Introduction

In June 2015, the Draft Cybersecurity Law of the People's Republic of China was first deliberated on at the 15th meeting of the Standing Committee of 12th National People's Congress. The Draft Cybersecurity Law of the People's Republic of China is now posted on the official website of NPC for soliciting comments. The public may visit www.npc.gov.cn to make comments, or may send comments by mail to the Legislative Affairs Committee of the Standing Committee of NPC (address: 1 Qianmen Xidajie, Xicheng District, Beijing, 100805, please indicate Comments on the draft Cybersecurity Law on the envelope). The deadline for the solicitation is August 5, 2015.

After the document was issued, several organizations made the translations. SESEC expert chose the best translation from them and made the proof-reading.

Below is the whole text translation of the draft Cyber Security Law of the People's Republic of China

Draft Cybersecurity Law of the People's Republic of China

Table of Contents

Chapter 1 General

Article 1 This Law is developed with a view to assuring cybersecurity, safeguarding China's sovereignty over cyberspace and national security and public interests, protecting the legitimate rights and interests of citizens, legal persons and other organizations, and promoting healthy development of informatization in the economy and society.

Article 2 This Law applies to construction, operation, maintenance and use of networks, as well as supervision over and management of cybersecurity within the territory of China.

Article 3 The State emphasizes both cybersecurity and informatization development, and by keeping in mind the tenets of "active utilization, scientific development, law-based management and assuring security", drive the development of network infrastructure, encourage the innovation and application of network technology, build a sound cybersecurity assurance system, and boost the cybersecurity protection capabilities.

Article 4 The State advocates honest, sincere, healthy and civilized cyber behaviors, and will take measures to enhance the cybersecurity awareness and levels of all walks of life, aiming to create a favorable environment enabling all walks of life to participate in efforts to drive cybersecurity.

Article 5 The State will actively launch international exchange & cooperation programs in terms of cyberspace administration, cyber technology R&D and standards development and crackdown upon web-based violations and crimes, in a bid to build a peaceful, secure, open and cooperative cyberspace.

Article 6 The State-level cyberspace administration authorities are responsible for overall planning and coordination of nationwide cybersecurity efforts and relevant supervision and management work. The industry & information technology, public security and other relevant departments under the State Council shall, per this Law and applicable laws and administrative regulations, and within their respective sphere of responsibility, carry out protection, supervision and management of cybersecurity.

The responsibility of relevant departments under the People's Governments above county level for cybersecurity protection, supervision and management will be developed per the State's relevant regulations.

Article 7 When developing and operating networks and offering services over networks, technical measures and other necessary measures shall, per the provisions of laws and regulations and the mandatory requirements of national and industry standards, be taken to ensure cybersecurity and stable operation, effectively respond to cybersecurity incidents, prevent violations and crimes, and maintain the integrity, confidentiality and availability of network data.

Article 8 Internet-related industry associations shall, per their articles of association, enhance self-discipline awareness of the industry, develop code of safe cyber conduct, to give guidance for members to strengthen cybersecurity, improve cybersecurity levels and promote healthy development of industry.

Article 9 The State will protect the right of citizens, legal persons and other organizations to access networks, promote the widening of network access, improve online service levels, provide safe and convenient network services for all the people, and ensure law-based, orderly and free flows of information over networks.

All individuals and organizations, when using cyberspace, shall abide by the Constitution and laws, follow the public order, respect social morals, and must not endanger cybersecurity, or use cyberspace to engage in such activities as to disrupt national security, publicize terrorism and extremism, advocate ethnical hatred and ethnical discrimination, spread porn information, insult or slander others, disturb social order, undermine public interests,
Infringe upon others' intellectual property and other legitimate rights and interests.

Article 10 Any individual and organization has the right to expose any behaviors eroding cybersecurity to the cyberspace affairs, industry and information technology and public security departments. The departments having received the complaints shall handle this per laws, without delay. Where the cases are beyond their sphere of responsibility, such cases shall be referred to the competent departments.

