DIGITALEUROPE

18 SEPTEMBER 2020

DIGITALEUROPE comments to the Proposed Revision of Commercial Cryptography Administrative Regulation

Executive Summary

DIGITALEUROPE welcomes the opportunity to submit comments to the draft Commercial Cryptography Administrative Regulations (Amended Draft for Comment) published by the Office of State Commercial Cryptography Administration (OSCCA) on 20 August 2020.

DIGITALEUROPE believes that the current proposal put forward by the OSCCA could be improved by addressing the following concerns:

- The scope of the draft regulation is too broad and regulatory restrictions on commercial cryptography unprecedented: the approach seems inconsistent with the spirit of the existing Cryptography Law and the current Encryption Regulation ("core function" principle), therefore further clarifications would be much needed.
- The draft regulation lacks a commitment to utilize commonly used international standards which would undermine interoperability of products and services and would impinge on security, considering the global nature of ICT supply chain.
- Proposed requirements on import and export are too restrictive and unprecedented.
- Intellectual property aspects are not adequately covered by the revision.

Table of Contents

General comments

In previous submissions to OSCCA and State Administration for Market Regulation (SAMR)[1], DIGITALEUROPE highlighted how elements of encryption are included in almost all modern information and communication technology (ICT) products for cybersecurity purposes. Most governments around the world do not regulate the importation or domestic use of cryptographic features in mass-market products, and the few economies that do typically use a very limited regulatory touch with a narrow product scope.

According to the World Semiconductor Council (WSC) principles for commercial cryptographic technologies in mass marketed ICT products, the regulation of commercial encryption should be limited, and encryption technology mandates prohibited, acknowledging the widespread use of encryption and the limited value in regulating the commercial market. The approach outlined in the Proposed Revision of Commercial Cryptography Administrative Regulations is not consistent with the obligations and commitments taken by the Government of China, along with the other members of the Government and Authorities Meeting on Semiconductors (GAMS), under the WSC's Encryption principles.[2]

China's competitiveness and long-term prosperity relies also on timely and efficient import and export of ICT products. Regulating market access because of the use of commercial encryption functionalities translates to restricting the Chinese market and hindering competition, foreign investments, trade flows and innovation.

Detailed comments and recommendations

Expansive scope

The scope of the draft regulation is too broad and regulatory restrictions on commercial cryptography unprecedented: the approach seems inconsistent with the spirit of the existing Cryptography Law and commitments made regarding the current Encryption Regulation ("core function" principle), therefore further clarifications would be much needed.

[1] https://www.digitaleurope.org/resources/digitaleurope-comments-to-opinions-on-implementation-of-testing-and-certification-of-commercial-cryptography/ (March 2020) and https://www.digitaleurope.org/resources/digitaleurope-and-esia-response-to-the-office-of-state-commercial-cryptography-administration-draft-cryptography-law/ (September 2019)

[2] Joint Statement of the 17th Meeting of the World Semiconductor Council (WSC), 23 May, 2013 (Lisbon, Portugal), as endorsed by member country governments in Government/Authorities Meeting on Semiconductors, September 26, 2013 (Jeju, Korea)

Firstly, the proposed regulation covers nearly all encryption technologies used by industry and consumers in China, posing a threat to innovation, interoperability, security and China's competitiveness. Since 2000, industry relied on the clarification published by the State Encryption Management Commission (predecessor to SCA) with regard to commercial cryptography: it introduced the concept of "core function", the scope of the management of 'encryption products and equipment containing encryption technology' incorporated in these regulations, only limits specialized hardware and software for which encryption and decoding operations are core functions; other things, including wireless telephones, Windows software, browser software, etc., are not included in the scope." [3] The definition of commercial cryptography under the draft regulation should be limited to products that have cryptography as such "core" or "primary function", and this should be taken into consideration when developing the "List of Commercial Cryptography Subject to Import Licensing" as referred to in Article 31.

Secondly, the current proposal fails to support the provision laid out in article 28 of the Cryptography Law, exempting mass consumer products from import licensing or export control. Finally, In the draft regulation, Article 9 defines the guidance directory of commercial cryptography technology which is beyond the scope of the Cryptography Law, and the security review mechanisms and criterion conditions are unclear.

Therefore, DIGITALEUROPE recommends to:

- Maintain China's commitment to the "core function" concept, as per 2000 SEMC clarification.
- Explicitly exclude importation and exportation of cryptography in mass consumer products.
- Delete Article 9.

Lack of interoperability

The lack of interoperability of products and services would impinge on security, provided the global nature of ICT supply chain.

International standardization in the field of cryptography plays a critical role in enabling both security and interoperability. The technologies that form the basis of global cryptography standards are developed, tested and peer reviewed to ensure robustness, resolve weaknesses, and quickly introduce and update innovative technology for global use. Many governments around the world

[3] "Clarification" issued 13 March 2000 by the State Encryption Management Commission

acknowledge the benefit of using voluntary global standards instead of regulating encryption in commercial/industrial market ICT products locally.

