CRITICAL INFRASTRUCTURE PROTECTION BILL [B22 – 2017]

RESPONSE TO SUBMISSIONS: PORTFOLIO COMMITTEE ON POLICE

06 February 2018

civilian secretariat for police service

Department:
Civilian Secretariat for Police Service
REPUBLIC OF SOUTH AFRICA

CIVILIAN SECRETARIAT FOR THE POLICE SERVICE AND SOUTH AFRICAN POLICE SERVICE RESPONSE TO SUBMISSIONS BY VARIOUS ENTITIES

1. TAGGING

Comment by	Comment	Response
Western Cape Government	Bill should be tagged as section 76 Bill	State Law Advisers are of the opinion that it is a section 75 Bill

2. LONG TITLE

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.

Comments by	Comments	Response
Greenpeace	The long title should clearly state that the measures referred to are in the public interest"	See clause 2(e)

3. **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,

Comments by	Comments	Response
Greenpeace	Preamble should refer to rights that are affected	The Constitution already guarantees the rights

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;

Comments by	Comments	Response
Right2Know	Definition is too broad	It must be kept in mind that clause16(2) limits the declaration of infrastructure to instances where the loss, damage, unlawful disruption or immobilisation of such infrastructure may *severely prejudice* the provision of basic public services. There is an internal limiter in clause 16(2)
APCOF	Definition is too broad	See comments above
Cosatu	Welcomes the amendment to "basic public services"	See first comment

''critical infrastructure'' means any infrastructure 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 determined as such in terms of section 16(3);

Comments by	Comments	Response
Research Unit and APCOF	"critical infrastructure" should be clearly defined	The Bill makes it clear that CI is **only** those infrastructure that has been declared as such by the Minister. If there is no declaration, it is not CI and the provisions of the Bill are not applicable.
NERSA	Delete definition of "critical infrastructure complex"	The critical infrastructure complex is declared when multiple critical infrastructures need to be managed together – Durban Harbour is an example
Right2Know	"Strategic installations" are unaccounted for in the Bill	This concept will disappear and be taken into the CI process

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

Research Unit	NEDLAC disagreement in respect of Cybercrimes and Cybersecurity Bill	During the NEDLAC process the matter was raised by Business. They were of the opinion that the Bill cannot refer to legislation (i.e. the Cybercrimes and Cybersecurity Bill) that is not enacted. It is submitted that there was a fundamental lack of understanding regarding the drafting issues involved. The Department of Justice was consulted who proposed that the Minister of State Security has “first choice” on whether infrastructure should be declared under the CIP Bill or under the Cybercrimes and Cybersecurity Bill. There is clarity that the CIP Bill ony deals with physical infrastructure.
Western Cape Government	Definition is too wide	It is submitted that the proposed definition conveys the same meaning
Right2Know	Overlaps with Cybercrimes and Cybersecurity Bill	There is clarity that the CIP Bill ony deals with physical infrastructure.

‘‘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;

Comments by	Comments	Response
Western Cape Government	Exclude “information infrastructure”	The comment is noted and will be discussed with the State Law Adviser. A proposal will be drafted for submission to the committee during the clause-by-clause deliberations

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

Comments by	Comments	Response

Research Unit	Include definition of “national security”	A definition could be considered. However, when words are interpreted, it must be done with reference to their ordinary meaning. A dictionary definition does not convey anything beyond that meaning that would be specific to the Bill and it is espectfully submitted that the proposed definition is lacking in that respect. It is therefore proposed that a more specific definition be inserted where all the *components* of national security are covered. These are usually regarded as the military component, but it also includes the aspects of politics (Constitutional democracy), society (law and order), economics environment (financial stability), energy (electricity) and natural resources (water, mining) that has an influence on the manner in which a nation exists.

‘‘organ of state’’ means an ‘organ of state’ as defined in section 239 of the Constitution;

Comments by	Comments	Response
		The Constitution defines “organ of state” as follows: (a) any department of state or administration in the national, provincial or local sphere of government; or (b) any other functionary or institution— (i) exercising a power or performing a function in terms of the Constitution or a provincial constitution; or (ii) exercising a public power or performing a public function in terms of any legislation, but does not include a court or a judicial officer; This would include the Reserve Bank (sec 223) and the Gautrain Management Agency (Gautrain Management Agency Act 5 of 2006).

