queries@ispa.org.za
010 500 1200
www.ispa.org.za
PO Box 518, Noordwyk, 1687

25 January 2024

**Department of State Security**

**Attention: Irene Moetsana-Moeng**

Per email: irenem@ssa.gov.za and HellenMakh@ssa.gov.za

Dear Irene

SUBMISSIONS: DRAFT CYBERSECURITY BILL

1. The Internet Service Providers' Association of South Africa (ISPA) has taken note of the circulation of a draft Cybersecurity Bill 2023 for comment and has set out submissions raised by its members below.

**ISPA's interest in the process**

2. ISPA is aware that this consultation represents an initial engagement in what is likely to be an extended process. The subject matter of the draft Bill is highly technical and complex, while the political and legal terrain underpinning the draft Bill is likely to be contentious.
3. The interest of ISPA members is, however, limited in scope to those aspects of the draft Bill which have the potential to have an impact on electronic communications service providers (ECSPs) and the environment in which they operate.
4. ISPA has an active security working group with substantial collective experience and expertise in cybersecurity as well as constructive relationships with SAPS, the Office for Interception Centres, the Financial Intelligence Centre and the Cybersecurity Hub.
5. ISPA has established an internet sector CSIRT in South Africa.
6. Further, ISPA has actively participated in the development of the Cybercrimes Act (CCA) and the implementation of the Regulation of Interception and Provision of Communication-related Information Act (RICA).
7. Aside from the networks operated by its members, ISPA's INX-ZA division operates multi-site internet exchange points (IXPs) which could conceivably fall within the definitions of critical information infrastructure (CII) or special critical information infrastructure (SCII) set out in the draft Bill.

**Public participation in the development of secondary legislation**

8. ISPA submits that section 53 of the draft Bill should as a default position provide for a public participation process as an element of the development of secondary legislation under the draft Bill.
9. This is particularly the case where industry and entities outside of Government – such as responsible persons in respect of infrastructure which could potentially be designated as CII or SCII or critical database administrators - will be affected.

10. The Department recognises that taking effective cybersecurity measures must be a collective responsibility of Government and industry and that current industry approaches to cybersecurity are significantly more advanced than those adopted by Government.

11. Allowing for a public participation process will serve to strengthen the regulatory framework by allowing Government to leverage industry expertise and facilitate alignment between the approaches adopted.

**Critical databases**

12. ISPA notes that Chapter 6 of the draft Bill is based on and repeals Chapter 9 of the Electronic Communications and Transactions Act 2002 (ECTA).

13. ISPA is not convinced that this carve out of powers to the Minister of Communications and Digital Technologies is necessary or advisable, given that this seems to be based on the approach adopted under ECTA which has never been implemented.

14. The powers to be exercised by the MCDT in respect of critical databases and the Minister of State Security in respect of CII / SCII are based on similar considerations and the current approach appears to risk unnecessary fragmentation in the institutional framework.

15. Further, the relationship between critical databases and CII / SCII and the degree to which these overlap is unclear, and it may be that the legacy provisions relating to critical databases are superfluous given the provisions on CII / SCII. Note that the definition of CII is broad and includes “data”.

16. In support of its submission relating to public participation, ISPA notes that:

    16.1. the regulations contemplated in subsection 20(1)(b);

    16.2. the regulations contemplated in subsection 21(3); and

    16.3. the minimum standards and prohibitions contemplated in subsection 22(1)

    should all be developed after a proper stakeholder engagement process.

**Conclusion**

17. ISPA looks forward to the planned workshop and to deepening its understanding of the draft Cybersecurity Bill throughout the consultation process so that it can provide more detailed submissions.

**Warm regards**

**ISPA**