As a WTO member, China should abide by the agreement on Technical Barriers to Trade (TBT) and use relevant international standards as the basis for its technical regulations and national standards unless the relevant international standard is ineffective or inappropriate to fulfil a legitimate objective, such as national security.[4] Unfortunately the current proposal put forward by OSCCA does not require China to adopt international cryptographic standards and introduces in art. 9 and 39 the reference to new on catalogue on commercial cryptography technologies, which should be revised to include international as well as domestic standardized cryptography.

DIGITALEUROPE urges OSCCA to:

- Include a commitment to utilize commonly used international standards as the basis for national and industrial standards in article 10 of the proposed regulation.
- Include international standardized technologies and algorithms in the catalogue mentioned in articles 9 and 39.

Restrictive import and export requirements

The current proposal lacks clarity on what kind of items will be considered as "Commercial cryptography concerning national security and social & public interests and having encryption protection capability" as well as "Commercial cryptography concerning national security and social & public interests or on which China undertakes international obligations" that may be subjected to import license or export control.

In addition, product developers and manufacturers would not be able to determine how to comply with the license approval procedure described in article 32, unless OSCCA clarifies criteria to identify the items falling in the two lists.

Therefore, DIGITALEUROPE recommends OSCCA to:

- Clarify what kind of items will be included in the new "List of Commercial Cryptography subject to Import Licensing" as well as the "List of Commercial Cryptography subject to Export Control".
- Exclude from this regulation and exempt from import/export requirements cryptographic features in mass consumer products and cryptographic products in which the "core function" is not encryption.

[4] TBT Agreement, Article 2.4, and Annex 3, Paragraph F.

- Consider establishing designations based on the nature of the item – similar to those utilized by other major trading partners – which will reduce regulatory burdens and better harmonize China’s proposed system with those of its major trading partners.
- Clearly define licensing procedures and requirements for dual use items, to avoid burdensome requirements and unpredictability to cross-border activity.

Lack of intellectual property protection

The regulation fails to ensure that sensitive intellectual property (IP) will be protected when products and technologies undergo testing and certification. International standards in the area of assessment and certification, such as ISO/IEC 19790 or ISO/IEC 15408, created with the participation of Chinese experts, represent a solid baseline for a broadly applicable certification framework. International standards and experience would enable non-discriminatory transparent testing and certification frameworks, as well as the development of certification-related processes, with industry involvement, to overcome fragmented approaches.

The need for IP protection has gained even more prominence, due to the fact article 39 of OSCCA’s Commercial Cryptography Administrative Regulations makes certification mandatory in critical infrastructures, Level 3+ MLPS, and government information systems. On the contrary, certification is described as voluntary in article 25 of the Cryptography Law, and according to Article 26 in the same law, only products listed under “Network Critical Equipment” and “Network Security Specific Products” require mandatory certification. The inconsistent approach in article 39 should be fixed to align with articles 25 and 26 of the Cryptography Law.

Finally, the current proposal by OSCCA put a product developer’s most sensitive information and intellectual property (including trade secrets and customer sales data) at risk. In fact, the draft regulation would *de facto* force the disclosure of extensive IP that would further risk violating China’s TRIPS obligations and the licensing requirements of foreign government authorities.

DIGITALEUROPE asks OSCCA to:

- Use existing relevant guides or recommendations issued by international standards bodies for testing and certification.
- Accept testing and certification performed by accredited foreign labs in accordance with globally recognised standards as equivalent to that of licensed local labs to avoid unnecessary duplication.

- State explicitly in the regulation that testing and certification procedures shall not require the disclosure of sensitive and proprietary intellectual property (IP) and confidential information and in particular to remove the reference to the need to submit source code for the purpose of testing or certification, consistent with international practices.
- Align article 39 of the proposed regulation with article 25-26 of the Cryptography Law, to keep certification requirements mandatory only for products listed under “Network Critical Equipment” and “Network Security Specific Products”.

Conclusion

The current proposal lays down cumbersome requirements for certification, disclosure of IP, severe penalties for non-compliant technology developers and users (article 51), unprecedented import and export requirements for commercial cryptography. Also, its approach and provisions are inconsistent with the current rules on commercial cryptography and the existing Cryptography Law. A similar regulatory regime creates strong disincentives for technology firms to develop and offer advanced security solutions in China.

DIGITALEUROPE looks forward to continued discussions and consultations on revisions to the draft Commercial Cryptography Administrative Regulation, as well as review draft versions of applicable catalogues and other implementing measures.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell
Privacy and Security Policy Officer

martin.bell@digitaleurope.org / +32 492 58 12 80

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world’s largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world’s best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France

Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC

Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK