THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

US-China Business Council Comments on The Draft Cybersecurity Law

August 4, 2016

On behalf of the more than 200 members of the US-China Business Council (USCBC), we appreciate the opportunity to provide comments to the National People's Congress (NPC) on the latest draft of the Cybersecurity Law. Our member companies represent a wide variety of industries, including companies that sell and purchase information security products and services, as well as companies that operate and use information networks. These diverse members are united in their commitment to promoting and participating in an open, healthy commercial environment that supports China's development and promotes the use of information technology as a driver of economic growth.

USCBC and our members recognize that the drafting of this law reflects a desire by the Chinese government to promote information security and the lawful rights of Chinese citizens and organizations. Our companies share these goals, and have global expertise in working with governments and other industry players to achieve these objectives while promoting robust industry development. Many of our members have long offered high-quality information security products and services in China, contributing actively to the development of this industry.

We welcome the call in this draft for better international cooperation in cyberspace governance, the development of technology and cyberspace standards, and efforts to address criminal activity. We also welcome the encouragement of industry-led development of standards for cybersecurity, and appreciate that the definition of personal identifiable information (PII) was revised to exclude IP addresses.

It would be helpful for the draft to clarify and assure equal treatment of domestic and foreign enterprises, as was originally specified in the first reading of this draft (Section II of the explanatory note in the first reading). We also encourage China to leverage international standards and industry best practices in the implementation of this law, in ways that are not overly prescriptive to the detriment of international commerce.

As the NPC further revises this law, we encourage China to prioritize ensuring transparency in government processes, consistency with other Chinese laws and regulations, and uniform implementation across agencies. Additionally, we encourage the NPC to actively engage with industry, including foreign companies in relevant industries, throughout the remainder of the

drafting process for this law and for other relevant documents such as the cybersecurity strategy mentioned in Article 4. Follow up issues of great interest to industry include:

- The interaction between mandatory standards and the existing standards that have been developed by companies and used internationally (Article 10);
- The use of the term "secure and trusted" (Article 15);
- The development of the definition for the Cybersecurity Multi-Level Protection Scheme ("MLPS"; Article 20);
- Requirements on content retention logs (Article 20);
- The scope of reporting cyber incidents (Article 24);
- The definition and scope of critical information infrastructure ("CII"; Article 29) and network operators (Article 72);
- The certification, authentication, and testing processes, as well as the scope of critical network equipment and related products (Article 22, 33, and 72);
- The localization of data and questions relating to the free flow of information across borders (Article 35).

We recognize that the draft Cybersecurity Law is part of a broader emerging legal framework that includes the draft cybersecurity strategy, the Counterterror Law, and the National Security Law. USCBC encourages clarification of how the draft law will interact with these measures and existing laws and regulations, including but not limited to China's Criminal Law, the development of China's cybersecurity review regime, and the existing MLPS framework that was promulgated by the Ministry of Public Security in 2007.

USCBC appreciates the opportunity to offer additional comments on the draft law. We recommend clarification of some articles, as well as certain obligations imposed on companies and government agencies that may hinder the cybersecurity goals of the law. Addressing these concerns in a comprehensive manner will ensure China's information security by encouraging companies to deploy the best and most secure technology available in China.

Definitions and Scope of Coverage

Article 2 describes a broad mandate that the law applies to the construction, operation, maintenance, and usage of networks in China. Subsequent articles provide a variety of terms to clarify the law's scope, such as network operators, critical information infrastructure, and citizens' personal data. While Article 72 defines several key terms used throughout the law, questions remain about other definitions:

- **Critical information infrastructure** Article 29 states that priority protection will be given to "critical information infrastructure" (CII) and that the specific scope of CII will be developed by the State Council. Because this term is undefined and based on broad parameters including national security, the economy, people's livelihoods, and public interest, the range of industries affected could include a large number of information systems that may or may not be truly critical.

