MEMORANDUM ON

The Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations 2023

Submitted to:
The Ministry of Interior and National Administration, State Department for Internal Security and National Administration

By: Kenya ICT Action Network (KICTANet) 8 May 2023

Nine Planet Apartments, Unit E9, Kabarnet Gardens Road, Nairobi, Kenya +254 721 847178 or +254 722 701495 | info@kictanet.or.ke | www.kictanet.or.ke

22 September 2023

The Principal Secretary,
State Department for Internal Security & National Administration,
Ministry of Interior & National Administration,
Harambee House,
P.O. Box 30510-00100,
Nairobi.

Dear Sir,

RE: Memorandum on The Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations 2023

Greetings from KICTANet.

KICTANet is a multistakeholder think tank for ICT policy and regulation. Its guiding philosophy encourages synergies for ICT policy-related activities and initiatives. KICTANet's overall mission is to promote an enabling environment in the ICT sector that is robust, open, accessible, and rights-based. Its strategic objectives during 2022 - 2024 are effective multistakeholder participation; promoting an enabling environment; building capacities and empowered communities; and institutional strengthening.

We submit this memorandum in response to the call for input on The Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations 2023

We have included herein a matrix presentation that captures our concerns, and highlights our proposals on relevant provisions of various Regulations for your review and consideration.

We would be glad to provide further input and perspectives on the Regulations, as and when required. We look forward to your response.

Regards,

Grace Githaiga

Grace Githaiga

For KICTANet

THE COMPUTER MISUSE AND CYBERCRIMES (CRITICAL INFORMATION INFRASTRUCTURE AND CYBERCRIME MANAGEMENT) REGULATIONS, 2023

NAME OF ORGANIZATION/PERSON**: Kenya ICT Action Network - KICTANet**

Submission of Comments on the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Draft Regulations

S/No	**Section of Regulation Proposal**	**Comments**	**Justification**
Preliminary Provisions	Transfer of critical information infrastructure is defined as inclusive of copying or moving a program or data to any computer system, device or storage medium other than that in which it is stored and a number of other inclusive definitions.	Wording and definition is vast especially when read with section 43 (1) could mean a browser of any website of a critical information infrastructure would need written authorization.	Need for more specificity and clarity in its definition

Interpretation:	"owner of critical information infrastructure" includes the operator, authorized person in control or any person in control of critical information infrastructure;	This is significantly problematic because it places ownership on every individual who has any access to change anything – and including potentially junior engineers who simply require access to provision new customers etc. It creates potential significant liability for people without management control.	Specify and make it fully clear to ensure accountability and clear reference on the same.
	"critical information infrastructure" includes critical information infrastructure system or data and national critical information infrastructure;	Consider adapting the definition from the Computer Misuse and Cybercrime Act, 2018.	Need for more clarity. This is the core term used throughout the regulations. Clarity in the definition will make the regulations clearer to anyone reading them.

Objects of the Regulations (3)	(a) provide a framework to monitor, detect and respond to cyber security threats in the cyberspace belonging to Kenya; (i) promote coordination, collaboration, cooperation and shared responsibility amongst stakeholders in the cybersecurity sector including critical infrastructure protection;	Is this sufficient to allow each government related cyber unit to operate efficiently without turf wars on who is more superior? How do you ensure the framework remains adaptable to rapidly evolving cyber threats and ongoing updates and flexibility are not hampered by bureaucratic processes It is too soon to have multiple entities handling cyber security. The status quo should be maintained where the Communications Authority has been at the centre of coordinating multistakeholder efforts aimed at guaranteeing the nations cyber security, “if it ain’t broken, it doesn’t need to be fixed”. NC4 should focus on R&D and situations where gateways are involved.	Consider a dedicated cyber security agency or task force with clear authority and leadership to oversee the regulation's implementation. This entity should be responsible for coordinating efforts among stakeholders. Develop a flexible regulatory framework that can adapt to evolving cyber threats. Regularly update the regulation to reflect emerging risks and technologies, ensuring it remains relevant. Have a comprehensive national cyber security strategy that aligns with the regulation's goals and provides a

			long-term vision for securing cyberspace. Domestic affairs can be handled by Government and Independent agencies such as the Communications Authority.
	(g) approve the identification and designation of critical information infrastructure;	Who will be identifying and is there criteria available for this definition?	Have an extensive and elaborate criteria and identification specifications.

