MINISTRY OF INTERIOR AND NATIONAL ADMINISTRATION

OFFICE OF THE CABINET SECRETARY

REGULATORY IMPACT STATEMENT

ON

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

AUGUST, 2023

This Regulatory Impact Statement (RIA) has been prepared by the Ministry of Interior and National Administration pursuant to sections 6 and 7 of the Statutory Instruments Act (No. 23 of 2013).

Table of Contents

1. BACKGROUND

1.1. Cyberspace is fundamental to the growth of a digital economy. Driven by increased connectivity and the wide adoption of digital technologies, cyberspace has become the new nervous system supporting the functioning and delivery of services to citizens by the Government of Kenya and businesses. However, the wide adoption and the evolving nature of cyberspace has created new risks. These risks expose individuals, businesses, national infrastructure, and government to cyber threats emanating from a wide variety of sources and which manifest themselves in disruptive activities. Their effects carry significant risks to public safety, security of the nation, and stability of the globally linked economy.

1.2. While constant technological advancements may make it extremely difficult to protect or eliminate the vulnerability of all critical infrastructure throughout the country, strategic legislative interventions in security can make it more difficult for attacks to succeed and can lessen the impact of cyber-attacks that may occur. In addition to legislative approach, synergy between the public and the private sector in information sharing is vital to deter, mitigate, or neutralize potential cyber-attacks.

1.3. The Government enacted the Computer Misuse and Cybercrimes Act, No. 5 of 2018 (The Act) to provide for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation, and prosecution of computer and cybercrimes and to facilitate international co-operation in dealing with computer and cybercrime matters.

1.4. The Act establishes the National Computer and Cybercrimes Co-ordination Committee (the Committee) as the institution mandated to *inter alia* provide advise to the Government on security related aspects touching on matters relating to blockchain technology, critical infrastructure, mobile money and trust accounts; advise the National Security Council on computer and cybercrimes; co-ordinate national security organs in matters relating to computer and cybercrimes and to receive and act on reports relating to computer and cybercrimes.

1.5. The implementation of the Act has experienced a number of challenges partly due to emerging trends in technology which pose enormous danger to the integrity of the cyberspace. Further, some of the provisions in the Act are not self-executing, giving rise to the need to review and enact Regulations to facilitate better implementation of the Act.

1.6. For effective implementation of this law, it requires regulations to address increasing cybercrimes, reduce Critical Information Infrastructure (CIIs) exposure to cyber threats, enhance quick investigation and prosecution of offenders, and bolster local and international cooperation. Additionally, the regulations would provide for National Public Key Infrastructure (NPKI) implementation, and management and cybersecurity skills and capacity among other issues.

1.7. Therefore, the Ministry of Interior and National Administration through a Taskforce established in February, 2023 developed the Regulations to give effect to the provisions of the Act and to enable the Committee to discharge its mandate effectively.

1.8. The Regulations, being subsidiary legislations, fall in a category of statutory instruments which are regulated by the Statutory Instruments Act No. 23 of 2013 which provides for the making, scrutiny, publication and operation of statutory instruments.

1.9. In this regard, the Taskforce embarked on a legislative review exercise of the existing Act, with a view to developing Regulations to cater for emerging technology and operationalize the provisions of the Act.

2. REQUIREMENT FOR REGULATORY IMPACT STATEMENT

2.1 A Regulatory Impact Statement (RIA) is an evaluation conducted before a new regulation is introduced. It provides a detailed and systematic appraisal of the potential impact of a new regulation in order to assess whether the regulation is likely to achieve the desired objectives. RIA promotes evidence-based policy-making as new regulations typically lead to numerous impacts that are often difficult to foresee.

2.2 The central purpose of RIA is to ensure that regulation is welfare-enhancing from the societal viewpoint, in that, the benefits will surpass costs. RIA therefore has objectives of improving understanding of the real-world impact of regulatory action, including both the benefits and the costs of action, integrating multiple policy objectives, improving transparency and consultation; and enhancing Governmental accountability. The conduct of RIA involves a range of methods aimed at systematically assessing the negative and positive impacts of proposed and existing regulations.

2.3 The Statutory Instruments Act, No. 23 of 2013 is the legal framework governing the conduct of RIA in Kenya. Sections 6 and 7 require that if a proposed statutory instrument is likely to impose significant costs on the community or a part of the community, the regulation-making authority shall, prior to making the statutory instrument, prepare a regulatory impact statement about the instrument.

2.4 The Act further sets out certain key elements that must be contained in the RIA, namely:

(a) a statement of the objectives of the proposed legislation and the reasons;
(b) a statement explaining the effect of the proposed legislation;
(c) a statement of other practicable means of achieving those objectives, including other regulatory as well as non-regulatory options;
(d) an assessment of the costs and benefits of the proposed statutory rule and of any other practicable means of achieving the same objectives; and
(e) the reasons why the other means are not appropriate.

2.5 This Statement is therefore made to fulfil the requirement of section 6 of the Statutory Instruments Act, 2013.

3. REGULATIONS UNDER THE ACT

3.1 The Act under section 70 delegates Regulation making powers to the Cabinet Secretary to make the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2023, which Regulations are likely to result in the imposition of a significant cost to the community.

3.2 Therefore, an impact assessment of the proposed Regulations has been made in addition to carrying out extensive consultations with stakeholders.

4. PURPOSE, OBJECTS AND OVERVIEW OF PROPOSED REGULATIONS

4.1 The purpose of the proposed Regulations is to *inter alia* provide a framework to monitor, detect and respond to cybersecurity threats in the cyberspace belonging to Kenya; provide for frameworks for establishment and management of Cybersecurity Operations Centres; provide for protection, preservation and management of critical information infrastructure; promote access to, transfer and control of data in any critical information infrastructure; provide for storage and archiving of critical data or information and provide for audit and inspection of national critical information infrastructure.

5. PUBLIC CONSULTATIONS

5.1 Regulations should be developed in an open and transparent fashion, with appropriate procedures for effective and timely input from relevant key stakeholders and the general public. An evaluation of the public consultation process will be necessary to ascertain whether all stakeholders were given an opportunity to present their views which will ameliorate the proposed Regulations.

5.2 With regard to the subsidiary legislation making process, the Statutory Instruments Act requires that the Regulatory Making Authority shall undertake consultations before making statutory instruments (Regulations), and in particular, where the proposed regulations are likely to have a direct or a substantial indirect effect on the community.

5.3 The Statutory Instruments Act, 2013 provides that in determining whether any consultation that was undertaken is appropriate, the Regulation Making Authority shall have regard to all relevant matters, including the extent to which the consultation: drew on the knowledge of persons having expertise in fields relevant to the proposed statutory instrument; and ensured that persons likely to be affected by the proposed statutory instrument had an adequate opportunity to comment on its proposed content.

5.4 The Statutory Instruments Act, 2013 further requires that the persons to be consulted should either directly or by advertisement through representative organizations be invited to make submissions by a specified date, which should not be lesser than 14 days or be invited to participate in public hearings concerning the proposed instrument.

5.5 Pursuant to section 5 of the Statutory Instruments Act, the Ministry has identified the key stakeholders whom it intends to engage for consultations. These include the relevant MDAs, Private Sector Players, Civil Society Organizations, Mainstream Media and General Public. In particular, they include:

(a) Implementers of the proposed Regulations such as operators of the critical infrastructure
(b) Subject Matter Experts.
(c) Other subjects of legislation.
(d) Professional bodies and Academia.

5.6 The Ministry has identified the following nine regions that were earmarked for public participation being geographically representative of the territory of Kenya:

a) Nairobi
b) North Rift
c) South Rift
d) Coast
e) Central
f) Eastern
g) Western
h) Nyanza
i) North Eastern

6. APPROACH AND METHODOLOGIES

6.1 The Ministry intends to undertake the stakeholder consultations engagements in the month of September, 2023. The engagements shall adopt the following methodology:

(a) Publication of the notice calling for public comments on the draft Regulations and Regulatory Impact Statement;
(b) Publication of the draft Regulations together with the draft Regulatory Impact Statement on the Ministry's and the Committee's website and their social media platforms, and in newspapers of nation-wide circulation;
(c) Publication of the Regulatory Impact Statement in the Kenya Gazette;
(d) Write letters and emails to the stakeholders calling for comments on the draft Regulations and Regulatory Impact Statement within a specified time;
(e) Hold physical meetings with the general public and select stakeholders; and
(f) Validation of the draft Regulations incorporating comments received during public consultations and stakeholder engagement.

