SUMMARY OF WRITTEN SUBMISSIONS AND RESPONSES THERETO: CYBERCRIMES AND CYBERSECURITY BILL

[B 6 - 2017]

PART B

(CHAPTERS 10 TO 13)

11. CHAPTER 10: STRUCTURES TO DEAL WITH CYBERSECURITY			
11.1 General	11.1.1 Cell C, Telkom and Vodacom - page 28 (paragraph 2.11.2) 11.1.2 Mr Heyink - page 5 (paragraphs 25 to 27)	11.1.1 The Chapter is in general supported. 11.1.2 Unlike frameworks that have been developed in other countries relating to cybercrime, where cooperation between the private and public sectors is seen as key to cybersecurity, the Bill takes an authoritarian approach to cybersecurity. Chapter 11 of the Bill must facilitate public private partnerships which despite being addressed in the National Cybersecurity Policy Framework (the NCFP) are absent from the Bill. Most critical information infrastructure is owned and operated by the public sector. The document entitled the "Minimum Information Security Standard" (MISS) still regulates information security in government, despite it not having been amended since 1996. This is out-dated and must be replaced with a more inclusive approach. However, the approach to cybersecurity must be more	11.1.1 Noted 11.1.2 The NCPF deals with public-private partnerships relating to cybersecurity and it is submitted that it is not necessary to provide for this in the Bill. Chapter 10 mainly deals with the establishment of the overseeing body that will implement the NCPF and aims to place obligations on Departments to acquire the necessary capacity to deal with their mandate to implement the NCPF. Partnerships in essence mean that there must be a consensual basis of cooperation and the coercive basis of legislative obligations that must be adhered to is

		creative than what is contemplated in MISS and used by the State Security Agency as a benchmark within government.	not necessary.
	11.1.3 Mr Heyink - pages 5 and 6 (paragraphs 28 to 35)	11.1.3 Information security or cybersecurity is closely linked to the protection of personal information. The Bill does not take the status of privacy and protection of personal information into account as it undoubtedly should. Although the Information Regulator has now been appointed and the global acceptance that good privacy law, properly implemented and monitored by an independent regulator, provides a balance against overbroad security laws, the operative portions of the Bill have not yet been proclaimed to commence. Cybersecurity frameworks established in democracies are characterised by the balance provided by data protection or privacy laws. The AU Convention on Cybersecurity and Personal Data Protection, which informed some of the drafting of the Bill, deals with both issues and emphasises the importance of data protection. The importance of privacy and the powers of the Information Regulator have not been recognised in the Bill.	11.1.3 The protection of personal information is a sub-division of data protection. The building blocks for cybersecurity were referred to in paragraph 1.25, and the aim of these principles is to ensure the confidentiality, integrity and availability of computer systems. It is submitted that the Bill, deals with the general principles of cybersecurity. The protection of personal information is provided for in the Protection of Personal Information Act (the POPIA) and it is not necessary to specifically refer in other law to aspects that are already comprehensively dealt with in the POPIA. The Bill, if considered in conjunction with the POPIA, caters for the objectives of the AU Convention that specifically differentiates between protection of personal information and cybercrimes. The commentator does not take into account that the AU Convention in Chapter II deals with the protection of personal information and then separately under Chapter III deals with matters relating to cybersecurity

			and cybercrime. The approach which Government has taken is therefore in line with the AU Convention as well as the approach that was taken by most other countries in the world. The protection of personal information and also privacy are facilitated in the Bill by offences, special measures to investigate and seize, international co-operation, obligations on entities to report certain cybercrimes, capacity that must be develop to ensure that the Republic come to terms with cybercrime, information sharing and protection of the most critical information infrastructures. It will be fallacious to argue that the Bill does not take the status of privacy and protection of personal information into account.
	11.1.4 Cell C, Telkom and Vodacom - page 28 (paragraph 2.11.1)	11.1.4 There is no clarity as to which organ of State ultimately holds supreme authority to ensure that these entities all operate and interact seamlessly and that the overall objectives of the Bill are achieved.	11.1.4 The coordinating role to ensure implementation of the measures provided for in the Bill is assigned to the Cyber Response Committee as is provided for in clause 53. The CRC consists of the Heads of representative Departments as is defined in clause 53(8). The CRC is chaired by the SSA and the Cabinet member responsible for State Security is accountable to Parliament regarding the functioning of

			the CRC. Furthermore, in terms of the NCPF, various Departments need to ensure that measures are taken to implement South Africa's cybersecurity initiative. The Ministers of these Departments are accountable to Parliament regarding the implementation of those initiatives. Other provisions of Chapter 10 place obligations on certain Departments to implement measures and the Ministers of these Departments account to Parliament.
	11.1.5 Professor Von Solms University of Johannesburg	11.1.5 There is a massive shortage of ICT professionals which are required to address cybersecurity, internationally and locally. The Bill does not take this skill shortage into account. The Bill aims to establish at least three CSIRTs, namely the 24/7, Government CSIRT and the Cyber Hub. Extensive experience and technical expertise are required to man a CSIRT. It is submitted that South Africa does not have the capacity to man three CSIRTs and this may further lead to the dilution of any available capacity and the three structures will not function adequately. The massive skill shortage in South Africa on this terrain will adversely affect the implementation of the Bill. It is proposed that: The structures should be merged into a single structure and all available skills, which would have been deployed in the 3 structures, should be consolidated. This single structure should then provide services to all constituents.	11.1.5 * The comments are noted. The reason for not having one structure is to cater for the different constitutional mandates of the departments. The approach and technical expertise that needs to be acquired to address their objectives substantially differs and a one-size-fits-all approach cannot be used to address these different objectives. For example, the obligations to secure infrastructures against cyber attacks substantially differ from the skill requirements to investigate cybercrimes. * Clause 54 imposes obligations on different Departments to obtain the required capacity in order to come to

		* A national cybersecurity capacity program on national level should be implemented immediately to produce more skills. * In time, when more skills become available, progressively split/divide the one national CSIRT structure into more as required. * The establishment of a National Cyber Coordinator, as was previously suggested was not taken into account and is a serious deficiency in the national Cyber Strategy of South Africa.	terms with their obligations imposed on them in terms of the Bill. * The CRC has a general obligation to ensure the implementation of the NCPF as well as the Bill. The CRC therefore fulfils the obligation of a coordinating body.
	11.1.6 SABRIC - pages 2 and 3	11.1.6 The establishment of the proposed structures in the public and private sector may focus attention on skills development. The successful implementation of the Bill rests on the development of the required skills which should be fast tracked. A suggestion is made that special training programs be established to deal with capacity building.	11.1.6 Agree.
11.2 Clause 53: Establishment, composition and functions of the Cyber Response	11.2.1 Media Monitoring - page 13 (paragraphs 30, 31 and 32)	11.2.1 A concern is raised regarding the Cabinet Member responsible for State Security is responsible for the oversight of the Cyber Response Committee. According to the representation the role of the Cabinet member for State security is questionable in light of the general focus of the Bill. It is suggested that the	11.2.1 As pointed out under paragraph 11.1.4, the CRC consists of Heads of various Departments that have different constitutional mandates. The Director-General: State Security is the chairperson and responsible to ensure

