

# How Chinese Cybersecurity Standards Impact Doing Business in China

*By Samm Sacks and Manyi Kathy Li*

AUGUST 2018

## THE ISSUE

- [The Chinese government has issued close to 300 new national standards related to cybersecurity over the past several years.](#) These standards cover a range of information and communications technology (ICT) services as well as products including software, routers, switches, and firewalls.
- [These standards contribute to making China an increasingly difficult market for foreign firms to operate.](#) This holds true not just for selling to government or state-owned enterprise (SOE) customers, but across the commercial market in China, spanning all sectors reliant on ICT infrastructure, from manufacturing to transportation.
- [The cybersecurity standards create a suite of challenges.](#) The Chinese government can use standards to pressure companies to undergo invasive product reviews where sensitive intellectual property (IP) and source code (even if not explicitly written) may be required as part of verification and testing. To comply with some standards, foreign firms may need to redesign products for the China market where they are not compatible with international standards. Chinese standards also create a competitive advantage for Chinese competitors for two reasons. First, they may not have the same concerns foreign companies do about providing sensitive information to the government as a condition of meeting the standards. Second, Chinese regulators may also deem Chinese companies as being more secure under the vague criteria contained in the standards simply because they are local and therefore perceived to be more “controllable” without influence from foreign governments (something China suspects of foreign technology, regardless of whether it is true).
- [Although officially most standards are deemed “recommended,” in practice many may often be required to do business in China.](#) This is the case when standards are listed as procurement requirements for government or SOEs. Beyond government customers, some Chinese customers may not buy from vendors who lack a certification associated with certain standards (which varies widely by business or product). There have been cases in which customer deals do not go through because a product lacks a certain certification, for example. Standards also become required when paired with regulations that reference those standards. The government may audit companies against standards, even if those standards are not officially required. There may be a significant cost from a sales perspective.
- [Beijing uses vague language in standards, like in many Chinese laws and regulations, to avoid issues, such as World Trade Organization \(WTO\) challenges, while allowing the government maximum flexibility and discretion to apply onerous provisions when it sees fit.](#) Beijing may also rely on the fact that most standards are recommended to avoid backlash. Over 1000 Chinese standards (not just cybersecurity standards) submitted to the WTO were downgraded from required national standards to recommendations in 2017 alone.

- As bilateral U.S.-China tensions intensify, standards related to a new system of cybersecurity reviews are likely to be among the first tools Beijing may use to retaliate against U.S. companies in a trade war. They offer openings for the Chinese government to delay certifications or licenses needed for market access or to shut down a company which may already be successful in China.
- If Beijing were to use cybersecurity standards as a tool of retaliation—during the 2018 U.S.-China tariff escalation, for example—it would be almost impossible to quantify the cost. Unlike tariffs, the government would likely not adjust how these standards are applied in negotiating to end a trade war. As a result, Beijing could use standards to shift the baseline for foreign firms operating in China in ways that would have an effect long after a period of short-term bilateral tension has passed.
- CSIS created a framework for analyzing and tracking the growing body of cybersecurity standards which have come out since the early stages of drafting the Cybersecurity Law in 2015. Our framework examines standards across eight schemes:
  1. Cybersecurity Review of Network Products and Services
  2. Certification and Evaluation for Network Key Devices and Cybersecurity-Specific Products
  3. Secure and Controllable Products and Services
  4. Multi-Level Protection Scheme (MLPS)
  5. Critical Information Infrastructure (CII) Cybersecurity Protection
  6. Cross-Border Data Transfer
  7. Personal Data and Important Data Protection
  8. Encryption
- Many more standards are likely to come as Beijing is still only in the early stages of a national effort to build out its cybersecurity standards regime. Important questions remain about how authorities will audit companies against the new standards, their effect on business operations, and how these standards fit into the regulatory process. A key question to monitor is the extent to which Beijing will lay out understandable processes for foreign firms to follow to prevent arbitrary auditing against the new standards.
- Chinese companies seeking to expand globally would benefit from China accepting international standards in parallel with domestic standards. Chinese companies are at a disadvantage by having to build two sets of products to be compatible with domestic and international standards.

In March 2018, the Office of the U.S. Trade Representative (USTR) issued a definitive report on the discrimination and intellectual property (IP) challenges that U.S. companies face operating in China.<sup>1</sup> The report (the 301 investigation findings) was groundbreaking because it is the most comprehensive and detailed public documentation to date of problems that are making the China market so difficult for U.S. companies. A central feature of the report is the now notorious Made in China 2025 plan (cited 116 times in the report), a state blueprint released in 2015 for China to become “self-sufficient” in high-tech sectors including advanced information and communication technology (ICT), aviation, and new energy vehicles.<sup>2</sup> The report also touched on challenges posed by China’s Cybersecurity Law,<sup>3</sup> a sweeping piece of legislation with a suite of market access issues, particularly around cross-border data transfer and new cybersecurity reviews. U.S. policymakers are grappling with how to manage the industrial policy and technological leadership challenges posed by China.

While it is not news that foreign companies in China face intensifying IP and market access risks, policymakers have paid far less attention to a factor that could soon create even greater challenges. Since 2015 when the drafting process of China’s Cybersecurity Law began, the main national standards body, the National Information Security Standardization Technical Committee (TC260), has issued close to 300 standards related to cybersecurity.<sup>4</sup> These new standards cover products ranging from software to routers, switches, and firewalls. Many are still in draft form and officials have indicated that more standards will be released in the near future as part of a national standardization effort only now in early stages.

The role of these standards and their impact from a commercial and security standpoint is not widely understood. What is clear is that the Chinese leadership views standards as playing a big role in the country’s ambitions for leadership in technology and cybersecurity.

This CSIS report first looks at how Beijing uses standards as national policy tools meant to flesh out the details of

higher level law, especially the Cybersecurity Law and draft Encryption Law. It unpacks why even standards that are officially recommended can sometimes, in practice, often become required to operate successfully in the market.

In particular, standards play an important role in supporting a new system of cybersecurity-related reviews by providing a basis for testing and certification. We identify three main risks for foreign firms around this growing body of cybersecurity standards: invasive security audits requiring submission of IP and source code as part of security evaluations, compliance costs around redesigning products for the China market, and, most recently, how Beijing may use cyber standards as a tool for punitive measures against U.S. companies in a trade war between the United States and China.

