Fraunhofer SIT

Fraunhofer SINGAPORE

SURVEY

CHINA ELECTRIC VEHICLE AND CONNECTED VEHICLE SECURITY AND PRIVACY

GOVERNMENT, INDUSTRY AND STANDARDIZATION PERSPECTIVE (2015-2021)

Singapore/Darmstadt, July 2021

Imprint

Layout and Setting
Sophie Seeber

Contact
Fraunhofer Institute for
Secure Information Technology SIT
Rheinstraße 75
64295 Darmstadt, Germany

Phone +49 6151 869-100
E-mail info@sit.fraunhofer.de

Fraunhofer Singapore
50 Nanyang Avenue, NS 1-1 Level 5
639798 Singapore

Disclaimer

The work results in this document have been prepared carefully and on the basis of the known state of the art, but represent research approaches. For this reason, no liability or guarantee is assumed that the work results or the information meet the requirements of the current legal situation. The same applies to the usability, completeness or freedom from errors, so that any liability for damages that may arise from the use of these work results or information is excluded. These objects are not liable in cases of intent.

CONTENTS

Contents . . . III

List of Figures . . . VII

List of Tables . . . VIII

List of Abbreviations . . . X

I Introduction 17

1 Introduction . . . 18
- 1.1 Survey Methodology . . . 18
- 1.2 Project Team and Collaborators . . . 18
- 1.3 Report Structure . . . 19
- 1.4 Background Information . . . 19
- 1.5 Important Government Stakeholders . . . 19

II NEV and ICV Industry in China: Policy-Driven and Market-Driven 22

2 NEV and ICV Industry in China: Policy-Driven and Market-Driven . . . 23
- 2.1 Landscape of NEVs and ICVs Cybersecurity in China (2020) . . . 23
- 2.2 National High-Level Policies (2015-2017) . . . 24
- 2.3 National Cybersecurity Activities (2015-2020) . . . 25
- 2.4 NEV Policy and Market Driven Activities (2009-2020) . . . 27
  - 2.4.1 Institutional Reform (2010) . . . 27
  - 2.4.2 Subsidies (2009-2016) . . . 28
  - 2.4.3 Tax Incentives (2012-2014) . . . 29
  - 2.4.4 Industrial Development (2012-2020) . . . 29
  - 2.4.5 Market Access (2017-2020) . . . 30
  - 2.4.6 EV Infrastructure Standardization Activities (2015-2020) . . . 31
  - 2.4.7 Government Spending . . . 32
- 2.5 ICV Policy-Driven Activities (2017-2020) . . . 33
  - 2.5.1 Standardisation (2017-2020) . . . 33
  - 2.5.2 Industrial Development (2020) . . . 34
- 2.6 Summary . . . 34
  - 2.6.1 NEV Market Trends . . . 35
  - 2.6.2 EV Infrastructure Market Trends . . . 36
  - 2.6.3 ICV Market Trends . . . 37
  - 2.6.4 Automotive Cyber Security Market Trends . . . 38
  - 2.6.5 Shared Mobility Market Trends . . . 39

III China NEV and ICV Cybersecurity Law and Standardization Activities (2015-2020) 40

3 China NEV and ICV Cybersecurity Law and Standardization Activities (2015-2020) 41
3.1 National Cybersecurity and Cryptography Law 41
3.1.1 China Cybersecurity Law (CSL June 2017) 41
3.1.2 China Cybersecurity Review Measures (June 2020) 44
3.1.3 China Cryptography (Encryption) Law (CEL – Oct 2019) 45
3.2 Standardization Layers and Procedure 50
3.2.1 Standardization Layers 50
3.2.2 Publishing Procedure 51
3.3 NEV and ICV Security Standards 52
3.3.1 TC114 NEV Security Standards 52
3.3.2 TC260 NEV Information Protection Standards 54
3.3.3 CEC EV Charging Security Standards 56
3.3.4 CCSA Communications Security Standards 57
3.4 China Cryptography Standards 58
3.4.1 State Cryptography Administration 58
3.4.2 Cryptography Standards System 58
3.4.3 Chinese Cryptographic Algorithms 60
3.4.4 Comparisons: China and International Cryptography Standards 60
3.5 Summary 61

IV China Data Security and Personal Information Protection Regulations 62

4 China Data Security and Personal Information Protection Regulations 63
4.1 Data Security: Law and Standards 63
4.1.1 China Data Security Law (2020 – Draft) 63
4.1.2 Data Security Standards 66
4.1.3 Map Data Security 67
4.2 Measures for Security Assessment of Cross-border Transfer of Personal Information (Draft for Comments 2019) 67
4.3 Personal Information Protection: Laws, Standards 68
4.3.1 China Personal Information Protection Law (Expert Proposal 2019 - Draft) 68
4.3.2 Personal Information Protection Standards 69
4.3.3 Overview of International PI Protection Laws 70
4.3.4 Personal Information Protection in Mobile Apps 71
4.3.5 Personal Information Protection in "Internet+" 74
4.4 Summary 75

V China IoV Security – Academic Survey 76

5 China IoV Security – Academic Survey 77
5.1 Domestic Summits and Conferences in Automotive Security (2017-2020) 78
5.2 Industrial and Academic Initiatives to IoV Security Challenges (2015-2020) 80

5.3 Corp and Academic Labs: Research Highlights in IoV Security (2015-2020) 81
5.4 ICV Non-Govermental Organizations 83
5.4.1 TIIA: Telematics Industrial Application Alliance 83
5.4.2 China Industry Technology Innovation Strategic Alliance for ICV 84
5.4.3 CAICV: China Intelligent Connected Vehicle Industry Innovation Alliance 85
5.4.4 C-ITS: China Intelligent Transportation Industry 85
5.5 Gaps in IoV Security: Academic Standpoint 86

VI IoV Security and Privacy: Outlook and Trends 88

6 IoV Security and Privacy: Outlook and Trends 89
6.1 EV Charging: Trends and Gaps 89
6.1.1 EV Wireless Charging 89
6.1.2 5G and Bi-Directional Charging (V2G) 89
6.1.3 EV Charging Infrastructure Security Gaps 90
6.2 Summary: ICV Security Standards and Roadmap 90
6.3 Vehicle Personal Information and Data Compliance 91
6.3.1 Personal Information Collection Compliance 91
6.3.2 In-Vehicle Data Collection Compliance 91
6.3.3 In-Vehicle Personal Information Scope 92
6.4 Cross-Border Vehicle Data Transfer Requirements 92

VII Appendix 93

7 Appendix 94
7.1 Guidelines for National ICV Standard System 94
7.2 Relevant ICV/IoV Security Industry Standards 95
7.3 C-V2X and 5G IoV Development in China 96
7.4 Table Catalogue 97
7.4.1 Table17: List of Critical Network Equipment and Network Security Special Products (First Batch) 97
7.4.2 Table 18: Certification Catalog for Commercial Cryptographic Products (First Batch) and Certification Rules for Commercial Cryptographic Products 98
7.4.3 Table 19: Overview of Cybersecurity Standards of TC114/SC34 102
7.4.4 Table 21: Summary of SCA Cryptographic Standards (Industrial layer) 104
7.4.5 Table 22: ISO/IEC 19790 vs GM/T 0028 (Security Requirements for Cryptographic Modules) 107
7.4.6 Table 23: GM/T 008 vs FIPS-140-2 (cryptography test criteria for security IC) 110
7.5 China Security Testing Centers 110
7.5.1 CATARC -Testing and Certification Division 110
7.5.2 CCID- China Software Testing Center (CSTC) 110
7.5.3 Apollo Cybersecurity Service – Cybersecurity Test 111
7.5.4 China Tyre Laboratory - CAICT 111
7.5.5 China Intelligent and Connected Vehicles (CICV) 111

LIST OF FIGURES

Figure 1: Relevant China Gov. and Non-Gov. Authorities for Automotive Cybersecurity 21