‘‘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, 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;

Comments by	Comments	Response
South African Reserve Bank	Needs to be included	See comment at “organ of state”
Gautrain Management Agency	Situation is unclear in terms of responsibility under clause 24 and clause 25	This is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	A situation could arise where concessionaire applies	This is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
Western Cape Government	The words in (b)(ii) “any other person” is vague and specific reference must be made	This is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations

Comments by	Comments	Response
Western Cape Government	Include definition of “Republic”	It is submitted that such a definition would not add to the interpretation of the Bill

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

Comments by	Comments	Response
Right2Know	Risk categories are not clearly	The comment is noted and will be discussed with the State Law Adviser. A

	defined	proposal will be drafted for submission to the committee during the clause-by-clause deliberations

''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;

Comments by	Comments	Response
Right2Know	The definition is open-ended and may be abused	It is submitted that clause 27(1)(n) adequately provides for standards

''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;

Comments by	Comments	Response
Right2Know and South Durban Community Environmental Alliance	The definition is open-ended and may be abused	It is submitted that clause 27(1)(n) adequately provides for standards

''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;

Purpose of Act

2. The purpose of this Act is to—

(a) secure critical infrastructure against threats;
(b) ensure that information pertaining to critical infrastructure remains confidential, subject to the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), or any other legislation 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.

Comments by	Comments	Response
Research unit	Insertion of the words”security measures applicable to” in 2(b)	The recommendation is sound. A proposal will be drafted for submission to the committee during the clause-by-clause deliberations

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.

Comments by	Comments	Response
Research Unit and South African Catholic Bishops'Conference	Commented on the exclusion of Department of Defence infrastructure	The exclusion of DoD infrastructure was on request of the DoD. Section 104(4) and 104(19) of the Defence Act 42 of 2002 provide for offences relating to entering and access of defence installations. Furthermore, the CIP Bill provides for the securing of infrastructure by security service providers while the DoD secures its own installations. As these installations are related to the defence of the country, somemay have stringent controls.
Greenpeace	The Bill should state that it does not limit certain constitutional rights except to the extent necessary to prevent significant harm or damage etc.	The Constitution already guarantees the rights stated.

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 subsection (3).
(3) Subject to subsection (5), the Minister must appoint the following persons as members of the Council:
(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 Communications;
(ii) Department of Defence;
(iii) Department of Home Affairs;
(iv) Department of Justice and Constitutional Development;

(v) Department of Public Works;
(vi) Department of Transport;
(vii) National Disaster Management Centre;
(viii) South African Local Government Association;
(ix) South African Police Service; and
(x) State Security Agency; and

Comments by	Comments	Response
Research Unit	Government officials should be vetted	Agreed

(c) five members appointed in terms of subsection (6) from the private sector who are—
(i) not disqualified in terms of section 5; and
(ii) appropriately qualified, knowledgeable and experienced in critical infrastructure protection, risk management, disaster management or basic public services.

Comments by	Comments	Response
Research Unit, Western Cape Government and South African Catholic Bishops'Conference	Strengthen the appointment process to ensure impartiality	This determination can only be done by the Committee. Should the Committee feel that the appointment process should rather be through Parliament, it is proposed that the clause be amended in consultation with the State Law Adviser to reflect this process. An improved oversight role could be created through this amendment.
South African Reserve Bank and APCOF	It was alluded to that private sector members should have more versatile qualifications	It is submitted that this aspect may be considered. See also comments in respect of the functions of the National Commissioner

(4) In addition to the officials contemplated in subsection (3)*(b)*, the Minister may request the Head of a Government department—
(a) to designate an appropriately qualified official; or

(b) any other person, on an *ad hoc* basis, to assist in general or 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 institution in question; and

(b) members referred to in subsection (3)*(c)* after complying with subsection (6).

(6) The Minister appoints members of the Critical Infrastructure Council contemplated in subsection (3)*(c)* on such terms and conditions as the Minister may determine, after—

(a) publishing 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) appointing a panel consisting of a person who is admitted as an advocate or an attorney, and has practised as such for a cumulative period of at least 10 years after being admitted, as chairperson, and four other persons who are appropriately qualified, knowledgeable or experienced in infrastructure protection, to—

(i) compile a list of not more than 20 persons from— *(aa)* the applications and nominations referred to in paragraph *(a)*; and *(bb)* persons serving on the Council who qualify for a further appoint
ment in terms of subsection (8); and

(ii) conduct interviews with the persons referred to in subparagraph (i) for purposes of compiling a list of 10 recommended candidates in order of preference;

(c) the chairperson of the panel has submitted the list of 10 recommended candidates with their résumés to the Minister;

(d) the Minister has submitted the list of recommended 10 candidates to the State Security Agency for vetting;

(e) the Minister has consulted the Cabinet on the list of the top five recommended candidates who are not disqualified in terms of section 5*(b)*; and

(f) the Minister has submitted a report setting out the list of the top five recommended candidates together with their résumés to the Parliamentary Portfolio Committee on Police for noting.

