Left | **Jim Dao** — Registered Foreign Attorney – jim.d@tilleke.com
Center | **Giang Thi Huong Tran** — TMT Consultant – giang.t@tilleke.com
Right | **Tu Ngoc Trinh** — Attorney-at-Law – ngoctu.t@tilleke.com

New Law on Cyber Security in Vietnam

Vietnam's new Law on Cyber-Information Security (LCIS) was passed on November 19, 2015, and it will take effect this year on July 1. This is the first comprehensive law ever issued in Vietnam on the security of "cyber-information," which is information exchanged in a telecommunications or computer network environment. Previous regulations on the subject had been scattered throughout different pieces of legislation, such as the Law on Information Technology; the Law on Telecommunications; the Law on E-Transactions; Decree 72 on the management, provision, and use of Internet services and online information; the Penal Code; and information security regulations for specific sectors such as banking and finance.

The key aspects of the LCIS include assurances for the safety and security of cyber-information; protection of personal information in the network environment; protection of information systems and infrastructure; production, trading, and use of civil ciphers; standards and technical regulations on information security; provision of information security services; prevention of spam, computer viruses, and harmful software; and emergency responses.

The LCIS retains the main principle of existing data privacy regulations in that the collection, processing, and use of personal information of an individual requires the consent of that person. It also reemphasizes the importance of active prevention, detection, stopping, and handling of computer viruses and harmful software as well as the prevention and stopping of sabotage or use of information for the purpose of terrorism.

The new law requires intermediary service providers (e.g., enterprises providing email services or transmitting and storing information) to have malware-filtering systems in the course of sending, receiving, and storing information via their systems and to send reports to competent state agencies in accordance with the law. It also requires organizations and individuals, within their authority and responsibilities, to prevent the sabotage of information originating from their information infrastructure, to collaborate with one another in identifying sources, and to counter and remedy the consequences of cyber-attacks carried out via the information systems of domestic and foreign organizations and individuals.

The new law further aims to enhance capacity-building in cyber-information security and encourage organizations and individuals to invest in and enter into joint ventures and associations with other organizations in building higher-education institutions and vocational-training institutions with a view to training human resources for cyber-information security.

A current problem with the LCIS is that its scope of applicability is quite broadly defined. Accordingly, it seems to pose some new requirements and challenges which could apply to many business operators in Vietnam. On its face, the law includes a number of provisions that might apply to many organizations that own information and information systems, defined as a combination of hardware, software, and databases for creating, transmitting, and storing information, among other matters, in a network environment. Needless to say, many businesses could fall under this broad scope. These provisions include the following:

- Organizations which own information must classify information based on varying levels of secrecy in order to take appropriate protective measures.
- Those collecting information are subject to inspections and examinations on an annual basis, and on an extraordinary basis when deemed necessary by the relevant state agencies.
- Organizations which own information systems must classify their systems according to levels of security from 1 to 5 (with 5 as the highest level). These levels reflect the potential harm that a security breach could cause to other entities, social order, and national security, among other matters. These organizations must also formulate policies and rules to ensure cyber-information security when designing, developing, managing, operating, using, updating, or deactivating information systems.
- Organizations which own information systems are also responsible for protecting their information systems, and must determine the security level of their information systems; assess and manage security risks to information systems; supervise, monitor, and check the protection of information systems; take measures to protect information systems; comply with the reporting regime; and conduct activities to disseminate information and raise awareness about cyber-information security.

It is not clearly defined in the LCIS as to what suffices as compliance for many of the aspects set out above.

While the LCIS retains the existing requirements that the production, trading, or importation of civil cryptographic products requires a license, it poses a new requirement for the use of civil ciphers (i.e., cryptographic techniques and products used to keep secret or authenticate information that is not classified as state secrets). In particular, organizations and individuals that use civil cryptographic products provided by enterprises which are not licensed to do business in those products must declare such use to the Government Cipher Committee. Certain organizations, such as foreign consular offices, are exempt from making this declaration.

The LCIS sets out regulations for new types of products and services:

- Cyber-information security products, which include, among others: civil cryptographic products; cyber-information security testing and evaluation products; and products to counter cyber-attacks and hacking.
- Cyber-information security services, which include, among others: cyber-information security testing and evaluation services; services relating to information confidentiality which do not use civil cryptography; civil cryptographic services; e-signature certification services; data recovery services; and cyber-attack prevention and countering services.

The provision of cyber-information security services and trading in cyber-information security products are subject to licensing. An importer might need to obtain a cyber-information security product import permit depending on its cyber-information security imports.

While the new law is a welcome step in codifying the regulations on the vital issue of cyber-information security, it still needs further detail and guidance in several areas. The expectation is that subordinate legislation will soon be issued to clarify the practical realities of the LCIS, and will hopefully include a more narrow scope of applicability.