Confidential – FOR USITO MEMBERS ONLY

美国信息产业机构
United States Information Technology Office

July 27, 2018

To: The Ministry of Public Security of the People's Republic of China
Cc: The Cyberspace Administration of the People's Republic of China

Subject: USITO Comments on the "*Cybersecurity Classified Protection Regulations (Draft for Comments*)"

Dear Ministry of Public Security ("MPS"),

The United States Information Technology Office ("USITO") welcomes the opportunity to comment on the ***Cybersecurity Classified Protection Regulation (Draft for Comments)*** ("*Draft CCPS Regulation*") **released by MPS on June 27, 2018**. USITO represents global ICT enterprises, many of which have longstanding investments in China and are strongly committed to helping foster the sustainable growth of China's economy and ICT industry. USITO's aim is to ensure that MPS achieves its public policy goals without imposing any undue regulatory burden on the commercial activities of the business community. We hope our input will be carefully evaluated, and hope to have continued opportunities to provide comments and perspective on further iterations of the guiding documents.

It is both appropriate and commendable that China adopt smart, agile policies to support a balanced, comprehensive approach to cybersecurity. However, in its current form, the *Draft CCPS Regulation* mandates specific means to achieve outcomes rather than mandating the outcomes that should be attained. This approach expands the Multi-Level Protection Scheme ("MLPS") established in the *Information System Multi-Level Protection Administrative Measures* released in 2007, prescribing a rigid set of rules for the ICT industry and establishing prescriptive and burdensome requirements without necessarily enhancing cybersecurity or achieving its intended objectives. The *Draft CCPS Regulation*, as drafted, will also result in unnecessary confusion and concern for the industry, and is potentially in conflict with its upper law, the *Cybersecurity Law* ("*CSL*"). These issues are elaborated on below:

- The *Draft CCPS Regulation* expands the scope of China's cybersecurity classified protection scheme and lowers the threshold for cybersecurity classified protection Level 3. First of all, this draft regulation far exceeds the scope of the *Information Security Multi-Level Protection Administrative Measures*, released in 2007. While originally focused on information systems,

北京市朝阳区太阳宫中路 12 号太阳宫大厦 1104 室 邮编：100028
联系电话：（86-10）8429-9070 传真：（86-10）8429-9075

the scope of this legislation has now been enlarged to include network foundational infrastructure security, network operations security, and data and information security, and has highlighted the management and control of currently existing and emerging technologies (such as artificial intelligence, etc.). We recommend that the *CCPS Draft Regulation* accord with the its upper law, *CSL*, avoid expanding the scope of MLPS, and refrain from adding unnecessary regulatory items. Secondly, the *CCPS Draft Regulation* has, for the first time, defined important networks whose damage will cause especially serious harm to the legitimate rights and interests of citizens, legal persons and other organizations as Level 3 systems. This revision will create a worrying precedent. According to the *2007 Information Security Multi-Level Protection Administrative Measures*, systems related to national security are defined as Level 3. By characterizing the scope of individual and organizational interests covered by the commercial market as equivalent in importance to national security, the current *CCPS Draft Regulation* not only expands the scope of Level 3, but also includes certain rapidly developing, highly promising ICT markets within this category. This expanded scope provides no truly meaningful benefits for the protection of national security, and could possibly lead to the wasting of scarce public resources and excessive interference in the commercial market.

- The *Draft CCPS Regulation* introduces unreasonable requirements, dramatically adds new obligations for network operators, broadens the scope for log retention, introduces numerous requirements for filing, reviews, inspections, testing, evaluations, and more. Take a Level 3 system, for example: at this level, a network operator must connect to a public security organ at the same level of government. On this point, we would like to emphasize that public security organs should not, under any circumstances, interfere with corporate networks; these types of strict requirements are ineffective and, furthermore, increase cybersecurity vulnerabilities and user privacy risks. In addition, the Draft CCPS Regulation stipulates that Level 3 network operators must undergo one round of cybersecurity-level testing and evaluation every year, conduct a self-inspection every year, pass a cryptographic compliance assessment, and undergo inspection by a public security organ. If the system involves scenarios including the cross-border transfer of personal information and/or important data, an annual assessment is required on top of regular self-assessments and possible regulatory assessments. If the system happens to be identified as critical information infrastructure ("CII"), there is another set of unnecessarily duplicative inspections and assessments that appear to apply under the *Draft Critical Information Infrastructure Protection Regulation* ("*Draft CIIP Regulation*") released in July 2017. Aside from these burdens, the *Draft CCPS Regulation* would also require organizations to obtain additional administrative approvals and licenses, such as the

cybersecurity occupation license in Article 21. These mandatory and broad reporting and compliance requirements in the *Draft CCPS Regulation* can be counterproductive. Imposing such requirements would tend to incentivize businesses to shift scarce resources away from proactively managing evolving risks in a dynamic threat environment to instead complying with retroactive checklists capable of addressing only those vulnerabilities that are already known.