	(l) monitor databases established for purposes of establishing their integrity and confidentiality for the attainment of the objectives of the Act and these Regulations;	Is this realistic? It feels like wanting to control but maybe not. Extensive monitoring may raise concerns about individual privacy and data protection. Striking the right balance between safeguarding data and respecting privacy rights is essential. The vastness of critical information databases across different sectors may render this provision inoperable. It would be more realistic to put in place provisions to measure compliance relating to integrity and confidentiality. Perhaps provide for officers to ensure this within an entity similar to data protection officers. Also, a compliance certificate would suffice, where an entity submits proof of compliance for a certificate of compliance running for a specific period. Where there is proof of noncompliance the same can be revoked.	Rather than attempting to monitor all databases in the country comprehensively which is a massive undertaking, focus on risk-based and sector-specific approaches to cyber security such as having a risk-based cyber security framework. Conduct assessments to ensure monitoring complies with data protection laws and respects privacy rights.

		Several concerns arise regarding data protection. This provision is too wide. Access to critical information infrastructure should be on a need basis i.e. where there is proof of breach, loss or disaster. Otherwise left as is, the provision is prone to abuse leading to surveillance and other data protection risks.	
8 (k)	conduct research on cybersecurity matters envisaged in the Act;	Should we also ask that they produce quarterly reports on what NC4 has undertaken in the quarter, its achievements, and gaps that need addressing? Who are the researchers? Is there a criteria or threshold for them considering there are professional bodies that qualify them and oversee such related matters such as ISACA?	Collaboration with other professional bodies dealing with cyber security to ensure qualified researchers and expert advice on the same. Work with different stakeholders in the cyber security research matters. No need to reinvent the wheel.

10. 2(b)	Have the capability to perform the functions of a Sector Cybersecurity Operation Centre and Critical Information Infrastructure Cybersecurity Operation Centre;	Seems to imply a hierarchy in cybersecurity operation centers – critical infrastructure security operations centers are subservient to sector cyber security operations centers which are in turn subservient to the national cybersecurity operations center. Since the Kenyan national cyber security strategy document makes no reference to sector SOC's this is problematic.	Have a clear outline of the functions of each sector. Need for more clarity.
10 (c)	Co-ordinate any cybersecurity incidents in the Sector Cybersecurity Operations Centre and Critical Information Infrastructure Cybersecurity Operations Centre	Insert the word "response to" after the word "co-ordinate"	Editing for clarity

13. (c)	guide individual behaviour and the security culture of the organisation.	Check this section INCLUDING 13(1) on the words “all persons who use, operate and manage the critical information infrastructure including…. (For example mpesa infrastructure is critical II used by Wananchi and staff).	Need for more clarity

(2)	The cybersecurity awareness programme under paragraph (1) shall include the following topics—	Does it need to be this prescriptive? Does one size fit all? How about emerging cyber threats? Borrowing from ISO Standards, maybe its bast for the programme to be as comprehensive and as prescriptive as possible to avoid assumptions. This provision is definitely too restrictive. Due to the rampant pace technology is advancing at, cybercrimes and threats are equally advancing at the same pace. It is therefore likely that mitigating measures will need to advance as we go on . Therefore such a restrictive provision will not be ideal to cover future threats and awareness programs	Recommendations may include that the committee publishes guidelines on topics for the awareness program. Further, owners of critical information infrastructure can come up with a curriculum. The curriculum should be formulated in collaboration with all relevant stakeholders.