Committee		oversight function should be allocated to the Cabinet member responsible for the administration of justice and that the Director-General: Justice and Constitutional Development should be the Chairperson of the CRC. The submissions are motivated with reference to the fact that the Department of Justice and Constitutional Development is not directly involved in matters that is addressed in the Bill and would therefore be impartial.	that the CRC fulfils its function is assigned to it in terms of the Bill. It is submitted that the CRC cannot therefore be regarded as being under the control of the SSA.
	11.2.2 Media Monitoring - page 13, 14 (paragraph 30) and page 15 (paragraphs 33 to 37)	11.2.2 The composition of the CRC is criticised due to the fact that persons outside Government is not represented on the CRC. It is suggested that the CRC must be structured similar to the Judicial Services Commission. According to the representation: * The CRC may act as the interdepartmental steering committee. * The large number of Departments and representatives may restrict the effective functioning of the CRC in emergency situations and suggestions are made to limit the number of persons. * The following additional category of persons should be included as members of the committee: - Representatives from opposition parties represented in the National Assembly; - two teachers of law, or members of the attorneys' or advocates' profession, with knowledge of cybersecurity-related laws who are approved by the Chairperson of the CRC following a public call for nominations; - two technical experts in cybersecurity who are approved by the Chairperson of the CRC following a	11.2.2 This concern is noted. Paragraph 6 of the NCPF defines the role of the Cyber Hub as is envisaged in clause 54(4) of the Bill as as follows: * The NCPF has identified the need to ensure appropriate consultation between the JCPS cluster departments, the private sector and civil society regarding cybersecurity matters. To that end the NCPF promotes coordination and consultation between the JCPS cluster departments, the private sector and civil society regarding cybersecurity matters through the establishment of a Cybersecurity Hub within the DTPS. * To enhance interaction, consultations and promote a coordinating role regarding engagements with the private sector and civil society, the Cybersecurity Hub will, according to the NCPF, have the responsibility, inter alia, to coordinate general cybersecurity

		public call for nominations; and - two members of civil society organisations working on cybersecurity policy who are approved by the Chairperson of the CRC following a public call for nominations.	activities, in consultation with Cyber Response Committee as well as including identifying stakeholders and developing public-private relationships and collaborating with any sector Computer Security Incident Response Teams that may be established. Public participation in the CRC through the Cybersecurity Hub is therefore ensured.
	11.2.3 Western Cape - page 3 of Annexure to letter	11.2.3 Provision should be made for provincial representatives on the Cyber Response Committee.	11.2.3 It is submitted that telecommunications does not fall within the ambits of Schedule 4 or 5 of the Constitution that deals with functional areas of concurrent national and provincial legislative competence and exclusive provincial legislative competence, respectively. The aim of the CRC is to deal with matters relating to ICTs that falls within the domain of exclusive national legislative competence. However, Chapter 3 of the Constitution needs to be taken into account where matters are dealt with that may infringe on the competency of a province and in such circumstances it will be necessary to include representatives of provinces in meetings of the CRC. It may be prudent to specifically amend clause 53(8) to

			ensure provincial and local government inclusion in the activities of the CRC, when necessary. See amendment proposed under paragraph 11.2.4. .
	11.2.4 Minister of Finance - paragraph (c)	11.2.4 Clause 53 provides among others that the Cyber Response Committee includes the National Treasury, the South African reserve Bank and the South African Revenue Services. Although any other department or public entity may be requested to assist the CRC, it is submitted that the word "public entity" may be limited to public entities as listed in Schedules 2 and 3 of the Public Finance Management Act, 1999. It is proposed, in order to allow for the participation of the Prudential Authority to be established in terms of the Financial Sector Regulation Act in the CRC that the phrase "other department or public entity" be substituted for the phrase "any other organ of the state" as defined in section 239 of the Constitution.	11.2.4 The Department agrees. Proposed amendment: Substitution for subparagraph (xiv) of the following paragraph: "(xiv) any **[other Department or public entity]** "organ of state" as defined in section 239 of the Constitution which is requested, in writing, by the Chairperson of the Cyber Response Committee to assist the Committee."
	11.2.5 TBCSA - page 3 (Item 5)	11.2.5 The private sector in the form of Business Against Crime as well a South African Banking Risk Information Centre (SABRIC), should be included since they have information, expertise and technology which the other institutions may not have.	11.2.5 See paragraph 11.2.4, above.
	11.2.6 SAHRC - page 8 (paragraph 3.8)	11.2.6 The CRC consist of state actors and it is recommended that Chapter 9 Institutions, experts in the field of cybersecurity and civil society should also be included in this decision making structure.	11.2.6 See paragraph 11.2.4, above.

	11.2.7 Information Regulator - page 5; IM Governance - page 4 (paragraph 9)	11.2.7 The Information Regulator should also be included in the CRC.	11.2.7 The powers of the Information Regulator are restricted to the ambit of the POPIA. The protection of personal information, like all other data is important. However, the Information Regulator should not be included in a decision making structure within Government that is mandated to implement measures to deal with cybersecurity as it plays a crucial oversight role. The participation of the Information Regulator in such initiatives may create an adverse perception regarding the independence of the Information Regulator.
	11.2.8 Freedom of Religion - paragraph 8.1	11.2.8 The CRC reports to the Joint Standing Committee on Intelligence that is not accessible to the public. The public can further not participate in the proceedings of the CRC that has extensive powers to regulate the Internet.	11.2.8 Not all reports that are submitted to the Joint Standing Committee on Intelligence are closed documents. Various reports of the designated RICA judge were made available in the spirit of transparency and accountability.
11.3 Clause 55: Establishment of Nodal points and private sector computer security incident response teams	11.3.1 Cell C, Telkom and Vodacom - page 28 (paragraph 2.11.2)	11.3.1 The costs involved in the establishment of nodal points and the obligations of the nodal points are unclear. It is proposed that there should be a cost and impact assessment before implementation of the clause.	11.3.1 Nodal Points are essential for a cybersecure South Africa. Nodal Points do not imply that service providers must establish CSIRTs to deal with cyber threats. Nodal Points imply that a sector, for instance the mobile service providers, must bring into operation a

			contact point for the mobile cellular sector to impart information of, or receive information of cyber threats, which must be made known to other sector participants or the Cyber Hub (see clause 55(3)). In many sectors there is already information sharing of cyber threats and technical solutions that can be implemented to address such threats. It is submitted that cost implications would be minimal.
	11.3.2 Credit Bureau Association - paragraph 2.5 (comments based on a previous version of the Bill)	11.3.2 The Bill places onerous and costly obligations on the private sector to establish CSIRTs.	11.3.2 The Bill does not specifically provide that the private sector must establish CSIRTs. There is however an obligation to establish Nodal Points, which have a limited cost implication as pointed out in paragraph 11.3.1.
	11.3.3 SABRIC - page 3	11.3.3 Regulations which may be issued to regulate CSIRTs should not be over prescriptive. The proposed structures with information sharing capabilities are necessary in order to enhance cybersecurity.	11.3.3 To establish a CSIRT and the day to day functioning of a CSIRT is expensive. No obligations are imposed on sectors to establish CSIRTs. Clause 55(6) of the Bill provides that the Cabinet member responsible for communications may recognise a CSIRT that has been established for a sector. In order to facilitate the effectiveness of a CSIRT and possible

			full participation of other entities in a sector, regulations may be made to regulate the effectiveness of a CSIRT.
11.4 Clause 56: Information sharing	11.4.1 Cell C, Telkom and Vodacom - pages 28 and 29 (paragraph 2.11.3)	11.4.1 A consultation process with all interested parties must take place in respect of the regulations that will be issued to regulate information sharing. Exchange of information should only take place in circles of trust where it can be verified that information is protected, used appropriately, proportionate to the threat and reciprocated.	11.4.1 A full public consultation process will take place on the regulations. The exchange of information will, as a matter of fact, be kept confidential and appropriate confidentiality provisions will be included in the regulations.
	11.4.2 Information Regulator - page 5	11.4.2 The regulations could possibly impact on the mandate of the Information Regulator and the clause should be amended to specifically include the Information Regulator.	11.4.2 This is dealt with above.
	1.4.3 SAHRC - pages 8 to 9 (paragraph 3.8)	11.4.3 Noting the fact that personal and other information may be shared, appropriate safeguards should be put in place. The Information Regulator and other entities should also have a say in this aspect.	11.4.3 Information sharing is an essential building block in cybersecurity. Various countries provide for information sharing to deal with cyber threats. Information sharing is to ensure that other entities are timeously warned of a threat and to enable them to mitigate the threat. The UK, USA and