USCBC recommends that regulators clearly and narrowly define the scope of CII, so that it covers only infrastructure that is essential and specific to the performance of core functions. Without a narrowed scope, CII could encompass entire functions of the ICT sector, which creates enforcement and compliance challenges for companies and government agencies. Targeting finite enforcement and compliance resources will optimize efforts to meet China's cybersecurity goals.

We encourage regulators to work with companies, industry associations, international organizations, and other relevant stakeholders to clearly define CII. We recommend the State Council release a draft definition for public comment before finalizing, and delay implementation of the Cybersecurity Law until these parameters are clarified and published. We also recommend an additional definition for "critical information infrastructure operators" to clarify how these categories are used in other laws and regulations, such as "critical infrastructure" in the Public Security Law.

- **Secure and Trusted** Article 15 calls for the use of "secure and trusted" network services and products, without defining the term. Because of its similarity to the term "secure and controllable," which has already concerned foreign stakeholders, USCBC recommends regulators clearly define this phrase through collaboration with foreign and domestic industry to develop an objective, transparent, fair, and technically based standard. We further recommend that any definition reflect bilateral commitments that technology security not be linked to product nationality, but rather via technological assessments of security functions and processes.

  USCBC understands that the National Information Security Standardization Technical Committee (TC260) under the Cyberspace Administration of China (CAC) is working on standards related to secure and controllable technology. We encourage regulators to continue working with foreign companies and stakeholders to develop standards that make use of international best practices and security standards, and to ensure the healthy development of China's domestic cyber environment.

- **Multi-Level Protection Scheme** Article 20 states that China will introduce a cybersecurity multi-level protection scheme (CMLPS), and includes obligations to protect networks from interference, unauthorized access, or other types of disruptions, divulgence of information, or theft. It is unclear how this tiered system might relate to existing schemes, such as the 2007 MLPS scheme that impacts how technology-based products can be certified and sold in China. USCBC asks that regulators clarify how the CMLPS within this draft law will interact with the existing MLPS scheme — such as whether this will upgrade, complement, replace, or be integrated with the existing MLPS framework.

  China's existing MLPS framework has previously raised foreign companies' concerns because of discriminatory provisions that require companies to locally register intellectual property (IP) and turn over sensitive source code. If the CMLPS scheme under the draft Cybersecurity Law will be integrated with the existing MLPS framework,

USCBC encourages regulators to remove discriminatory language prohibiting the use of foreign products handling data classified as "Level 3" or above.

We recommend that China's MLPS structures be integrated to increase clarity, reduce regulatory burdens, and ensure fair treatment between foreign and domestic players. We also recommend that measures developed by the State Council in this area be aligned with other government security initiatives.

- **Network operators**: Article 72(3) defines network operators as the "owners and administrators of networks, and network service providers." USCBC appreciates that this scope has been simplified since the first reading of the law, but we remain concerned that this broad definition could include any company using telecommunications or internet services. This could include companies operating noncommercial websites that provide company information or promote offline business. Such sites are less vulnerable than the networks on which they operate. Applying every obligation of a network operator to these companies would significantly raise costs and licensing hurdles, ultimately limiting their ability to serve their customers through the internet.

  Additionally, the law as written could apply these obligations to internal corporate IT networks, which could require companies to monitor employees' personal activity on their official networks and raise privacy issues.

  We recommend clarifying the definition of "network operators" to specify telecommunications, internet, network hardware, and network software providers that construct, operate, and maintain networks within China, and narrowing the scope to public networks available to end-users. This definition should exclude noncommercial websites and networks (including internal corporate IT networks). Additionally, we recommend that the definition be revised to be consistent with other regulations, such as the Administrative Rules on Internet Information Services.

- **Mandatory Cybersecurity Standards** Article 10 sets compliance requirements with mandatory national standards. Mandatory cybersecurity standards should not require disclosure of source code, use of local encryption standards, or other burdens that would compromise IP usage and protection. USCBC recommends that more consideration be given to voluntary global standards and best practices, which have been developed after years of testing by and consultation with international experts. These requirements should not constrain foreign companies from deploying their existing global security measures for the benefit of their China-based users, networks, operations, and customers.

