U.S. CHAMBER OF COMMERCE
Middle East

To: National Cybersecurity Authority
Kingdom of Saudi Arabia

From: U.S. Chamber of Commerce
Department of Middle East Affairs

RE: Input on Cloud Cybersecurity Controls Draft (CCC – 1:2020)

Date: 23 March 2020

The U.S. Chamber of Commerce ("the Chamber") is the world's largest business federation, representing the interests of more than three million businesses of all sizes and sectors, many of whom are major employers and provide significant investment in the Kingdom of Saudi Arabia. At home and abroad, the Chamber is an acknowledged leader in digital economy policy, including digital trade, cybersecurity, data privacy, artificial intelligence, and e-commerce issues. Through the U.S.-Saudi Arabia Business Program, the Chamber engages closely with U.S. and the Kingdom of Saudi Arabia governments to address the most pressing policy issues and concerns that hinder the growth of trade and investment between the two countries. In fact, the U.S. Chamber most recently hosted H.E. Dr. Majid Al-Qasabi, Minister of Commerce; HRH Princess Reema bint Bandar Al-Saud, Saudi Ambassador to the United States; and, H.E. Dr. Eiman Al-Mutairi, Assistant Minister of Commerce and CEO of the National Competitiveness Center, for a major U.S.-Saudi Arabia Business Leaders Forum in Washington.

The Chamber commends the National Cybersecurity Authority (NCA) for launching the draft Cloud Cybersecurity Controls (CCC) document for public consultation. Incorporating a wide range of stakeholder perspectives serves to enrich the quality of the draft. Technological integration and mass data storage via cloud sharing are becoming commonplace in business, necessitating new security protocols to address growing vulnerabilities. We fully support NCA's CCC efforts given its significance in protecting the security of the country, in addition to its role in supporting, promoting and attracting investments in the field of information technology.

The Chamber considers cybersecurity to be a top priority. Businesses of all sizes are investing in effective cloud computing and cloud backup systems. With more companies and organizations tapping into the flexibility, agility and cost savings that come along with moving data to the cloud, there are additional compliance risks and security threats. These systems must be adequately protected against cyber threats if we are to ensure that the benefits created by the digitization of our economies are not outweighed by the risks.

Accordingly, the Chamber has worked with more than 35 governments to develop and implement approaches to cybersecurity that ensure appropriate levels of cybersecurity for businesses of all sizes and in all sectors of the economy. This engagement has afforded us the opportunity to see first-hand what makes for effective cybersecurity policy.

Governments and businesses face shared, cross-border cyber threats. Unnecessary divergence in the regulatory frameworks and responses of governments makes our defenses weaker, and our adversaries stronger. As such, we support international efforts aimed at aligning regulatory approaches to better reflect globally-accepted best practices. The U.S. Chamber of Commerce comments NCA for leveraging many international standards, frameworks, controls and international practices in the field of cybersecurity to establish the minimum requirements for CCC laid out in the draft document.

There are certain areas where we believe the text of the draft controls could be improved, to better facilitate our shared goal of improving cybersecurity outcomes in The Kingdom of Saudi Arabia.

The U.S. Chamber of Commerce recommends the following:

Recommendation No. 1: Defining the term "information" in the CCC in harmony with existing designations

In relation to the requirements that the information of users of hosting and cloud computing services must be hosted and stored inside the Kingdom of Saudi Arabia (ECC 4-2-3), we strongly recommend defining the term "information" in the CCC in harmony with existing designations, such as Traffic Light Protocol (TLP) mentioned in the CCC.

We understand that this approach is designed to preserve the security of particularly sensitive information, but we also need to be mindful of the restriction so it would

not result in limiting Saudi entities access to innovative offerings but without necessarily providing more security.

The term "information" is overly broad and can create confusion. If the restrictions remain as drafted, it will be challenging to provide cloud services in the Kingdom. For example, even if providers host and store the data locally there needs to be some level of communication between different servers globally to provide configuration, technical support, etc. Therefore, it is highly recommended that data that falls into the scope of this section is to be reserved for sensitive and confidential data.

Accordingly, we recommend defining the term "information". The NCA can advise cloud customers to categorize data according to the TLP and indicate that data falling into the scope of this section be reserved for sensitive and confidential data. The below sets of data should be excluded from the requirements mentioned in 4-2-3, and providers should be allowed to store this data inside the Kingdom when they can evidence an adequate level of cybersecurity through appropriate levels of certifications:

- Metadata
- Network Management information (not user traffic data) and technical support data
- Data that is only available when a cloud service is used and is never stored on the cloud
- Identification number such as the MAC address or IP address, which are usually required for providing support services

Recommendation No. 2: Enable data exports through globally recognized transfer mechanisms.