			other countries also provide for information sharing to achieve the aforementioned objectives. The regulations must among others address topics such as: * Restriction of information that can be distributed; * purpose for which it may be used; * confidentiality; * quality and integrity of data that is distributed; * transparency, etc. In most instances, for purposes of information sharing, it is not necessary to identify the data with a person. The main objective is to bring cyber threats to the attention of other entities that need it to protect themselves or their clients. The drafting of regulations will entail a process consultation in order to obtain the views of various persons and entities that have an interest in the subject matter.
	11.4.4 SABRIC - page 3	11.4.4 Information sharing is absolutely essential for cybersecurity. Information sharing between the various structures in Government and the private sector is supported.	11.4.4 Noted. Information sharing is an essential building block for cybersecurity. The Cyber Hub performs an essential role to ensure the cyber safety of citizens. This information may be used to warn citizens of cyber threats and measures that can be

			implemented to guard against such threats. Since the Chapter 10 provides for the establishment of Nodal Points in sectors that must report to the Cyber Hub who in turn must inform the public and other structures that need to be established in terms of this Chapter, comprehensive information sharing will take place to cater for the needs of the citizens, businesses in different sectors and Government alike.
	11.4.5 Freedom of Religion - paragraph 8.2	11.4.5 Regulations in terms of clause 56 may be used to withhold information from the public and civil societies.	11.4.5 The Department disagrees. The primary aim of these regulations is to restrict the information that may be shared in order to protect the right to privacy.
12. CHAPTER 11: CRITICAL INFORMATION INFRASTRUCTURE PROTECTION			
12.1 General	12.1.1 Cell C, Telkom and Vodacom - page 31 (paragraphs 2.12.13 and 2.12.14)	12.1.1 Standards for protection of critical information infrastructures should be aligned with international best practices. Standards such as the National Institute of Standards and Technology (NIST) Cyber Security framework can be considered. The revision of prescribed standards of protection of critical information infrastructures are welcomed and must be maintained in order to ensure that best practices continue to prevail.	12.1.1 The Department agrees.
	12.1.2 Banking	12.1.2 Reference is made to section 76(1)(*d*) and (*e*) of	12.1.2 Clause 57(3)(*h*) and (5)(*f*) of the

	Association SA - page 5	the Financial Sector Regulation Act (the FSRA) relating to cooperation and collaboration between financial sector regulators and the South African Reserve Bank (section 76(1)(*d*)(vii) and (*e*)), data collection measures (section 76(1)(*d*)(vii), and the establishing and using of common or shared data bases and other facilities (section 76(1)(*e*), and it is recommended by BASA that the financial sector regulators and the South African Reserve Bank should take the provisions of clauses 57 and 58 in this Bill into account when applying section 76 of the FSRA in order to ensure that consistency is maintained between the provisions of the Bill and the FSRA. Furthermore, there should be consistency between the standards to be issued in terms of section 108(i) of the FSRA and clauses 57 and 58 of the Bill.	Bill provides for an extensive consultation process in the declaration of critical information infrastructure where a financial institution is involved. The imposition of measures to deal with the protection of critical infrastructures in terms of a direction in terms of clause 57(4) must take place in consultation with the financial sector regulators. It is submitted that these measures will ensure that sections 76 and 108(i) of the FSRA and the provisions of this Chapter of the Bill are aligned.
	12.1.3 Zoelpha Carr - pages 1 to 3	12.1.3 The use of biometric information as a security tool is discussed and the following questions are asked: (a) Does the Bill adequately deal with the protection of biometric servers and databases as critical information infrastructures?	12.1.3 (a) Biometric information is behavioural or physiological characteristics that are used to determine or verify identity. Finger or retina scanning is a commonly used biometric verifier. If this form of data is stored within an information infrastructure that will fall within the ambit of clause 57(2) of the Bill that demarcates the factors that need to be taken into account to declare such information infrastructure a critical information infrastructure, this category of data will be protected. The various offences in Chapter 2 of the Bill aim to

			protect the integrity and availability of data and persons who contravene these provisions are guilty of offences.
		(b) How does the Bill deal with oversight by the State Security Agency in the implementation of information security standards by the private sector to ensure the protection of biometric information in critical information infrastructures?	(b) The information security standards that are required to be implemented are regulated by the directive that the Cabinet member responsible for State security must issue in terms of clause 57(4) of the Bill. Clause 58 of the Bill ensures oversight in that critical information infrastructures must be audited to ensure compliance with the standards that are imposed on them by means of the section 57(4)-directive.
	12.1.4 STRATE	12.1.4 Certain information infrastructures that may be declared critical information infrastructures are, in terms of other legislation subject to equivalent or higher information maintenance standards than those required by Chapter 11 of the Bill. Reference is made to the Financial Markets Act, 2012 (Act 19 of 2012) and regulatory measures issued by the Financial Service Board, that requires the implementation of security measures and back-up procedures to ensure the integrity of records, business continuity plans and disaster recovery plans and ancillary procedures for protection of the infrastructure. These infrastructures must also be audited regarding measures that were implemented to ensure protection of the infrastructure and on site inspections are requirements. In this regard	12.1.4 See paragraph 12.1.2, above. It is submitted that the consultation requirement will ensure alignment of measures to be implemented in respect of protection of critical information infrastructures.

		it is submitted that the Bill does not deal with this duplication. Two options are recommended, namely – * that the measures do not apply to market infrastructure as defined in section 1 of the Financial Markets Act; or * that an exemption be granted to such infrastructures by the Cabinet member responsible for State security.	
	12.1.5 Credit Bureau Association - paragraph 2.1	12.1.5 The Credit Bureau Association points out that credit bureaus are regulated by the National Credit Act, 2005, and when the POPIA is implemented additional measures will be imposed on its members to deal with the protection of personal information. The Credit Bureau Association has a concern that its members may be declared critical information infrastructure in terms of clause 57 of the Bill and they propose that credit bureaus be exempted from this Chapter of the Bill.	12.1.5 Clause 57(2) of the Bill provides for the following circumstances under which an information infrastructure may be declared as a critical information infrastructure, namely, that the loss, damage, disruption or immobilisation may – * substantially prejudice the security, the defence, law enforcement or international relations of the Republic; * substantially prejudice the health or safety of the public; * cause a major interference with or disruption of, an essential service; * cause any major economic loss; * cause destabilisation of the economy of the Republic; or * create a major public emergency situation. Taking the above factors into account, consideration will be given as to whether information infrastructure will fall into the category of critical information infrastructure. The mere fact

			that an infrastructure need to comply with other legislation does not entitle that infrastructure from exemption. The aim of this Chapter is to ensure that adequate measures are imposed to ensure the results as is contemplated in clause 57(4), which relates to the integrity and availability of data and systems which is not covered in terms of the POPIA or the National Credit Act.
	12.1.6 ODAC - pages 7 to 9	12.1.6 This Chapter should be considered as a National Key Points Act for electronic communications systems. The National Key Points Act is a controversial law that is currently being revised. It is pointed out that the Chapter will also apply to Government in the national, provincial and local sphere and it is argued that the Minimum Information Security Standards should be adequate to deal with aspects provided for in this Chapter. The fact that the MISS was not updated since 1996 is criticized. The cost implications for compliance are further discussed. It is proposed that this Chapter should be deferred.	12.1.6 It is correct that the Bill, similar to the National Key Points Act and the Critical Infrastructure Bill that has been introduced in Parliament, aims to protect critical interests of the Republic. The National Key Points Act and the Critical Infrastructure Bill deal with physical structures whilst Chapter 11 of the Bill deals with information infrastructures and data. The objectives of the MISS are to protect classified information in the national interest in both the public and private sphere. The MISS does not deal with the protection of data against vulnerabilities, the management of cybersecurity incidents, data contingency and recovery measures that need to be implemented, and physical or technical security

			measures that are needed to protect information infrastructures, which are dealt with in Chapter 11 of the Bill. The MISS is therefore inadequate to deal with this aspect. The implementation of these measures may have cost implications which are in terms of the Bill placed on the owners of such information infrastructures. The measures are intended to offer a measure of protection against cybercrime and to protect essential information systems.
	12.1.8 SABRIC - pages 2 to 3	12.1.8 The Bill places the initiative to protect critical information infrastructure under Government control only. It is submitted that the public and private sector should work together in this regard. It is pointed out that the private sectors equally has an interest in the protection of critical information infrastructure and have experience in this regard. It is also pointed out that a public private partnership may expedite the implementation of critical information infrastructure protection. It is also proposed that provision should be made for a structure that will facilitate engagements between the public and private sector on cybersecurity.	12.1.8 Noted.
	12.1.9 Information Regulator - page 6	12.1.9 The Information Regulator indicates that there are concerns about the identification and declaration of Critical Information Infrastructures and the power of the	12.1.9 The concerns are noted. It must however be pointed out that the grounds on which an information