- **'Personal' and 'Important Business Data' and Cross-Border Security Audits**: Article 35 states that CII operators must store citizens' personal information and "important business data" within the Chinese mainland, and that this data may only leave the country after a security audit.

Article 72(5) broadly defines personal data, with provisions that include "other information (that can be used) to identify the personal identity of citizens." We recommend that definition be clarified so companies can ensure compliance. USCBC also recommends clarifying how provisions within this law related to personal data interact with other similar provisions in other laws and regulations, such as privacy provisions in the Consumer Rights Law, the Ninth Amendment to the Criminal Law, and the 2015 Measures for Penalties for Infringing upon the Rights and Interests of Consumers from the State Administration of Industry and Commerce (SAIC).

The draft law also does not define the scope of "important business data." So that companies can comply with these provisions, USCBC recommends that regulators clarify and narrowly define "important business data" according to considerations strictly related to national security, and independent of commercial or economic considerations.

USCBC also recommends that regulators clarify how security audits for data flows will interact with existing restrictions governing the flow of data overseas, and provide details on relevant specifications, certification or authentication processes, or other procedures that must be completed in order to qualify. To ensure conformity with global best practice and smooth integration between China and the rest of the global digital economy, we recommend that implementation of this law be delayed until these specifics are published to allow domestic and foreign stakeholders to offer comments and recommendations.

- **Other items** A number of other terms remain undefined, including "active utilization" in Article 3; "Internet-related industry associations" in Article 11; "network products, operations, and services" in Article 14; "users," a term used throughout the document which could refer to governments, corporate entities, or individuals; "network security incidents" in Article 24; as well as "providers of electronic messages and application software," "electronic messaging service providers," and "software download service providers" in Article 46. We recommend that these terms be clearly defined based on consultation with foreign and domestic stakeholders.

Certification of Information Security Products

Article 22 states that "critical" network equipment and "dedicated" network security products must go through a security inspection and certification process before they can be sold in China, based on a catalogue of such products. Article 33 further requires that such products undergo an additional security inspection when they are purchased by CII operators. Neither article, however, provides detail on how such processes will work, or how they might interact with each other.

This raises a number of concerns. First, there are significant questions about both processes, particularly if they require companies to disclose source code or use local encryption algorithms. Although the draft law does not detail the certification process, other recent Chinese policies have raised similar concerns, such as the suspended China Banking Regulatory Commission's Guidelines on Promoting the Application of Secure and Controllable Information Technology in

the Banking Industry (2014-2015). These types of requirements put companies' core intellectual property at risk, endangering their competitiveness and their ability to innovate. In addition, such a certification process would be redundant, as Article 10 already requires these products and services to comply with relevant national and industry standards.

Second, provisions in Article 33 requiring the purchaser to undergo a security check when buying network products and services will create challenges for companies and government agencies. Purchasing firms frequently do not have access to the source code and intellectual property of products sourced from technology firms, making it difficult to comply with Article 33. In sectors such as financial services, compliance requirements in international markets sometimes bar them from making these kinds of disclosures. Both Chinese and foreign firms in this sector would be unable to comply with the requirements in the current draft law without violating international regulations.

Third, the provision does not define "critical" or "dedicated," and gives little guidance as to what types of products will be included in the catalogue, creating uncertainties for companies faced with determining whether their products are covered.

Companies already subject their products to vigorous security testing and certification processes based on international requirements and standards in global markets. Requiring companies to undergo a state-sponsored security review and choose hardware, software or services based on parameters that foreign companies may not be able to meet will limit the security of domestic company networks in China by preventing them from using the best products.

