WE WILL START AT 10:00 AM (CET)

SESEC V Webinar

China Cybersecurity and Data Protection in 2020-2022:

Policies, Laws & Regulations, and Standards

- ✓ You are ***muted***
- ✓ Use the ***Q&A or Chat Panel*** to submit your questions
- ✓ Keep your questions ***short and concise***
- ✓ Your questions will be answered after the presentation
- ✓ ***Slides and recording*** will be sent to you afterwards

- ✓ Contact us: assistant@sesec.eu
- ✓ Welcome to our website: https://sesec.eu/

SESEC INTRODUCTION

A Project co-funded by EC, EFTA, CEN CENELEC & ETSI

- **Promote** European and International standards in China
- **Improve** contacts between Project Partners and different levels of the Chinese administration, industry and standardization bodies
- **Enhance** visibility and understanding of the European Standardization System (ESS) in China.
- **Gather** regulatory and standardization intelligence
- **Undertake** technical lobbying

Goals

- The SESEC initiative supports **EC policy** and **ESOs strategic objectives** in China.
- Our ultimate goal is the enhancement of **EU-China dialogue and cooperation** in the field of standardization.
- It is notably expected to support the Framework Cooperation Agreement in place **between the ESOs and SAC.**

SESEC V LAUNCHED IN OCT 2022

Goals and Tasks

Call for stakeholders' Strategic Comments on Standardization Cooperation with China

Please contact

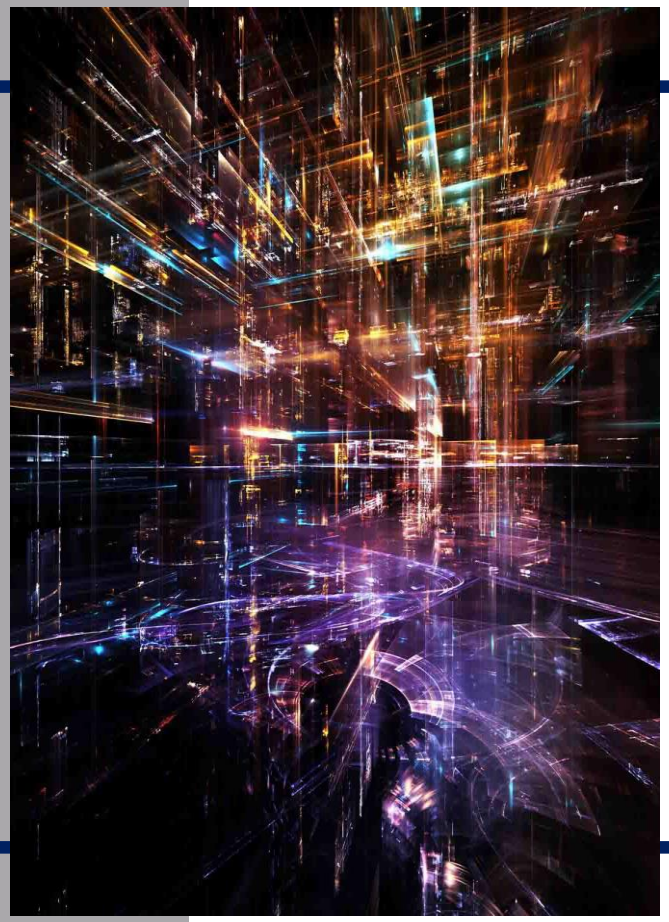
SESEC team via assistant@sesec.eu

Ms. Zhuohua Chen zchen@cencenelec.eu in CEN/CENELEC Management Centre,

Ms. Margot Dor margot.dor@etsi.org in ETSI,

Ms. VACCARO Silvia Silvia.VACCARO@ec.europa.eu in European Commission, and

Ms. Gudrun Rögnvaldardóttir, gur@efta.int in EFTA, for more details of SESEC project.



China Cybersecurity and Data Protection in 2020-2022:

Policies, Laws & Regulations, and Standards

CONTENT

1

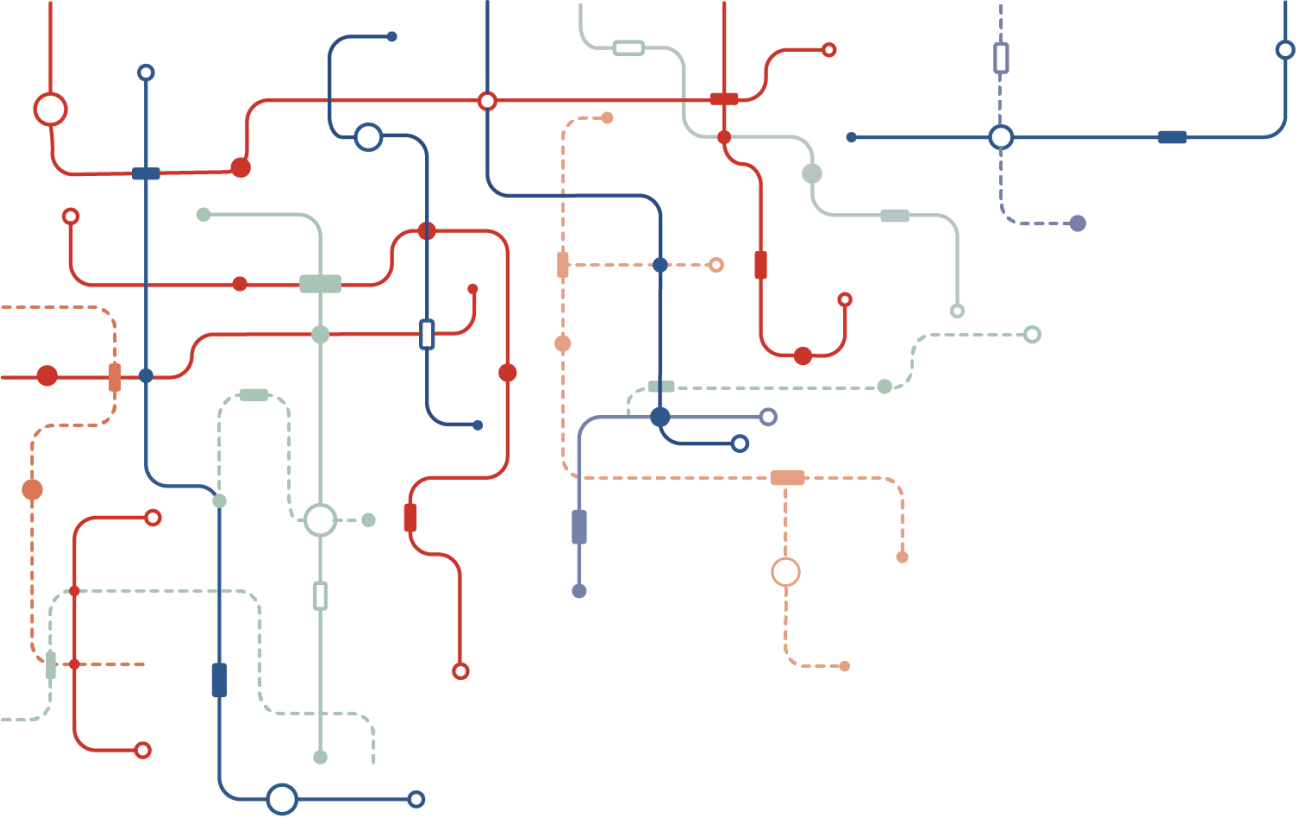
Policies
2020-2022

2

Laws and Regulations
2020-2022

3

Standards
2020-2022



01

Policies 2020-2022

Policies (2020-2022)

