SESEC IV

China Cybersecurity Regulation and Standardization

Monthly

Newsletters

January 2019

SESEC IV China Cybersecurity Standardization Monthly Newsletter

JANUARY 2019

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 three SESEC projects in China, SESEC I (2006-2009). SESEC II (2009-2012) and SESEC III (2014-2017). In April 2018, SESEC IV 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 IV China Cyber Security Standardization Newsletter

Cyber Security became a very important market access and standardization harmonization issues for EU ICT/IT Sectors who have business in China. To let the EU ICT/IT know more in this area, SESEC IV team started to make China Cyber Security Standardization Newsletter from June 2018.

SESEC IV China Cyber Security Standardization Newsletter is the gathering of China regulatory and standardization intelligence in Cyber Security areas. Most information of the Monthly Newsletter were summarized from China official websites and major news media. Some of them were the first-hand information from TC meetings, forums/workshops, or meetings/dialogues with China government authorities.

In this Newsletter

In this Newsletter, some news articles were abstracted from Chinese government organizations. All new published standards, implementation or management regulations and notice are summarized; original document and English version are available by SESEC IV.

Abbreviations

SAMR	State Administration for Market Regulation	国家市场监督管理总局
CAC	Cyberspace Administration of China & Office of the Central Cyberspace Affairs Commission	国家互联网信息办公室&中共中央网络安全和信息化委员会办公室
CAS	China Standardization Association	中国标准化协会
CCC	China Compulsory Certification	中国强制认证
CCSA	China Communication Standardization Association	中国通信标准化协会
CEC	China Electricity Council	中国电力企业联合会
CEEIA	China Electrical Equipment Industrial Association	中国电器工业协会
CELC	China Energy Labelling Centre	中国能效标识中心
CERT	National Computer Network Emergency Response Technical Team/Coordination Centre of China	国家互联网应急中心
CESI	China Electronic Standardization Institute	中国电子标准化研究所
CNCA	Certification and Accreditation Administration of China	中国国家认证认可监督管理委员会
CNIS	China National Institute of Standardization	中国国家标准化研究院
CNREC	China National Renewable Energy Centre	中国国家可再生能源中心
EPPEI	Electric Power Planning and Engineering Institute	电力规划设计总院
MIIT	Ministry of Industry and Information Technology of People's Republic of China	中国工业和信息化部
MOHRSS	Ministry of Human Resources and Social Security of China	人社部
MoHURD	Ministry of Housing and Urban-Rural Development	住房与建设部
MOR	Ministry of Railway	中国铁道部
MOT	Ministry of Transport	中国交通运输部
MOST	Ministry of Science and Technology	中国科学技术部
MPS	Ministry of public security	公安部
NDRC	National development and reform commission	中国国家发改委
NHFPC	National health commission	国家卫生健康委员会
NSSI	National Standard Literature Sharing Infrastructure	国家标准文献共享服务平台
OSCCA	State Cryptography Administration Office of Securit y Commercial Code Administration (OSCCA),	国家商用密码管理办公室
SAC	Standardization Administration of China	国家标准化管理委员
SAMR	State Administration on Market Regulation	国家市场监督管理总局
SCA	State Cryptography Administration	国家密码管理局
SCLAO	State Council Legislative Affairs Office	国务院法制办公室
SGCC	State Grid Corporation of China	国家电网
SIPO	State Intellectual Property Office	国家知识产权局
TC	Technical Committee for Standard Development	标准化技术委员会
SAC TC 260	the National Information Security Standardization Technical Committee (TC260)	国家信息安全标委会

Table of Contents

1. **CAC & MIIT & MPS & SAMR: Announcement on Launching the Crack-down on Apps Illegally Collecting and Using Personal Information**

   On 25 January 2019, the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS) and the State Administration of Market Regulation (SAMR) jointly announced a campaign to crack down on apps illegally collecting and using personal information.

   The announcement reiterates the obligation for operators of apps to strictly comply with the requirements of the Cybersecurity Law, requiring them to adopt effective safeguards for personal information, refrain from collecting personal information that is irrelevant to their services, describe personal information collection and use rules in clear and easily understandable ways, and obtain personal information subjects' consent. The announcement also calls for operators of apps to allow users to opt out of push notifications.

   Under the announcement, supervision and administration by regulatory authorities will be tightened, whereas the National Information Security Standardisation Technical Committee (TC260), the China Consumers Association (CCA), the Internet Society of China (ISC) and the Cybersecurity Association of China (CSAC) will be granted the power to develop rules governing the basic functions of apps and the information that needs to be collected for the performance of such functions, and to define the key aspects that an assessment determining whether an apps illegally collects and uses personal information should take into consideration. These organisations will also be tasked with entrusting professional institutions to carry out assessments on popular and important apps.