- The new obligations and administrative burdens in the *Draft CCPS Regulation* are potentially much broader than the scope of the *CSL*, under which the *Draft CCPS Regulation* is being created. At the same time, the relationship between certain articles of the *Draft CCPS Regulation* and sections of the *CSL* concerning certification and testing for network(cyber) critical equipment and cybersecurity specific products, as well as the cybersecurity review regime, remains unclear. In order to avoid redundancy and the addition of unnecessary regulations, we recommend that the *Draft CCPS Regulation* should clearly explain the basis and necessity of each regime. This is in line with State Council's proposals and determination to streamline and reduce government administration, including cutting back on vocational qualification licenses, administrative approval items and other measures.[1, 2]

- It is also important to note that the *Draft CCPS Regulation* is not aligned with the *Draft CIIP Regulation,* the latter of which is also being created under the *CSL* but appears to contain a slightly different set of requirements for the protection of CII. This discrepancy will result in not only confusion within the industry, but also unnecessary compliance costs as relevant organizations attempt to comply with both regulations.

---

1 Legislation Law (2015) Article 82: "Without a basis in laws, administrative regulations, or local regulations, or local government rules must not establish norms impairing the rights of, or increasing the duties of, citizens, legal persons, or other organizations."

[2] Legislation Law (2015) Article 80: "The matters provided for by departmental rules shall be within the scope of enforcing laws or State Council administrative regulations, decisions, or orders. Departmental rules not based on a law, State Council administrative regulation, decision or order must not impair the rights of citizens, legal persons or other organizations, or increase the scope of their duties; and must not increase the power of that department or reduce that department's legally-prescribed duties."

- Besides apparent contradictions between the *CSL* and the *Draft CIIP Regulation*, certain clauses in the *Draft CCPS Regulation* are written in broad terms that could make compliance difficult, and that could also leave companies uncertain as to how to satisfactorily address concerns surrounding intellectual property ("IP") and data privacy protection. Additionally, many companies are unclear as to how MPS defines terms such as "new technology," or what steps it will expect them to take to manage and control security risks. Without providing more clarity regarding these issues, the *Draft CCPS Regulation* runs the risk of inadvertently creating obstacles to ensuring IP and data privacy protection.

To ensure effective cybersecurity while addressing all the problems highlighted above, as well as to facilitate global connectivity, USITO recommends that the *Draft CCPS Regulation* should be recrafted to focus on desired cybersecurity outcomes and principles that the industry should incorporate into the network protection measures they adopt. This approach will ensure that the *Draft CCPS Regulation* not only remains within the scope of the *CSL*, but is also consistent with the *Draft CIIP Regulation* and the efforts of the State Council to streamline and reduce government administration.

Finally, the *Draft CCPS Regulation*, like any policy establishing complex cybersecurity obligations, should exempt networks established before the legislation's formal enactment, and should grant an implementation grace period of at least one year for networks currently under construction in order to allow companies to gradually transition and to prepare to implement the new rules. This grace period should be clearly stated in the *Draft CCPS Regulation*. At the same time, work such as compliance checks should only proceed once the final version of the regulation and all corresponding regulatory details have been formally released.

Given the broad implications that the *Draft CCPS Regulation* poses for businesses in China – likely beyond the intentions of the drafters – we hope to engage in further discussions and to have the opportunity to comment on future drafts prior to implementation. As always, USITO remains ready and willing to assist the MPS in developing sound regulations and policies that meet MPS objectives while ensuring that the overall environment for business innovation and growth is not stifled. We thank you for your time and consideration.

United States Information Technology Office (USITO)

USITO is pleased to provide input on specific articles below:

Article	Original Text	Recommendations	Comments
1	**(Purpose and basis)** The Regulations are developed for the purposes of strengthening cybersecurity classified protection work, enhancing cybersecurity protection capability and levels, safeguarding cyber sovereignty and national security and the social public interest, protecting the legitimate rights and interests of citizens, legal persons and other organizations, and promoting the healthy development of informatization in the economy	We recommend clarifying the legal terms included in this section.	Several imprecise wordings (such as "social public interest" or the "healthy development of informatization") can be found throughout the text. Without clear definitions, it will be difficult for industry to understand concretely which requirements are included in the terms highlighted here.
2	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.	We recommend the scope be narrowed to networks intended for government usage.	The scope of the *Draft CCPS Regulation* is excessively broad, which could cause it to apply to all commercial networks.
6	**(Responsibilities and obligations of network operators)** Network operators shall, according to the law, carry out work such as grading networks and determining security levels, security construction and rectification, security level testing & evaluation and self-inspection, taking managerial and technical measures, ensuring infrastructure security, ensuring network operation security, and ensuring data and information security so as to effectively respond to cybersecurity incidents and guard against online violations and crimes.	"Ensuring infrastructure security, ensuring network operation security, and ensuring data ~~and information~~ security"	This should be made consistent with Article 4.
9	**(Setting of standards)** The State shall build and improve a cybersecurity classified protection standard system. The administrative departments	(Setting of standards) The State shall build and improve a cybersecurity classified protection standard system. The administrative	Since the standards supporting rule implementation are quite important, it would be risky to have them be fragmented by industries. For this reason, they should be all national standards.

	for standardization, public security, secrecy, and cryptography under the State Council shall, within their respective responsibilities, develop national/industry standards for cybersecurity classified protection. The State shall support enterprises, research institutions, universities and network-related industry organizations to participate in the setting of national/industry cybersecurity classified protection standards.	departments for standardization, public security, secrecy, and cryptography under the State Council shall, within their respective responsibilities, develop national~~/industry~~ standards for cybersecurity classified protection. The State shall support enterprises, research institutions, universities and network-related industry organizations to participate in the setting of national~~/industry~~ cybersecurity classified protection standards.	
10	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.	We recommend removing the reference to "promoting secure and trusted network products and services", as this language has been used in some contexts to encourage the procurement of Chinese products.	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 international products that could result in IP disclosures.
14	**(Encouraging innovation)** The State encourages the use of new technology and applications to develop cybersecurity classified protection in management and technical protection, and encourages the adoption of technologies such as proactive protection, trusted computing and artificial intelligence to innovate cybersecurity technical protection measures and boost cybersecurity protection capabilities and levels.	(Encouraging innovation) The State encourages the use of new technology and applications to develop cybersecurity classified protection in management and technical protection ~~and encourages the adoption of technologies such as proactive protection, trusted computing and artificial intelligence~~ to innovate cybersecurity technical protection measures and boost cybersecurity protection capabilities and levels.	Since technologies progress quickly, it is not appropriate to point out specific technologies in the *Draft CCPS Regulation*.
15	(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	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~~	Under the previous *Information System Multi-Level Protection Administrative Measures* ("MLPS") released in 2007 (which we understand the CCPS under the *Draft CCPS Regulation* would replace), a network breach would need to cause "serious damage to social order and public interests or harm to national

	serious harm to social order and the social public interest, or will cause harm to national security.	serious harm to social order and the social public interest, or will cause harm to national security.	security" for the network to be classified as a Level 3 or above. Citizens, legal persons and other organizations can protect their legitimate rights and interests by civil or criminal remedies; therefore, it would be best to ensure that Level 3 to Level 5 is only related to the "social order, social public interest and national interests" (i.e. keeping the definition as it was before). Expanding the Level 3 definition will significantly increase the compliance burden for companies, since Level 3 networks require testing and certification. As the threshold for stringent regulation, Level 3 should continue to be limited to specific sectors which are consistent with MLPS1.0. Additionally, what constitutes "serious harm" to social order and the social public interest lacks a clear definition.
16	(Grading of networks) **Network operators** shall determine the security protection levels of networks during the stage of planning & design. When network functions, service scope, targets of service and processed data face significant changes, network operators shall change the security protection level of the network according to law.	We recommend clearly defining what constitutes "significant changes." Additionally, we recommend creating detailed network protection level classification standards to ensure that operators conduct classification accurately.	We would urge MPS to confirm whether the process of re-classification requires a qualified third party.
17	**(Security level examination)** For the proposed L2+ networks, their operators shall organize an expert examination; should the operator be overseen by a relevant department, the examination results shall be reported to the regulatory department for approval. Cross-province or nationwide-operating networks shall be assigned a unified security protection level by the sector-specific regulatory department, which shall organize a unified security level examination. A sector-specific regulatory department may, according to national standard or specification, and based on the sector's network characteristics, develop the guiding opinions on grading of	We recommend creating detailed rules for network operators' self-reviews, including clear requirements for expert selection and expert review procedures. We recommend that the *Regulations* should rely on international standards rather than Chinese national standards. We recommend changing the threshold for arranging "expert reviews" of classification levels to Level 3.	This requirement seems inconsistent with Article 5.2 of the draft standard "Information Security Technology -- Guidelines for grading of classified cybersecurity protection. The standard says that "the special network of cross-provincial services may be classified as a whole or divided into several grading objects by region" (rather than being assigned a unified security protection level). Additionally, no reason has been given for newly requiring network operators at Level 2 to arrange "expert reviews" of their classification levels.

	networks for cybersecurity classified protection.		
18	**(Registration of security levels)** Operators of L2+ networks shall, within 10 work days upon determination of security protection levels of networks, file such results with the public security organs at or above the county level. If a security protection level needs to be changed as a result of withdrawal or change of network, the operator shall, within 10 work days, apply to the original public security organs accepting registration applications for a withdrawal or change of registration. Specific measures for registration shall be developed by the public security department under the State Council.	We recommend that currently existing networks be exempted since they originally complied with all regulations and requirements at the time of their establishment. If currently existing networks are mandatorily required to reconfigure their systems according to the proposed requirements, it could lead to the overall migration or removal of such systems, placing a heavy burden upon enterprises. In addition to exempting currently existing networks, we also recommend that such networks be granted a grace period for filing records in order to ensure that operators fully complete filing procedures.	
20	**(General security protection obligations)** Network operators shall, according to the law, perform the following security protection obligations to assure network and information security: (1) To appoint a leader of cybersecurity classified protection work, build a cybersecurity classified protection work responsibility system and implement the liability investigation system; (2) To develop security management and technical protection rules, and develop personnel management, education & training, system security construction, system security operation & maintenance systems; (3) To implement the rules for server room security management, equipment &	**Article 20 (General security protection obligations)** Network operators shall, according to the law, perform the following security protection obligations to assure network and information security: (1) To appoint a leader of cybersecurity classified protection work, build a cybersecurity classified protection work responsibility system and implement the liability investigation system; (2) To develop security management and technical protection rules, and develop personnel management, education & training, system security construction, system security operation & maintenance systems; (3) To implement the rules for server room security	We suggest clarifying the term "identity authentication" in Article 20 (4) to clarify whose identity needs to be authenticated. We also suggest deleting 20 (5) and using the same "network log" retention requirement in the *CSL,* as this requirement goes beyond the demands of the *CSL*. Additionally, *CSL* Article 50 stipulates "state cybersecurity and informatization departments and relevant departments shall fulfill their responsibility for supervision and management of network information security according to law, and when discovering the release or transmission of information which is prohibited by laws or administrative regulations, shall request the network operators to stop transmission." Thus, we suggest removing "discovering" in Article 20 (8), since this is not the network operator's obligation according to the *CSL* and goes beyond the *CSL* requirement by placing the burden of determining what qualifies as illegal information and evidence of violations and crimes onto the network operator, who may not be the best party to determine this question. For Article 20 (10), we suggest that the

	media security management, and cybersecurity management, and to develop operating specifications and workflows; (4) To implement managerial and technical measures for identity authentication, prevention of infection and dissemination of malicious code, and prevention of network intrusion & attacks; (5) To implement managerial and technical measures for monitoring and recording network operational status, cybersecurity incidents and online violations & crimes, and to retain relevant network logs for more than 6 months that can trace online violations and crimes; (6) To implement the measures such as the categorization, backup, and encryption of important data; (7) To collect, use or process personal information according to the law, as well as implement personal information protection measures to prevent the leaking, destruction, tampering, theft, loss, and abuse of personal information; (8) To implement measures such as discovering, blocking, and removing illegal information, and to implement measures such as guarding against the widespread dissemination of illegal information and the destruction and loss of evidence of violations and crimes; (9) To perform the responsibility such as Internet access filing and	management, equipment & media security management, and cybersecurity management, and to develop operating specifications and workflows; (4) To implement managerial and technical measures for identity authentication, prevention of infection and dissemination of malicious code, and prevention of network intrusion & attacks; ~~(5) To implement managerial and technical measures for monitoring and recording network operational status, cybersecurity incidents and online violations & crimes, and to retain relevant network logs for more than 6 months that can trace online violations and crimes;~~ (5) Adopt technical measures for monitoring and recording network operational statuses and cybersecurity incidents, and follow relevant provisions to store network logs for at least six months; (6) To implement the measures such as the categorization, backup, and encryption of important data; (7) To collect, use or process personal information according to the law, as well as implement personal information protection measures to prevent the leaking, destruction, tampering, theft, loss, and abuse of personal information; (8) To implement measures such as ~~discovering,~~ blocking~~,~~ and removing	reporting duty should be limited to only Level 3 or above networks and on those serious incidents known or discovered by the network operator. 72 hours is the standard global practice for this kind of security incident reporting. Finally, because “incidents” in Chinese covers both incidents and law cases, this term must be defined more clearly.

	to check users' real identity; (10) Any incidents in the network shall be reported to local public security organs within 24 hours; in cases involving State secrets, such incidents shall also be reported concurrently to local administrative departments for secrecy. Other cybersecurity protection obligations specified in laws and administrative regulations.	illegal information, and to implement measures such as guarding against the widespread dissemination of illegal information and the destruction and loss of evidence of violations and crimes; (9) To perform the responsibility such as Internet access filing and to check users' real identity; (10) Any serious incidents in the network that is a Level 3 or above network and that are known to or discovered by the network operators shall be reported to local public security organs within ~~24~~72 hours after it is known or discovered by the network operator; in cases involving State secrets, such incidents shall also be reported concurrently to local administrative departments for secrecy. Other cybersecurity protection obligations specified in laws and administrative regulations.	
21	**(Special security protection obligations)** Operators of L3+ networks, in addition to performing the cybersecurity protection obligations specified in Article 20 of the Regulations, shall also perform the following security protection obligations: … (2) To develop and implement the overall cybersecurity plan and holistic security protection policy, as well as develop a security construction plan which shall be reviewed by professional personnel for approval; … (3) To conduct a security background review for the cybersecurity leader and	**(Special security protection obligations)** Operators of L3+ networks, in addition to performing the cybersecurity protection obligations specified in Article 20 of the Regulations, shall also perform the following security protection obligations: … ~~(2) To develop and implement the overall cybersecurity plan and holistic security protection policy, as well as develop a security construction plan which shall be reviewed by professional personnel for approval;~~ … (5) To implement the monitoring & alert measures associated with cybersecurity	We seek clarification on the connection required under 21 (5). Does the connection mean a personnel point of contact for MPS for regular reporting/filing or a real-time system-to-system connection? This requirement seems excessively intrusive if it requires a technical connection with the network operator's system. This type of unfettered connection with public security organs would make it extremely difficult for network operators and users to determine if their privacy, proprietary information and legal interests were properly protected when using the network. The *CSL* also contains a requirement that network operators provide technical support and assistance to public security organs. The *Draft CCPS Regulation* should refrain from expanding the *CSL*'s scope by asking for excessive access to network operators' networks. For these reasons, we believe it would be too burdensome for all Level 3 + systems to be required to

	employees holding critical cybersecurity posts, and to implement the occupational license-based work system; … (5) To implement the monitoring & alert measures associated with cybersecurity situation awareness, to build a cybersecurity protection management platform, to conduct a dynamic monitoring and analysis for network operational status, network traffic, user behavior and cybersecurity incidents, and to connect with public security organ systems of the same level;	situation awareness, to build a cybersecurity protection management platform, to conduct dynamic monitoring and analysis for network operational status, network traffic, user behavior and cybersecurity incidents under the premise of protecting personal information, private information and commercial secrets in accordance with the law, ~~and to connect with public security organ systems of the same level;~~	"connect with public security organ systems". This requirement should be removed or only limited to personnel points of contact. Additionally, since Level 3 certification testing and the annual cybersecurity level testing & evaluation already cover the requirements stated in Article 21 (2). We suggest deleting Article 21 (2). This will help reduce the compliance burden for legal entities without affecting security. The detailed contents of the "security background review" specified in Article 21 (3) remain unclear. These contents should be specified.
22	**(Test before getting online)** Newly built L2 networks, before getting online, shall, according to relevant cybersecurity classified protection standards, undergo a network security test. Newly built L3+ networks, before getting online, shall undergo security level testing & evaluation conducted by a cybersecurity level testing & evaluation organization according to relevant cybersecurity classified protection standards, and will start operations only after the testing & evaluation process proves compliance.	In order to avoid redundancy, we recommend clarifying the division of work for security testing and reviews between the *Draft CCPS Regulation* and the *CSL*. Additionally, we recommend clarifying that security level testing and evaluation should be conducted by an authorized cybersecurity level testing & evaluation organization.	If a service or product has passed the security review required by the *CSL*, will it have to go through testing again? What is the relation between *Draft CCPS Regulation* and the *CSL*? If so, this requirement runs the risk of leading to redundancy in licensing, which would act as another burden for the industry.
23	**(Security level testing & evaluation)** Operators of L3+ networks shall conduct a cybersecurity level testing & evaluation every year, identify and rectify potential risks, and report to the regulatory public security organs on the cybersecurity level testing & evaluation process and results every year.	We recommend clarifying whether such annual testing & evaluation is a self-action or a third-party action, as well as whether this article will require companies being measured according to the GBR/T28448, 28449 standard.	
25	**(Self-inspection)** Network operators shall conduct at least one self-inspection of their implementation of cybersecurity classified		The "networks" here cover Level 1. According to Article 18, only networks above Level 2 must report to regulatory public security organs. Will Level 1 entities also be required to file reports?

	protection and their network security status every year. They shall also identify potential risks and make timely rectifications, and report to the regulatory public security organs.		
27	Network service providers, including cybersecurity level testing & evaluation organizations, shall keep confidential the State secrets, personal information and important data they access during the service process…	Network service providers, including cybersecurity level testing & evaluation organizations, shall keep confidential the State secrets, commercial secrets, personal information and important data they access during the service process…	We believe commercial secrets should also be well-protected in this case. Additionally, according to the *CSL* definition, the term "network service provider" refers to the network operator. It appears that here, the "network service provider" also includes third-party organizations such as "network security evaluation service providers." Why has this change been made?
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 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.	**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 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.~~	We seek further information as to what would be considered "compliant network products" and "important positions." These phrases are so vague that they might be used to justify preferential treatment for certain products. It is important that the *Draft CCPS Regulation* avoid creating the conditions for breaches of important obligations in the GATT, GATS and TBT Agreement. *See e.g.,* GATT Article III:4; GATS Article XVII; TBT Agreement Art. 2. We would like to point out that according to Article 35 of the *CSL*, only CII operators "purchasing network products and services that might impact national security shall undergo a national security review." We believe that Level 3 network operators are not equal to CII operators, and therefore suggest deleting this requirement to avoid the improper expansion of administrative power, as well as to avoid stifling innovation in China. Finally, this Article seems to introduce a new testing requirement for operators of Level 3+ networks when they procure and deploy certain network products and services. The introduction of new certification and testing & evaluation schemes is redundant, does not enhance cybersecurity, and may only cause more market uncertainties.
29	**(Technical maintenance requirements)** L3+ networks shall receive technical maintenance within China, not from overseas. Should remote technical maintenance from	**(Technical maintenance requirements)** L3+ networks that are identified as CII, shall receive technical maintenance ~~within China, not from overseas. Should remote~~	Since Level 3 network operators are not equal to CII operators, we suggest adding the phrase "that are identified as CII" to make sure the words are more accurate, to help avoid the improper expansion of administrative power, and to avoid stifling innovation in China.

	overseas be required for business reasons, a cybersecurity assessment shall be conducted, while risk management & control measures shall be taken. For each technical maintenance, the operator shall generate and retain a technical maintenance log and provide unaltered maintenance logs when public security organs conduct an inspection.	~~technical maintenance from overseas be required for business reasons, a cybersecurity assessment shall be conducted, while risk management & control measures shall be taken.~~ For each technical maintenance, the operator shall generate and retain a technical maintenance log and provide unaltered maintenance logs when public security organs conduct an inspection.	We also propose removing the requirement that technical maintenance be undertaken only within China, as it would be burdensome for international vendors and may limit the range of products available to network operators. If the technical maintenance requirement is kept, its scope must be defined, and the specifics of which entities will conduct "cybersecurity assessments" and the methods they will use in remote cases must be provided.
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.	We recommend narrowing Article 31 to align with Article 37 of the *CSL*. Additionally, we suggest removing the word "remote" to align with the *CSL*.	The data provisions of the *Draft Regulation* are extremely broad, far surpassing the provisions laid out in the *CSL*, and are vaguely worded. For example, it is not clear what would constitute the "important data" noted in the *Draft Regulation*. Moreover, the *Draft Regulation* would apply to network operators in general, not just operators of CII. Article 37 of the *CSL* 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." Secondly, according to Articles 21 and 34 of the *CSL*, only CII operators shall conduct disaster recovery backups (remote backups) of important systems and databases. Network operators shall just "adopt measures such as data classification, back-up of important data."
33	**(Requirements for audit & checks)** In cases where a network operator constructs, operates, maintains and uses its network to provide the public with service activities requiring an administrative license, the regulatory department shall include the implementation of the cybersecurity classified protection system in the scope of audits and checks.	We recommend removing this Article.	Increasing the auditing and examination powers of numerous industry regulators would heighten industry concerns over confidentiality, and would also risk creating issues of inconsistency and duplicated work between MPS and other agencies.
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	We would urge the removal of text that refers to commercial sectors such as cloud computing, big data, artificial intelligence, IoT, industrial control systems, and mobile internet. The regulatory	Article 34 of the *Draft CCPS Regulation* would newly extend the security ranking system to the commercial arena. This could be a huge obstacle for companies due to limited resources, employees, and data. For instance, many new technology companies have industrial control system networks. Would this automatically

