November 2012

China's Cloud Computing Policies and Implications for Foreign Industry

EXECUTIVE SUMMARY

Cloud computing is one of the hottest topics in China's information technology space today, particularly for companies engaged in IT and telecom products and services for both the commercial and public sectors, but also for a growing number of industry sectors expanding into e-commerce and Internet-based services. While there is much discussion about the potential role of cloud computing technologies and services in stimulating economic development and addressing challenges in healthcare, education, environment and energy efficiency, cloud computing technology poses unique challenges for China's regulators, particularly in the areas of information security, privacy, cross-border data flows, and information control.

In particular, China's overall regulatory approach presents significant challenges to the development of cloud computing. For one, China's preference for top-down mandatory regulation is often at odds with the type of public-private collaboration and industry self-regulation so critical to growing new technologies. Second, data protection and data sovereignty fears, as well as cybersecurity concerns, are creating barriers for deployment of leading global technologies. Further complicating the policy environment is China's drive to promote domestic industry, as well as preserve its existing market access controls.

Foreign technology companies are keen to identify opportunities in the cloud computing market in China, and are closely monitoring the development of the domestic cloud computing industry. But despite China's designation of cloud computing as one of the seven "strategic and emerging industries" in the 12th Five-Year Plan, some of the world's largest cloud computing service providers remain barred from the market, and others face a number of challenges in specific areas, including:

- Opaque and confusing market entry restrictions, including equity caps and restrictions on value-added telecommunication services;

- Hardware and software import and procurement restrictions, including information security restrictions;

- National technical standards that often diverge from global standards;

- Internet content restrictions; and

- Privacy and cross-border data flow restrictions.

This paper provides an overview and preliminary analysis of government plans for developing the cloud computing industry in China, as well as laws and regulations affecting foreign companies' ability to compete in this emerging space. It also includes an overview of the government and commercial authorities involved in cloud computing industrial development and policy-making.

STATE SUPPORT FOR THE CLOUD COMPUTING INDUSTRY

Cloud computing has been designated as a Strategic and Emerging Industry ("SEI", under the category of Next-Generation IT) in China's 12th Five-Year Plan. As with many of China's top technology initiatives, China's central government authorities aim to guide the development of cloud computing policy and standards in a coordinated, top-down fashion to promote local companies and technology. Examples include:

- **NDRC Cloud Computing Cities:** In October 2010, the NDRC and MIIT released nationwide plans for cloud computing pilot projects in five cities: Beijing, Shanghai, Hangzhou, Shenzhen, and Wuxi. Other cities have also followed suit to fund cloud computing infrastructure and technology development.[1]

- **National Supercomputing Centers:** China is constructing national supercomputing centers to support cloud computing, engaging in various aspects of computing, chip development, processing, and software research and development. The four completed centers to date are in Shenzhen, Jinan, Changsha, and Tianjin.

- **Cloud Experts' Committee:** On September 19th, the National Development and Reform Commission (NDRC), China's top macroeconomic planning authority, held the first "Cloud Computing Guiding Documents Drafting Experts Committee"[2] meeting in Beijing. This new group, administered by NDRC and led by a prominent member of China's academic community, could potentially wield considerable influence in the overall development of this industry in China.[3]

While this level of central government support clearly raises the profile of cloud computing, it should be noted that such top-down approaches often fail to achieve desired objectives, especially in the ICT space. Examples include the WAPI security algorithm and EUHT wireless standards. Such approaches have also led to rigid technical standards and discrimination against foreign technology.

CLOUD COMPUTING POLICY CONCERNS

The provision of cloud computing services in China is limited by both long-standing policies and emerging technical regulations and standards that apply to various aspects of cloud computing. Moreover, as cloud computing policies and technical standards evolve, there are a number of areas in which government regulation could further limit innovation and deployment of cloud computing in China.

The following is an initial analysis of policies that directly or indirectly affect foreign companies' provision of cloud computing services in China.

Equity Caps and Restrictions on Value-Added Telecom Services
Telecom Law[4]*:* China limits foreign direct investment in telecommunications to 49 percent for basic services and 50 percent for value-added services (VAS). Furthermore, joint venture

---

[1] Please see Appendix III: NDRC/MIIT Cloud Pilot Cities Supplement for more information.

