PARLIAMENT
OF THE REPUBLIC OF SOUTH AFRICA

RESEARCH UNIT

PO Box 15 Cape Town 8000 Republic of South Africa
Tel: 27 (21) 403 8273 Fax: 27 (21) 403 8118
www.parliament.gov.za

17 August 2018

PORTFOLIO COMMITTEE ON POLICE AMENDMENTS TO THE CRITICAL INFRASTRUCTURE PROTECTION BILL [B22B – 2017]

TABLE OF CONTENTS

1. INTRODUCTION

In terms of the current National Key Points Act 102 of 1980 (dating back to the Apartheid era) South Africa has approximately 200 national key points or national key point complexes, which *inter alia* prohibits them *being photographed* for national security reasons, and carries severe penalties for those infringing these provisions. The National Key Points Act gives the Minister wide discretion in deciding what a national key point is; and he or she can declare any place as a national key point if he or she deems it (i) necessary, expedient or "in the public interest", or "so important" that its loss, disruption or immobilisation may prejudice the country; (ii) necessary or expedient for the "safety of the country" to declare a place a key point or (iii) considers it in the "public interest" to declare a place a key point.

In 2012, the Right2Know Campaign (R2K), a civil society initiative, approached the South Gauteng High Court to order the release of the list of national key points held by the police as the Minister had refused to release the list when requested under the Promotion of Access to Information Act of 2000 (PAIA). The reasons for the refusal was ostensibly that revealing their identities and locations would draw unnecessary attention to national key points and pose a threat to national security.

The High Court judgment handed down in December 2014, disagreed that disclosure of the national key points posed a national security threat and ordered the release of the list. The Court suggested the review of the National Key Points Act to allow for the disclosure of national key points in certain instances in the interest of public interest, having due consideration for the Constitutional rights of freedom of movement, expression and access to information.[1] Knowledge of national key points would safeguard persons from unwittingly committing an offence by omission or by doing certain actions prohibited in respect of national key points.

[1] *Right2Know Campaign and Another v Minister of Police and Another* (2013/32512) [2014] ZAGPJHC 343; [2015] 1 All SA 367 (GJ) (3 December 2014)

2. CRITICAL INFRASTRUCTURE PROTECTION BILL, 2017 INTRODUCED TO REPLACE OUTDATED NATIONAL KEY POINTS ACT

The Minister of Police introduced the Critical Infrastructure Protection Bill [B22 – 2017] in 2017 to repeal the outdated National Key Points Act 102 of 1980, and corresponding laws of the former TBCV states (Transkei, Bophuthatswana, Ciskei and Venda) and replace them with constitutionally compliant legislation. An important objective of the Bill is the expansion of the definition of critical infrastructure, formerly known as national key points, with an emphasis on safeguarding and "preventative security measures".

The Bill makes the Minister of Police responsible for the administration of the Act, which will apply to all critical infrastructure, except those under the control of the Department of Defence. Existing national key points are deemed as critical infrastructure and will be subject to review within five years of the Act coming into effect.[2] In line with the Constitutional Court's decision in the R2K case mentioned above, the Bill provides that the Minister of Police must, by notice in the Gazette and within 60 days after the Act comes into operation; publish a list containing the names of national key points or national key point complexes deemed to be critical infrastructure.

3. PUBLIC SUBMISSIONS RECEIVED AND PORTFOLIO COMMITTEE PROCESS

- The Portfolio Committee on Police held public hearings in January and February 2018, and considered oral presentations from various commentators in its deliberations on the Bill.
- The Portfolio Committee received a number of submissions from *inter alia* Nedlac (organised business), Cosatu, South African Catholic Bishops Conference, the Right to Know (R2K), the Reserve Bank and the Western Cape government.
- ***General concerns raised by commentators included the (a) potential for abuse of the Minister's power to declare any infrastructure as critical infrastructure, (b) extremely wide discretion as to what conditions may be imposed on individuals entering critical infrastructure", and (c) need to ensure that the Critical Infrastructure Council (established by the Bill to review applications for the declaration of infrastructure as critical infrastructure) is adequately funded and independent.***
- ***Photography of critical infrastructure was raised as a major concern and it was proposed that restrictions in this regard should apply to sensitive security measures and not those in plain sight, like turnstiles and metal detectors.***
- ***Commentators slated the lengthy imprisonment sentences in the Bill as "draconian" and warned that this could put pressure on magistrates to impose lengthy sentences for minor offences. In particular, they questioned the validity of a 30-year prison sentence, which was more than a "life sentence" that require a maximum of 25 years to be served to qualify for parole.***
- The original bill referred to, but did not define, "**national security**". The amended Bill simply states in Clause 1 that ''national security'' has the same meaning ascribed to it in section 198 of the Constitution".[3]

[2] Clause 30(8).