These risks do not only exist when foreign firms sell to government or SOE customers, but potentially impact all sectors of the economy that rely on ICT infrastructure, from manufacturing to transportation. One reason why the scope of the new rules is so broad is because the term “network operator” is sprinkled throughout the Cybersecurity Law and many accompanying regulations. “Network operator” does not just refer to telecommunications or internet service providers (ISPs) but has vast meaning that can refer to anyone who uses ICT systems. There is also a lot of confusion around a second term, critical information infrastructure (or CII). Any company that falls in the scope of CII will face a host of new requirements, but the government has not yet issued an official definition of the term, nor has it sorted out the relationship between new rules for CII and existing regulations like the Multi-Level Protection Scheme (MLPS). Until the government detangles these issues, companies across all sectors face tremendous uncertainty about what exactly they are required to do under the new cybersecurity regulatory regime.

We then lay out a framework for analyzing the dozens of cybersecurity standards to help track their status and identify where impact is most concerning for industry. The framework categorizes standards in eight schemes:<sup>5</sup> cybersecurity review of network products and services, certification and evaluation for network key devices, secure and controllable, MLPS, CII, cross-border data transfer, personal information, and encryption. Across the eight schemes, we identify which standards are required for companies and which are recommended—with the caveat that many standards can become de facto required for a variety of reasons.<sup>6</sup>

This CSIS report focuses on standards made by TC260. TC260 is China’s leading organization for writing national standards related to cybersecurity, covering areas from testing and evaluation to encryption technology.<sup>7</sup>

Appendix A contains a list of cybersecurity standards by TC260 since the early stages of the drafting process of the Cybersecurity Law. Appendix B shows standards still in draft form that are undergoing internal discussion. Appendix C has the CSIS framework that identifies these standards according to the eight most important categories for impact on industry.

China’s cybersecurity standards will play a pivotal role as Beijing presses forward with national plans to move up the value chain and build up its domestic ICT industry. For foreign firms caught in the cross fire of U.S.-China trade and technology tension, these standards can also form a channel for Beijing to exact new costs on companies if they so choose, underscoring that foreign ICT players must abide by Beijing’s terms.

## BEIJING’S PUSH TO BUILD OUT CYBERSECURITY STANDARDS

Several developments in the past two years underpin the rapid build-out of dozens of Chinese cybersecurity standards. In August 2016 (a year before the Cybersecurity Law took effect), a group of three government agencies all involved in cybersecurity standards work issued a joint opinion that underscored the pivotal role standards should play in actualizing President Xi Jinping’s vision of building China into a “cyber superpower.” The statement also described how standards would support implementation of the Cybersecurity Law.<sup>8</sup>

In parallel, the National People’s Congress released the Standardization Law in November 2017 (a revision of a law last updated in 1988). The new law codifies the leadership’s effort to modernize China’s standards system to keep pace with the development of industry and technology.<sup>9</sup>

Chinese national standards are best understood as policy instruments, a form of regulation that spell out requirements that companies can be audited against or used as the basis for testing and certifications.<sup>10</sup>

As indicated in the full chart, some of these standards are required as a precondition for market access or to sell on government procurement lists. These standards have the letters “GB” in front, which stands for “national standard,” or *guobiao* (国标). Others are recommended, but not formally binding. These are marked by the term “GB/T”, which standards for “recommended,” or *guobiao/tuijian* (国标/推荐).

## *TC260 standards become required when they are combined with specific regulations. In this way, they do not have to go through lengthy interagency wrangling.*

Even if standards are not officially required, companies can still be audited against them by regulators, and they can become required in practice when: (1) they are listed as procurement requirements for government or SOEs; and (2) when customers will not buy without a specific certification. The latter varies widely by sector or business segment, yet there are cases in which customer deals do not go through because a product lacks a certain certification, underscoring how failure to comply with even recommended standards may result in a heavy cost to sales in China. Standards also become required when paired with regulations that reference those standards. The government may audit companies against standards, even if those standards are not officially required. As a result, compliance with standards may be necessary to do business in China even if those standards are only “recommended.”

In fact, the government may rely on most standards being recommended to avoid backlash. Domestically, all required standards must go through a process to be officially endorsed. This is not an easy process in the Chinese political and legal bureaucracy. Moreover, internationally Beijing must disclose required standards to the World Trade Organization (WTO). In fact, in 2017 the government downgraded over 1000 Chinese standards<sup>11</sup> submitted to the WTO previously from required national standards to recommendations.<sup>12</sup> TC260 does not have the authority to issue required standards. Yet there is a workaround; TC260 standards become de facto required when they are combined with specific regulations. In this way, they do not have to go through lengthy interagency wrangling or draw international attention.

In effect, companies often need to treat even recommended standards as required in order to be successful in the China market. Failing to do so can create tremendous regulatory and political risk. This risk is only likely to increase in an environment where Beijing is looking for ways to punish U.S. companies as trade tensions ratchet up this year (and perhaps beyond).

### **WHY THE CYBERSECURITY STANDARDS MATTER**

China’s growing body of cybersecurity standards creates several challenges for foreign firms.<sup>13</sup>

First, foreign firms may face pressure to submit source code or undergo other kinds of invasive audits of IP to comply. Many standards use intentionally vague language around verification and testing to give the government broad discretion. This means that even if source code is not explicitly mentioned, the risk is still there. In fact, most standards do not have explicit source code requirements because there is now a sort of unspoken agreement that TC260 will not include it in most standards.<sup>14</sup> TC260 reportedly deleted the source requirement in final drafting stages for a standard for evaluating the security and controllability of a central processing unit (CPUs), for example.<sup>15</sup> However, even without mentioning source code, other language contained in the standard—such as testing or verification—can signal that source code and other sensitive material may be required to attain a higher score as part of the security assessment process.<sup>16</sup>

While the government may not always choose to enforce these unwritten rules, the government’s position can change at any time as it leverages the vagueness of the rules.

## *Many standards use intentionally broad language around verification and testing to give the government broad discretion.*

This is an example of a broader trend in which unwritten rules may dictate whether foreign firms can successfully operate in China. While the government may not always choose to enforce these unwritten rules, the government’s position can change at any time as it leverages the vagueness of the rules. This reinforces that foreign firms are only in China on Beijing’s terms. Unwritten rules and ambiguous language also provide another benefit to Beijing by giving the government space to deal with interagency conflict. Foreign firms can be caught in the crosshairs of such internal turf battles.

Second, the sheer volume of cybersecurity standards creates an enormous compliance burden for foreign firms that must redesign products or change business practices around China’s requirements. Doing so is expensive and impractical from a business perspective. It also creates a duplicative system in which companies may need to build two different versions of ICT products: one that is compatible with China and one for the rest of the world. Foreign industry groups have lobbied Beijing to accept more international standards as a way to demonstrate

*Standards supporting an emerging system of cybersecurity reviews are likely to be among the first tools that Beijing will turn to in order to punish U.S. ICT companies for U.S. trade actions taken against China.*

compliance with Chinese domestic standards, but there is more work to be done in this area.