Figure 2: NEV and ICV Cybersecurity Landscape in China 23

Figure 3: Growth and Sales of NEV's (2009-19).. 35

Figure 4: New energy vehicle safety value-chain. 36

Figure 5 Comparison of number of charging stations vs NEV's 36

Figure 6: Electric Vehicle Charging Pile Industry Chain 37

Figure 7: Automotive Cybersecurity Vehicle-Side market estimation 38

Figure 8: Automotive Cybersecurity value chain 38

Figure 9: Overview of Working Groups in TC 114 52

Figure 10: Overview of Working Groups under SAC/TC260 54

Figure 11: Overview of China Cryptography Standards System 59

Figure 12: Scenarios among apps investigated with implicit user PI collection 72

Figure 13: Proportion of different user PI stored as plaintext in 25% of investigated apps 73

Figure 14: Shanghai EV Public Data Collecting, Monitoring and Research Centre 75

Figure 15: TIAA: National Planning of IoV Industry in China 84

Figure 16: Roadmap of IoV Security 87

LIST OF TABLES

Table 1: List of Important Government Stakeholders in NEV and ICV Cybersecurity 19

Table 2: Terms of label in Figure 8 39

Table 3: Layers of Chinese Standardization 50

Table 4: Requirements for Publishing National standard 51

Table 5: TC114/SC34 NEV Cybersecurity Standards 53

Table 6: Relevant NEV cyber security standards from TC260 55

Table 7: Important CEC Series of Standards for EV charging and EV 56

Table 8: CCSA communications security standards 57

Table 9: Comparison for GM/T 0008 vs. FIPS-140-2 and GM/T 0028 vs ISO/IEC 19790 60

Table 10: Important Articles from the draft Data Security Law 64

Table 11: Data Security Standards 66

Table 12: Personal Information Protection Standards 69

Table 13: Local Summits and Conferences in Automotive Security (2015-2020) 78

Table 14: Industrial and Academic Initiatives on IoV security challenges 80

Table 15: ICV/IoV Security Industry Standards 95

Table 16: Outline of China Cybersecurity and Cryptography Law from OEM Perspective 2020 96

Table 17: List of Critical Network Equipment and Network Security Special Products (First Batch) 97

Table 18: Certification Catalog for Commercial Cryptographic Products (First Batch) and Certification Rules for Commercial Cryptographic Products 98

Table 19: Overview of Cybersecurity Standards of TC114/SC34 102

Table 20: Summary of SCA Cryptographic Standards (Industrial layer). 104

Table 22: Comparison between GM/T 0028 and ISO/IEC 19790 110

Table 23: Comparison between GM/T 0008 and FIPS-140-2 114

LIST OF ABBREVIATIONS

Abbreviation	Term
BAIC	Beijing Automotive Group Co. Ltd
CAC	Cyberspace Administration of China
CAFC	Corporate Average Fuel Consumption
CAICT	China Academy of Information and Communications Technology
CAICV	China Intelligent Networked Auto Industry Innovation Alliance
CATARC	China Automotive Technology and Research Center
CAS	Chinese Academy of Sciences
CAERI	China Automotive Engineering Research Institute
CCRC	China Cybersecurity Review and Certification Center
CCSA	China Communications Standards Association
CEC	China Electricity Council
CEL	China Encryption Law
CESA	China Electronics Standardization Association
CESI	China Electronics Standardization Institute
CII	Critical Information Infrastructure
CNCA	Certification and Accreditation Administration of China
CNCERT	National Computer Network Emergency Response Team
CQC	China Quality Certification Centre
CRAES	China Research Academy of Environmental Sciences
CSP	Critical Security Parameters
CSTC	China Software Testing (Evaluation) Center

CSL	China Cybersecurity Law
CSTC	Cryptography Standardization Technical Committee
CV	Connected Vehicle
C-V2X	Cellular Vehicle to Everything Communication
DPAC	Defective Product Administrative Center
EIC	Electronic Instrument Cluster
EV	Electric Vehicle
EIDC	Equipment Industry Development Center
FIPS	US Federal Information Processing Standards
GB	Guobiao. Mandatory National Standard in China
GB/T	Guobiao/Recommended. Recommended National Standards in China
GDPR	EU General Data Protection Regulation
GRVA	UNECE Working Party on Automated/Autonomous and Connected Vehicles
IC	Integrated Circuit
ICP	Internet Connection Provider
ICV, IoV, CAV	Intelligent Connected Vehicle, Internet of Vehicles, (ICV and IoV used interchangeably) Connected Autonomous Vehicle
IEC	International Electrotechnical Commission
IPR	Intellectual Property Rights
ISO	International Standards Organisation
IVI	In Vehicle Infotainment System
MEE	Ministry of Ecological Environment
MIIT	Ministry of Industry and Information Technology

MoT	Ministry of Transportation
MoST	Ministry of Science and Technology
MPS	Ministry of Public Security
NEA	National Energy Administration
NEA/TC3	EV Charging Infrastructure Standardization Technical Committee
NEV	New Energy Vehicle. Term used in China for vehicles not powered by an internal combustion. NEV's include pure Battery EV's (BEV) and plug-in hybrids (PHEV) Fuel Cell EV. Term "electric vehicles (EV)" is a general notion
NDRC	National Development and Reform Commission
NGO	Non-governmental organisations
NTCAS	National Technical Committee of Automotive Standardisation (Largest Technical Committee under SAC)
OBD	On Board Diagnostics
OEM	Original Equipment Management
OSCCA or SCA	Office of the State Commercial Cryptography Administration (Also known as State Cryptography Administration)
PI	Personal Information
SAC	Standardization Administration of China
SAC/TC114/SC34	SC34: Subcommittee 34 TC114: Intelligent and Connected Vehicle of National Technical Committee 114 on Road Vehicles
SAC/TC260	National Information Security Standardization Technical Committee
SAMR	State Administration for Market Regulation
SCA	State Cryptography Administration
SDLC	Software Development Life Cycle
SSP	Sensitive Security Parameters

TBT	Technical Barriers to Trade
T-BOX	Telematics BOX
TC10: IoT	Internet of Things Technical Working Committee
TEE	Trusted Executed Environment
TIAA	Telematics Industry Application Alliance
TPMS	Tire Pressure Monitoring System
V2X, V2V,V2I	Vehicle to Everything, Vehicle to Vehicle, Vehicle to Infrastructure Communication
V2G	Vehicle to Power Grid Communication
V2H	Vehicle to Smart Home
VECC	Vehicle Emission Control Center
WFOE	Wholly owned Foreign Enterprise
WTO	World Trade Organization
YD/T	Recommended communications industry standardization

Goals and key results of the survey

This survey provides a broad and comprehensive overview of automotive activities related to security and privacy of Electric Vehicles (NEV) and Connected Vehicles (ICV) in China in 2015-2020. The expected audience of this survey includes Original Equipment Manufacturers (OEMs) of NEV/ICV, technology providers, standardization organizations, researchers, and developers who are interested in the recent developments in Chinese NEV/ICV market.

Methodology

To achieve the necessary coverage, the survey was carried out in collaboration with industry and standardization automotive security experts in China and Singapore as well as Chinese academia, and included extensive research and analysis of relevant publications from government, industry and NGO agencies in China including national laws, regulations, and standards as well as academic works.

Results

The survey demonstrates that electric and connected vehicles are becoming integral part of the transportation and mobility industry in China, with market trends showing higher estimated sales growth for such vehicles and higher ratio of charging stations, including shared charging stations.

NEV/ICV security ecosystem in China is a mix of vast, multi-domains (e.g. automotive, electricity, communications), multi-agency stakeholders comprising different government ministries, agencies, NGOs, industry and trade association, as well as hardware, and software associations. MIIT is lead government ministry for development of EV industry, its development plan, industrial policy and standards in China and NEA is lead government agency for development of EV charging facilities across China.

In current phase of NEV/ICV development and deployment, Chinese government and industry are in process to establish the cybersecurity and privacy legislation framework through a variety of new regulations, standards and measures, which are often closely aligned with UN and international security standards and regulations.