[3] Constitution of the Republic of South Africa, 1996

- Section 198 of the Constitution does not define "national security" *per se*, but rather sets out the **governing principles in respect of national security**, as follows:

> "(a) National security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life.
>
> (b) The resolve to live in peace and harmony precludes any South African citizen from participating in armed conflict, nationally or internationally, except as provided for in terms of the Constitution or national legislation.
>
> (c) National security must be pursued in compliance with the law, including international law.
>
> (d) National security is subject to the authority of Parliament and the national executive."

- In response to the question why the ambit of the Bill does not apply to infrastructure under the control of the Department of Defence, the Civilian Secretariat for Police Services (CSPS) stated that the exclusion in clause 3(2) are based on sections 104(4) and 104(9) of the Defence Act 42 of 2002, which set out penalties and offences.
- In terms of s104(4) of the Defence Act, a person "who obstructs, damages, removes, destroys or commits any other act on or against any property used for protecting or safeguarding the Republic, is guilty of an offence and liable on conviction to a fine or imprisonment for a period not exceeding 25 years".
- Section 104(9) of the Defence Act provides that "[a]ny person who falsely represents himself or herself to be a member or an employee of the Defence Force or Department, is guilty of an offence and liable on conviction to a fine or imprisonment for a period not exceeding five years."
- Because members of the security forces have unhindered access to critical infrastructure, Clause 13 of the amended Bill now requires that they "must produce proof of his or her appointment and identity to the satisfaction of the person in control of the critical infrastructure or an appointed security manager".
- The Portfolio Committee also inserted a provision that security personnel who render security services at a critical infrastructure must comply with standards and training courses determined and recognised by the Private Security Regulatory Authority (PSIRA).[4]

- **AmaBhungane submitted a legal opinion by Dr Milo and Adv. Winks that Clause 26 could be subject to Constitutional challenge. They also proposed the insertion of a public interest defence in respect of the offences listed in Clause 26** (in terms of the original Clause 26 it was an offence to for example, photograph security measures that are visible to the public).
- The PC on Police consequently delayed the adoption of the Bill pending the obtainment of a second legal opinion from Senior Counsel on the Constitutionality of especially Clause 26.
- **The PC considered the legal opinion by Adv. Wim Trengrove, SC on 3 July 2018**.
- **Trengrove, SC confirmed that the provisions of Clause 26 would not pass constitutional muster, but was of the view that a public interest defence clause (recommended by Dr Milo and Adv. Winks) would not cure such unconstitutionality.**

[4] Clause 27

- **According to Trengrove, SC an amendment of the definition of "security measures" to limit them to those not clearly visible to the public eye, would (a) make Clause 26 Constitutionally compliant and (b) remove the need for a public interest defence**.
- **Trengrove, SC also proposed that the Bill prescribe objective criteria for the determination of critical infrastructure to guide the Minister's determination of critical infrastructure in order to prevent unfettered discretion in this regard**.
- The Department presented the redrafted clauses in line with the legal opinion to the PC on 14 August 2018. **The PC accepted the proposals and adopted the whole Bill with amendments on 14 August 2018**. Its report on the Bill was published on 15 August 2018 in the ATC.
- The Critical Infrastructure Protection Bill [B22B – 2017] must now be passed by the National Assembly and transmitted to the National Council of Provinces for consideration.
- As the Bill is tagged as a Section 75 Bill not affecting provinces, the Select Committee can *propose amendments* for consideration by the Portfolio Committee.

The following sections set out the objectives and the main provisions of the Bill.