While the two factors above are more longstanding, a more recent challenge of the growing body of cybersecurity standards is that they are likely to become an important new tool that the Chinese government can use to retaliate against U.S. companies in the current and growing climate of trade tension. Standards supporting an emerging system of cybersecurity reviews are likely to be among the first tools that Beijing will turn to in order to punish U.S. ICT companies for U.S. trade actions taken against China. If Beijing were to use this tool, it would be almost impossible to quantify the cost, and the damage would probably be long-term. Unlike tariffs, the government would likely never adjust how these standards are applied in negotiating to end a trade war. That is because the standards are part of the backbone of a broader cyber policy system that is much bigger than near-term tit-for-tat with Washington. As a result, Beijing could use standards to shift the baseline for foreign firms operating in China in ways that would have effect long after a period of short-term bilateral tension has passed.<sup>17</sup>

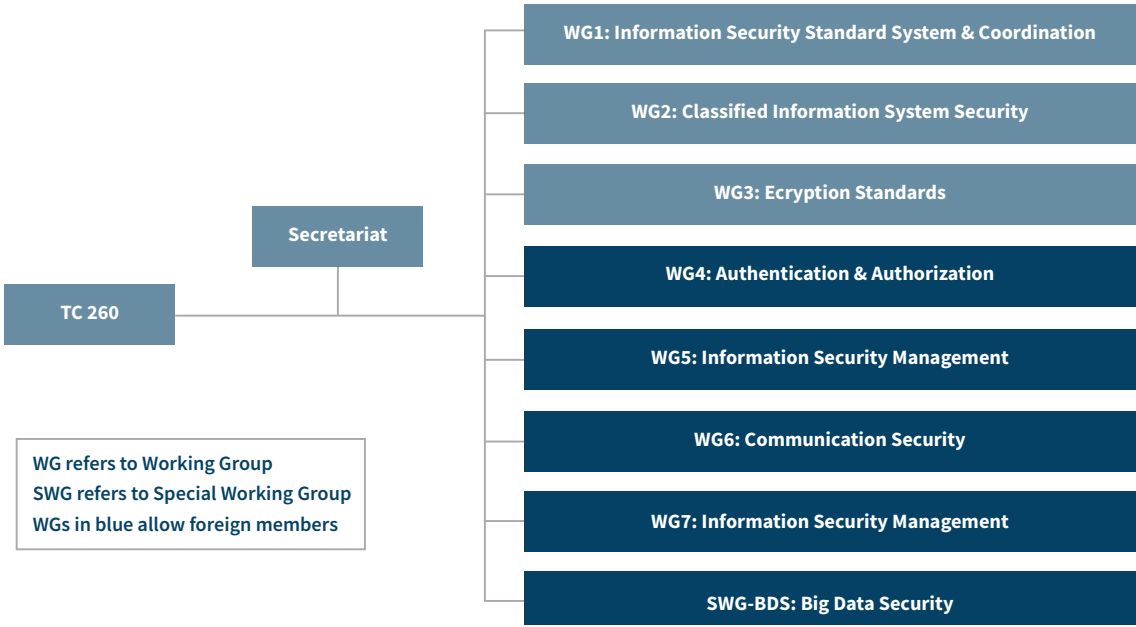
In addition, these three challenges are compounded by other pressures on foreign firms to implement Chinese standards. Chinese law requires companies to make public all the standards implemented in their products. It also encourages whistleblowing by offering payment to reward those who report violations of this requirement.<sup>18</sup>

**THE ROLE OF FOREIGN COMPANIES IN SHAPING CHINESE CYBERSECURITY STANDARDS**

In 2016, an important breakthrough for foreign companies in China occurred when TC260 invited foreign participants to join the committee to help draft China’s cybersecurity standards.<sup>19</sup> While this development has been important in terms of foreign companies finally being a part of certain discussions and staying updated, overall their influence remains limited, with local companies and the TC260 Secretariat driving the core work.

The graphic below illustrates the working groups (WGs) under TC260, highlighting in blue which are open to foreign participation.<sup>20</sup> There are now a total of 16 foreign companies who are TC260 members via these working groups.

According to foreign industry participants, TC260 only accepts comments by foreign members if they do not pose real obstacles to the TC260 agenda. When foreign member comments create conflict with TC260 plans or domestic companies’ interests, TC260 has used a strategy of moving the issue to one of the working groups closed to foreign participation. This approach was on display in a disagreement that occurred around an initiative for interoperability with an international standard, the Trusted Platform Module (TPM). Chinese homegrown versions of the TPM standard have required that certain cryptographic algorithms for security tasks like verification are based on Chinese technology.<sup>21</sup> When a vote by WG7—which includes foreign members—stopped the initiative, TC260 took up the issue instead in WG3 (encryption standards), which does not accept foreign participants.



TC260 is likely to become even less responsive to input from its foreign members given the negative dynamic in the U.S.-China relationship. Participating in TC260 may help foreign companies gain political support from the government, but their presence could become increasingly symbolic.

## **MOST IMPORTANT BATCHES OF CYBERSECURITY STANDARDS: A FRAMEWORK FOR UNDERSTANDING IMPACT**

With nearly 300 cybersecurity standards rolled out intermittently over the past several years (final and draft form), keeping track of the different standards and their impact in practical terms on the ICT industry is challenging. CSIS created a framework (Appendix C) for analyzing the effects of these standards. The framework is built on the eight categories below that represent the most pressing challenges for industry, and identifies which standards support each scheme:

1. Network Products and Service Security Review
2. Network Key Devices and Cybersecurity-Specific Products Certification and Evaluation
3. Secure and Controllable Products and Services
4. Multi-Level Protection Scheme (MLPS)
5. Critical Information Infrastructure (CII) Cybersecurity Protection
6. Cross-Border Data Transfer
7. Personal Data and Important Data Protection
8. Encryption

### **1. NETWORK PRODUCTS AND SERVICE SECURITY REVIEW**

China's Cybersecurity Law lays the foundation for a cybersecurity review of network products and services, also known as the Cybersecurity Review Regime (CRR). In May 2017, the Cyberspace Administration of China (CAC) issued draft measures as the basis for the CRR called the Security Review Measures for Network Product and Service Security Inspection (Interim).<sup>22</sup> There is some uncertainty because these measures appear to be finalized and ready for implementation despite the use of the word "interim."

The government designed the CRR to be a "black box" and does not appear to have plans to announce any standards that companies can use as the basis for approval under the system. As a result, companies have no information about the criteria and metrics needed to comply. Therefore, this is the only category in our framework (Appendix C, Category 1) in which we do not list any standards.

