



Development and Prospect of China's Information Security Certification Scheme

CHINA INFORMATION SECURITY CERTIFICATION CENTER



Contents

01

Cyber Security Assurance and Conformity Assessment System

02

Construction of Information Security Certification Scheme in China

03

Prospect of Information Security Certification Scheme in China

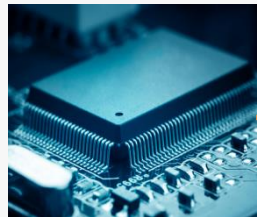
Cyber Security Assurance and Conformity Assessment System



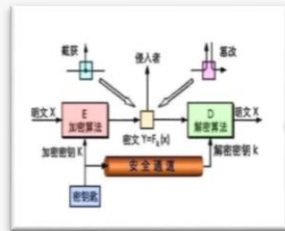
Critical Information Infrastructure



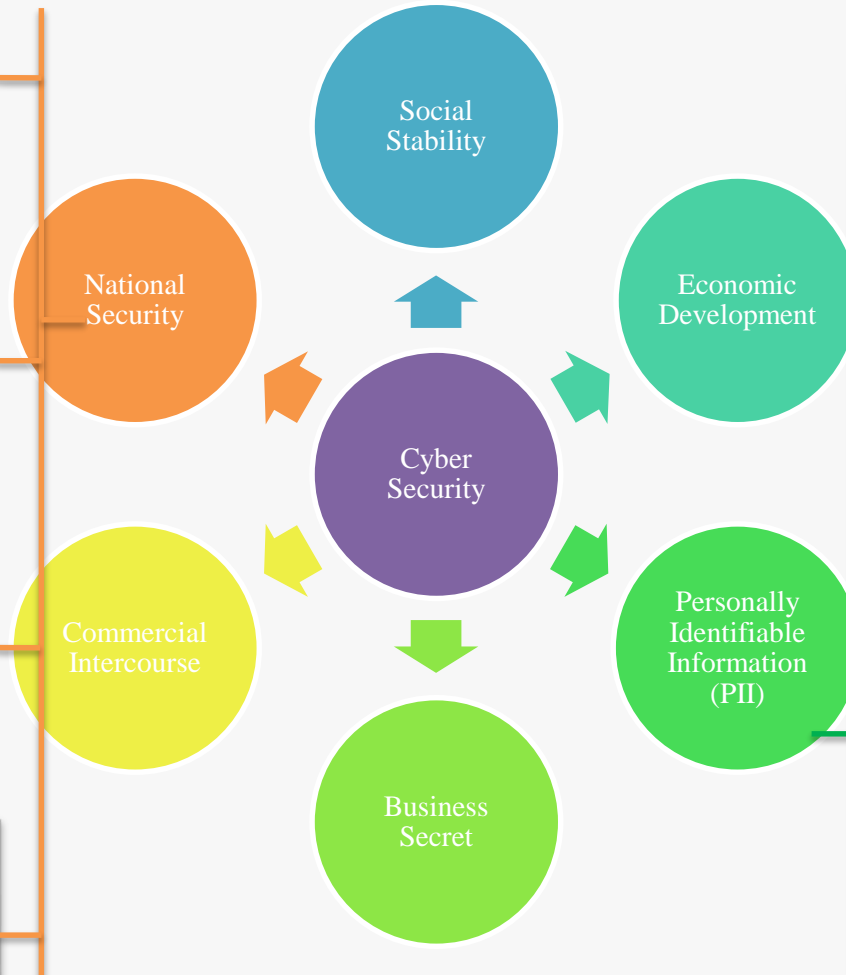
Government & Important Industries



Fundamental Hardware & Software



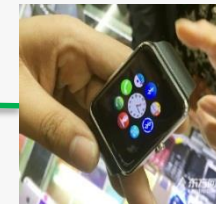
Core Technologies



Privacy



Payment

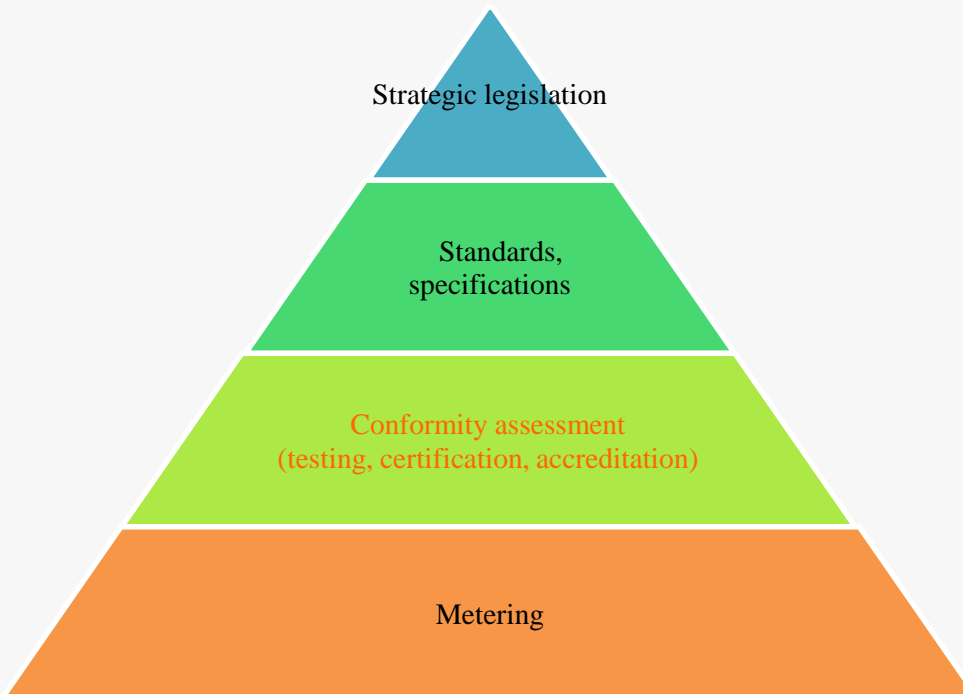


Wearable Devices



Internet of Things

■ Conformity assessment, standards and metering (national quality infrastructure (NQI))



- Determine the basic legal principles and strategic objectives
- Detail the behaviors for restraining manufacturing and use, and support the law enforcement
- Verify the conformity, transfer the trust, and support the supervision
- Establish the reference, and provide the consistent foundation

Conformity assessment is the key component of the cyber security assurance system



Functions of conformity assessment activities for cyber security assurance

- Testing and Assessment: To prove that the assessed subject conforms to the requirement, generally be responsible for the received samples
 - Products and systems
- Certification: To prove a certain batch of subjects being assessed conforms to the requirement, and require it to keep the conformity
 - Product certification: To provide the assurance bases for cyber security on the physical layer of products
 - System certification: To provide assurance for cyber security in management system and business process
 - Service certification: To provide assurance for cyber security in supplier's capabilities, process and behaviors
 - Personnel certification: To provide assurance for cyber security in personnel's knowledge, capabilities and qualifications
- Accreditation: A third party's proof for formally indicating that the qualified assessment institution has the working capability of implementing conformity assessment
 - Accreditation for the abilities of testing institutions and certification institutions



