Cybersecurity Classified Protection Regulations
(Draft for Comments)

First Draft to USITO July 13 COB Beijing time, 2018

(Note: relevant text is underlined).

Text of Draft Measure	**Comment**	**Recommendation**
Article 2 (Scope) The Regulations apply to the cybersecurity classified protection work and relevant supervision and management work over the networks constructed, operated, maintained and used within the territory of the People's Republic of China, but not to networks constructed by individuals and families for their own use.	The scope of the regulations is excessively broad, essentially applying to all commercial networks.	We recommend the scope be narrowed to networks intended fo government usage.
Article 10 (Support and assurance) People's Governments at all levels shall encourage and support cybersecurity classified protection-related key actions and projects, support the R&D and application of cybersecurity classified protection technology, and promote secure and trusted network products and services.	The "secure and trusted" formulation has been used in the past to informally signal a preference for domestic Chinese products and/or require intrusive testing of foreign products that could result in IP disclosures.	We recommend removing the reference to "promoting secure an trusted network products and services", as this language has be used in some contexts to encourag the procurement of Chinese produ

Chapter 3 Network Security Protection (3) Level 3 refers to important networks whose damage will cause especially serious harm to the legitimate rights and interests of citizens, legal persons and other organizations, or will cause serious harm to social order and the social public interest, or will cause harm to national security.	Under the previous 2007-era policy that has until now guided MLPS implementation, a network breach would need to cause "serious damage to social order and public interests or harm to national security" for the network to be classified as a level 3 or above.	We recommend removing the nev added factor in the draft regulatio that expands the definition of a le three network to include those wh damage "will cause especially ser harm to the legitimate rights and interests of citizens, legal persons other organizations." While cybersecurity breaches involving individuals are undoubtedly cause serious concern, they do not belor the same category as attacks that would cause harm to national security.
Article 28 (Security requirements for purchase and use of products/services) Network operators shall purchase and use network products and services complying with the requirements of laws and regulations and relevant standards. Operators of L3+ networks shall adopt network products and services commensurate with their security protection level; for the network products to be used for important positions within the network, the operators shall authorize a professional testing & evaluation organization to conduct tests, and based on test results, choose compliant network	We seek further information as to what would be considered "compliant network products."	In the absence of information as t what would constitute "compliant network products," we recommen removing this reference, which m be used to justify preferential treatment of domestic Chinese products.

products. Should a network product/service possibly affect national security, such product/service shall undergo the national security review conducted by the Cyberspace Administration of China in conjunction with the departments involved under the State Council.		
Article 29 (Technical maintenance requirements) L3+ networks shall receive technical maintenance within China, not from overseas. Should remote technical maintenance from overseas be required for business reasons, a cybersecurity assessment shall be conducted, while risk management & control measures shall be taken.		We propose removing the requirement that technical maintenance be undertaken only within China, as it would be burdensome for foreign vendors a may limit the universe of product available to network operators.
Article 31 (Data & information security protection) Network operators shall develop and implement the security protection system for important data and personal information, take protective measures to protect the security of data and information in the course of collection, storage, transmission, use, provision, and destruction, and develop technical measures such as remote backup and recovery to ensure the integrity, confidentiality and availability of important data.	Article 37 of the Cybersecurity Law offers a much narrower construction, saying that "operators of critical information infrastructure shall store, within the territory of the People's Republic of China, personal information and important business data."	The data provisions of the CCP regulations are extremely broad, f surpassing the provisions laid out the CSL, and are loosely worded. example, it is not clear what woul constitute "important data" noted the CCP regulations, though that would appear to be a much broad category than the "important busi data" referred to in the CSL. Moreover, the CCP regulations w apply to network operators in gen not just operators of critical

		information infrastructure. We recommend narrowing Article 31 align with Article 37 of the CSL.
Article 34 (Management and control of risks from new technology and applications) Network operators shall, according to the requirements of the cybersecurity classified protection system, take measures to manage and control security risks from new technology and new applications such as cloud computing, big data, artificial intelligence, the Internet of Things, industrial control systems and mobile Internet, to remove potential security risks.	Article 34 of the CCP regulations would newly extend the security ranking system to the commercial arena.	We would urge the removal of tex that refers to commercial sectors s as cloud computing, big data, artificial intelligence, IoT, industr control systems, and mobile intern The regulatory system described i this document would impose significant and onerous procedure that may have the effect of impos undue costs and slowing the grow of fast-growing technology sector China without yielding compensa cybersecurity benefits. A more effective approach would be to fo on truly critical, national security- related networks such as those rel to the military and government.
Article 47 (Cryptographic protection of non-secrets-related networks) Non-secrets-related networks shall, according to the State's cryptography management laws and regulations and standards, use cryptographic technology,	We seek more information about the process by which cryptographic technology would be approved for use in Level 3+ networks.	We recommend removing this requirement. With the expansion MLPS to cover not just governme but also commercial networks, the provision would effectively mean

products and services. L3+ networks shall adopt cryptographic protection, and use the cryptographic technology, products and services approved by the State's cryptography administrative department. Operators of L3+ networks shall, at the stage of network planning, construction and operation, according to the administrative measures for cryptographic application security assessment and related standards, authorize a cryptographic application security testing & evaluation organization to conduct a cryptographic application security assessment. The network can get online only after the assessment proves compliance.		the state must approve cryptograp technology before it can be emplo in commercial networks. Such a requirement would unnecessarily limit the pool of cybersecurity products and services available to non-governmental/commercial ac As the field of cybersecurity is dynamic and frequently changing there is a risk that companies wou not be able to use the most advanc or recently released versions of so products, because they have not y been state-approved.
Article 50 (Security inspection) Public security organs shall conduct a security inspection for operators of L3+ networks at least once a year. In cases involving other sectors, the security inspection shall be conducted together with the sector's regulatory department. If necessary, public security organs may authorize social entities to provide technical support.	We seek further information on what constitutes a "social entity."	Article 50 suggests that third parti could be authorized by the government to conduct intrusive security inspections, raising conce about the potential for IP disclosu