- ✓ **Cyber Security Topic has been one of the priorities of China Policy makers since 2015 !**
- ✓ **A bunch of polices were published in 2020-2022.**

Subject	Issuing body (or bodies)	Year of release	Name
Horizontal Policies	State Council	2022	The 14th Five-Year Plan for Digital Economy Development
	CAC	2021	The 14th Five-Year Plan for National Informatization
	State Council	2020	The 14th Five-Year Plan and the Long Range Objectives for 2035.
	Central Committee	2020	Implementation Program for Building a Law-based Society (2020-2025)
Data-related and Cybersecurity	MIIT	2021	Three-year Action Plan for High-quality Development of Cybersecurity Industry (2021-2023) (Draft for Public Comment)
	MPS	2020	Guidelines on the Implementing Cybersecurity Classified Protection Mechanism and the Security Protection Mechanism for Critical Information Infrastructure
	Central Committee and State Council	2022	Guidelines on Building Basic System for Data
	MIIT	2021	The 14th Five-Year Plan for the Development of Big Data Industry
	NDRC, CAC, MIIT, and NEA	2020	Guidelines on Accelerating the Construction of a National Collaborative Innovation System for Integrated Big Data Centers
Industry-specific	MIIT	2022	Guidelines for the Construction of Internet of Vehicles Cybersecurity and Data Security Standard System
	MIIT	2020	Guidelines for the Construction of Data Security Standard System in Telecommunications and Internet Industries
	NMPA (国家药监局)	2022	The 14th Five-Year Plan of Cybersecurity and Informatization Construction in Drug Administration
	SAMR and three other ministrial level department	2022	The 14th Five-Year Development Plan for Standardization in Financial Field
	MIIT	2021	The 14th Five-Year Plan for the Development of the Information and Communication Industry
	MIIT	2021	The 14th Five-Year Plan for the Development of Software and Information Technology Services
	MIIT	2022	Guidelines for the Construction of National Industrial Standard System for Internet of Vehicles (Intelligent Connected Vehicles) (2022 Edition) (Draft for comment)
	MIIT	2022	Administrative Measures for Data Security in Industry and Information Technology Sectors (Trial)
	MIIT	2022	Notice of Pilot Programme of Data Security Management in Industrial Sector
	MIIT	2021	Guidelines on the Submission and Sharing of Data Security-Related Risk Information in Industry and Information Technology Sectors (Trial) (Draft for Comment)
	NGSA（国家医疗保障局）	2021	Guidelines on Strengthening Cybersecurity and Data Protection

Key Policy 1: The 14th Five-Year Plan for Digital Economy Development

Issuing Body: State Council
Year of Release: 2021

Strengthen Cybersecurity-related Capability：

1. Strengthen coordinated application of cybersecurity technology in terms of its **planning, construction and use** to ensure the safe and orderly operation of key systems and facilities;
2. Strengthen the construction of **cybersecurity infrastructure**, the **cross-sector information sharing and coordinating**, the **incidents alerting system**, and **increase related capacity**
3. Strengthen the capacity for **emergency response**, and **CII's capacity** for cybersecurity, especially for **CII in key industries,** such as telecommunication, finance, energy, transportatation, etc.; Carry out regular **security assessment,** and strengthen **classified protection of cryptography** applications evaluation.
4. Support R&D of relevant technology, application, product, services and solutions
5. Strengthen security-related research management for **emerging technology** and application
6. Develop the industry of cybersecurity and accelerate the application of relevant technology
7. Increase awareness and talents training

Key Policy 2: Three-year Action Plan for High-quality Development of Cybersecurity Industry (2021-2023) (Draft for Public Comment)

Issuing Body: MIIT
Year of Release: 2021

Structure of the policy

General requirement: guiding phylosophy, basic principles, goals of development

Supporting measures

Key tasks:

- Support other industries
- Make actions driven by security needs
- Deepen the coperation between the cybersecurity industry and financial institutions
- Cultivate talents
- Optimize the ecology of cybersecurity industry

Key Policy 3: Guidelines on the Implementing Cybersecurity Classified Protection Mechanism and the Security Protection Mechanism for Critical Information Infrastructure

Issuing Body: Ministry of Public Security
Year of Release: 2020

Key words: Grading, Filing for record, Measures and system construction for cybersecurity, **Testing and evaluation**, and Supervision

Structure

1. General requirement: guiding philosophy, basic principles, goals of development

2. Requirement for implementing **Classified Protection**

3. Requirement for construction of **CII Security Protection Mechanism**

4. Coordination between different stakeholders and supporting measures

02

Laws and Regulations 2020-2022

LAWS

Revision of Cybersecurity Law (Draft for Comment) - 2022

Personal Information Protection Law - 2021

Data Security Law - 2021

Intensive Laws making for Cyber Security in 2 years !

Revision of Cybersecurity Law (Draft for Comment) - 2022

Cyber Security Law was published in 2016
Major Adjustments in Revised Draft for Comment:

1. Increasing, in the general provisions of the legal liability system, the **severity of punishment for non-compliance**. The increase of severity is reflecting in:

- addition of **new types of administrative punishment** - the amount of the fine might be linked to the turnover of the company
- **cancellation of the upper limit of the fine** – which can now exceed 1 million RMB
- **prohibition for relevant personnel from working** in relevant areas or taking relevant positions if necessary.

Controversies include but not limited to:

- Large discretion for law enforcement bodies
- Lack of the principle of “no penalty for compliance”
- Unclear definition of certain types of personnel that are hold accountable, which could potentially result in improper punishment

Revision of Cybersecurity Law (Draft for Comment) - 2022

Major Adjustments in Revised Draft for Comment:

2. Optimising, in the provisions relating to **critical information infrastructure (CII) protection** and cyberspace information security protection, the penalties for non-compliance.

3. Adding reference to other existing laws, mainly the ***Personal Information Protection Law***, for addressing non-compliance cases of personal information protection, with the purpose of avoiding overlaps and maintain the consistency of the legal system.

Data Security Law – published in 2021

Application Scope

Art. 2

1. **In the territory of China:** data processing activities and the security supervision thereof conducted
2. **Outside the territory of China:** those that conduct data processing activities to the detriment of the
   - national security
   - public interest, or
   - lawful rights and interests of citizens and organizations of China

Structure of the Law:

- General Provisions
- Data Security and Development
- Data Security Systems
- Data Security Protection Obligations
- Security and Public Availability of Government Data
- Legal Liablity
- Supplemental Provisions
- General Provisions

Data Security Law – published in 2021

Data Classification and Grading

Art. 21 Data Classification and Grading System:
requires relevant authorities to classify and grade data based on：

i). its importance in socio-economic development

ii). its importance and the degree of harm that will be caused by leakage or illegal use.

Support

Support

Regulations

Administrative Regulations on Network Data Security (Draft for Comment) - 2021

Official Guidelines:

Practice Guidelines for Cybersecurity Standards — Guidelines for Network Data Classification and Grading - 2021

Data Security Law – published in 2021

Art. 21 Protection of Important Data

Catalogue

↓

All regions and departments shall determine the specific catalogues of important data:

- region-wise
- industry-wise (e.g. automobile)

Note:
the official draft newly adds and highlights the **Core Data Protection** which will be stricter than the important data protection

Obligations for Processors

↓

- **Duty holders:** Identify the person in charge and management bodies for data security (Art. 27)
- **Regular obligations:** Risk Assessment + Report (Art. 30)
- ***Cross-Border* transfer:** *Measures for the Security Assessment of Cross-Border Data Transfer* - 2022

Personal Information Protection Law – published in 2021

It is also regarded as China Privacy Law

Definition of personal information?

