DIGITALEUROPE

ESIA
The voice of the Semiconductor Industry in Europe

**DIGITALEUROPE and ESIA response to the Office of State Commercial Cryptography Administration Draft Cryptography Law**

*Brussels, 1 September 2019*

DIGITALEUROPE and ESIA greatly appreciate the opportunity to submit comments to the draft Cryptography Law of China put forward by the Office of State Commercial Cryptography Administration (OSCCA).

For the information society to flourish and grow, it must be based on the principles of trust and security, in particular with regard to the transmission and computing of data. DIGITALEUROPE's and ESIA's members remain highly committed to the principles of trust and security. Therefore, we greatly appreciate the efforts put forward by the People's Republic of China to build towards to a more trustworthy and prosperous information society. Please find below summarised descriptions of our comments.

- **Articles 6, 7 and 8**: The functional definition of cryptography, i.e. the division into core, common and commercial cryptography, could benefit from further explanation. If essentially 'core' and 'common' encryption describe technology and services for securing two different levels of state-classified information, the technical characteristics could be further defined by the competent bodies. The transition between the two fields also needs to consider security measures (handling of classified information) beyond encryption.

  In particular, the distinction between the three fields (as outlined in Article 7) is not clear and may be even more blurred when it comes to the use of commercial cryptography in products and services that are or could be used by government entities or fully/partially state-owned enterprises. We recommend that the law include a definition of commercial cryptographic products. We believe that such a definition should be fully compatible with the core function clarification issued by the State Encryption Management Commission in March 2000.

  Commercial Cryptography should be defined as cryptography implemented in commercial products where cryptographic functions use standardised algorithms to support clearly identified product features. While including encryption/decryption functions, Commercial Cryptography excludes authentication or digital signatures. In our proposed amendment to the definition of Commercial Cryptographic Product, encryption should be the main function, rather than a subsidiary feature of the product or one of its components.

  A component in a product should not be considered a Cryptographic Commercial Product in the following cases:

1) Cryptography is not the primary function or set of functions of the component;
2) The component does not change any cryptographic functionality in the products; or
3) The feature set of the component is fixed, cannot be modified to customer specification or is not specifically designed for a particular customer.

For all three categories, it should be made clear that products and services that may be used are admitted on a non-discriminatory basis and on a market-based approach.

- **Articles 21, 22 and 23:** We appreciate the commitment towards the promotion of a competitive commercial cryptography industry. In this context, we understand this also as a commitment to include Foreign-Invested Enterprises (FIEs) under this definition.

  When it comes to the development of 'national' standards, we reiterate our recommendation to use products and services based on commercial encryption regardless of the geographic origin of the underlying standards, thus allowing private, commercial and government entities to use best-in-class products that are globally accessible. As is required of all WTO members, China's national standards should use international standards, or relevant parts thereof, as their basis, except where the use of such standards or parts of such standards would be ineffective or inappropriate.

  Clearly, 'group' or 'enterprise' standards that are even higher should be promoted, notwithstanding the origin of the innovator. They could then lead, of course, to an even higher (general or industry) standard that is publicly accepted. However, we are concerned that the reference made to 'independent innovative technology' may hamper the pursuit of this objective as it indicates a decoupled development, putting in danger economies of scale for users and industry alike. This lowers, rather than raises, the security profile.

  Furthermore, the mention of 'independent' should be eliminated in accordance with Article 23, in reference to which we applaud OSCCA's commitment to engaging in applying international standards and bringing in, at the same time, Chinese expertise. In addition, Article 23 should not only encourage participation in the creation of international standards but should also encourage organisations to base their standards on already established and relevant international standards.

- **Article 24:** We suggest a clarification in the encouragement to apply 'voluntary national' and 'industry' standards. In order to avoid incompatibilities, and due to existing obligations under WTO agreements, there should be a clear preference for internationally accepted and used standards (which may be de-facto standards set up and used by industry or standards that have been worked out in international standardisation bodies), attributing an auxiliary function to national standards in fields where there is no other standard.

- **Articles 25 and 26:** We welcome and support the modifications in the second Draft Law aimed at separating commercial cryptography from core and common cryptography, as

well as the exclusion of commercial cryptography used in mass consumer products from import licensing system or export control.