		DG: State Security to inspect these structures.	infrastructure can be declared a critical information infrastructure is limited (clause 57(2)). Declaration of information infrastructures is not in the sole discretion of the Cabinet member of state security. Clause 57(1) provides that the identification of critical information infrastructure must take place as a result of a consultative process that involves the CRC which is composed of various Heads of Departments with different mandates. Clause 57(3) provides for an extensive consultation process involving the infrastructure as well as entities that have an interest in these structures. Clause 57(4) provides that the directive imposing obligations to protect the critical infrastructure is limited to measures that are necessary to protect the critical infrastructure and to promote cybersecurity. The SSA is not given any powers to access any information on a critical information infrastructure. In terms of clause 57(5), the directive must be approved by the relevant Ministers which among others includes the Ministers of DTPS and Justice and Constitutional Development. Clause 57(7) makes provision that the declaration of a critical information

			infrastructure as well as the directive can be disputed, first through an administrative process (clause 57(7)(a) to (e)), secondly through a process of arbitration (clause 57(7)(e) to (h)) and thirdly through a court process (clause 57(7)(i) and (j)). The auditing process contemplated in clause 58 does not allow the SSA any access to such a critical information infrastructure. The powers of the Director-General: State Security is limited to evaluation of the result of an audit and to appoint members to evaluate and report on the effectiveness of an audit. It is submitted that the SSA are not given any powers to use this Chapter for purposes of intelligence gathering or to access any information that falls within the protection of the POPIA.
12.2 Clause 57: Protection of critical information infrastructure	12.2.1 IM Consultancy - page 7 12.2.2 IM Consultancy - page 7	12.2.1 A clear definition of critical information infrastructure is necessary. 12.2.2 The power of the Minister of State Security to declare any information infrastructure a critical information infrastructure is too broad and should be	12.2.1 It is submitted that clause 57(2) sufficiently identifies a critical information infrastructure in relation to the results that the damage or disruption may have for the public or Government. 12.2.2 The various safety mechanisms that are built in clause 57 are discussed under paragraph 12.1.19.

		narrowed down.	
	12.2.3 IM Consultancy - page 7	12.2.3 It is submitted that the Chapter need not provide for critical information infrastructures under control of the State, since the State can as a matter of course implement the required protection measures.	12.2.3 There is currently no prescript that regulates the protection of critical information infrastructure that is in the control of the State. This provides for an opportunity to put in place universal prescripts that will regulate this aspect in both the private and public domain.
	12.2.4 IM Consultancy - page 7	12.2.4 Section 52(4) provides that the Minister of State Security must issue directives to regulate the minimum standards, which is a departure from the 2015 version of the Bill, where regulations were required. When regulations are made there must be consultation which is not per se necessary where a directive is issued. Consultation on directives only happens with the relevant cabinet members including those listed in clause 52(5).	12.2.4 See 12.2.5 below regarding consultation on directives. Subordinate legislation must usually undergo a public consultation process and must be published in the *Gazette.* If the information is made publicly available, it could lead to– * identifying the technical specification of the computer system involved; * determining what security measures are in place at a critical infrastructure; * determining what intrusion measure will be effective against the measures that is implemented to secure the infrastructure against unauthorised access; * determining what payload can be delivered to disrupt the infrastructure effectively, etc. It will therefore be bad practice to publish this information

	12.2.5 IM Consultancy - page 7	12.2.5 (a) The Minister is not best-placed to decide on the minimum standards as contemplated in section 52(4)(*a*) to (*g*), especially if the Minister does not consult with industry stakeholders.	12.2.5 (a) Clause 57(5), specifically provides for a comprehensive consultation process in respect of the directive, which does not only involve the information infrastructure in question but also other role-players that may have an interest in the information infrastructure.
		(b) The directives can give the Minister the power to prescribe the implementation of measures in order to establish a backdoor into data held by the critical information infrastructure. It is submitted that the RICA already allows for access to information on critical information infrastructures and that it is not necessary to prescribe additional measures to attain this objective which would in any event be unconstitutional. The Bill must specifically provide who may gain access to critical information infrastructures. The regulations should deal with access control and not who may access.	(b) The powers of the Minister to determine what measures must be implemented in terms of the directive is limited to the aspects contemplated in clause 57(4)(*a*) to (*g*) and the general ambit of the Chapter. It is submitted that the Bill by means of the offences contained in Chapter 2 and Chapter 5 (investigations that is not authorised), prohibits such backdoor access. RICA can also be used to prosecute any person who accesses data without judicial authority. As pointed out in paragraph 12.1.9, the directive can be challenged in terms of clause 57(7).
	12.2.6 IM Consultancy - page 7	12.2.6 Clause 54(4)(e): (a) Security measures are continuously changing. To prescribe minimum security measures is flawed and does not take into account how the different sectors function. It does not take into account the size of the infrastructure and that minimum	12.2.6 * The reason why clause 57 makes provision for the issuing of directives and not to formalise this process through legislation or subordinate legislation is to allow for

		standards differs depending on the size of the infrastructure.	flexibility in the matter. Directives can be changed more rapidly than legislation. This is necessary due to the fact that security measures changes as a result of the fast development of ICTs and cyber threats and measures that are developed to address such threats. The fact that different measures may apply to different sectors due to their size or system under their control was also taken into account and it is submitted that the draft provision caters for this in that different directives may be issued for different sectors.
		(b) Security measures should be left to the infrastructure to decide, or should be determined by the specific industry or sector to which the infrastructure belong. Section 19 of the POPIA also adequately deals with this issue.	(b) The nature and extent of the directive is subject to a consultation process that involves sector regulators and the institutions. These structures and entities with a specific interest in their operation will therefore be important in the formalisation of the directives that are applicable to them. The ambit of section 19 of the POPIA is restricted to personal information that does not include information such as trade secrets, information about scientific research, plans of our weapon systems, specs and programmes of our computerised weapons etc. This has a higher need for protection in most

			instances than personal information. Section 19 also does not impose specific obligations on affected parties to deal with the matters provided for in clause 57(4) of the Bill.
	12.2.7 IM Consultancy - pages 7 and 8	12.2.7 The following criticism is raised against the dispute resolution clause in clause 57(7): (a) The arbiter is appointed at the request of the Minister of State Security and the infrastructure merely has to agree thereto. It is recommended that the arbiter should rather be an independent person to whom both parties agree to.	(a) This clause is invoked when a dispute process has already been lodged against the directive or the declaration, which has not been resolved (meaning that the information infrastructure is not required to accept the declaration or implement the direction). The Minister of the SSA then needs to decide if he or she wants to proceed in the public interest and the obligation is then placed on the Minister to refer the matter for arbitration. The words “to be agreed on” means that there must be consensus on the body that will conduct the arbitration and the process to be followed. The infrastructure may in other words request that person x should be appointed. Both parties therefore have to agree to the person that must be appointed as arbiter.
		(b) The decision of the arbitrator is final and binding. This is a problem because there is no other right of recourse available to the aggrieved CII. The mechanism	(b) Clause 57(7) does not provide or even by implication provide that the decision of the arbitration is final.

