Comments on CBRC Draft Regulations Affecting Technology Purchases

14 September 2015

Introduction

The American Chamber of Commerce in China, American Chamber of Commerce in Shanghai, Asia Securities Industry & Financial Markets Association (ASIFMA), BSA | The Software Alliance (BSA), Canada-China Business Council, European Banking Federation (EBF), Financial Services Forum (FSF), Information Technology Industry Council (ITI), International Swaps and Derivatives Association (ISDA), Japan Electronics and Information Technology Industries Association (JEITA), Securities Industry and Financial Markets Association (SIFMA), Semiconductor Industry Association (SIA), Software and Information Industry Association (SIIA), Transatlantic Business Council (TABC), United States Information Technology Office (USITO), US Chamber of Commerce, US-China Business Council (USCBC), US Council for International Business (USCIB) and their member companies appreciate the opportunity to offer input on technology regulations affecting banks operating in China and thank the China Banking Regulatory Commission (CBRC) for considering revisions to these policies.
Our organizations represent companies from Asia, Europe and the North America and engage in business across all industry sectors in China. Among our members are both financial institutions and global technology and innovation leaders. These companies have made significant investments in China that have contributed greatly to China's economic and technological development over the past three decades.

Chinese companies have developed many world class technologies and its policymakers have an important role to play in the global discussion of cybersecurity. Our organizations support China's desire to create a secure operating environment for banks. Incidents that disrupt the integrity of banking infrastructure not only impact individual bank operations, but also undermine the confidence of consumers and investors, and threaten the stability of global financial systems. As a consequence, effectively addressing cyber risks in the banking sector is critical to maintaining public confidence and mitigating financial risks. We hope this submission will help achieve those shared goals for effective security.

In recognition of the potential impact of cyber intrusions on the broader economy, global banking regulators and the international financial sector have established a variety of mechanisms to mitigate potential risks and collaborate on ways to protect the systems they oversee from being disrupted. Underpinning these is a set of important principles which are essential to the formation of effective policy on cybersecurity. We strongly encourage China to implement a prudential regulatory framework which reflects these principles, allowing appropriate industry-level benchmarking and avoiding the pitfalls associated with mandating prescriptive mechanisms of technology and cybersecurity standard-setting. Using these internationally recognized approaches will also help ensure consistent global practices in this important area.

Global Cybersecurity Environment

There are two crucial issues that must be recognized at the outset before principles for effective policymaking can be established.

First, cybersecurity is a global issue and it requires global solutions to be truly effective. Global systems play an important role for financial institutions to promote security. Cyber risks transcend national borders, so countries – through their governments and private sector institutions – need to work together to develop safeguards that protect the integrity of global markets.

As a consequence, the financial sector is subject to a significant and diverse number of laws, regulations and examination standards related to cybersecurity that, together, broadly reflect an emerging international consensus regarding what is most effective. And, in some instances, standards are being established at the international level itself. For example, the Payment Card Industry Data Security Standard (PCI-DSS) is a global industry standard setting security requirement for all payment card systems used by financial institutions. Thus, the use of internationally accepted cybersecurity standards can minimize the risks for global financial networks by ensuring that best practices are widely implemented. Use of such standards also avoids the insurmountable challenge of asking international firms with global platforms to comply with conflicting rules and regulations between markets. To that end, we urge the CBRC to consult with other national regulators for rules that avoid exclusive use of localized solutions, prescriptive technologies and restrictions on data flows.

The international perspective is, for example, crucial in governing policy decisions on encryption standards. In particular, the use of local encryption standards which may not be consistent with international practices would raise security concerns for companies and international regulators. Leveraging internationally accepted approaches to encryption – such as used in Singapore and the United Kingdom, for example - minimizes conflicts across systems in different countries and ensures that client data is as well protected as possible – something that globally recognized industry regulations require as well. A comprehensive global approach will ensure that companies based in China are better able to compete globally.

Similarly, requirements to disclose source code are problematic in a globalized economy which is one reason they are not a feature of prevailing rules and regulations in other markets. Internationally-accepted standards on software and Intellectual Property (IP) licensing typically preclude banks from disclosing or holding third party IP in escrow without permission from the owners (or licensors) of that IP. Such disclosure would expose firms to unquantifiable financial risk from litigation and IP actions by software and IP licensors for breach of standard controls and contractual provisions protecting supplier IP.

Second, cybersecurity risks and the technology that mitigate them shift faster than regulations and standards can respond. As a consequence, policies that require specific technology requirements, detailed technical reviews or other processes by regulators will be reactive to the environment and to adversaries that seek to take advantage of vulnerabilities. In addition, written regulations and prescriptive standards become quickly outdated as cyber risks and the technology to address them evolve and create an obstacle to protecting financial institutions and their clients. As recognized by the approaches taken by policymakers in a number of markets, effective

regulations go beyond assessing whether an institution is **compliant** with a particular standard and instead ensure that sufficient people, processes, and technology are in place to **manage risks**.

General Principles for Enhancing IT Security in Banking Sector

Given the global and constantly evolving nature of banking technology, we encourage China to base its regulations on the following high-level principles for workable and effective cybersecurity policies.

- **Transparency** in the policymaking process – together with **sufficient time for consultation** with industry on proposed approaches – will help address and resolve complex and challenging policy issues. CBRC's request for input on its policy revisions is a welcome confirmation of China's intent to do that. We encourage CBRC to release its revised regulations in draft form prior to implementation so that banks, technology companies and other interested parties can have an opportunity to provide formal feedback.

