LIRNEasia
Pro-poor. Pro-market.

17th August 2023

Jayasiri Amarasena
CEO, Sri Lanka CERT|CC
BMICH
Colombo 07

Dear Mr. Amarasena:

LIRNEasia's Response to Ministry of Technology's Invitation for Comments on the Cyber Security Bill

LIRNEasia welcomes the opportunity to submit our views and comments on the proposed Cyber Security Bill uploaded to the website of Sri Lanka CERT (www.cert.gov.lk).

LIRNEasia is a pro-poor, pro-market think tank whose mission is catalyzing policy change through research to improve people's lives in the emerging Asia Pacific. LIRNEasia has been active in Sri Lanka and the rest of the Asia-Pacific region since 2004.

Our response is attached for your kind consideration.

For questions regarding this submission, please contact Ms Chiranthi Rajapakse, Research Manager, LIRNEasia at <chiranthi@lirneasia.net> (0777 258014)

Thank you.
Sincerely,

<signed>

Helani Galpaya
Chief Executive Officer
helani@lirneasia.net

Pranesh Prakash
Research Fellow
Co-founder, Center for Internet and Society
pranesh.prakash@gmail.com

Ashwini Natesan
Research Fellow & Legal Consultant
aswini.natesan@gmail.com

CC:
(1) Professor N. Gunawardana, Secretary, Ministry of Technology
(2) Professor Malik Ranasignhe, Chairman, ICTA

Attachment: LIRNEasia's comments on proposed Cyber Security Bill

LIRNEasia
Pro-poor. Pro-market.

Attachment: LIRNEasia's comments on proposed Cyber Security Bill

This submission is in response to Ministry of Technology's invitation to comment on the Cyber Security Bill uploaded to the website of Sri Lanka CERT in August 2023 (www.cert.gov.lk)

Our submission addresses specific concerns related to the requirement for accreditation of Cyber Security service providers, the composition of the Cyber Security Regulatory Authority and the definition of the term Critical National Information Infrastructure.

A) Accreditation of Cyber Security service providers

Current proposal:

Section 23 of the draft Cyber Security Bill provides for the accreditation of cyber security service providers for a comprehensive set of activities:

- To operate sectoral CERTs and CSIRTs;
- To conduct vulnerability assessments and penetration tests;
- To conduct cyber security audits and risk assessments;
- To monitor cyber security through operating Cyber Security Operation Centre;
- To conduct cyber security forensic investigations;
- To provide cyber security advisory and consultative services;
- To design, develop, implement, install, and troubleshooting cyber security solutions;
- Importing, distributing, installing and maintaining cyber security solutions that safeguard computers, computer programs, computer systems, relevant devices from cyber threats and incidents; and
- Managing the cyber security of client organizations.

Our objections and concerns:

The objections we have to this (above mentioned) provision are:

1. Harmful effects on Sri Lankan providers of cyber security services
   This section creates a very high barrier to entry into the field, whereas the aim should be to encourage more people to join the field of cyber security. These provisions apply not only to the services that Sri Lankan companies can seek, but also to the conduct of Sri Lankan citizens. One way that novices can engage in cyber security work is by participating in 'bug bounties'. This law, specifically section 23(b), would prohibit them doing so without accreditation.

2. Harmful effects on Sri Lankan users of cyber security services

Such licensing requirements would prevent Sri Lankan companies and the government from being able to use foreign expertise, especially when it is required urgently. This limits the cyber security talent pool that Sri Lankans have access to, which runs contrary to the aims of this law.

3. Lack of evidence for need of an accreditation system (no market failure)
   There already are a number of certifications — OSCP, CISSP, etc. — that are available to signal the competence of cyber security service providers. (This is a list of certifications that the US government's NICCS recognizes: https://niccs.cisa.gov/about-niccs/cybersecurity-certifications) It is not clear why a separate accreditation is needed, what benefit it would provide, nor what market failure it seeks to address.

4. Complexity of accreditation
   Given the diversity of possible cyber security services, it is unclear what the basis for the accreditation would be. Will the government conduct a test? If so, what specific skills would the test include? Penetration testing is very different from security architecture and design, which is very different in turn from incident management and response. Or would an accreditation mean that the service provider has paid the requisite license fees? In which case, the accreditation itself becomes devalued.