Comments by	Comments	Response
Research Unit	Vetting process was regarded as intrusive by NEDLAC	It would not be advisable to forego the vetting process
	Bill must set out clearance level	Comment is noted

(7) The Secretary for the Police Service is the Chairperson of the Council and the Minister must designate, from the persons contemplated in subsection (3)*(c)*, a member as deputy chairperson.

Comments by	Comments	Response
Western Cape Government	Chairperson should be appointed on recommendation of Parliament	It is submitted that this is typically an oversight role that falls within the functions of the Secretary

(8) Subject to subsection (10), members of the Council appointed in terms of subsection (3)*(c)* hold office for a period not exceeding four years.

Comments by	Comments	Response
Research Unit	Period should be extended to five years	Agreed

(9) Upon the expiry of an appointed member's first term of office as contemplated in subsection (8), the member may be re-appointed for one further term only.
(10) A member of the Council appointed in terms of 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 as contemplated in subsection (12).
(11) *(a)* 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 (6)*(b)*, within a period of 90 days, appoint a new member for the unexpired portion of that period after having consulted with the Cabinet.
(b) Despite paragraph *(a)*, the Minister may in order to select a candidate for appointment in terms of this subsection, comply with subsection (6)*(b)* or choose a candidate from the remainder of the list of 10 candidates as contemplated in subsection (6)*(d)*.
(12) The Minister may, after due process, remove a member of the Council appointed in terms of subsection (3)*(c)* from office on account of—
(a) misconduct, incapacity or incompetence;
(b) absence from three consecutive meetings without good cause;
(c) becoming disqualified as contemplated in section 5; or
(d) any other lawful reason.

Comments by	Comments	Response
Research Unit	4(11)(b) should be strengthened to	It is submitted that the process is clear: the Minister may decide to choose a

	clarify process	shortlisted candidate instead of using the procedure in 4(6)(b)

(13) The Minister may request the Cabinet member responsible for an institution which is represented on the Council, as contemplated in subsection (3)*(b)*, to nominate another representative for appointment to substitute the institution's representative in the Council.
(14) Members of the Council who are appointed as contemplated in subsection (6) and are persons outside the public sector may be paid for their services such remuneration and allowances as the Minister may, with the concurrence of the Minister of Finance, determine.

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

Comments by	Comments	Response
NERSA	Propose adding: "has been removed from a position or an office of trust"	The comment is noted and will be discussed with the State Law Adviser. A proposal will be drafted for submission to the committee during the clause-by-clause deliberations

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(14), must be defrayed from the budget 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).

Comments by	Comments	Response
Research Unit	Financial implications of the Bill – this will put the CSP budget under pressure	The costs involved will only be the payment of the private sector members. A preliminary costing was done Column1 Column2 **Board members** Compensation 459099.1685 Accommodation 228340 Meals 35280 Travel 196000 Provisional Cost 918719.1685
NERSA	The Council should be allocated its own budget to enhance independence	The proposal is noted. However, allocation of a budget will require permanent staff and all the concomitant expenses. It is submitted that the proposed structure will be the most economical.

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 infrastructure;

(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) on the budgetary implications relating to critical infrastructure protection; and

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

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

(c) make recommendations to the Minister on—

(i) applications for the declaration as critical infrastructure, including any conditions for such declaration, 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 physical security assessments, resilience reports and any recommendations from the National Commissioner or the cyber response committee 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 they relate to critical infrastructure protection;

(g) compile and submit a report to the Minister within three months after 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) the level and extent of public-private sector cooperation; and

(v) any other matter that may impact on critical infrastructure or 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.