	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.	system described in this document would impose significant and onerous procedures that may have the effect of imposing undue costs and slowing the growth of fast-growing technology sectors in China without yielding compensatory cybersecurity benefits. A more effective approach would be to focus on truly critical, national security-related networks such as those related to the military and government. Additionally, we also recommend to more precisely define the term "new technologies."	qualify these new companies for CCPS Level 3?
45	**(Determine cryptography requirements)** The State's cryptography administrative department shall, according to a network's security protection level and the secret level and protection level of secrets-related networks, determine the security assessment requirements for the configuration, use, management and application of cryptography, and develop cryptographic standards for cybersecurity classified protection.		We seek clarification on when "**security assessment requirements**" will be determined, and when "**cryptographic standards for cybersecurity classified protection**" will be set up. USITO hopes that new rules will refrain from setting up new testing and assessment requirement for cryptography if the same requirements can already be found in existing rules and regulations. In addition, it would be helpful to clarify whether chapter 5 – "Cryptographic management" – is referring to 1) Products with encryption as their core function or 2) All products containing encryption. We suggest that the Year 2000 clarification [3]that these regulations only apply to products with encryption as their core function should be kept.
46	**(Cryptographic protection of secrets-related network)** Secrets-related networks and the State's secret information transmitted over the network shall, according to law, adopt	**(Cryptographic protection of secrets-related network)** Secrets-related networks and the State's secret information transmitted over the network shall, according to law, adopt	In modern IT, almost all products use cryptographic technology. By requiring products that use cryptographic technology but are not "cryptographic products" as defined by the cryptography administrative department to be subject to cryptographic tests (which may

[3] In an announcement issued March 2000 by the People's Republic of China State Encryption Management Commission General Office (SEMC), China confirmed that "*the scope of the management of "encryption products and equipment containing encryption technology" incorporated in the [commercial encryption] regulations, only limits specialized hardware and software for which encryption and decoding operations are core functions; other things, including wireless telephones, Windows software, browser software, etc., are not included in the scope.*"

	cryptographic protection. Cryptographic products shall be approved by the cryptography administrative department, and the products containing cryptographic technology such as software system and hardware shall pass the cryptographic test. The testing, deployment, purchase and use of cryptography is uniformly administered by the cryptography administrative department. The system design, operation & maintenance, routine management and cryptography assessments shall follow the State's cryptography management regulations and standards.	cryptographic protection. Cryptographic products shall be approved by the cryptography administrative department~~, and the products containing cryptographic technology such as software system and hardware shall pass the cryptographic test~~. The testing, deployment, purchase and use of cryptography is uniformly administered by the cryptography administrative department. The system design, operation & maintenance, routine management and cryptography assessments shall follow the State's cryptography management regulations~~ and standards~~.	require Chinese encryption), there is a risk that China would exclude many products – particularly hardware and software products made by multinational companies – from being used in secrets-related networks. This will negatively impact global trade. Furthermore, excluding products containing cryptographic technology from secrets-related networks would also hinder systems connectivity and the achievement of connectivity globally. As a member of the World Semiconductor Council (WSC) and an active contributor to the Government/Authorities Meeting on Semiconductors (GAMS), China has promised to abide by WSC encryption principles concerning commercial-use encryption technology for popular ICT products, including limiting the supervision of commercial-use encryption and forbidding the designation of certain encryption technology. Abiding by these principles also ensures that China upholds the promises it made when it entered the WTO, which include complying with the GATT, GATS and the TBT Agreement (s*ee e.g.,* GATT Article III:4; GATS Article XVII; and TBT Agreement Article 2, which states that members shall not have "prepared, adopted or applied with a view or with the effort of creating unnecessary obstacles to international trade".) (https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm).
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, 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	We recommend removing this requirement. With the expansion of MLPS to cover not just government but also commercial networks, the provision would effectively mean that the state must approve cryptographic technology before it can be employed in commercial networks. Such a requirement would unnecessarily limit the pool of cybersecurity products and services available to non-governmental & commercial actors. As the field of cybersecurity is dynamic and frequently changing, there is a risk that companies would not be able to use the most advanced or recently released versions of some products, because they have not yet been	We seek to understand the stipulations concerning the encryption products and services used by Level 3+ networks. Most products and services made by multinational companies only use internationally accepted cryptographic encryption, and do not support Chinese encryption. This will exclude most MNC products from being used in Level 3 networks, and will significantly impede global trade in IT. These stipulations will also contravene the WSC/GAMS and WTO/TBT principles noted in our comments on Article 46. Secondly, allowing only "cryptographic technology products and services that are approved by the State's cryptography administrative department" will also disable and affect users (including commercial companies) in achieving the connectivity globally. Furthermore, requirements on cryptographic technology is too granule and lacks flexibility. Finally, cryptography assessment "at least once

