TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org
Tel: +1.703.907.7700
Fax: +1.703.907.7727

Statement of K.C. Swanson, Director, Global Policy
Telecommunications Industry Association (TIA)

Before the
Office of the U.S. Trade Representative
Hearing on Investigation under Section 301 of the Trade Act of 1974
September 28, 2017

The Telecommunications Industry Association (TIA) appreciates the opportunity to provide testimony to USTR on the investigation under Section 301 of the Trade Act of 1974 regarding China's policies related to technology transfer, intellectual property (IP) and innovation.

TIA represents approximately 250 manufacturers and suppliers of high-tech telecommunications networks and services here in the United States and around the world. TIA is also an ANSI-accredited standards development organization. Our members' products and services empower communications in many industries and markets, including healthcare, education, security, public safety, transportation, government, the military, the environment, and entertainment.

Background: Beijing's goals for the ICT market Below, we briefly consider the political and regulatory context of Chinese policies affecting the U.S. ICT industry and related IP.

Chinese industrial plans. Through a lengthy series of industrial roadmaps, China has made clear its plans to become a global leader in key technology fields such as telecommunications equipment, semiconductors, software, cloud computing and artificial intelligence.[1] Promoting the development of Chinese IP is a key component of that long-term strategy. In August 2017 Beijing issued a five-year plan outlining a goal to boost IP royalty exports to reach US $10 billion by 2020[2].

Push to replace foreign technology. This striking drive to boost domestic industry has been accompanied by a more concerning attempt to undermine and shrink the role of U.S. and other foreign technology firms.

[1] A partial list of recent industrial roadmaps would include: *China Manufacturing 2025*, State Council, May 2015; *Cloud Computing Development Three-Year Action Plan 2017-2019,* Ministry of Industry and Information Technology (MIIT), April 2017; *13th Five-Year Plan for the Development of Strategic and Emerging Industries (SEI),* State Council, December 2016; *Smart Hardware Industry Innovation and Development Initiative 2016-2018,* MIIT and National Development and Reform Commission, September 2016*; Outline of National Informatization Development Strategy,* General Office of the CPC Central Committee and State Council, July 2016; *13th Five-Year Plan on National Scientific and Technological Innovation*, State Council, September 2016; *New Generation Artificial Intelligence Development Plan*, State Council, July 2017

[2] *13th Five-Year Plan National Intellectual Property Protection and Use Plan Major Tasks and Division of Labor*, inter-agency group including State Council office, August 24, 2017

Chinese President Xi Jinping publicly pushed in 2016 for China to master "core technologies," which he has called necessary to ensure national security.[3]

IP is a key component in the state campaign to promote the interests of Chinese firms and displace foreign technology. Xi has spoken of foreign technology as a means for IP transfer, commenting: "[First] we need to import new technologies only if they are safe and controllable. Second, we need to determine what technologies can be re-innovated after introduction, and what technologies require cooperation with others."

In another speech last year, Xi called for speeding up the adoption of "Chinese-made, indigenous, controllable" products used in its critical infrastructure[4].

Impact of national security policies on ICT market. Beijing formally committed not to discriminate against foreign products when it joined the World Trade Organization. However, the WTO affords its members broad discretion to formulate policies deemed necessary for national security. As such, China has proceeded to issue a complex array of overlapping rules and standards it says are necessary for national security, many associated with the Cybersecurity Law that took effect in June 2017. As we describe below, some of these policies would appear to pose risks to U.S. IP, while threatening the ability of American firms to compete in China's technology market.

Broad definition of critical information infrastructure (CII). Beijing has sought to project its security umbrella far beyond the sensitive military or government systems where valid national security concerns might normally apply; its formulation of national security has expanded to include many commercial markets. The Chinese government has shown itself increasingly inclined to categorize commercial industries as CII, which it uses to justify restrictions on foreign involvement.

The Cybersecurity Law says critical information infrastructure includes but is not limited to public communication and information services, energy, transportation, water conservancy, finance, public services and e-government. Other measures have offered broader definitions of CII.

After seeking to establish that large segments of the economy are subject to special security considerations, the Cybersecurity Law offers legal justification for an expansive state-led testing regime. Over the past year China has issued a complex and overlapping series of policies and standards that purport to vet foreign technologies to determine their "security." Though many are not yet finalized, the text of draft measures has already raised concerns about the potential for IP disclosures.

TIA members are concerned that China's growing slate of security rules may disadvantage U.S. exporters selling into China's commercial markets. The regulations conflict with China's multiple formal commitments to the U.S., including that its security policies not unnecessarily limit sales for foreign companies. They set a worrying precedent that other countries might follow.

But there are also issues of concern for US business that do not relate to security, including Beijing's approach on standards and competition policy. Below, we describe a series of recently-issued final and

---

[3] Speech by President Xi Jinping at the the Working Session on Cyber Security and Information Industry, April 19, 2016, http://www.cac.gov.cn/2016-04/25/c_1118731366.htm

[4] Speech by President Xi Jinping before the CPC Central Committee, October 9, 2016, http://www.cac.gov.cn/2016-10/09/c_1119682237.htm

draft policies, including those implemented to carry out the Cybersecurity Law, which could potentially have a discriminatory impact on U.S. ICT commerce.

The shortlist of policies we will examine in further detail below includes the following:

- Security testing of ICT products by the Chinese government as a requirement for market entry
- Equity caps and operational restrictions on cloud computing
- Restrictions on cross-border data flows
- Standards-setting approaches that depart from global norms
- Implementation of competition policy

(Note that in the rest of this document, policy outcomes appear in boldface type, with the titles of relevant measures in italics.)

State-led security testing as a requirement for market entry.

- **Critical infrastructure defined to include commercial digital economy** (Draft *Critical Information Infrastructure Protection Regulations*). The CIIP measure defines essential infrastructure to encompass much of the digital economy, then advances a legal basis for random security tests and evaluations to be conducted by the state. It is not clear what guiding parameters would govern such reviews.

  The draft measure defines the scope of CII to include not only systems relevant to national security, but also those that affect the "national economy, people's livelihoods and public interests." It also specifies that a vast swath of the commercial ICT sector will be subsumed under the CII designation, including "telecommunications networks, radio and TV networks and the Internet, and organizations providing cloud computing, big data and other large-scale public information network services." Such broad designations would appear to allow for significant government interference in China-based commercial activities in the name of security.

- **Mandatory state testing of commercial ICT products** (*Catalogue of Network(Cyber)- Critical Equipment and Cybersecurity-Specific Products, Batch 1)*. In June 2017 the Cyberspace Administration of China (CAC) published a list of "network-critical equipment," including routers, switches, servers, programmable logic controllers and cybersecurity products, which will need to undergo unspecified government security tests in order to be sold in the commercial market. Products will be tested to ensure compliance with "relevant national standards" before they can appear on the approved list for commercial sale.

  The labs carrying out unspecified testing will be accredited by China's Ministry of Public Security and CAC, among other agencies. While the rule nominally took immediate effect, it has not been implemented in practice because CAC is still drafting the standards in question.

  There was no comment period or consultation with industry before the policy was released.

- **Mandatory security assessments of new Internet services** *(*Draft *Administrative Measures for New Internet Services Security Assessments).* Proposed rules would grant the government blanket authority to conduct security reviews over all new telecommunications services to be developed in

the future. A confidentiality requirement within the text acknowledges the potential for government officials to learn of trade secrets in the course of evaluations. A number of other elements of the review appear excessively intrusive, notably the potential for telecommunications administrations to question staff of a given company and enter their offices to investigate and collect evidence.

- **Mandated access to IP** (Draft *Baseline for Cybersecurity Classified Protection: Special Security Requirements for Mobile Interconnection (Draft);* Draft *Security Controllable Level Evaluation Index of Information Technology Products for CPUs*). In 2017, Beijing issued cybersecurity draft standards that require suppliers of mobile Internet and IoT services provide access to source code[5]. This followed the release of a proposed procurement ranking system for software and semiconductors in the fall of 2016; under those rules, companies accrue more security points by providing details about their IP[6].

Security ranking system for commercial markets. One important element of Beijing's plan to replace foreign technologies is the expansion of a security ranking system to commercial markets, called the Cybersecurity Classified Protection Scheme (previously known as the Multi-Level Protection Scheme, or MLPS). For the past decade, Chinese government and state enterprise networks deemed "sensitive" have been required to use only products with Chinese domestic IP[7]. But over the past year Beijing has announced it will also apply the ranking system to the commercial insurance industry[8], civil aviation[9], and a wide swath of other fast-growing commercial sectors, including insurance, aviation, cloud computing, mobile internet, the Internet of Things, industrial controls, and big data[10]. Taken together, the moves represent the vast expansion of an approach that is premised on excluding foreign ICT equipment from many Chinese information networks.

China has meanwhile announced plans to build up its own cloud computing, mobile Internet, IoT and big data[11] markets.

Equity caps and operational restrictions for cloud computing *(Telecommunications Services Classification Catalogue)* Besides leveraging the pretext of national security to favor domestic firms, Beijing has resorted to the blunt policy of closing off markets to full U.S. participation. As of March 2016, American firms in China are only allowed to offer services in cloud computing – a vital and fast-

---

[5] *Baseline for Cybersecurity Classified Protection: Special Security Requirements for Mobile Interconnection (Draft); Baseline for Cybersecurity Classified Protection: Special Security Requirements for Internet of Things (Draft),* The National Information Security Standardization Technical Committee (TC260), January 2017

[6] *Security Controllable Level Evaluation Index of Information Technology Products for CPUs,* (plus similar documents that apply to Office Suites and OS), TC260, October 2016

[7] *American Business in China White Paper*, American Chamber of Commerce in the People's Republic of China, 2010, p. 226

[8] Draft *Supervision Rules on Insurance Institutions Adopting Digitalized Operations*, China Insurance Regulatory Commission, April 2016

[9] *Interim Provisions on Administration of Network Information Security in Civil Aviation*, Civil Aviation Administration of China (CAAC), February 2016

[10] *Information Security Technology - Implementation Guide for Cybersecurity Classified Protection*, General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, November 2016

[11] *Informatization-Industrialization Integration Development Plan 2016-2020,* MIIT, July 2016

growing market – if they form a joint venture with a Chinese partner[12]. The cloud computing restrictions mark a major retreat in market access.

The new restrictions took the form of a revision to China's catalogue governing telecommunications, which now incorrectly classifies a range of ICT technologies and services including cloud computing as "telecommunications value-added services" (in the parlance of the World Trade Organization) when in fact they are "computer and related services" that are merely delivered over a telecom network. This distinction matters because companies that provide telecom value-added services in China can only operate through joint ventures, and foreign ownership is capped at 50%. The new rule left foreign firms that want to compete in a fast-growing ICT market in China, cloud computing, with no option but to undertake a joint venture with a Chinese partner. (In contrast, Chinese firms are currently allowed to establish commercial operations in the U.S. without need of either a license or foreign partner).

Then in October 2016, regulators issued a draft rule that would restrict even what foreign firms are allowed to do within JVs *(Notice on Regulating Business Behaviors in the Cloud Service Market)*. It would regulate such details as which party can sign contracts, how the two partners use trademarks and brands and the degree to which they may share data.

Meanwhile, China is seeking to build up its own cloud industry: the *Cloud Computing Development Three-year Action Plan (2017 - 2019)* issued in the spring of 2017 sets a goal for two to three Chinese firms to emerge as key players with substantial market share in the international arena. Cloud computing was also highlighted as a key strategic area for China in the *13th Five-Year Plan on National Scientific and Technological Innovation* issued in 2016.

Restrictions on cross-border data flows (*Cybersecurity Law, Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data, Revised Draft*). China's Cybersecurity Law call for CII operators to store within China "personal information and important business data." A draft regulation issued this year sought to extend that obligation beyond operators of CII by requiring *all* personal information and important data from within the country be stored in China. The latter policy has since been scaled back. However, because China has defined CII to include much of the digital economy, American ICT firms that operate in China are still likely to be subject to the data localization requirement spelled out in the Cybersecurity Law.

Standards-setting approaches that depart from global norms (*Guidelines on Foreign Participation in Standards Work;* revisions of *Standardization Law).* In its approach to standards-setting, China may sometimes treat participant firms from the U.S. and other countries differently than its own domestic companies. This was underscored in 2017 when the Standards Administration of China invited international comment in drafting the *Guidelines on Foreign Participation in Standards Work.*

Such a framework, which would distinguish standards participants based on their national origin, creates the potential for foreign participants to be treated less favorably than those from domestic firms. It also undermines the core principle of "openness without discrimination" in standards policy outlined in the WTO Technical Barriers to Trade Committee in its "Decision…on Principles for the Development of International Standards." In order for voluntary participation to be viable, any related policies should establish impartial rules and guidelines that apply equally to all participants.

[12] *Telecommunications Services Classification Catalog*, MIIT, March 2016

In another standards concern, draft revisions of China's *Standardization Law* carve out an important role for "enterprise standards." This is a construct unique to China, in which companies will be obligated to reveal important and possibly proprietary details about their products and services. Enterprise standards could potentially be employed to compel disclosures of confidential business information. The specifications subject to disclosure may include product features and/or information about manufacturing and assembly that is protected by patents, copyrights and trade secrets.

Implementation of competition policy (*Anti-Monopoly Law*). TIA appreciates that the purpose of China's 2007 Anti-Monopoly Law (AML) is the legitimate prevention of cartels, mergers and monopolistic behavior that would distort competition in Chinese markets. While this is a laudable goal, we are concerned with the State Council's focus on abuse of intellectual property rights and, more specifically, the Ministry of Commerce's use of its merger review authority to require foreign parties in several cases to give concessions related to IPR that would not be required under traditional antitrust analysis. Furthermore, the Chinese companies benefiting from AML enforcement cases to date have on occasion been national champions in various strategic sectors, including the telecommunications sector.

TIA believes it is important to ensure that the AML and related anti-monopoly guidelines are equally enforced against Chinese and non-Chinese companies alike, and not used to target foreign companies as an additional policy tool to support China's national industrial policy objectives[13].

Conclusion. We appreciate the work of the U.S. government to support transparent, equitable business policies that will promote open markets, in keeping with China's WTO commitments, and allow for fair competition by U.S. ICT firms.

[13] See Department of Justice Deputy Assistant Attorney General Roger Alford's August 2017 speech acknowledging the importance of non-discrimination in this area.