4. OBJECTIVES OF THE CRITICAL INFRASTRUCTURE PROTECTION BILL [B22B – 2017]

The Bill seeks to:

- **Repeal** the outdated apartheid-era National Key Points Act 102 of 1980, and corresponding TBCV legislation;
- **Secure** critical infrastructure (a) against threats[5] and (b) by creating an environment that promotes "public safety, public confidence and basic public services…through the implementation of measures aimed at securing critical infrastructures; and…by mitigating risks to critical infrastructures through assessment of vulnerabilities and the implementation of appropriate measures";
- **Ensure** (a) the confidentiality of information pertaining to critical infrastructure, subject to PAIA and other legislation, (b) that objective criteria are developed for the identification, declaration and protection of critical infrastructure; (c) public-private cooperation in the identification and protection of critical infrastructure and (d) critical infrastructure complies with regulatory measures aimed at securing them against threats;
- **Promote** cooperation and a shared responsibility between role-players and a multi-disciplinary approach to deal with critical infrastructure protection; and
- **Enhance** the collective capacity of role-players responsible for the protection of critical infrastructure to reduce potential security risks.

5. OVERVIEW OF MAIN PROVISIONS OF CRITICAL INFRASTRUCTURE PROTECTION BILL

5.1 Important Definitions: Clause 1

- **Threat:** Includes any action or omission of a criminal, terrorist or accidental nature, which may potentially cause damage, harm or loss to critical infrastructure or interfere with the

[5] See 5.1 for definition of "threats".

ability or availability of critical infrastructure to deliver basic public services, and may involve any natural hazard, which is likely to increase the vulnerability of critical infrastructure to such action or omission.

- **Basic Public Service:** Includes a public or private sector service provided 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.

- **Infrastructure:** Any building, centre, establishment, facility, installation, pipeline, premises or systems needed for the functioning of society, the Government or enterprises of the Republic, including any transport, electricity and water networks, but excludes information infrastructure contemplated in cybersecurity legislation.

- **Critical infrastructure:** Any infrastructure declared as such in terms of the Bill, including a **critical infrastructure complex** (more than one critical infrastructure **grouped together** for practical or administrative reasons).

5.2 Responsibilities of designated persons in the Bill

- **Minister of Police**: Overall responsibility for the administration of the Act and reports to Parliament on the work of the Critical Infrastructure Council and matters pertaining to the implementation of the Act. Has the power to declare infrastructure as critical infrastructure or critical infrastructure complexes on application by a person in control of an infrastructure or by the National Commissioner (on recommendation from the Critical Infrastructure Council[6]), and issues certificates[7] setting out the premises, category and conditions in this regard. The Minister must consider certain factors, including the sector, strategic importance, risk category, resources available, environment, health, safety and interest of the public or any other infrastructure dependent on the functions and functioning of the critical infrastructure in question.[8] The Minister, in consultation with the Minister of Finance and other affected Ministers, makes a determination regarding the costs flowing from a declaration of critical infrastructure.

- **National Commissioner of Police (functional)**: Administers the Act and advises the Critical Infrastructure Council ("the Council") in consultation with key role players such as the State Security Agency, South African National Defence Force and other affected stakeholders in the private sector. The Commissioner must *inter alia* (a) develop guidelines, standards, structures and mechanisms for government and other cooperation (the Bill provides for the establishment of *ad hoc* or standing committees (including a cyber-response committee) to assist the Commissioner in this regard); (b) establish procedures and directives, (c) consider applications, (d) provide risk assessments, (e) make recommendations on applications, to the Council (f) ensure designated persons from SAPS (from the rank of warrant officer and upwards) and government carry out inspections to verify information pertaining to infrastructure and ensure compliance with a notice of declaration of critical infrastructure; and (g) compile and submit quarterly reports to the Council.

---

[6] Clause 20

[7] Clause 22

[8] Clause 17

- **Critical Infrastructure Council:** Comprises 16 members representing various government departments and five private persons with relevant expertise, who must be South African citizens and with top security clearance certificates by the State Security Agency. It advises the Minister on guidelines and standards; receive and consider applications, reports and assessments of security risks, make recommendations on applications; evaluates, monitors and reviews the implementation of policy, legislation and reports and establishes procedures regarding critical infrastructure. The Council reports to Minister annually on its activities.

- **Civilian Secretariat for Police Services (CSPS):** Chairs and provide secretarial services to the Critical Infrastructure Council. It funds the Council from the CSPS budget.

- **Person in control of critical infrastructure:** The owner or the person (including the Head of a Government department and relevant employees) who has lawful right to occupy, possess, control or is responsible for the operation or administration of such critical infrastructure.

- **Security Manager**: The person responsible for monitoring and implementing security of a critical infrastructure on behalf of the owner or the person in control of such infrastructure. The Bill provides that no person may enter upon any critical infrastructure without the permission of a security manager, or the security personnel under his or her direction. Such persons may be (a) requested to provide specific information and (b) searched. The restriction on entry of critical infrastructure does not, however, apply to members of the security services in terms of s199 of the Constitution[9], namely members of the police, defence force and intelligence officers.