The ability for data to flow through the global economy as important as the ability to move goods, services, and capital. Data flows have increased global GDP by at least 10 percent over the past decade.[1] We note that, at the same time, jurisdictions around the world have conditioned transfers of personally identifiable information on the ability of foreign governments and organizations to ensure a high standard of data protection. These mechanisms include government whitelists of jurisdictions that have been found to possess an equivalent level of data protection, standard

[1] Global flows of goods, services, finance, people and data have increased world GDP by at least 10 percent over the past decade, or $7.8 trillion. Of that increase, $2.8 trillion can be attributed directly to the value of CBDFs, which is greater than the increase attributed to global goods trade of $2.6 trillion - McKinsey Global Institute Study

contractual clauses, intragroup transfers ("binding corporate rules"), and certifications. The ECC deviates from the above, which can be detrimental as it limits the number of providers that government and the semi-government customer can use in certain situations and thus prevents them from availing the best available innovative solution in the market. The Chamber recommends an "all-of-the-above approach" to data transfers, pursuing adequacy with foreign jurisdictions while recognizing the validity of contractual and certification mechanisms that are already global standards. With regards to certifications, we point the NCA to the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System.

Recommendation No. 3: Allow CSTs to use CSP services hosted on a registered CSP provider

Under the terms of the draft proposal, customers (CSTs) are required to contract licensed Cloud Service Providers (CSPs), presumably with associated terms to own and/or manage a data center in the Kingdom of Saudi Arabia in line with the registration requirements established by the Saudi Communications and Information Technology Commission (CITC). In order to comply with the CCC location requirements, Software-as-a-Service (SaaS) providers may choose to contract an Infrastructure-as-a-Service (IaaS) provider who is registered in Saudi Arabia and has the ability to host data locally. In this circumstance, the customer's contract is with the SaaS provider, not the IaaS provider (who is contracted to the SaaS provider). It should be clarified that such arrangements are acceptable, as opposed to requiring the SaaS provider to establish and register their own data center in the Kingdom.

Recommendation No. 4: Personnel requirements in accordance with international data security standards

The draft document requires certain data center personnel be of Saudi nationality for level 3 data and above. We recommend implementing an approach based on international data security best practices instead, such as ISO 27001:2013 human resource security requirements (section A.7). This includes measures relating to screening of employees, contract terms, training, discipline and change of employment.

Recommendation No. 5: Prior general authorization of vendors

While third-party providers should be held accountable to the equivalent level of data protection and security as the CSP, it is unrealistic for all such providers to be whitelisted by the government (level 3 and above for government customers) given

this is an oft changing landscape. Instead, the government should require such vendors only to be engaged with prior general authorization of the customer (in this case, the government) and a duty of the CSP to inform the customer of any changes in vendors by keeping the list updated. This is in line with international data protection laws such as GDPR (Article 28.2).

The Chamber firmly believes that a well-crafted cloud security strategy is the basis upon which sustainable digital growth can be built. We look forward to working with you to implement such a strategy, which will facilitate further growth in Kingdom of Saudi Arabia -U.S. trade ties.

Please feel free to reach out to us with questions. We would be honored to work with you in the future, and will follow up with your office about future opportunities for collaboration.

Warm regards,

Steve Lutes
Vice President, Middle East Affairs
U.S. Chamber of Commerce
slutes@uschamber.com

Liz Clark
Manager, Middle East Affairs
U.S. Chamber of Commerce
lclark@uschamber.com

U.S. CHAMBER OF COMMERCE
Middle East

APPENDIX – Cloud Cybersecurity Controls Draft Input

Prepared 23 March 2020 by the U.S. Chamber of Commerce

This document serves as an appendix to the input submitted by the U.S. Chamber of Commerce on 23 March 2020 on the draft Cloud Cybersecurity Controls (CCC) of the Kingdom of Saudi Arabia. The below recommendations are an aggregation of supplemental recommendations on specific parts of the CCC draft, submitted by member companies of the U.S. Chamber's U.S.-Saudi Business Program.

Please reach out to Steve Lutes, the Chamber's Vice President for Middle East Affairs at the U.S. Chamber (slutes@uschamber.com) or Liz Clark, Manager for Middle East Affairs (lclark@uschamber.com) with any questions.