	cryptographic application security testing & evaluation organization to conduct a cryptographic application security assessment. The network can get online only after the assessment proves compliance. After starting operations, an assessment shall be conducted at least once a year. The cryptographic application security assessment results shall be filed with the public security organs accepting registration applications and the local cryptography administrative department.	state-approved. Furthermore, we recommend that after starting operations, any assessment should be conducted only if there are significant changes in the network.	a year" is unnecessary and burdensome.
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. When public security organs conduct supervision & inspections according to the law, network operators shall provide assistance and cooperate, and at the request of public security organs, provide unaltered data information.	**(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~~ qualified security inspection agencies to provide technical support. When public security organs conduct supervision & inspections according to the law and with sufficient prior written notification of the contents in question, participants involved, and actions to be undertaken during the inspection, network operators shall provide assistance and cooperate after receiving prior written notification from public security organs, and at the request of public security organs, provide unaltered data information.	We seek further information on what constitutes a "social entity." Article 50 also suggests that third parties could be authorized by the government to conduct intrusive security inspections, raising concerns about the potential for IP disclosures.
55	**(Incident investigation)** Public security organs shall, according to relevant rules, dispose of cybersecurity incidents, conduct investigations of incidents, determine the responsibility for incidents, and	We recommend removing the final sentence of this article. However, if the final sentence is kept, we recommend changing it as follows: "Network operators shall	Given that it has already been stated that "public security organs may order network operators to take emergency measures such as blocking information transmission, suspending network operation, and making backups", the final sentence of this article is redundant.

	deal with violation/criminal activities endangering cybersecurity according to law. If necessary, public security organs may order network operators to take emergency measures such as blocking information transmission, suspending network operation, and making backups of relevant data. Network operators shall assist and support public security organs and departments involved to investigate and respond to incidents.	lawfully assist and support public security organs and departments involved to investigate and respond to incidents."	
56	**(Access cutoff measures in emergency cases)** Should potential risks in the network seriously threaten national security, social order and the public interest, public security organs, in emergency cases, may order the operator to cut off network access and suspend system operations for rectification purposes.	**(Access cutoff measures in emergency cases)** Should potential risks in the network seriously threaten national security, social order and the public interest, public security organs, in emergency cases, may order the operator to cut off network access and suspend system operations for rectification purposes with the decision or approval by the State Council.	According to Article 58 of the *CSL*, for major social security emergencies, the adoption of interim measures, such as limiting network communications for certain regions, will be subject to approval by the State Council.
59	**(Industry supervision & management)**		This section requires greater clarity. What will supervision and management entail?
62	**(System for arranging cybersecurity-related meetings)** When the public security department, secrecy administrative department and cryptography administrative of the People's Governments at or above the provincial level identify relatively serious potential risks in the network while performing supervision and management of cybersecurity classified protection, or if security incidents occur, these departments may arrange to meet and talk with the legal representative and head of the network operator involved and the sector-specific regulatory department.	**(System for arranging cybersecurity-related meetings)** When the public security department, secrecy administrative department and cryptography administrative of the People's Governments at or above the provincial level identify relatively serious potential risks in the network while performing supervision and management of cybersecurity classified protection, or if security incidents occur, these departments may arrange to meet and talk with the legal representative and head of the network operator involved and the sector-specific regulatory department. Relevant departments shall provide	

		prior written notification to the liable parties before any meeting.	
66	**(Cybersecurity service responsibility)** In the case of violating the provisions of Article 26 third paragraph or Article 27 second paragraph, public security organs shall order rectification, and depending on the circumstance, give a warning alone or concurrently, confiscate illegal income, and impose a fine of more than 1 time but less than 10 times the illegal income, and in case of no illegal income, impose a fine of less than 1 million yuan.	**(Cybersecurity service responsibility)** In the case of violating the provisions of Article 26 ~~third~~ second paragraph or Article 27 second paragraph, public security organs shall order rectification, and depending on the circumstance, give a warning alone or concurrently, confiscate illegal income, and impose a fine of more than 1 time but less than 10 times the illegal income, and in case of no illegal income, impose a fine of less than 1 million yuan.	
73	**(Effective date)** The Regulations shall come into force as of _____.	**(Effective date)** The Regulations shall come into force as of _____ and the *Administrative Measures for the Multi-Level Protection of Information Systems (2007)* will abolished once this Regulation becomes effective.	