The New Chinese Encryption Regime: Towards a Sustainable Approach

January 2, 2020

Authors
Susan Munro, Michael Vatis, Stewart A. Baker, Edward Lin (Legal Consultant)

Overview

With the coming into effect of the new PRC Encryption Law on January 1, China is moving steadily to develop and implement an encryption regime that protects core state security interests, while allowing businesses that do not implicate state security to create, trade and use encryption relatively freely. Additionally, it appears that restrictions on foreign investment in the encryption sector and the deployment of foreign encryption technologies, products and services in Mainland China are to be relaxed. The expectation is that the new regime will be rolled out on a phased basis in 2020.

The Standing Committee of the PRC National People's Congress passed the PRC Encryption Law on October 26, 2019 and government authorities were required to issue amendments to existing encryption regulations and rules by January 1, 2020. On December 30, 2019, however, the State Cryptography Administration (SCA) and other PRC authorities issued two administrative notices regarding the import, export, and certification of encryption products that provided for phased implementation of the Encryption Law.[1]

Overview

PRC law defines encryption as “products, technologies and services that use certain transformations to effect encryption protection and security authentication.” Encryption is divided into three categories: core encryption, common encryption and commercial encryption. Core encryption and common encryption are used to protect state secrets, whereas commercial encryption is used to protect information that does not constitute state secrets. State secrets transmitted via wire communications and wireless communications and information systems that store and process state secrets must be encrypted and are subject to security authentication. Core encryption and common encryption are themselves state secrets, and their research, manufacture, testing, deployment, use and destruction is subject to state secrecy laws and regulations.

The Encryption Law contains general requirements imposed on the SCA in relation to regulation of core encryption and common encryption, and on enterprises participating in research and development, manufacturing, testing, deployment, use, and destruction of core encryption and common encryption.

Towards a Level Playing Field

The Encryption Law aims to establish a “robust, unified, open, competitive and orderly commercial encryption system,” and to “encourage and promote the development of the commercial encryption industry.” Government authorities at all levels must abide by this non-discrimination principle and treat all entities, including foreign invested enterprises (FIEs) that engage in commercial encryption research, production, sales, service, import and export (Commercial Encryption Practitioners), equally. Specifically, administrative agencies and their staff must not use administrative means to force the transfer of commercial encryption technologies, including foreign encryption technology.
Except for certain commercial encryption products discussed below, the Encryption Law does not impose licensing requirements on commercial encryption research, development, production, sale, import or export. If no further restrictions are introduced in forthcoming amendments and implementing regulations, FIEs generally will be able to engage in research, development, production, sale, import, and export of commercial encryption products and technologies in China without obtaining specific licenses or authorizations from the SCA.\[2\]

**Domestic Standards and Interoperability with International Standards**

The Encryption Law provides for the establishment of a commercial encryption standards system that functions together with the three encryption categories, comprising national, industrial, group and enterprise standards. National standards are either mandatory or voluntary, while generally industrial standards, group standards and enterprise standards are voluntary.

Commercial Encryption Practitioners must comply with both mandatory national standards and published standards. Currently, there is no mandatory commercial encryption-related standard, but it is expected that regulations defining such standards will be issued.

The potential divergence between Chinese encryption algorithms and similar algorithms developed outside of Mainland China resulting in the non-operability of the latter has been of concern to foreign companies operating in China. The Encryption Law provides in very general terms that the state will promote participation in international commercial encryption standardization activities and the interoperability of domestic and foreign standards. Further clarification of this provision is awaited.

**Development of Commercial Encryption Testing and Certification System**

The Chinese government will promote construction of a commercial encryption testing and certification system, and formulate technical specifications and rules. Enterprises manufacturing commercial encryption will be encouraged to submit their products and services for testing and certification on a voluntary basis in order to improve their commercial competitiveness.\[3\] Enterprises are not required to procure certified encryption products, but may be subject to certain requirements under the PRC Network Security Multi-Level Protection Scheme as provided in the Cybersecurity Law that impact which products they can purchase.\[4\]

Under the new encryption regime, commercial encryption testing and certification institutions (Testing Institutions) must obtain relevant qualifications, and perform testing and certification in accordance with relevant laws, regulations, standards, etc. Importantly, testing institutions are required to keep confidential any state secrets or trade secrets that come to their attention in the course of commercial encryption testing and certification activities.