Rule / provision number	Description of rule/provision	Recommendation
8.3.2.3.2	Applicable laws on data access	The provision crafted for level 4 data on compliance with foreign laws relating to data access is appropriately balanced. Recommendation: Apply across level 3 data. Additionally, call on government to engage in direct dialogue with one another to resolve potential conflicts in law that stem from extraterritorial government data access rules.
8.3.2.5	CSP obligation: [CSP must] provide cloud computing services from within the KSA, including all systems used, including storage, processing, monitoring, support, and disaster recovery centers.	This requirement can normally be implemented for the core functions of storage, processing, and disaster recovery centers. However, monitoring and support typically involve global systems for additional resiliency and for providing tools to experts needed to maintain or fix systems. These experts may not reside in

		KSA, and can be highly experienced computer scientists who have designed the systems. The use of external monitoring and support will not require storing KSA data out of the country. Recommendation: limit requirement of all systems in KSA to the storage and processing systems while permitting monitoring and support systems at other locations. In addition, if applicable to disaster recovery centers, then customers will have the additional expense of supporting additional geographically separate regions in KSA.
8.4.2.3	CSPs will work with the competent Saudi authorities to develop a technical solution that shall ensure that any third-party providers in the Cloud ecosystem comply with all KSA data classification and protection requirements and regulations. Both parties will work together to develop a technical solution that will allow the Saudi Government to whitelist suppliers in the ecosystem that want to offer their services to the Saudi Government organizations.	While we understand the motivation for the inclusion of this type of requirement, it would be better dealt with bilaterally through a contract between the CSP and the relevant public agency so that technical solutions can be properly scoped and implemented. Recommendation: Require CSTs to consider inclusion of this requirement in their procurement processes to allow for proper scoping and implementation of an appropriate technical solution.
8.5.1.1 and 8.5.2.1	Cybersecurity obligations for level 2 and level 1 state that the CSP and CST will verify isolation of the cloud from other obligation levels. The use of "isolation" can be subjectively interpreted and may lead to confusion as to whether this is	Define "isolation" requirements between Level 1, Level 2, Level 3, and Level 4. Recommendation: More explicit definition of the expected level of isolation to avoid misinterpretation by the cloud customer is needed.

	required to be physical isolation or logical isolation. In addition, CSTs may integrate or connect services hosted within the cloud environment to services hosted outside of the cloud environment; as an example, there may be identity federation to a separate identity service to centralize identifies for CST administrators.	
8.5.2.1	[CSP shall] isolate the cloud assigned to this level from other classification levels.	It is unclear if the requirement calls for virtual isolation or whether physical isolation using different data centers is required to isolate each classification level. Virtual isolation can create technical challenges for the customer as it will be difficult for the customer to perform operations that involve data from more than one classification level. Physical isolation, using different data centers, will likely involve increased expense. Because the CSP does not inspect a customer's data, ultimately it is the customer's responsibility to choose the cybersecurity features appropriate for its data. Recommendation: Customers know the classification level of their data best and should use the appropriate cybersecurity measures required by the most sensitive classification level.
2-3-P-1-4	Referring to the ECC control 2-12-3-5, all logs must be retained	Customers are best positioned to store and retain their own logs on cloud platforms. Different jurisdictions have

	(for at least 18 months) and backed up.	different retention requirements, and many prohibit retention for 18 months. Thus, customers should customize their own logging according to their legal and compliance needs, and those of their users.
2-6-P-1-6	Provision of metadata labelling mechanism to meet all applicable data privacy, data sovereignty, and data protection laws and regulations.	Current cloud systems do not offer specific metadata labeling systems designed to operate across multiple different legal regimes. Customers are best positioned to build systems that handle data according to their own compliance and legal requirements.
2-7-T-1-4	Multi-factor authentication for privileged cloud accounts.	Accounts used for programmatic access or that are integrate to automated processes are often limited in their ability to support multi-factor authentication. <u>Recommendation:</u> The requirement for multi-factor should be limited to privileged accounts that support interactive use.
2-15-T-3-2	Trusted key storage for the cloud service, strictly external to cloud.	Use of trusted key storage external to the cloud may introduce risks during the key export, transfer, and import process. While not every key management system provided by a CSP is expected to meet requirements for every data classification or obligation level, there may be services that satisfy the requirements in 2-15 and provide an adequate level of control for CST. <u>Recommendation:</u> Requirement for external trusted key storage be modified to require definition and validation that

		key storage is both appropriately protected to prevent unauthorized disclosure, recoverable to meet availability requirements, and allow an exit strategy to remove information or key material from the CSP.