Furthermore, forcing companies to select from pre-approved, China-specific technology equipment or solutions, rather than allowing them to use the technologies they have already employed in their global networks, may disrupt or weaken companies' security operations within China. For example, if data leakage or theft occurs on an isolated, China-based network that global monitoring systems cannot quickly detect because of network incompatibility, this could seriously undermine the speed of the company's response, its ability to contain the data leakage, and the promptness of its customer alerts. Such consequences work against China's overall goal of improving IT security.

We recommend that Articles 22 and 33 be removed entirely, or edited to provide significantly more detail about the scope and processes described in these articles. If these articles are revised, we also recommend that new language explicitly states that qualified private institutions, including foreign institutions, will be permitted to certify products to meet these standards, and that government and private institutions should strive for uniform implementation of certification and inspection standards and procedures.

Cross-border data flows

Article 35 requires CII operators to store citizens' personal and other important data within China's borders, and to store or provide the information to those outside of China only after a security assessment. Local data storage and transfer requirements impede the development of China's IT sector by isolating Chinese companies from the best data-related technology and

business expertise. Not only do such restrictions present obstacles to China's integration with the global information and communications technology (ICT) ecosystem, they may also negatively impact Chinese government policy goals such as promotion of cloud-based services or smart technologies.

Data localization requirements threaten to increase costs and regulatory hurdles for companies operating in China without increasing data security. Due to the development of data storage and retrieval techniques, limiting the physical location where data can be stored does not decrease the risk of data breaches from outside of China, but it does limit the ability of foreign companies to employ globally unified IT security systems. System uniformity is important in ensuring day-to-day functionality of global operations, and is essential to global monitoring networks that identify security breaches, data leaks, theft, or other instances of criminal or unwanted behavior. Data localization would require companies to employ local IT solutions that may not be immediately or fully compatible with companies' global network security frameworks. Using solutions that are out of sync with global security networks would create security vulnerabilities specifically for data that has been collected in China, thereby working against the information security goals of this draft document.

Restrictions on cross-border data flows are more troubling; such flows are critical to the growth of the global digital economy that supports the development of the information industry as well as economic development in general. Mandating security audits before data moves overseas may limit security processes and thereby inhibit security. For example, a Chinese customer seeking to verify a transaction at an international branch of a Chinese bank who voluntarily transmits personal information, or a Chinese citizen who exchanges information with family and friends in other countries could be covered by this provision and required to obtain a security assessment for each instance—even if the customer gives consent in advance. The provision limiting data flows also raises other questions, including the definition of CII operators; the types of data that could be covered, such as proprietary business information or human resources data; details of the security assessment required to request an exemption; and the scope of the requirement, such as whether it would only apply to newly collected data or retroactively apply to existing data.

USCBC strongly recommends that Article 35 be revised in close consultation with industry stakeholders to ensure that attempts to regulate data flows are done with consideration of security and practical business needs. Open discussion on this issue will help ensure China meets its cybersecurity needs, while simultaneously fostering the sustainable development of its ICT sector.

Cybersecurity Standards

USCBC appreciates the specific language in Article 14 encouraging enterprises to participate in the development of national and industry cybersecurity standards. Active, open engagement with industry in the development of standards is the best way to ensure that those standards are comprehensive, achievable, and widely accepted. Draft technology security standards should reflect bilateral commitments that technology security will not be linked to product nationality, but rather technological assessments of security functions and processes. We encourage the Chinese government to ensure transparency in standard-setting, and recommend adding a

sentence to Article 14 to clarify that "domestic, foreign-invested, and foreign enterprises are eligible to participate in these standard-setting activities."

Additionally, we strongly encourage language throughout the law mandating harmonization with international standards and best practices wherever possible. Greater consistency with international standards would serve the needs of Chinese customers, by giving them the widest array of choices to protect cybersecurity, and Chinese companies, by allowing them easier access to the global marketplace. Conversely, China-specific standards in these areas could undermine the goals of the draft law by slowing industry's ability to respond to evolving cyber threats. Provisions where such language would be most appropriate include Articles 10, 14, 21, and 22.