In addition, the overall scope of 'Commercial cryptography-based services used for network-critical equipment and cybersecurity-specific products' has incrementally expanded and will ultimately have a significant impact on organisations that provide network-critical equipment and cybersecurity-specific products. This concern is aggravated by the duplicative testing that seems to be proposed under the Draft Law.

The vast majority of organisations already use commercial cryptography. Needing to obtain certain certification through a security agency or pass a security test for such cryptography already in use would stifle industry. The concerns articulated under this Article are already addressed by the draft of proposed measures recently published and Article 23 of the Cybersecurity Law. Thus, and given China's obligations under the World Semiconductor Council's Encryption Principles[1] and international agreements,[2] the Article should clearly state that sales of products should not be restricted and, to the extent needed, only the deployment of or specific use of a product in network-critical settings may require certification or testing.

Commercial products with elements of cryptography that are a subsidiary feature should be completely exempt from licensing, testing and certification requirements that limit import, export or sales. This includes all products where cryptography is not the core function or set of functions of the product.

In addition, the new added term 'Commercial cryptography-based service,' which is unclear, should not exceed the scope of currently regulated PRC services, as e-government digital certificate service, and defined as a service where encryption serves as the main function of the service, rather than as a subsidiary service or as one of many features.

- **Article 28:** In order to secure and extend the manufacturing base of innovative FIEs in the People's Republic of China, we encourage the State Council to consider that China has meanwhile become, for many companies, a hub for global production, including the export to other countries in Asia. Therefore, any additional restrictions on technology export could hamper this development and slow down FDI.

  It is therefore recommended that Article 28 be limited to commercial encrypted products where encryption is core function and expanded beyond the existing 2013 list (OSCCA), ensuring greater alignment to already implemented international standards and agreements. Import and export of commercial encryption products should not be regulated.

[1] WSC Encryption Principles of Joint Statement of the 17th Meeting of the World Semiconductor Council (WSC), (23 May 2013) (Lisbon, Portugal), endorsed in Government/Authorities Meeting on Semiconductors, 26 September 2013 (Jeju, Korea), available at www.semiconductorcouncil.org/wp-content/uploads/2016/04/May-2013-WSC-WSC-Encryption-Principles-FINAL.doc

[2] Annex 1 to WSC Encryption Principles of Joint Statement of the 17th Meeting of the World Semiconductor Council (WSC)

- **Article 30**: We are highly interested to bring in our knowledge when it comes to building up a Chinese commercial cryptography industry association and both submit our request to be included in the consultative phase of setting up such a body.

  However, it is recommended that the draft law provide greater clarity with regard to the details of the 'commercial cryptography industry association.' We recommend that such an association should allow both foreign and domestic companies to be members with full participation rights.

- **Article 31:** With reference to the social credit system, we would appreciate receiving further information on implications for industry and its activities in People's Republic of China.

  In addition, whilst we welcome the changes made to the originally broad enforcement powers (Article 29), it is recommended that Article 31 state that any 'random checks' shall not impact intellectual property and privacy rights. Overall, any checks should be conducted with minimal disruption to business operations and provide protection for intellectual property rights and confidential information.

- **Article 32:** Although Articles 9, 10 and 11 encourage RandD, subsequently Articles 12, 21 and 32 seem to impinge on this possibility. It is recommended that an exception should be added to Article 32 for good faith security and vulnerabilities research aimed at improving security of the technology and products. Such research should not be considered illegal/criminal nor subject to any penalty or legal liability.