(3)		The owner of critical information infrastructure shall in consultation with the Committee, review the cybersecurity awareness programme at least once every twelve months to ensure that the programme is adequate and that it remains upto-date and relevant.	Is this a role for NC4? How does it review curriculum on infrastructure that it does not own? This is where the roles of NC4 and the regulatory bodies need to be defined clearly. The fact that we are discussing security does not meet NC4 needs to be mentioned everywhere. This is our creme de la creme when we are cornered. NC4 should not be involved in domestic affairs. “Some situations just need our registered security companies to address”.	Conducting a one-size-fits-all review may result in ineffective and impractical recommendations that do not address the unique cyber security needs of each entity. Need for multi-stakeholder approaches. Organizations, especially critical infrastructure providers, operate in various sectors, each with distinct cyber security requirements. Eg; a financial institution faces different threats and compliance obligations compared to a healthcare provider. A uniform review may not consider these differences. Encourage entities to conduct cyber security

			awareness assessments that are tailored to their specific needs, sector, and risk profile. Have sector-specific guidelines and risk-based approaches. We need to separate roles and responsibilities in the ecosystem and encourage self-regulation since most Cyber Security challenges emanate from Social Engineering.

Outsourced capabilities. 14. (1)	An owner of a critical information infrastructure including government-owned critical information infrastructure who intends to outsource any operations shall, in writing, notify the Committee prior to outsourcing…	Are businesses not allowed to make independent decisions? Administrative overheads and delays, potential delays slowing down the outsourcing process. Slow decision-making, risk-aversion, inadvertent security risks, compliance focus, complexity and bureaucracy could potentially limit innovation. The need for rapid action when faced with cyber security risk shall prove difficult with this requirement. This requirement does not make sense. It is usurping roles of Regulatory bodies such as the Communications Authority and Office of the Data Protection Commissioner which Registers Data Controllers. The enactment of such regulations supplants the functions of well-established regulatory authorities and may potentially	This section could be made more flexible or deleted in totality Need for more clarity. The process can become more complex when dealing with multiple layers of government and various critical infrastructure elements, leading to bureaucratic challenges. The requirement for prior notification may not accommodate urgent or rapidly changing situations where immediate outsourcing is necessary to address emerging threats or vulnerabilities.

		cause discord leading to contradiction, ambiguity, and operational inefficacy.	
(2)	The external service provider shall report to the owner of the critical information infrastructure, at least quarterly, notifying on the status of implementation of their obligations under the agreement including notifying on any security incident.	Should this not be a business arrangement between the provider and its contractee? This will become an administrative burden, again. Service providers report periodically to the agencies overseeing their ecosystem such as the Communications Authority.	More flexibility in terms of this regulation especially on why NC4 wants to be involved in businesses that it has no mandate? Have this regulation removed/deleted.
Monthly briefs and compliance reports. 15.		Should include a number (3) for the Director to produce half-yearly reports providing a summary of the briefs and compliance (cyber risks, threats, and incidents) to the public.	Flexibility or expansion of the time-limit as according to the agreements within the organization.

Risk assessment and evaluation of cybersecurity operation centres 18. (4)	The business impact analysis of an organization shall be based on— (a) the potential impacts of business disruptions for each prioritized business function and process including financial, operational, customer, legal and regulatory impacts;--	Is this not too prescriptive? Is the committee not assuming the role of big bro in some areas that are of individual organisations?	Sector-specific approach needed. Need for harmonization of the regulations, laws, agencies to ensure clarity, avoid overlapping and overreaching in terms of functions. NC4 should avoid giving itself unnecessary administrative burden.
19 3 (a)	The following criteria shall guide the classification of a critical information infrastructure – (a) sensitivity of the critical information infrastructure including sensitive (ICT based sector) critical information infrastructure or nonsensitive critical information infrastructure;	The term “sensitivity” may require further elaboration to help the Director in his task of determining what is “sensitive”.	This will guard against arbitrary decision-making and ensure that the framework for designation is clear to both the designator and the designee.