6.2 In this regard, it is expected that the proposed Regulations and Regulatory Impact Statement shall have undergone an extensive and thorough public participation exercise.

7. IMPACT STATEMENT

7.1 The assessment considered the likely impact of the Regulations on general positive externalities, impact on the fundamental rights of the people, the impact on the economy and the public and private sector, economic impact on individuals and environmental considerations. The summary of the key findings is as follows:

7.1.1 Impact on Fundamental Rights and Freedoms

a) The Regulations are not expected to have a negative impact on fundamental rights of persons or institutions that are subject to it. The Regulations address matters that relate to the Bill of Rights, particularly on the economic, social, and cultural rights under Article 43 of the Constitution. The Regulations do not have a negative impact on the environment or environmental rights of the people.
b) The Regulations do not impair the right to any fair administrative action.
c) The Regulations promote the Right to privacy by transposing the provisions of the Data Protection Act.

7.1.2 Economic Impact on the Private Sector

(a) The Regulations will motivate the legal compliance of all entities specified under the Act and the Regulations.
(b) In relation to reporting and information sharing, it is anticipated that the Regulations will enhance the confidentiality, integrity and availability of critical infrastructure.
(c) In relation to cybersecurity operations centres, it is anticipated that the centres shall promote the detection, monitoring, prohibition, prevention, response and investigation of cyber threats, computer and cybercrimes on Cybersecurity in Kenya.

7.1.3 Impact on the Public Sector

The Regulations shall have a positive impact on the public sector by enhancing coherence and streamlining registration critical infrastructure which will greatly contribute to the integrity of cyberspace and boost public confidence.

7.1.4 Impact on the Constitution and existing legal framework

The draft Regulations are in conformity with the Constitution and in harmony with the Act, legislation in *pari materia* and other existing legislation.

7.1.5 Impact on National Security include:

(a) The regulations are expected to enhance national security measures by providing physical and technical measures for combating cybercrimes in Kenya;
(b) The regulations are expected to increase the ability to detect and manage cybersecurity issues;
(c) The regulations are expected to reduce the number of cybercrimes in Kenya and promote a digital economy;
(d) The regulations are expected to enhance the implementation of CMCA in aspects such as cybercrime investigation and mitigation of cybercrimes; and
(e) The regulations are expected to complement other laws making their implementation more effective.

8. OPTIONS TO REGULATIONS

8.1 This Part considers the question whether the proposed regulation is the best form of Government action. The Statutory Instruments Act requires a regulator to carry out, early in the regulatory process, an informed comparison of a variety of regulatory and non-regulatory policy measures, considering relevant issues such as costs, benefits, distributional effects and administrative requirements. Regulation should be the last resort in realizing policy objectives. There are alternatives, which could come in handy in dealing with certain aspects of social security. The options considered under this part are as follows:

(a) Self-regulation- This is where the industry regulates itself with the minimal role of Government and norms from a regulator. Various actors in the sector set the standards and the need for prescriptive legislation is lessened.
(b) Regulations- Entails coming up with legally binding regulations to implement the law

8.2 The impact assessment involved evaluating the costs and benefits of implementing the regulations based on the policy options outlined above.

8.3 A policy change is considered desirable if it will result in real or potential improvement. This is determined by accumulating its direct and indirect benefits and costs. Based on this philosophy, the two policy options present strengths and weaknesses and therefore may result to ineffective implementation of the Act.

9. EVALUATING THE POLICY OPTIONS IN RELATION

9.1 The impact assessment involved evaluating the costs and benefits of implementing the regulations based on the policy options outlined above.

The impact assessment involved evaluating the costs and benefits of implementing the regulations based on the policy options outlined above. A policy change is a Pareto improvement if public and sector entities are better off, and no one is worse off after the change. Some policy changes benefit some at the cost of others. An exchange could have those who benefit compensate those who suffer, and thus make everyone better off. A policy change is a potential Pareto improvement if an exchange could be made among data controllers or data processors that would make it a Pareto improvement, even if that exchange never occurs.