In *Personal Information Protection Law* (PIPL):
"personal information" refers to all kinds of information related to an identified or identifiable natural person stored in both electronic and non-electronic form. Anonymized information will not be deemed as personal information.

Structure of the PIPL:

- Scope of personal information;
- Basic principles of personal information processing;
- Rights of personal information and its protection;
- Regulation of cross-border flow of personal information;
- Obligations of personal information processors.

Personal Information Protection Law – published in 2021

Application Scope:

Within China:
PIPL is applicable to all personal information processing activities conducted in China.

Beyond China:
PIPL also has extraterritorial jurisdiction. Processing activities conducted outside China will also be subject to PIPL, if:

a. the purpose of the processing is **to provide products or services to natural persons in China;**
b. the purpose of the processing is **to analyze and evaluate the behavior of natural persons in China**; or
c. **other circumstances** provided by laws and administrative regulations.

Personal Information Protection Law – published in 2021

Cross-border Transfer of Personal Information (PI)

General requirements	Duty holders	Specific requirements	Supporting policies/standards/regulations
1. Equal protection principle 2. Individual's separate consent(Art. 39) 3. Personal information protection impact assessment (“PIPIA”)(Art. 55)	CIIO operators	1. Recored within Chinese border (Art. 40) 2. Security Assessment (Art. 38)	*Measures for the Security Assessment of Outbound Data Transfer (In force) - 2022.7*
	Processors for certain volume and nature of PI	As long as one of the following conditions is met: 1. Certification for PI protection 2. Bilateral Contract 3. Others	*Certification Requirements for Cross-border Transmission of Personal Information - 2022.6*
	Other PI processors		*Provisions on Standard Contracts for Cross-border Transfers of Personal Information (draft for comments)*
			Others

LAWS

Cybersecurity Law – 2016 (mod 2022)

Personal Information Protection Law - 2021

Data Security Law - 2021

KEY REGULATIONS

CIIO：
Regulation on Protecting the Security of Critical Information Infrastructure - 2021

Cybersecurity Review:
Measures for Cybersecurity Review - 2021

Data Security System：
Regulation on the Administration of Network Data Security (Draft for Comments) - 2021

Management of important Data and Certain Personal Information：

- General: *Regulation on the Administration of Network Data Security (Draft for Comments) - 2021*
- Cross-border transfer: *Measures for Assessment of Outbound Data Transfer - 2022*

Cyber Protection of Minors:
Regulation on the Cyber Protection of Minors (Draft for Comment) - 2022

Others

03

Standards and relevant documents 2020-2022

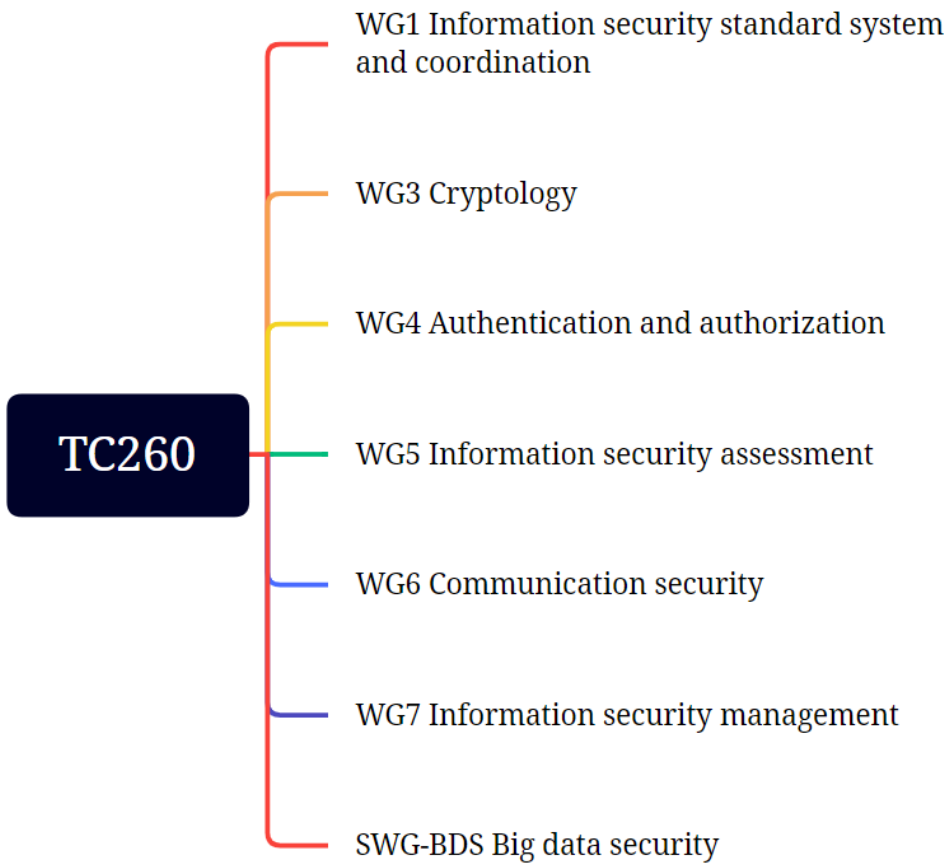
Key SDOs making Cyber Security Standards in China – SAC TC 260

National Information Security Standardization Technical Committee (TC 260)

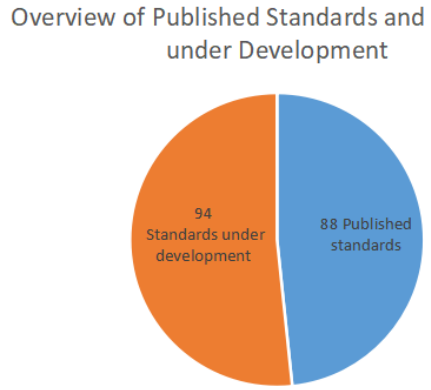
- TC260 is **a technical work organization engaged in the formulation of information security standards**. TC260 is responsible for organizing the development of standardization technology related to domestic information security.
- Set up in 2002, become very important after 2015
- Mirroring ISO/IEC JTC/SC27
- The Secretariate in China Electronics Standardization Institution (CESI)
- The superior organizations of TC 260 is China Standardization Administration (SAC) and China Cyberspace Administration (CAC)
- Since 2016, SAC TC 260 has published 400+ national standards in cyber security, and submitted 20+ ISO/IEC Standards

Overview of the Technical Committee and Standards Development

National Information Security Standardization Technical Committee (TC 260)



Overview of TC260's published standards and those under development in 2020-2022 August



#	Code of plan	Name in Chinese	Name in English	Newly-drafted/revised	Status
1	20220164-T-469	信息安全技术 软件供应链安全要求	Information security technology－Security requirements for supply chain of software	newly-drafted	drafting
2	20220166-T-469	信息安全技术 电子发现 第1部分：概述和概念	Information Security technology — Electronic discovery — Part 1: Overview and concepts	newly-drafted	calling for comment
3	20220163-T-469	信息安全技术 网络安全服务成本度量指南	Information security technology – Guide of cyber security service cost measurement	newly-drafted	calling for comment
4	20220165-T-469	信息安全技术 网络安全从业人员能力基本要求	Information security technology -Capability basic requirements of cybersecurity workforce	newly-drafted	calling for comment
5	20220167-T-469	信息安全技术 互联网平台及产品服务隐私协议要求	Information security technology—Requirements of Internet Platform、product and service privacy policy	newly-drafted	calling for comment
6	20220173-T-469	信息安全技术 电子政务移动办公系统安全技术规范	Information security technology - security technology specifications of mobile e-government system	revised	calling for comment
7	20220159-T-469	信息安全技术 信息安全控制评估指南	Information Security technology - Guidelines for the assessment of Information security Controls	revised	calling for comment
8	20220172-T-469	信息安全技术 无线局域网接入系统安全技术要求（评估保障级2级增强）	Information security technology - Security technology requirements for wireless local area network (wlan) access system (EAL2+)	revised	drafting
9	20220170-T-469	信息安全技术 射频识别（RFID）系统安全技术要求及测试评价方法	Information security technology - Security technical requirements and test evaluation approaches for radio frequency identification systems	revised	calling for comment