		for dealing with disputes should rather be solved in terms of the Bill and not with an arbitrator. According to the commentator, the appeal mechanism, as previously proposed, has been removed from the Bill.	Clause 57(7)(*i*) and (*j*), provides specifically that the decision of the arbiter is subject to appeal or review.
	12.2.8 IM Consultancy - page 8; Liquid Telecom - page 8 (paragraphs 34 and 35)	12.2.8 (a) If a critical infrastructure does not comply with the directives, the Minister of State Security must take the required steps and recover costs from the person. It is unclear why the costs go directly to the Minister and not a fund as was previously proposed. (b) It is further remarked that if the State wants to secure a critical information infrastructure in private hands, the State must contribute to such costs since these measures may have severe financial implications for information infrastructures.	12.2.8 (a) The Minister will incur the costs for implementing the steps which the person failed to implement, in other words funds that were allocated to the budget of the SSA are used to pay for such costs, and the Minister should have the powers to recover such costs. (b) Similar to the declaration of Key Points, the argument is that certain activities must be protected the good of the state as well as its inhabitants. It is submitted that businesses have flourish under the protection of the state and from contributions of the citizens which make their activities profitable and they therefore have a social obligation to ensure that in the interest of society that their services are protected. The Bill also affords additional protection to these structures that are declared critical information infrastructures by providing for elevated sentences that may be imposed if cybercrimes are committed against these information infrastructures. An amendment is also

			effected to the Disaster Management Act, 2002 (Act 57 of 2002), that entitles these critical information infrastructures to disaster funds in case of damage and disruption of their essential functions, which is the flipside of the social contract that the State has obligations to protect.
	12.2.9 Media Monitoring - pages 5, 16 and 17 (paragraphs 38 to 40); Credit Bureau Association - paragraph 2.1.2 (definition of critical information infrastructure is vague)	12.2.9 (a) The broad definition of critical information infrastructure as contemplated in clause 57(2), read with the definition of "information infrastructure" in clause 57(12)(*d*), is criticised.	12.2.9 (a) It is submitted that critical information infrastructure is sufficiently identified in relation to the consequences that may result if the infrastructure is damaged or interfered with (clause 57(2)).
		(b) Information infrastructures belonging to the media, civil society organisations, and non-governmental organisations, journalists, and human rights defenders may be declared critical information infrastructures in terms of clause 57. In the absence of clear legislative guidance on the content of the "directives" that the Minister may issue to owners of a critical information infrastructure in terms of section 57(4), particularly the "classification of data held", this provision may violate information rights, particularly the rights to freedom of expression and privacy.	(b) The provision that defines what must be considered critical information infrastructures will ensure that only essential information infrastructures will be declared critical information infrastructures. The declaration of critical information infrastructures is subject to dispute mechanisms and other safeguards see paragraph 12.1.9, above.
		(c) It is proposed that a more comprehensive definition of critical information infrastructure should be considered	(c) It is submitted that the definition of "critical information infrastructure" is

		and that an independent authority be established to review the declaration of critical information infrastructures, particularly in so far as it relates to the media, civil society organisations, non-governmental organisations, journalists, and human rights defenders.	comprehensive. The process to challenge a declaration or the directives that may be issued is discussed under paragraph 12.1.9, and it is submitted that this is adequate to allay fears of possible undue interference with the rights of the media, civil society organisations, and non-governmental organisations, journalists, and human rights defenders.
	12.2.10 Western Cape - page 3 of Annexure to letter	12.2.10 Clause 57(3)(*b*) provides that the Cabinet member responsible for State security must consult with a Premier before an information infrastructure that relates to or is incidental to a functional area listed in Schedule 4 or 5 of the Constitution or assigned to the province by legislation, is declared a critical information infrastructure. It is proposed that in light of the impact on and the Constitutional mandate of provinces in the listed matters, the consultation requirement should require the concurrence of the Premier.	12.2.10 Agree. Proposed amendment to clause 57(3)(*b*): "consult with and obtain the permission of the Premier of the province concerned;
	12.2.11 , Western Cape - page 3 of Annexure to letter	12.2.11 Clause 57(11) authorises the Cabinet member responsible for State security to implement measures which the person in control of a critical information infrastructure fails to implement. Where a province is involved, section 100 of the Constitution will be applicable, which deals with National Intervention in provincial administration, where a province does not fulfil an executive obligation. It is proposed that the clause should be amended to specifically include a reference to	12.2.11 Agree, but to the extent that the critical information infrastructure falls within the ambit of clause 57(3)(*b*) of the Bill. Proposed amendment to clause 57(11): * Current clause becoming paragraph (*a*); and * the addition of the following paragraph:

		section 100 of the Constitution.	"(*b*) The Cabinet member responsible for State security must, when a provincial government cannot or does not take the steps specified in the notice within the period specified therein, intervene by taking any appropriate steps in accordance with section 100 of the Constitution to ensure fulfilment of that obligation.".
	12.2.12 Cell C, Telkom and Vodacom - pages 29 to 30 (paragraphs 2.12.2.1 to 2.12.6)	12.2.12 The extensive consultation process provided for in this clause before an information infrastructure is declared a critical information infrastructure is commendable. It is, however, submitted that it may be prudent to look at extending the definition to also specifically refer to critical information infrastructure, which includes any critical database and the data housed thereon. Furthermore, the definition must also not lose sight of the processes used to control, enable and protect the data contained in such critical databases.	12.2.12 Noted. It is submitted that the information infrastructure that is to be declared a critical information infrastructure is defined in clause 57(12)(*d*) and means "any data, computer program, computer data storage medium, computer system or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto", which will include a "data base and data housed thereon".
	12.2.13 Cell C, Telkom and Vodacom - page 30 (paragraphs 2.12.7 to 2.12.9); MTN - page 10 (paragraph 3.4.4)	12.2.13 The regulations dealing with dispute resolution should deal with the length of the arbitration process and that implementation of measures in terms of the directive should be suspended pending finalisation of the dispute resolution process.	12.2.13 The suspension of a declaration as contemplated in clause 57(2) as well as the directive as contemplated in clause 57(4) is by implication not of force and effect if it is disputed. It may however provide clarity if a provision is

			inserted that the declaration or directive is suspended if it is disputed. Proposed amendment: * Substitution of clause 57(7)(*a*): "(7) (*a*) A financial institution or a financial sector regulator contemplated in subsection (3)(*h*), or company, entity or person contemplated in subsection (3)(*i*), may dispute— (i) the decision of the Cabinet member responsible for State security**[—** **(i)]**in terms of subsection (3)(h)(iv), or (i)(v); or (ii) any aspect relating to the directives referred to in subsection (4) or any subsequent amendment of the directives."; and * The addition of following paragraph after paragraph (*j*) of clause 57(7): "(*k*) The lodging of a dispute in terms of paragraph (*b*) has the effect that— (i) the decision of the Cabinet member responsible for State security in terms of subsection (3)(*h*)(iv), or (*i*)(v); or (ii) compliance with the directives or any amendment to the directives, as contemplated in subsection (8), is suspended pending finalisation of proceeding contemplated in this

			subsection.”.
	12.2.14 Cell C, Telkom and Vodacom - pages 30 and 31 (paragraphs 2.12.10 to 2.12.11); MTN - page 10 (paragraph 3.4.5)	12.2.14 (a) The issuing of a direction will have cost implications for an electronic communications service provider and the financial impact of the measures that must be implemented must be ascertained before obligations are imposed on the electronic communications service provider.	(a) Financial implications will be considered. See paragraph 12. 2.15, below.
		(b) It must further be kept in mind that many electronic communications service providers do not own the physical network which is used to render a service.	(b) It is foreseen that in some instances where there are shared services that the directive may impose security measures on both the network provider as well as the service provider.
	12.2.15 MTN - page 5 (paragraph 2.6); IM Consultancy - page 5 (paragraph 13) and page 6 (paragraph 14)	12.2.15 Standards for protecting critical information infrastructures should be aligned with global standards such as the National Institute of Standards and Technology Cyber Security framework and clause 57(4) should be amended accordingly.	12.2.15 International standards would, to a large extent, dictate what measures must be implemented by service providers. It is submitted that most service providers that fall within the category of critical information infrastructures would already have