The respective automotive security activities can be broadly divided into main four categories: NEV promotion and supervision, national cybersecurity strategy, ICV market development, and 5G-V2X promotion. Example measures of government NEV market promotion and incentive policies include Institutional reforms, subsidides, tax incentivies, and market access.

These activities are supported by strategic national policies such as: Made in China 2025, Internet Plus and Automotive Industry Mid and Long-Term Development Plan.

The three major influencing forces for NEV and ICV security industry are Cybersecurity and Cryptography Law to protect national security, national policy and regulation on NEV/ICV industry, and overseas market and UN type approval regulations. With respect to cybersecurity, the most important are regulations also on CII (critical information infrastructure) protecting the supply chain, on Personal Information Protection restricting the transmission of specific personal information abroad (still available as drafts, i.e., have no enforcement in China), on important data protection for, e.g., geographical maps data, and on data cross border transfer, cryptography, threats disclosure and data collection.

With respect to standardization activities, both national layer and industrial standardization layers are equally important. Industrial layer focuses on detailed technology to supplement the national layer standards, if national layer does not cover the topic. Among key NEV standardization agendas are optimization of EV standard systems till 2025, fulfillment of international responsibilities towards UNECE/WP.29, and participation in formulation of ISO/TC22 (Road Vehicles Communication) and IEC/TC69 (Electric Vehicles Communication). With respect to ICV, the key agendas are covering vehicle information interaction using LTE-V2X, requirements for vehicle information security, security early warning system, digital certificates, vehicle passwords, conversion of ISO 21434 "Road Vehicle

Information Security Engineering" and ISO 20077 "Road Vehicle Networked Vehicle Methodology" standards. It is expected that there will be around 30+ China automotive security standards until 2025. SAC/TC114/SC34 and SAC/TC260 (information protection) are government national EV security standardization technical committees that draft and publish EV security and protection standards in China and consists of the most relevant working groups for automotive security. TC114/SC34 also participates in the formulation of international standards, regulation and harmonization such as of ISO/TC22 and UNECE/WP.29. SAC/TC260 comprises standards for classified protection 2.0, personal information protection and also comprises of software WG for Big data that focuses data security and privacy.

China cryptography is administered by OSCCA (SCA), the government top cryptography administrative body, which publishes the industrial layer standards. Some of its industrial standard proposals are submitted to SAC/TC260 WG3 to upgrade to national layer standard. SAC/TC260 WG3 is the most important working group for cryptography standard development in China. SM2 (a public key cryptography algorithm like RSA), SM3 (password hash algorithm), SM4 (block cipher like DES / AES) and SM9 (identity-based cryptographic algorithm) are important Chinese cryptographic algorithms.

Trade associations CEC and CCSA are responsible for drafting of EV charging standards and communication security standards. CEC charging standards also cover charging related security aspects including charging payment security. CEC has also collaborated with Japanese fast-charging standard ChaDeMo and jointly developing charging standard Chaoji. Sometimes, relevant standard projects may get re-assigned, e.g. from TC114/SC34 to CEC, and also have the potential to become national standard. Thus it is important for those interested in China e-drive security to track such NGOs as well.

Main findings of this study are as follows:

- Deep know-how of the different stakeholders, including the national standards-making tech-nical committees, of their strengths and influences in China EV security regulation is crucial for planning and preparation of security architecture and features for NEV/ICV, e.g.,
  - TC114. A TC114 standard might not have the desired quality or its clauses could be difficult to impement, and it may remain a recommended standard (GB/T), but can become mandatory standard (GB) if a higher administrative agency or ministry like SAMR or MIIT or a mandatory standard refers it.
  - EIDC, CQC, MIIT or SAMR would be likely agencies to refer for security testing or certification or testing procedure information.
  - membership in NGOs like CEC and CCSA provides important insights into EV charging and communication security standards being drafted in China while EVICPA helps monitoring the development in Chinese charging infrastructure.
- OEMs are recommended to become acquainted with Chinese standardization process and steps, e.g., in order to be able to contribute to draft standards and to influence their development.
- EV/ICV security standardizations in China are strongly inspired by UN and international standards, i.e., many Chinese standards are expected to be a conversion, extensions or a complete adaptation of existing international standards such as ISO 21434.
- there appears to be a gap in security best practices or guidelines for China's EV infrastructure or secure communication between EV and charging infrastructure or infrastructure security testing, due to lack of such information available publicly.
- in quite a few regulations regarding EV security and privacy in China, e.g., clauses in security laws are not clearly defined or their interpretation is uncertain, even among experts; thus, in many cases a dedicated legal support is advisable, especially, for OEMs.
- China Cryptography Law is likely to be applicable to NEV/ICV in some of the following ways:

- EV charging infrastructure will likely be classified as Critical Information Infrastructure (CII) and covered by TC260 standards Classified Protection v2.0.
- if a backend system is required to connect to a Chinese government backend, it might need to use Chinese crypto algorithms SM2, SM3, SM4.

Structure

- Results of the study are structured in seven chapters including an appendix covering additional information. Chapter 1 describes the relevant government and non-government stakeholders that address NEV/ICV security administrative regulations, policy, standards, technology and product development, testing, certification, cryptography, and market access activities in China. Chapter 2 chronologically lists national cybersecurity, policy and market-driven activities in China that impact automotive security and specifically NEV security ecosystem and reviews ICV security standardization framework activities. Chapter 3 provides information on China Cybersecurity Law (2017), Cybersecurity Review measures (June 2020) and China Cryptography Law (2019), lists national NEV and ICV security standards and ongoing projects in China. Industry security standards from important associations such as CEC and CCSA are also listed in the Chapter together with an overview of China Cryptographic standards and products. Chapter 4 looks into data security and privacy laws and regulations in China, in particular, the recently introduced Data Security and Personal Information Protection Law.

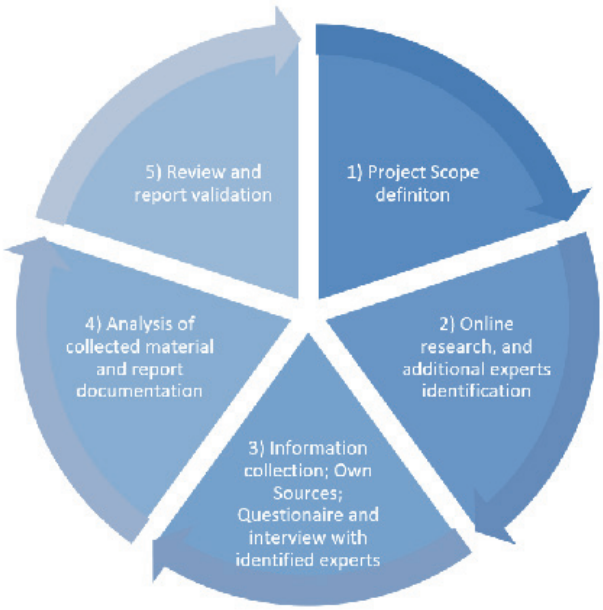
  Chapter 5 presents academic survey on internet of vehicle (IoV) security in China that covers domestic summits and conferences on automotive security, industrial and academic initiatives, ICV non-governmental organizations as well as corp. and academic labs focusing on IoV security research. In addition, this chapter highlights gaps in IoV security from academic standpoint. Chapter 6 presents IoV security outlook and trends such as wireless charging and bidirectional charging (V2G) for EV, 5G and ICS security standard roadmap. Furthermore, requirements concerning vehicle personal information and data compliance, in-vehicle personal information scope and cross-border vehicle data transfer requirements are discussed in Chapter 6. Chapter 7 is an appendix that provides detailed information on cybersecurity and cryptographic standards and products in China, offers comparison to international standards ISO/IEC 19790 and FIPS-140-2 and lists China Security Testing Centers.