Chapter 2 Cybersecurity Strategy, Planning and Promotion

Article 11 The State will develop a cybersecurity strategy clearly stating the general requirements for and main objectives of assuring cybersecurity, and proposing the policy measures aimed to improve the cybersecurity assurance system, boost cybersecurity protection capabilities, promote the development of cybersecurity technology and industry, and drive the whole community to participate in cybersecurity efforts.

Article 12 The departments in charge of communications, radio and TV, energy, transport, water resources and finance respectively and other relevant departments under the State Council shall, in line with the national cybersecurity strategy, prepare cybersecurity plans for key sectors vital to national security and national economy and people's livelihood, and oversee their enforcement.

Article 13 The State will set up and improve the cybersecurity standards system. The standardization department and other relevant departments under the State Council shall, per their respective duties, develop the national & industry standards for cybersecurity management and for security of cyber products, services and operations, and revise them at due time.

The State supports enterprises in participating in the development of national standards and industry standards for cybersecurity, and encourages enterprises to develop enterprise standards more stringent than national standards and industry standards.

Article 14 The State Council and the provincial-level People's Governments shall make overall plans to increase investments and support key cybersecurity technology industry and projects, support the R&D, application and promotion of cybersecurity technologies, protect intellectual property over cyber technologies, and support scientific research institutes, institutions of higher learning and enterprises in participating in the national cybersecurity technology innovation projects.

Article 15 The people's government at all levels and their relevant divisions shall organize cybersecurity publicity and education programs regularly, and direct and urge relevant organizations to press ahead with cybersecurity publicity and education.

The mass media shall launch widespread cybersecurity publicity and education targeting different groups of people.

Article 16 The State supports enterprises, institutions of higher learning and vocational schools to set up cybersecurity education and training programs, and train cybersecurity specialists in many ways and promote the exchange of cybersecurity specialists.

Chapter 3 Safe Operation of Network

Section 1 General provisions

Article 17 The State implements a cybersecurity multi-level protection system. The network operators shall, per the multi-level protection system, fulfill the following security protection obligations to protect networks from intrusion, damage or unauthorized access, and prevent divulgence or theft or falsification of network data:

(1) Develop an internal security management system and operating procedures, appoint a cybersecurity officer, and clearly define the responsibility for cybersecurity;
(2) Take technical measures against the behaviors endangering cybersecurity such as computer viruses, network attacks and network intrusion;
(3) Take technical measures to keep a record and track of network operational status, monitor and record cybersecurity incidents, and keep network logs as required;
(4) Take the measures such as data classification, backup and encryption of key data;
(5) Other obligations as specified in laws and administrative regulations.

Specific measures for cybersecurity multi-level protection scheme will be developed by the State Council.

Article 18 The network products and services shall comply with relevant national and industry standards. The suppliers of network products and services shall not install malicious programs; where their products and services have capability of collecting user information, the suppliers shall clearly inform users and get user consent; where risks such as security defects or vulnerabilities exist in their network products or services, the suppliers shall promptly inform the users and take remedial measures.

The suppliers of network products and services shall continuously provide security maintenance for their products and services. The provision of security maintenance shall not discontinue during the period as specified or as agreed with the users.

Article 19 Critical equipment for networks and dedicated products for cybersecurity can be sold only after they are accredited through a security certification conducted by a qualified institution or found compliant with security testing requirements per the mandatory requirements of national or industry standards. The State-level cyberspace administration authorities shall work with relevant departments under the State Council to develop and release a catalogue of network-critical equipment and dedicated products for cybersecurity, and drive mutual recognition of security certificates and security testing results, and avoid redundant certification and testing.

Article 20 When the network operators offer users such services as network access and registration of domain name, and provide network access to user's landline phones and mobile phones, or release information among users, they shall require users to provide real
ID information at the time of signing contracts with users or when confirming the provision of services. Where a user fails to provide his real ID information, the network operators shall not provide relevant services.