   Finally, the announcement also makes reference to a voluntary information security certification scheme for apps, encouraging search engines and app stores to clearly indicate whether an app has passed such certification, and prioritise those that have done so.

   Chinese Website：网信办、工信部、公安部、市监总局：关于开展App违法违规收集使用个人信息专项治理的公告

2. **CAC: Administrative Provisions on Blockchain Information Services**

   On 10 January 2019, the Cyberspace Administration of China (CAC) issued the Administrative Provisions on Blockchain Information Services, applicable to blockchain information services provided within China and with an effective date of 15 February 2019. The Administrative Provisions defines 'blockchain information services' as 'the provision of information services to the public through internet websites, applications and other forms, using blockchain technology or systems.'

   The Administrative Provisions outlines a series of obligations for providers and users of blockchain information services. For example, providers are required to complying with a series of security requirements and accepting periodic inspections, carry out real-name registration for their users, file a report to relevant cyberspace authorities for security assessment when introducing new products, applications or functions, conducting record filing on an CAC online platform, and keeping user data and logs for record for not less than 6 months. Users are prohibited from conducting activities that may jeopardise national security, social order, and the lawful rights of others.

   Chinese Website：网信办：区块链信息服务管理规定

3. **MIIT: Call for Comments on the Notice on Matters Concerning the Use of Spectrum by Enhanced Machine-Type Communication (eMTC) Systems (Draft for Comments)**

   On 16 January 2019, the Ministry of Industry and Information Technology (MIIT) issued for public consultation the Notice on Matters Concerning the Use of Spectrum by Enhanced Machine-Type

Communication (eMTC) Systems (Draft for Comments), with an official deadline of 16 February 2019. The draft defines eMTC as LTE-based cellular IoT enhanced machine type communication technology. It requires, among others, a radio regulatory authority's prior approval before eMTC system deployments, and the radio transmission equipment manufactured and imported for eMTC system use to obtain the Radio Transmission Equipment Type Approval. It contains two appendixes, the RF Technical Requirements for eMTC System Macro Stations, and the Administrative Requirements for eMTC System Base Station Setup and Interference Coordination.

Chinese Website：工信部：公开征求对《关于增强机器类通信（eMTC）系统频率使用有关事宜的通知（征求意见稿）》的意见

4. MIIT: Notice on Issuing the Interim Implementation Measures on Radio Transmission Equipment Sales Filing

On 10 January 2019, the Ministry of Industry and Information Technology (MIIT) released the Interim Implementation Measures on Radio Transmission Equipment Sales Filing, effective since 1 March 2019. The Interim Implementation Measures provides practical guidelines on how sellers of radio transmission equipment with the Radio Transmission Equipment Type Approval Certificate should conduct filing per the requirements of Article 44 of the Radio Regulation. A seller will be required to file a report with the local provincial-level radio regulator where it has completed its business registration, via a dedicated information platform and within 10 days of the start of a sales activity.

Chinese Website：工信部：关于印发《无线电发射设备销售备案实施办法（暂行）》的通知

5. MIIT: Notice on Issuing the Guidelines for the Construction and Promotion of Industrial Internet Networks

On 29 December 2018, the Ministry of Industry and Information Technology (MIIT) issued the Guidelines for the Construction and Promotion of Industrial Internet Networks.

Chinese Website：工信部：关于印发《工业互联网网络建设及推广指南》的通知

6. MIIT: Internet of Vehicles (Intelligent Connected Vehicles, ICVs) Industry Development Action Plan

On 28 December 2018, the Ministry of Industry and Information Technology (MIIT) unveiled its ICV Industry Development Action Plan. The Action Plan aims to achieve the goal of high-quality development of Internet of vehicle in stages. By 2020 (Stage I), ICV industry cross-industry integration will be achieved. The large scale application of ICVs with high-level automated driving functions will be realised in certain scenarios, whereas Internet of vehicles will reach a penetration rate of over 30%. Intelligent road infrastructure will also enjoy significant improvements. From 2020 onwards (Stage II), systems for technological innovation, standardisation, infrastructure, application services and safety assurance will be completely established, whereas ICVs with high-level automated driving functions and 5G-V2X will gradually reach the stage of large scale commercial application.

To realise such goals, the Action Plan proposes 5 major tasks, including 1) achieving key technological breakthroughs and promoting their commercialisation, by accelerating the development of critical components and systems as well as decision-making control platforms for ICVs, and supporting the research and development (R&D) and commercialisation of critical technologies such as LTE-V2X and 5G-V2X; 2) improving the standards system and promoting testing, verification and application demonstration, by fully implementing the National ICV Industry Standards System Development Guidelines, formulating important ICV standards, issuing spectrum licences where appropriate, establishing a testing and evaluation system for ICVs, and encouraging the application demonstration

of automated driving, intelligent logistics and other scenarios in airports, ports and industrial parks; 3) improving infrastructure for the ICV industry, by enhancing cross-ministerial coordination and central-local synergies, and building network infrastructure based on wireless communications technologies such as LTE-V2X and 5G-V2X as well as integrated big data and cloud platforms, with a view to boosting the digital transformation of road infrastructure; 4) encouraging a variety of application scenarios to boost the penetration rate of ICVs; and 5) ensuring security assurances with a special focus on ICV system operational security, data security and network security.