*China's cybersecurity regulatory system is better understood as a system of many layers, some of which may be dormant but can kick in and affect a company trajectory at any moment.*

Despite the current vagueness, the CRR presents a unique challenge since the circumstances which would trigger review are subjective and unknown. Customers or competitors could raise a concern, leading authorities to review a product or service even after it has been in the market successfully for some time. This is a very different problem from standards-based certification and evaluation programs required at the beginning for market access. If a review is triggered after a company already has market share in China, there may be factors that could put it in a weaker negotiating position (i.e., sunk cost, existing customers, established partnerships, etc.). Moreover, a review post-market entry underscores that the legal and regulatory system does not consist of a linear process. Outside of China, it would be unusual for a company to encounter new reviews needed after getting approval to enter the market in the first place. As such, China's cybersecurity regulatory system is better understood as a system of many layers, some of which may be dormant but can kick in and affect a company trajectory at any moment.

### **2. CERTIFICATION AND EVALUATION REGIME FOR NETWORK KEY DEVICES AND CYBERSECURITY-SPECIFIC PRODUCTS**

Just after the Cybersecurity Law took effect on June 9, 2017, a joint government group published a catalogue of equipment and products that would need to pass review and certification before being sold in China, called the Catalogue of Network (Cyber) Critical Equipment and Cybersecurity-Specific Products (Batch 1).<sup>23</sup> The catalogue includes what it defines as equipment (e.g., routers, switches, and PLCs) and products (e.g., firewalls and intrusion detection systems).<sup>24</sup> All items on the list cannot be sold in the China market without first getting certification.

Standards play an important role in this certification regime because they serve as the basis for testing. Unlike the CRR, companies know which standards they will be audited against. (The list of these standards is found

under Appendix C, Category 2). To date the standards released for this regime cover 9 of the total 15 categories from the catalogue. The items and the number of standards accompanying each are as follows:

- routers (1)
- switches (1)
- servers (1)
- firewalls for hardware (5) and web applications (1)
- intrusion detection system and intrusion prevention systems (2)
- secure gateways (5)
- network comprehensive audit system (4)

As the government has not yet released all the standards that support this certification regime, there will likely be new ones released in the near-future. These coming standards will be important to watch since the government uses them as preconditions for market entry into China.

It is telling that within days of the Trump administration's announcement that it would move ahead with 25 percent tariffs on Chinese goods in June 2018, the Chinese government released a list of the 22 organizations designated to conduct testing and certification.<sup>25</sup> Identifying these organizations marks a big step forward in beginning to operationalize this regime. It is possible Beijing went forward with identifying the 22 organizations to get this regime ready as a tool to deploy against U.S. companies.

### **3. SECURE AND CONTROLLABLE PRODUCTS AND SERVICES**

For the past several years, the Chinese government has used the term “secure and controllable” or “indigenous and controllable” as code words to favor local Chinese companies.<sup>26</sup> The idea is that Chinese products and services are more secure simply by being local. It is based on the inaccurate assumption that geography matters for security.

The terms appear throughout national level plans that call for “building a secure and controllable ICT industry ecosystem”,<sup>27</sup> as well as sector-specific rules covering everything from medical devices to what China terms “Internet Plus” sectors. Internet Plus refers to a state plan that is related to Made in China 2025 and aims to support ICT sectors including cloud computing, mobile technology, e-commerce, and Internet of Things (IoT). “Secure and controllable” first received widespread attention outside of China when it surfaced in a banking regulation in 2013 that aimed to replace foreign technology sold to Chinese banks with domestic alternatives.<sup>28</sup> Although Beijing officially suspended the banking regulation in 2015 after strong backlash from foreign industry and the U.S., European, and

Japanese governments, the concept has rapidly proliferated across other parts of the ICT regulatory landscape.

Even after the government suspended the “secure and controllable” banking regulation, it left a lasting impact because it made clear to Chinese industry that the government favored procurement from domestic vendors. Even with no official written requirement, foreign ICT vendors observed an impact on their market shares. Informally, Chinese banks and other companies began inquiring whether their vendors met vague undefined criteria as “secure and controllable.”<sup>29</sup> Many Chinese ICT vendors even began using “secure and controllable” in their marketing materials, recognizing that it gave them a commercial competitive advantage over foreign competitors, despite having no official written definition of the term. More recently, in May 2018 the CEO of Baidu, Robin Li, commented that “the highest principle for artificial intelligence (AI) research and development is “security and controllability” to promote the company’s AI technology.<sup>30</sup> Li’s comment shows how the term “secure and controllable” is shaping the competitive landscape for private Chinese companies far beyond SOEs, the banking sector, or other industries tied directly to the government.

Indeed, one of the main criticisms of “secure and controllable” by foreign industry and governments was the lack of transparency around what the term actually meant. Since the backlash against the banking regulation, Beijing has moved to put in place a framework for evaluating “security and controllability.” To date, the “secure and controllable” standards cover the following four products: CPUs, operating systems, software office suites, and general-purpose computing hardware (namely servers and desktops). (For this batch of standards, please see Appendix C, Section 3). There is also a fifth standard in this batch which lays out a set of principles.

Technically, the “secure and controllable” standards are only recommended. There is a scoring system used to demonstrate adherence to the standards, although there is no official government threshold for what score is required. Instead, customers may decide what score they want their vendors to meet and can choose not to purchase from a vendor that does not have a certain score.

The problem is that the scoring system and the verification process required to get a score is highly subjective and opens up foreign companies to a host of risks.<sup>31</sup> Where the language does get more specific, it leaves ample space for the government to pressure companies to give up sensitive company IP or even source code. These requirements represent the antithesis of what most foreign firms are

## *There are places in the scoring system that are extremely vague, which Beijing could easily use as a retaliation tool against the United States.*

willing to do, tilting the advantage to local companies. The following examples illustrate the point.

First, as part of the assessment process for three of the four products (CPUs, operating systems, software office suites), suppliers need to submit verification materials including product IP, source code, and design and development documents. Industry sources say that the source code requirement has been deleted from the final versions of these standards, but it is not clear how these standards will be enforced. Under the criteria for evaluation called “product design reproductivity,” suppliers must “completely reproduce the full process of product design” and provide explanation of all critical technology principles and applications.

Second, there are places in the scoring system that are extremely vague, which Beijing could easily use as a retaliation tool against the United States. Under a section called “product sustainability,” suppliers are judged on whether the core team<sup>32</sup> and products are “without influence by economic and political factors.” Scoring also examines something called “enterprise market credibility and reputation” which has no clear definition. Chinese local companies will likely have a clear advantage on these elements.

Lastly, although a relatively small part of the overall score, there is a section on “encryption algorithm compliance.” This part references Chinese national cryptography management requirements without spelling them out in detail. In effect, it means that local companies will receive higher scores because they probably use only Chinese algorithms. (See section below on encryption standards.)