Overview of the TC 260's Work Focus and Progress in 2022

Overview of T260's Work Focus in 2022:

Basic Direction——Provide Support to:

- Cyber Security Law
- Data Security Law
- Personal Information Protection Law
- Cryptography Law
- Regulation on Protecting the Security of Critical Information Infrastructure

1. important Standards Development

a. Cybersecurity Law, Data Security, PIPL, and Regulation on Protecting the Security of CII:

- important data protection
- Risk assessment for data security
- Data transaction Security
- Governmental Data Processing
- Basic security requirements for pre-installed applications on smartphones
- Sensitive Personal Information Processing
- Requirements for large Internet enterprises personal information protection supervision agency
- Critical information infrastructure security assessment requirements

b. To guide the development of the cybersecurity technology industry, develop standards of:

- Interconnection framework for network security products
- Cyber security service capability
- Security specification for office devices
- IPv6 address coding

Overview of the TC 260's Work Plan and Progress in 2022

2. Research and Plan on Cybersecurity Standard Development

a. Technical Paper on

- Integrated defense against the attacking tools used for commercial monitoring
- Windows 7 operating system security reinforcement
- Internet users dynamic verification

b. White paper on secruity and risks in

- Artificial Intelligence
- Network trusted identity

c. Standardization System Establishment:

- National Standardization System (2022)
- Data Security Standardization System (2022)
- CII Security Standardization System (2022)

3. Standards publicizing and implementation

5. Capacity Building


全国信息安全标准化技术委员会秘书处

网络安全标准化工作月报

2022 年第 7 期（总第 13 期） 2022 年 9 月 30 日

4. International standards development:

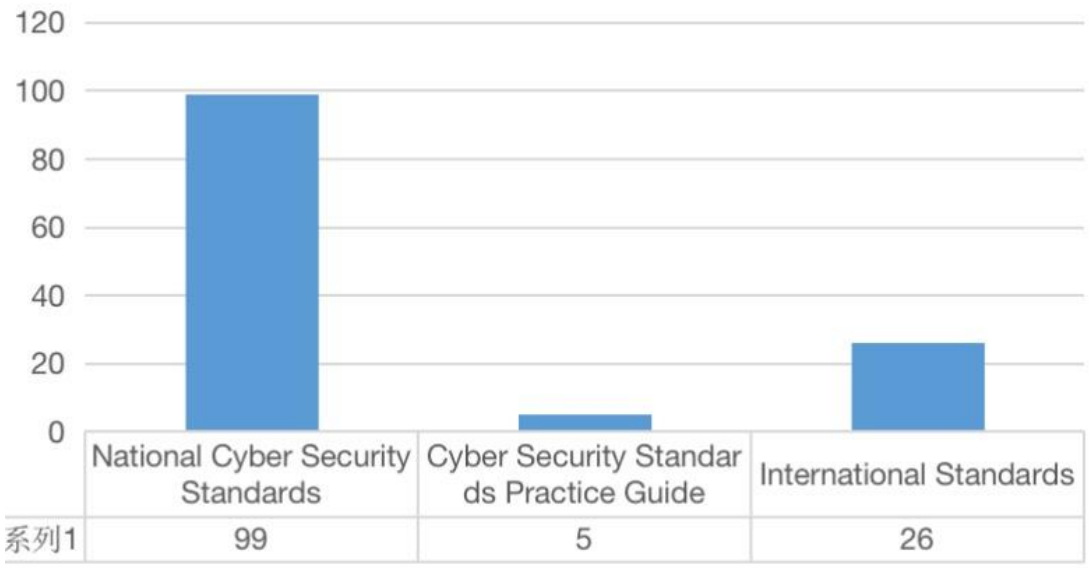
- At least 2 Approved International Standards Projects about Confidential Computing
- At least 2 standard Quasi-proposals Big Data Security and Privacy Protection, Virtual Network Security
- Professional cultivation
- Keep updated with European and US's Cybersecurity related strategy and standards' trend of development published and publish the findings on International Activties Updates on Cybersecurity
- 5 Research paper on technical standards that fall in the scope of ISO/IEC JTC1/SC27

Approved Projects in 2022 for National Cybersecurity Standards

No.	Name of the Standard Projects	WG	Newly-drafted/Revised
1	Interconnection of security products framework	WG5	Newly-drafted
2	Controllability evaluation method for security of open source software	WG5	Newly-drafted
3	Technical specification for security operation and maintenance system	WG5	Newly-drafted
4	Requirements for large Internet enterprises personal information protection supervision agency	WG7	Newly-drafted
5	Risk assessment method for data security	WG7	Newly-drafted
6	Capacity requirements for assessment organization of data security	WG7	Newly-drafted
7	Certification requirements for cross-border transmission of personal information	WG7	Newly-drafted
8	Cybersecurity testing and evaluation requirements for critical information infrastructure protection	WG7	Newly-drafted
9	Definition and description of Internet malware	WG7	Newly-drafted
10	Guidelines for cybersecurity insurance application	WG7	Newly-drafted
11	Security requirements for processing of key data	SWG-BDS	Newly-drafted
12	Security requirements for government data processing	SWG-BDS	Newly-drafted
13	Public data openness security requirements	SWG-BDS	Newly-drafted
14	Security requirements for processing of sensitive personal information	SWG-BDS	Newly-drafted
15	Security requirements for automated decision making based on personal information	SWG-BDS	Newly-drafted
16	General framework for confidential computing	SWG-BDS	Newly-drafted
17	Aritificial intelligence computing platform security framework	SWG-BDS	Newly-drafted
18	Security techniques--Hash-function--Part 1:General	WG3	Revised
19	Hash-functions--Part 2:Hash-functions using an n-bit block cipher	WG3	Revised
20	Hash-functions--Part 3:Dedicated hash-functions	WG3	Revised
21	Entity authentication— Part 2: Mechanisms using symmetric encipherment algorithms	WG4	Revised
22	Message Authentication Codes (MACs)—Part 2: Mechanisms using a dedicated hash-function	WG4	Revised
23	Public key infrastructure-- Online certificate status protocol	WG4	Revised
24	Security specification for office devices	WG5	Revised
25	Technical specification for network and terminal separation products	WG5	Revised
26	General security technical specification for terminal computer	WG5	Revised
27	Chinese government desktop core configuration specifications	WG5	Revised
28	Security specification of data recovery service for storage media	WG7	Revised
29	Information security controls practice guide	WG7	Revised
30	Security requirements for data transaction service	SWG-BDS	Revised

Overview of the TC 260's Work Plan and Progress in 2022

Overview of T260's Work Progress in 2022:



Please note:

1. those standards include both published standards and standards under development
2. the international standards only include the ones that are led by China
3. recengly-approved projects in the last slide are not taken into account

a. Key national standards:

Subject	Status	Note
Key data protection	Approved projects	
Risk assessment for data security	Approved projects	
Data transaction Security	Approved projects	This standard intends to revise GB/T 37932-2019
Governmental Data Processing	Approved projects	
Basic security requirements for pre-installed applications on smartphones	20220777-T-469 Information security technology — Basic security requirements for pre-installed applications on smartphones	
Sensitive Personal Information Processing	Approved projects	
Requirements for large Internet enterprises personal information protection supervision agency (draft)	Approved projects	
Critical information infrastructure security assessment requirements	Approved projects	
Interconnection framework for network security products	approved projects	
Cyber security service capability	approved projects	This standard intends to revise GB/T 32914—2016
Security specification for office devices	approved projects	This standard intends to revise GB/T 29244—2012 and 38558—2020
IPv6 address coding	approved projects	

Overview of the TC 260's Work Plan and Progress in 2022

Overview of T260's Work Progress in 2022:

White paper (standards-related ones):

- AI Security Standards (2022) (about to be published)
- Network Security Situation Awareness Standards (2020)
- 5G Network Security Standards (2021)

Cyber security standards practice guide:

Name	Status
Guidelines for Windows 7 operating system security reinforcement	Under development
Guidelines for information system backup during disasters	Under development
Security certification specification for cross-border personal information processing activities (Version 2.0)	Published
Technical guidelines for health code anti-counterfeiting	Published

International standards: A total of 26 standards that are led by China

- Information security — Encryption algorithms — Part 7: Tweakable block ciphers
- Information security — Secure multiparty computation — Part 2: Mechanisms based on secret sharing
- Information technology -Security techniques Security recommendations for establishing trusted connections between devices and services
- Information technology — Security techniques — Storage security
- Information technology — Security techniques — A framework for identity management — Pan 2 Relcrencc architecture and requirements
- ...

Standards Supporting of Data Security Law & Personal Information Protection Law

Standards in Support of Data Security Law: Part 1

General Mechanism	Specific Items	Articles to Suppor	Needs for Standard	Existing Standards
1. Data security system	Classification and grading system for data protection	Art. 21	Identify rules and methods for data classification and grading, as well as identification key data and core data so as to protect data in a category- and class-basis; Strengthen the protection for key data.	Requirements for classification and grading of network data (draft for comment); Rules for identification of key data (draft for review); Security requirements for processing of key data (draft).
	Data security risk assessment	Art. 22 and 23	Identify the method, process, and assessment report compliation requirement for data security risk assessment; Formulate critera for data security assessment organisations and personnel management, as well as qulification assessment and technical	Risk assessment method for data security (draft); Capacity requirements for assessment organization of data security (draft).
	Data security risk information monitoring system and early warning system	Art. 22 and 29	Support data security risk information acquisition, reporting, sharing, analysis, research and judgment, monitoring and early warning; Guide data processors to carry out data processing activities to strengthen risk monitoring; Take immediate and remedial measures when data security defects, vulnerabilities and other risks are found.	Relevant standards for cybersecurity information monitoring and early warning can be referred, for instance, GB/T 36643-2018 Cyber security threat information format; GB/T 32924-2016 Guideline for cybersecurity warning; Guide of cyber security information sharing (draft for review); Guidelines for cyber security information submission (draft for comments); General technical requirements for network security situation awareness system (draft for approval).
	Emergency response to data security incidents	Art. 23 and 29	Clarify relevant requirements or guidelines for data security incidents, emergency plans, and emergency response; Guide data processors to take immediate measures in case of data security incidents, and inform users in time according to regulations, and report to relevant competent authorities.	Relevant standards for emergency response to cybersecurity incidents can be referred, for instance, GB/Z 20986 Guidelines for the category and classification of information security incidents (in revision); GB/T 38645-2020 Guide for cybersecurity incident emergency exercises; GB/T 20985.2-2020 Information security incident management—Part 2: Guidelines to plan and prepare for incident response; Assessment criteria for cybersecurity emergency response capability (draft for

Standards Supporting of Data Security Law & Personal Information Protection Law

Standards in Support of Data Security Law: Part 2

General Mechanism	Specific Items	Articles to Suppor	Needs for Standard	Existing Standards
2. Data Security and Relevant Industry Development	Data as a production factor and relevant market safety	Art. 7	Clarify relevant security rules on data sharing, transaction, opening up, development and utilization, and integrated computing so as to meet the needs of the healthy development of the digital economy where data is taken as the key factor, and to promote the orderly and free flow of data in accordance with the law.	GB/T 39477-2020 Government information sharing—Data security technology requirements; GB/T 37932 Security requirements for data transaction service (in revision); Public data openness security requirements (draft); etc.
	Security of intelligent public service	Art. 15	Intelligent public services shall give full consideration to the data security and protection needs from the elderly and the disabled so as to avoid obstacles to their daily	
	Data security related technology and product	Art. 16	Standardize the development and use of data security related products; Guide and promote the application of data security technology and industry practices.	General framework for confidential computing (draft); GB/T 29765-2021 Technical requirements and testing and evaluating approaches for data backup and recovery products; GB/T 29766-2021 Technical requirements and testing and evaluating approaches of website data
	Data security related inspection, assessment and certification	Art. 18	Support data security inspection, evaluation, certification and other professional organisations to provide services; Promote the development of services regarding data security related inspection, assessment, certification,	GB/T 41479-2022 Network data processing security requirements; GB/T 37988-2019 Data security capability maturity model; Capacity requirements for assessment organization of data security (draft); Risk assessment method for data security (draft); etc.
	Security of data transaction	Art. 19 and 33	Clarify the security requirements on intermediary service organisations in data transaction , data transaction participants, transaction objects and transaction process so as to standardise data transaction behavior.	GB/T 37932 Security requirements for data transaction service (in revision)
	Professionals cultivation for data security	Art. 20	Support data security related education and training; Promote the cultivation of data security professionals.	Relevant standards in cybersecurity can be referred, for instance, Basic requirements for competence of cybersecurity workforce (draft for approval)

Standards Supporting of Data Security Law & Personal Information Protection Law

Standards in Support of Data Security Law: Part 3 and 4

General Mechanism	Specific Items	Articles to Suppor	Needs for Standard	Existing Standards
3. Data security and relevant protection obligations	Whole-process data security management	Art. 27	covering the whole process of data processing such as data collection, storage, use, processing, transmission, provision, disclosure and deletion, providing guidance for data processors to establish and improve the whole-process data security management.	GB/T 37988-2019 Data security capability maturity model; GB/T 35274 Security capability requirements for big data services (in revision); GB/T 37973-2019 Big data security management guide.
	Data processing ethics	Art. 28	Data processing activities and research and development of new data technologies shall conform to social morality and ethics.	Assessment specification for Machine learning algorithms (draft for review); Security requirements of genetic recognition data (draft for approval); Standardised technical document - Cybersecurity standards practice guide - Guidelines for the prevention of ethical security risks in artificial intelligence
	Legitimate data collection	Art. 32	Data shall be collected in a lawful and legitimate manner; data shall not be stolen or obtained by other illegal means; Data shall be collected and used within the purpose and scope prescribed by laws and	Currently the standardisation activities are focused on the collection of personal information, such as GB/T 35273-2020 Personal information security specification; GB/T 41391-2022 Basic requirements for collecting personal information in mobile internet applications; etc.
4. Security and opening of government data	Security of government data	Art. 38, 39 and 40	Standardize government data processing activities carried out by government departments themselves and by the entrusted third parties; Clarify security management requirements and technical requirements on government data processing, as well as safety supervision requirements for all types of data	Security requirements for government data processing (draft); GB/T 39477-2020 Government information sharing—Data security technology requirements.
	Sharing and opening of government data	Art. 42	Regarding the government data or public data sharing and opening up, clarify requirements on personal information protection, as well as on data security technology and management; Promote the construction of government data sharing and opening-up platforms, as well as the opening up and utilisation of government	GB/T 39477-2020 Government information sharing—Data security technology requirements; Public data openness security requirement (draft)