Network Operator Obligations and Liabilities
The draft law addresses obligations for network operators, as well as liability for operators that do not comply with the law's provisions.

- **Article 20(3)** requires network operators to keep network logs for six months. The scope of "network logs" is very broad and can vary in content from recording users who logged into a network or device, to what connections were allowed or denied based on the access control lists, to logging every packet of every session. To ease the operational burden of compliance, USCBC recommends that this law be clarified with language stating companies must keep "network logs directly related to security incidents."

- **Article 21** requires that network products and services comply with relevant standards and requires companies to promptly notify users when information is collected or when they discover potential security risks. The article also requires them to provide security maintenance for products and services within the contract period, but does not indicate whether the company is obligated to do so if the contract is terminated early or is breached by the other party. Additionally, it leaves a number of key questions unaddressed, including how companies should obtain consent from users or whether companies would be liable if a third party alters the products or installs them incorrectly. We recommend new language be added to this provision to address these specific concerns.

- **Articles 21, 24, 41, 53, and 58** require network operators that discover security risks or network intrusions to "promptly" address issues and inform users as well as provide information to government entities. The law does not define "promptly." Given language in Chapter VI that defines legal liabilities when companies do not meet these provisions, this lack of clarity is a significant concern. When there is a security risk, companies often develop remedial measures before informing users to prevent the knowledge of an exploitable vulnerability from spreading before legitimate users can be protected. We recommend that the word "promptly" be replaced with "as soon as is practicable when the operator is made aware of the threat."

- **Articles 21 and 46** prohibit malicious programs that are either installed by network product and service providers or included among information sent by application

software providers. Both articles raise questions about whether companies are liable if they are unaware of such programs because they have been installed by third parties or rogue employees. We recommend that new language be added to both articles to state that "providers of software applications shall not *intentionally* distribute software containing malicious programs," or to state that providers should take reasonable precautions to prevent the distribution of software containing malicious programs.

- **Article 23** mandates that network operators conducting key services require users to provide real identity information, and prohibits them from providing services otherwise. Such requirements may conflict with broader Chinese goals of protecting user privacy and security, while also creating significant challenges for network operators. In addition, such a requirement is unduly burdensome for companies to enforce, particularly in cases where users present fabricated identification to service providers who are unaware.

  These requirements could also heighten the risk created by any individual network incident by increasing the cache of citizens' personal data available to an attacker. For these reasons, we encourage the NPC to engage stakeholders to revise these requirements in accordance with international best practices. USCBC also recommends regulators specify which types of services require the verification of real name identification beyond "information posting" and "instant messaging" services.

- **Article 25** states that relevant provisions must be followed when a network operator conducts a certification/assessment and unveils vulnerabilities. In standard practice, such vulnerabilities would be corrected as part of the certification/assessment. USCBC recommends drafters provide further clarification of "relevant provisions" with specific examples of those applicable under Article 25.

- **Articles 27 and 47** allows government entities conducting security or criminal investigations to request the technical support and assistance of network operators, but provides no further detail on the scope of assistance that companies can or should provide. USCBC recommends that the responsibilities of network operators in these circumstances be clearly defined to include activities, information, or documentation that network operators would be expected to provide under these circumstances.

- **Articles 32 and 36** should also be revised to incorporate new language stating that government reporting and inspections should strive to minimize the negative impact on network function, that government agencies conducting these activities should protect proprietary information, trade secrets, and intellectual property, and that these activities are subject to government oversight. We recommend new language be added to hold accountable any officials that fail to protect trade secrets, confidential information, or citizens' personal data as required under the revised Articles 32, 36, and 43.

- **Article 34** requires CII operators to sign agreements with equipment providers to clarify responsibilities for security and confidentiality. However, the scope of these agreements is unclear, making it difficult for network providers and equipment providers to ensure

compliance. We recommend that the Chinese government release more details about such agreements or a template of how such an agreement would be structured.

