COVINGTON

China Releases Updated Draft Encryption Law for Public Comment

July 17, 2019

Data Privacy and Cybersecurity
Trade Controls

On July 5, 2019, China's Standing Committee of the National People's Congress (NPC) published a new draft Encryption Law ("the draft Law") for public comment. The draft Law, if enacted as drafted, would bring significant new changes to China's commercial encryption regime.

The State Cryptography Administration ("SCA") previously issued an initial draft of this law for public comment on April 13, 2017 ("the 2017 Draft") (see Covington's alert on the previous version here). After the release of the 2017 draft, the regulatory regime in China for commercial encryption products was revamped significantly (see Covington's previous alert here). The State Council removed certain approval requirements for the production, sale, and use of commercial encryption products in late September 2017, and the SCA issued further notices reducing the burden imposed on manufacturers, distributors and users of commercial encryption products. The draft Law proposes further changes to this revamped regime, including for example introducing different categories of encryption, and establishing license requirements for certain imports and exports, while carving out items in "general use."

The comment period ends on September 2, 2019.

Key Points of the Draft Law

Definition and Classification of Encryption

Consistent with the 2017 draft, "encryption" is defined as "products, technologies or services applying specific transformations to information to effect encryption protection or security authentication" (Article 2). The draft Law retains the three categories of encryption as in the 2017 draft: core encryption, ordinary encryption, and commercial encryption (Article 6). "Core" encryption and "ordinary" encryption are used for the protection of information constituting "state secrets,"[1] while commercial encryption is used to protect information that is not considered state secrets. Commercial encryption is not further defined, so companies are still left without significant guidance regarding when a particular technology is "commercial encryption" and thus subject to the Law.

[1] Under Chinese law, state secrets are classified into three levels, top secret, secret and confidential. The difference between "core" and "ordinary" encryption is that "core encryption" can be used to protect all three levels of state secret, but "ordinary encryption" can be used only to protect state secrets at the secret and confidential levels.

Furthermore, core encryption and ordinary encryption -- but not commercial encryption -- are themselves considered state secrets, and the draft Law requires SCA to implement strict regulatory requirements for the "research, production, testing, deployment, use and destruction" of core encryption and ordinary encryption (Article 7).

Commercial Encryption

Use of Commercial Encryption

The draft Law confirms that any entity and individual can use commercial encryption to protect network and information security in accordance with laws. Note that this provision would not distinguish domestically produced commercial encryption and foreign-produced commercial encryption, which significantly departs from the existing regime.

According to the *Regulations on Administration of Commercial Encryption*, the existing regulations released in 1999, no entity or individual is allowed to distribute or use foreign-produced commercial encryption products (Article 13 and 14). As a general rule, entities and individuals must use approved encryption products manufactured in China. For foreign entities (including foreign-invested entities) and individuals, the regulations offer an exception: such entities and individuals can apply to the SCA to import foreign-produced commercial encryption products for their own use.

The draft Law also states that the government will encourage the development of the commercial encryption industry and will seek to create an open market with "orderly competition" (Article 8).

Import and Export Control Requirements

The draft Law establishes an import licensing and export control framework that governs (i) the import of commercial encryption that "may impact national security or the public interest" and "provide an encryption protection function," and (ii) the export of commercial encryption that "may impact national security or the public interest" or is required by China's international obligations. The list of commercial encryption in scope of this framework is expected to be published by the Ministry of Commerce in conjunction with the SCA and the General Administration of Customs at an unspecified later date (Article 28).

The same provision also makes clear that these import licensing and export control requirements do not apply to commercial encryption used in "products for consumption by the general population." The draft Law does not define this term, leaving unclear how this important exemption would work in practice. Note that as explained above, under the existing regime, only foreign individuals and entities (including foreign-invested enterprises) may import foreign-produced encryption products for their own use, and such imports may be subject to the prior approval by the local SCA.

Standards for Commercial Encryption

The draft Law stresses the role of standard setting in the development of the commercial encryption industry and vows to encourage not only the development of national standards, but also industry and enterprise standards with more stringent technical requirements than the national standards (Article 22). With respect to international standards, the draft Law states that the Chinese government will actively participate in formulating international standards and promote the interoperability of domestic and international standards. The government also will encourage organizations and enterprises to participate in international standard-setting activities (Article 23).

Article 24 provides that companies engaging in the "research, production, sale, service and import/export" of commercial encryption shall comply with mandatory national standards in this area and their own published technical standards, in addition to complying with laws and regulations.

Testing and Certification

Similar to the Cybersecurity Law, the draft Law establishes a testing and certification system and encourages organizations and enterprises to voluntarily apply for the testing and certification of their commercial encryption products (Article 25).

Special Requirements for Critical Network Equipment and Critical Information Infrastructure

The draft Law also sets out special requirements for Network Equipment and Network Security-specific Products. Commercial encryption products listed in the Catalogue of Critical Network Equipment and Network Security-specific Products ("Catalogue") (the first edition of the Catalogue can be found here) must pass the security certification or security testing conducted by qualified institutions (Article 26). Commercial encryption services provided for products listed in the Catalogue are also subject to such testing and certification requirements.

Separately, if operators of critical information infrastructure (CII) are required to adopt commercial encryption for security purposes (in order to comply with other laws and regulations), the draft Law requires such CII operators to carry out a security assessment on their use of commercial encryption. If the procurement and use of commercial encryption products and services may impact national security, CII operators must apply for a *national security* review led by the Cyberspace Administration of China ("CAC") and SCA (Article 27). It is possible (but not certain) that the national security review referenced in this provision will follow the same process proposed in the draft *Measures on Cybersecurity Review*, which was released by CAC on May 24, 2019 (see our summary here).

Enforcement and Penalties

The draft Law provides an enforcement structure that requires the SCA and other government agencies to establish a regulatory framework combining daily supervision with random inspections. In addition, the government plans to link this enforcement mechanism with China's social credit system (Article 31), although it is unclear how the two systems will interact.

The final section of the draft Law includes a number of provisions specifying penalties for non-compliance. For example, if an entity distributes or sells commercial encryption products or services that do not obtain certification or fail testing, then the Administration for Market Regulation may issue a warning and confiscate illegal gains (Article 36). CII operators that fail to comply with Article 27 and exporter/importers failing to comply with Article 28 will be penalized under the relevant provisions of the Cybersecurity Law and the Customs Law.

Potential Implications

The draft Law, if enacted as drafted, would represent significant changes in how commercial encryption is regulated, including imports and exports. While the long-term effect of the draft

Law may result in overall simplification, a number of key provisions remain unclear,[2] and without those details, it is difficult to predict how the draft Law may (or may not) impact companies operating in China.

Finally, the draft Law may overlap with the Cybersecurity Law and its implementation regulations. For instance, the draft Law requires CII operators to apply for a national security review in the event the network products or services involving commercial encryption they procured might impact China's national security. It is unclear whether this refers to the same review process as proposed by CAC in its draft *Cybersecurity Review Measures* or a separate process to only evaluate encryption security for CII operators.

Companies with encryption-related technologies operating in, selling into, or developing encryption-related solutions in China should monitor these developments closely.

If you have any questions concerning the material discussed in this client alert, please contact the following Covington attorneys:

Yan Luo	+86 10 5910 0516	yluo@cov.com
Eric Carlson	+86 21 6036 2503	ecarlson@cov.com
Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com

[2] For example, the draft Law is silent on whether manufacturers still have to obtain a *Product Model Certificate of Commercial Encryption Products* before they can produce such products, as currently required.