While rare jurisdictions, such as Singapore, may have a licensing requirement, they are far more limited in their scope. For instance, Singapore's Cybersecurity Act, 2018 only requires licensing for two kinds of services: managed security operations centres and penetration testing. It does not require licensing or accreditation for security audits, forensic investigations, advisory services, etc. The scope of the provision as currently drafted is overbroad, and lacks a clearly articulated problem that it addresses.

Our Recommendations:

1. There is no evidence of a market failure in the provision of cyber security that requires the institution of a licensing mechanism as a solution. Given this lack of evidence for an accreditation mechanism combined with the harms that accreditation would create, we recommend **removing Part V (Section 23) in its entirety**.
2. Alternatively, if it is established that consumers are facing difficulties in distinguishing good cyber security services providers from bad, and if the government does not believe the dozens of existing courses and certifications are sufficient, then the government could run a **non-mandatory accreditation service**.
3. In the alternative, if the government believes that some kind of mandatory accreditation requirement is necessary for government entities, the provision could be amended such that clauses (f), (g), and (h) are removed, and **clauses (a), (b), (c), (d), and (e) are made applicable only for provision of services to the government**. However, as we point out

above, this limits the expertise that the government would have access to, especially if it is foreign expertise.

We strongly urge the adoption of option 1.

B) Composition of the Cyber Security Regulatory Authority of Sri Lanka ("Authority")

Current proposal:

Section 6 of the Cyber Security Bill provides for the composition of the Board of Directors of the Authority. It is noted that government / State sector members are already in the Board as ex-officio members namely -

(I) the Secretary to the Ministry of the Minister to whom the subject of information and cyber security is assigned or an Additional Secretary of such Ministry nominated by the Secretary of such Ministry;

(II) the Secretary to the Treasury;

(III) the Director General of the Defence Cyber Command, established under the Defence Cyber Command Act, No. of 2023;

(IV) the Director General of Telecommunication Regulatory Commission

(V) Chairperson of Information and Communication Technology Agency of Sri Lanka

In addition, the President is empowered to appoint 4 other members under Section 6 (b). The provision reads as follows:

"four persons appointed by the President, (hereinafter referred to as the "appointed members") each of whom shall have over fifteen years of experience and demonstrated professional excellence in the fields of cyber security, information and communication technology, public or corporate sector administration, management, law or finance."

Similarly, Section 7 (1) (a) of the Bill provides for appointment of Chairperson from the "appointed members". It reads as follows:

"The President shall appoint from among the appointed members, a member of the Board who has demonstrated effective leadership qualities in public or private sector entities to be the Chairperson of the Board."

Our Objections and concerns:

Under Section 6 (b), the "appointed members" should be from the private sector since the public sector in the form of ex-officio members is a majority of the Board. The Authority has wide powers under the Bill and our recommendation is to ensure that such power is balanced between the ex-officio and appointed members.

Our Recommendations:

1. We strongly recommend that the "public" sector option be removed from Section 6 (b).
2. We also recommend that the word "public" be removed from Section 7 (1) (a), for the reasons mentioned above.

C) Critical National Information Infrastructure

Current Proposal:

The draft Cyber Security Bill provides for the identification of a computer, computer program, computer system or related device as a "Critical National Information Infrastructure" (CNNI). The definition of CNII given in Section 38 (interpretation) reads as follows;

"Critical National Information Infrastructure" means, the computer, computer program, computer system, or related device identified by the Authority as a Critical National Information Infrastructure under this Act, which is located wholly or partly in Sri Lanka, and its disruption or destruction would create a serious impact on the national security, public safety, public health and economic wellbeing of citizens, delivery of essential services or effective functioning of the government or the economy of Sri Lanka";

Our Objections and concerns:

1. We are of the view that identification of CNII should be limited to organisations that have the potential to cause large scale impact and such impact should be more stringently worded.
2. It is hoped that further guidance will be provided on CNII once the Bill is passed, and the Authority is established. The CNII will be subject to strict controls and monitoring by the Authority. Therefore, identification of CNII should be based on clear and transparent criteria.

Our Recommendation:

1. While we welcome the guidance given to CNNI in the interpretation section of the Bill, we would recommend that the word “serious” be substituted with “debilitating”. Our recommendation is in line with the cabinet approved Information and Cyber Security Policy for Government Organisations that became effective in August 2022. The said Policy defined CNNI as follows:
   “CNII providers are defined as the organizations that maintain information and IT assets whose incapacity or destruction would have a debilitating impact on national security, governance, economy, health and social well-being of a nation. A list of CNII providers will be published by the Sri Lanka CERT”.