[2] In Chinese: 云计算指导性文件起草专家组. Please see the NDRC website for this announcement (in Chinese): http://gjss.ndrc.gov.cn/gzdt/t20120926_506666.htm. Participants included officials from the NDRC High-Tech Department, MIIT Planning Department, and 25 additional cloud computing subject matter experts. The group is led by Beijing Aeronautics University President and Chinese Academy of Sciences Academician Huai Jinpeng. According to the announcement, the purpose of this experts' group is to 'lead and promote the healthy and orderly development of China's cloud computing industry'.

[3] NDRC has also set up similar groups for other sub-sectors, such as Internet of Things, which have made little impact on the industry to date.

[4] China's *Telecom Ordinance* can be found at http://www.miit.gov.cn/n11293472/n11294912/n11296257/11937080.html.

partners for foreign telecom service providers are limited to the three incumbent state-owned telecom providers.

The *Telecom Services Categories Catalog,* a document last released in 2003 and currently undergoing revision by MIIT Telecommunication Administration Bureau (TAB), defines basic- and value-added telecom services[5]. Earlier this year, TAB was engaged in research regarding the status of IaaS cloud computing as a value-added telecom service, although no formal pronouncements or decisions have been made to date. Across broader Internet policy, Chinese authorities are incorporating new technology applications, such as microblogs, BBS, and smart phone applications, into existing regulatory frameworks. Currently, some backbone PaaS services[6] accessible in other markets are not accessible in China partially due to equity caps in this sector.

Internet Content Provider (ICP): The ICP license, issued by MIIT only to domestic companies, is required for any company providing content or services over the Internet that are hosted in China. Only licensed ICP holders may sell online advertising (issuing corresponding tax receipts), publish content online, and host Internet content for content providers, e-commerce, or other online applications. Data centers in China are required to host only those sites with a registered ICP license. While many Internet sites in China have foreign investors, uncertainty regarding the legal structures of foreign-invested Internet companies and lack of transparency regarding the approval process present significant risk and challenges.[7]

Internet Service Provider (ISP): ISP is a value-added telecommunications business operation license issued by Communication Administration offices. MIIT has not approved any entities to provide Internet services aside from the country's major carriers.

Hardware and Software Import and Procurement Restrictions

Security is an important consideration for any user deploying cloud computing services. Both new and existing cloud computing security regulations will impact market access for companies in this sector.

The most concrete example of this is the *Multi-Level Protection Scheme (MLPS).* MLPS stipulates that any critical infrastructure information system classified at Level-3 and above must procure domestic information security products. Information systems from key industries are included in the scope of MLPS, including finance, education, transportation, and healthcare. Companies hoping to provide hardware (servers, routers, etc.) or software (databases, storage OS, etc.) to cloud computing systems, especially those products containing encryption, are subject to these regulations.

MLPS also ties in closely with other key information security policies, including the *Commercial Encryption Regulations,* which regulate the import, development, and sale of encryption products, and China Compulsory Certificate for Information Security Products (CCCi), which outlines conformity assessment requirements for 13 categories of information security products for the government procurement market. These policies require cloud-based solutions for storing/protecting data as well as cloud security software and services to

---

[5] China's Telecom Services Categories Catalog can be found at http://www.china.com.cn/chinese/PI-c/300857.htm.

[6] For example, Amazon Web Services (AWS). Others, such as Microsoft's Azure platform, will be accessible through a joint venture with 21 Vianet, a Chinese data center operator. The establishment of Microsoft's joint venture highlights challenges foreign companies face in making cloud services available in China.

[7] A widely used structure for foreign investment in Internet businesses in China is the Variable Interest Entities (VIE) structure. The official legal status of VIEs in China is unclear. Further complicating this status is the non-transparent manner in which provincial Communication Administration offices issue ICP licenses. As an example, the Beijing Communications Administration website can be found here: http://www.bca.gov.cn/default/index.jsp. China's national ICP registration portal can be found here: http://www.miibeian.gov.cn.

obtain licenses from information security regulators in order to gain access to certain markets. Because these licenses include requirements for disclosure of source code and other proprietary information, foreign companies seeking to protect their IP are effectively barred from competing in these markets.

