**Critical Infrastructure Bill**

**[B 22B—2017]**

**Summary of Submissions**

|  |  |  |  |
| --- | --- | --- | --- |
| **ORGANISATION** | **RELEVANT SECTION OF THE BILL** | **MOTIVATION FOR SUBMISSION** | **RECOMMENDED CHANGES** |
| 1. **AmaBhungane** | S 26Any person who unlawfully … furnishes, disseminates or publishes in any manner whatsoever information relating to the security measures applicable at or in respect of a critical infrastructure other than in accordance with the Protected Disclosures Act, 2000 (Act No. 26 of 2000), Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004) or any other Act of Parliament that provides for the lawful disclosure of information …commits an offence and is … liable upon conviction to a fine or to imprisonment for a period not exceeding three years, or to both a fine and imprisonment | Concerned that the Bill in its current form still imposes undue, and potentially unconstitutional limitations to the right of freedom of expression and right to information entrenched in section 16 and 32 of the Constitution.  Our view therefore is that an express public interest defence clause against the criminal sanctions contained at s26 of the Bill must inserted for it to meet constitutional muster. The public domain defence now contained in the Bill is important improvement, but still falls short of an adequate defence. | (1) No person shall be guilty of an offence under section 26(2)(b) to the  extent that the disclosure was in the public interest or was made in the  reasonable belief that it was in the public interest.  (2) For the purposes of this section, a disclosure is in the public interest if:  (a) it reveals wrongdoing that has occurred, is occurring or is likely to  occur, including:  (i) any criminal offence or other contravention of law;  (ii) any danger to public health, safety or the environment;  (iii) any abuse of public office, neglect of public duty, misleading  of the public in the purported performance of public duties or  functions, or misuse, mismanagement or waste of public  resources;  (iv) any miscarriage of justice; or  (v) deliberate concealment of any such wrongdoing; and (b) any reasonably foreseeable risk of harm caused by the disclosure is  outweighed by the need to bring the wrongdoing to the attention  of the person or persons to whom it is disclosed. |
| 1. **BASA (The Banking Association of South Africa)** | Section 17 (4) Where it appears from the application that the infrastructure contemplated in subsection (1) partly consists of, incorporates or houses, any information infrastructure as contemplated in any legislation on cybersecurity, the National Commissioner must follow the procedure contemplated in section 20(4).  **Powers of Minister to declare infrastructure as critical infrastructure**  (4) The Minister must, in consultation with the Cabinet member responsible for State security, determine the procedure that the National Commissioner and the State Security Agency must follow when dealing with an application contemplated in section 17(4).  (5) Where an application contemplated in section 17(4) is referred to the Cabinet member responsible for State security in terms of any legislation on cybersecurity, the Cabinet member responsible for State security must, within 60 days or such further period as agreed upon between the Ministers, decide whether the infrastructure in question, or any part thereof must be dealt with in terms of any legislation on cybersecurity or not, and inform the Minister in writing of the decision.  (6) Where the Cabinet member responsible for State security decides that an application must not be dealt with in terms of legislation on cybersecurity, the Cabinet member responsible for State security must return the application to the Minister, whereafter the application must be dealt with in terms of this Act. | **Sections 17(4) and 20(4) – (6):**   * There is concern that the application of sections 17(4) and 20(4) – (6) of the Bill may be constitutionally questionable on the basis, *inter alia*, that legislation should clearly set out objective criteria for decision making, where administrative discretion is granted to the executive. * Section 17(3) purports to include the head of a government department or head of an organ of state in an application to declare an infrastructure as critical, but for certainty (given that information infrastructure has been specifically excluded from the definition of infrastructure), a similar provision should be set out in section 20(4)-(6), so that the head of a government department or head of an organ of state with functional control over an impacted sector forms part of the decision making process to bring such information infrastructure back into the ambit of the Critical Infrastructure Protection legislation.   **Powers of the Minister**:   * There is a concern that while the Bill gives the Minister the power to declare infrastructure as critical infrastructure, it does not adequately circumscribe the extent, limitations and duties associated with this power. Importantly, the Bill does not define the rights of, and protections for, critical infrastructure controllers and owners in the event of such a declaration by the Minister (especially where such owners or controllers are not government agencies). | BASA recommends that the Bill provides for the following:  • the designation of a function in the Minister’s office that may have access to a critical infrastructure for non-governmental infrastructures;  • the conditions and regularity of the access to a critical non-governmental infrastructures;  • authorisation and identification (certificate of authorisation) of individuals who will have access to a critical non-governmental infrastructure;  • consequences of acting contrary to authorisation;  • the rights of the owner or controller of a critical infrastructure; and  • prohibition on disclosure of information by members of law enforcement/investigator on such critical infrastructures. |
| 1. **SANEF (South African National Editors Forum)**     These submissions are made by the South African National Editors Forum (SANEF), the SOS: Support Public Broadcasting Coalition (SOS) and Media Monitoring Africa (MMA) (collectively, the Group) | *Suggests introduction of new provision.* | SABC has been appointed as a NKP and as a result they have concerns with:   * the State Security Agency (SSA) has been approaching non-security personnel at the SABC and more specifically, editorial staff, that is journalists and/or management personnel and informing them of the necessity of completing a very detailed and invasive security vetting questionnaire, * power is being exercised in a manner that we believe to be an unconstitutional violation of the right to freedom of the press which is a specifically protected aspect of the right to freedom of expression as is provided for in section 16(1)(a) of the Constitution of the Republic of South Africa, 1996 (the Constitution). * The Group requests the NCOP to ensure that specific protection of editorial integrity and freedom of work as a journalist be provided for with regard to the staff of the SABC, other than, of course, in respect of the security staff needed to secure the SABC as a National Key Point or, in due course, a Critical Infrastructure or Critical Infrastructure Complex. | The group suggests the introduction of a new section 24 to be contained in Chapter 3 of the Bill as follows:  “Specific Protections for the SABC as the independent public broadcaster  24. In recognition of the vital role that the SABC, the independent public broadcaster, plays in ensuring that the public has access to a wide range of news and information, nothing in this Act shall require the security vetting, other than of the SABC’s security staff, of the SABC staff, in particular, no journalist or non-security staff member shall be required to disclose any communication undertaken in the course of his or her employment and sources of journalistic information as a result of the SABC being declared critical infrastructure and/or a critical infrastructure complex.” |
|  | **Offences and penalties**  **26.** (1) Any person who unlawfully—  *(a)* furnishes, disseminates or publishes in any manner whatsoever information relating to the security measures applicable at or in respect of a critical infrastructure other than in accordance with the Protected Disclosures Act, 2000 (Act No. 26 of 2000), the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004) or any other Act of Parliament that provides for the lawful disclosure of information;  *(b)* takes or records, or causes to take or record, an analog or digital photographic image, video or film of the security measures at a critical infrastructure;  *(c)* 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;  *(d)* hinders, obstructs or disobeys any person while performing a function or in doing anything required to be done in terms of this Act;  *(e)* enters or gains access to critical infrastructure without the consent of the security manager or person in control of that critical infrastructure;  enters or gains access to critical infrastructure in contravention of the notice contemplated in section 24(8) or 25(8);  *(g)* damages, endangers or disrupts a critical infrastructure or threatens the safety or security at a critical infrastructure or part thereof;  *(h)* threatens to damage critical infrastructure; or  *(i)* colludes with or assists another person in the commission, performance or carrying out of an activity referred to in paragraphs *(a)* to *(h)*, commits an offence and is, subject to subsection (3) and (4), liable on conviction to a fine or to imprisonment for a period not exceeding three years, or to both a fine and imprisonment. | The Bill contains severe penalties for violations in relation to critical infrastructure as provided for in section 26. These range from 20 years imprisonment for tampering with, damaging or destroying critical infrastructure (section 26(4)) to a fine and/or three years imprisonment.   * A penalty of up to 3 years imprisonment is currently provided in section 26(1) for activities that could be described as journalism, namely section 26(1)(a), (b), (e) and (f), which sections prohibit, *inter alia*, publishing information, being at or taking photographs of critical infrastructure. While it is true that these are subject to this being done “unlawfully” – this term is never defined - and we are concerned that this would have a chilling effect on reporting about activities taking place at critical infrastructure sites. * The Group therefore supports the call that the Bill specifically contains a public interest override to ensure, in particular, that the information-disclosure activities contained in what is currently section 26(1) of the Latest Bill would not constitute offenses if the disclosure of information and related activities regarding critical infrastructure would be in the public interest. | It is suggested that a new sub-section (3) be inserted into what is currently section 26 the Bill as follows:  “(3) Notwithstanding the provisions of sections (1)(a), (b), (e) and (f), where a disclosure of information regarding critical infrastructure would reveal evidence of:   1. (a) a substantial contravention of, or failure to comply with, the law; or 2. (b) an imminent and serious public health, safety or environmental risk; and 3. (c) the public interest in the disclosure clearly outweighs the harm in question, the disclosure and related activities falling within those listed in section 26(1)(a), (b), (e) and (f), shall be lawful.” |