Draft Chinese Cybersecurity Rules Don't Offer Clarity for Companies

By John Butcher

New draft regulations to implement China's cybersecurity law have failed to quash compliance concerns among U.S. companies operating there, cybersecurity compliance professionals told Bloomberg BNA.

The recently released draft regulations provide a definition of critical information infrastructure (CII) covered by the country's new cybersecurity law. The draft regulations also detailed other obligations for companies considered CII by the Chinese authorities. But, far from providing enough clarification to ease concerns about Beijing's cybersecurity efforts, the draft regulations raise new questions about what companies fear is a worryingly broad law, the cybersecurity pros said.

Jake Parker, vice president of the U.S.- China Business Council in Beijing, told Bloomberg BNA that the draft was “mischievously vague,” allowing for a wide interpretation by Chinese regulators.

“Companies are concerned about how broad the definition remains,” he said, and there is unlikely to be much greater clarification after a comment and discussion period on the draft concludes Aug. 10.

“We may see some changes around the fringes, but the feeling is that it is purposefully vague to give flexibility on how it is enforced,” Parker said.
Manuel Maisog, privacy partner and chief representative of law firm Hunton & Williams in Beijing, told Bloomberg BNA that the draft is spreading concern to a wider range of companies than previous drafts, because it includes sectors such as the media and food and drug companies that weren't expected to be regarded as within the CII framework.

Covered Business Sectors

The draft details the scope of what constitutes critical information infrastructure as potentially including energy, finance, transportation, water conservation, health care, education, social insurance, environmental protection, public utilities, telecommunications, media, cloud computing, big data, large-scale public information network services, science and technology for national defense, large equipment manufacturing, chemical manufacturing, food, and drug sectors.
True clarification of what is counted as CII is likely to come only when the Cyberspace Administration of China publishes a handbook setting out the rules, a step alluded to in the draft, Maisog said.

Until then the current draft remains merely an “offer of clarification” which sets out industries that might be affected, Maisog said.
Previous guidance documents have highlighted health care in general. Carly Ramsey, a

regulatory risk specialist at risk consulting company Control Risks Group Holdings Ltd in Shanghai, said the inclusion of pharmaceuticals separately under the new draft is also significant.

“The new specific listing of pharmaceuticals suggests there is a focus on that area and companies should be particularly careful,” she told Bloomberg BNA.

Liability Issues

The draft adds a provision that would make both a critical information infrastructure company and the person in charge of operations at a CII company liable for cybersecurity breaches. “From a legal compliance perspective this raises risks that legal teams don't like to think of,” Parker said.

While the draft remains vague on who might be considered the person in charge, other areas of Chinese government regulation where enforcement is more advanced, such as tax, bribery, product quality and environmental rules, provide a pointer to who the government might hold responsible.

“The authorities can and have gone after both the employee in charge of that particular area and the legal representative,” Ramsey said.

Requirements in the underlying cybersecurity law that companies store CII data within China and meet industry regulator standards in addition to the cybersecurity law present a huge compliance burden, she said.

Compliance Officer, Audits

The draft requires CII operators to have a specific cybersecurity compliance team or officer and to conduct an annual compliance audit. Both of these requirements are causing concern among U.S. companies, according to Parker.

There are fears that the requirement for a compliance officer will be tailored to Chinese companies, he said. This could potentially mean that a non-Chinese person couldn't be hired for the role, which is likely to require government certification, Parker said.

The draft allows for the annual cybersecurity compliance audit to be conducted either internally or by an external service provider. It is likely, according to Parker, that these external service providers will require government certification, and that again could exclude foreign companies.

If only Chinese companies are allowed to conduct audits, multinationals may not be comfortable with providing information largely because of concerns over the security of any data collected, Parker said.