act may have a negative impact on the critical infrastructure and cause deterioration or failure, such inspector may—

(a) demand immediate discontinuation of such non-compliance or failure; and

(b) afford the person in control of that critical infrastructure a reasonable period, but no more than 30 days, to rectify such practice in order to ensure compliance with the Act.

(5) The person in control of a critical infrastructure and the security manager must assist an inspector in the performance of his or her functions under this Act.

(6) The Minister may by notice in the *Gazette* in consultation with the heads at public entities or statutory body, either generally or subject to such conditions as may be specified in the notice, extend the powers contemplated in this section to any person employed by a public entity contemplated in 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 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977).

(7) The notice contemplated in subsection (6) 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*)(i) are applicable to such person in the exercise of such powers.

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 (1) and (2) may include persons who are not police officials.

(4) If a committee or working group consists of more than one member, the National Commissioner must designate a police official who is a member of such 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 Republic or elsewhere, been sentenced to imprisonment without the option of a fine;

(b) does not have a valid security clearance certificate issued to him or her by an intelligence service established in terms of the Constitution, on the level as determined by the Minister;

(c) is an unrehabilitated insolvent;

(d) is not a South African citizen;

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

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

(8) The Cyber Security Centre shall function as a standing committee to advise the Council on any matter relating to national critical information infrastructures and related matters.

Persons who may enter critical infrastructure without permission

13. Subject to permission of the person in control of a critical infrastructure, the restrictions on entry as contemplated in section 25(2) do not apply in respect of any

member of the security services established in terms of section 199 of the Constitution, 1996 who is required in the performance of his or her functions and carrying out his or her duties to enter or enter upon any critical infrastructure and who produces proof of his or her appointment and identity to the satisfaction of the person in control of the critical infrastructure or appointed security manager.

Delegations 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 section 27; or

(b) the duty imposed on the Minister by sections 4, 12, 16, 19 and 20.

(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;

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

(e) 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) Any 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 an annual basis, table a report in Parliament through the Joint Standing Committee on Intelligence on the activities of the Critical Infrastructure Council, substantially corresponding with the format of the report in section 7*(g)*.

CHAPTER 3

DECLARATION AS CRITICAL INFRASTRUCTURE AND INFRASTRUCTURE COMPLEX

Power of Minister to declare critical infrastructure and 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) the National Commissioner.

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

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

(i) significant economic operations;

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

(iii) the provision of goods or services essential for the daily operations, economic activity, livelihood or well-being of the public; or

(iv) national security;

(b) any prescribed guidelines for the identification of critical infrastructure; and

(c) recommendations of the Critical Infrastructure Council.

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

(4) In the event where any infrastructure, partly consists of, incorporates or houses any information and communications infrastructure as contemplated in the Cybercrimes and Cybersecurity Act, 2015, the Minister must consult with the Cabinet member responsible for State security before exercising any power contemplated in subsection (1).

(5) The Cabinet Member responsible for State Security must—

(*a*) consider whether the information and communications infrastructure referred in subsection (4) should be dealt with in terms of section 58(2) of the Cybercrimes and Cybersecurity Act, 2015; and

(*b*) inform the Minister, in writing, of his or her decision.

(6) Where the Cabinet member responsible for State Security decides that the information and communications infrastructure referred to in subsection (4) should not be dealt with in terms of section 58(2) of the Cybercrimes and Cybersecurity Act, 2015, the Minister must deal with the application contemplated in subsection (1), 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 takes 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 essential public services or maintain law and order;

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

(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 critical infrastructure, including its equipment, materials or service; or

(iii) recover 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) level of risk or threats to which such an infrastructure is exposed;

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

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

Application for declaration as critical infrastructure by the 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 17(1) to have such infrastructure declared as critical infrastructure.

(2) The National Commissioner may require of the person in control of that infrastructure to provide any information necessary for the proper consideration of the application.

(3) Upon receipt of an application and the information contemplated in terms of subsection (2), the National Commissioner must within 30 days—

(a) conduct a physical risk assessment of the infrastructure in order to—

(i) determine the level of importance of the infrastructure;

(ii) determine the risk category where such infrastructure may be categorised; and

(b) within 30 days after the physical risk assessment has been conducted, submit a written evaluation report together with the application made in terms of subsection (1) to the Critical Infrastructure Council for consideration.