Contents

01

Cyber Security Assurance and Conformity Assessment System

02

Construction of Information Security Certification Scheme in China

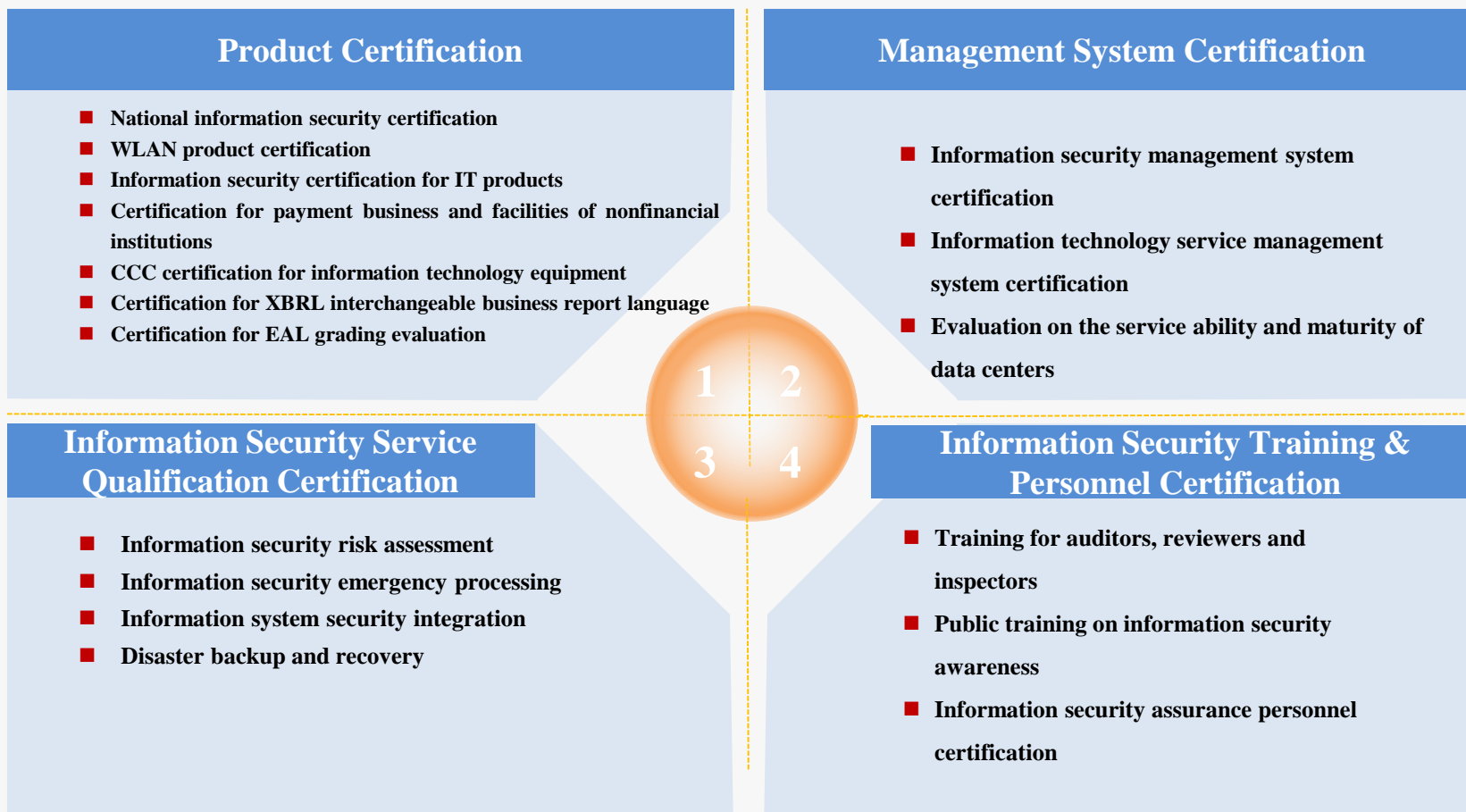
03

Prospect of Information Security Certification System in China

Establishment of information security certification scheme in China

- In 2003, the *Opinion of the National Leading Group of Informization Concerning Reinforcing the Information Security Assurance Work* (No. 27 issued by the Central Government Office) required to “standardize and reinforce the assessment and certification of information security products”.
- In 2004, the 8 ministries and commissions of the former National Internet Information Office, the General Administration of Quality Supervision, Inspection and Quarantine, the Certification and Accreditation Commission, the Ministry of Public Security, etc. issued the *Notification on the Establishment of National Certification and Accreditation Systems for Information Security Products* (No. 57 by the national certification union) required to establish the unified certification and accreditation systems for information security products.
- In June, 2006, the State Commission Office of Public Sectors Reform (SCOPSR) approved to establish China Information Security Certification Center as the public institution directly under the General Administration of Quality Supervision, Inspection and Quarantine,
- After foundation, the Office of Central Leading Group for Cyberspace Affairs clearly required to speed up to consummate the certification system for cyber security products.