A policy change is considered desirable if it is a real or potential Pareto improvement. This is determined by accumulating its direct and indirect benefits and costs. Based on this philosophy, the two policy options present strengths and weaknesses and therefore may result to ineffective implementation of the Act. For instance, issuing policy guidelines without regulations would certainly occasion a suboptimal result because of limited options for enforcement. The Self-regulation option would require a body that would set requirement for cybersecurity sector. The regulations would serve as a guide and can be employed for self-regulation and may be adopted by some players in the sector. The Self-regulation option would work well in a mature sector which is not the case with the cybersecurity sector in Kenya. Providing procedural rules option is more practical and sounds effective. However, it is worth to note that all the options were considered, and it was found necessary that the regulations be formulated in order to effectively implement the Act.

Net Benefit is derived from total Cost deducted from Benefit (**Net Benefit=** Benefit- Cost)

If Benefits outweighs Costs, it is recommended to proceed for implementation (Benefits ≥ Costs = Proceed)

Table 1: Cost Benefit Analysis for the two options

Option	Possible Costs	Possible Direct Benefits	Net Benefits (Ksh)	Policy implications
Option 1 A group of industry players within the cyber ecosystem, voluntarily developing rules or codes of conduct that regulate or guide the behaviour, actions, and standards of the ecosystem	Hiring 1 cybersecurity professional- Ksh 3,600,000/annually/per entity Average cost of buying/license fee for Antivirus/antimalware and other cybersecurity solutions- network security applications/access control/authentication/firewall/IDPS/digital certificates =Ksh 16,000,000/per entity/annually Average cost of training a group of key personnel- Ksh 10,000,000/per entity/ annually Average cost of assessment/Audit fee – Ksh 4,000,000/per entity /annually *Cost to establish standard organizational SOC – Ksh 1,200,000,000 Cost to develop cybersecurity policies/strategies/plans - Ksh 5,000,000/per entity Cost for data backup and recovery – Ksh 10,000,000/per entity	• To avoid cybersecurity losses – disruption and customers loss/data breaches/reputation risks • Average cost of a data breach is USD 4.45 million (Ksh 670,000,000) based on IBM's Cost of Data Breach Report 2023 • Cost savings achieved by organizations with high levels of Incident Response planning and testing is USD 1.49M (Ksh 223,500,000) based on IBM's Cost of Data Breach Report 2023 • 60% of small businesses go bankrupt within half a year after suffering from data breaches or cyberattacks (Ponemon Institute) • Maximum Penalties/fines to pay (CMCA) =Ksh 5,000,000	-350,100,000	When used in the right circumstances self-regulation can offer significant advantages within the cyber ecosystem such as greater flexibility and adaptability to evolving nature of the ecosystem; potentially lower compliance and administrative costs; an ability to address industry-specific and consumer issues directly; and quick and low-cost complaints handling and dispute resolution mechanisms. The option works well where the sector has matured. However, this option has negative consequences in the implementation of the CMCA as government lacks national visibility of cybersecurity in this era of cyberwarfare Organizations are required to invest heavily on cybersecurity since sharing of resources may not be ideal for this option

				The option is likely to lead inadequate protection for the cyber ecosystem because of narrow interests rather than the wider national interests Additionally, the cross-cutting nature of the cyber ecosystem makes it difficult for the players in a particular industry, say energy to establish codes of practice that regulates the entire ecosystem
Option 2 This entails coming up the regulations that are legally binding to implement the CMCA,2018	Hiring 1 cybersecurity professional- Ksh 3,600,000/annually/per entity Average cost of buying/license fee for Antivirus/antimalware and other cybersecurity solutions- network security applications/access control/authentication/firewall/IDPS/digital certificates =Ksh 16,000,000/per entity/annually Average cost of training key personnel - Ksh 1,000,000/per entity/ annually Average cost of assessment/Audit fee – Ksh 4,000,000/per entity /annually *Cost to establish basic organizational SOC – Ksh 300,000,000; Cost of establishing standard sector SOC –	• To avoid cybersecurity losses – disruption and customers loss/data breaches/reputation risks • Average cost of a data breach is USD 4.45 million (Ksh 670,000,000) based on IBM's Cost of Data Breach Report 2023 • Cost savings achieved by organizations with high levels of Incident Response planning and testing is USD 1.49M (Ksh 223,500,000) based on IBM's Cost of Data Breach Report 2023 • 60% of small businesses go bankrupt within half a year after suffering from data	289,900,000	The regulations ensure expeditious, efficient, lawful, reasonable, and procedurally fair management of cybercrimes in Kenya This option ensures that government has national visibility of cybersecurity that is well coordinated in this era of cyberwalfare The regulations will protect both government and private sector critical assets and information The regulations will provide guidelines and standards for local and international cooperation in matters

