U.S. CHAMBER OF COMMERCE

1615 H Street, NW
Washington, DC 20062-2000
www.uschamber.com

Response to the Kingdom of Saudi Arabia's Public Consultation on *The Cybersecurity Regulatory Framework for the ICT Sector*

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 investors in the Saudi Arabian economy. We welcome the opportunity to provide comments to the Kingdom of Saudi Arabia Communications and Information Technology Commission's ("CITC") draft *Cybersecurity Regulatory Framework for the ICT Sector* ("the Framework").

The Chamber's *Project Security* initiative has worked collaboratively with more than 30 governments around the world to develop cybersecurity policies. Through our engagement with leading public and private experts, we have identified a series of principles that promote effective cybersecurity programs, while minimizing disruption to businesses, trade and the economy.

In particular, the Chamber encourages governments to take an approach which is:

- Flexible enough to keep pace with rapidly-evolving cyber threats;
- Risk-based, enabling organizations to tailor programs to their individual business structure, digital footprint and risk tolerance;
- Multi-stakeholder, to ensure that the expertise in government, industry and academia is leveraged and aligned; and
- International, to ensure that threat information can be shared globally and that organizations can deploy best-in-class practices seamlessly across borders.

The Chamber is greatly encouraged by CITC's references to best-in-class international standards, including *ISO/IEC 27001* and *National Institute of Standards & Technologies: Framework for Improving Critical Infrastructure Cybersecurity*. We also share the objectives outlined by CITC in the Framework. In particular:

- Increase the overall cybersecurity maturity level of the ICT sector;
- Define a comprehensive set of cybersecurity requirements that shall be implemented based on a risk-oriented approach; and
- Ensure confidentiality, integrity, and availability of the services provided to the customers.

We offer the following comments, however, in the belief that they will more effectively achieve these shared cybersecurity objectives. We thank you for the opportunity to comment on the draft Framework and look forward to working with you to develop an approach to cybersecurity that addresses cybersecurity needs while ensuring the continued growth of the Saudi economy.

Detailed Comments

Section	Concerns	Recommendation
3. Scope: "Without prejudice to the provisions of CITC regulations and other related regulations, the provisions of this Framework shall apply to licensed service providers." 4. Applicability: "This framework is applicable to all the LSPs and their subsidiaries, staff, third parties and customers."	A large number of companies are required to obtain a license from CITC for the provision of a broad range of communications services. Relatively few of these companies' operations represent a significant risk to the Kingdom's economic or national security if interrupted, yet each is treated equally from by the Framework. This runs counter to the principle of a risk-based approach, unnecessarily stretching the resources of both CITC, which must manage compliance, and its licensees. This challenge is further exacerbated by the language of the Applicability section, which extends compliance requirements to third parties and customers. Given the inter-	CITC should designate the Critical Information Infrastructure (CII) that falls within its regulatory domain, in line with international best practices. From a regulatory standpoint, the Framework should apply only to those companies operating CII, and remain voluntary for all other companies. This will ensure the appropriate allocation of finite private and public sector resources according to risk. Furthermore, we would welcome clarification from CITC that the scope of entities covered by the law – and thus subject to enforcement – does not extend to companies that

	connected nature of digital supply chains, this would not only represent a regulatory overreach by the CITC – pre-empting the ability of other agencies to regulate within their sector – the vast scope that it would create will make it near-impossible for CITC to manage compliance in a way that is fair and consistent.	are outside of regulatory domain (i.e. that are not CITC licensees).
5. Roles and Responsibilities Responsibilities of CITC: “Monitor and steer the LSPs compliance with the defined requirements through various ways, for example inspections of LSPs facilities, compliance workshops, active and reactive audits.”	Inspections and audits may be necessary on occasion to ensure compliance with the law. Governments should refrain, however, from overburdening companies with compliance. Finite resources that are utilized on compliance are drawn away from operational cybersecurity activities. Where inspections *are* necessary, strict guidelines should be put in place to ensure that regulators execute their work in a manner that does not lead to the interruption or	Self-certification mechanisms are a helpful tool for ensuring compliance, without overburdening companies with inspections and audits. We welcome references to self-certification later in this section. CITC should develop and make public clear guidelines which govern the conduct of CITC regulators when conducting audits and inspections including, where necessary, penalties for activities which cause harm or undermine trust in CITC among licensed entities.

	critical activities, cause damage to property or lead to the disclosure of sensitive information to third parties.	
6.1.5 CL 1 “Ensuring the hosting and storage site of the organization’s data is in the Kingdom of Saudi Arabia.”	The requirement to store data locally undermines CITC’s stated aim in issuing the Framework: to enhance the cybersecurity of Saudi Arabian industry. Cybersecurity threats are global in nature. It is therefore counter-productive to inhibit the ability of companies to respond in a cross-border manner. Companies transfer data across geographies and markets to aggregate and analyze threat information and tackle fraud, resulting in better cybersecurity outcomes. A requirement to store data locally will inhibit Saudi Arabia from access to global threat information sharing and, consequently, from best-in-class cybersecurity practices and services.	We strongly recommend that the CITC remove this provision from the Framework.