Standards Supporting of Data Security Law & Personal Information Protection Law

Standards in Support of Data Security Law: Part 5

General Mechanism	Specific Items	Articles to Suppor	Needs for Standard	Existing Standards
5. Data security in different industries	/	Art. 6	On the basis of generic data security standards, carry out research on the data security guidelines for industries while giving considertation to the data categorisation and classification in key industries, as well as characteristics of data processing and industry needs in data security; The guidelines will provide reference for data security work in the industry.	services (draft for approval); Data security requirement for online shopping services (draft for approval); Data security requirements for instant messaging services (draft for approval); Data security requirements for express logistics services (draft for approval); Data security requirements for internet payment services (draft for approval); Data security requirements for online audio and video services (draft for approval); 3. In Intelligent Connected Vehicles sector: Security requirements for processing of motor vehicle data (draft for approval); 4. In hygien and health sector: GB/T 39725-2020 Guide for health data

Standards Supporting of Data Security Law & Personal Information Protection Law

Standards in Personal Information Protection Law： Part 1 and 2

General Mechanism	Specific Items	Articles to Support	Needs for Standard	Existing Standards
1. General requirement	/	Art. 5,6,7,8,9	Provide specific requirements for processing personal information in accordance with the principles of legality, legitimacy, necessity and integrity, clear purpose and minimal processing, openness, transparency, personal information quality, responsibility and security.	GB/T 35273-2020 Information security technology—Personal information security specification GB/T 41391-2022 Information security technology—Basic requirements for collecting personal information in mobile internet applications
2. PI processing rules	PI Processing	Art. 10,19,20,21,22,23,25,27, 59	Provide general requirements for personal information processing activities such as collection, storage, use, processing, transfer, provision, disclosure and deletion.	GB/T 35273-2020 Information security technology—Personal information security specification GB/T 41391-2022 Information security technology—Basic requirements for collecting personal information in mobile internet applications
	Informed Consent	Art. 13,14,15,16,17,18,22,23, 25,26,27,29,30,31,39	Stipulate the formulation of personal information processing rules and disclosure requirements, and clarify the contents and methods of personal information processing notification; In terms of the legal basis of personal information processing and personal consent rules, clarify requirements in terms of different situations of consent.	GB/T 35273-2020 Information security technology—Personal information security specification GB/T 41391-2022 Information security technology—Basic requirements for collecting personal information in mobile internet applications 20210985-T-469 Information security technology—Implementation guidelines for notices and consent in personal information processing (draft for approval) 20220167-T-469 Information security technology—Requirements of Internet Platform、product and service privacy policy (draft for comments)
	Sensitive PI	Art. 28,29,30,31,32	Regarding sensitive personal information such as medical and health care information, financial accounts, whereabouts and tracks, clarify security requirements for data processing activities such as collection, storage, use, processing, transfer, provision, disclosure and deletion; Put forward the requirements for collection necessity, security protection, desensitization rules, informed consent, etc.	Security requirements for processing sensitive personal information (draft)
	Automated Decesion	Art. 24	Clarify the data security and personal information protection requirements of data processors in the process of automated decision making and related applications.	Automated decision security requirements based on personal information (draft) 20211000-T-469 Information security technology— Assessment specification for security of machine learning algorithms (draft for review)

Standards supporting of Data Security Law & Personal Information Protection Law

Standards in Personal Information Protection Law： Part 3 and 4

General Mechanism	Specific Items	Articles to Support	Needs for Standard	Existing Standards
3. Personal Information Outbound Transfer	/	Art. 38 and 39	Clarify security principles, security requirements and certification rules for cross-border transfer of personal information.	information transfer (draft) Cyber Security Standards Practice Guide - Security Certification Specification for cross-border Personal Information Processing activities
4. Personal Rights in PI Procesing Activities	/	Art. 44,45,46,47,48,49,50	Specify requirements or guidelines to protect the rights of individuals in personal information processing activities, such as the right to access, copy and carry, the right to correct, supplement, delete, explain and so on.	GB/T 35273-2020 Information security technology—Personal information security specification

Standards Supporting of Data Security Law & Personal Information Protection Law

Standards in Personal Information Protection Law： Part 5

General Mechanism	Specific Items	Articles to Support	Needs for Standard	Existing Standards
5. Obligations of PI Processors	PI Protection Technology	Art. 51	Specify technical requirements or application guidelines for personal information de-identification, including objectives, principles, implementation process, methods, etc., as well as evaluation methods for implementation effects.	GB/T 37964-2019 Information security technology—Guide for de-identifying personal information GB/T 41817-2022 Information security technology—Guidelines for personal information security engineering 20210996-T-469 Information security technology — Guide for evaluating the effectiveness of personal information de-identification (draft for approval)
	PI Security management	Art. 51 and 52	Provide management requirements or guidelines for classification management of personal information, and management requirements or guidelines for person in charge of personal information protection.	GB/T 35273-2020 Information security technology—Personal information security specification 20220787-T-469 Information security technology — Requirements for classification and grading of network data (draft for comment) Security requirements for processing sensitive personal information (draft)
	PI Protection Impact Assessment	Art. 55 and 56	Provide basic principles and specify implementation process of personal information security impact assessment so to provide guidance for personal information processors to carry out personal information	GB/T 39335-2020 Information security technology—Guidance for personal information security impact assessment
	PI Security Emergency Resposne	Art. 51 and 57	Provide requirements for the formulation and implementation of emergency plans for personal information security incidents, and clarify requirement regarding the redress and notification of personal information security incidents.	GB/T 35273-2020 Information security technology—Personal information security specification; Also could refer to emergency response related standards, for instance: GB/Z 20986 Information security technology - Guidelines for the category and classification of information security incidents (in revision) GB/T 38645-2020 Information security technology—Guide for cybersecurity incident emergency exercises

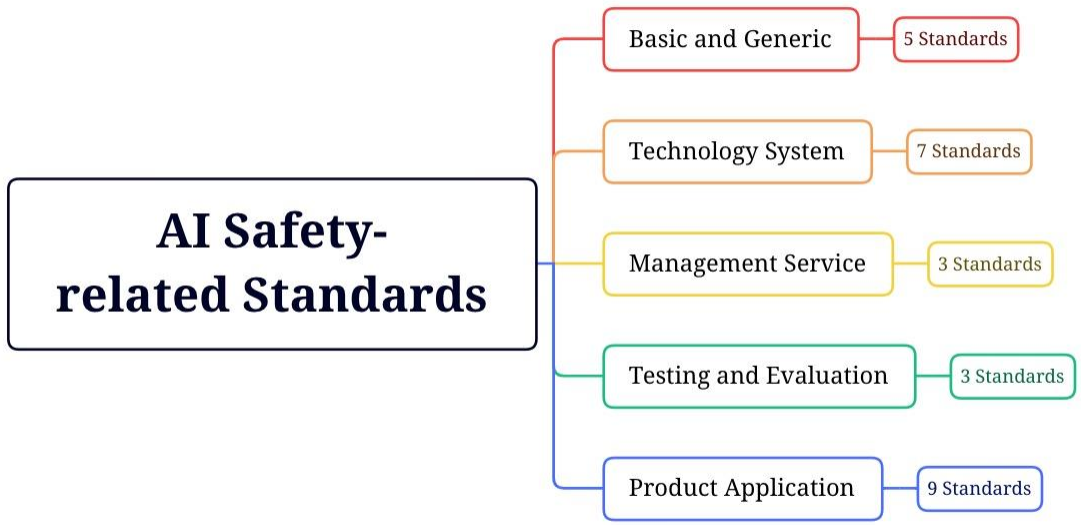
Standards Supporting of Data Security Law & Personal Information Protection Law

