



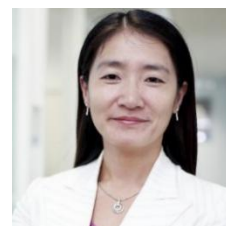
*Author: Betty XU
Distributed to: SESEC Partners,
EU standardization stakeholders
Date of issue: 19-07-2018*

SESEC IV
China Cybersecurity
Standardization Monthly
Newsletter
June 2018



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.

Table of Contents

Horizontal issues 5

- 1. TC260: The 2018 second director's meeting was held in Beijing..... 5**
- 2. TC260: Call for Comments on 24 Information Security Standards..... 5**
- 3. SAC TC260 officially issued 7 national standards in June 2018..... 7**
- 4. CNCA Releases the Announcement on the Rules for Implementation of Security Certification of Critical Network Equipment and Specialized Network Security Products 8**
- 5. CNCA MIIT MPS CAC Announcement on Releasing the List of Entities Undertaking Security Certification and Testing of Critical Network Equipment and Specialized Network Security Products (First Batch) 9**
- 6. MPS: Call for Comments on the Cybersecurity Multi-level Protection Regulation 9**
- 7. 6. MIIT, Call for Comments on the Administrative Provisions on Using 5905-5925 MHz Frequency Band for Direct Connected Communication of Internet of Vehicles (Intelligent Connected Vehicles) 10**
- 8. 7. Introduction of the working group on electronic products safety standards of the MIIT..... 10**
- 8.The project undertaken by CESI passed successfully 10**
- 11.TC260 issued a notice on the establishment of the information security standard project in 2018 8**
- 12.The latest recommended contents of national Cybersecurity Multi-level Protection evaluation institutions 9**
- 13.The practice guideline for cybersecurity..... 10**

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 Security 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会
SAMR	State Administration on Market Regulation	国家市场监督管理总局
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

Contents

1. TC260: The 2018 second director's meeting was held in Beijing

On 27 June 2018, the National Information Security Standardization Technical Committee (TC260) held the 2018 second director's meeting in Beijing, and the conference reviewed the proposal of the national standard project plan for network security in 2018. It approved 22 standard revised projects and 23 standard research projects, and adopted 30 national standards drafts.

Chinese website:

<https://www.tc260.org.cn/front/postDetail.html?id=20180628205342>

2. TC260: Call for Comments on 24 Information Security Standards

On 13 June 2018, the National Information Security Standardization Technical Committee (TC260) issued a public consultation on 24 information security draft standards. The titles of these 24 standards are listed below:

- Information security technology – Security impact assessment guide of personal information
信息安全技术 个人信息安全影响评估指南
- Information security technology – Cybersecurity protection requirements of critical information infrastructure
信息安全技术 关键信息基础设施网络安全保护要求
- Information security technology – Security controls of critical information infrastructure
信息安全技术 关键信息基础设施安全控制措施
- Information security technology – Evaluation approaches for industrial control systems information security
信息安全技术 工业控制系统信息安全防护能力评价方法
- Information security technology – Cybersecurity guide for automotive electronics systems
信息安全技术 汽车电子系统网络安全指南
- Information security technology – Security test requirements for cryptographic modules
信息安全技术 密码模块安全检测要求
- Information security technology – Guidance of cryptographic application for electronic records
信息安全技术 电子文件密码应用指南
- Information security techniques – Security technical requirements for operating system on smart mobile terminal
信息安全技术 移动通信智能终端操作系统安全技术要求
- Information security technology – Guide to malware incident prevention and handling
信息安全技术 恶意软件事件预防和处理指南

- Information security technology – Trusted computing architecture
信息安全技术 可信计算体系结构
- Information security technology – Guide to Bluetooth usage security
信息安全技术 蓝牙安全指南
- Information security technology – Secure coding guide for application software
信息安全技术 应用软件安全编程指南
- Information security technology – Code security audit specification
信息安全技术 代码安全审计规范
- Information technology – Security techniques – Network security – Part 1: Overview and concepts
信息技术 安全技术 网络安全 第 1 部分：综述和概念
- Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security
信息技术 安全技术 网络安全 第 2 部分：网络安全设计和实现指南
- Information technology – Security techniques – Anonymous digital signatures – Part 1: General
信息技术 安全技术 匿名数字签名 第 1 部分：总则
- Information technology – Security techniques – Anonymous digital signatures – Part 2: Mechanisms using a group public key
信息技术 安全技术 匿名数字签名 第 2 部分：采用群组公钥的机制
- Information security technology – Security technical requirements and test evaluation approaches of smart mobile terminals
信息安全技术 移动智能终端安全技术要求及测试评价方法
- Information security technology – Security technical requirements and testing and assessment approaches for firewall
信息安全技术 防火墙安全技术要求和测试评价方法
- Information security technology – Trusted computing specification – Trusted connect testing specification
信息安全技术 可信计算规范 可信连接测试规范
- Information security technology – Technical framework for authentication of mobile smart terminals based on biometric
信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架
- Information security technology – Technical requirements for mobile internet security audit products
信息安全技术 移动互联网安全审计产品技术要求
- Information security technology – Light-weight authentication and access control mechanism
信息安全技术 轻量级鉴别与访问控制机制
- Information security technology – Technical requirements for remote face recognition authentication system based on trusted environment
信息安全技术 基于可信环境的远程人脸识别认证系统技术要求

Chinese website:

<https://www.tc260.org.cn/front/bzzqyjList.html?start=0&length=10>

3. SAC TC260 officially issued 7 national standards in June 2018

On 7 June 2018, the National Information Security Standardization Technical Committee (TC260) officially issued 7 national standards, as follows:

- GB/T 20518-2018, Information security technology –the digital certificate format of the public key
Replace GB/T 20518-2006
Implementation Date: 2019-01-01
GB/T 20518-2018 《信息安全技术 公钥基础设施 数字证书格式》 代替标准号: GB/T 20518-2006 实施日期: 2019-01-01
- GB/T 25056-2018, Information security technology–Certificate authentication system password and related safety technical specification.
Replace GB/T 25056-2010,
implementation Date: 2019-01-01
GB/T 25056-2018 《信息安全技术 证书认证系统密码及其相关安全技术规范》 代替标准号: GB/T 25056-2010 实施日期: 2019-01-01
- GB/T 36322-2018, Information security technology–Code device application interface specification,
implementation Date: 2019-01-01
GB/T 36322-2018 《信息安全技术 密码设备应用接口规范》 实施日期: 2019-01-01
- GB/T 36323-2018, Information security technology–Basic requirements for safety management of industrial control system,
implementation Date: 2019-01-01
GB/T 36323-2018 《信息安全技术 工业控制系统安全管理基本要求》 实施日期: 2019-01-01
- GB/T 36324-2018, Information security technology–Classification specification for information security of industrial control system,
implementation Date: 2019-01-01
GB/T 36324-2018 《信息安全技术 工业控制系统信息安全分级规范》 实施日期: 2019-01-01
- GB/T 36466-2018, Information security technology–Guidelines for the implementation of risk assessment for industrial control systems,
implementation Date: 2019-01-01
GB/T 36466-2018 《信息安全技术 工业控制系统风险评估实施指南》 实施日期: 2019-01-01
- GB/T 36470-2018, Information security technology–General safety function requirements of field control equipment for industrial control system,
implementation Date: 2019-01-01
GB/T 36470-2018 《信息安全技术 工业控制系统现场测控设备通用安全功能要求》 实施日期: 2019-01-01

Chinese website:

<https://www.tc260.org.cn/front/postDetail.html?id=20180613184531>

4. SAC TC260 issued a notice on the information security standard project in 2018

On 12 July 2018, the National Information Security Standardization Technical Committee (TC260) issued a notice on the establishment of the information security standard projects in 2018. The specific contents of the notice include: the information safety standard projects in 2018. The list of these projects was now issued to all committee members, and the standard development shall be launched accordingly.

<https://www.tc260.org.cn/front/postDetail.html?id=20180712171505>

5. CNCA Releases the Announcement on the Rules for the Implementation of Security Certification of Critical Network Equipment and Specialized Network Security Products

CNCA Releases the Announcement on the Rules for the Implementation of Security Certification of Critical Network Equipment and Specialized Network Security Products in June 2018.

It is stipulated in the Cybersecurity Law that critical network equipment and specialized network security products shall comply with the mandatory national standards, and shall obtain certificate from a qualified certification body or meet the requirements of security testing, before being sold or provided.

According to the implementation rules, the process of security certification is divided into the following stages: application, documentation verification, type approval, factory inspection, result evaluation and approval, and ex-post supervision. Usually, the whole process will take no longer than 90 working days, unless the time needed for rectification.

The new scheme therefore can be regarded as the requirements for market access., Government assures that it “has been designed to improve coordination among the existing cybersecurity conformity assessment schemes managed by different ministries, namely the Information Security China Compulsory Certification (ISCCC), the Network Access Licensing (NAL) and the Sales Licensing for Specialized Computer Information System Security Products”. **A list of critical network equipment and specialized network security products, covering 15 product categories, was released on 9 June 2017.** Manufacturers of the products in the Catalogue should choose security certification or testing.

The release of other additional rules, such as the Rules on the Implementation of Security Certification for Critical Network Equipment and Specialized Network Security Products, are still pending.

Chinese website:

http://www.cnca.gov.cn/xxgk/ggxx/2018/201807/t20180702_56737.shtml

6. CNCA MIIT MPS CAC released the List of Security Certification and Testing bodies for Critical Network Equipment and Specialized Network Security Products (First Batch)

On 19 June 2018, CNCA, MIIT, MPS, and CAC jointly published the Announcement on Releasing the List of Entities Undertaking Security Certification and Testing of Critical Network Equipment and Specialized Network Security Products (First Batch).

Chinese website:

http://www.cnca.gov.cn/xxgk/ggxx/2018/201806/t20180619_56714.shtml

http://www.cnca.gov.cn/xxgk/ggxx/2018/201806/t20180619_56715.shtml

7. MPS: Call for Comments on the Cybersecurity Multi-level Protection Regulation

The drafted “Cybersecurity Multi-level Protection Regulation” aims to implement Article 21 of the Cybersecurity Law, which requires China to establish a Cybersecurity Multi-level Protection Scheme. The new regulation currently comprises of 8 chapters: General Provisions, Support and Assurance, Protection of Networks, Protection of Classified Networks, Regulation of Cryptography, Supervision and Regulation, Legal Liability and Supplementary Provisions. It classifies networks into five security levels and specifies accordingly the security safeguard measures that shall be adopted. Built upon the 2007 Administrative Measures for Information Security Multi-level Protection, the draft Regulation avoids controversial provisions for systems at level three and above, including that such products shall be developed by Chinese state-owned enterprises, and China enterprises shall have independent IPR in the core technology and key components of the products.

In addition, the draft Regulation encourages the promotion of secured and trustworthy network products and services, and requires network administrators to procure secure network products and services based on the network’s security level; the network products used in key network components shall be tested by professional testing bodies; and the network products and services shall pass national security review if national security will be affected. Remote technical maintenance for networks at level three and above will be prohibited, unless a security assessment is conducted, risk prevention measures shall be taken and maintenance logs shall be kept for regulatory inspections.

Chinese website:

<http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html>

8. Update of National Evaluation Bodies for Cybersecurity Multi-level Protection

In June 2018, China's Cybersecurity Multi-level Protection Portal released the new catalogue of the recommended evaluation bodies for national Cybersecurity Multi-level Protection . The catalogue includes nearly 200 evaluation bodies in China, listing their key information such as the names, contact information, recommendation date and validity period of For more details, please visit the link:

<http://www.djbh.net/webdev/web/HomeWebAction.do?p=getZxdt&id=402885cb35d11a540135d168e41e000c&xx=b119edd7e8fd93b6599def8b273b2701>

9. MIIT, Call for Comments on the Administrative Provisions on Using 5905-5925 MHz Frequency Band for Direct Connected Communication of Internet of Vehicles (Intelligent Connected Vehicles)

On 20 June 2018, the Ministry of Industry and Information Technology (MIIT) issued a public consultation on the Administrative Provisions on Using 5905-5925 MHz Frequency Band for Direct Connected Communication of Internet of Vehicles (Intelligent Connected Vehicles). For more details in Chinese, please see below:

Chinese website:

http://zmhd.miit.gov.cn:8080/opinion/noticedetail.do?method=notice_detail_show¬iceid=1960

10. CESI 2017 cybersecurity standards development project has been finished

On 8 July 2018, CESI announce the completion of the project of ‘ 2017 cybersecurity standard development, education and internationalization.

This project was a national funded project and some of the research results have been showed in the standards drafting processes of SAC TC 260.

Chinese website:

<http://www.cesi.cn/201807/4068.html>

11. TC260 released Guideline for the implementation of cybersecurity

‘Guideline for the implementation of cybersecurity’ is the technical document issued by the National Information Security Standardization Technical Committee (TC260). The guideline aims to promote network security standards, deal with network security incidents, improve network security and enhance awareness on network security. For more details in Chinese, please see below:

Chinese website:

<https://www.tc260.org.cn/front/cbw.html?start=0&length=4&type=3>

12. Introduction of the working group of MIIT electronic products safety standards

The working group on electronic products safety standards of the Ministry of Industry and Information Technology (MIIT) (hereinafter referred to as the safety working group) was established in 2004. It is mainly responsible for the standardization for sound and video equipment, information technology equipment, communication technology equip-

ment, related parts and components, and testing methods. It mirrors IEC/TC 108, ‘electronic products safety technology committee in the field of audio and video, information technology and communication technology’.

Approved by MIIT and SAC, the WG will be transformed into the National Electronic Product Safety Technical Committee.

The working group has developed GB 4943.1-2011 "information technology equipment safety first parts: General requirements", GB 8898-2011 "audio, video and similar electronic equipment safety requirements" and other mandatory national standards, recommended national standards, ministry-level standards supporting the implementation of relevant laws and regulations and playing a vital role in the field of electronic product safety.

Chinese website:

<http://www.cesi.cn/201806/4025.html>

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@sesecc.eu