5.3 Delegation of powers and functions[10]

The Bill allows the Minister to delegate certain powers to the National Commissioner, who in turn can delegate any function conferred upon him or her to any police official with a minimum rank of level 13 (senior management)[11]. The Portfolio Committee also amended the Bill to require that police officials designated as inspectors must have appropriate security clearance certificates[12] and must identify themselves and show such clearance certificates to the person in charge of critical infrastructure when conducting inspections.

6. MAIN PORTFOLIO COMMITTEE AMENDMENTS

The following table sets out selected comments/concerns raised in respect of specific clauses in the Bill, and the extent to which the CSPS responses and amendments address them.

SELECTED CONCERNS RAISED ON ORIGINAL BILL [B22 – 2017]			CSPS RESPONSES / AMENDED BILL [B22B – 2017] VERSION
1.	**APCOF**	Definition of "basic public service" is too broad - should expressly exclude e.g.	**Clause 1: not amended**

[9] Constitution of the Republic of South Africa, 1996

[10] Clause 14

[11] South African Police Service (2018). Annual Report 2016/17.

[12] Clause 10

		medical clinics, schools and universities.	
2.	**APCOF**	"Critical infrastructure" is not defined.	**Clause 1:** "**critical infrastructure"** means any infrastructure which is declared as such in terms of section 20(4) and includes a critical infrastructure complex where required by the context; ''**critical infrastructure complex''** means more than one critical infrastructure grouped together for practical or administrative reasons, which is determined as such in terms of section 16(3)[13]
3.	**Western Cape Government**	Exclude "information infrastructure" - Bill must only deal with physical infrastructure.	**Clause 1: ''infrastructure''** means any building, centre, establishment, facility, installation, pipeline, premises or systems needed for the functioning of society, the Government or enterprises of the Republic, and includes any transport network or network for the delivery of electricity or water **but excludes any information infrastructure as contemplated in any legislation on cybersecurity.**
4.		No definition for "national security".	**Clause 1:** ''national security'' has the meaning ascribed to it in section 198 of the Constitution"[14].
5.	**Reserve Bank**	• Include Reserve Bank as a "person in control of a critical infrastructure" (Clause 1). • Insert a new clause 12(9): "Notwithstanding the provisions of subsections (1) and (2), the National Commissioner must in exercising any function contemplated under section 9(2) and (3) consult with the South African Reserve Bank in matters that may affect financial stability".	**CSPS response:** It would be impractical to declare the vast private banking infrastructure (including ATMs) as critical infrastructure. The Reserve Bank is an organ of state as defined in section 239 of the Constitution.
6.	**R2K**	Risk categories not clearly defined.	• **Clause 1** defines a risk category as that contemplated in section 20(4)(b). ***The latter, however, only refers to classification of critical infrastructure as low-, medium- or high risk categories***. • **Clause 27(1)(i)** states that the Minister must make Regulations regarding "guidelines and standards to **establish** a system to categorise critical infrastructure or parts thereof in a low-risk, medium-risk or high-risk category, as contemplated in section 20(4)(b)".
7.	**SA Catholic Bishops Conference**	Why is infrastructure under the control of the Department of Defence excluded from ambit of the Bill?	**CSPS response:** The exclusion in Clause 3(2) is based on Sections 104(4) and 104(9) of the Defence Act 42 of 2002.

[13] Clause 16(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".

[14]