Standards in Personal Information Protection Law： Part 6

General Mechanism	Specific Items	Articles to Support	Needs for Standard	Existing Standards
6. Special Standard for PI Protection	Internet Platform	Art. 58	and have complex business types; ii)the requirements for the selection, structure, qualifications, constraints, and operation mechanism of supervisory bodies in large Internet enterprises; iii) data security and personal information protection requirements proposed to typical Internet platforms.	GB/T 42014-2022 Information security technology—Data security requirements for online shopping services GB/T 42015-2022 Information security technology—Data security requirements for internet payment services GB/T 42016-2022 Information security technology—Data security requirements for online audio and video services GB/T 42017-2022 Information security technology—Data security requirements for online ride-hailing services Requirements for large Internet enterprises personal information protection supervision agency (draft)
	APP	Art. 6,16 and 61	Support personal information protection assessment work for APPs, and promote the compliance of mobile APP ecology to the requirements of the *Personal Information Protection Law*.	GB/T 41391-2022 Information security technology—Basic requirements for collecting personal information in mobile internet applications 20210997-T-469 Information security technology — Personal information security testing and evaluation specification in mobile internet applications (draft for approval) 20210999-T-469 Information Security Technology — Guidelines for SDK security in mobile internet applications (draft for comment) 20220784-T-469 Information security technique - Audit and management of mobile internet applications collection and use of personal information guidelines for App store (draft for comment) 20220783-T-469 Information security technology - Personal information processing management guide for mobile internet applications of smart mobile devices (draft for comment) 20220777-T-469 Information security technology — Basic security requirements for pre-installed applications on smartphones
	Biometric Information Protection	Art. 26 and 62	Provide security requirements for collection, storage, use, supply, disclosure, deletion and other processing activities in terms of facial information and other biometric information.	GB/T 40660-2021 Information security technology—General requirements for biometric information protection GB/T 41819-2022 Information security technology—Security requirements of face recognition data GB/T 41806-2022 Information security technology—Security requirements of genetic recognition data GB/T 41773-2022 Information security technology—Security requirements of gait recognition data GB/T 41807-2022 Information security technology—Security requirements of voiceprint recognition data
	Evaluation and Certification	Art. 38 and 62	Provide the relevant basis and rules of personal information protection assessment and certification, and support relevant institutions to carry out personal information protection assessment and certification services.	20210997-T-469 Information security technology — Personal information security testing and evaluation specification in mobile internet applications (draft for approval) GB/T 35273-2020 Information security technology—Personal information security specification GB/T 41391-2022 Information security technology—Basic requirements for collecting personal information in mobile internet applications Requirements for authentication of cross-border personal information transfer (draft) Cyber Security Standards Practice Guide - Security Certification Specification for cross-border Personal Information Processing activities
	PI for Trustee	Art. 21 and 59	Provide requirements or guidelines for the protection of personal information of the trustee regarding typical scenarios of accepting the commission of processing personal information	GB/T 41574-2022 Information technology—Security techniques—Code of practice for protection of personal information in public clouds
	PI protection required in other emerging technology and	Art. 62	Formulate special personal information protection standards for emerging technologies and applications such as automobile data processing technology.	GB/T 41871-2022 Information security technology—Security requirements for processing of motor vehicle data

TC260 - SWG-BDS's White Paper on AI Safety-Related Standards (2022 draft)

AI Security-related Standard System



Please note that: standards identified by the White Paper under each of 5 catagories are based on needs of the industry. It means that the number of standards under each catagory continue to increase as more needs come out.

SWG-BDS is working on the White Paper on AI Security-related Standards (2022 Version)

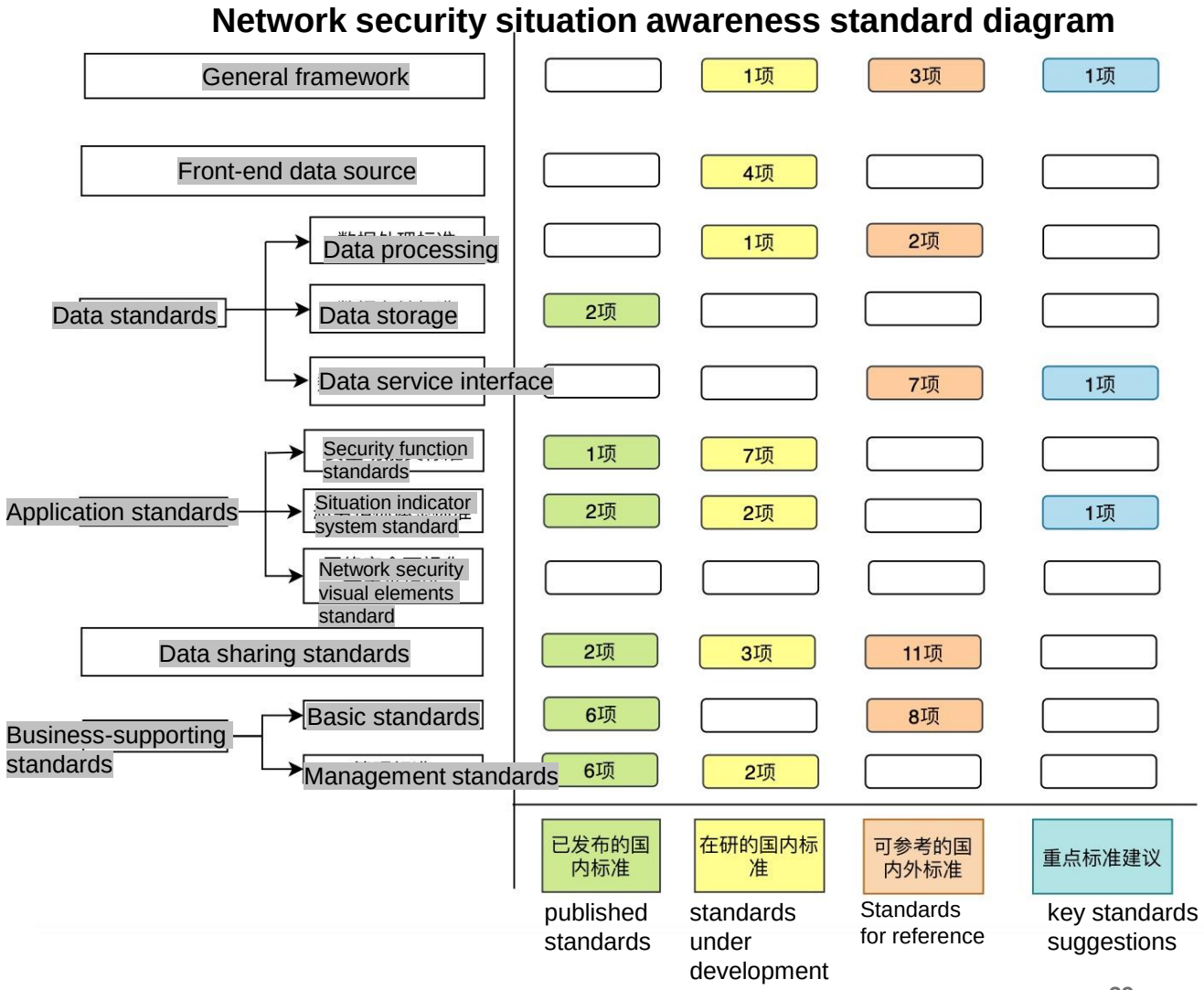
Key standards

- *GB/T 41871-2022 Information security technology—Security requirements for processing of motor vehicle data*
- *GB/T 41819-2022 Information security technology—Security requirements of face recognition data*
- *20211000-T-469 Information security technology— Assessment specification for security of machine learning algorithms*
- *Security criteria for classification and classification of AI applications (draft)*
- *AI computing platform security framework (draft)*
- *Security requirement for automated decision based on personal information (draft)*