			implemented some of these measures. There is other policy objectives that has an influence on cost of compliance, among others the need to ensure universal coverage and affordable communications. Costly measures will in most instances be passed of to the clients of the information infrastructures and may also restrict expansion of services. It is submitted that other Government policy considerations will ensure that security measures are not disproportional. The approach was considered. However, cybersecurity is in its infancy in South Africa and a concern was raised that full compliance with international standards may be too onerous and costly for information infrastructures.
	12.2.16 MTN - pages 9 to 10	12.2.16 The extensive consultation process provided in the Bill relating to the declaration of critical information infrastructure is supported. However, the following concerns are raised: (a) The Electronic Communications and Transactions Act (the ECTA) defines electronic communications infrastructure as “electronic communications products or systems used to transmit or store critical electronic communications”. The definition of the Bill differs from the ECTA. The definitions of the Bill should be aligned	12.2.16 (a) The Bill aims to do away with the provisions in the Electronic Communications and Transactions Act that deals with critical information infrastructure protection and to that extent the Bill repeals Chapter IX of the ECTA, and the definitions of ''critical data'', ''critical database'' and ''critical database administrator'' in section 1 of the ECTA. Critical information

		with that of the ECTA who also addresses cybersecurity.	infrastructure therefore needs to be interpreted with reference to clause 57(2) of the Bill read with the definition of information infrastructure.
		(b) The Bill seems to aim to regulate critical databases by way of directives. The directives may potentially overhaul existing management approaches and may not necessary be in line with international best standards. MTN makes the following proposals: * The directives must be issued in consultation with person, owner or person in control of critical information infrastructure in order to ensure compliance with industry specific regulation and the non-disclosure of consumer information. (paragraph 3.4.3)	(b) The need to align the protection measures with international standards has been discussed under paragraph 12.2.15, above. The extensive consultation process that must be followed in declaring critical information infrastructures and the directives are dealt with in clauses 57(1) and (3), respectively. It is acknowledged that industry specific regulations are necessary to be considered when formulating such a directive. The aspect of privacy of customer information has already been discussed and it is submitted that the directives cannot infringe on any other obligation that exists on the Statute Book that compels a person or entity to protect the privacy of information. Directives, in a form of subordinate legislation, which are always subject to primary legislation, cannot be used to override other provisions of primary legislation.
		(c) The guidelines to be issued in terms of clause 57(7)	(c) The regulations that must be issued

		should cover the whole arbitration process. (paragraph 3.4.4)	in terms of clause 57(7)(*d*) are restricted to the form and manner in which a dispute must be lodged and matters necessary or incidental to the process for settlement of disputes where this dispute is dealt with in terms of the administrative process contemplated in paragraphs (a) to (*c*) of clause 57(7). Although clause 57(7) does not aim to regulate the arbitration process as contemplated in paragraphs (*e*) to *(i*) of clause 57(7) through regulations, it expressly provides that the the provisions of the Arbitration Act, 1965, apply, with the changes required by the context, to arbitration proceedings.
	12.2.17 Banking Association SA - page 4	12.2.17 Section 57(4)(b) - the storing and archiving of data per directive should be aligned to other laws relating to the same aspect.	12.2.7 Other provisions that relate to the archiving and storage of data will as a matter of course be taken into account in the issuing of the directives in question.
	12.2.18 Banking Association SA - page 4	12.2.18 It is noted that a financial sector regulator is not referred to in sub-clause 57(7)(*a*). It is however referenced in sub-clause 57(7)(*e*) relating to the choice of body for the resolution of the dispute. The financial sector regulator should also be included in clause 57(7)(*a*) to have the option to challenge the decision of the Cabinet member responsible for State security, in so far as it relates to a financial institution as contemplated	12.2.18 Agree. Proposed amendment to clause 57(7)(a): "(a) A financial institution or a financial sector regulator contemplated in subsection (3)(*h*), or company, entity or person contemplated in subsection (3)(i), may dispute the decision of the Cabinet member responsible for State

		in clause 57(3)(*h*) of the Bill.	security—".
	12.2.19 Banking Association SA - page 4	12.2.19 There is no reference to a "financial institution" in sub-clause 57(7)(i) to have the option to appeal the decision of the arbitrator to the High Court. We note this as a concern since the financial institution could be the subject of the dispute in terms of sub-clause (7)(a). The financial institution should therefore have the option to appeal to the High Court.	12.2.19 Clause 57(7)(i) is couched in general terms to provide that a "company, entity or person" may appeal the decision of the arbiter, and it is submitted that it would include a "financial institution". However to clarify this aspect the following amendments is proposed: "(i) The Cabinet member responsible for State security**[, company, entity or person]** or a financial institution or a financial sector regulator contemplated in subsection (3)(*h*), or company, entity or person contemplated in subsection (3)(i) may appeal the decision of the arbitrator to the High Court.".
	12.2.20 Internet Solutions - pages 10 and 11 (paragraph 2.2)	12.2.20 (a) There is no definition of critical information infrastructure and this gives the Minister of State Security a wide discretion to declare any information infrastructure as a critical information infrastructure. It is submitted that critical information infrastructures should only be such structures that is absolutely essential for the State to function.	12.2.20 (a) It is submitted that clause 57(7) read with clause 57(12)(*d*), sufficiently and narrowly defines "critical information infrastructure" to limit the discretion of the Cabinet member responsible for State security to declare critical information infrastructures. These infrastructures cannot be restricted to those that are necessary for the State to function, since the

			primary objective is to secure information infrastructures that are essential to the Republic as a whole.
		(b) The Minister is, in terms of clause 57(4), given wide powers to dictate to critical information infrastructures to implement various measures relating to data protection. It is acknowledged that protection of essential information infrastructure is necessary but it is submitted that protection measures should not be "far reaching and obstructive".	(b) The directives need to ensure that measures are implemented to achieve the objectives referred to in clause 57(4) otherwise critical information infrastructure will not sufficiently be protected. It is submitted that the protection of critical information infrastructures in South Africa needs to be aligned with international standards imposed on such information infrastructures and the Bill is a good starting point to deal with those aspects. It is however not foreseen that disproportional obligations will be imposed on entities to deal with cybersecurity.
		(c) A concern is further raised that a person in control of critical infrastructure may be criminally liable if the prescribed measures cannot on a practical level be implemented. It is further submitted that the criminalisation of non-compliance of a directives which still needs to be drafted is unconstitutional.	(c) The rationality of the directive contemplated in clause 57(4) can be challenged through the mechanisms provided for in clause 57(7). Where a person is charged with a contravention of clause 57(10), that person can raise a defence that the directive is not implementable. The criminalisation of contravention of subordinate legislation still to be drafted is not unconstitutional.

	12.2.21 IM Consultancy - page 4 (paragraph 10)	12.2.21 Section 57(1)(a) should be amended to read as follows: "in consultation with the Cyber Response Committee and the Information Regulator; and"	12.2.21 The Information Regulator is a creature of statute whose powers and function are provided for in section 40 of the POPIA and it is submitted that it should not be extended to a process relating to the identification of critical information infrastructures.
	12.2.22 IM Consultancy - pages 4 to 5 (paragraphs 11 to 12)	12.2.22 (a) The categorization of critical information infrastructure as contemplated in section 57(2), should exclude critical information infrastructure holding or comprising personal information.	12.2.22 (a) According to such an argument the databases of the Departments of Home Affairs and the Deeds Office should be excluded. It is submitted that this recommendation does not take into account the reality of cybersecurity and the need to protect systems that process and store this essential information and the information itself. During a recent incident personal information of between 20 million and 30 million South African citizens were recently leaked due to alleged negligence.
		(b) Clause 57(3)(*i*)(i): The POPIA defines personal information as being the property of the data subjects. It will be impossible to consult with each and every data subject whose personal information is under consideration to be declared critical information infrastructure, but not to do so will undermine the Constitutional rights of South Africa's citizens. Critical	(b) The aim of declaring critical information infrastructures is to ensure that additional protection measures are put in place to deal with cyber vulnerabilities. There is no requirement in the POPIA that persons whose personal information is assigned special

		information infrastructure holding or comprising personal information must therefore be excluded.	protection need to be consulted.
	12.2.25 IM Consultancy - page 6 (paragraph 15)	12.2.25 Clause 57(7)(a): It is submitted that it will be impossible for a person to dispute the decision of the Cabinet member unless represented by the Information Regulator.	12.2.25 See paragraph 12.2.21. The Information Regulator has its own remedies in terms of the POPIA to enforce compliance. The Information Regulator also does not have the powers to represent a wronged party in a dispute.