The State supports the R&D of safe and convenient electronic ID authentication technology, and push ahead with the mutual recognition and widespread application of different electronic ID authentication technologies.

Article 21 The network operators shall develop emergency response plans with respect to cybersecurity incidents, so as to promptly respond to security risks such as system vulnerabilities, computer viruses, network intrusion and network attacks. When a cybersecurity incident occurs, the emergency response plans shall be initiated immediately to take corresponding remedial measures, and as required, inform the competent department.

Article 22 No individual or organization may engage in the activities endangering cybersecurity such as intruding into other networks, interfering with normal operations of other networks or stealing network data, or provide tools and methods for the activity of intruding into other networks, interfering with normal operations of other networks or stealing network data, or provide help such as technical support, advertising and promotion, and payment & settlement for others to engage in activities undermining cybersecurity.

Article 23 For reasons of national security and criminal investigation, the investigation departments may, per relevant laws, require the network operators to provide necessary support and assistance.

Article 24 The State supports cooperation between network operators in the collection, analysis and communication of cybersecurity information as well as emergency response, so as to boost the security assurance capability of network operators.

Relevant industry associations shall develop sound cybersecurity protection specifications for their respective industries and a collaborative mechanism, enhance analysis and assessment of cybersecurity risks, regularly give risk warnings to members, and support and assist members in responding to cybersecurity risks.

Section 2 Safe operation of critical information infrastructure

Article 25 The State gives priority to protection of basic information networks providing public communications and radio & TV transmission services, the important information systems operating in key sectors such as energy, transport, water resources and finance and the public service fields such as power supply, water supply, gas supply, medical & health and social security, the networks for military purposes, the government networks

used by state organs in the cities with districts, and the networks and systems owned or managed by the network service providers having large numbers of users (hereinafter referred to as critical information infrastructure). The measures for protection of the critical information infrastructure will be developed by the State Council.

Article 26 The departments in charge of communications, radio and TV, energy, transport, water resources and finance respectively and other relevant departments (the department in charge of critical information infrastructure protection, below) under the State Council shall, per their duties assigned by the State Council, be responsible for directing and supervising the efforts to protect the safe operation of critical information infrastructure.

Article 27 The critical information infrastructure shall be developed to ensure it has capability of enabling the business it supports to operate stably and continuously. The security technology measures shall be simultaneously planned, implemented and used together with the critical information infrastructure.

Article 28 In addition to following Article 17 herein, the operators of critical information infrastructure shall fulfill the following security protection obligations:

(1) Set up a dedicated security management body and appoint a security officer, and a background investigation shall be conducted for the officer and persons undertaking key jobs;
(2) Regularly provide cybersecurity education and technical training to staff and conduct skill assessment;
(3) Maintain disaster recovery backup of key systems and database;
(4) Develop an emergency response plan for cybersecurity incidents, and organize drills regularly;
(5) Other obligations specified in laws and administrative regulations.

Article 29 The operators of critical information infrastructure, when purchasing network products and services, shall sign a security & secrecy agreement with the suppliers, clearly defining the security & secrecy obligations and responsibilities.

Article 30 Where the operators of critical information infrastructure purchase network products or services, possibly influencing national security, they shall pass the security review organized by the

State-level cyberspace administration authorities together with relevant department under the State Council. Specific measures will be developed by the State Council.

Article 31 The operators of critical information infrastructure shall store, within the territory of China, the important data such as personal information of citizens collected and generated during the operations; where overseas storage of data or offering of data to overseas organizations or individuals is required for proper reasons, a security assessment shall be conducted per the measures developed by the State-level cyberspace administration authorities together with relevant department under the State Council.

Where other laws or administrative regulations otherwise prescribe, such prescriptions shall be followed.

Article 32 The operators of critical information infrastructure shall conduct on their own, or authorize a specialized institution to test and assess the security of their networks and possible risks at least once a year, and generate a cybersecurity report on test & assessment results and improvements made, which shall be submitted to the relevant department in charge of critical information infrastructure protection.