The Encryption Law and other PRC foreign investment related laws and regulations currently do not impose special restrictions on foreign investors with regard to establishing and operating commercial encryption testing and certification institutions. In theory, foreign investors will be permitted to establish wholly owned commercial encryption testing and certification institutions in China, which may help to allay the concerns of foreign companies submitting proprietary encryption for testing. According to the SCA, currently there is only one commercial encryption certification institution and four commercial encryption testing institutions, none of which is foreign invested.

**Commercial Encryption Supervision System**

The Encryption Law also provides that the SCA and other departments will establish a commercial encryption supervision system that includes day-to-day monitoring and random checks, establishes a uniform commercial encryption supervision and management information platform, and promotes coordination between the commercial encryption supervision system and the forthcoming Chinese social credit system. During the course of their supervisory activities, the SCA are prohibited from requiring Commercial Encryption Practitioners and testing and certifying institutions to disclose encryption-related proprietary information, such as source codes.

**Critical Network Equipment and Network Security Product Catalog**

Under the Encryption Law, commercial encryption products that involve national security, national economy, or implicate people's livelihoods or societal interests are included in the Critical Network Equipment and Network Security Product Catalog (Security Product Catalog) formulated by the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology, the Ministry of Public Security, and the Certification and Accreditation Administration. Commercial encryption products that fall within the catalog may be sold in or supplied in China only after passing relevant security certification or testing conducted by qualified testing or certification institutions. Commercial encryption services that use critical network equipment and network security products also are required to pass designated security certification or testing conducted by qualified testing or certification institutions before they can be provided to customers.

**Critical Information Infrastructures**
Operators of critical information infrastructures – defined in the Cybersecurity Law as information infrastructures that, if experiencing damage, loss of function, or data leakage could threaten national security, the national economy, or people's livelihoods or the public interest – must use commercial encryption to protect their infrastructures and perform commercial encryption application security assessments. The SCA has formulated the Administrative Measures on the Security Assessment of Commercial Cryptography Application (Trial) (Security Assessment Measures), mandating commercial encryption application security assessments for entities that construct, use, or manage networks or information systems in key areas that implicate national security and societal interests. Currently, it appears the Security Assessment Measures have been implemented in specific geographical areas as pilot projects, and it is expected that the SCA will issue new application security assessment measures applicable to all networks and information systems in due course. The Encryption Law suggests that operators of critical information infrastructures should coordinate commercial encryption application security assessments, critical information infrastructure safety evaluations, and network security multi-level protection schemes in order to avoid duplicating processes.

Network products and services involving commercial encryption procured and used by critical information infrastructure operators and government agencies that could affect national security must pass a national security review jointly organized by the CAC and the State Cryptography Administration.

Import and Export of Commercial Encryption

The Encryption Law provides that commercial encryption contained in mass consumer products will not be subject to control upon import from or export to Mainland China. However, commercial encryption that possesses the function of encryption protection and affects national security or societal interests will be subject to import controls, and commercial encryption that affects national security or societal interests or is subject to international obligations to which China has committed, will be subject to export controls. MOFCOM, SCA and the General Administration of Customs are due to formulate and publish a catalog listing commercial encryption products subject to import and export controls. Before publication of the catalog, Commercial Encryption Practitioners engaging in import of encryption products and equipment containing encryption technologies and export of encryption products still need to obtain licenses from the SCA.

[1] Notice Regarding Adjustment of Regulatory Approach for Commercial Encryption Products of the State Cryptography Administration and the State Administration for Market Regulation (Notice 39) and the No. 38 Notice of the State Cryptography Administration, the Ministry of Commerce and the General Administration of Customs (Notice 38).

[2] Notice 39 confirms that producers of encryption products will no longer be required to obtain model certificates.

[3] Notice 39 provides that the SCA will issue a catalog of encryption products, and encourage Commercial Encryption Practitioners to certify those products.

[4] Article 47 of the Draft Network Security Multi-Level Protection Regulations published by the Ministry of Public Security on June 27, 2018 provides that networks of Tier III and above shall use encryption technologies, services and products recognized by the SCA. The Information Security Technology - Basic Requirements of Network Security Multi-Level Protection, which is a voluntary standard used for MLPS compliance assessment, requires that networks of Tier II and above use only encryption technologies and products that have been certified and approved by the SCA.

[5] According to Notice 38, MOFCOM, SCA and GAC are still formulating the import and export catalog.

Practices
Privacy & Cybersecurity