Directives upon designation.	Without prejudice to the generality of paragraph (1) and in addition to the directives specified under section 9(4), the Director may direct the owner critical information infrastructure to— (a) conduct regular risk assessment;	How regular is regular to avoid overreaching?	Checks and Balances are needed on the Director's powers in reference to the Act.
22	Check this one on Failure to implement directives. (c) be under twenty-four hours surveillance by the Director;	Check this one on Failure to implement directives. Specify parameters and limits for 24/7 surveillance by the Director; in line with the Constitution of Kenya and the Data Protection Act of 2019 Striking a balance between digital rights and the penalties or consequences thereof This language sounds …	Review the regulation to accommodate data protection and privacy rights. If not regulated, this may lead to breach of the right to privacy of both institutions and individuals; any surveillance activity should be only in accordance with the Constitution and the provisions of the Data Protection Act, 2019 Oversight to avoid abuse of

			powers bestowed upon him/her
22 (2)		Administrative action and suitable action should be specifically defined.	The Regulation grants the Director powers to impose some penalties outside the scope of the Act; the same must be clear and concise to ensure appropriate checks on the discretionary powers of the Director
Baseline security for critical information on infrastructure 23. 2(d)	Conduct security screening on all personnel handling critical information infrastructure information or data in the designated critical information infrastructure;	Will this be through a certificate of good conduct? What screening is envisaged here?	

24(2) Application by owner Of critical infrastructure	An owner of a critical information infrastructure may, in writing, apply, to the Director for declaration of a system as a critical information infrastructure: (2) The application under paragraph (1) shall— (d) detail the resources available to the owner or person in control of the system to— (e) safeguard the system against destruction, disruption, failure or degradation; (f) repair or replace the system, including the critical infrastructure's equipment, materials or service; or (g) recover the system from any destruction, disruption, failure or degradation; and	Revise the numbering by deleting (e),(f),(g) and inserting the sub numbering (i),(ii),(iii) instead as follows: (d) detail the resources available to the owner or person in control of the system to— (i) safeguard the system against destruction, disruption, failure or degradation; (ii) repair or replace the system, including the critical infrastructure's equipment, materials or service; or (iii) recover the system from any destruction, disruption, failure or degradation;	Editing for purposes of clarity and better understanding.

Application by the owner of critical information infrastructure 26.		Read with Section 4 of the Act. While this regulation sets guidelines, criteria, a structured application process, it does not appear to overreach its functions due to the description in the Act; however, whether this regulation requires a broader regulatory framework that includes other functions such as monitoring, compliance enforcement, penalties, is the question. The Register should be made accessible to the public within the provisions of the Access to Information Act. There is an error in section 26(2) where he is referred to as the Director of a critical information infrastructure	Regulation requires a more comprehensive assessment of the entire legal framework. May not be catered for when read with the act in terms of implementation of the regulation.

27 (1)	states that the owner of a critical information infrastructure shall not make any significant change to the design, configuration, security, or Operations of a critical information infrastructure without prior approval.	"Significant changes" could include anything. The term is very vague and regulation ambiguous such that any different design, system, or network changes are included. This can be impractical given business continuity, cause administrative burden as considering all changes by all critical information infrastructure and due to the ever-evolving technology landscape and emergency situations would not be catered for	Need to redefine what exactly is "Significant changes" What exact designs, configuration, security and operations need approval. Change approval to include notify instead.
27 (3)	the director must consider the application within forty-eight hours and may approve or decline the change.	When emergency changes need to be made that can be substantive to rectify issues, this would impose a burden that could be catastrophic on private entities.	Administrative burden and delay possibilities. Make the regulation more flexible or include notify instead of approvals. Time is of the essence during emergency situations.