1 Introduction

1 Introduction

The main objective of this work is to conduct a survey on automotive security activities in China over last 5 years and develop a report on specific information related to Electric Vehicles (EV) and Connected Vehicles (CV) Security and Privacy in China.

1.1 Survey Methodology



1. **Project scope definition:** establishing the scope of the project and identifying the main topics, and structure of the report, important topics and depth to be considered during the study.
2. **Online research and optional experts' identification:** extensive research of relevant documents to gather as much information as possible about EV/CV security and privacy related activities in China. If beneficial, additional experts will be also identified and invited to validate scope and provide feedback.
3. **Information collection on own sources and interviews with identified experts:** Fraunhofer interviews the identified experts in order to get their point of view and additional public information.
4. **Analysis of collected material and report development:** collected information from own sources, online research and from the identified experts is analysed and a draft report is developed.
5. **Review and report validation:** Fraunhofer shares the draft for expert review. Considering the feedback, the proposed final version of the report is issued.

1.2 Project Team and Collaborators

Fraunhofer Singapore

1. Jianzhong Huang (Expert, Industry & Standardization China)
2. Sanat Sarda (Senior Cybersecurity Researcher, Singapore)
3. Michael Kasper (Project Manager, Singapore)

Tongji Automotive University, Shanghai

4. Professor Bi Xin (Automotive Expert, Academic Sector, China)

Industry Expert, China

5. Wang Yi Estelle (Expert, Industry and Standardization, China)

Fraunhofer SIT, Germany

6. Maria Zhdanova (Cybersecurity Researcher, Germany)
7. Prof. Dr. Christoph Krauß (Project Manager, Germany)

1.3 Report Structure

Chapter 2 gives a background of electric vehicle and connected vehicle industry in China from policy and market perspectives and its influence and impact on its security landscape. Chapter 3 covers the various electric vehicle and connected vehicle cybersecurity and cryptography laws and standards in China. Chapter 4 looks into data security and privacy laws and regulations. Chapter 5 presents academic survey on internet of vehicle security in China. Chapter 6 presents internet of vehicle security outlook and trends. Section 7 is an appendix that provides detailed information of cybersecurity and cryptography products, list of cybersecurity testing companies, and connected vehicle and V2X standards development in China.

1.4 Background Information

EV are becoming integral part of the transportation and mobility industry in China. The EV environment in China is a mix of multiple stakeholders (government ministries, agencies, NGOs, industry), domains (automotive, electricity, communications), hardware, and software. In addition to the vulnerabilities present in conventional vehicle, EVs present unique cybersecurity vulnerabilities because of their connections to other infrastructure and communication systems. Conventional vehicles are prone to malicious cyber-attacks, vulnerabilities due to increased connectivity - telematics, V2X, keyless entry, unauthorized access to internal CAN networks and so forth. However, EV additionally connect and exchange information with EV charging stations, which in turn are connected to power grid, and have the ability to cause disruptions across multiple sectors if compromised. In present phase of EV development and deployment, Chinese government and industry are in process to address cybersecurity, privacy and data security regulatory framework for EV, EV infrastructure and for connected vehicles with slew of laws, regulations, standards and measures in tandem with UN and other international security regulations. This framework appears to be nascent and evolving, while China continues to release guidelines improving vehicle cybersecurity and encourages industry to adopt practices that improve security posture of vehicles.

1.5 Important Government Stakeholders

Table 1 puts together a list of the important administrative bodies, ministries and agencies responsible and those that specifically address cybersecurity for NEV's and ICVs in China cybersecurity framework. The organisation labelled in light blue come under the umbrella of organisation in dark blue on the left. Important NGO's are represented in brown.

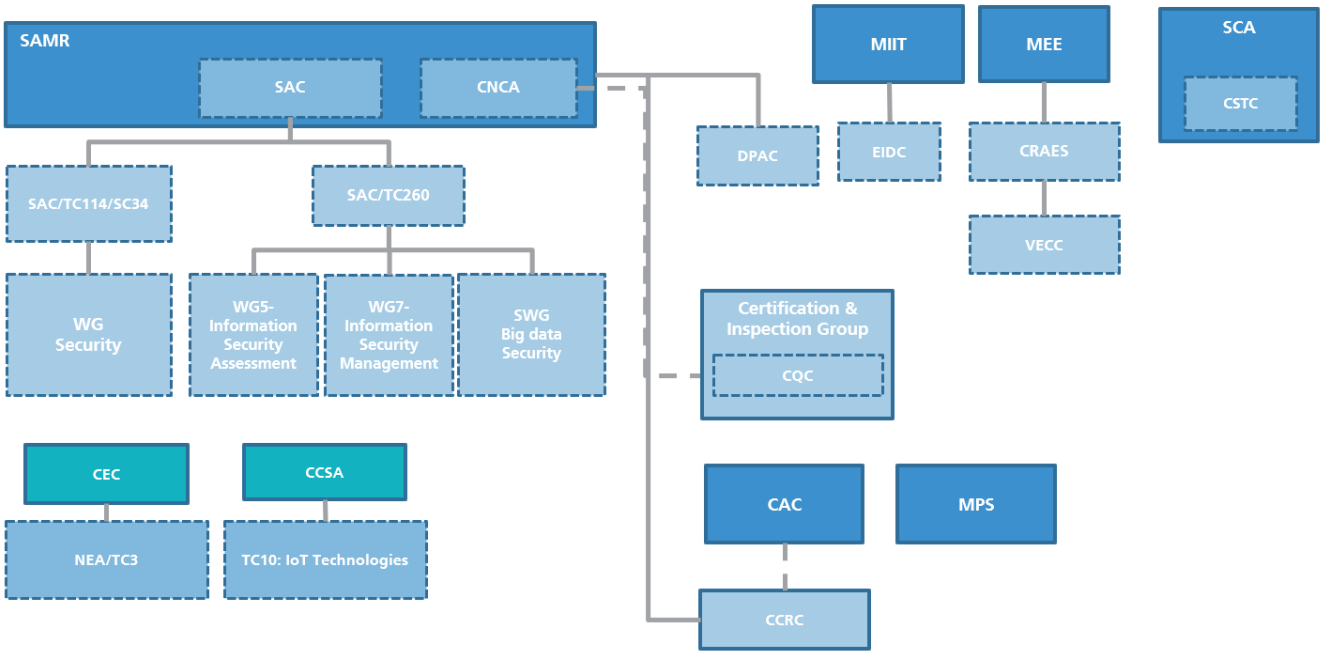
Table 1: List of Important Government Stakeholders in NEV and ICV Cybersecurity

Abbreviation	Term	Abbreviation	Term
CAC	Cyberspace Administration of China	CCRC	China Cybersecurity Review and Certification Center
MPA	Ministry of Public Security		
SCA	State Cryptography Administration	CSTC	Cryptography Standardization Technical Committee
MEE	Ministry of Ecological Environment	CRAES	China Research Academy of Environmental Sciences
		VECC	Vehicle Emission Control Center
MIIT	Ministry of Industry and Information Technology	EIDC	Equipment Industry Development Center

Abbreviation	Term	Abbreviation	Term
SAMR	State Administration for Market Regulation	SAC	Standardization Administration of China
		CNCA	Certification and Accreditation Administration of China
SAC	Standardization Administration of China	SAC/TC114/ SC34	SC34: Subcommittee 34 TC114: Intelligent and Connected Vehicle of National Technical Committee 114 on Road Vehicles
			WG Security: Automotive Information Security Standard work group
		SAC/TC260	National Information Security Standardization Technical Committee
			WG5: Info Security Assessment working group
			WG 7: Info Security Management working group
			SWG: Big Data Security standards task force
CNCA	Certification and Accreditation Administration of China	DPAC	Defective Product Administrative Center
		CCRC	China Cybersecurity Review and Certification Center
		CQC	China Quality Certification Centre
CEC	China Electricity Council	NEA/TC3	EV Charging Infrastructure Standardization Technical Committee
CCSA	China Communications Standards Association	TC10: IoT	Internet of Things Technical Working Committee
Other Important NGO's			
CATARC	China Automotive Technology and Research Center		
CAICT	China Academy of Information and Communications Technology		
CAICV	China Intelligent Networked Auto Industry Innovation Alliance		
TIAA	Telematics Industry Application Alliance		
CESI	China Electronics Standardization Institute		