Suggestions for AI Security-related Standardization

1. Accelerate standards development so as to meet urgent needs
(mainly: data protection and personal information protection; ethics and safety issues)
2. Strengthen the verfication and implementation of those standards
3. Deeply engage in international standards development

TC260's White Paper on Network Security Situation Awareness Standards (2020)



TC260's released the White Paper on Network Security Situation Awareness in 2020

Key SDOs

- TC 260
- TC 28
- CCSA
- Information System Security Standardization Technical Committee of the Ministry of Public Security

TC 260:

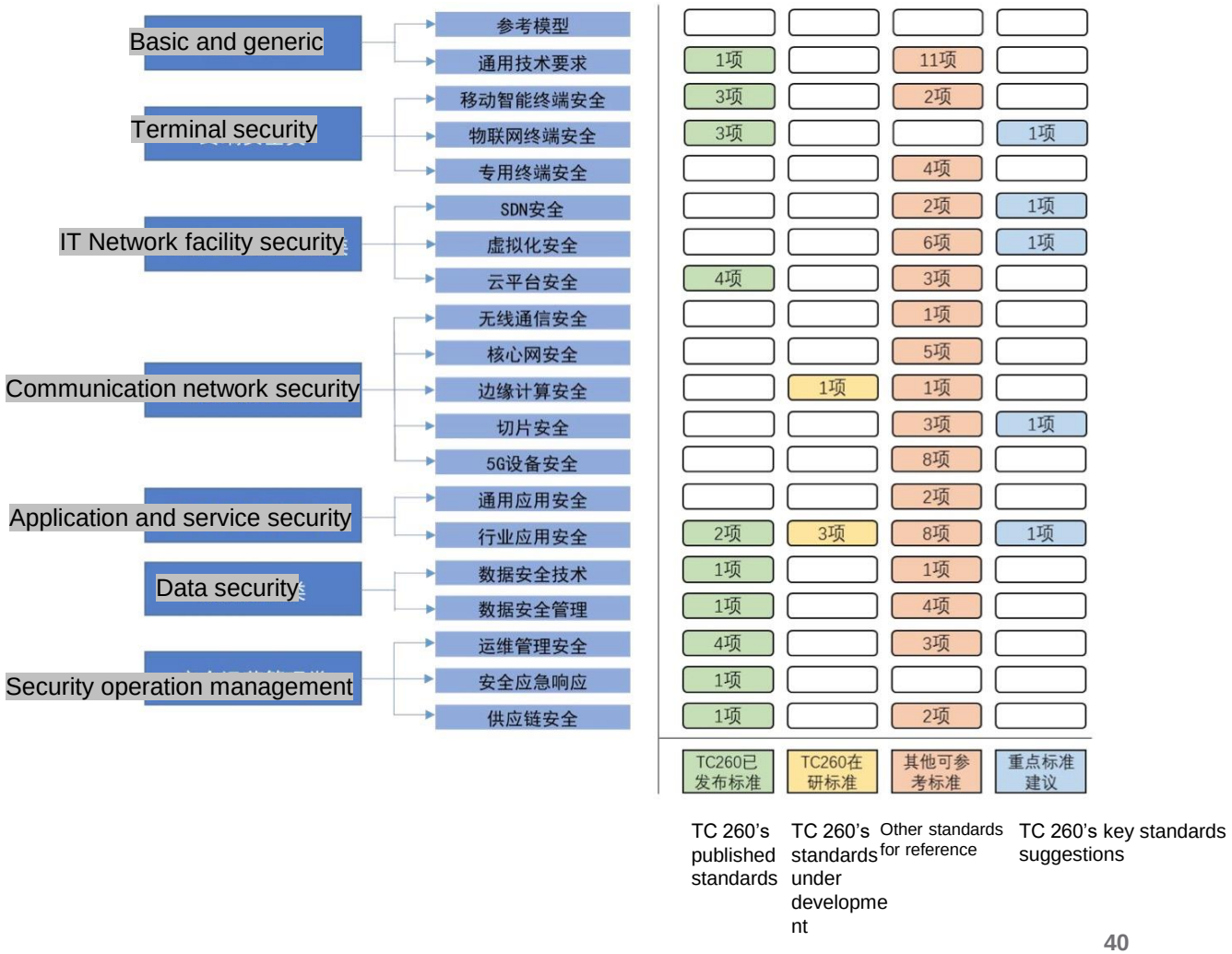
20210989-T-469 Information security technology — General technical requirements for network security situation awareness

Suggestions for AI Safety-related Standardization

1.Overall planning on standards of network security situation awareness
2. Accelerate the development of urgently-needed standards
3. Promote standards application

TC260 - WG 6's White Paper on 5G Network Security Standards (2021)

5G Network Security standard diagram



TC260's released the 5G Network Security Standards in 2021

Key SDOs

- MIIT: compulsory standard of GB 40050-2021 Critical network devices security common requirements:
- TC 260: recommended national standards
- TC 485: recommended national standards
- CCSA: sector standards

Suggested standards

1.Technical requirements for lightweight terminal security protection
2. Guidelines for network virtualization security
3. Software - defined network application security requirements
4. Technical requirements for network slicing security
5. Security technical requirements for open network capability

Case Study: Office equipment security standard

- In April 2022, TC260/WG5 a new standard proposal: *Information security technology – security specification for office devices*.

Specifically, the Draft stipulates that officer devices providers shall:

- Complete the design, development, production, delivery, operation, and maintenance of office devices within China, and use key components that are designed and manufactured in China. These key components include, but are not limited to, main control chips, laser scanner assembly, capacitance, resistance, motor, etc.
- Employ third party technologies for office devices, chips, engine, materials, software authorization, update, and technical support services, that do not have records of supply chain disruptions originating from political, diplomacy, trade or service capability factors.

- rule out the possibility for overseas office devices providers to participate in government procurement in China, as most of their products rely heavily on overseas components.
- Overseas manufactures' businesses with more state-owned enterprises could be negatively affected by this standard once adopted in government procurement and commercial bidding projects in the future.

Future standardization work

- **Standard development in support of the *Data Security Law* and *Personal Information Protection Law***
- **Complete the rule system (assessment, certification, standardized contract) in support of outbound data transfer**
- **Construction of basic system for data management**
- **Standard development in support of specific industries, such as automobiles, medical services, and finance, etc.**
- **Stricter requirements on large internet companies**
- **Cooperation with international communities, and compliance with international rules and standards in terms of data management and outbound transfer**

Thank you!

Dr. Betty Xu

Seconded European Standardization Expert in China (SESEC)

Room 1005,The Oriental Place, #9 East Dongfang Road, North-Part of Beijing East Third Ring, Chaoyang, Beijing, 100106, P R China

Phone: +86 10 85275366-802

Mobile: +86 185 118 20197

E-mail: betty.xu@sesec.eu

Wesite: www.sesec.eu