Article 33 The State-level cyberspace administration authorities shall coordinate relevant departments to set up a collaborative mechanism. The following measures may be taken to protect the critical information infrastructure:

(1) Conduct a spot check for the security risks of critical information infrastructure, propose improvements, and when necessary, authorize a specialized institution to assess the security risks of networks;
(2) Regularly organize the operators of critical information infrastructure to conduct a cybersecurity emergency drill, to improve the capability of critical information infrastructure against cybersecurity incidents and collaboration capability;
(3) Drive the sharing of cybersecurity information among relevant departments, operators of critical information infrastructure and cybersecurity service providers, and relevant research institutes;
(4) Provide technical support and assistance for emergency response and recovery with respect to cybersecurity incidents.

Chapter 4 Network Information Security

Article 34 The network operators shall set up a sound system for the protection of user information, to enhance the protection of personal information, privacy and business secrets of users.

Article 35 The network operators, when collecting and using personal information of citizens, shall do so on a legitimate, justified and necessary basis, state the purpose, method and scope of the collection and use of such information, and obtain the consent of such citizens.

The network operators shall not collect personal information of citizens irrelevant to the services they provide, shall not collect or use personal information of citizens in violation of the provisions of laws and administrative regulations and the agreement reached between both parties, and shall, per the provisions of applicable laws and administrative regulations or the agreement reached with users, handle personal information of citizens they keep.

The network operators, when collecting and using personal information of citizens, shall unveil the rules for collection and use of information.

Article 36 The network operators must keep confidential the personal information of citizens they collect, shall not disclose, falsify, destroy or sell such information, or illegally provide such information to others.

The network operators shall take technical measures and other necessary measures to ensure the security of personal information of citizens, and prevent the divulgence, destruction or loss of personal information of citizens they collect. Where the divulgence, destruction or loss of information occurs or possibly occurs, remedial measures shall be taken immediately while informing users possibly affected, and informing the competent department per the regulations.

Article 37 Where a citizen finds a network operator collects or uses his personal information in violation of the provisions of laws and administrative regulations or the agreement reached between both parties, he has the right to require the network operator to delete his personal information; where the personal information collected and stored by the network operator contains errors, he has the right to require the network operator to make corrections.

Article 38 No individual or organization may steal or use other illegal means to obtain personal information of citizens, or sell or illegally provide personal information of citizens to others.

Article 39 The department legally tasked with supervision and management of cybersecurity must keep confidential the personal information, privacy and business secrets of citizens obtained when performing its duties, and shall not divulge, sell or illegally provide such information to others.

Article 40 The network operators shall tighten management of information released by their users, and when finding the information prohibited by laws and administrative regulations is released or transmitted, shall immediately terminate the transmission of such information and eliminate such information, prevent spread of information, keep relevant record, and inform the competent department.

Article 41 Electronic messages sent by the electronic message senders, and application software provided by the software suppliers shall not install any malicious software and shall not contain information whose release or transmission is prohibited by laws and administrative regulations.

The electronic messaging service providers and software download service providers shall perform the obligations of security management. Where the electronic messaging service providers or software download service providers are found committing the behaviors specified in the preceding paragraph, they shall terminate service offering, eliminate such information, keep relevant the records, and inform the competent department.

Article 42 The network operators shall set up a platform for complaints and reporting with respect to network information security, publicly report information such as methods used to submit complaints and receive and handle relevant complaints with respect to the network.

Article 43 The State-level cyberspace administration authorities and relevant departments shall perform their responsibility for the supervision and management of cybersecurity per laws, and when finding that the information prohibited by laws and administrative regulations is released or transmitted, shall require the network operator to terminate transmission, eliminate such information, and keep relevant record. For the above information from overseas sources, relevant institutions shall be informed to take technical measures and other necessary measures to block information.