Chinese Technical Standards

China's future cloud standardization effort reflects both national technology development objectives as well as the indigenous technologies borne out of the national pilot program and other mechanisms[8]. China is thus pursuing policies to promote the development of domestic standards, and these domestic standards sometimes lack interoperability with global standards. Specific standards include storage, data center hardware and security[9], cloud OS specifications, data management software, P2P platforms, search engines and interconnection interface protocols.

The Standardization Administration of China (SAC)'s 12th Five-Year Plan calls for the 'development of standards for cloud computing terminology and reference models; standards for cloud data management and storage; standards for the cloud platform interface and virtualization; standards for the new generation of search engines; standards for new model network operating systems; standards for mass storage systems; and standards for intelligent mass data".[10]

Given the relatively fragmented and complex standardization framework that is emerging for cloud computing in China, participation by foreign companies in the standards development process is critical to ensuring that China's cloud computing development is integrated with the global cloud computing standards ecosystem. Currently, foreign companies participate in some, but not all, relevant standards bodies. Foreign companies do participate in China Electronics Standards Institute (CESI) Service-Oriented Architecture (SOA), China Communications Standards Association (CCSA) and National Information Security Standards Technical Committee (TC260) standards groups, but often not as full voting members, limiting foreign companies' influence and ability to contribute meaningful input. However, other important working groups, such as select groups under TC260, do not allow foreign company participation, even as observers. The lack of full participation by foreign companies in Chinese cloud-related SDOs, or other SDOs setting standards that will impact cloud's adoption and industry development, creates a risk that China will develop non-interoperable country-specific cloud computing standards.

Other specific developments in cloud computing standardization include:

- On July 12th, TC260 published the draft for comment of the *Information Security Technology: Government Department Cloud Computing Service Provider Basic Security Requirements,* with a comment period that concluded September 1st [11]. The draft standard sets guidelines for data retention, data sovereignty, identity management, cloud service provider size and operational experience, and business dealings between cloud service providers and government customers. Initial drafts were completed without formal industry participation, as foreign companies are restricted from becoming voting members of TC260. In some areas, foreign industry

---

[8] CCSA TC1 WG4 is currently discussing a standard called *Telecommunication Network-Based Cloud Computing Overall Technological Framework*.

[9] CCSA TC1 WG4 is currently discussing two standards called *Internet Data Center Overall Technological Framework Requirements* and *Internet Data Center Energy Consumption Testing Methods*.

[10] SAC's 12th Five Year Plan for Standardization can be downloaded in Chinese at http://www.sac.gov.cn/zhywglb/zxtz_823/201112/t20111228_100505.htm.

[11] Please see the following link to TC260's call for public comment, and a copy of the standard (in Chinese): http://tc260.org.cn/getIndex.req?action=quary&req=modulenvpromote&id=2019&type=0&moduleId=654&sid=45.

has been able to participate in the standards development process, but in other critical areas, including security, they have not. On October 16th, USITO held an informational exchange with TC260 to discuss its comments to the draft submitted in September 2012. After both industry and inter-ministerial review, the draft has undergone significant revision and is still under discussion.

- On September 20th, the China's National Information Technology Standards Technical Committee (NITS) [12] held the first meeting of its Cloud Computing Standards Working Group.[13] At the kick-off meeting, key Chinese officials, including CESI President Mr. Zhao Bo, and Standardization Administration of China Vice Director Fang Xiang, delivered keynote remarks, stating that the purpose of this group was to promote domestic cloud computing standards.

Internet Content and Service Restrictions

Internet Content Censorship: China's Internet content censorship presents significant challenges to foreign companies seeking to provide cloud computing products and services in the China market, or seeking to utilize cloud computing technology and services in their China operations. A variety of well-known and widely used 'cloud computing' services are currently inaccessible from Chinese IP addresses. Internet access controls also disrupt cloud-based services deployed on internal corporate networks.