## Annex I

### Specific comments and proposals on the Draft of the PRC Cryptography Law

| Article | Original Text | Comments | Recommendations |
|---|---|---|---|
| | | **Chapter 1 – General** | |
| **Article 2** | The term Cryptography as used in this Law refers to products, technology and services that are used to, via certain conversion techniques, provide encryption protection or perform security authentication for information and so on. | Some examples for the products, technology and service, alongside clarifying the definition and scope would be highly beneficial. | We recommend the definition of products, technology and services here, encryption should be the main function, rather than a subsidiary feature of the product or one of its components.<br><br>*See recommendation in Article 8 for definitions of products, technology and services.* |
| **Article 6** | Cryptography is classified into core cryptography, common cryptography and commercial cryptography. The State introduces a classification-based approach to cryptography. | We welcome and support the approach aimed at separating commercial cryptography from core and common cryptography. We have suggested a definition for commercial cryptography in Article 8 in this regard. | The three categories of cryptography (core, common and commercial) should be further explained. More detailed comments below (Article 8). |
| **Article 8** | Commercial cryptography is used to protect information not falling within State secrets. Citizens, legal persons and other organisation may all use commercial cryptography to protect the network and information security, in accordance with the law. | We propose that Commercial cryptography should be defined as cryptography implemented in commercial products in the case that cryptographic functions use standardised algorithms to support product features which are defined. It should include encryption or decryption functions but not include authentication, digital signatures and hash-based integrity checks. Most jurisdictions around the world distinguish products where cryptography is used to strengthen another functionality, such as authentication, or to ensure integrity of a products, e.g. digital signature. The regulatory approach in China also recognises this distinction for cryptography.<br><br>We deem key characteristics of commercial products with elements of cryptography: 1) being offered for sale on open markets, without restrictions, to consumers, businesses and governments; 2) implementing standardised cryptographic algorithms in support of defined features of the product.<br><br>In a commercial cryptographic product, encryption is the main function, rather than a subsidiary feature of the product or one of its components. | This Article should include the following definitions:<br><br>***Commercial cryptography means cryptography implemented in commercial products where cryptographic functions use standardised algorithms to support defined product features.***<br><br>***Commercial cryptographic (or cryptography-based) product means a product where encryption is the main function, rather than a subsidiary feature of the product or one of its components.***<br><br>***Aligned with this approach, a component in a product, in this regard, is not considered a cryptographic commercial product if:***<br><br>***a) Cryptography is not the primary function or set of functions of the component.***<br>***b) The component does not change any cryptographic functionality in the products.***<br>***c) The feature set of the component is fixed, cannot be modified to customer specification or is not*** |

| | | | |
|---|---|---|---|
| | | We would suggest adding also a definition of commercial cryptographic or cryptography-based service. This should not exceed the scope of current PRC regulated service, as e-government digital certificate service (see also below Article 26). | ***specifically designed for the customer.***<br><br>***Commercial cryptographic (or cryptography-based) service means a service where encryption serves as the main function of the service, rather than as a subsidiary service or as one of many features.*** |
| **Chapter 3 – Commercial Cryptography** | | | |
| **Article 21** | The State encourages the research and development and application of commercial cryptographic technology, works towards a unified, open, pro-competitive and orderly commercial cryptography market system, and encourages and promotes the development of the commercial cryptography industry.<br><br>The scientific research, production, sale, service and import and export of commercial cryptography shall not impair national security, social and public interests or the legitimate rights/interests of citizens, legal persons and other organisations. | Although Articles 9, 10 and 11 encourage RandD, Articles 12, 21 and 32 seem to impinge on this possibility. In particular, the language of Article 21 regarding national security, social and public interest seems too broad and could potentially undermine both the import of strong cryptography and the strength of encryption. | Delete the sentence: *'The scientific research, production, sale, service and import and export of commercial cryptography shall not impair national security, social and public interests or the legitimate rights/interests of citizens, legal persons and other organisations.'* |
| **Article 22** | The State shall develop a commercial cryptography standard system while improving it.<br><br>The administrative department for standardisation under the State Council and the State cryptography administration department shall, per their respective responsibilities, lead the efforts to develop national and industry standards for cryptography.<br><br>The State supports social organisations and enterprises in harnessing their own innovative technologies to develop social organisation standards and enterprise standards for commercial cryptography which are higher than relevant technical requirements of national standards and industry standards. | The law should require that national and industrial standards use international standards associated with cryptography, except when they would not be effective or appropriate, provided the importance of international standards in the field of cryptography as well as China's obligations under the WTO TBT agreement (notably Article 4.1 and Annex 3, paragraph F).<br><br>We further recommend that social organisations and enterprises use international standards, according to relevant requirements in WTO TBT agreement (Article 4.1 and Annex 3, paragraph F). In fact, if social organisations and enterprises adopt standards higher than the national industry standards, this would lead to inconsistency and confusion between conflicting standards.<br><br>Additionally, the Law should minimise the mandatory nature of national standards for cryptography, but rather encourage a voluntary use. In fact, the Chinese government and five other governments adopted the World Semiconductor Council's Encryption | We recommend that the Article be modified as follows (additions in bold, deletion in bold strikethrough):<br><br>*The State shall develop a commercial cryptography standard system while improving it.*<br><br>*The administrative department for standardisation under the State Council and the State cryptography administration department shall, per their respective responsibilities, lead the efforts to develop national and industry standards for cryptography*.<br><br>***National and industry standards for cryptography shall use international standards, or relevant parts thereof, as their basis, except where the use of such standards or parts of such standards would be ineffective or inappropriate. These standards shall be voluntary and not mandatory. Social organisations and enterprises shall use the same international standards.*** |