The Action Plan also outlines 6 concrete measures guaranteeing its implementation, including 1) strengthening the leadership of the Special Committee on Internet of Vehicles under China's Leading Group for Building National Manufacturing Power, enhancing cross-ministerial and central-local cooperation, concentrating on key issues and leveraging local/regional advantages; 2) increasing policy support, by giving play to existing financial channels, encouraging local governments to increase investments while attracting all forms of social capital, and increasing support for the R&D, application demonstration and commercialisation of key technologies; 3) cultivating an industrial ecosystem, by accelerating the development of the ICV manufacturing innovation centre, and leveraging platforms such as the World ICVs Conference and relevant industry alliances as they foster collaborative innovation by bringing together enterprises, academia, research institutes and customers; 4) creating conditions conducive to industry development, by formulating policies and regulations that can foster industrial innovation, revising rules that restrict industry development in a timely manner, providing policy and institutional guarantees for large-scale tests, demonstrations and commercial applications, enhancing the in- and post-market supervision of products and applications as well as the protection and effective utilisation of intellectual property rights (IPR), and improving the credit management system; 5) improving the talent cultivation system; and 6) encouraging international cooperation and cooperation with Hong Kong, Taiwan and Macau.

An MIIT official interpretation is available here.

Chinese Website：工信部：《车联网（智能网联汽车）产业发展行动计划》

7. SAC: Announcement on Releasing A Number of National Standards and Amendments to National Standards

In December 2018, the SAC approved a total of 646 national standards and 11 amendments to national standards. The released standards cover a wide range of areas, including but not limited to classified cybersecurity protection, IT security, IoT security and cryptography. Below please find a partial list of the standards issued that may concern members of the ICT and Cybersecurity Working Groups. Their full texts are now available on SAC website.

Implementation guide for cyber security classified protection of electric power information system

Information security technology—Testing and evaluation process guide for classified protection of cybersecurity

Semiconductor devices—Integrated circuits—Part 21-1：Blank detail specification for film integrated circuits and hybrid film integrated circuits on the basis of the qualification approval procedures

Information technology—Security techniques—Digital signature schemes giving message recovery—Part 3：Discrete logarithm based mechanisms

Information technology—Generic cabling for customer premises—Part 5: Data centres

Integration of informatization and industrialization management systems—Assessment guidance

Information security technology—Security technique requirements for citizen cyber electronic identity—Part 3: Verification service message and processing rules

Information security technology—Security technical requirements of smart card (EAL4+)

Information security technology—Security requirements for cryptographic modules

Information security technology—Security technical requirements for application of sensing terminals in internet of things

Information security technology－Security technical requirements of gateway in sensing layer of the internet of things

Information security technology－Security technical requirements of data transmission for internet of things

Information security technology—Security requirements for IoT sensing layer access to communication network

Information security technology —Requirements for disaster recovery service

Information security technology—Technical requirements of security management center for classified protection of cybersecurity

Information security technology —Capability requirements and evaluation specification for assessment organization of classified protection of cybersecurity

Information security technology —Technical specification for IPSec VPN

Information security technology-Security techniques requirement for electronic mail system

Information security technology—Specifications of definition and description for network attack

Information security technology—Technical requirements for cryptographic application for radio frequency identification systems—Part 1: Cryptographic protection framework and security levels

Information security technology—Technical requirements for cryptographic application for radio frequency identification systems—Part 2: Technical requirements for cryptographic application for RF tag, reader and communication

Information security technology—Technical requirements for cryptographic application for radio frequency identification systems—Part 3: Technical requirements for key management

Data specification for wearable product

Information technology—Biometrics used with mobile devices—Part1: General requirement

Information security technology—Security reference model and generic requirements for internet of things

Information technology — Biometrics—Fingerprint processing chip technical requirements

Information security techniques —Assessment criteria for disaster recovery service capability

Information security technology—Technical requirements for fingerprint recognition system

Information security technology—Security technical requirements, testing and evaluation methods for antivirus products

Information security technology—Security office USB disk technology requirement

Information security technology—Security management requirements for office information systems

Information security technology—Security basic technical requirements for office information systems

Information security technology—Security testing specification for office information systems

Chinese Website：国标委：关于批准发布部分国家标准和国家标准修改单的公告

8. SCA: Notice on Issuing the Quality Assessment Requirements for E-Government Electronic Certification

On 29 December 2018, State Cryptography Administration issued the revision version of the Quality Assessment Requirements for E-Government Electronic Certification. This new version will take effect on the first day of March 2019.

Chinese Website：国密局：关于印发《电子政务电子认证服务质量评估要求》的通知

9. SCA: Notice on Issuing the Specifications for E-Government Electronic Certification Business

On 29 December 2018, State Cryptography Administration issued the revision version of Specifications for E-Government Electronic Certification Business. This new version will take effect on the first day of March 2019.

Chinese Website：国密局：关于印发《电子政务电子认证服务业务规则规范》的通知

10. TC 260: Call for Comments on Information Security Technology – Specification for the Management of Information Identification on Social Networking Platform

On 1 February 2019, TC 260 issued a call for Comments on Information Security Technology – Specification for the Management of Information Identification on Social Networking Platform. If you would like to comment on the draft, please send your input to (Ms) Wang Jiao at wangjiao@cesi.cn by 3 March 2019.

Chinese Website：信安标委：关于征求《信息安全技术 社交网络平台信息标识规范》国家标准意见的通知

11. TC260: Call for Comments on 16 Information Security Standards

On 27 December 2018, the National Information Security Standardisation Technical Committee (TC260) called for comments on 16 draft information security standards, with an official deadline of 11 February 2019. The draft standards include:

Information security technology – Certificate request and application protocol based on multiple channels

Information security technology – Guide for health information security

Information security technology – XML digital signature syntax and processing specification

Information security technology – Security technique requirements and evaluation criteria for servers

Information security techniques – Cybersecurity vulnerability management specification

Information techniques – System security engineering capability maturity model

Information security technology – Guidelines for the category and classification of cybersecurity vulnerability

Information security technology – Light-weight authentication and access control mechanism

Information technology – Security techniques – Message authentication codes (MACs) – Part 1: Mechanisms using a block cipher

Information security technique – Entity authentication assurance framework

Information technology – Security techniques – Guidelines for information security management systems auditing
Information security techniques – Terminology

Information security technology – Security techniques – Information security incident management – Part 2: Guidelines on planning and preparing for incident response

Information security technology – Cybersecurity vulnerability identification and description specification

Information security technology – Security protection technical requirements and testing and assessment approaches for industrial control systems

Information security technology – Requirements for data security technology of government information sharing

Chinese Website：信安标委：关于征求 16 项国家标准意见的通知

12. TC 260: Call for Comments on Information Security Technology – Personal Information Security Specification (Draft)

Less than a year since the effectiveness of the recommended national standard GB/T 35273-2017 Information Security Technology—Personal Information Security Specification, the National Information Security Standardisation Technical Committee (TC260) issued a revised draft for public consultation on 1 February 2019, with the following updates:

Added 3.15: Personalised display

Added 5.3: No forced personal information collection

Revised 5.7: Exceptions to obtaining consent

Added 7.4: Personalised display and opt-out

Added 7.5: Aggregation of personal information collected for different business purposes

Added 8.7: Third-party access management

Revised 10.1: Identifying responsible departments and personnel

Added 10.2: Keeping record of personal information processing activities

Revised Appendix C: Methods for preserving personal information subjects' option to give or withhold consent

Added Appendix C.1: Distinction between basic business functions and additional business functions; C.2: Ensuring notification and explicit consent to realise basic business functions; and C3: Ensuring notification and explicit consent to realise additional business functions

Chinese Website：信安标委：关于开展国家标准《信息安全技术 个人信息安全规范（草案）》征求意见工作的通知

13. TC260: Notice on Issuing the 2019 Guidelines for the Application of National Cybersecurity Standards Projects

On 18 January 2019, the National Information Security Standardisation Technical Committee (TC260) issued the 2019 guidelines for the application of national cybersecurity standards projects. In addition to detailing the application procedures, eligibility criteria and a list of standards that are set to be

revised, the guidelines also outline certain key standardisation areas, covering personal information and data protection, critical information infrastructure (CII) protection, industrial control system security, automotive cybersecurity and smart door lock security. The TC260 will also support standardisation feasibility studies relating to artificial intelligence (AI), next-generation networks (5G and IPv6), quantum computing, security and controllability, supply chain security and data manipulation.

Chinese Website：信安标委：关于印发《2019 年网络安全国家标准项目申报指南》的通知

Contact details for SESEC IV

Dr. Betty XU
Seconded European Standardization Expert in China (SESEC)
A project co-funded by CEN, CENELEC, ETSI, EC and EFTA
Room 1005, The Oriental Place, No. 9 East Dongfang Road,
Chaoyang, Beijing, 100106, P R China
Phone: +86 10 85275366-802
Fax: +86 10 8527 6363
Mobile:+86 185 118 20197
E-mail: betty.xu@sesec.eu