Developed information security certification businesses



Certification for information security products

- National certification for information security products

- Range of certification: Forcibly implemented within the range specified by the Government

Procurement Law

- Product catalog: 13
- Based standards: National standards for relevant products
- Institutions for detection and certification: 1 certification institution (ISCCC), and 7 designated

laboratories

- Information security certification for of IT products

- Range of certification: As the supplementation of compulsory certification, autonomously developed according to the market need

- Product catalog: 70
- Based standards: General requirements (GB/T18336)+technical specifications
- Institutions for testing and certification: 1 certification institution (ISCCC), and 9 designated

laboratories

Management system certification

- Information Security Management Systems (ISMS)
 - Based standards: GB/T22080/ISO/IEC27001
- Information Technology Service Management Systems (ITSMS)
 - Based standards: GB/T24405.1/ISO/IEC20000-1
- Business Continuity Management Systems (BCMS)
 - Based standards: GB/T30146/ISO22301

■ Service certification

- Information security service qualification certification
 - Range of certification: Emergency processing, risk assessment, security integration, disaster backup and recovery, software security development, and security operation and maintenance service
 - Based standards: *GB/T 32914-2016 Information Security Technology – Information Security Service Provider Management Requirements, Regulations on the Implementation of Information Security Risk Assessment Service Qualification Certification (ISCCC-SV-002)*, etc.
- B2C e-commerce transaction service certification

Information security personnel certification

- Subjects of certification: formal personnel + reserved personnel;
- Professional fields: Covering the two aspects of technology and management, including nine professional fields of security software, security integration, security management, security operation and maintenance, security of government affairs, service management, risk management, network attack and defense, business continuity, etc.

Type of Certification	Grade	Requirements for Certification
Professional Certification	Grade III (professional senior)	Professional courses (Grade II)+additional courses
	Grade II (professional)	General courses (Grade II)+professional courses (Grade I)
Qualification Certification	Grade I (basic)	Basic course + General courses (Grade I)
Reserve Certification	Reserve grade	Accreditation courses for universities and colleges + basic course + general courses (Grade I)

Business progress of information security certification

As of August, 2017, 2013
product certificates have been issued.

As of August, 2017, 353
Management system certificates have been issued.

As of August, 2017, 1949
information security service certificates have been issued.

As of August, 2017, nearly 10,000
information security personnel certificates have been issued.



Contents

01

Cyber Security Assurance and Conformity Assessment System

02

Construction of Information Security Certification System in China

03

Prospect of Information Security Certification Scheme in China

Requirements of laws and regulations on testing and certification

Article 23 of the *Cyber Security Law*

- Key network equipment and specialized cybersecurity products shall, in accordance with the compulsory requirements of relevant national standards, pass the security certification conducted by qualified institutions or meet the requirements of security detection before being sold or provided. The national cyberspace administration shall, in conjunction with relevant departments of the State Council, develop and release the catalogue of key network equipment and specialized cybersecurity products, and promote the mutual recognition of security certification and security detection results to avoid repeated certification and detection.