8.	**SA Catholic Bishops Conference; Western Cape Government**	Strengthen selection criteria for members of Critical Infrastructure Council.	**Clause 4(3)(c) was amended:** The five members appointed to the Critical Infrastructure Council by the Minister must now also include member(s) from civil society.
9.	**Nedlac**	Vetting of private-sector members of the Critical Infrastructure Council intrusive.	**Clause 4(6)(d): CSPS response:** It would not be advisable to forego the vetting process.
10.	**Portfolio Committee**	Oversight role of Parliament in appointment of Critical Infrastructure Council needed strengthening; and simplify appointment process.	***The Portfolio Committee redrafted Clause 4 to strengthen the role of Parliament, viz.:*** • The Minister must request the National Assembly (NA) to submit to him a list of names of persons from the private sector and civil society for appointment to the Critical Infrastructure Council. • The Speaker must refer the matter to the relevant Committee which must publish a notice in the Government Gazette and at least two national newspapers inviting interested parties and members of the public to nominate persons; compile a shortlist of persons who must be vetted by the State Security Agency; conduct interviews with eligible candidates; submit a final list of 10 recommended candidates to the NA. • The NA then submits the list of 10 candidates, together with their resumes, for the Minister to appoint of five of them to the Critical Infrastructure Council.
11.	**Portfolio Committee**	Four-year term should be five-year term.	**Clause 4(9)** now provides for the appointment of Members of the Critical Infrastructure Council for a period not exceeding five years.
12.	**National Energy Regulator of South Africa (NERSA)**	The Critical Infrastructure Council should have its own budget to enhance independence.	**Clause 6: CSPS response**: • A dedicated budget will require permanent staff and concomitant expenses. • Deriving the Critical Infrastructure Council budget from the CSPS budget will be the most economical. • The only costs involved will be for the payment of private sector / civil society members. • **Preliminary costing**: Column1 | Column2 **Board members** Compensation 459099.1685 Accommodation 228340 Meals 35280 Travel 196000 Provisional Cost 918719.1685
13.	**Western Cape Government**	The Critical Infrastructure Council must also approve the policies, in addition to	**Clause 7(1)(b)(iii) was amended to provide that the functions of the Critical Infrastructure Council**

		considering guidelines and standards developed by the National Commissioner.	**include the approval of guidelines** regarding "policies, protocols and standards regarding any matter necessary to achieve the purpose of this Act".
14.	**SA Catholic Bishops Conference**	• Inspection of private property declared as critical infrastructure should only be done with the owner's consent. • Inspectors may issue compliance notice without a magistrate. • Make provision for possible negative consequences of declaration.	**Clause 11: CSPS response**: • The requirement to obtain consent could potentially hamper access to inspectors for routine inspections (not invasive and does not amount to a search). • The Portfolio Committee inserted a **new sub-clause 11(10) requiring that an inspector**, "prior to exercising any power in terms of this Chapter, must identify himself or herself to the person in control or the security manager of the critical infrastructure in question and **must produce the certificate issued by the National Commissioner referred to in section 10(2)"- i.e. that he or she is a designated inspector in terms of the Act**.
15.	**R2K**	Avoid proliferation of critical infrastructure.	**Risk categories** (to be dealt with in Regulations) will limit the number of critical infrastructures requiring extreme security measures.
16.	**Gautrain Management Corporation**	Regarding **Public Private Partnership property** in respect of which a "Concession Agreement or similar arrangement exists, only the head of an organ of state that owns, is in control of, or is responsible for the administration of the infrastructure may lodge such an application" to have it declared as critical infrastructure.	The provision was already covered in Clause 1 under **definition of Person in control of critical infrastructure** which includes "(b) the person who, by virtue of...any other right acquired from any other person whether **by way of a public-private partnership or similar agreement**...occupies, possesses, is in control of, or is responsible for the operation or administration of such a critical infrastructure".
17.	**Western Cape Government**	No time-frames provided for making written representations to the National Commissioner after notification of application to declare infrastructure as critical infrastructure.	**Clause 19 was amended** to afford the relevant head of a Government Department affected by an application for declaration as critical infrastructure "an opportunity to submit written representations within 60 days on any aspect relating to the intended application of the National Commissioner". (Clause 19(4)(b))
18.	**Banking Association South Africa (BASA)**	**Clause 20 –** A declaration by the Minister of a financial institution as critical infrastructure should be done in consultation with the Financial Stability Committee as defined in the Financial Sector Regulation Act 9 of 2017.	**This proposal was not taken up. CSPS response:** Ostensibly, banks do not comply with the requirements in clause 16(2)(a) for infrastructure to be declared critical infrastructure as "the loss, damage, unlawful disruption or immobilisation of such infrastructure [would not] 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").
19.	**R2K**	Transparency requires knowledge of the identity of critical infrastructure.	**CSPS response: Clause 21(5) and (6)** adequately provides for standards - the National Commissioner must enter the declaration or termination of