Most of the above mentioned parent and subordinate bodies also address the larger automotive cybersecurity activities. Names of these organisations broadly hint on their role and activities. Briefly CAC, SCA, MPS, MIIT, MEE, SAMR are the primary bodies, and broadly speaking at a similar level of administrative authority in China. CAC is headed by the Chinese President and among the highest administrative bodies in cybersecurity in China. MPS is responsible for cybersecurity oversight and setting policies. MIIT is the main ministry responsible and leads EV development in China. Its covers EV policy, standardization, technology and product development including complete vehicle testing. MEE and its sub-ordinate bodies, as shown in Figure 1, are responsible for environmental protection laws and vehicle emission regulations. SCA overseas China cryptography laws and standards. SAMR covers security standardization. CNCA coordinates certification, testing, quality and defect vehicles. CQC, subordinate body of CNCA, is responsible for quality and can be considered similar to Germany's, TUV SUD. DPAC, another subordinate of CNCA, overseas vehicle recalls and defect vehicles. SAC/TC114/SC34 and SAC/TC260 look after critical and important security standards development for NEV and ICV. CEC and CCSA are important NGO's. CEC is responsible for some of the EV charging infrastructure security standards and regulations. Further detailed information on each of these organizations' activities and structure is provided on their respective websites. Following is pictorial representation that provides some of broader interconnections between these bodies.

Figure 1: Relevant China Gov. and Non-Gov. Authorities for Automotive Cybersecurity



II NEV and ICV Industry in China: Policy-Driven and Market-Driven

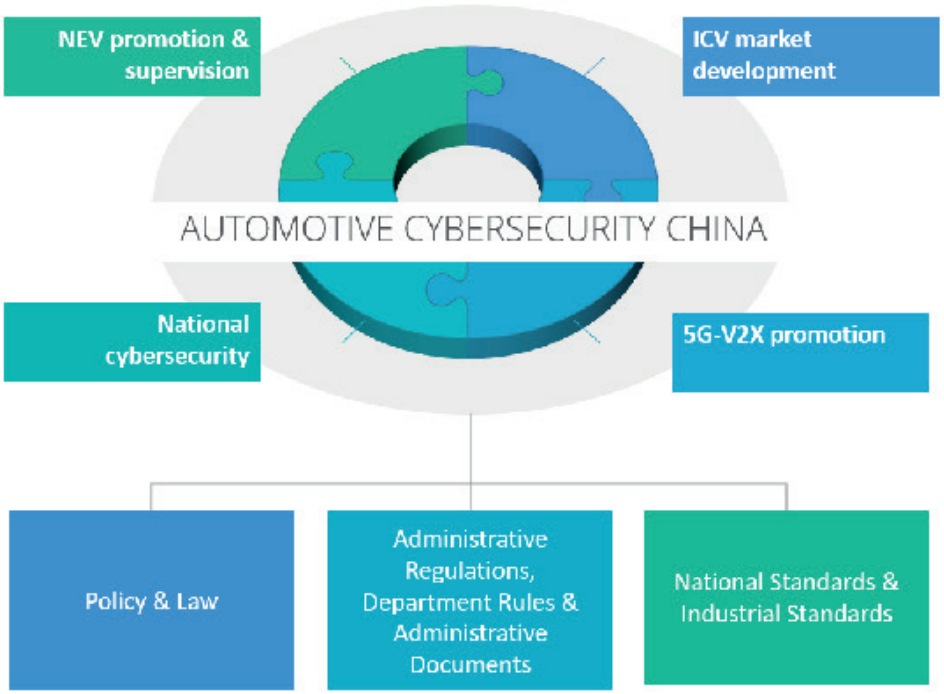
2 NEV and ICV Industry in China: Policy-Driven and Market-Driven

This section provides information about the NEV and ICV security industry, governmental policy and market driven activities in China, broadly from 2015 -2020. It chronologically covers EV security landscape, important government stakeholders, EV, EV charging infrastructure and ICV development strategies, security market, value chains, governmental strategic invests towards EV and EV charging infrastructure.

2.1 Landscape of NEVs and ICVs Cybersecurity in China (2020)

To acquaint with NEV and ICV cybersecurity landscape in China, we identify specific group of activities, that directly and indirectly, encompass EV and ICV security industry in China. Figure 2 presents the high-level overview of these activities.

Figure 2: NEV and ICV Cybersecurity Landscape in China



Activities are broadly divided in four categories; **NEV Promotion & Supervision** – As early as 2009, China has been running multiple initiatives for development of NEV technology, growth and its market adoption at scale. **National Cybersecurity** – Since 2015, China has been continually strengthening and introduced overarching national security laws, policies, standards for state's assets, critical industries and infrastructure, data and personal information security. **ICV market development** – refers to the increasing activities of development of ICV technology, standards and regulations. **5G-V2X promotion** – In recent years, 5G, V2X and development of its related applications are given high priority.

These activities are led by various national administrative bodies, ministries, agencies, in consultation with members from local, foreign OEMs, local and international automotive consortiums, NGO's, related national infrastructure governing bodies and automotive regulatory bodies. The activities, broadly, lead to three different directions: 1) development of security strategy, laws and policies 2) development of administrative regulations, department rules and measures, administrative documents and 3) development of national and industry standards.

The following sections look into each of these activities and directions that have shaped security ecosystem of NEV, in particular, and ICV industry in China, in the past years.

2.2 National High-Level Policies (2015-2017)

There are 3 **strategic industry development** national policies that are not only concerned with China's economy but also to its evolving automotive cybersecurity industry.

I. **Made in China 2025 (May 2015)[1]:** Manufacturing is central to Chinese economy. "Made in China 2025" is national strategic industry development plan to develop China into advanced manufacturing nation. Broadly, the plan aims for transition of China's large manufacturing industry from developing low value goods towards high tech value products and services, in aerospace, semiconductors, biotech, etc., banking on its relatively low labour costs and supply chain advantages. The plan provides the blueprint to upgrade its manufacturing capabilities from labour-intensive to more technology-intensive, competitive manufacturing and close gaps in its innovation capability, industrial structure, informatization, quality and efficiency. Green Energy and **Green Vehicle** is one of the key industry sectors mentioned in the plan. Past growth of China's NEV industry, highlights determination of achievement of its goals set in Made in China 2025[2].

II. **Internet Plus (July 2015)[3]:** Internet is a central backbone and integral to China's current and future phases of economic and social development. The "Internet Plus" plan aims at achieving rapid, high-quality economic growth and industry development, through deeper and comprehensive integration between Internet and the real economy, leveraging China's already developed large scale internet infrastructure and applications. Plan includes general requirements, targets, detailed action plans, and supportive policies. Plan outlines eleven key actions: 1) entrepreneurship and innovation 2) collaborative manufacturing 3) modern agriculture 4) smart energy 5) inclusive finance 6) public services 7) efficient logistics 8) e-commerce 9) convenient transportation 10) green ecology 11) artificial intelligence.

In addition, it includes 25 relevant supportive measures. Measures are divided in five categories, as below:

1. Policy Environment: Eliminate unreasonable mechanisms and policies, ease market access of web-integrated products and services, promote entrepreneurship and innovation.

2. New-Generation Information Infrastructure Development: Accelerate R&D of new hardware engineering, such as chips and high-end servers, as well as applications of cloud computing, big data.

3. Public Resources Sharing: Enhance public services and start pilot programs for public access to government data, encourage traditional small and medium enterprises online access to national innovation platforms.

4. Business Operation Support: Increase government procurement of cloud services, innovate credit products and services, pilot equity crowdfunding.

5. Safety Regulations: Improve risk assessment, safeguard network and information security, and protect fair competition.

