



## EICTA Position on China's WTO Proposal concerning Compulsory Certification for Products incorporating Encryption Technologies

Brussels, 24 June, 2008

On August 27, 2007 the People's Republic of China (PRC or China) issued 13 Technical Barriers to Trade (TBT) Notifications, G/TBT/N/CHN/278-290, on proposed technical Regulations that seek to impose compulsory certification for a broad range of software and hardware information and communication technology (ICT) products incorporating encryption technologies.

The 13 product areas directly touch on products where EU software and hardware firms are leaders in global markets namely: website recovery, firewalls, routers, smartcard Chip Operating System (COS), data backup and recovery, operating system, databases, anti-spam, intrusion detect, network vulnerability and security audit products. Without such mandatory certification, China indicated that "no products shall be allowed to be put into the market within the territory of China after the enforcement of the rules."

This notification was the first specific public indication that a sweeping set of mandatory tests for conformance would be applied to commercial products as a condition for access to the Chinese commercial market. There have been little or no documents or public reference materials made available of essential information to enable interested parties to evaluate these standards.

Based on a preliminary analysis, EICTA members have the following concerns:

TBT Article 2.2 requires that technical regulations satisfy a legitimate policy objective which includes the following: national security requirements, prevention of deceptive trade practices, protection of human health or safety, and protection of animal and plant life or health or the environment. Under the TBT, technical regulations that fail to pursue a legitimate objective are considered, as a matter of law, unnecessary obstacles to international trade. China's notifications of the proposed regulations state "Information Security" as the objective rationale; however, they do not articulate any legitimate policy objective on which China bases the proposed regulatory requirements, according to the TBT language. We have failed to identify the policy objective for these Regulations.

The ICT products and software referred to in the Regulations are generally used in commercial contexts. We believe that their use in the commercial context does not pose a national security risk, nor any of the other legitimate regulatory objectives listed in the TBT Agreement. Thus, "Information Security" - the only objective and rationale stated for these significant draft Regulations, which appears only in the TBT notifications and not in the draft Regulations themselves - is not justified and does not appear to be legitimate for TBT or other purposes.

TBT Article 2.2 also requires that technical Regulations "shall not be more trade restrictive than necessary in fulfilling a legitimate objective." This means that, even if there is a legitimate objective, a technical regulation cannot be "prepared, adopted or applied with a view to, or with the effect of, creating unnecessary obstacles to international trade." There are several significant reasons why the 13 draft Regulations are being prepared, and are likely to be adopted and applied, in a manner that is significantly more trade restrictive than necessary.

EICTA strongly believes that relevant international standards already exist and no further Regulation is needed. The TBT requires that technical regulations be based on international standards that exist or whose completion is imminent, if such standards have less trade restrictive effects and would be effective and appropriate for achieving the policy objective. This requirement is especially valuable in the ICT industry.

The technology revolution, its worldwide dissemination, and the resulting massive productivity gains along with other benefits are all based on connectivity and interoperability. Information security also has to be achieved on an interoperability basis to ensure economies of scale. The value of global interoperability for business interests cannot be overstated. The draft Regulations, however, rely on a number of unique Chinese national standards. It is unclear why the Chinese promote a national model. There is no other country in the world that relies on national security standards and related conformity assessments because there are global standards already in use today.

China's proposed Regulations depart from internationally accepted standards and norms. China's proposed regulations do not appear to rely on existing standards. Instead, China seeks to require conformity assessment of a wide variety of products containing encryption functionality with Chinese standards; such products containing encryption would need to receive a CCC-mark certification. The proposed conformity assessment would be highly unusual, including requirements for unknown technical standards, provision of product samples, physical "factory" inspections, design and functionality requirements (G/TBT/N/CHN/287), unknown common criteria-like references and security attestation. No country has ever regulated the sale or importation of computer security products for the commercial market in the manner proposed by the Chinese regulations.

While a myriad of governments have laid out frameworks to address the important issue of protecting critical infrastructures and promoting cyber-security, none have implemented regimes that include government-mandated conformance testing to standards relating to "information security" as a prerequisite to being sold in a domestic market in a commercial context.

If the referenced standards are inconsistent with relevant international standards, we would ask the PRC government to explain how existing international standards are ineffective or inappropriate to achieve China's policy objectives.

China's proposed regulations are more burdensome than existing international standards. Industry anticipates a costly and burdensome impact on high-tech industry as a result of the proposed regulations. The potential impact of these regulations includes the following:

The Regulations undermine current innovation and development, forcing companies to develop China-specific designs and products (or creating de-facto Chinese standards as the international standard). Many of the regulations make very specific requirements as to the design and feature set of the regulated products. These requirements will constrain innovation by locking evolving software systems (e.g., Anti Spam draft regulation) used all over the world into particular approaches and methodologies that are determined by the Chinese and applicable only in China. To summarise, industry would either be forced to adopt the Chinese standard or bifurcate all development for new products: (i) products for the China market alone and (ii) products for the rest of the world.

Key elements of existing international standards in the marketplace today are that they provide common building blocks of protection, integrity of a product and attestation and privacy—the result is that there are many commercially-available products that meet these standards from vendors around the world.

It appears that China has rejected, without adequate explanation, an internationally recognized approach that facilitates global trade and meaningful independent security evaluations.

The Common Criteria for Information Technology Security Evaluation (Common Criteria or CC) is an internationally accepted standard meant to be used as the basis for evaluation of security properties of IT products. By setting up a common criteria foundation, it allows for meaningful security evaluation to a wider audience.