	400,000,000; Cost of establishing national SOC – 600,000,000 Cost to develop cybersecurity policies/strategies/plans - Ksh 5,000,000/per entity Cost for data backup and recovery – Ksh 10,000,000/per entity Establish monitoring and enforcement mechanism – Ksh 15,000,000/annually	breaches or cyberattacks (Ponemon Institute) • Average cost saving for better coordinated cybersecurity initiatives including Zero trust is 2 million per breach/per CII organization (Ksh 300,000,000) • Cost savings by adopting coordinated sector capacity building approach -offered through a national body -Ksh 450,000,000 for every 50 CIIs • Maximum Penalties/fines to pay (CMCA) =Ksh 5,000,000		of cybercrime especially in a growing cybersecurity sector of a developing country like Kenya The proposed regulatory instruments will enhance the fundamental rights of persons or institutions by protecting them against cyber actors and ensuring that offenders are prosecuted

1USD=Ksh 150

* *SMBs typically spend around 10% of their annual budget on cybersecurity (https://imagineiti.com/how-much-does-cybersecurity-cost-for-small-to-mid-sized-businesses/)*

**Companies spend $250,000 on cybersecurity solutions and training with annual IT budgets of $2.5M. Each full-time employee costs a company $2,500 – $2,800 for solid cyber security protection (https://imagineiti.com/how-much-does-cybersecurity-cost-for-small-to-mid-sized-businesses/)*

Serianu report (2018) indicates that the total estimated cost of cybercrime is about Ksh. 29.5 Billion. The Direct cost that arose as consequence of cybercrime such as loss of money, law suits, fines, insurance claims and investigation was about Ksh. 8.85 Billion while indirect cost incurred in deterring and detecting cybercrime through purchase of equipment and training was about Ksh. 20.65 Billion.

**The cost of building a SOC can vary greatly depending on your current level of maturity and the end state you want to achieve*

** Organizations with a mature zero trust approach spent $1.51 million less than organizations just starting their journey - IBM 2022 Cost of a Data Breach Report*

The analysis further indicates that public and private entities stand to gain a lot from the regulations. This is expected to create a positive impact in terms of providing incentives to the enterprises including the CII operators. Option 2 offers the best scenario in terms of efficient and effective implementation of the regulations as well as net benefits.

It is also expected that the net benefit will further as cybersecurity sector grow and particularly when entities continue investing in cybersecurity solutions and building capacity to their staff on cybersecurity. In addition, there are other numerous non-monetary benefits that entities stand to gain including improving their reputation and trust with key stakeholders, including clients and funders. Other benefits include:

(a) Enhanced consumer protection: through availability of the critical infrastructure;
(b) Guarantee availability of life sustaining services including the supply of water, health services and energy;
(c) Guarantee a robust economy of the Republic;
(d) Avert massive casualties or fatalities;
(e) Guarantee availability of the money market of the Republic; and
(f) Improve the security of the Republic including intelligence and military services.

It is noted that the Benefits derived from cost savings (not incurring avoidable costs such as litigation and fine costs) which is the benefit that entity will realize by ensuring compliance with the Cybersecurity Regulations is Positive. The Policy in this case, the cybersecurity Regulations will positively impact on entities directly and indirectly. Overall, it is expected that newer industries in the cybersecurity ecosystem will be created thus creating jobs and improving the growth of Kenyan economy. Finally, the regulations are expected to boost the international trade because trading partners are expecting countries to adopt cyber and data protection measures.

10. CONCLUSION

The proposed Regulations (Option 2) are necessary in the operationalization of the CMCA Act, 2018 and is therefore the preferred option. It is clear that the benefits and impact of developing these Regulations by far outweigh any estimated cost of its implementation.

11. RECOMMENDATION

Given that the proposed Regulations 2023 (Option 2) will facilitate effective implementation of the CMCA Act, 2018, it is recommended that the Regulations be approved for public participation.

……

HON. PROF KITHURE KINDIKI
CABINET SECRETARY FOR INTERIOR AND NATIONAL ADMINISTRATION

DATE……