30. Obligations of owners	(2) An owner of a critical information infrastructure shall implement effective measures for ensuring— (d) facilitate prompt access to the critical information infrastructure by authorized persons;	Insert the following words after (d) “the facilitation of ” and before the word prompt. Insert the words “in the event of a cybersecurity incident or during auditing for compliance under section 13 of the Act” immediately after the words authorized persons.	For security, and to prevent abuse of this provision, it is important to ensure that access to critical infrastructure is limited to clearly established instances

29 Localisationon of critical information 31. (2)	An owner of a critical information infrastructure who intends to have critical information located outside Kenya, shall apply to the Committee in Form CMCA 3 set out in the Third Schedule.	Check out this entire section and the implications of such clouds as AWS. How can regulations mandating the localization of critical information infrastructure strike a balance between enhancing data sovereignty and potential downsides such as operational complexity and business continuity risks, particularly when organizations utilize global cloud services like AWS? The regulation's primary focus on localizing critical information infrastructure within Kenya may introduce operational complexity, particularly for multinational organizations. Duplicating infrastructure locally could strain resources and create operational challenges. Additionally, centralizing critical data within Kenya	Consider introducing flexibility for multinational organizations to meet localization requirements while ensuring data sovereignty. Encouraging robust business continuity planning and incentivizing investments in redundant systems can mitigate business risks. Support mechanisms and clear guidelines should be established to assist small businesses in complying with these regulations. Stakeholder consultations, periodic reviews, and alignment with global best practices since this regulation could impact innovation, and competitiveness, and deter foreign investment due to operational

		might pose business continuity risks during local disruptions or natural disasters. These stringent localization requirements might deter foreign investment, potentially limiting economic growth opportunities, and smaller enterprises could face resource constraints and disproportionate compliance burdens.	complexities, uncertainty and administrative burden for businesses especially the SMEs
Integration of critical information infrastructure. 35. (1)	An operator of critical information infrastructure shall not integrate or permit the integration of the critical information infrastructure with any other information infrastructure without prior authorization from the Director.	Should this not be a business decision that businesses can make independently? Overreaching its mandate and not envisaged in the Act? According to the Act regulations aim to serve the citizens. Overregulation could affect the business continuity causing financial implications as well as time constraints.	Delete the regulation or review by changing the terms (language).

Transfer of critical information infrastructure. 42.	(1) An owner of a critical information infrastructure shall not, without written authorization of the Director. (2) An owner of a critical information infrastructure who contravenes paragraph (1) commits an offence chargeable under section 20 of the Act.		
42 2 (a)	(2) The owner of critical information infrastructure shall—	Insert the words "ensure that the critical information shall" immediately after the words shall	To ensure clarity of understanding
46 (5)	(5) Upon consideration of the compliance report under paragraph (3), the Committee shall issue recommendations and the Director shall within seven days communicate the recommendations to the Committee.	Delete the word "Committee" at the end of the sub-section and replace it with the following words "owner of the critical information infrastructure"	Editing for clarity

48 (2)	The committee may direct their auditors to carry out a compliance test to ascertain the adequacy and effectiveness of controls.	When we consider that such controls could include things like DDOS prevention mechanisms – this could create a situation where the committee auditing process by the auditors could end up destabilizing systems with their compliance tests.	Auditing reports to be internally submitted ascertaining with some proof the adequacy and effectiveness of the controls Ensure confidentiality, especially with critical private information.
	National Public Key Infrastructure		
National Public Key Infrastructure Components. 50.	(2) The National Public Key Infrastructure Components comprises— (a) the National Bridge Certification Authority; (b) the Sector Bridge Certification Authority; (c) the Root Certification Authorities; (d) the Certification Authority; (e) the Registration Authorities;	Are all these entities going to be established as independent entities? And if so, what are the cost implications? And will report NC4?	