1 Notice of the State Council on Printing and Distributing Made in China 2025 Plan - May 2015

2 How China's manufacturing rises from the perspective of NEVs - Jun 2015

3 Guiding Opinions of the State Council on Actively Promoting the Internet + Plan - July 2015

A total of 65 comprehensive development tasks are specified and plan is stated to complete in line with Made in China 2025 plan.

III. Automotive Industry Mid and Long-Term Development Plan (Apr 2017)[4]: The plan is to promote development of the Chinese automobile industry in the next phase and to be in-line with China manufacturing strategy of Made in China 2025. Plan envisions China to become a top automobile manufacturing country in ten years. In particular, to have several Chinese companies in world's top ten **electric vehicles** companies, top ten automobile sellers and automobile parts companies by 2025. Plan designates the **NEV, ICV**, and energy-saving automobile as key areas to develop. As supportive measures, plan calls on industrial investment funds, automobile industry funds, science and technology funds to support automobile projects, calls to both policy and commercial banks to increase financial support to key development areas and support Chinese automobile companies to explore foreign markets.

2.3 National Cybersecurity Activities (2015-2020)

The China Cybersecurity Law (June 2017) and China Cryptography Law (January 2020) are the most important security laws. There is also an upcoming China Data Security Law (anticipated in 2021). Requirements of the Cybersecurity Law are the most important for NEV and ICV industry, including NEV and ICV backend/ infrastructure security. However, requirements of the law in some context or cases relevant to the NEV sector don't provide clear interpretations. Detailed product management rules (like for NEV products) are expected to be published in next years that may clear ambiguities. For example, for those products listed in the first batch of commercial encryption products of 2017 or critical network equipment and network security special product batch of 2017, may have its administrative rules published soon.

The following are the various national cybersecurity activities undertaken in past five years in chronological order. Broadly, the activities are classified as either reform, law or regulation and further sub-classified as per the security area it addresses. Some items are also provided with keywords that highlight its important notions. Each item below is provided with descriptive color labels. Brown label refer to the classified activity and blue refer to their sub-classifications. Each item is provided with reference/s, in case, further information is required.

INSTITUTIONAL REFORM | CYBER SECURITY

Jul 2015, Cyber and Information Security coordination responsibility assigned to CAC (Cyberspace administration of China) on state level[5]. CAC is one of the premier central governing body of China, headed by the Chinese President.

REGULATION | DATA SECURITY | INFRASTRUCTURE

Dec 2015, Regulations on the administration of maps[6].
Keywords: market access

4 "Medium and Long-Term Development Plan for the Automotive Industry" – Apr 2017 [Last Visited:05/07/2021]; Summary: Medium and Long-term Development Plan for the Automobile Industry - April 2017

5 Relevant Duties and Institutional Adjustment of the MIIT - July 2015 [Last Visited:05/07/2021]

6 Regulations on the administration of maps - Dec 2015

LAW | OVERALL CYBER SECURITY | PRIVACY

Nov 2016 , **China's Cybersecurity Law**[7]: The uppermost law for all cyber security laws/regulations, 3 key concepts, 1) Critical information infrastructure 2) Personal information protection 3) Important data protection

REGULATION | CII SECURITY | INFRASTRUCTURE

July 2017, Provision on Critical Information Infrastructure (CII) Protection[8] (Draft).

REGULATION | DATA SECURITY

May 2019, Data Security Management Measures[9] (Draft).

REGULATION | PRIVACY

Jun 2019, Personal Information Outbound Transfer Security Assessment Measures[10] (Draft)
Keywords: cross border, personal information.

LAW | CRYPTOGRAPHY

Oct 2019, **Cryptography Law of China**[11],[12] : Basis for making commercial cryptography regulations in the future. Law classifies cryptography into 3 levels: core, general and commercial cryptography. Core and general cryptography regarded as national secrets, and controlled strictly and uniformly, while commercial cryptography is to protect information that is not a national secret
Keywords: core, general and commercial cryptography.

REGULATION | INFORMATION SHARING

Nov 2019, Administration Measures for Disclosure of Cybersecurity Threats Information[13] (Draft)
Keywords: threat intelligence, information disclosure

REGULATION | PRIVACY

Nov 2019, **First regulation that provides methods to identify illegal collection of personal information (PI) via apps** (applications)[14]
Keywords: personal information collection, violation, methods.

REGULATION | CII SECURITY | INFRASTRUCTURE

7 China's Cybersecurity Law - Nov 2016
8 Provision on CII Protection (Draft for Comment) - Jul 2017
9 Notice on Measure of Data Security Administration (Draft for Comment) - May 2019
10 Measures for the Assessment of Personal Information Outbound Transfer Security (Draft for Comment) - Jun 2019
11 Cryptography Law of China - Oct 2019
12 Interpretation of the "Cryptography Law of China" - Oct 2019
13 Notice on Measure on Administration of the Disclosure of Cybersecurity Threats Information (Draft for Comment) - Nov 2019
14 Notice regarding the issuance of the "Measure on Verdict of APP Illegal Collection and Use of Personal Information - Dec 2019

REGULATION | CII SECURITY | INFRASTRUCTURE

Apr 2020, **Cybersecurity Inspection Measures**[15],[16] . Mainly focusing on **CII** (critical information infrastructure) **supply chain security**. Defined CII operator as the subject being inspected by the government.
Keywords: supply chain security, CII operator, security inspection.

2.4 NEV Policy and Market Driven Activities (2009-2020)

There have been numerous NEV and EV Infrastructure related promotion and supervision activities in China in the past decade that have subsequently effected the NEV security industry. Broadly, we classify these activities into institutional reforms, subsidies, tax incentives, industry development, market access and standardization.

2.4.1 Institutional Reform (2010)

Historically, China started with issuing many guidelines and planning for development of electric vehicles. The 'Automotive Industry Adjustment and Revitalization Plan' of 2009, post financial crisis, suggested NEV as a breakthrough point and set goals to develop its ecosystem. The 'Fostering and Development of Strategic Emerging Industries Plan' of 2010, passed resolution to accelerate development of NEV industry. Shortly, an institutional reform was issued to streamline NEV and EV infrastructure development activities.

INSTITUTIONAL REFORM | EV INFRASTRUCTURE

Dec 2010, Clarification of division of responsibilities of management of electric vehicles and charging facilities[17]. **Clarified that NEA is responsible for EV charging infrastructure** as the government authority.
Keywords: clarification, division of responsibilities.

The reform clarified division of responsibilities among various government bodies:

1. MIIT was assigned to lead development of the EV industry, drafting the development plan, industrial policy and related standards.
2. NEA was made responsible for development of EV charging facilities and lead in formulating its development plans and policies and linking them with the national energy plan.
3. The General Administration of Quality Supervision, Inspection and Quarantine (National Standards Commission) was assigned to lead in formulation of national standards and regulations for electric vehicles and charging facilities.

15 Cybersecurity Inspection Measures - Apr 2020 [Last Visited:05/07/2021]
(Interpretation) http://www.cac.gov.cn/2020-05/03/c_1590051734208776.htm

16 Interpretation "Cyber Security Review Measures" - May 2020

17 Division of responsibilities for management of electric vehicles and charging facilities - Dec 2010

2.4.2 Subsidies (2009-2016)

China began to subsidize new energy vehicles in 2009 and initiated programs from a few pilot cities to promote purchase of non-private and later private electric vehicles. The subsidy programs were revised frequently to tighten the technical requirements for qualifying vehicles towards high-performance and long range EV, and subsequently the programs were phased down as the technologies matured and adoption increased.

Central subsidies given to city governments that met certain requirements, were passed down from the cities to vehicle manufacturers and users. The magnitude of the central subsidies had a direct impact on local subsidies, as many pilot cities provided a matching local subsidy.

Below are selected activities related to NEV and EV infrastructure subsidy.