In particular, the arbitrary nature of China's Internet censorship measures poses significant risk to providers of cloud services for the following reasons:

- Internet censorship lacks transparency, with no clear guidelines as to what types of content might trigger censorship; censorship is as much about retaining political stability as about more "universal" concerns such as blocking fraudulent or indecent content;

- There is no clear recourse for determining why sites are blocked, which office has initiated the blocking, or how to subsequently restore access;[14]

- Internet censorship takes place at multiple levels, including self-censorship within Internet companies, censorship at Internet data centers, and censorship at numerous administrative offices, driven by self-preserving interpretation of shifting government sensitivities and often vague directives;

- Internet censorship is often retaliatory in nature, and is widely perceived to be a means of punishing companies for transgressions, often of an ideological nature.[15]

Privacy and Cross-Border Data Flow Regulations

Cloud computing's development internationally has been hindered by privacy and cross-border data flow issues. While Internet users are concerned about protecting their privacy online, governments worldwide worry about information gathered without explicit knowledge of the user, the risks of data stored in central locations without adequate

---

[12] In Chinese: 全国信息技术标准化委员会. NITS is China's representative to ISO/IEC JTC1 standards working group.

[13] For more information on the establishment of this group, please see http://info.chinabyte.com/443/12433443.shtml.

[14] In October 2011, the U.S. government submitted to China a request for clarification of China's Internet restrictions under paragraph 4 of Article III of the General Agreement on Trade in Services (GATS). The official reply shed little light on the arbitrary nature of China's Internet restrictions.

[15] Recent blockages that are widely believed to be retaliatory in nature include Internet sites of Bloomberg and The New York Times, which were blocked following publication of articles detailing the family wealth of senior Chinese officials.

protection, and sensitive information leaving national borders and becoming subject to foreign laws that may not be compatible with domestic regulations.

China's Privacy Guidelines: In January 2011, MIIT released draft guidelines on the protection of personal information online. The guidelines allow transfer of personal information to overseas entities only in instances where explicitly allowed by law or regulation, or with the consent of the appropriate administrative agency. The consent of the data subject is also required. In addition, the draft guidelines establish a basic presumption that personal information shouldn't be shared between data users. MIIT has not announced any revisions or changes to the draft guidelines since their initial release.

USITO Recommendations[16]

Given the rapid development of cloud computing globally, and the high-level government support for development of cloud computing in China, the US ICT industry has a unique opportunity to work with China's policy-makers in developing a regulatory environment in China that supports the healthy growth of cloud computing globally. In order to achieve the full potential of cloud computing, however, it is critical that policy-makers embrace the following principles:

- Aggressively build out **broadband** capacity to allow maximum deployment of cloud and other Internet services.

- Avoid cloud-specific rules and policies, in favor of policies that apply broadly to a wide range of technologies and services, and those that maintain a level playing field for cloud computing and all approaches to remote computing and data storage.

- Encourage innovation by avoiding mandates or preferential support for specific technologies or companies, or that favor one particular business model or technology over another.

- **Cross-Border Data Flows**: implement policies that allow, to the greatest extent possible, unrestricted transfer of data across borders and do not require data to be stored on-shore; avoid localization mandates, or any policies that would give preference to data processors using local facilities or operating locally.

- Promote **interoperability and mutual recognition** in data privacy and security laws and policies.

- Approach **cybersecurity** holistically, rather than specifically targeting cloud technologies and applications. Embrace a global approach to cybersecurity that recognizes the global nature of interconnected systems and provides for data to be protected regardless of where it is located, and that seeks international consensus standards that avoid fragmented, unpredictable national requirements.

- Adopt **global ICT standards** developed via standard-setting processes that are consensus-based, transparent, and industry-led, with participation open to interested parties.

Finally, it is important to recognize that policy-maker concerns can and are being addressed through industry-led voluntary action, public-private partnerships and best

---

[16] Consolidated from Software and Information Industry Association Guide to Cloud Computing for Policymakers (2011), TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud – "Cloud First, Cloud Fast: Recommendations for Innovation, Leadership and Job Creation" (September 2011), and Information Technology Industry Council (ITI) Comments on Korea's Proposed Bill for the Development of Cloud Computing and Protection of Users" (August 2012).

practices enforced through contracts and existing legislation. Industry plays a leading role in developing solutions to the challenges presented by rapid development of cloud computing technologies. USITO strongly encourages increased collaboration and dialogue between industry and policy-makers in the areas of cloud applications, platforms, policies and standards in order to promote the development of a robust global cloud-computing ecosystem.