50 (3)	3) Upon consideration of the audit report under paragraph (3), the Committee shall issue recommendations and the Director shall within seven days communicate the recommendations to the	Delete the word "Committee" at the end of the sub-section and replace it with the following words "owner of the critical information infrastructure"	Editing for clarity
Root Certification Authority 54. (1)	A sector shall establish and operate a Root Certification Authority.	The Root Certification Authority needs to be the regulator of the PKI.	
Certification Authority. 55. (1)	A certification authority shall utilise a trustworthy system in performing its services and be either public body or private entities.	What constitutes a trustworthy system?	
PART V	**CYBERSECURITY CAPABILITY AND CAPACITY**		

Cybersecurity capabilities. 58.	(1) Pursuant to section 6 (1) (j) of the Act, the Committee shall formulate a National Cyber Protection Framework. (d) establish a Centre of Excellence which shall be a Directorate of the Committee for purposes innovation, research and development for cybersecurity in Kenya through threat intelligence and analysis including researching and developing methodologies and tools for the identification, classification and characterization of cyber threats;--	Will the framework establish a directorate, which apart from innovation, has similar roles with what is provided for NC4 (earlier in these guidelines). A center of excellence would be a better place for these tasks. It is important not to have duplication of efforts to avoid turf wars.	
Training Guide. 59. (1)	The Committee shall formulate a National Training Guide to provide tools and information required by training institutions on cybersecurity in the Country.	Should this role not be left to the Professional Bodies? Several are doing it such as ISACA.	

Information sharing arrangements. 60.	The Committee shall for purposes of establishing effective practices to protect against cyber threats promote the following information sharing arrangements— (a) establishing trusted networks of information sharing partners including administrative guidelines for identifying trusted organizations; (b) establishing relationships regarding the sharing of cyber security information;		
Self-regulation. 61.	Check section.	Feels jumpy and like an afterthought and someone decided it be fixed there.	
Collaboration with training institutions. 65.	A cyber security or cyber-crime training institution shall collaborate with the Director in the development of cybercrime and cybersecurity modules of training and the mechanisms to assess the	Will this affect the already established ones such as those by ISACA?	

	effectiveness of the cybercrime training.		
70 (1)		allows for anonymous reporting channels for cybersecurity incidents. While this is good – this section directly contradicts section 69(1)(a) of the same regulations.	Need for review of its drafting. Can this be implemented accurately?
THIRD SCHEDULE FORMS FORM CMCA 1 APPLICATION FOR DESIGNATION OF CRITICAL INFORMATION INFRASTRUCTURE	Reasons why you are considering yourself Critical; Can disruption of the system/Service result in— (a) the interruption of a life-sustaining service (b) including the supply of water, health services and (c) energy; (d) an adverse effect on the economy of the Republic; (e) an event that would result in massive casualties or (f) fatalities; (g) failure or substantial disruption of the money (h) the market of the Republic; and (i) adverse and severe effect of the Security of the (j) Republic, including intelligence and military services.	Delete the unnecessary numbers and renumber the reasons correctly: Reasons why you are considering yourself Critical; Can disruption of the system/Service result in— a. the interruption of a life-sustaining service ~~(b)~~ including the supply of water, health services and ~~(c)~~ energy; ~~(d)~~ b. an adverse effect on the economy of the Republic; c. ~~(e)~~ an event that would result in massive casualties or ~~(f)~~ fatalities; d. ~~(g)~~ failure or substantial disruption of the money ~~(h) the~~ market of the Republic; and	Editing for clarity

		~~(i)~~ adverse and severe effect of the Security of the ~~(j)~~ Republic, including intelligence and military services.	
	Systems/Information Infrastructure (p.83) Do you run Systems/Information Infrastructure audits? (a) If yes, How often? (b) Annually (c) Semi-Annually (d) How is it done?	Delete the unnecessary numbers and renumber the options correctly: Do you run Systems/Information Infrastructure audits? (a) If yes, How often? ~~(b)~~ (i) Annually ~~(c)~~ (ii) Semi-Annually ~~(d)~~ (b) How is it done?	Editing for clarity.
FORM CMCA 3 TITLE	APPLICATION FOR CHANGES LOCATION OF A CRITICAL INFORMATION INFRASTRUCTURE	Insert the word “IN” immediately after the word “CHANGES” APPLICATION FOR CHANGES IN LOCATION OF A CRITICAL INFORMATION INFRASTRUCTURE	Editing for clarity.