Comments by	Comments	Response
Research Unit	Organise Business requested that roles of stakeholders in the Cybercrimes and Cybersecurity Bill be clarified	That clarification can not take place in a different piece of legislation
	Public Private cooperation needs to be promoted	7(a)(viii) could be inserted: <u>(viii) any relevant manner or mechanism to promote public-private sector cooperation.</u>
	CIC should approve policies and guidelines developed by the National Commissioner	As political head of the departments one would expect those policies to be approved by the Minister. The role of the CIC is to provide a mechanism to assist the Minister in applying his or her mind

NERSA	Proposal to delete a word in clause 7(b)	It is unclear what the proposal entails
	Proposal to insert the words “at least” in clause 7(g)	It is submitted that the proposal will not change the current meaning and that it could contribute to vagueness.

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) *(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.

Comments by	Comments	Response
NERSA	Clause 8 must provide for a quorum	It is submitted that clause 27(1)(b) provides for regulations on the issue

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 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 consideration by the Council regarding—
(a) the manner in which—
(i) infrastructure must be identified, categorised and declared critical infrastructure;
(ii) any 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; 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 that infrastructure as critical infrastructure;
(b) conduct or facilitate a security assessment or other physical security 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 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) *(a)* In the event that the infrastructure referred to in an application partly consists of, incorporates or houses any possible critical information infrastructure, the National Commissioner must, before making any recommendations to the Council as contemplated in subsection (3)*(c)*, refer the application to the cyber response committee.
(b) The cyber response committee must—
(i) conduct an assessment of the infrastructure referred to in the application to determine the extent to which such infrastructure consists of, incorporates or houses, any critical information infrastructure;
(ii) compile a report setting out recommendations on the manner in which the physical security measures of the infrastructure referred to in the application and the physical or technical security measures of the critical information infrastructure must be dealt with in terms of this Act or any directive issued under any cybersecurity legislation; and
(iii) submit the report to the National Commissioner.
(c) The National Commissioner must submit the report contemplated in paragraph *(b)*(iii), with the recommendations contemplated in subsection (3)*(c)*, to the Council.

Comments by	Comments	Response

Research Unit	Clause 9(4)(a) to (c) creates a dual process with clause 16(4)	The matter will be discussed with the State Law Adviser responsible for the Cybercrimes and Cybersecurity Bill with the view to submit a redrafted process for consideration of the Committee
NERSA	Insert “and recommend to the Council” in 9(3)(a)	It is submitted that 9(3)(c) covers this aspect
	Delete the word “such” before “critical”	The proposal is noted. However it is submitted that the word “such” links the paragraph to the preceding paragraphs
	9(3)(h)(ii) – insert the phrase “for declaration as infrastructure” after “application”	It is submitted that the phrase is already contained in the text.
Western Cape Government	Clarify the recommendation in 9(2) to insert the words “and approval” to ensure the CIC approves the standards etc. Links to clause 7.	This is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations

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

Comments by	Comments	Response
Research Unit	Establishment and maintenance of an administrative system	The current NKP system will be adapted for use and a new system will be unnecessary

Designation of inspectors

10. (1) The National Commissioner may designate police officials 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 (7) 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.

Comments by	Comments	Response
Research Unit and South African Catholic Bishops'Conference	Inspectors should obtain consent from person in control to enter	In principle there is no issue with that. However, this could create a situation where inspectors are not allowed access for routine inspections. It is submitted that routine inspections are not invasive and does not amount to a search. 11(1)(a) provides for a limited scope in terms of the inspections, limited to compliance.
	Inspector may issue compliance notice without magistrate.	it is submitted that the limitation of the powers in 11(1)(a) as well as the provisions in clause 27(1)(g) where the standards will be promulgated in regulations
NERSA	Insertion into clause 11(3)(b)	It is submitted that the commentator may have been working on a previous draft version of the Bill
	Clause 11(7)(a) – delete commas	The clause is now clause 8. It is submitted that the commentator may have been working on a previous draft version of the Bill.
South African Catholic Bishops'Conference	Clause 11(9) incorrectly refers to (7) and not (8)	

***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) 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 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 national critical information infrastructure and related matters.

Comments by	Comments	Response
Research Unit	Clarity on 12(4) in respect of the committee members and private sector advisers	The intention is not to create the possibility for use of private sector advisers. In many cases the ad hoc committees wil not necessarily be involved in work that requires security clearance. It is also not invisaged that private sector experst need to be employed and remuneration will therefore not be an issue.
	Valid security clearance certificates	It is envisaged that regulations to this effect will be promulgated under clause 27(1)(c)
	Vetting to be done by SAPS	Section 2A of the National Strategic Intelligence Act 39 of 1994 assigns this function to the National Intelligence Acency (SSA)
	Cyber Response Committee as standing committee	The Cyber Response Committee is created in terms of the Cybersecurity and Cybercrimes Bill and is therefore not answerable to the National Commissioner but as a separate entity. The intent is to create a link between the Council and the Cybersecurity Bill to consult on matters of mutual interest. The Cyber Response Committee does not advise the national Commissioner, as the SAPS is represented on that committee.
SARB	Proposes insertion of clause 12(9) to ensure consultation with the reserve bank in cases where financial stability is an issue	The comment is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations

Exemption of certain persons

13. Subject to the permission of a person in control of a critical infrastructure, 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 and who produces 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.