- **Articles 39-48** discuss privacy obligations for network operators, including how they should handle personal information, protect privacy, and address actual or potential information leaks. These provisions are described as broad principles. USCBC recommends that language be added to clarify the obligations of network operators or other businesses handling personal data, and reference which privacy rules are applicable. Additionally, we encourage China to consider international best practices, including the APEC Privacy Framework, which provides an effective foundation for creating a formal data protection system.

  Article 43 forbids the illegal selling of personal information. We recommend that this article define the difference between "legal" disclosure to third parties and "illegal" disclosure. Clearer guidance will ensure that companies properly understand how some important business functions—such as consumer analytics, online advertising, or analyzing personal information to tailor services and products to certain consumer bases—will be treated under these provisions.

- **Articles 45 and 48** require network operators to halt transmission of information published by users under specific circumstances. This raises two questions: first, the ability of an operator to halt transmission often depends on the way the information is released by users. For example, information posted to a website is transmitted differently from information sent via a social media platform. We encourage the NPC to engage directly with network operators to revise Article 45 to ensure reasonable standards for handling such information. Second, government direction to halt transmission of such information can create potential liability for companies unless they are protected against action from the affected user. As such, we recommend new language be added to Article 45 protecting network operators from such liability.

- **Article 51** calls for the creation of a cybersecurity risk assessment and emergency response mechanism to develop cybersecurity emergency response plans to be tailored to different industries and sectors. USCBC recommends that state-level cyberspace administration officials work with foreign and domestic industry to leverage their commercial perspectives and technical know-how. USCBC recommends the adoption of a common framework to ensure uniformity among sectors, which will ease implementation of these plans by companies with cross-industry businesses.

- **Article 56** authorizes government agencies to enact temporary measures related to network communications in order to protect national security and public order during "major social security incidents." The provision does not clarify what might constitute such an incident, nor does it specify what types of measures can be taken and for how long. Such a lack of clarity raises major questions for government agencies that might invoke this authority, as well as network operators who need to understand how such restrictions might impact their operations. We recommend new language be added to

define the scope and types of measures that can be taken, the permissible duration of such measures, and requirements by which governments exercising this authority provide justification.

Network Vulnerability Testing

Articles 26 and 36 contain contradictory language regarding network vulnerability testing. Article 36 states that CII operators should inspect and assess their networks' security at least once a year, either personally or by retaining a specialized institution. This language appears to allow companies to hire outside experts to assess their system through tools such as vulnerability scans and internal security penetration tests. However, Article 26 prohibits any form of network intrusions, thus restricting companies from engaging in behavior that Article 36 seems to encourage as a way of enhancing network security. This contradiction could lead companies to determine that even authorized vulnerability scans are prohibited, limiting their ability to guarantee the safety of their networks—and undermining the broader goals of this law.

We recommend revising Article 26 to state that "individuals or organizations must not engage in network intrusions or interfere with the ordinary function of other networks, steal network data, or engage in other activities harmful to network security unless authorized by the network's operator as part of a security assessment; they must not provide either the tools or methods for creating network intrusions, interfering with the ordinary function of networks or stealing network data or other activities harmful to network security unless authorized by the network's operator as part of a security assessment; they must not intentionally provide assistance such as technical support, advertising/promotion, or financial support to others that is aimed at engaging in activities that undermine cybersecurity." Such focused language would give companies the freedom to regularly assess their network vulnerabilities, while maintaining the essence of the original provision's goal of preventing cyber-based criminal activity.

Conclusion

USCBC thanks the National People's Congress for providing this opportunity to comment on the draft Cybersecurity Law. We hope that these comments are constructive and useful to the National People's Congress Legislative Affairs Commission as it reviews the draft measures. We welcome the opportunity to continue to discuss these points in the future.

—END—

The US-China Business Council
Contact: Jacob Parker, Vice President for China Operations
Tel: 010-6592-0727 Fax: 010-6512-5854
E-mail: jparker@uschina.org.cn