			declaration of critical infrastructure into a prescribed register that is accessible to the public, as well as by notice in the Gazette.
20.	**Gautrain Management Corporation**	**Include a new clause 24(9)**: "*To the extent that a Concession Agreement, or similar arrangement, exists in respect of critical infrastructure, the Concessionaire, or its equivalent, shall be responsible for the discharge of the responsibilities prescribed in this section and section 25".*	**Proposal not responded to / included.** **A new Clause 24(9) was inserted as follows:** "A person to whom functions are assigned in terms of this Chapter must exercise such powers and perform such duties subject to the Constitution and with due regard to the fundamental rights of every person."
21.	**COSATU; R2K**	Persons should be notified before they enter critical infrastructure that they can be searched. Searches are open to abuse and violation of rights. The clause must expressly prohibit searches requiring workers to be stripped naked or have their orifices probed.	**Clause 25(6) was amended to place greater emphasis on the dignity and privacy of persons being searched, viz.:** (6)*(a)* Any search of a person's body…must be carried out by a person of the same gender, or …with strict regard to the right to privacy and dignity and must be in accordance with the provisions of this section and any other prescribed directive. *(b)* When conducting a search of a person's body…the manner of search is restricted to a pat-down of the person's outer garments to establish whether that person is in possession or control of a prohibited or dangerous object. *(c)* A search of a person's body...may only be performed if— (i) a reasonable suspicion exists that such a person did not declare a dangerous or prohibited object in his or her possession or under his or her control; and (ii) the manner of or place where the search is performed does not infringe upon the privacy and dignity of the person to be searched. *(d)* Before a security manager or security personnel under the direction of the security manager may search a person referred to in paragraph *(c)*(i), the person to be searched must be— (i) informed of the gender of the person who will conduct the search, the manner of search and the place where the search will be performed; (ii) provided with an opportunity to express a preference regarding the gender of the member of the security personnel who must conduct the search.

22.	**APCOF**	• The Bill potentially criminalises acts of protest, information disclosure and free expression. • Restrictions on disclosure of information could be unconstitutional in terms of Section 35(3) and legislation dealing with whistle-blowers. • Amend Clause 26 to ensure that the disclosure of information about critical infrastructure that does not undermine state security is free from criminal sanction. • Prison terms are excessive and possibly invalid.	**Clause 26: CSPS response:** Offences are divided into three groups or types of offences - Serious offences that will form part of an investigation into terrorism and espionage; offences that require an element of "unlawfulness" and excludes "negligent" acts by a person"; and violations by persons in control, e.g. failure to put up relevant warning notices, etc. Note – these types of offences are not to be confused with the categories of offences listed under Clause (26(1)(a) to (j)), the penalties in respect of which are discussed below. • In the list of violations under Clause 26(1)(a) to (j), the Portfolio Committee reduced the maximum years of imprisonment to three years, with the option of a fine (previously 30 years and 20 years respectively). • The Committee further included categories of offences that the court may consider and the recommended period of imprisonment or fine if there was intention to cause damage or substantial harm, namely: • Low-risk, impose a fine or imprisonment for a period not exceeding three years or both a fine and imprisonment; • Medium-risk, impose a fine or imprisonment for a period not exceeding five years, or both a fine and imprisonment; or • High-risk, impose a fine or imprisonment for a period not exceeding seven years, or both a fine and imprisonment. Prison sentences increase substantially if the offence "in fact caused damage, substantial harm or loss of property": • Low-risk, impose a fine or imprisonment for a period not exceeding 10 years or both a fine and imprisonment; • Medium-risk, impose a fine or imprisonment for a period not exceeding 15 years, or both a fine and imprisonment; or • High-risk, impose a fine or imprisonment for a period not exceeding 20 years, or both a fine and imprisonment. *Clause 26(4) provides for mitigating factors if the person charged with furnishing, disseminating or publishing information relating to security measures applicable at or in respect of a critical*