Chapter 5 Monitoring & Early Warning and Emergency Response

Article 44 The State sets up a system for cybersecurity monitoring & early warning and information communication. The State-level cyberspace administration authorities shall coordinate relevant departments to enhance efforts to collect, analyze and communicate cybersecurity information, and per regulations, uniformly release the cybersecurity monitoring & early warning information.

Article 45 The departments in charge of critical information infrastructure protection shall set up a sound system for cybersecurity monitoring & early warning and information communication in their respective sectors and fields, and per regulations, submit the cybersecurity monitoring & early warning information.

Article 46 The State-level cyberspace administration authorities shall coordinate relevant departments to set up a sound cybersecurity emergency response mechanism, to develop cybersecurity emergency response plans and conduct drills regularly.

The departments in charge of critical information infrastructure shall develop the cybersecurity emergency response plans for their respective sectors and fields, and conduct drills regularly.

In the cybersecurity emergency response plans, cybersecurity incidents shall be classified by extent of hazards and scope of influence, and corresponding response measures shall be defined.

Article 47 When the cybersecurity incidents are imminent or their likelihood is increasing, the relevant department under the People's Government above county level shall, per the applicable laws and administrative regulations and the rights and procedures specified by the State Council, issue warnings corresponding to the level of threat, and based on a consideration of the characteristics of such imminent incidents and their possible consequences, take the following measures:
(1) Require relevant departments, institutions and their staff to collect and communicate relevant information without delay, and enhance the monitoring of incident developments;

(2) Organize relevant departments, institutions and their staff to analyze and assess the information of cybersecurity incidents, predict the possibility, scope of influence and extent of hazards of the incidents;
(3) Release the forecast information and analysis & assessment results relevant to the public;
(4) Per the regulations, give public warnings about possible harm of cybersecurity incidents, and announce the measures to avoid and mitigate the hazards.

Article 48 In case of cybersecurity incidents, the relevant departments under the People's Government above county level shall immediately initiate the cybersecurity emergency response plans, conduct an investigation and assessment of the cybersecurity incidents, require the network operators to take technical measures and other necessary measures to eliminate security perils, prevent spread of hazards, and promptly unveil the warning information relevant to the public.

Article 49 Where emergencies or work safety incidents occur due to cybersecurity incident, the provisions of the Emergency Response Law of the People's Republic of China and the Work Safety Law of the People's Republic of China shall apply.

Article 50 To safeguard national security and social public order, or responding to major social security emergencies, the State Council, or the provincial-level People's Government, with the approval from the State Council, may take temporary measures such as limited network communication in certain regions.

Chapter 6 Legal Liabilities

Article 51 Where a network operator fails to perform the cybersecurity protection obligations specified in Article 17 and Article 21 herein, the competent department shall order a rectification to be made, and give a warning. Where the operator refuses to make rectifications or causes a harm to cybersecurity, a fine of RMB 10,000 (not including, same below) - 100,000 (not including, same below) will be imposed. The supervisor directly in
charge shall face a fine of RMB 5,000 – 50,000.

Where an operator of critical information infrastructure fails to perform the cybersecurity protection obligations specified in Articles 27 - 29 and Article 32 herein, the competent department shall order a rectification to be made, and give a warning. Where the operator refuses to make rectifications or causes harm to cybersecurity, a fine of RMB 100,000 – 1,000,000 will be imposed. The supervisor directly in charge shall face a fine of RMB 10,000 – 100,000.

Article 52 In one of the following cases that the providers of network products and services, electronic message senders and software suppliers violate this Law, the competent department shall order a rectification to be made, and give a warning. Where they refuse to make rectifications or cause harm to cybersecurity, a fine of RMB 50,000 – 500,000 will be imposed. The supervisor directly in charge shall face a fine of RMB 10,000 – 100,000.