	When considering the security of data, the physical location is not of paramount importance. Security is a function of how a product is made, used, and maintained, not by whom or where it is made. The ability to store data in different geographic areas increases information security and mitigates the effects of potential cyber-attacks as security practices are better implemented by global teams. Conversely, by localizing and concentrating data in-country, data is more susceptible to breaches where local services offer weaker security measures, and thus present a more convenient target for theft. Overall, data localization increases the ‘attack surface’ for bad actors to target while decreasing the security of networks and systems by creating barriers to threat visibility, slowing response times when time is of the essence in preventing or containing attacks.	

	More broadly, data localization policies will negatively affect Saudi Arabia’s economic competitiveness. Businesses across all sectors and of all sizes rely on and benefit from the seamless flow of data into and out of the country.	
7. Regulatory Framework	While the majority of requirements listed are in line with cybersecurity best practices, the level of detail in which they are enumerated risks making the Framework outdated.	We suggest reducing the number and scope of requirements enumerated within the Framework. This will ensure that the document is flexible enough to remain relevant as the cyber threat landscape evolves, while enabling companies to assess the risks inherent to them and allocate resources accordingly.
7.1.8. “Ensure cybersecurity requirements related to human resources are addressed in case of any changes of their working relationship.”	The purpose of this requirement is unclear.	We would welcome further clarification as to what is required under this provision.

7.4.4. "Ensure security patches are applied to the information assets in an appropriate timeframe to fix known issues and enhance their resilience."	According to a recent study,[1] only 5.5% of known vulnerabilities have ever been used by hackers. In a situation of finite resources, cybersecurity practitioners must make determinations as to which vulnerabilities merit the cost and operational disruption to patch, particularly as this applies to SMEs. While most companies will choose to patch and update systems frequently and this is commonly deemed as a best practice, under certain circumstances they may determine via a risk assessment that the costs outweigh the benefits.	The language should be amended to such that it enables companies the flexibility to not implement a security patch where they deem the operational disruption to outweigh the risk of the vulnerability.
7.4.6. "Monitor and protect the event logs of the information assets and report any suspicious activities that need further investigation."	As part of routine monitoring of logs, "suspicious activities" may be identified regularly, raising a number of false positives that aren't obvious until further investigation. Requirements to report such	We would welcome clarification that the appearance of suspicious activity would not trigger any reporting requirements to regulators.

[1] Improving Vulnerability Remediation Through Better Exploit Prediction: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf

	incidents to regulators would trigger a large volume of information that will both impose an unnecessary burden on companies and overwhelm regulators with unhelpful information.	
7.4.13. "Implement baseline configuration settings to increase the resilience of the information assets."	The purpose of this requirement is unclear.	We would welcome further clarification as to what is required under this provision.
7.4.16. "Conduct penetration tests to evaluate the organization's defense capabilities and detect vulnerabilities."	Penetration testing is a valuable tool in developing an effective cybersecurity program. Yet its utility varies from organization to organization according to their risk profile. Mandating the use of penetration testing for all organizations will at best lead to wasted resources for some and, for others, may undermine the effectiveness of their cybersecurity programs. For many SMEs, requirements to conduct regular pen	We encourage CITC to remove the requirement for companies to conduct penetration tests. Instead CITC may make reference to penetration tests being a *potentially* valuable tool for organizations, as part of their cyber risk identification and protection processes.

	testing may consume their cybersecurity budgets, forcing them to remove resources from other important areas.	
Annex 1. Compliance Level "CITC will set a security target by defining three compliance levels following a risk based approach."	Given the asymmetry of information between company and regulator regarding the systems that a company operates and their potential risk in the event of disruption, regulators may make a determination, based upon incomplete information, that imposes unnecessary burdens upon a non-CII entity.	For those companies that are not owners or operators of Critical Information Infrastructure (as defined in our first comment), compliance levels should be determined by companies, based upon their determination of risk.
2.5.4 CL2 "Perform remote monitoring and tracking (e.g. using location tracking technologies) of the information assets and ensure that they are kept within the organization controlled areas."	This clause would be very difficult and costly to implement relative to the risk profile and the potential benefits it could bring. While it may be a valuable tool for some companies, for many others it would not.	We suggest that this clause be replaced with a recommendation to periodically track and account for all assets and regularly monitor critical assets to protect against their removal from organization controlled areas.