12.3 Clause 58: Auditing of critical information infrastructures to ensure compliance	12.3.1 Cell C, Telkom and Vodacom - page 31 (paragraph 2.12.12)	12.3.1 The obligation that the owner or person in control of the costs of an audit of a critical information infrastructure should be reviewed.	12.3.1 King III Code brings IT management into the domain of corporate governance (see Chapter 5). This by implication entails that IT Governance need to be audited in order to ensure that IT Governance is effective in an organisation. Where a special measure needs to be implemented in order to deal with critical information infrastructure it is submitted that this will become part of IT Governance and as a guideline auditing of compliance will provide assurances to management of a company that IT governance is effective in their organisation. From this perspective cost of compliance is an integral part of the day to day running of a business and costs related thereto should be borne by the company in question.
	12.3.2 IM	12.3.2 Clause 58(1): Reference to compliance with	12.3.2 See paragraph 12.2.15, above.

	Consultancy - pages 10 to 11 (paragraph 17)	directives should be substituted with compliance with "appropriate and generally accepted international information security standards".	
	12.3.3 IM Consultancy - page 11 (paragraph 18)	12.3.3 Clause 58(3): There is a general shortage of skills and it is submitted that the State Security Agency would probably not be in a position to monitor the adequacy and effectiveness of an audit.	12.3.3 Clause 58(3) provides for capacity constraints in that it also provides that the Director-General: State Security may appoint any other person to monitor the effectiveness of an audit.
	12.3.4 IM Consultancy - page 11 (paragraph 18)	12.3.4 The question is asked whether it is possible to monitor an audit since the result will only be known at the end of an audit.	12.3.4 It is submitted that the actions taken during an audit and the extent of an audit can be monitored.
	12.3.5 IM Consultancy - page 11	12.3.5 Clause 58(5) read with 58(11)(*d*), compels the owner of a information infrastructure to provide the DG: State Security additional information as may be necessary to evaluate the report and the question is asked whether the intention is to allow a backdoor access to the State.	12.3.5 A "backdoor" entails a surreptitious measure, such as a built-in vulnerability in hardware or software that can be used to bypass security measures. The purposes of a request for additional information in clause 58(5) is to acquire additional information to evaluate the audit report, which may for instance entail the specifications of software that is implemented to secure access.
	12.3.6 IM Consultancy - page 12 (paragraph 19)	12.3.6 Clause 58(6)(*b*): The requirement of "to the satisfaction of the DG: State Security" is vague and it must be kept in mind that an independent auditor is	12.3.6 Clause 58(6)(*b*) must be read in conjunction with clause 58(4), which provides that reporting must be done "in

		involved.	the prescribed form and manner" which provides for an objective standard of compliance.
	12.3.7 IM Consultancy - page 12 (paragraph 20)	12.3.7 Clause 58(8) provides that the DG: State security may nominate auditors at its discretion to conduct an audit. However no qualifications or additional requirements seem to be necessary. Certain specific requirements are suggested.	12.3.7 Clause 58(13) specifically provides that "The Cabinet member responsible for State security must, by notice in the *Gazette*, prescribe the persons or the category or class of persons who are competent to be appointed to perform an audit as contemplated in this section". It is submitted that only competent and qualified persons can be appointed.
	12.3.8 IM Consultancy - page 13 (paragraph 21)	12.3.8 Clause 58(11): The scope of the audit is to audit compliance with the clause 57(4) directive, but should be substituted with generally accepted international information security standards.	12.3.8 See paragraph 12.2.15, above.
	12.3.9 IM Consultancy - page 13 (paragraph 22)	12.3.9 Clause 58(11)(*d*): An audit relies on professional judgment and sampling of evidence. Information security is technical and complex. It might be difficult, and it will be very costly "to know something to be true". Except for forensic investigations, auditors express opinions rather than make statements of fact as this is a more cost effective approach.	12.3.9 The clause states "he or she knows to be false or which he or she does not know or believe to be true". The opinion will be covered by the phrase "not ….. believe to be true". In many instances a fact can be stated which is objectively not false, but the person who made the statement in the circumstances does not know it to be true. This phrase is used in various other laws on the Statute Book.

	12.3.10 IM Consultancy - page 13 (paragraph 23); page 14 (paragraph 24)	12.3.10 (a) Clause 58(12): This provision is problematic. It ignores the complexity and highly technical nature of processing and the skills availability within the auditing community. It also ignores the audit time and costs involved. It refers to adequacy and effectiveness of an audit, something very few people can determine. (b) The reason someone "fails to assist or provide technical assistance and support to a person authorized to carry out an audit" could be a lack of skill or confidence to offer assistance. Tremendous damage could happen if incorrect audit test procedures are followed. No one would want to be responsible for doing or saying something they are uncertain about. Therefore, the reason someone doesn't answer an auditors question could be because they don't have an answer. It would not be because they don't want to cooperate.	12.3.10 (a) The provision merely states that a person commits an offence if he or she "hinders, obstructs or improperly attempts to influence any member of the State Security Agency, person or entity to monitor, evaluate and report on the adequacy and effectiveness of an audit". Like all audits, a cyber audit must comply with certain criteria in order to ensure that the audit is adequate and effective. The directive issued in terms of clause 57(4) is the objective standards which must be covered during such an audit and standards were already adopted to deal with such audits (b). The provision in question will only be applicable where there is failure to comply with auditing requirements.
	12.3.11 Freedom of	12.3.11 The auditing mechanism may interfere with	12.3.11Clause 58 was specifically

	Religion - paragraph 8.3	private entities allowing the state to invade privately owned data, devices and networks or infrastructures and may infringe on the constitutional right of privacy.	framed to ensure that the SSA, as controlling entity, does not directly gain access to the systems, data and storage devices of a private entity that has been declared a critical information infrastructure. The following safeguards are in place: * In ordinary course a private independent auditor appointed by the service provider must conduct the audit. * If the infrastructure fails to comply with the auditing requirements, the Director-General must in terms of clause 58(6) take measures to ensure there is compliance and for this purpose must- - appoint a private auditor; - must in writing authorise the audit; - issue a certificate to the auditor which must be handed to the person in control of the infrastructure; It is also a requirement that an auditor appointed in terms of clause 58(6) must be accompanied by a person from the infrastructure during audits.
13. CHAPTER 12: AGREEMENTS WITH FOREIGN STATES			
13. Clause 59: National Executive may	13.1 Cell C, Telkom and Vodacom - page 31 (paragraph 2.13)	13.1 Current procedures for mutual assistance between South Africa and foreign countries in the investigation of cybercrimes do not effectively take into account the	13.1 Noted. The format of the evidence that is required is usually specified in the request and in cyber matters are

enter into agreements		transient nature of electronic evidence and the need to act expeditiously. The resultant effect is that essential evidence is lost. Various other countries enacted legislation to provide for urgent action to preserve information and to provide expeditious assistance to identify the origin of communications involved in a cybercrime. International cooperation in matters dealing with cybercrime is supported. It is assumed that the 24/7 Point of Contact will be commissioned to provide expert guidance should evidence be required in electronic format in a manner that will ensure that such evidence should not be rejected in a court of the Foreign State on grounds of misalignment with local prescripts to preserve and ensure the integrity of such electronic evidence.	aimed at ensuring the integrity of the information. The SOPS in clause 24 will further deal with aspects of evidence collection and preservation. Clause 46(6) of the Bill give the designated judge wide powers to regulate aspects relating to the preservation of evidence as is specified in a request for mutual assistance and appropriate measures may be introduced to ensure that the evidence that is collected will comply with the legal system of the requested country. The fact that a member of the National Prosecuting Authority must assist the 24/7 Point of Contact will further ensure that regard will be had to the requirements of admissibility of evidence in a foreign State.
	13.2 SABRIC - page 3	13.2 International collaboration is absolutely essential to address cybercrimes and cybersecurity and to be informed of new developments. The private sector makes great effort to participate in these collaborations. It is suggested that Government should likewise participate in these international collaborations.	13.2 Noted.
14. CHAPTER 13: GENERAL PROVISIONS			
14.1 Clause 60: National	14.1.1 Cell C, Telkom and Vodacom - page	14.1.1 The obligation on the SAPS to report on these same statistics should be reviewed to ensure accurate	14.1.1 The provisions of clause 60 must be read with 54(2)(*c*) that imposes