SUBSIDY | NEV | PROMOTION

- Jan 2009, Launch of national NEV subsidy program, began with 13 pilot cities, covering non-private NEVs[18].
  Keywords: pilot, non-private purchase

- Jun 2010, Added more cities, 20 pilot cities totally[19]
  Keywords: pilot, non-private purchase

- Jun 2010, The national NEV subsidy program expanded to include private NEV, and began with 5 pilot cities. Defined the scope of NEVs as Pure Electric and Plug-in Hybrid[20]
  Keywords: pilot, private purchase

- Sep 2013, Notice to continue promotion and application of NEV until 2015 to accelerate development[21]

SUBSIDY | NEV | ANTI – FRAUD ADMONISHMENT

- Nov 2016, **GB/T 32960** (Technical Specification for Electric Vehicle Remote Service and Management System) mentioned first time, required qualified NEVs in the field to upload real-time monitoring data to the government's backend[22]
  Keywords: monitoring platform, adoption of standard, anti-fraud.

- Dec 2016, Severely punish the fraudulent acts of new energy vehicles, standardize the order of industrial development[23]
  Keywords: anti-fraud, admonishment

18 Notice on launch the pilot program of demonstration and promotion of energy saving and new energy vehicles - Jan 2009

19 Notice on expanding the work related to the demonstration and promotion of energy saving and new energy vehicles in the public service field - Jun 2010

20 Notice on launching the pilot program of subsidies for private purchase of new energy vehicles - Jun 2010

21 Notice on continuing to promote and apply new energy vehicles - Sep 2013

22 Notice of the MIIT in the Safety Supervision of the Promotion and Application of NEV - Nov 2016 [Last Visited:05/07/2021]

23 Punish the fraudulent acts and standardize the order of industrial development, Dec 2016 [Last Visited:05/07/2021]
https://www.reuters.com/article/china-green-enr-auto-subsidiary-penalty-idCNKBS14A09S

SUBSIDY | EV INFRASTRUCTURE | PROMOTION

- Jan 2016, Released the 13th Five-Year NEV Charging Infrastructure Reward Policy to continue to accelerate development of EV infrastructure and strengthen promotion and application of new energy vehicles[24]

2.4.3 Tax Incentives (2012-2014)

Wide range of consumer incentives were adopted by city governments to stimulate purchase and use of electric cars. Broadly, there were about ten direct tax incentives and four indirect incentives. Direct incentives offered a direct monetary value that reduced cost of electric vehicle during purchase, ownership, and use. The ten direct incentives included waiving of new vehicle purchase tax, annual tax incentive, parking fee incentive, license plate fee waiver, charging fee reduction, vehicle usage subsidy, vehicle replacement subsidy, insurance incentive, home charger subsidy, and road toll incentive. Indirect incentives offered benefits that impacted daily vehicle operation not available to conventional car owners like public charger availability, dedicated parking spaces, vehicle registration, and road access privileges.

Select tax incentive notices:

TAX INCENTIVE | NEV

- Mar 2012, First NEV tax incentive policy published[25].
  Keywords: Vehicle and ship tax reduction

- Aug 2014, Exemption on purchase tax on new energy vehicles. Catalogue of qualified duty-free NEV models was released[26]
  Keywords: vehicle purchase tax exemption

2.4.4 Industrial Development (2012-2020)

Series of industrial development policies for NEV's and EV charging infrastructure were released to build strong industrial value chain.

Following are select policies for NEV's:

INDUSTRY DEVELOPMENT | NEV | MID-TERM PLAN

- Jun 2012, Development Plans (2012-2020): **Provided definition of NEV**, which only include electric, plug-in hybrid and fuel cell vehicles[27].

24 Notice on the "13th Five-Year" New Energy Vehicle Charging Infrastructure - Jan 2016

25 Notice on Energy Saving and Use of New Energy Vehicle and Ship Tax Policy - Mar 2012

26 Announcement on exemption from purchase tax on new energy vehicles - Aug 2014

27 Notice of the State Council on Printing and Distributing Energy Saving and New Energy Vehicle Industry Development Plans - Jun 2012

INDUSTRY DEVELOPMENT | NEV | PROMOTION

- Jul 2014, Guidelines on accelerating promotion and application of New Energy Vehicles[28], [29]

INDUSTRY DEVELOPMENT | NEV | LONG-TERM PLAN

- April 2020, New Energy Vehicle Industry Development Plan (2021-2035)[30]
  Keywords: 2021-2035

Following are select development policies for EV Infrastructure:

INDUSTRY DEVELOPMENT | EV INFRASTRUCTURE | PROMOTION

- Sept 2015, Guiding Opinions issued on accelerating development of Electric Vehicle Charging Infrastructure by State Council (2015-2020)[31],[32]

- Oct 2015, Guidelines released by NDRC on development of Electric Vehicle Charging Infrastructure (2015-2020)[33]

Guidelines by NDRC were the first of its kind that clearly established goals for national and regional electric charging infrastructure layout. Earlier, due to lack of such guidelines, city governments couldn't ensure building adequate electric charging infrastructure nor qualify for central subsidies. Its planning too was up to local officials and local equipment providers. As per the guidelines, China has set to build national fast charging network along three vertical (north-south) and three horizontal (east-west) corridors, with an addition of 800 intercity fast-charging stations.

2.4.5 Market Access (2017-2020)

The "Market Access Regulations" are prepared keeping in tandem with factors like changes in domestic and international situation, needs of China's NEV industry, entry barriers, market vitality, extent of high quality development in China. Following are select policies and measures of market access in NEV:

MARKET ACCESS | NEV | TYPE APPROVAL

- Jan 2017, New Energy Vehicle Manufacturing Enterprise and Product Access Management Provisions[34]. **Department rule for NEV type approval**

28 Guidelines on Accelerating the Promotion and Application of New Energy Vehicles - Jul 2014
29 Guidance on accelerating the promotion of new energy vehicles - Jul 2014
30 New Energy Automobile Industry Development Plan (2021-2035) - Apr 2020 [Last Visited:05/07/2021]
31 Opinions by State Council on Accelerating the Construction of Electric Vehicle Charging Infrastructure - Sep 2015
32 Interpretation of Opinions on Accelerating the Construction of Electric Vehicle Charging Infrastructure - Sep 2015
33 Guidelines of NDRC on Accelerating Construction of EV Charging Infrastructure - Oct 2015 [Last Visited:05/07/2021]
34 Regulations on NEV Manufacturing Enterprise and Product Access Management Provision - Jan 2017 [Last Visited:05/07/2021]

- Aug 2020, Released revised version of the 2017 'New Energy Vehicle Manufacturing Enterprise and Product Access Management Provisions'. Department rule for NEV type approval.

The 2020 version revised some clauses compared to 2017, the two main ones are:

4. The "Administrative Regulations" have deleted "design and development capabilities" requirements for applying for the entry of new energy vehicle manufacturers.

4. The "Administrative Regulations" adjusted the upper limit time for new energy vehicle manufacturers to stop production from 12 months to 24 months. The new policy was formally implemented in 2020.

MARKET ACCESS | NEV | CAFA

- Sep 2017, Measures for Parallel Management of Average Fuel Consumption of Passenger Car Enterprises and New Energy Vehicle Points Also known as "CAFC" regulation[35]

- Sep 2019, Released revised Measures of 2017 CAFA regulation (draft)[36]

2.4.6 EV Infrastructure Standardization Activities (2015-2020)

In this sub-section, select standardization activities of EV infrastructure are briefly described.