(4) The National Commissioner must, before compiling the evaluation report, provide the person in control of that infrastructure with an opportunity to make written submissions regarding any physical risk assessment which is conducted as contemplated in subsection (3)*(a)*

(5) The National Commissioner may request any other member of the security services established under section 199 of the Constitution to assist with the physical risk assessment contemplated in subsection (3)*(a)*.

(6) Where the National Commissioner is unable to comply with the timeframes as contemplated in subsection (3), the National Commissioner must in writing apply to the Council in the prescribed form and manner for an extension.

(7) The Critical Infrastructure Council must at its quarterly meeting consider the application and all other facts pertaining to the matter.

(8) The Council must within 7 days of its last quarterly meeting, submit the application and its recommendations to the Minister for a decision.

(9) Where the Council is unable to comply with the timeframes as contemplated in subsection (8), the Council must in writing request the Minister for an extension.

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

Application for declaration as critical infrastructure by the National Commissioner

19. (1) Where the National Commissioner makes an application for the declaration of an infrastructure as a critical infrastructure, the application must, subject to subsection (3), be made in the prescribed form and manner and submitted to the Critical Infrastructure Council for consideration.

(2) After consideration, in terms of subsection (1), the Council must submit the application to the Minister for his or her decision.

(3) Where the National Commissioner intends to make an application to have any infrastructure declared a critical infrastructure, the National Commissioner must—

(a) notify the person in control of an infrastructure, in the prescribed form and manner, of the intention of the National Commissioner;

(b) afford the person in control of an infrastructure an opportunity to make written representations on any aspect relating to the intended application of the National Commissioner;

(c) consider the representations of the person in control of an infrastructure; and

(d) in writing, notify the person in control of an infrastructure of his or her decision.

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—

(a) whether to declare the infrastructure as critical infrastructure or not; 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 decision and the reasons for such decision; and

(b) afford the person in control of that critical infrastructure a period of no less than 30 days to make representations.

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

(4) The Minister may declare an infrastructure as critical infrastructure after consideration of the application, the recommendation of the Critical Infrastructure Council and any other information which he or she deems appropriate.

(5) The Minister may—

(a) categorise a critical infrastructure that is declared in terms of subsection (4) in a low, medium- or high-risk category as may be prescribed; and

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

(6) 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 or infrastructure complex as a critical infrastructure;

(b) the risk category of such declaration;

(c) the conditions contemplated in subsection (5)(b);

(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).

(7) When making the recommendation contemplated in subsection (1), the Council may, taking into account the probability of compromising the security of the critical infrastructure in question, recommend that the Minister determine that the publication of information regarding the security measures which should be implemented at such critical infrastructure be restricted.

Certificate of declaration as critical infrastructure

21. (1) Where 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 category as determined by the Minister;

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

(c) the conditions as the Minister may deem necessary to impose for purposes of securing the critical infrastructure.

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

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

(4) The declaration of any infrastructure as critical infrastructure does not exempt a person in control of a critical infrastructure from having to comply with the provisions of any other law, except as may be provided for in this Act.

(5) The National Commissioner shall enter the particulars of any declaration as critical infrastructure or the termination of such declaration, into the prescribed register.

Amendment or variation of information or conditions by Minister

22. (1) If there is a change in the circumstance of any critical infrastructure, the Minister may, on the advice 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 section 20(5); 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 of the Council to amend or vary the risk categorisation, 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 should not amend or vary the risk categorisation, information or conditions on the certificate of declaration .

(3) The Minister must consider 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 subsections (3) or (4).

(2) The person in control of a critical infrastructure must notify the Minister 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 Minister may revoke the declaration as critical infrastructure if the person in control of the critical infrastructure—

(a) after having considered the notice as contemplated in subsection (2); or

(b) fails to comply with any—

(i) condition of declaration; or

(ii) of the provisions of this Act.

(4) The Minister may revoke the declaration as critical infrastructure if the infrastructure in question is declared as critical infrastructure on the basis of incorrect or false information.

