On 13 April 2017, the Office of the State Commercial Cryptography Administration ("OSCCA") published the first draft Cryptography Law of the People’s Republic of China. The draft law seeks to provide a unified approach to the regulation of cryptography (defined as “any object or technology which uses a special alteration to encrypt or authenticate data or other information”), including its production, sale, import, export, testing, certification and use. The draft consolidates various aspects of the existing cryptography regime (which has been in place since 1999), and earmarks certain areas for further detailed regulation.

We consider below the key areas of the draft law that are likely to be of general interest to users of cryptography in the PRC.

**Critical information infrastructure ("CII") encryption**

<table>
<thead>
<tr>
<th>Relevant draft provisions</th>
<th>CII should be encrypted in accordance with applicable law and national cryptography standards. Encryption is to be planned, built and operated simultaneously with the related CII.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implications</td>
<td>The Cyber Security Law provides that the State Council will pass rules defining the scope of CII and the terms of its protective measures. It is unclear whether new cryptography standards are to be set by the State Council, or if the standards under the current rules (last issued in 2008) will apply. The current cryptography standards are not publicly available.</td>
</tr>
</tbody>
</table>

“Critical information infrastructure should be encrypted in accordance with applicable law and national cryptography standards.”
National security review of CII

Relevant draft provisions

CII-related cryptographic products, services and systems which affect national security will be subject to a national security review.

For the purposes of conducting the review, the State is to categorise the cryptographic applications in CII according to their respective security level.

Implications

The draft law expressly includes cryptography (including cryptographic systems) within the requirement of the Cyber Security Law for a national security review to be conducted on CII products/services which affect national security. Presumably, such review is to be initiated by the State authorities. No details of the national security review requirements or process are provided.

Cryptographic products – import and export controls

Relevant draft provisions

The import/export licensing regime is to be administered by OSCCA and the Ministry of Commerce (“MOFCOM”). MOFCOM, in consultation with OSCCA and the General Administration of Customs (“GAC”), will publish a list of products subject to import and export control.

Implications

The draft law gives MOFCOM new roles in the issue of these licences and the publication of the product list (both of which are handled by OSCCA and GAC under the current rules).

It is unclear whether MOFCOM’s new roles will lead to changes to the current procedures for import/export licensing, or to the composition of the current nine-item list which was last updated at the end of 2013.

Licensing

Relevant draft provisions

OSCCA administers a licensing regime for the sale/business use of cryptography products and provision of cryptography services (excluding cryptography used for state secrets, which is subject to a separate regime).

“Critical information infrastructure-related cryptographic products, services and systems which affect national security will be subject to a national security review.”

“MOFCOM, in consultation with OSCCA and the General Administration of Customs, will publish a list of products subject to import and export control.”

“In addition to the current catalogue of approved cryptography products, a catalogue of cryptography services is to be published by OSCCA.”
### Implications:

In addition to the current catalogue of approved cryptography products, a catalogue of cryptography services is to be published by OSCCA.

### Crisis management

<table>
<thead>
<tr>
<th>Relevant draft provisions</th>
<th>OSCCA, in consultation with other ministries, will put in place procedures to monitor cryptography and provide early warnings, and to report, consult on important issues and handle crises in relation to cryptography.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implications</td>
<td>The Cyber Security Law contains requirements to collect, analyse and report information in order to monitor IT networks and provide early warnings, and for the Cyberspace Administration of China to coordinate network security contingency plans. To the extent these initiatives relate to CII, they are to be coordinated by the responsible ministries (e.g. China Banking Regulatory Commission, “CBRC”). The draft law requires that these contingency plans should specifically address cryptography issues. In most cases, specific crisis management measures will be contained in industry-level rules (generally, yet to be published). Taking the published CBRC rules as an example, banks are required to have contingency plans and set contingency recovery benchmarks at key departments and dedicated teams. Banks are required, on an annual basis, to conduct an overall rehearsal, compile a report on the adequacy of the procedures and act on the findings.</td>
</tr>
</tbody>
</table>

### Decryption

<table>
<thead>
<tr>
<th>Relevant draft provisions</th>
<th>Telecoms business operators and Internet service providers/users can be required to provide decryption support if required for national security or criminal investigation by the people’s procuratorate, public security bureau or national security authorities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implications</td>
<td>This extends the principle in the Anti-terrorism Law (which only requires decryption support to prevent or investigate terrorist activities). Thus, the authorities could cite economic, social or other strategic justifications, in addition to terrorism, in requiring businesses to provide support in decrypting their networks.</td>
</tr>
</tbody>
</table>

“OSCCA, in consultation with other ministries, will put in place procedures to monitor cryptography and provide early warnings, and to report, consult on important issues and handle crises in relation to cryptography.”

“Telecoms business operators and Internet service providers/users can be required to provide decryption support if required for national security or criminal investigation by the people’s procuratorate, public security bureau or national security authorities.”
Sanctions and other powers

| Relevant draft provisions                                                                 | The draft law broadens the range of powers available to OSCCA, including empowering it to act alone in enforcing its provisions. To impose sanctions under the current rules, a joint decision by OSCCA and other authorities such as GAC is required. The new sanctions largely track the Cyber Security Law. In addition to sanctions, the draft law enables OSCCA to take the following action when carrying out monitoring and investigation: (i) entry into premises; (ii) interrogation of personnel; (iii) review and copy contracts and records; (iv) lock down or detain equipment and facilities; and (v) lock down of premises. |
| Implications                                                                             | Businesses should take the proposed provisions into consideration when deciding where their cryptography-related facilities and information are to be located. |

“In addition to sanctions, the draft law enables OSCCA to take the following action when carrying out monitoring and investigation: (i) entry into premises; (ii) interrogation of personnel; (iii) review and copy contracts and records; (iv) lock down or detain equipment and facilities; and (v) lock down of premises.”

As the draft law has yet to complete the multiple readings at the National People’s Congress or its Standing Committee required by the PRC legislative process, whether or not it will be passed in its current form is unclear. That said, it shows the clear intention of the PRC authorities to bring cryptography within the stricter regulatory framework of the Cyber Security Law and its related rules. Cryptography users in the PRC should therefore pay attention to the provisions on CII and import/export of cryptographic products, in particular, as well as the additional compliance obligations on crisis management and decryption.
References

*Cryptography Law of the People’s Republic of China (Draft for Discussion)* 《中华人民共和国密码法（草案征求意见稿）》, OSCCA, 13 April 2017

*Cyber Security Law of the People’s Republic of China* 《中华人民共和国网络安全法》, National People’s Congress Standing Committee, 7 November 2016 (the “Cyber Security Law”)

*Anti-terrorism Law of the People’s Republic of China* 《中华人民共和国反恐怖主义法》, National People’s Congress Standing Committee, 27 December 2015 (the “Anti-terrorism Law”)

Author: Bryan Chan

This publication is intended merely to highlight issues and not to be comprehensive, nor to provide legal advice. Should you have any questions on issues reported here or on other areas of law, please contact one of your regular contacts, or contact the editors.

© Linklaters LLP. All Rights reserved 2017

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of the LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP and of the non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ, England or on www.linklaters.com.

This firm is not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services to clients because we are regulated by the Law Society of England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide.

We currently hold your contact details, which we use to send you newsletters such as this and for other marketing and business communications.

We use your contact details for our own internal purposes only. This information is available to our offices worldwide and to those of our associated firms.

If any of your details are incorrect or have recently changed, or if you no longer wish to receive this newsletter or other marketing communications, please let us know by emailing us at marketing.database@linklaters.com.