To date there are only four products covered under the batch of “secure and controllable” standards, but it is likely the government may issue additional standards for other products in the future because “secure and controllable” is such a political priority for the government. Further, when this batch of four products was released, it included an ambiguous ellipsis symbol, suggesting space to add more to the product list.

## **4. MULTI-LEVEL PROTECTION SCHEME (MLPS)**

On June 27, the Ministry of Public Security (MPS) released a draft of a new version of the Multi-Level Protection Scheme<sup>33</sup> (hereafter referred to as MLPS 2.0).<sup>34</sup> The draft regulation updates the original scheme from 2007 based on the new principles set out in the Cybersecurity Law.

Under the original scheme, MLPS ranks from 1-5 the ICT networks and systems that make up China’s CII based on national security, with Level 5 deemed the most sensitive. Level 3 or above triggered a suite of regulatory requirements for ICT products and services sold into that CII, including indigenous Chinese IP in products, product submission to government testing labs for certification, and compliance with encryption rules banning foreign encryption technology. A higher MLPS ranking meant that companies would be subject to enhanced monitoring by MPS systems. These factors have created market access barriers as well as security risks for foreign firms.

One of the most confusing yet important issues under the new cybersecurity regulatory regime is what exactly CII means. Under the Cybersecurity Law, entities deemed CII face a suite of new requirements (see Section 5 below for more details on the new CII system). Yet, the government has not yet issued an official definition of CII, nor explained how these rules work with the existing MLPS. There now appear to be two parallel regulatory systems for CII: one under the original MLPS and another under the new system laid out in the Cybersecurity Law. The government has not clarified the relationship between these two regimes. Moreover, two government agencies (MPS and CAC) have overlapping jurisdiction over CII.<sup>35</sup>

What is clear is that MLPS 2.0 is likely to create more regulatory scrutiny on foreign technology. At first glance, MLPS 2.0 appears to relax the original regime because it drops the Chinese indigenous IP requirements for Level 3 and above. Yet, the draft MLPS 2.0 may increase scrutiny in other areas. For example, the document would potentially cover ICT products that did not previously fall under the scope of MLPS by expanding the scheme to cover all network operators rather than just those in CII or government agencies. Under MLPS 1.0, industries like manufacturing or retail would not have fallen in the scope of MLPS because they are not defined as CII. But according to the draft, MLPS 2.0 will cover any industry with ICT infrastructure because it covers the vague category called “network operators,” which can include anyone who uses an ICT system. MLPS 2.0 also appears to have a focus on cloud computing, mobile internet, and big data.

## More companies (both Chinese and foreign) would be subject to enhanced monitoring by the MPS, third-party certification, and domestic encryption requirements.

Another challenge, MLPS 2.0 may lower the threshold for Level 3 status in the graded ranking, which means that more companies (both Chinese and foreign) would be subject to enhanced monitoring by the MPS, third-party certification, and domestic encryption requirements. (Chinese companies will probably have less issues with these requirements.) Overall, MLPS 2.0 shifts toward more government audits and scrutiny rather than self-reporting by companies.<sup>36</sup>

Standards play a key role in supporting the MLPS regime because they are used as the reference for testing, evaluation,

and classification against technical requirements at each level (Appendix C, Category 4). The graphic below illustrates the overall structure of the standards that make up the existing MLPS system.

The baseline MLPS standard<sup>38</sup> (the foundation for the other standards) requires source code delivery when a Level 3 or above company outsources software development.

MLPS standards related to access control may also favor local Chinese companies that have robust censorship systems in place. One standard<sup>39</sup> calls for censoring and filtering content at critical network nodes to control access. In this way, censorship of digital content could be a market access barrier.

In a trade war scenario, the MLPS standards also provide ample tools for Beijing to take punitive measures against foreign companies under vague rules related to approvals. The network and system security management requires all connection to the outside networks be authorized and

MULTI-LEVEL PROTECTION SCHEME CYBERSECURITY STANDARDS	
STANDARDS ON GENERAL REQUIREMENTS OF MULTI-LEVEL PROTECTION SCHEME	<p><b>INFORMATION SECURITY TECHNOLOGY</b></p> <p>Baseline for Cybersecurity Classified Protection</p> <p>PART 1: Security General Requirements</p> <p>PART 2: Security Special Requirements for Cloud Computing</p> <p>PART 3: Special Security Requirements for the Mobile Interconnection</p> <p>PART 4: Special Security Requirements for Internet of Things</p> <p>General Requirements for Classified Protection of Cybersecurity Information Security Technology</p> <p>PART 5: Special Security Requirements for Industrail Control System</p>
STANDARDS ON DESIGN REQUIREMENTS OF MULTI-LEVEL PROTECTION SCHEME	<p><b>INFORMATION SECURITY TECHNOLOGY</b></p> <p>Technical Requirements of Security Design for Cybersecurity Classified Protection</p> <p>PART 1: General Security Design Requirements</p> <p>Technical Requirements of Security Design for Network Security Classified Protection</p> <p>PART 2: Cloud Computing Security Requirements</p> <p>Technical Requirements of Security Design for Cybersecurity Classified Protection</p> <p>PART 3: Security Requirements for Mobile Internet Things</p> <p>PART 4: Security Requirements for Internet of Things</p> <p>PART 5: Security Requirements of Industrial Control</p>
STANDARDS ON TESTING AND EVALUATING OF MULTI-LEVEL PROTECTION SCHEME	<p><b>INFORMATION SECURITY TECHNOLOGY</b></p> <p>Evaluation Requirement for Cybersecurity Classified Protection</p> <p>PART 1: Security General Requirement</p> <p>Testing and Evaluation Requirement for Classified Protection of Network Security</p> <p>PART 2: Testing and Evaluation Requirement of Cloud Computing Security</p> <p>Evaluation Requirement for Cybersecurity Classified Protection</p> <p>PART 3: Special Security Requirements for the Mobile Interconnection</p> <p>PART 4: Special Requirements for internet of things information</p> <p>PART 5: Industrail Control System Security Extension Requirement</p>

The Framework of the Series of Multi-Level Protection Standards<sup>37</sup>

## *Despite the regulation still pending in draft form, there are reports that the Chinese government has already approached numerous foreign firms to inquire if they conform to the new regulation.*

approved, with regular inspections for violation. Other murky kinds of approvals are needed in areas like “security plan design,” which calls for validation of security plans and supporting documents.

Despite the regulation still pending in draft form, there are reports that the Chinese government has already approached numerous foreign firms to inquire if they conform to the new regulation.<sup>40</sup> In enforcing the new rules, local and provincial level officials did not appear to differentiate between the old and new versions of MLPS. Foreign firms do not have clarity on the new rules and yet are already facing pressure from the government to comply with more onerous requirements.