- Given the growing and evolving nature of cyber threats, policies need to be **flexible and adaptable** to confront emerging threats while enabling companies to continue to innovate. It is important for regulators to avoid a "one size fits all" approach in developing IT security guidelines in the banking sector. Policies should be flexible to accommodate different approaches to address cybersecurity risks. Banks face unique risks and cyber threats, so cybersecurity guidelines should enable firms to choose specific technology solutions to meet their unique needs and ensure the integrity of global financial networks. Regulations that call for specific technologies will never be able to keep pace with innovation and the creation of new solutions driven by the needs of the market and the evolution of the threats the financial sector faces. Regulators should not limit the options that are available for firms to protect themselves and their clients.

- Take a **risk-based approach to examining whole systems** for cyber threats to foster a prudential regulatory framework that can be more efficient and more effective than focusing on individual functions or processes. Banking institutions make significant investments to protect client data and to limit disruption and preserve the integrity of data processing from those who seek to attack corporate networks. To do so, international banks leverage global platforms to limit the number of attack surfaces to ensure the highest level of security possible for their customers. This enables banks to maximize system security, efficiency and interoperability across their operations around the world. In policy terms, for example, requiring the use of specific domestic technologies or processes - without regard to industry best practices and already established global platforms and investments - runs counter to international norms, which base technology decisions on holistic assessments of risk.

- Reliance on **global security standards** based on consensus industry processes will ensure that the best practices from around the world are incorporated and that security requirements will be regularly updated to respond to evolving threats.

- There is an important role for **market-based approaches** that achieve desirable outcomes. Regulators in major economies work closely with banks and their counterparts in other markets to help achieve those goals sustainably and mindful of both the local and international context. To do so, they use a successful approach of empowering private financial institutions to implement risk-based cybersecurity policies and protections that are specific to their individual circumstances. In addition, regulators have established standards to enable individual institutions to continually evaluate the risks faced by their networks and respond appropriately based on those needs. Network security is an ongoing process, so effective cyber policies must enable financial institutions to respond rapidly to constantly changing threats and use the most appropriate and innovative technologies for their unique business circumstances. Coordination between regulators and banks creates an environment that meets the needs of all sides.

Several regulatory authorities around the world have incorporated these principles in their domestic bank technology requirements. For example Canada, Germany, Hong Kong, Singapore, the United Kingdom and the United States have successfully adopted risk based approaches that focus on whole systems.

Conclusion

The best approach for developing technology policies is open and transparent formulation and implementation, which allows stakeholders to provide helpful input to regulators. This helps ensure that the resulting regulations are effective, compatible with global norms, and unlikely to cause unintended consequences. In particular, effective prudential frameworks and policies must allow companies to conduct their own risk assessments and determine what technology best meets their security needs.

As a consequence, we respectfully urge CBRC to base its revised regulation on the internationally accepted principles that other banking regulators have used as described above to ensure that financial systems in China and around the world address the risks that may cause the most harm and are as secure as possible.

—END—

Local Contacts:

AmCham China, US Chamber of Commerce (USCC)
Contact Person: Ian Curtiss, Senior Manager for Policy Initiatives
Phone: 8610 8519-0854
Email: icurtiss@amchamchina.org

AmCham Shanghai
Contact Person: Veomayoury Baccam, Director, Government Relations
Phone: +86.21.6279-8066
Email: v.baccam@amcham-shanghai.org

Asia Securities Industry and Financial Markets Association (ASIFMA)
Contact Person: Rebecca Terner Lentchner, Executive Director – Head of Policy and Regulatory Affairs
Phone: +852.2531.6560
Email: RTernerLentchner@asifma.org

BSA | The Software Alliance
Contact Person: Jared Ragland, Director, Policy - APAC
Phone: +65 6262 9609
Email: jaredr@bsa.org

Canada-China Business Council (CCBC)
Contact Person: Travis Joern, Managing Director
Phone: +86-21-6236-6370, x808
Email: travis@ccbc.com.cn

European Banking Federation (EBF)
Contact Person: Sebastien de Brouwer, Executive Director, Retail Financial services, Legal, Economic and Social Affairs
Phone: +32 2 508 37 65
E-mail: S.deBrouwer@ebf-fbe.eu

Financial Services Forum (FSF)
Contact Person: John Dearie, Acting Chief Executive Officer
Phone: 1-202-457-8761
Email: john.dearie@financialservicesforum.org

International Swaps & Derivatives Association (ISDA)
Contact Person: Donna Chan, Communications Director, Asia Pacific
Phone: +852 2200 5906
Email: dchan@isda.org

Japan External Trade Organization of Beijing Office (JEITA Beijing Office)
Contact Person: Mengyun Hu, Senior Assistant
Phone: 010-6513-9015
Fax: 010-6513-7079
E-mail: Mengyun_Hu@jetro.go.jp

Securities Industry & Financial Markets Association (SIFMA)
Contact Person: Peter Matheson, Managing Director, International Policy
Phone: 1-202-962-7324
Fax: 1-202-962-7305
E-mail: pmatheson@sifma.org

US-China Business Council (USCBC)
Contact Person: Jake Laband, Manager, Business Advisory Services

Phone: 010-6592-0727
Fax: 010-6512-5854
E-mail: jlaband@uschina.org.cn

US-Council for International Business (USCIB)
Contact Person: Barbara Wanner, Vice President, ICT Policy
Phone: 1-202-617-3155
Email: bwanner@uscib.org

USITO Associations (ITI, SIA, SIIA, USITO)
Contact Person: GU Xiyun, Policy Manager (*顾希韫*）
Phone: 156-1896-5695
Fax: 010-8429-9075
Email: xgu@usito.org