18th June 2021

Michael R. Sialai, EBS
The Clerk of the National Assembly
Office of the Clerk, Main Parliament Buildings
P.O. Box 41842 – 00100
Nairobi, Kenya

Dear Sir,

RE: SUBMISSION OF MEMORANDUM ON THE COMPUTER MISUSE AND CYBERCRIMES (AMENDMENT) BILL 2021

We refer to the above matter and your public notice inviting the public to submit their comments on the Computer Misuse and Cybercrimes (Amendment) Bill 2021.

Please see annexed to this letter a brief schedule setting out our comments and recommendations relating to the Bill.

Should you require any clarifications, please do not hesitate to contact me on (Maxwell@amcham.co.ke).

Yours faithfully,

Maxwell Okello
Chief Executive Officer
American Chamber of Commerce, Kenya

AMCHAM SUBMISSIONS ON THE COMPUTER MISUSE AND CYBERCRIMES (AMENDMENT) BILL 2021

Issues/Provision in Bill	**Provisions in the Computer Misuse and Cybercrimes (Amendment) Bill 2021**	***Recommendations/Comments***
Functions of the Committee	*Section 6 of No.5 which is intended to be amended* *(1) The Committee shall –* *(a-h)* *General advice and guidance to the government*	AmCham through its members sees an opportunity to cooperate and be involved with the Committee by providing system solutions, processes and global best practices to aid government in their own cybersecurity missions.
Section 27 Cyber Harassment	*Section 27 of No.5 which is intended to be amended* *27 Cyber Harassment* *(7) The court may order a service provider to provide any subscriber in its possession for the purpose of identifying a person whose conduct is complained of under this section.*	The Cloud Service Providers (CSP's) do not have access to the data (it can be encrypted to further security and customers own and maintain the encryption keys) and thus the language should consider who this applies to. CSP's do not control where customers host their workloads, thus the laws of that jurisdiction apply. Where the data is hosted in Kenya on the CSPs servers, CSPs will notify the customer of the data request, unless compelled by a valid binding court order that prevents it from doing so.

		Shared Responsibility Model - Public cloud security differs from traditional on premise data centres in that Security and Compliance is a shared responsibility between the CSP and the customer. This shared model can help relieve the customer's operational burden as the CSP operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the CSP provided security services. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. The differentiation of responsibility is commonly referred to as Security "of" the Cloud (CSP) versus Security "in" the Cloud(customer).

		CSP responsibility "Security of the Cloud" – CSPs are responsible for protecting the infrastructure that runs all of the services offered in the Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run cloud services. Customer responsibility "Security in the Cloud" – Customer responsibility will be determined by the cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. Customers are responsible for managing their data (including encryption options), classifying their assets, and using tools to apply the appropriate permissions. As such cloud service providers do not have access to any customer data and the customer owned encryption keys used by customers.