APPENDIX I: CHINA CLOUD COMPUTING GOVERNMENT STAKEHOLDERS

National Development and Reform Commission (NDRC)

The NDRC is China's main macroeconomic planning body responsible for the drafting and dissemination of the 12th Five-Year Plan and Strategic Emerging Industries (SEI) development plans. Although line ministries promulgate industry-specific regulations, NDRC holds significant power in determining which sectors receive national-level funding and other regulatory support. For example, NDRC guides the drafting process for documents such as *China's 12th Five Year Plan for Software Industry Development*, *12th Five-Year Plan for Information Security Industry Development*, and the *12th Five-Year Plan for Cloud Computing Industry Development*.[17]

Key Departments:

- Hi-Tech Department

Specific Policy Roles and Responsibilities:

- National Pilot Cities oversight, in partnership with MIIT

- 12th Five Year Plan drafting oversight, including industry-specific plans

Ministry of Industry and Information Technology (MIIT)

MIIT is China's principle regulator for the software, information security, telecommunications, and Internet industries. It coordinates with private and state-owned companies to administer state funding for national research projects. It guides standards bodies in the areas of software and telecommunications. It follows NDRC's guidance in drafting industry-specific 12th Five-Year Plans.

Key Departments:

- Science & Technology Department

- Telecom Development Department

- Software Services Industry Department

- Telecommunication Administration Bureau

- Software and Integrated Circuit Promotion Center (under S&T Department)

Specific Policy Roles and Responsibilities:

- Oversees National Pilot Cities project, in partnership with NDRC

- Drafts industry-specific 12th Five Year Plans, under guidance from NDRC

- Administers ICP license (local affiliates carry out administrative process; MIIT manages national registration database)

- Through its Science & Technology Department, allocates funding for national level research projects and cloud computing research facilities, also makes standards in the relative areas

State Administration of Industry and Commerce (SAIC)

SAIC sets national commercial policy, and local affiliates grant business operation licenses along with line ministries in specific industries (in this case, MIIT for telecom companies).

---

[17] USITO has documented sector-specific 12th Five Year Plans, finalized by MIIT with guidance from NDRC. To date no such Cloud Computing plan has been released or discussed.

Specific Policy Roles and Responsibilities:

- Manages ISP business license

China Communication Standards Association (CCSA)

CCSA is China's primary standards development organization (SDO) for the telecommunications industry. It primarily develops telecommunication industry standards (designated 'YD'), some national standards (designated 'GB'), and also adopts global ITU-T standards for use in China. CCSA reports directly to MIIT's Science & Technology Department Standards Office. Membership is open to foreign enterprises as observer members and domestic enterprises and domestic research and academic institutions. Many members are also concurrently members of ITU-T Study Groups (SCs).[18]

Key Departments:

- Technical Committee 1 WG4: IP and Multimedia Communications

- Technical Committee 8: Information Security

Specific Policy Roles and Responsibilities:

- Develops telecommunications, data center and storage, P2P, and other important cloud computing-related standards

China Electronics Standardization Institute (CESI)

CESI is a professional institute for standardization in the field of electronics and ICT under the Ministry of Industry and Information Technology (MIIT). CESI is China's main interlocutor authority for most ISO/IEC JTC1 sub-committees and facilitates correspondence between Chinese experts and these SCs. CESI reports directly to MIIT and is also co-administrated by the Standardization Administration of China (SAC). CESI houses the secretariats of key standards technical committees including the China IT Technical Standards Committee and National information Security Standards Technical Committee (TC260). While foreign companies participate in some CESI groups as observers, such as the NITS SOA (see below), other groups are fully closed to foreign participation, such as working groups under TC260 (see below). For more information about the China Standardization System, please see *USITO White Paper on China Standardization System*.

Key Departments:

- National Information Technology Standardization Technical Committee (NITS): SOA (Service-Oriented Architecture) Standardization Working Group

- China National Information Security Standards Technical Committee (TC260)

- National Information Technology Standards Technical Committee (NITS) Cloud Computing Standards Working Group

Specific Policy Roles and Responsibilities:

- Discusses and sets relevant cloud computing technical standards

State Internet Information Office (SIIO)

SIIO shares its office and staff with the State Council Information Office (SCIO). Created in 2011, SIIO plays an important role in Internet content censorship as well as the revision of China's *Internet Information Service Regulations*. SIIO also interfaces with foreign

---

[18] Most CCSA technical committees are open to foreign participation as voting members. Some TCs, including TC8: Network Security, limit foreign participation to observer status.

government on Internet policy issues and, in conjunction with its provincial branch offices, fulfils a policy-coordinating role within the Chinese government.