CC also permits comparability between the results of independent security evaluations. The CC has been adopted and recognized as an international standard – ISO/IEC 15408:2005". CC is continuously updated to reflect experience gained over time.

The PRC regulations may restrict cryptographic applications to a certain proprietary national standard and set of algorithms that specifically prohibit non-PRC technology and prohibit non-PRC company involvement in the process going forward. This would restrict competition, hinder innovation and negatively impact cross-border commerce that relies upon standards based encryption today (e.g., financial services and supply chains).

Companies would be required to expend significant resources to comply with the proposed regulation. The cost of determining what will be required, based on the content of the current notifications is difficult to assess but will be significant because of requirements for conformity assessment. These Regulations will touch every aspect of product design and development in IT companies. As such, they constitute substantial and unnecessary trade barriers.

Moreover, currently drafted the regulations fail to provide sufficient details. For example, the CCC-certification program is typically related to ensuring the safety of hardware and electronics devices (like "CE listing"). It is applied here to software products. It is unclear how the certification processes and Regulations would be applied in a software context. Based on the information available, the mandated "CCC mark" will present an unwarranted barrier to market entry for non-Chinese IT products.

Few, if any, Chinese companies will be affected by these Regulations. The proposed Regulations reference only indigenous "GB/T" standards and eschew globally recognized processes for achieving information assurance by both commercial and government users.

The proposed technical Regulations lack the necessary specificity upon which conformance can be tested. Rather than contributing to greater confidence in IT security and information assurance, the testing regime presents grave risks to legitimate commercial interests. It is also highly unlikely that the testing regime will facilitate product compliance with the May 2009 deadline.

Chinese standards were not developed in an open forum with international stakeholders.

Our experience is that the central government plays a major role in the development of almost all significant national standards in China. To the extent the Chinese standards were developed by or with support from central government bodies, they should have complied with Code of Good

Practice (CGP) requirements. TBT Article 4.1, Annex 3, Sections F & L of the CGP requires, among other things, that proposed standards be (i) subject to a minimum 60 day comment period and (ii) based on relevant international standards.

We are not aware of any of the standards cited in the 13 draft regulations having been opened up to WTO members for comment.

Industry will not have fair access to encryption algorithms.

TBT Article 2.1 requires that “products imported from the territory of any Member shall be accorded treatment no less favorable than that accorded to like products of national origin and to like products originating in any other country.” Moreover, “Upon accession, China shall ensure that the same technical regulations, standards and conformity assessment procedures are applied to both imported and domestic products.” In addition to the references above, there are references in two additional draft regulations that refer companies back to “related encryption regulations.” Moreover, the Security Operating Systems draft regulation itself (G/TBT/N/CHN/285) has two standards referenced (GB/T20008-2005 and GB/T20272-2006), and G/TBT/N/CHN/2861 (referencing GB/T 20009-2005 and GB/T 20273-2006), which indicate that the “encryption support” for the test standards and test items related to those draft measures are “To be implemented according to related regulations of the state encryption authorities.”

Accessing underlying algorithms requires significant operational change.

Industry’s ability to access the underlying encryption algorithms required to comply with is difficult and would require either a Chinese partner in the business, or possibly releasing company-specific information. This is especially difficult when all algorithm references go back to the SEA, which as far as we are aware, has never released these algorithms to a non-Chinese entity.

## EICTA MEMBERSHIP

### About EICTA:

EICTA, founded in 1999 is the voice of the European digital technology industry, which includes large and small companies in the Information and Communications Technology and Consumer Electronics Industry sectors. It is composed of 59 major multinational companies and 41 national associations from 29 European countries. In all, EICTA represents more than 10,000 companies all over Europe with more than 2 million employees and over EUR 1,000 billion in revenues.

### The membership of EICTA:

#### Company Members:

Adobe, Agilent, Alcatel-Lucent, AMD, Apple, Bang & Olufsen, Brother, Canon, Cisco, Corning, Dell, EADS, Elcoteq, Epson, Ericsson, Fujitsu, Hitachi, HP, IBM, Infineon, Ingram Micro, Intel, JVC, Kenwood, Kodak, Konica Minolta, Lexmark, LG Electronics, Micronas, Microsoft, Motorola, NEC, Nokia, Nokia Siemens Networks, Nortel, NXP, Océ, Oki, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Samsung, Sanyo, SAP, Sharp, Siemens, Sony, Sony Ericsson, STMicroelectronics, Sun Microsystems, Texas Instruments, Thales, Thomson, Toshiba, UMC, Xerox.

#### National Trade Associations:

**Austria:** FEEL; **Belarus:** INFOPARK; **Belgium:** AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Czech Republic:** ASE, SPIS; **Denmark:** ITEK, IT-Branchen; **Estonia:** ITL; **Finland:** FFTI; **France:** ALLIANCE TICS, SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT Ireland; **Italy:** ANIE, AITech-ASSINFORM; **Latvia:** LIKTA; **Lithuania:** INFOBALT; **Malta:** ITTS; **Netherlands:** ICT-Office, FIAR; **Norway:** ABELIA, IKT Norge; **Poland:** KIGEiT, PIIT; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AETIC, ASIMELEC; **Sweden:** IT Företagen; **Switzerland:** SWICO, SWISSMEM; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT Ukraine; **United Kingdom:** INTELLECT.