| | | | |
|---|---|---|---|
| | | Principles,[3] which 'make it clear that generally there should be no regulation of cryptographic capabilities in widely available products used in the domestic commercial market because mandating or favouring specific encryption technologies will reduce, not increase, security and also raise product costs.' These WSC Encryption Principles are meant to prevent unnecessary restrictions to trade and negative impact on industry's competitiveness.<br><br>Further clarification that both foreign and domestic enterprises, industry associations and research institutes can participate in standards development activities in China is needed under the Law. | ~~***The State supports social organisations and enterprises in harnessing their own innovative technologies to develop social organisation standards and enterprise standards for commercial cryptography which are higher than relevant technical requirements of national standards and industry standards.***~~ |
| **Article 23** | The State encourages participation in commercial cryptography-related international standardisation activities, in the development of international standards for commercial cryptography, and promotes the mutual conversion between Chinese and foreign standards for commercial cryptography, and their application.<br><br>The State encourages enterprises, social organisations and educational and research institutes to participate in international standardisation activities associated with commercial cryptography. | Instead of merely encouraging participation in development of international standards, the law should encourage organisations to base their standards on relevant international standards. | We recommend adding the following paragraph at the end of Article 23:<br><br>'*The State fosters the adoption of cryptography-related international standards, except where using these standards would be ineffective or inappropriate*.' |
| **Article 25** | The State shall press ahead with the development of the commercial cryptography testing and certification system, develop the technical specification and rules on commercial cryptography testing and certification, and encourage the organisations working on commercial cryptography to voluntarily go through the testing and certification of commercial cryptography.<br><br>The organisations engaging in commercial cryptography testing and certification shall obtain relevant license according to the law and carry out commercial cryptography testing and certification work in accordance with the provisions of laws and administrative regulations as well as the technical specification and rules for commercial cryptography testing and certification. | Article 25 should be redrafted to reflect the fact that products that are not Commercial Cryptographic Products shall not be required to undergo testing and certification, and that these procedures shall not require any disclosure of sensitive information or proprietary intellectual property.<br><br>According to our proposed definition of Commercial Cryptographic Products (see above, Article 8), encryption is the main function in those products, rather than a subsidiary feature of the product or one of its components.<br><br>Voluntary test and certification for commercial cryptographic products should be based on existing international standards in the area | We recommend amending the Article as follows (additions in bold):<br><br>*The State shall press ahead with the development of the commercial cryptography testing and certification system, develop the technical specification and rules on commercial cryptography testing and certification, and encourage the organisations working on commercial cryptography to voluntarily go through the testing and certification of commercial cryptography.*<br><br>*The organisations engaging in commercial cryptography testing and certification shall obtain relevant license according to the* |

[3] Annex 1 to WSC Encryption Principles of Joint Statement of the 17th Meeting of the World Semiconductor Council (WSC)

| | | | |
|---|---|---|---|
| | | of assessment and certification, such as ISO/IEC 19790 or ISO/IEC 15408, as required by WTO TBT Article 5.2.<br><br>If testing and certification are conducted by accredited foreign labs following international standards, they should be accepted as equivalent to those of licensed local labs. In fact, duplication of testing and certification would create delays in the products delivery to customers and increase costs.<br><br>Testing and certification done locally should not require the disclosure of sensitive and confidential product information to government entities or entities with whom contracts and agreements regarding the protection of intellectual property cannot be enforced. Voluntary testing and certification should not be enforced through other government regulations or documents to make it as de facto compulsory requirements. | *law and carry out commercial cryptography testing and certification work in accordance with the provisions of laws and administrative regulations as well as the technical specification and rules for commercial cryptography testing and certification.*<br><br>***Where relevant guidance or recommendations issued by international standards bodies exist, they shall be used as the basis for voluntary testing and certification of commercial cryptographic products.***<br><br>***Products that are not Commercial Cryptographic Products shall not be required to undergo licensing, testing and certification.***<br><br>***Testing and certification procedures shall not require the disclosure of sensitive and confidential information or intellectual property.*** |
| **Article 26** | Commercial cryptography-based products concerning national security, national economy and people's life and social and public interests are included in the catalogue of network- critical equipment and cybersecurity-specific products can be sold or supplied only after accredited through a security certification or found compliant with the requirements in a security test by a qualified body.<br><br>Commercial cryptography-based services used for network-critical equipment and cybersecurity-specific products can be provided only after accredited through a security certification or found compliant with the requirements in a security test by a commercial cryptography certification/testing body. | In line with the definitions we proposed above in Article 8, commercial products, services and components with elements of cryptography that are a subsidiary feature (not the primary function) should be exempt from licensing, testing and certification requirements.<br><br>This Article risks creating duplication when requiring testing for network-critical equipment as envisioned in Article 23 of the Cybersecurity Law and its associated standards and measures that had been released for comment.<br><br>In fact, only one certification should be required, with no need for separate tests since this is addressed under Article 23 of the Cybersecurity Law. Cumbersome certification regimes would undermine China's digital infrastructure across different economic sectors. Chinese users and consumers would be impacted by an increase in costs due to duplicative testing. International competitiveness of Chinese tech industry and developers would also be negatively affected. Invoking | We recommend adding the following sentence at the end of the Article:<br><br>***Sales and licensing of products that are not Commercial Cryptographic Products shall not be restricted by any accreditation requirement.*** |

| | | | |
|---|---|---|---|
| | | additional restrictions does not comport with obligations under the World Semiconductor Council's Encryption Principles.[4]<br><br>Furthermore, national certifications may create a false sense of security for general purpose ICT products, if those certifications diverge from existing international frameworks.<br><br>To the extent testing is considered for CII, it should focus only on the deployment or use of the product in CII settings, not the product or its sale. | |
| **Article 27** | Regarding the critical information infrastructure that should be protected by using commercial cryptography as required by laws, administrative regulations and the State's relevant rules, their operators shall use commercial cryptography to provide protection, and carry out a security assessment for the application of the commercial cryptography.<br><br>Operators of critical information infrastructure and State organs, when purchasing and using network products and services involving the use of commercial cryptography possibly affecting national security, shall pass the national security review conducted by the State cyberspace department together with the State cryptography administration department and other relevant departments. | Article 31 of the Cybersecurity Law already provides for protection measures for CII. The current proposal of security assessment for the application of commercial cryptography creates duplicative requirements for testing or certification schemes that will add costs and delays as well as hinder product innovation.<br><br>The national security review should not create additional market-entry schemes. The review should only be activated by CAC. | We suggest **deleting Article 27** because:<br>• The same requirements are already enshrined in the Cybersecurity Law; and<br>• Cybersecurity review measures should not be defined in this piece of legislation. |
| **Article 28** | The administrative department for commerce under the State Council and the State cryptography administration department, in accordance with the law, introduce an import licensing system for the commercial cryptography concerning national security and social and public interests and having encryption protection features, and impose an export control on the commercial cryptography concerning national security and social and public interests or on which China undertakes international obligations. The list of commercial cryptography subject to import licensing and export control shall be developed by the commerce department under the State Council in consultation with the State cryptography administration department and the General Administration of Customs before announced. | According to the approach followed by the majority of legal systems and further reinforced by international standards and agreements, domestic use of commercial cryptography, as well as import and export of commercial products deploying commercial cryptography, should not be regulated.<br><br>As expressed in our comments to Article 22, the WSC Encryption Principles – acknowledged by the PRC government – are meant to prevent unnecessary restrictions to trade and negative impact on industry's competitiveness. OSCCA already has a 'catalogue of encryption products and equipment with encryption technology subject to import administration' (2013 list) | |

[4] Annex 1 to WSC Encryption Principles of Joint Statement of the 17th Meeting of the World Semiconductor Council (WSC)

| | | | |
|---|---|---|---|
| | Commercial cryptography used in mass consumer products is not subject to the import licensing system or export control. | guiding the import control of cryptography. This list covers commercial cryptographic products where the core function is encryption and should therefore guide the development of the new list proposed in this Draft Law.<br><br>Furthermore, consistent with our definitions proposed in Article 8, products that are not commercial cryptography-based should be exempted from import and export control. Therefore authentication, digital signature and hash-based integrity technologies would be excluded, as would all products where cryptography is a subsidiary feature.<br><br>We also recommend that the Chinese government clarify that the scope of 'mass consumer products' includes commercial off-the-shelf products used by business enterprises for commercial purposes. Commercial products used internally (e.g. not for commercial sale) by firms, such as multinational corporations (MNCs), should be exempt from certification and licensing requirements.<br><br>These clarifications will help ensure that China's encryption-related regulations are focused only on significant threats to national security. Such a focus will minimise trade barriers and avoid disrupting China's pivotal role in the global ICT market. | |
| **Article 30** | The commercial cryptography industry association shall, in accordance with laws and administrative regulations and the provisions of its Articles of Association, provide commercial cryptography-related information, technical and training services for organisations working on commercial cryptography, and guide and compel the organisations to, according to the law, carry out the activities such as scientific research, production, sale, service and import and export of commercial cryptography, strengthen self-discipline, enhance good-faith awareness industrywide, and promote the development of the industry. | The Article should provide more operational details about the commercial cryptography industry association, and ensure participation is open to foreign companies. | Additional information is needed about:<br>• Role and composition of the association;<br>• Involvement of the association in reviewing foreign technology;<br>• Relationship with the China Customs and the State Cryptography Administration. |
| **Article 31** | The cryptography administration departments and relevant departments shall build a concurrent and ex post oversight system for commercial cryptography based on a combination of routine supervision and random checks, | While we welcome the changes made to Article 29 regarding enforcement powers that appeared too broad, we believe Article 31 should state that checks shall not affect intellectual property and | We recommend adding an additional paragraph to this Article:<br><br>***Any checks that are part of a supervision and management*** |

| | | | |
|---|---|---|---|
| | set up a unified commercial cryptography supervision and management information platform, promote the connectivity of the concurrent and ex post oversight model and the social credit system, and make the commercial cryptography-related organisations enhance self-discipline awareness while strengthening public supervision over them. | privacy rights and shall be conducted with minimal disruption to business operations.<br><br>In fact, the original Draft raised serious concerns as it would have *de jure* or *de facto* forced the disclosure of extensive intellectual property that would violate China's TRIPs obligations and the licensing requirements of foreign government authorities.<br><br>Additionally, the proposed 'concurrent and ex post oversight system' should be better described and justified. According to Article 39 TRIPs requiring government protection of undisclosed information, the Draft Law should also ensure appropriate intellectual property and privacy protections, while minimising disruption for business in case of checks. | ***platform shall ensure that intellectual property, confidential information and privacy rights are protected and shall be conducted in a way that minimises disruption to business operations.*** |
| **Chapter 4 – Legal Liabilities** | | | |
| **Article 32** | Should any organisation/individual, in violation of the provisions of Article 12 of this Law or relevant laws and administrative regulations, steal others' encrypted information, illegally hack into others' cryptographic protection systems, or use cryptography to engage in the activities endangering national security, social and public interests and others' legitimate rights and interests, or other illegal/criminal activities, the violator shall be subject to legal liability in accordance with the law. | Although Articles 9, 10 and 11 encourage RandD, Articles 12, 21 and 32 seem to impinge on this possibility. In fact, an exception should be added to Article 32 for good faith security and vulnerabilities research into vulnerabilities aimed at improving security of the technology and products, which should not be considered illegal/criminal nor subject to any penalty or legal liability. | |
| **Article 36** | Should any entity, in violation of the provisions of Article 26 of this Law, sell or provide commercial cryptographic products or services not undergoing security certification/testing or failing the security certification/testing, the market regulation department shall order the violator to rectify or stop the violation, give a warning and confiscate illegal products and illegal income; should the illegal income exceed 100,000 Yuan, may impose a fine of 1-3 times the illegal income concurrently; should the illegal income be zero or below 100,000 Yuan, may impose a fine of 30,000-100,000 Yuan concurrently. | See our comments on Article 26 | |
| **Article 37** | Should any entity use commercial cryptography in violation of the provisions of the first paragraph of Article 27 in this Law, or purchase and use the products or services not undergoing a security review or failing the security review in violation of the provisions of the second paragraph of | See our comments on Article 27 | |

| | | | |
|---|---|---|---|
| | Article 27 in this Law, penalty shall be imposed in accordance with the provisions of the Cybersecurity Law of the People's Republic of China. | | |
| **Article 38** | Should any entity import or export commercial cryptography in violation of the provisions of Article 28 of this Law, the commerce department under the State Council or the customs authority shall impose a penalty in accordance with the law. | See our comments on Article 28 | |