Specific Policy Roles and Responsibilities:

- Internet content censorship management

- Policy coordination

APPENDIX II: REGULATIONS, LAWS & STANDARDS ON CLOUD COMPUTING IN CHINA

Cloud Computing Policies & Initiatives	
October 2010	**State Council Circular 32: Decisions of State Council on Accelerating the Cultivation and Development of Emerging Strategic Industries** – designates cloud computing as a component of 'Next-Generation IT' in the 12th Five Year Plan. Released by China's State Council (finalized). Source: http://www.gov.cn/zwgk/2010-10/18/content_1724848.htm
October 2010	**Cloud Services Pilot Cities Notification** – outlines plans to develop 5 cloud computing pilot cities. Released by National Development & Reform Commission (NDRC) and Ministry of Industry and Information Technology (MIIT) (finalized; currently being implemented). Source: http://www.ndrc.gov.cn/zcfb/zcfbtz/2010tz/t20101025_376673.htm
July 2012	**12th Five Year Plan for the Development of the Software & IT Service Industry** – further clarifies development goals mentioned in SEI outline, including for cloud computing. Released by Ministry of Industry and Information Technology (MIIT) (finalized). Source: http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/14542600.html
July 2012	**Information Security Techniques – Basic Requirements for Security for Government Department Cloud Computing Service Providers** – proposed security standard for companies providing cloud services to the Chinese government. Drafted by China National Information Security Standards Technical Committee (TC260) (under revision). Source: http://tc260.org.cn/getIndex.req?action=quary&req=modulenvpromote&id=2019&type=0&moduleId=654&sid=45
October 2012	**Establishment of Cloud Computing Guiding Documents Drafting Experts' Committee** – National Development & Reform Commission (NDRC). Source: http://gjss.ndrc.gov.cn/gzdt/t20120926_506666.htm
October 2012	**Establishment of Cloud Computing Standards Working Group** Source: http://info.chinabyte.com/443/12433443.shtml

Other Relevant PRC Policies	
March 2003	**China Telecom Services Categories Catalog** – defines 'basic' and 'value-added' telecom services scope and regulation. Currently managed by Ministry of Industry and Information Technology (MIIT) (under revision). Source: http://www.china.com.cn/policy/txt/2003-03/26/content_5300857.htm
June 2007	**Administrative Measures for Multi-Level Protection Scheme (MLPS)** – China's overall critical information infrastructure protection (CIIP) information security policy. Administered by Ministry of Public Security (MPS) (finalized). Source: http://www.mps.gov.cn/n16/n1282/n3493/n3793/n494630/494907.html
February 2009	**Telecom Law** – China's comprehensive telecom services regulations that stipulate regulation of basic and value-added telecom services. Currently managed by Ministry of Industry and Information Technology (MIIT) (finalized; under ongoing revision). Source: http://www.miit.gov.cn/n11293472/n11294912/n11296257/11937080.html
June 2012	**Internet Information Service Measures** – rules for the operation of Internet services, including new applications such as microblogs. Jointly managed by State Internet Information Office (SIIO) and Ministry of Industry and Information Technology (MIIT) (under revision). Source: http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/14649221.html

APPENDIX III: NDRC / MIIT CLOUD PILOT CITIES SUPPLEMENT

In October 2010, China's National Development and Reform Commission (NDRC) and Ministry of Industry and Information Technology (MIIT) selected 5 cities to carry out government-funded cloud computing services pilot projects. These pilot cities are tapped to become hubs to promote cloud applications in areas such as healthcare, education and the delivery of government services. The pilot projects also aim to create new cloud computing technologies that could eventually be vetted as Chinese national standards.