国家互联网信息办公室
中华人民共和国工业和信息化部
中华人民共和国公安部
中国国家认证认可监督管理委员会

公 告

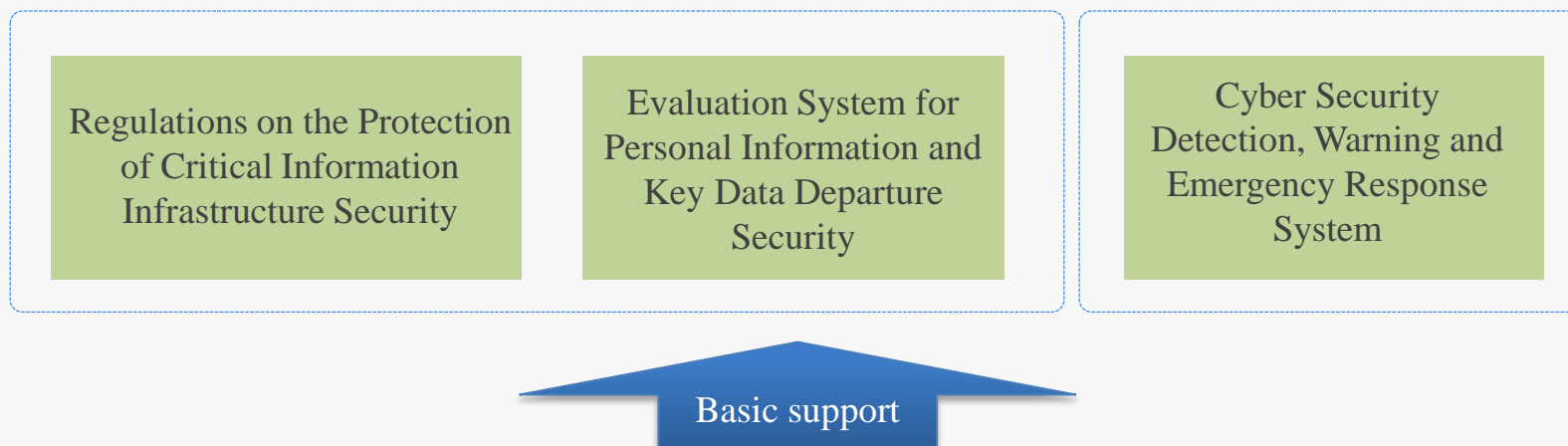
2017年 第1号

关于发布《网络关键设备和网络安全专用产品
目录(第一批)》的公告

为加强网络关键设备和网络安全专用产品安全管理，
依据《中华人民共和国网络安全法》，国家互联网信息办
公室会同工业和信息化部、公安部、国家认证认可监督管
理委员会等部门制定了《网络关键设备和网络安全专用产品

- 1 -

Other support provided by information security certification for *Cybersecurity Law*



- Data security certification: According to Article 37 of *Cyber Security Law*, “Personal information and important data which are indeed required by overseas bodies shall undergo security evaluation according to the provisions made by Cyberspace Administration of China and the State Council.”
- Management system certification: According to Article 25 of Regulation (exposure draft), “To organize to set up cyber security regulations and operating instruction and to monitor the implementation.”
- Personnel certification: According to Article 34 of *Cyber Security Law*, “To regularly implement cyber security education, technical training and skill assessment to employees.” According to Article 26 of Regulation (exposure draft), “A professional personnel of key positions for an operator’s cyber security shall take the appointment with a certificate.”

The executive meeting of the State Council (on September 6) determines to promote the construction of the quality certification system

- Firstly, vigorously popularized the advanced standards and methods for quality management, focusing on the industries of aviation, railway, automobile, **information**, etc.
- Secondly, combine guidance with compulsion. Carry out compulsory certification for the products concerning security, health, environmental protection, etc.
- Thirdly, explore the innovative methods for quality standard management, and carry out prudential supervision for new technologies, new products and new types of operation
- Fourthly, strengthen the supervision, and rigorously enforce the qualification accreditation standard
- Fifthly, deepen the mutual recognition of **international cooperation for quality certification**

Summary and prospects

- Implement the requirements for testing and certification in the *Cyber Security Law* and relevant regulations, improve the effectiveness of certification, and reduce the certification cost.
- Support the *Cyber Security Law*, aiming at the requirements for security protection of critical information infrastructure, promote to establish the voluntary certification systems for **big data security, industrial control security, security of the Internet of Things, robot security, security employees, service security**, etc., and exert the role of security certification in the baseline security assurance and compliance management.
- Implement the requirements of the executive meeting of the State Council for promoting the construction of quality certification system, accelerate the consummation and upgrading of the information security quality management system suitable for the characteristics of the information industry (e.g., big data enterprises), guide various enterprises, especially the service enterprises and medium, small and micro-scale enterprises, to obtain the quality certificate, and strengthen the international cooperation and exchanges in the field of information security certification.

ISCCC

Thank You!