			infrastructure; recording or photographing photos or videos thereof or caused such photos or videos to be made in contravention of a notice, if "the security measures at the critical infrastructure in question were not clearly visible to the public or in the public domain".
23.	**DR. MILO & ADV. WINKS (O.B.O AMABUNGANE)**	• Clause 26, especially sub-clause (1) (a), (b) and (c), will not survive a constitutional challenge. • Insert a public interest defence in relation to clause 26 (1)(a) - (c) offences.	• The PC sought a second legal opinion from Adv. Wim Trengrove, SC on the Constitutionality of Clause 26, which it considered on 3 July 2018.
24.	**ADV. WIM TRENGROVE, SC**	• **What is critical infrastructure?** • **Clause 20(4)(a)** empowers the Minister to declare any infrastructure to be critical. It does not lay down any objective standard the Minister must apply in making the classification and merely requires the Minister to have regard to a confusing array of factors specified in **clauses 16(2), 17 and 20(4).** • The Bill does not prescribe any objective criteria for the determination of critical infrastructure, not does it guide the Minister's determination. • It gives him or her a free hand in the identification of critical infrastructure; and says in effect that critical infrastructure is whatever the Minister says it is. • The offence in **clause 26(1)(c)** is problematic in its interpretation. • The prohibition of the prescribed conduct, only if it is "*unlawfully"* done, is of little value and renders the meaning of the prohibition uncertain. When is a contravention of the prohibition lawful? Or does it give the court an overriding discretion in every case to determine whether a contravention is unlawful? If not, what does it mean? • The phrase "security measures" was too wide, causing the offences to possibly be in conflict with the right to freedom of expression contained in section 16 of the Constitution. • The constitutional issue could be cured if the definition of "security measures," was narrowed down only for purposes of **clause 26(1)(a) and (b)**. A public interest defence is also then	• The proposed **Clause 20** contain the powers of the Minister to declare infrastructure as critical infrastructure which are extracted from the existing clauses 16 (1) and 20, and combined to form a more logical process on its own in one clause. It addresses the concern that the Minister had unfettered powers, which may have been an unforeseen consequence of the previous wording of clauses 16 and 20. • **Clause 26(1)(c) was removed.** • An official may lawfully perform an action referred to in **Clause 26 (1) (a) - (b).** The word "unlawfully" was a drafting convention, and would constitute an element of the offence the prosecution must prove. • **Clauses 26 (1) (a) and (b)** prohibit the unlawful disclosure of information, or the unlawful taking of a picture of the security measures at critical infrastructure. • **A new sub-clause (2) was proposed:** (2) For purposes of subsection (1) (a) and subsection (1) (b), "security measures" means those security measures at critical infrastructure

		unnecessary if the clause was limited to prohibit disclosure of information that was not in the public domain, and the taking of pictures of security measures at critical infrastructure, which were not on public display.	that are not clearly visible to the public or in the public domain. ***The PC also dealt with the following redrafted clauses on 4 July 2018:*** **Clause 16** The clause deals with the power of the Minister to declare any critical infrastructure and determine critical infrastructure complex. Some criteria for declaration were contained in clause 16 (2), while other factors were contained in clause 17. The proposed clause 16 deals only with the requirements for declaration of infrastructure as critical infrastructure, as proposed by Adv Trengrove. **Clause 17** This clause contains factors to be considered in the declaration of critical infrastructure. The proposed clause 17 deals with the application for declaration as critical infrastructure and critical infrastructure complex by persons in control, and contains procedural aspects of clause 18. Relevant factors from clause 17 are now required as part of the application process. **Clause 18** The proposed clause 18 contains the procedure for application for declaration as critical infrastructure and a critical infrastructure complex by the National Commissioner. It replaces original clause 19. **Clause 19** The proposed clause 19 contains consideration of an application for declaration as critical infrastructure by the Critical Infrastructure Council, and its recommendation. It extracts the functions of the Council relating to the application from the existing clause 20, and puts it into a more logical process on its own.
25.	**Nedlac**	The Act and the Regulations must be put into operation simultaneously.	**Clause 27: CSPS response:** The intention is to put the Bill into operation after the Regulations are finalised.

7. SOURCES

Constitution of the Republic of South Africa

Civilian Secretariat for Police Services (2018). Response to Submissions: Portfolio Committee on Police. 6 February 2018.

Critical Infrastructure Protection Bill [22 – 2017]

Critical Infrastructure Protection Bill [22B – 2017]

Defence Act 32 of 2002

National Key Points Act 102 of 1980

Parliament of South Africa (2018). Critical Infrastructure Protection Bill [22A – 2017]. Portfolio Committee Amendments to Critical Infrastructure Protection Bill [B 22—2017]. (As agreed to by the Portfolio Committee on Police) (National Assembly).

PMG (2018). Committees. Police. Available at https://pmg.org.za/committee/86/. Accessed 16 May 2018.

Adv. Wim Trengrove, SC. Opinion for Parliament on the Critical Infrastructure Protection Bill. 11 June 2018.

Van Zyl-Gous, N (2018). Summary of Concerns on the Critical Infrastructure Protection Bill, 2017. Research Unit. Parliament of South Africa.