ZICTA

Critical Information Infrastucture Localisation and Externalisation Fee

Concept Note

April 2022

A regulator at the nexus
of an inclusive digital economy

A regulator at the nexus
of an inclusive digital economy

ZICTA

Critical Information Infrastucture Localisation and Externalisation Fee

Background

The Cyber Security and Cyber Crimes Act No.2 of 2021 (The Act) seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by Cyber threat actors involvement in Zambia's cyberspace.

The Zambian Government is committed to protecting the essential services Zambians rely on by uplifting the security and resilience of infrastructure on which critical information lies (critical infrastructure). Critical information and Critical Infrastructure shall hereafter be referred to as Critical Information Infrastructure (CII).

As the threats and risks to Zambia's CII evolve in a post-COVID world, so too must the approach for ensuring the ongoing security and resilience of CII and the essential services they support.

Under the proposed Statutory instrument (S.I), CII are identified based on **critical information** in a given sector and also by the **Critical Infrastructure** that is vital to the provision of essential services.

The **essential services** include:

I. Generation, supply or distribution of electricity;
II. Medical or hospital;
III. Water supply and sewerage;
IV. Education;
V. Agriculture;
VI. Digital financial services;
VII. Internet banking;
VIII. Automatic teller machines;
IX. Payment gateway;
X. Aviation operation;
XI. Data center;
XII. Broadcasting;
XIII. Fire and police;
XIV. Emergency services;
XV. Metrological services;
XVI. Transportation services;
XVII. Tax collection; and
XVIII. Payment switch services;
XIX. Mineral mining and operation;

Eleven (11) sectors have been identified that support the provision of essential services, these are:

I. Banking and finance ;
II. Health;
III. Transport
IV. Communication;
V. Defence and national security;
VI. Energy;
VII. Insurance;
VIII. Education;
IX. Taxation;
X. Mining; and
XI. Public body

Consultation on the Proposed Localisation Regulations and Externalisation Fee

1. Localisation

Under the proposed S.I, a Critical Information Infrastructure Controller (CIIC) shall ensure that CII is located in Zambia. A CIIC who intends to externalise CII shall apply to the Minister.

The Minister may approve or reject the application, within thirty days of receipt of the application and inform the applicant.

1.1. Localisation Importance

I. Hosting of CII on Cloud Service Providers within Zambia will help grow the Zambian Cloud Service industry and other investments in the ICT sector.
II. Localisation of CII will create more technical jobs and business opportunities for local ICT providers.
III. Severe compromise of a CII has the potential to have lasting and direct effects on the nation and ordinary people. Drawing focus to the financial sector, a severe compromise of any of Zambia's large banks has the potential for severe and lasting economic and security impacts given their high volume of retail customers. For example, if a cyber-attack targets a system in a region outside Zambia (a foreign state), the effect should not cause a disruption in Zambia such that customers fail to withdraw funds via an automated teller machine (ATM) or make payments via point of sale or check their bank account via internet banking, USSD, mobile app or make mobile money payments.
IV. Investigation of incidents on CII which are hosted outside the country possess a logistical challenge and hamper regulatory inspections due to visa requirements, foreign or hostile environments and other factors.
V. National Security and Cyber Resilience necessitates that any geo-political situation outside Zambia's borders should have minimal tolerable risk to Zambia's sovereignty. This sovereignty extends to the cyber space and CII. Given cyber dependences between sectors, an interruption to one sector could lead to interruption in another sector and lead to catastrophic effect on the economy. Therefore **Physical location** of the critical infrastructure that supports essential services is an important consideration in geo-political risk assessment. Currently, most CII is hosted outside Zambia.
VI. Governments around the world are rapidly considering and proposing new legislation targeting data localisation and the protection of Critical Information Infrastructure (CII).

1.2. Localisation Proposal

I. Under the proposed localisation regulations, ZICTA intends to direct CIICs to localise within Twenty Four (24) months from the date the S.I is published in a gazette.

2. Externalization

The S.I states that the Minister of Technology and Science (The Minister) may, in considering an application by a CIIC to externalise CII, take into account:

I. Security measures being applied to the CII **are adequate**;
II. Whether **it is necessary** for the CII to be **hosted outside** the geographical **jurisdiction of Zambia**;
III. National security;
IV. Submissions by concerned data owners;
V. Consent by **data subjects**; and
VI. Any other factors that the Minister considers necessary.

The **Minister shall consult** ZICTA, the National Cyber Security Advisory Coordinating Council (the Council) and relevant security agencies when considering an application for externalisation.

2.1. Externalisation Proposal

For a CII that qualifies for externalisation, it is proposed that the externalisation fee of 0.5% of the CIICs previous annual turnover shall be paid to ZICTA. The fee is proposed to be an **annual fee**.

2.2. Rationale for Externalisation Fee Model

I. Taking cognizance of the need to **develop a model** that can be used **across board** to cover CIICs **in all sectors**, a single percentage fee is proposed.
II. The proposed fee is meant to encourage CIICs to host their \infrastructure in Zambia as there is already existing capacity for hosting.

2.3. Externalisation Fee Model

It is proposed that a fee be charged of a CIICs gross annual turnover. A standard fee percentage of 0.5% is adopted, which can then be incorporated into the simple formula below and paid annually:

*Fee Percent X ** gross annual turnover = Annual Fee Payable

*The fee percent would be within the percentage fee range charged by regulators (under 5%).

**The gross annual turnover indicates all the revenue derived directly or indirectly by a CIIC.

Therefore, in the event that an entity has k1, 000,000,000 (One billion Kwacha) gross annual turnover, the fee for that CIIC will be established as:

0.5% X ZMK 1, 000,000,000 = ZMK 5, 000,000 (Five Million Kwacha) P.A.

The Consultation Feedback Questions

1. Do you agree that critical information infrastructure should be located in Zambia either on premise or in-country data centers such as Paratus, NetOne or Infratel (Tier 3 Data Centers)?

Yes ☐ No ☐
(Select either Yes or No)

Comment Box (Please ensure to provide details on any comment that you may have)

Click here to enter text.

2. Do you agree that Zambia should provide an option to externalise CII?

Yes ☐ No ☐
(Select either Yes or No)

Comment Box (Please ensure to provide details on any comment that you may have)

Click here to enter text.

3. Do you agree with the proposed externalisation fee of 0.5% of annual turnover?

Yes ☐ No ☐
(Select either Yes or No)

Comment Box (Please ensure to provide details on any comment that you may have)

Click here to enter text.

4. Do you have any other matter you feel should be considered with regards to externalisation of CII?

Yes ☐ No ☐
(Select either Yes or No)

Comment Box (Please ensure to provide details on any comment that you may have)

Click here to enter text.

5. Are there any other matter you would like ZICTA to consider with regards to the proposed S.I?

Yes ☐ No ☐
(Select either Yes or No)

Comment Box (Please ensure to provide details on any comment that you may have)

Click here to enter text.

Conclusion and Next Steps

ZICTA is grateful for the input of all stakeholders that will participate in this consultation process by submitting their valuable comments and feedback.

The input that will be received will be useful in enhancing the protection of CII in Zambia as well as promoting National Cyber security and resilience.

ZICTA further wishes to assure all the respondents that their submissions will be accorded due consideration and taken into account in making improvements to the proposed S.I.

ZICTA