- **Chongqing:** Although not explicitly identified as a pilot city, the Chongqing government made headlines in April 2011 when it announced an investment of CNY 40 billion in a new cloud-computing facility at the Liangjiang New Economic Zone. The center, dubbed "Yun Duan" (roughly translated to "Cloud Tops") claimed international connections that bypassed China's Internet censorship filters.
- **Shanghai:** The Shanghai Municipal Commission of Economy and Informatization, an office focused on technological and economic development reporting directly to the Shanghai Municipality government, issued the Cloud Computing Service Innovation Development Pilot Program Implementation Measures and established the "Yun Hai" (roughly translated to "Sea of Cloud") Industry Alliance. In addition to specifying goals for attracting investment and training engineering and management talent, the Shanghai pilot project is distinguished from other projects in its focus on developing technology and standards for server operating systems used by cloud computing service providers.
- **Beijing:** The Beijing Municipal Commission of Economy and Informatization (an office equivalent to Shanghai's commission), Beijing Development and Reform Commission, and Zhongguancun Technology Park Management Commission issued the Beijing Xiang Yun Engineering Action Plan (2010 – 2015) on September 8th, 2010. The plan focuses on developing a cloud storage platform for business and personal consumers.

Other cloud pilot programs include Shenzhen's 'Kun Yun' (roughly translated as 'cloud of flying fish'), Guangzhou's 'Tian Yun' (roughly translated as 'sky cloud'), Ningbo's 'Xing Yun' (roughly translated as 'galaxy cloud'), Wuxi's 'Yun Gu' (roughly translated as 'cloud valley'), and Hangzhou's 'Yun Chaoshi' (roughly translated as 'cloud supermarket').

APPENDIX IV: NIST DEFINITION OF CLOUD COMPUTING SERVICE MODELS

According to the National Institute of Standards and Technology (NIST), cloud computing has three basic service models. NIST's definition has been reported by the Chinese media, and could gain a certain amount of influence domestically[19]. A basic understanding of these three models will help place the China market-entry question into context.

- **IaaS** (Infrastructure as a Service) The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

- **PaaS** (Platform as a Service) The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- **SaaS** (Software as a service) The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[20]

---

[19] For one example of this influence see (in CN): http://it.anhuinews.com/468871/979119231116.shtml
[20] The NIST Definition of Cloud Computing, Peter Mell and Tim Grance, Version 15, October 7, 2009

APPENDIX V: SIIA GUIDE TO CLOUD COMPUTING FOR POLICYMAKERS

Policymakers are rightly interested in fostering the growth of cloud computing to seize the economic benefits, and to protect their citizens against any potential for harm. Yet, because cloud computing is not a single technology or business model, for policy making purposes, there is no such thing as "the cloud."

…There is no need for cloud-specific legislation or regulations to provide for the safe and rapid growth of cloud computing, and in fact, such actions could impede the great potential of cloud computing.

Today, there are a number of existing and proposed public policies that could hurt the development of cloud computing, such as requirements for the location of computer facilities in particular jurisdictions, or restrictions of cross-border data flows – policymakers should take great effort to remove or avoid such types of policies…

…One-size-fits-all policies cannot apply properly to all the various technologies and business models that comprise cloud computing.

Policymaker concerns about specific issues can and are being addressed through industry-led voluntary action, public-private partnerships and best practices enforced through contracts and existing legislation.

SIIA recommends that policymakers embrace the following key principles in their efforts to develop policies that encourage the economic benefits of cloud computing and ensure that users are protected:

- Avoid cloud-specific rules and policies, in favor of policies that apply broadly to a wide range of technologies and services, and those that maintain a level playing field for cloud computing and all approaches to remote computing and data storage.

- Promote open standards for software and data interoperability, and avoid policies that would favor one particular business model or technology over another.

- Promote policies that allow, to the greatest extent possible, unrestricted transfer of data across borders.

- Encourage rules governing data to travel with the data in order to adequately recognize varying jurisdictional requirements, and ensure data subjects do not lose protection when their data is stored and processed in "the cloud", or in any remote computing environment.

- Avoid localization mandates, or any policies that would give preference to data processors using only local facilities or operating locally.

- Seek interoperable privacy regimes in which countries recognize each other's privacy rules to the greatest extent possible.

- Embrace a global approach to cybersecurity that recognizes the global nature of interconnected systems and provides for data to be protected regardless of where it is located, and that seeks international consensus standards that avoid fragmented, unpredictable national requirements.