Comments by	Comments	Response
Research Unit	Stated that the Minister may delegate regulation making to the National Commissioner	Not correct – excluded in terms of clause 14(1)

Reporting by Minister

15. The Minister must, on an 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*(g)*.

Comments by	Comments	Response
Right2Know	Reporting must be transparent	Previous references to the JSC on Intelligence have been removed

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) 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.

Comments by	Comments	Response
Research Unit,	There was a APCOF concern	Critical nfrastructure only gets the status of CI when declared by the Minister.

APCOF, Right2Know	about basic public service institutions that could be deemed critical – this could include clinics, schools, universities as well as a Right2Know concern about the proliferation of CI	It is clear that “infrastructure” may include clinics, schools universities. However, when regard is had to 16(2)(b), it is clear that the declaration of critical ifrastructure is limited to *only* infrastructure where 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. The Minister must have regard to the factors set out in 17, namely the sector (e.g. water energy, communication), the strategic importance in terms of the country’s ability to function, deliver basic public services or maintain law and order (e.g. government structures such as Parliament, the police etc.), the risk category, whether the applicant can afford to maintain the CI and its security measures (CI will be declared *on application* of the infrastructure itself), the effects or the risk of a destruction, disruption, failure or degradation on the environment the health or safety of the public or other infrastructure (e.g. Koeberg), the size and location of any population at risk (e.g. a terrorist attack on the Gariep Dam), historic incidents (e.g. previous attacks such as 9/11 in the u.s.), the level of risk or threats to which the infrastructure is exposed (vulnerability or desirability of an attack e.g. eNATIS), if there are special characteristics which enhance the resilience (e.g. the remoteness of a location) and the extent to which the declaration promotes the interests of the public (e.g an airport in terms of safety of travellers).
	Section 16 and 20 must be brought in line with each other	Section 16(1) states: *Subject* to the provisions of this Chapter, the Minister may declare… The sections are therefore linked. The Chapter first establishes the powers of the Minister (16), then sets out the factors to be taken into account (17), then the two processes of application (18, 19) and then deals with the declaration itself and how that must be done (20), followed by the effects of declaration. If the Committee is of the opinion that the chronology may be

		confusing, the order of the sections can be reconsidered for a redraft proposal.
	The role of the Council is not expressly provided for	See comment above
Western Cape Government	Council is better placed to decide on declaration	It is submitted that the Minister, as functionary, should ultimately carry the responsibility as the Council is advisory
	Clause 16(2) should include consultations with the provincial MEC where the CI falls within a provincial governments property portfolio	It is submitted that the province will in such a case be the applicant and theinput will be in the application
Greenpeace	Parliament should play a role in the declaration of CI	It is submitted that Parliament will play such a role in respect of the reports that must be submitted
Greenpeace, SJC and Right2Know	Avoid proliferation of CI	As the Bill seeks to address risks to more than pure secueity issues, it may happen that there will be more CI declared. However, the risk categories should actually limit those CI that are in need of extreme security measures.
SJC	Clause 16(2) factors are too wide: What constitutes “national security”?	See comments in definition section
Right2Know and South Durban Community Environmantal Alliance	Clause 16(2) is overly broad and vague and clause 17 is open-ended	See first comment.
South African Catholic Bishops’ Conference	Provision should be made for the possible negative consequences of declaration	It is submitted that clause 17(j) alludes to this. The proposed insertion is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations

(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) In the event where any infrastructure partly consists of, incorporates or houses, any information and communications infrastructure as contemplated in any legislation

on cybersecurity, the Minister must consult with the Cabinet member responsible for State Security before exercising any power contemplated in subsection (1).

