Published on *The National Law Review* https://natlawreview.com

China Releases New Regulation on Cybersecurity Inspection

Article By:

Yan Luo

Ashden Fein

Moriah Daugherty

On September 30, 2018, China's Ministry of Public Security ("MPS") released the *Regulation on the Internet Security Supervision and Inspection by Public Security Organs* (the "Regulation";??????????????), which will take effect on November 1, 2018.

As the latest regulation issued by MPS that implements China's Cybersecurity Law ("CSL"), which took effect in June last year, the Regulation sets forth detailed procedural guidance describing how Public Security Bureaus (China's police force, commonly referred to as "PSBs") conduct cybersecurity inspections of companies that provide a broad range of "Internet services" in China.

Scope and Applicability

Specifically, the Regulation permits local PSBs (at the county level and above) to conduct cybersecurity inspections on four types of Internet service providers and "network-using entities" (??????)[1] (collectively, "Internet service providers"):

- providers of Internet access, data centers, content distribution, and domain name services;
- providers of Internet information services;
- providers of Internet access to the public; and
- providers of other Internet services.

Precisely which companies will be subject to the Regulation is unclear, as the Regulation leaves local PSBs broad discretion to decide whether a company falls into the Regulation's purview, including the ability to interpret what services are considered "other Internet services."

PSBs' Power and Inspection Procedures

The Regulation provides local PSBs a wide range of power and discretion to inspect an Internet service provider's premises and network, both on-site and remotely. Specifically, PSBs are authorized to enter a company's physical premises—including data centers—to conduct an

unannounced onsite inspection, review and copy documents, and interview company executives. PSBs are also authorized to conduct remote inspections, provided that the company is informed of the time and scope of the inspection before the inspection is conducted. In addition, PSBs are allowed to engage qualified third party vendors to provide technical support for the PSB's inspections.

A PSB's inspection can focus on whether the company has:

- filed for record with the PSB as a "network-using entity";
- implemented internal cybersecurity programs and appointed an officer in charge of cybersecurity;
- recorded and retained registration information and web logs of users;
- taken measures to prevent computer viruses and cyberattacks;
- taken measures to prevent the transmission and publication of illegal content;
- cooperated and provided assistance to PSBs in investigations relating to national security, terrorism, and crimes; and
- fulfilled its obligations to meet the requirements of the Cybersecurity Multi-Level Protection Scheme ("MLPS"), which requires network operators take certain measures to protect their networks based on their relative impact on national security, social order, and economic interests if the system is damaged or attacked.

Further, PSBs are required to keep records of all inspections, which must be signed by the PSB officer(s) conducting the inspection and any qualified third party vendors who provided technical support for the inspection. In the case of an on-site inspection, a company executive or officer in charge of cybersecurity is also required to sign the inspection record. Although the company can offer explanations in the inspection record if it disagrees with the result of the inspection, the company representative is required to sign the record; refusing to sign the inspection record will be noted in the inspection record itself.

Penalties

If a company fails an inspection, PSBs are authorized to impose a range of penalties. For minor administrative violations, PSBs are authorized to request that the company remediates the issue. The company can request another inspection after it has completed the remediation.

For more substantive violations, the Regulation provides a laundry list of penalties under the CSL and China's Counter-Terrorism Law ("CTL"; ??????????) enacted in 2015 for failures to implement cybersecurity measures and engagement in illegal conduct relating to cybersecurity. These penalties, ranging from warnings and orders to remediate to the imposition of substantial fines and detention of individuals, are summarized in the chart below.

Violation	*Penalty*
Failure to implement cybersecurity management systems and procedures or failure to designate an officer in charge of cybersecurity. Article 21(1)	CSL Article 59 – order to remediate and a warning; monetary fines on company and on responsible individuals
Failure to take measures to prevent computer virus, cyberattacks and other activities endangering cybersecurity. Article 21(2)	
Failure to maintain records of Internet service	

users registration information and web logs. Article 21(3)	
Where the company is engaged in providing services relating to Internet content distribution or instant messaging, failure to request service users to provide true identity or provides services to users that did not provide true identity. Article 21(4)	CSL Article 61 – order to remediate; monetary fines on company and on responsible individual(s); shutting down websites and revoking business permit.
	CTL Article 86 (if failed to verify users' identity or provides services to unidentified users): monetary fines on company and on responsible individual(s)
Failure to cease, remove, and maintain records of the transfer of illegal or prohibited content in the course of providing public information services. Article 21(5)	CSL Article 68 or 69
	CTL Article 84 (if failed to remove, keep records of, or cease the transfer of terrorism information, or stop services) – monetary fines on company and on responsible individual(s); where the violation is deemed serious, in addition to monetary fines, individuals may also be detained for five to 15 days.
Failure to provide technical support and cooperate with PSBs' activities relating to national security or criminal investigation. Article 21(6)	CSL Article 69
	CTL Article 84
Where the inspection identifies that the company has illegally obtained, sold, or otherwise provided to others personal information and where the conduct does not constitute a crime. Article 22	CSL Article 64 – confiscation of illegal gains and a fine between one time and ten times of the illegal gains; where there is no illegal gains, a fine below RMB 1 million shall be imposed.
Where the inspection identifies that the company has placed malware in the services it provides. Article 23	CSL Article 60(1) – order to remediate and a warning; monetary fines on company and on responsible individual(s)
Where the company refuses inspection or obstructs the inspection. Article 24	CSL Article 69
	CTL Article 91 and 92 – monetary fines on company and on responsible individual(s); where the violation is deemed serious, in addition to monetary

fines, individuals may also be detained for five to 15 days.

Impact

Even though the Regulation codifies existing practices rather than imposing wholly new obligations, the Regulation will likely pave the way for more cybersecurity enforcement actions from PSBs in the future. The Regulation also potentially overlaps with other MPS regulations aiming to implement the CSL, such as the *Regulations on Cybersecurity Multi-level Protection Scheme*, and further guidance from MPS is expected to clarify how different implementing regulations interact.

---

[1] According to the *Administrative Measures for the Protection of International Networking Security of Computer Information Networks* (??????????????????????), which was issued by MPS in 1997 and amended in 2011, “network-using entities” are entities connected to the Internet and are required to file with local PSBs for record.

National Law Review, Volume VIII, Number 297