(1) Install malicious programs;
(2) Failure to clearly inform users and obtain user consent when offering products and services capable of collecting user information
(3) Failure to promptly inform users of the risks such as security defects or vulnerabilities existing in their products or services, and to take remedial measures;
(4) Unilaterally ending the provision of security maintenance for their products and services

Article 53 Where a network operator, in violation of this Law, fails to require users to provide real ID information, or provides relevant services for a user not providing real ID information, the competent department shall order a rectification to be made. Where the operator fails to make rectification or causes serious consequences, a fine of RMB 50,000 – 500,000 shall be imposed, meanwhile the competent department may order a suspension of relevant services, close of business for rectifications, shutdown of website, withdrawal of relevant business permit or revocation of business license. The supervisor directly in charge and other persons directly responsible shall face a fine of RMB 10,000 – 100,000.

Article 54 Where a network operator, in violation of this Law, infringes upon the right of citizens whose personal information is entitled to protection per laws, the competent department shall order a rectification to be made, and may, as the case may be, give a warning, confiscate illegal income, or impose a fine of 1-10 times the illegal income, or any combination of the above. Where illegal income is confiscated, a fine of less than RMB 500,000 shall be imposed; where consequences are serious, the competent department may order a suspension of relevant services, close of business for rectifications, shutdown of website, withdrawal of relevant business permit or revocation of business license. The supervisor directly in charge and other persons directly responsible shall face a fine of RMB 10,000 – 100,000.

Where a network operator, in violation of this Law, steals or otherwise illegally acquires, sells or illegally provides personal information of citizens to others, without constituting a crime, the public security department will confiscate illegal income, and impose a fine of 1- 10 times the illegal income. Where illegal income is confiscated, a fine of less than 500,000 shall be imposed.

Article 55 Where an operator of critical information infrastructure, in violation of Article 30 herein, uses the network products or services, which have not undergone or passed the security review, the competent department shall order a termination of such use, and impose a fine of 1-10 times the purchase amount. The supervisor directly in charge and other persons directly responsible shall face a fine of RMB 10,000 – 100,000.

Article 56 Where an operator of critical information infrastructure, in violation of this Law, stores network data overseas, or provides network data to overseas organizations or individuals without

undergoing a security review, the competent department shall order a rectification to be made, give a warning, confiscate illegal income, impose a fine of RMB
50,000 – 500,000, and may order a suspension of relevant services, close of business for

rectifications, shutdown of website, withdrawal of relevant business permit or revocation of business license. The supervisor directly in charge and other persons directly responsible shall face a fine of RMB 10,000 – 100,000.

Article 57 Where a network operator, in violation of this Law, fails to terminate the transmission of or eliminate the information whose release or transmission is prohibited by laws and administrative regulations, or fails to keep relevant record, the competent department shall order a rectification to be made, give a warning, and confiscate illegal income. Where the operator refuses to make rectifications or causes serious consequences,
a fine of RMB 100,000 – 500,000 shall be imposed, and the competent department may
order a suspension of relevant services, close of business for rectifications, shutdown of website, withdrawal of relevant business permit or revocation of business license. The supervisor directly in charge and other persons directly responsible shall face a fine of RMB 20,000 – 200,000.

Where the electronic messaging service providers or software download service providers fail to perform the security obligations specified in this Law, the preceding paragraph shall apply.

Article 58 Where the information whose release or transmission is prohibited by laws and administrative regulations is released or transmitted, the applicable laws and administrative regulations shall apply.

Article 59 Where a network operator, in violation of this Law, has one of the following cases, the competent department shall order a rectification to be made. Where the operator refuses to make rectifications or causes serious consequences, a fine of RMB 50,000 –
500,000 shall be imposed. The supervisor directly in charge and other persons directly responsible shall face a fine of RMB 10,000 – 100,000.

(1) Fail to inform the competent department of cybersecurity risks or cybersecurity incidents;
(2) Refuse or obstruct the inspection conducted by the relevant departments per laws;
(3) Refuse to provide necessary support and assistance.