It is telling that since the Cybersecurity Law took effect last year, a significant proportion of enforcement action against companies focused on MLPS violations. This trend underscores the growing risk companies face around MLPS as officials focus on this scheme in particular as they look to show progress implementing the Cybersecurity Law.

### **5. CRITICAL INFORMATION INFRASTRUCTURE (CII) CYBERSECURITY PROTECTION**

As discussed above, there is intense debate in Beijing over the relationship between MLPS and the new requirements for CII under the Cybersecurity Law. This is not yet resolved, nor do we know what sectors fall under CII.

One of the most significant developments in China’s Cybersecurity Law is that it imposes new and burdensome requirements on certain entities that are deemed CII.<sup>41</sup> According to the law, CII operators must only use network products and services that have undergone the vaguely defined national security review process (also known as the “black box” review above), store certain data within mainland China, and undergo security procedures like spot-testing and regular assessments.<sup>42</sup>

Companies are likely to be subject to uneven enforcement as government stakeholders with broad discretionary authority work to disentangle the competing regulatory regimes and assert primacy.

Given the new rules, the key question is what exactly is a CII operator? The Chinese government has yet to issue a final definition of what falls in scope of CII. The most recent definition leads to more questions than answers. As outlined in a draft regulation in May 2017, the scope of CII under the Cybersecurity Law covers sectors such as energy, finance, transportation, and others that meet the broad criteria in Article 18:

The network infrastructure and information systems operated or managed by the following work units, which whenever destroyed, cease functioning or leak data may gravely harm national security, the national economy, the people’s livelihood and the public interest, shall be brought into the scope of CII protection.<sup>43</sup>

The development of CII standards is moving extremely slowly (Appendix C, Category 5) amid much debate. The language in the draft regulation on CII suggests that standards will play an important role clarifying vague concepts, particularly the scope of CII itself, but so far many questions in this area remain. For example, a baseline standard<sup>44</sup> issued on June 11, 2018 offers little help narrowing down the definition of CII, using the phrase, “including but not limited to.”

Another standard<sup>45</sup> does have a section that covers MLPS compliance obligations for CII operators. It states that certain entities (“MLPS objects” or 定级对象) in CII areas like network infrastructure, big data, cloud, and IoT should undertake security measures according to their MLPS grade.

In the absence of clarity on these gray regulatory zones, companies are likely to get caught in the crosshairs between competing stakeholders in the cyber bureaucracy. MPS may move forward seeking to implement the MLPS 2.0 regime to assert its relevance as the CAC gains influence to press forward with a parallel CII protection system.<sup>46</sup> The turf battle is further complicated by the fact that the draft CII regulation says regulators responsible for different sectors should each identify CII within their own sector.<sup>47</sup> As a result, foreign companies are likely to be subject to uneven enforcement as government stakeholders with broad discretionary authority work to disentangle the competing regulatory regimes and assert primacy.

### **6. CROSS-BORDER DATA TRANSFER**

Restrictions on cross-border data transfer (CBDT) are among the top concerns for multinational companies operating in China. China’s rules governing CBDT (still in draft form) consist of a single regulation and its accompanying standard, which are meant to fill in the details of the

Cybersecurity Law. The regulation lays out general principles that, in combination with the standard (Appendix C, Category 6), determine implementation. These rules will become required when finalized (possibly by the end of 2018). They are (respectively):<sup>48</sup>

- Regulation (“Measures”): Personal Information and Important Data Cross-Border Transfer Security Evaluation Measures (draft for comment) (个人信息和重要数据出境安全评估办法 (征求意见稿))
- Standard (“Guidelines”): Information Security Technology Guidelines for Data Cross-Border Transfer Security Assessment (draft for comment) 信息安全技术 数据出境安全评估指南 (征求意见稿)

Data produced by CII operators (again, unclear what falls in scope) will need to be stored within mainland China. Beyond CII operators, data deemed “personal” or “important” must undergo a security assessment before outbound transfer. Companies conduct self-assessments that may trigger reporting to the CAC or sector-specific regulators to determine if the transfer can proceed.

The draft standard lays out the scope, methods, and criteria that should be used by companies and regulators in conducting security assessments on outbound data transfers. In this way it is meant to provide clarity on vague principles contained in the Cybersecurity Law and Measures; however, even the language of the standard itself leaves authorities broad discretion. Throughout different sections of the standard, the criteria for evaluating risk is defined by anything that would harm “national security, economic development, or social public interest.” The standard grants the CAC and sector regulators authority to initiate their own audits (rather than company self-assessments) when “deemed necessary.”

There is not consensus among government decisionmakers regarding how to define “important data”—which is one of the triggers of the assessment process for outbound transfer. As a result, progress on this regulation appears to have stalled—leaving companies to come up with their own interpretations about how authorities may implement this aspect of the CBDT rules in the future. Amid mounting trade tensions and tightening scrutiny in the ICT sectors, many foreign companies are opting to take a conservative interpretation of these pending rules. In practice, this means assuming that data (regardless of sector or kind of data) needs to be stored in mainland China to avoid regulatory scrutiny.

## 7. PERSONAL DATA AND IMPORTANT DATA PROTECTION

The Cybersecurity Law and an accompanying standard called the Personal Information Security Specification (the

## *There is not consensus among government decisionmakers regarding how to define “important data.”*

Specification) lay out broad rules for user consent and what companies should do in order to collect, store, process, and transfer personal data. Beijing views protection of personal data from fraud or misappropriation by companies or criminals as a fundamental element of cybersecurity—which may be quite different from a Western notion of data privacy.<sup>49</sup> MLPS 2.0 even stresses the importance of personal data protection with seven separate articles addressing network operators who illegally leak, sell, or share it without authorization.

In practice, enforcement of the Specification is likely to be uneven and subject to political discretion because of major regulatory gray zones. While the Specification is not officially required, regulators have already cited it in auditing companies like Alibaba-linked Ant Financial.<sup>50</sup> The government has no other criteria for assessing how companies handle personal data besides the Specification and the vague principles in the Cybersecurity Law. In the future, the legislature may draft a separate national privacy law, but in the meantime the Specification offers the only comprehensive rules on the issue, which in effect means it could be interpreted as required, if officials want to enforce it.

Conflict between the Specification and the Cybersecurity Law also creates openings for ad hoc enforcement by authorities. For example, there appears to be inconsistency around the definition of consent. Regulators could penalize a company for collecting personal data without explicit consent (required under the Cybersecurity Law), despite the Specification allowing for implied consent in some cases.

## 8. ENCRYPTION

Gray areas in China’s encryption regulatory regime give authorities broad discretion over enforcement. Moreover, the rules for what exactly foreign firms are required to do with regard to incorporating encryption into their products as well as using encryption in their own communications are now undergoing major changes. While a draft Encryption Law has been under review for a long time, a recent article in China’s official press stated that authorities may be accelerating the legislative progress.<sup>51</sup> This state of uncertainty increases risks at a time when foreign firms already face trade war retaliation.

If enacted and enforced, the law could be interpreted to require the use of only preapproved domestic encryption products<sup>52</sup>—a redline for many foreign companies in China. This has been a regulatory gray zone which has caused concern for foreign industry for years, and the Chinese government recognizes that enforcement would come at too high a cost for the foreign firms it needs to stay in the market. An exemption in the current regulation allows companies to apply for approval to use foreign-produced commercial encryption products. But in a trade war, all bets are off.

The draft law also includes vague decryption demands when national security is involved (a provision also found in China's Counterterrorism Law), on-site inspections to access data and seize equipment, and a national security review for certain kinds of encryption products and services. The law would significantly strengthen enforcement powers of China's State Cryptography Administration through expanded government supervision and access under China's first-ever uniform encryption regime.<sup>53</sup> Since the rules for this new regime are still being written, they can easily become another "backdoor" retaliation tool.

But there are still major gaps between existing laws and the standards which create more gray zones that authorities can interpret loosely (Appendix C, Category 8). For example, there are no standards laying out implementation details for the provision in the counterterrorism law requiring companies to provide "technical assistance" (which may mean decryption) to the government in support of national security investigations. There are also no standards related to encryption in CII sectors—perhaps because the meaning of CII itself is in flux—despite this being a focal point in the Cybersecurity Law.<sup>54</sup> The vague rules in this area give authorities ample space for ad hoc enforcement.

Looking at the existing standards related to encryption also reveals avenues for broad discretion by the government. First, while many Chinese standards related to encryption adopt international standards, they include modifications for using algorithms approved by Chinese state encryption management departments. There are numerous examples, including standards related to data integrity, digital signature, and identity authentication.<sup>55</sup>

Second, government authorities have broad leeway over what they require companies to provide in the process of conducting inspection related to encryption requirements.<sup>56</sup> One standard on security test requirements for cryptographic modules states that "the burden of proof lies on the inspected company. If there is any uncertainty

or vagueness, the inspectors should ask the inspected company to provide more information."<sup>57</sup>

There are likely to be many more encryption related standards to come out in the future once the new Encryption Law is finalized. Encryption standards related to CII in particular will be an important area to watch as the government moves forward with finalizing what exactly falls in the scope of this contested category.

## CONCLUSION

At this stage there are still a lot of unknowns. It is not yet clear what precisely the government is trying to protect under the hundreds of new standards described in this report or if and how companies will be audited against them. The government may provide more clarity on a clear set of processes that foreign firms should follow to avoid arbitrary auditing, which would be a positive development.

What is clear, however, is that cybersecurity standards are an important and growing factor shaping the operating environment for foreign firms in China for any business that relies on ICT infrastructure, spanning sectors dominated by state-owned, government, or private commercial players. They provide authorities with vague regulatory tools that can create security risks, add costs, and overall underscore that Beijing is ultimately in control. These challenges will only increase with trade war escalation between the United States and China, but in ways that will be difficult to quantify.

The aperture for doing business in China's ICT sector is closing, with standards supporting new kinds of cybersecurity reviews as a significant factor. Foreign firms face less space for maneuver.

What can be done in this environment?

First, foreign firms must have a clear picture of a layered and ambiguous nature of the regulatory landscape, and use this to inform their negotiating positions in dealing with Chinese partners and the government. An understanding of the practical effects of standards, especially how the growing numbers of new cybersecurity standards may change the status quo, can help prepare foreign firms.

Second, as discussed earlier, the vague language in these standards and laws is often used to appeal to different interests within the Chinese system. Foreign firms and governments should recognize where debates exist and look to engage with likeminded interest groups. There is debate over the relationship between regulatory control and business interests in China, particularly as many private Chinese companies look to expand into global

*The aperture for doing business in China's ICT sector is closing, with standards supporting new kinds of cybersecurity reviews as a significant factor. Foreign firms face less space for maneuver.*

markets. Chinese global companies also stand to gain by Beijing accepting more international standards.

Lastly, as the United States takes an increasingly confrontational stance with Beijing, we must recognize the consequences of our actions and where U.S. companies pay the costs—not just in the form of counter tariffs. Cybersecurity standards will not make the headlines, but they will be a crucial element of our technological and commercial relationship with China. ■

*Special thanks to Jim Lewis, Paul Triolo, and Han Ying.*

**Samm Sacks** is a senior fellow with the Technology Policy Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C. **Manyi Kathy Li** is an intern with the CSIS Technology Policy Program.

**VIEW AND DOWNLOAD THE APPENDICES HERE**

**China Cyber Security Standards**

---

**CSIS BRIEFS** is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s). © 2018 by the Center for Strategic and International Studies. All rights reserved.