Comments by	Comments	Response
Research Unit	There is a dual process in clauses 9(4) and 16(4) in respect of information infrastructure	See comment above at clause 9(4)
Western Cape Government	Clause 16(4) should be amended to delete “and communications” and to amend the reference to Cabinet member responsible for state security	This is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations

(5) The Cabinet member responsible for State Security must—
(a) consider whether the information and communications infrastructure referred to in subsection (4) must be dealt with in terms of any legislation on cybersecurity; 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 communication infrastructure referred to in subsection (4) must not be dealt with in terms of any legislation on cybersecurity, 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 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;

Comments by	Comments	Response
Research Unit	Risk categories should be defined and the terms on which the categories are determined	Clause 27(1)(i) provides for regulations in terms of which standards and guidelines may be regulated for. It is submitted that this is a dynamic implementation or operational issue that may need to be adapted from time to time.

(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;

Comments by	Comments	Response
Research Unit	Reason for this provision is questioned	The Special Account in the NKP Act was never utilised and the existence thereof criticised in the Right2know campaign judgment. The reason for this provision is that declaration of critical infrastructure will always follow on an application. If an applicant has the required resources, the security measures can be put in place. If, however, the applicant does not have the resources to secure the critical infrastructure, a physical security assessment must take that into account together with the measures that can be put in place over a period of time. Clause 24(4) provides for financial assistance, where required.

(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 promote 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.

Comments by	Comments	Response
Western Cape Government	Amend clause 17(k) to assign function to CIC and not Minister	See comment above – the Minister is the functionary

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 may require of the person in control of that infrastructure to provide any information necessary for the proper consideration of the application.
(3) 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) asses the risk category in which such infrastructure 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 (4) to the Critical Infrastructure Council for consideration.
(4) 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)*.
(5) 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.
(6) 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.
(7) The Critical Infrastructure Council must at its meeting consider the application and the physical security assessment report.
(8) 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.
(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 not exceeding 30 days or such other period as the Minister may determine.
(10) 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.
(11) Where an extension of time is granted as contemplated in subsection (6) or (9), the Council must inform the person in control of that infrastructure in writing.

Comments by	Comments	Response
Right2Know	There is lack of public participating in the decaration process	See clause 18(3)(a) – reports must accompany the application
South Durban Community Environmental Alliance	There is lack of public participating in the decaration process	See clause 18(3)(a) – reports must accompany the application

Application for declaration as critical infrastructure by 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 of the application 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 as critical infrastructure, the

National Commissioner must—
(a) notify the person in control of the infrastructure, in the prescribed form and manner, of the intention of the National Commissioner;
(b) afford the person in control of the 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 the infrastructure; and
(d) within seven days of taking a decision on whether or not to proceed with the application, notify the person in control of the infrastructure in writing of such decision.

Comments by	Comments	Response
Research Unit	19(3)(b) should provide for a time period	This is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	Written representations in terms of clause 19(3) should accompany the application to the CIC	This is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
BASA	Submits that banks can be declared CI if National Commissioner applies. If such a declaration is done, it must be in consultation with the Financial Stability Oversight Committee.(Financial Sector Regulation Act 9 of 2017)	It is submitted that banks do not, on the face of it, comply with the requiremen ts in clause 16(2)(a). However, the comment is noted. A proposal will be drafted and submitted to the Committee during the clause-by-clause deliberations
Western Cape Government	Clause 19(3)(b) – time frames must be limited to expedite the process	See comments above

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 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 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) categorise a 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 category 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.

Comments by	Comments	Response
Western Cape Government	Clause 20(2) – the custodian should also be afforded an opportunity to make written representations	This comment supports the Gautrain Management Agency contention. This is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	Clause 20(4) – declaration should be made by the CIC	See comments in this regard made above
South African Catholic Bishops' Conference	Clause 20(2)(b) – period for representations should be longer	It should be kept in mind that this clause refers to the applicant. The period could be extended to 60days.

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 category as determined by the Minister;
(b) the premises or complex where the critical infrastructure is located; and
(c) the conditions which the Minister may deem necessary to impose for purposes of securing the critical infrastructure.

(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) 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.

Comments by	Comments	Response
Western Cape Government	Clause 21(4) – wording is ambiguous and needs to be clarified	This is noted and a proposal will be drafted for submission to the committee during the

		clause-by-clause deliberations

(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.

Comments by	Comments	Response
Right2Know	Transparency requires that CI sites be known	It is submitted that clause 21(5) and (6) adequately provides for standards

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.

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).

Comments by	Comments	Response
Research Unit	This provision seems to apply only to government and state organs	Any type of service rendered by a privately owned critical infrastructure will, in some form or another, be in support of service delivery by government. This clause ensures that a privately owned institutuion such as an oil refinery (department of Mineral Resources) or explosives manufacturer (SAPS as the administrator of the Explosives Act) may be required to assist.
Western Cape Government	Clause 24(1) – if a person cannot afford the security measures, what are the next steps? Will	See comment above and below in respect of expenditure

	public funds be used for private sites?	
South African Catholic Bishops'Conference	Costs should be financed by the state	This is a matter of policy. If a private entity applies, it has someform of partnership with the state. Section 24(4) allows for assistance.

(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 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 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.

Comments by	Comments	Response
Research Unit	Responsibility for expenditure for security measures is unclear	Clause 24(1) is unambiguous. The financial resources of the applicant is but one of the factors that the Minister may consider before declaration. If, for instance, an applicant is not financially able to implement security measures, the application may be deferred for a period to provide the applicant the opportunity to obtain resources or apply in terms of clause 24(4)
	Clause 24(4) is not clear on whether it aplies to privately owned infrastructure	Clause 24(4) applies to privately owned infrastructure and state owned companies as it would be illogical for a government department to apply for assistance from itself. The phrase “person in control” includes private owners.
	Bill should state that security service provider referred to in 2493) is private security and should be subject to PSIRA	The definitions define “security personnel” and “security service provider” as subject to the PSIR Act
	Could a Security Manager be appointed from the private security service provider? - Clause 24(7)	The intention is that the person must be a full-time employee, hence the use of the word “appoint” instead of “designate”. The comment is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations.
	Determination of costs to be recovered in 24(6) must be clarified and more detail provided	Clause 24(6) was deliberately phrased broadly, as this would be a normal civil claim for damages that has to be proved in court.
Western Cape	Clause 24(6) - Minister must be	It is submitted this is a wide ranging proposal and will be draconian and possibly

Government	empowered to close CI and not only secure it.	unconstitutional. It may defeat the very object of the Bill.

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; and
(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 leaving the premises in terms of subsection (5).

(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) 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.
(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.

Comments by	Comments	Response
Research Unit and Cosatu	Clause 25(6) requires that searches be done with regard to decency and order. Reference should be made to sec 29 of the criminal Porocedure Act 51 of 1977.	The comment is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	A penalty should be imposed for a person in control who fails to comply with clause 24(8) and 25(8)	The comment is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
Western Cape Government	Persons should be notified before they enter a CI about the searches	The comment is noted and will be considered. A proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	Clause 25(2)(b) - Include personnel of service providers	The comment is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations

Right2Know	These powers may be abused	Note the words “lawful steps” in clause 25(1)(a) and also clause 27(1)(n) where regulations on the issue will be made
South African Catholic Bishops’ Conference	Clause 25 is too wide and allows for abuse	See comments above
APCOF	No private security – should be done by SAPS	Guarding duties is not part of SAPS mandate – will require a massive expansion
	Role of PSIRA is unclear	Refer to definitions of “security service provider” and “security personnel” where PSIRA is referenced

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.

Comments by	Comments	Response
Research Unit and APCOF	Concerns about the severity of the penalties and disclosure of information	The offences are divided into 3 groups: serious offences that will form part of an investigation into terrorism and espionage. With regard to the first group: As sabotage has been removed from the SA law by the Protection of Constitutional Democracty Against Terrorist and related Activities Act 33 of 2004, there is a need to have a statutory form of sabotage where a terrorism intention is not present. The comments in all the relevant submissions are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations. In respect of the penalties, it was argued that 30 years is very harsh and unreasonable. The comment is noted and a proposal will be drafted for submission to the committee during the clause-

		by-clause deliberations. With regards to the second group, the offences were carefully drafted to exclude any “negligent” act by, as the Right2Know judgment referred to it: a “somnambulent person”. All the offences in this group require an element of “unlawfulness”. It was submitted that “unlawful purpose should be defined. The issue at stake is whether these offences serve a legitimate government purpose and are reasonable and justifiable in an open and democratic society. Even though the right to freedom of expression is limited in some of the offences (disclosure, recordings, photos), the wording of the clauses is clear that there must be an unlawful element to it as well. It is submitted that the offences in this group conform to constitutional limitation requirements. In respect of the penalties, it was argued that criminalisation is very harsh and unreasonable. The comment is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations. The third group of offences concerns violations by persons in control. The comment regarding the failure to demarcate and put up notices in terms of sections 24(8) and 25(8) is noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
Gautrain	Minimum sentences should be introduced	Discretion of judicial officers is not interfered with lightly. Minimum sentences are prescribed only under- these could possibly be limited to the security measures the Criminal Law Amendment Act 105 of 1997.
Greenpeace and APCOF	Offences are overbroad and unconstitutional. A well researched input is made regarding unconstitutionality	See comments above. The Bill does not impose “blanket restrictions” and the input tends to overstate the limitations somewhat. The comments are however noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	Qualify offences to exclude acts that are not actually damaging or threatening	The comments are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations

	Decriminalise offences	The comments are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	Secrecy measures are too harsh	The offence relates to disclosure of security measures. Surely this must be a legitimate government objective to protect the security measures from disclosure.
	Inclusion of a “harm test”	The comments are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	Ban on photos and videos	The comments are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	Offences need to require “intention”	The comments are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	“Public domain test”/”Harms test”/Public interest defence	The comments are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	Criminalising protests and strikes	The comments are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
	Harsh penalties	See first comment
SJC	Echoes sentiments above e.g. Greenpeace	See comments above. The comments are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
JD Bothma	Bill can be used to prosecute persons for non-violent protests	See comments above. The comments are noted and a proposal will be drafted for submission to the committee during the clause-by-clause deliberations
South Durban Community Environmental Alliance	Concerns about the offences, similar to the above	See comments above
South African Catholic Bishops’ Conference	Concerns about offences and penalties	See comments above

(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) other than in accordance with the provisions of the Protected Disclosures Act, 2000 (Act No. 26 of 2000), or any other legislation that provides for the lawful disclosure of information, unlawfully furnishes, disseminates or publishes in any manner whatsoever information relating to the 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 section 24(8) or 25(8);
(f) unlawfully damages, endangers, disrupts a critical infrastructure or threatens the safety or security at a critical infrastructure or part thereof;
(g) unlawfully threatens to damage critical infrastructure;
(h) enters or gains access to critical infrastructure, for an unlawful purpose;
(i) enters or gains access to critical infrastructure, in contravention of the notice contemplated in section 24(8) or 25(8); 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 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) knowingly 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 section 24(1); or
(c) refuses or fails to take the steps specified in the notice contemplated in section 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 notice issued in terms of section 11(3) or 11(4), is guilty of an offence and is liable on conviction to a fine or imprisonment for a period not exceeding 12 months or to both a fine and such 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 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.

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 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—
(i) the administration, provisioning and functioning of security service providers at a critical infrastructure;
(ii) the standards and content of any training course 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 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.
(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*.

Comments by	Comments	Response
Research Unit	Consider whether 3 months is sufficient time to allow for regulations	The comment is noted. The intention is to put the Bill into operation after regulations are finalised. This will submission that the Act and regulations must be put into operation simultaneously.
	Notification to parliament or concurrence?	Regulations are normally seen as the measures for operational implementation and it is rare that regulations must be approved by Parliament. However, the Committee will guide the Department in that regard.
NERSA	Clause 27(1)(b) – now 27(1)(a) – factors should be contained in the Bill and not regulations	These factors are dynamic and may develop or change over time. The matter is of an implementation and functional nature and should be contained in regulations.

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.

Comments by	Comments	Response
Research Unit	Does SSA have capacity to perform vetting?	It is respectfully submitted that this is a SSA legislated function and that legislation cannot be shaped to accommodate capacity issues
	There should be a time limit for declaration	The 60 month period is applicable to the National Commissioner. It is submitted that a period of 60 months will be sufficient to perform the functions.
	Is the vetting process free of charge?	It is understood that ther are no costs involved if vetting is required by law
South African Catholic Bishops' Conference	List of "deemed" CIs must be published	Comment is noted for implementation

COSTS

Comments by	Comments	Response: Projections at the time of drafting
Research Unit	Budget of the CIP is under pressure and costs may be prohibitive.	**Board members** Compensation 459099.1685 Accommodation 228340 Meals 35280 Travel 196000 Provisional Cost 918719.1685 **SAS & NKP 2014/2015** Compensation 57000000 Goods and Services 4900000 Provincial & Local 14500 Capital 930000 Total 62844500 **SAS & NKP 2015/2016** Compensation 69780000 Goods and Services 7096000 Provincial & Local 18080 Capital 2967200 Total 79861280