Article 60 Where an operator commits the behaviors endangering cybersecurity specified in Article 22 herein, without constituting a crime, or commits other behaviors violating this Law, leading to a breach of the Public Security Administration Law, sanctions shall be imposed per the Public Security Administration Law.

Article 61 Where an operator of the government network at state organs fails to perform the cybersecurity protection obligations specified in this Law, its higher-level department or relevant departments shall order a rectification to be made. The supervisor directly in charge or other persons directly responsible shall be given sanctions per laws.

Article 62 Where any employees from the departments in charge of supervision and management of cybersecurity neglect their duties, abuse their power and practice fraud for personal purposes, without constituting a crime, administrative sanctions shall be imposed per laws.

Article 63 Where a violation of this Law causes harm to others, the civil liability shall be borne per laws.

Article 64 Where a violation of this Law constitutes a crime, the criminal liability shall be borne per laws.

Chapter 7 Supplementary Provisions

Article 65 The following terms used herein are defined as follows:
(1) Cyber refers to a network and system that are composed of computers or other information terminals and relevant devices, and serve to collect, store, transmit, exchange and process information per predefined rules and procedures.
(2) Cybersecurity refers to the capability of taking necessary measures to prevent attacks on, intrusion into, interference with, damage to, and illegal use of networks, as well as emergencies, aiming to enable networks to operate stably and reliably, and ensure the integrity, confidentiality and availability of information stored, transmitted and processed over networks.
(3) Network operator refers to the owner and administrator of network, and network service provider using the network owned or managed by others to provide relevant services, including basic carriers, network information service providers, and operators of key information systems.
(4) Network data refers to all electronic data collected, stored, transmitted, processed and generated via networks.
(5) Personal information of citizen refers to such personal ID information as name, data of birth, ID No., personal biometric information, occupation, residence address and telephone number of citizens recorded electronically or via other methods, as well as other information that can be used solely or used together with other information to identify citizens' personal identity.

Article 66 The security protection of the networks storing and processing the information involving state secrets, in addition to following this Law, shall comply with the provisions of the secrecy law and administrative regulations.

Article 67 The measures for protection of military networks and information security will be developed by the Central Military Commission.

Article 68 This Law will take effect from xxx _

Acknowledge of USITO
This document was translated by USITO and proof-read by SESEC team.

Introduction of SESEC Project

The Seconded European Standardization Expert in China (SESEC) is a visibility project co-financed by the European Commission (EC), the European Free Trade Association (EFTA) secretariat and the three European Standardization Organizations (CEN, CENELEC and ETSI).

Since 2006, there has been two SESEC projects in China, SESEC I (2006-2009) and SESEC II (2009-2012). In Dec 2014, SESEC III was officially launched in Beijing, China. Dr. Betty XU was nominated as the SESEC expert and will spend the next 36 months on promoting EU-China standardization information exchange and EU-China standardization cooperation.

The SESEC project supports the strategic objectives of the European Union, EFTA and the European Standardization Organizations (ESOs). The purpose of SESEC project is to

- Promote European and international standards in China;
- Improve contacts with different levels of the Chinese administration, industry and standardization bodies;
- Improve the visibility and understanding of the European Standardization System (ESS) in China;
- Gather regulatory and standardization intelligence.

SESEC III Monthly Newsletter

SESEC III Monthly Newsletter is the gathering of China regulatory and standardization intelligence. Most information of the Monthly Newsletter were summarized from China news media or website. Some of them are the first-hand information from TC meetings, forums/workshops, or meetings/dialogues with China government authorities in certain areas. Regulatory and standardization information summaries, translations, and strategic analyses in the prioritized areas selected by SESEC partners, were offered by SESEC III expert. With the limited resources of SESEC III, detailed translations of some news items only can be available on request.

SESEC III Special Reports

SESEC III Special Reports are the regulatory and standardization reports on some areas with deeper and wider overview or analyses. SESEC III Special Reports also cover the prioritized areas selected by SESEC partners. They also can be some hot topics or lobby activities reports in China.