(5) Before revoking the declaration as critical infrastructure contemplated in subsections (3)*(b)* or (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 30 days to submit written representations as to why the declaration as critical infrastructure should 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 state the reasons for and the date on which revocation takes effect in such notice.

(b) A notification contemplated in paragraph *(a)* must be served on the person in control of a 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 subsections (3) or (4), the person in control of that critical infrastructure must immediately—

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

(b) return all certificates to the Minister in the event of termination contemplated in subsection (1)*(a)*.

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(6), the owner of a critical infrastructure must take such steps as may be prescribed to secure such critical infrastructure at its own expense.

(2) The person in control of a critical infrastructure that is owned by the state must take steps to ensure that such critical infrastructure is protected by the state.

(3) Where the state is unable to protect a critical infrastructure referred to in subsection (2), the person in control of that critical infrastructure must take steps to appoint a security service provider to protect the critical infrastructure: Provided that the security service provider and its security officers are issued with a security clearance certificate by the State Security Agency or any other intelligence service established in terms of the Constitution.

(4) The Minister may, if the person in control of a critical infrastructure shows good cause in the application contemplated in sections 18(1) and 19(1), and in consultation with the Cabinet Minister of Finance and the Minister of the affected department, determine that a Head of a Government Department is, subject to such conditions as the Minister may determine regarding the recovery of cost from that person, responsible for all or some of the expenses necessary to implement the steps contemplated in subsection (1) and in writing inform the person in control of that critical infrastructure of the decision.

(5) In the event that a person in control of a critical infrastructure fails to take such steps as 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 said 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 cost thereof from that 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 security manager to—

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

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

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

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

(e) 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.

(8) A person in control of a critical infrastructure must 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.

Access to critical infrastructure

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

(a) take such steps as he or she may consider necessary and lawful 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; and

(b) issue a notification in the prescribed form that those critical infrastructures may only be entered upon in accordance with the provisions of subsection (2).

(2) *(a)* No person may without the permission of a 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 a security manager, or the security personnel under the direction of the security manager, may require of that 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 or 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;

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

(3) Where a security manager grants permission to a person in terms of subsection (2), he or she may do so subject to conditions regarding—

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

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

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

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

(e) escorting the person while he or she is on or in the critical infrastructure; and

(f) other requirements as he or she may consider necessary.

(4) Without derogating from the provisions of the Trespass Act, 1959 (Act No. 6 of 1959), a 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) the security manager considers it 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 require that persons and vehicles leaving that critical infrastructure be searched.

(6) Any search conducted under subsections (2)*(b)*(vi) and (5) must be carried out by a person of the same gender with strict regard to decency and order.

(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 and intentionally—

(a) tampers with, damages or destroys critical infrastructure; or

(b) colludes with or assists another person in the commission, performance or carrying out of an activity referred to in paragraph (a),

and who knows or ought reasonably to have known that it is critical infrastructure, is guilty of an offence and liable on conviction to a period of imprisonment not exceeding 30 years.

(2) Any person who—

(a) unlawfully 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;

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

(c) unlawfully furnishes, disseminates or publishes in any manner whatsoever information relating to the safety and security measures applicable at or in respect of a critical infrastructure;

(d) takes or records, or causes to take or record, an analog or digital photographic image, video or film of a critical infrastructure or critical infrastructure complex with the intent to use or distribute such analog or digital photographic image, video or film for an unlawful purpose;

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

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

(g) unlawfully threatens to damage critical infrastructure;

(h) unlawfully enters in or onto, or gains access to critical infrastructure,

,

commits an offence and is liable upon conviction to a fine or to imprisonment for a period not exceeding 20 years, or to both a fine and such imprisonment .

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

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

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

(c) refuses or fails to take the steps specified in the notice contemplated in 24(1) within the period specified in the notice,

is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment.

(4) Any person who fails to comply with a warrant issued in terms of section 11(3)(*a*), is guilty of an offence and is liable on conviction to a fine or imprisonment not exceeding 12 months or to both such fine and imprisonment.

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

CHAPTER 6

REGULATIONS

Regulations

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

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

(b) any procedure for an evaluation to be done in terms section 11(1)*(c)*;

(c) the form and content of a certificate contemplated in section 12(2)(b);

(d) guidelines for the categorisation of critical infrastructure in a low-, medium- or high risk category as contemplated in section 20(5);

(e) the format and contents of the register contemplated in section 21(5);

(f) the steps that must be taken by a person in control of a critical infrastructure as contemplated in section 24(1);

(g) scope and format of any security, policy and plan contemplated in section 9(2)(*f)* and section 24(7)(*a*);

(h) size, form, and content of any notice or sign that must be placed as contemplated in sections 24(8) or 25(8);

(i) establishment, functioning, meeting and reporting procedure of any committee or the Critical Infrastructure Council;

(j) size, form, and content of any direction that must be issued as contemplated in section 25(1)*(b)*;

(k) grounds which disqualify security personnel from appointment or continued employment at critical infrastructure;

(l) the measures and standards for safeguarding of critical infrastructure as well as the protection and security thereof;

(m) the requirements, qualification, security levels and procedure of appointment of security personnel;

(n) the standards and content of a training course that security personnel who are employed or whose services are hired, must comply with;

(o) access and egress control at critical infrastructure;

(p) administration, provisioning and functioning of security at critical infrastructure;

(q) the role and responsibilities of security personnel at critical infrastructure;

(r) emergency and evacuation procedures at critical infrastructure;

(s) guidelines for the identification of any infrastructure or infrastructure complex, including cyber-based or electronic systems, that may be considered for declaration as critical infrastructure or infrastructure complex;

(t) the form and manner of any application for declaration as critical infrastructure;

(u) any conditions relating to the declaration as critical infrastructure; format of any certificate of declaration and the manner in which such certificate is issued;

(v) the publication of areas and places declared as critical infrastructure and the requirements for information to the public; or

(w) any other ancillary or administrative matter that 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 imprisonment for a period not exceeding 12 months or a fine or both a fine or 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 notification before promulgation.

(6) Any regulation necessary for the immediate implementation of the Act must be promulgated within three months after the coming into operation of the Act.

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 National Key Points Act, 1980 (Act No. 102 of 1980) is hereby repealed.

Transitional arrangements

30. (1) Any National Key Point declared under section 2 of the National Key Points Act, 1980 (Act No. 102 of 1980) ("the previous Act") and a National Key Point complex declared under section 2A of the previous Act, shall be deemed to have been declared critical infrastructure, until after such declaration has been

reviewed by the National Commissioner and a recommendation has been made to the Critical Infrastructure Council.

(2) The Critical Infrastructure Council must ensure that all declarations contemplated in subsection (1) are reviewed and a recommendation made to the Minister within a period of 60 months after the coming into operation of this Act.

(3) Subject to subsections (4)*(a)* and *(b)*, this Act does not affect any proceedings instituted in terms of the previous Act 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.

(4) *(a)* Proceedings contemplated in (3) must be regarded as having been pending if the person concerned had pleaded to the charge in question.

(b) No proceedings may continue against any person in respect of any contravention of a provision of the previous Act 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.

(5) *(a)* Despite the repeal of the previous Act, 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 *(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.

(6) The functions, powers and duties assigned in terms of sections 3, 8 and 12 of the previous Act and the regulations related to those sections shall remain in force for the period contemplated in subsection (2) insofar as it is not in conflict with the provisions of the Act.

Indemnity against loss or damage

31. Neither the Minister nor any person in the service of the State is liable for any loss or damage as a result of bodily injury, loss of life or damage to property caused by or arising out of or in connection with any act ordered, performed or executed under this Act, except in the case of any wilful act or omission on the part of the Minister.

Short title and commencement

32. This Act is called the Critical Infrastructure Protection Act, 2015, and comes into operation on a date determined by the President by proclamation in the *Gazette*.

Printed by and obtainable from the Government Printer, Bosman Street, Private Bag X85, Pretoria, 0001
Contact Centre Tel: 012-748 6200. eMail: info.egazette@gpw.gov.za
Publications: Tel: (012) 748 6053, 748 6061, 748 6065