Director of Public Prosecutions must keep statistics of prosecutions	32 (paragraph 2.14)	reporting of these crimes and not only on those that actually make it to court. This would also contribute towards accurate reporting on how effective investigations into these types of offences are and what percentage of cases actually results in prosecutions.	obligations on the Minister of Police to report to Parliament on the offences that was reported to the SAPS, cases that resulted in criminal prosecutions and cases where no criminal prosecutions were instituted after a period of 18 months after a case was reported. This will ensure a comprehensive picture of the nature and extent of cybercrime in the Republic as well as the Republic's ability to deal with cybercrimes. Since these offences also relate to critical information infrastructures as contemplated in Chapter 11 of the Act, it will also provide checks and balances to evaluate the effectiveness of protection measures that were implemented to protect the most essential information systems in the Republic.
	14.1.2 All Rise - page 6	14.1.2 The instruction to the Director of Public Prosecutions in section 60 of the Bill, to keep and disclose statistics relating to clauses 16, 17 and 18 is important. Transparency and data insights will play a critical part in addressing cyber abuse worldwide. It is however, pointed out that the number of prosecutions sought will depend on the degree to which cyber abuse is a policing and prosecution priority.	14.1.2 The obligation of the Minister of police to report to Parliament includes the offences that deal with malicious communications. Although the prosecution of malicious communications may not be a police priority, the required statistics of crimes that have been reported will provide insight to the extent of cyber abuse.

			This in turn may give rise to further law reform to curb such abuses.
14.2 Clause 61: Amendment of laws		**Amendments to be effected to the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (**SORMAA)**:**	
	14.2.1 ISPA - paragraph 12	14.2.1 The definition of "electronic communications service provider" to be inserted into SORMAA is aligned with the definition proposed in the body of the Bill. The following definition is proposed: ''electronic communications service provider'' means any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005;".	14.2.1 Agree. Proposed amendment: On page 53 of the Bill to substitute definition of "electronic communications service provider": ''**electronic communications service provider**'' means any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005;".
	14.2.2 ISPA - paragraphs 15 to 24	14.2.2 All other provisions in the Films and Publication Act (the FPA) which have a bearing on child pornography, among others section 27A should be deleted. There is no need for the Films and Publications Board (which is an administrative body), to be involved in the investigation and prosecution of criminal conduct involving child pornography. This aspect was also acknowledged in recommendations done to the Portfolio	14.2.2 Agree. The remark that the offence is currently situated in legislation that deals with an administrative body that is responsible for the classification of films and publications is acknowledged. If sexual offences are comprehensively dealt with in the SORMA it will substantially

		Committee for Communications on 26 September 2016. The following amendments are proposed: - Definition of “child pornography” should be deleted. If the Films and Publications Act need a definition it should refer to the definition as proposed in the Bill. - Section 27A of the Films and Publications Act (that deals with the obligations of ISPs), should be deleted since the amendments proposed by the Bill to the Sexual Offences Act (proposed section 19A(9)) comprehensively deals with that aspect.	facilitate law reform. Section 24B of the FPA is repealed in terms of the Schedule to the Bill (page 47) and the offences are inserted in the SORMA through amendments that are proposed in the Schedule to the Bill (mainly the new proposed clauses 19A, amendments to section 20 of the SORMA and amendments to section 56A of the SORMA) * In terms of its mandate, the Films and Publications Board needs to classify certain material. Section 16(4) provides for the declaration of certain publications (other than films and games) as refused publications if it involves child pornography, which must in terms of section 16(6), be referred to the SAPS. Section 18 deals with the classification of films and provides that the classification of a film and game as a refused publication if it contains child pornography (section 18(3)), which must be handed over to the SAPS (section 18(5)). It is submitted, as was also suggested by the commentator that the definition of child pornography in section 1 of the FPA should be substituted by the definition of child pornography as contemplated in the Bill. The

			Department submits that this is necessary in order to ensure a single and comprehensive definition of child pornography on the statute Book. In order to deal with the proposed amendment the Department will need to consult with the Films and Publications Board. * It is submitted that section 27A of the FPA can be repealed. The proposed section 19A(8) to (9), extensively deals with the obligations of persons and service providers where communications involves child pornography, namely: - Subsection 19A(8), requires the reporting of child pornography to the police and the furnishing of particulars regarding the offence to the police. - Electronic communications service providers that have knowledge of a commission of an offence involving child pornography, must report that knowledge to the police, preserve information of the commission of the offence in question and take all reasonable steps to prevent access to the content. - Non compliance with these obligations is criminalised with penalties that are

			substantially more severe in nature than those prescribed in the current section 27A of the FPA. The only requirement in terms of section 27A of the FPA that is not addressed in this proposed amendment is the requirement that service providers must register with the Films and Publications Board in accordance with regulations that have been issued under the FPA. It is submitted that section 27A of the FPA can be repealed. See proposed amendment below. * Section 30B(1)(*b*) of the FPA, provides for a presumption in respect of accessing of child pornography and provides that if it is proved that access was gained or attempted to be gained to child pornography on a distributed network, including the Internet, by means of the access provided or granted to a registered subscriber or user, it shall be presumed, in the absence of evidence to the contrary which raises reasonable doubt, that such access was gained or attempted to be gained by the registered subscriber or user. The presumption is applicable where a certain condition of fact is proved before the accused are

			saddled with an onus to prove something to the contrary (see S v ZUMANI AND OTHERS 2015 (1) SACR 84 (GJ)) for an application of this burden of proof). However, this is not an evidentiary burden, which would not be unconstitutional, but relates to a factual presumption that is indeed unconstitutional and conviction may follow despite the existence of reasonable doubt. The effect of the presumption is that if it is proven that a service was used to access child pornography it is presumed that the client to which such services was RICA'ed is presumed to be the responsible person that has accessed the child pornography unless he or she adduces evidence to the contrary which raises reasonable doubt. A similar onus was not included in the proposed section 19A, and it is proposed that section 30B(1)(b) of the FPA be repealed: Proposed amendment to Schedule: On page 47 in the third Column of the Schedule to substitute the words "The deletion of section 24B." of the words "The deletion of sections 24B, 27A and [?30B(1)(*b*)?]."

	14.2.3 ISPA - paragraph 25; Liquid Telecom - page 8 (paragraph 38)	14.2.3 The proposed subsection 19A(9)(c), which requires an electronic communications service provider to "take all reasonable steps to prevent access to the child pornography by any person" where it is aware or becomes aware that its "electronic communications system" is being used or is involved in a criminal offence involving child pornography, may need to be reconsidered in light of current investigation practices by law enforcement agencies. Current practices may include that a webpage be kept alive in order to observe communications traffic to the webpage. In order to cater for this need the following amendment is proposed: "(9) An electronic communications service provider that is aware or becomes aware that its electronic communications system is used or involved in the commission of any offence provided for in subsections (1) to (7), must— (a) immediately report the offence to the South African Police Service; (b) preserve any information which may be of assistance to the law enforcement agencies in investigating the offence; and (c) take all reasonable steps to prevent access to the child pornography by any person, <u>unless lawfully instructed to do otherwise by a police official</u>."	14.2.3 This aspect was considered during the drafting of the Bill. There are two views to be considered. There are compelling arguments that the material must under certain circumstances be kept in place to facilitate police investigations. It must be pointed out that the big international successful operations against child harm material were facilitated through the fact that the material was kept in place to monitor who visited the material. On the other hand there is also the right of the victims that must be considered. Once the material is made available on the internet it is copied and redistribute at a rapid rate. Early actions to ensure that the content is blocked will ensure or guard against further harm. The SALRC is currently busy with an investigation relating to aspects of child harm material and it is submitted that the research may provide guidance on this aspect. In the revision of other legislation further attention is given to access of communications technologies for the detection and investigation of crime. A mechanism to deal with this aspect can more appropriately be dealt with in that legislation.