Photo: AdobeStock

## ENDNOTES

1. <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/march/section-301-report-chinas-acts>.
2. <https://www.cfr.org/blog/why-does-everyone-hate-made-china-2025>.
3. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress-pauses-power-shifts-chinas-cybersecurity-law-regime/>.
4. TC260 has issued 138 final standards with almost 200 draft standards out for comment.
5. Eight categories were identified based on conversations with industry experts in China as well as analysis of the cybersecurity law framework.
6. The analysis for this report is based on interviews with industry experts in Beijing and the United States, as well as a translation and analysis of a public catalogue of standards published by TC260, available at: <https://www.tc260.org.cn/front/cbw.html?start=0&length=4&type=2>.
7. Although several other technical committees also set cybersecurity standards, for example, the National Technical Committee 83 on Electronic Service, the National Technical Committee 28 on Information Technology Standardization, and the Ministry of Industry and Information Technology, the standards made by TC260 are the most authoritative for supporting the provisions in the Cybersecurity Law and Encryption Law (in draft). The CSIS standards framework (found in Appendix C) is based on the 2018 catalogue published by the TC260 Secretariat. We based the list of standards in draft since November 2016 from the section of drafts for comments on the TC260 website.
8. [http://www.cac.gov.cn/2016-08/22/c\\_1119430337.htm](http://www.cac.gov.cn/2016-08/22/c_1119430337.htm).
9. <http://www.usito.org/news/final-standardization-law-passes-chinas-legislature>.
10. Internationally, the Chinese government has also stressed the importance of playing a greater role in setting standards (in areas such as 5G, for example) that are international protocols or guidelines for design and interoperability. See, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/>.
11. Not just the TC260 body of cybersecurity standards.
12. <http://chinawto.mofcom.gov.cn/article/i/ac/201704/20170402545384.shtml>.
13. According to interviews with several foreign firms and Beijing-based industry associations during June and July 2018.
14. Ibid.
15. The full name of the standard is: “Information security technology - Security controllable level evaluation index of information technology products - Part 2: Central Processing Unit.”
16. The final version of the CPU standard has not yet been published and the most recent draft for public comment still calls for submission of source code from companies to check “transparency” in product design. (See section below on “secure and controllable standards” for more details.)
17. <https://www.csis.org/analysis/how-will-china-retaliate-beyond-tariffs>.
18. See China’s Standardization Law articles 27 and 35, [http://www.npc.gov.cn/npc/xinwen/2017-11/04/content\\_2031446.htm](http://www.npc.gov.cn/npc/xinwen/2017-11/04/content_2031446.htm).
19. <https://mspoweruser.com/china-invites-microsoft-to-join-technical-committee-260-tc260-to-draft-cybersecurity-rules/>.
20. There is no publicly available list of which WGs allow foreign participants. CSIS identified the above based on news reports from TC260 conferences which cited specific foreign members, as well as from conversations with industry representatives.
21. <https://www.usitc.gov/publications/332/pub4199.pdf>.
22. <https://chinacopyrightandmedia.wordpress.com/2017/05/02/interim-security-review-measures-for-network-products-and-services/>.
23. [http://www.cac.gov.cn/2017-06/09/c\\_1121113591.htm](http://www.cac.gov.cn/2017-06/09/c_1121113591.htm).
24. <http://www.bsa.org/~media/Files/Policy/Trade/09202017USITO2017WTOComplianceFiling.pdf>.
25. [http://www.cnca.gov.cn/xxgk/ggxx/2018/201806/t20180619\\_56714.shtml](http://www.cnca.gov.cn/xxgk/ggxx/2018/201806/t20180619_56714.shtml) and <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress-pauses-power-shifts-chinas-cybersecurity-law-regime/>.
26. <https://www.lawfareblog.com/addressing-chinas-technology-policies-beyond-whiplash-zte-deal>.
27. See the 13th Five Year Plan for Informatization at [http://www.gov.cn/zhengce/content/2016-08/08/content\\_5098072.htm](http://www.gov.cn/zhengce/content/2016-08/08/content_5098072.htm).
28. The Guidelines for Banking Applications of Secure and Controllable Information Technology (2014-2015), <http://www.usito.org/news/cbrc-secure-controllable-guidelines-officially-suspended>.
29. Interviews with industry experts in China.
30. <http://cj.sina.com.cn/articles/view/2853016445/aa0d937d020006u8v>.
31. See, “Information security technology - Controllability evaluation index for security of information technology products - Part 1: General Principles,” [https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20170524124825&norm\\_id=20150901183015&rcode\\_id=23310](https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20170524124825&norm_id=20150901183015&rcode_id=23310).
32. The language of the standard does not specify but the implication is that this refers to the core team of engineers.
33. The formal name is the Cybersecurity Classified Protection Regulation (for public comment). This regulation is the updated iteration of the Multi-level Protection Scheme (MLPS) from 2007. For simplicity, we refer to the regulation as MLPS in this report.
34. <http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html>.
35. For more details on the dynamic between MPS and CAC over regarding CII, please see: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress-pauses-power-shifts-chinas-cybersecurity-law-regime/>.
36. According to industry experts in Beijing, for more detail please see, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress-pauses-power-shifts-chinas-cybersecurity-law-regime/>.
37. This graphic is translated from the graphic in the article “Introduction of the Framework of the Series of Standards on Cybersecurity Multi-Level Protection Scheme (网络安全等级保护系列标准框架介绍),” by Ma Li from MPS MLPS Evaluation Center. <http://www.djbh.net/webdev/web/Academician-ColumnAction.do?p=getYszl&id=8a8182565deefd0d015e799ea2040094>.
38. See the standard called “Information Security Technology - Baseline for Cybersecurity Classified Protection: Part 1: Security General Requirements.”
39. See the standard called “Information Security Technology - Baseline for Cybersecurity Classified Protection Part 1: Security General Requirements.”
40. Interviews with industry experts in Beijing, June and July 2018.
41. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/>.
42. <https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/>.
43. See the CII Security Protection Regulations, draft for public comment released in July 2017, <https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/>.
44. See the standard called “Information Security Technology - Cybersecurity Protection Requirements of Critical Information Infrastructure.”
45. See the standard called “Information Security Technology - Security Controls of Critical Information Infrastructure.”

46. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/>.
47. “National sectoral controlling or supervision departments will, according to the CII identification guidelines, organize the identification of CII within those sectors and those areas, and report the identification results according to procedure,” <https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/>.
48. <https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/>.
49. For a more detailed discussion of the Specification, and what personal data privacy and protection means in China, please see <https://www.csis.org/analysis/what-facebook-scandal-means-land-without-facebook-look-chinas-burgeoning-data-protection> and <https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr>.
50. <http://tech.sina.com.cn/roll/2018-01-12/doc-ifyqqciz5880474.shtml>.
51. [http://www.xinhuanet.com/2018-03/27/c\\_1122597993.htm](http://www.xinhuanet.com/2018-03/27/c_1122597993.htm).
52. [https://www.cov.com/-/media/files/corporate/publications/2017/05/china\\_releases\\_draft\\_encryption\\_law\\_for\\_public\\_comment.pdf](https://www.cov.com/-/media/files/corporate/publications/2017/05/china_releases_draft_encryption_law_for_public_comment.pdf).
53. <https://www.insideprivacy.com/international/china/china-revises-proposals-on-regulation-of-commercial-encryption/>.
54. Article 12 of the Encryption Law stipulates that “CII shall be protected by the use of encryption according to the provisions of laws and regulations as well as the requirements of encryption-related national standards.” There are no standards that exist to support this area of the law.
55. A standard called “Information Technology - Security Techniques - Key Management - Part 1: Framework” adopts and modifies ISO/IEC 11770-1 but with major modifications, which include adding references to China’s commercial encryption algorithms, specifying that “(operators) should adopt cryptographic algorithms that are recognized by state encryption management departments,” and changing original standards for cryptographic algorithms into corresponding domestic cryptographic algorithm standards. Other examples with this same theme include the following standards: “Information Technology - Security Techniques - Message Authentication Codes (MACs) - Part 3: Mechanisms using a universal hash-function” (adopted from ISO/IEC 9797-3: 2011) and “Information Technology - Security Techniques - Authenticated Encryption,” in which all cryptographic algorithms in the standard must be recognized by state encryption management departments.
56. This supports Article 29 of the Encryption Law about what inspectors can do.
57. See Information Security Technology - Security Test Requirements for Cryptographic Modules (ISO/IEC 24759: 2014).