STANDARDIZATION | EV INFRASTRUCTURE

- Nov 2015, Listed standardization projects of charging infrastructure[37],[38]

- Dec 2015, Unveil **first batch of GB/T** recommended standards for **charging equipment**[39],[40]
  Keywords: standard release

- Jan 2016, **Enforced the first batch of GB/T charging equipment** standards by administrative document.
  Keywords: adoption of standard

35 Average fuel consumption of passenger car companies and new energy measures for the Parallel Management of Automobile Points-Sep 2017

36 Measures for Parallel Management of Average Fuel Consumption of Passenger Car Companies and New Energy Vehicle Credits (Draft) - Nov 2019 [Last Visited:05/07/2021]

37 Notice of the National Energy Administration on Printing and Distributing the "Electric Vehicle Charging Facilities Standard System Project Form (2015 Edition)"

38 List of Energy Industry Standardization Technical Committees

39 Announcement of the National Standards Committee on the approval of the release of 5 national standards including "Electric Vehicle Conductive Charging System Part 1: General Requirements

40 National Development and Reform Commission [Last Visited:05/07/2021]

- Apr 2020, **Revision plan of GB/T standard for charging equipment**, and drafting task **assigned to CEC instead of SAC/TC114**[41]
  Keywords: Standard revision plan, charging equipment

- May 2020, Released **national standard of wireless charging system for EV**. It's based on "**WiTricity**"[42]
  Keywords: Standard release, wireless charging

Below highlighted are key directions set out for standardization work in new energy vehicles in 2020[43].

1. To continue to optimize NEV standard systems for next five years

2. Develop, strengthen, evaluate key standards for EV's, charging and battery swapping

3. Fulfill responsibilities towards WP.29, participate in formulation of international standards of ISO/TC22 (Road Vehicles Comm.) and IEC/TC69 (Electric Vehicles Comm.)

2.4.7 Government Spending

1. Electric Vehicles
   From 2009 to 2017, the direct investment of central and local governments in the new energy vehicle industry exceeded 320 billion yuan. Among them, 245 billion yuan was used to issue new energy vehicle subsidies, and the remaining part is mainly used for government procurement, scientific research investment and infrastructure subsidies. From 2009 to 2017, the purchase tax reduction for new energy vehicles was about 70 billion yuan. Additionally, China invested more than 390 billion yuan, accounting for about 42.4% of the total domestic new energy vehicle sales during the same period.

2. EV Charging Infrastructure
   In 2015, 18 cities provided subsidies to EV public charging infrastructure to improve local charging infrastructure networks, including Shenzhen, Hangzhou, Wuhu, Lanzhou, Linyi, Haikou, Huzhou, Yichun, Ningbo, Nanchang, Chongqing, Xiamen, Taiyuan, Nanjing, Shijiazhuang, Hefei, and Nantong. Most cities offered subsidies for a percentage of the cost of the charging stations. For example, Lanzhou subsidized 5% of the total investment in the charging stations; Wuhu subsidized 20%, with the cost of each charging station not exceeding 1 million yuan; Shenzhen subsidized 30% of the total infrastructure cost. Nanjing subsidized cost proportional to power capacity: 800 yuan/kW for AC chargers and 1,200 yuan/kW for DC chargers. Linyi also had unique incentives where it subsidized the cost of the land used for charging infrastructure at 50,000 yuan/ mu (1 mu ≈ 0.067 hectares).

3. Shared-Mobility with EV
   In 2015, Ministry of Science and Technology, funded four local pilot electric car-sharing programs in Hangzhou, Beijing, Shanghai, and Shenzhen, with 30–50 million yuan for each city

41 Notice of the CEC on forwarding SAC's revision plans (2020)

42 Notice regarding the issuance of the "Implementation Plan for the New National Standard for the Interface of Electric Vehicle Charging Infrastructure", Jan 2016
Commercialization & global interoperability

43 Key points of new energy vehicle standardization work -APR 2020 [Last Visited:05/07/2021]

2.5 ICV Policy-Driven Activities (2017-2020)

The prosperity of the Internet industry and dynamic communication industry in China has laid a solid foundation for the development of ICV industry. China has set path for development of its industrial ecosystem. There is evolving development in its infrastructure, standards, technologies alongside autonomous driving.

2.5.1 Standardisation (2017-2020)

Selected notices as follows:

STANDARDIZATION | ICV | FRAMEWORK

- Dec 2017, Issued Guide for the development of National Standardization System for Networked Vehicles[44] (Intelligent Connected Vehicle)"
- Jun 2018, Released 3 subsequent documents to the Guide for the National Standardization System of Intelligent Connected Vehicle"[45] 1) General Requirements, 2) Information and Communication and 3) Electronic Products and Services
- Apr 2020, Released Guide for the development of the National Standardization System of Intelligent Connected Vehicle"[46] (Intelligent Vehicle Management)"

Further details on the five guidelines for the development of ICV standard system are mentioned in Appendix Section 7.1.

REGULATION | ICV

- Jan 2020, Amending the "Interim Measures for the Management of Online Booking and Rental Car Service"[47] Keywords: Mobility sharing, Operation, Administration

The first phase of the development of ICV standard system was ready in 2020. Following are highlighted key points that include security perspectives within standardization work of ICV in 2020[48].

1. Accelerate standards development for ICV general requirements and information security standards.
2. Complete review and approval of standards for vehicle information interaction system based on LTE-V2X direct communication, general technical requirements for vehicle information security, vehicle information interaction system information security; Complete pre-research of standards for the security early warning system based on networked communications, and begin research on key information security standards requirements such as digital certificates of ICV and vehicle passwords;
3. Carry out conversion work of ISO 21434 "Road Vehicle Information Security Engineering" and ISO 20077 "Road

44 Guidelines for the Construction of the National Vehicle Networking Industry Standard System (ICV) [Last Visited:05/07/2021]

45 Guidelines for the Construction of the National Vehicle Networking Industry Standard System (General requirement) [Last Visited:05/07/2021]

46 National Vehicle Networking Industry Standard System Construction guide [Last Visited:05/07/2021]

47 Interim Measures for the Administration of Online Taxi Booking Operation Service

48 Key points of standardization of intelligent and connected vehicles Apr 2020 [Last Visited:05/07/2021]

Vehicle Networked Vehicle Methodology" series of international standards.

In Appendix Section 7.2, a set of few ICV and IoV industry standards (published or in-draft) in wireless communication security, data security, in-vehicle application security and user privacy are mentioned.

2.5.2 Industrial Development (2020)

The "Intelligent Vehicle Innovation Development Strategy" was released in early 2020 and is considered as important a strategy as "Made in China 2025". No special high-level organization has been established yet to lead development of intelligent vehicles. For innovation and development of ICV, the strategy emphasizes against advancing alone or creating new approach, but to integrate and develop with other industries such as **new energy vehicles** and smart transportation. For 2025, strategy sets intelligent vehicles with conditional autonomous driving to reach mass production, and those that realize highly autonomous driving to be marketed in specific environments.

Selected notice is as follows:

INDUSTRY DEVELOPMENT | LONG-TERM PLAN | ICV

Feb 2020, Released "ICV Innovation Development Strategy"[49]

2.6 Summary

The main influencing forces for NEV and ICV security industry are:

1. Cybersecurity and Cryptography Law to protect national security
2. National policy and regulation on NEV/ICV industry
3. Overseas market and UN type approval regulations

Information security has risen to the "new bottom line"of vehicle safety. From China innovation strategy point of view, which introduces safety and privacy requirements, security features are required as an assurance method. China innovation strategy is also strongly influenced by the current ongoing WP29/GRVA regulation making activities. To summarize, the present policies that are shaping the NEV/ICV security industry are,

1. Motoring the effectiveness of NEV market incentive policies and regulations, e.g. subsidies and tax exemption/reductions.
2. Anti-fraud on OEMs' application for subsidies.
3. Regulation on CII regulation (draft).
4. Regulation on Personal Information Protection.
5. Regulation on Important Data Protection, e.g. map data
6. Regulation on Data cross border.
7. On-going 5G-V2X promotion.
8. Government spending

49 https://www.ndrc.gov.cn/xxgk/zcfb/tz/202002/t20200224_1221077.html

To summarize, security implications from market-driven perspective:

1. Rapid NEV development implies safety requirements on vehicle and charging infrastructure, thus introducing security requirements as well.

2. ICV market demand implies safety (on autonomous) and privacy (on connectivity) requirements on vehicle and service backend.

3. Shared-mobility market demands.

Following sub-sections analyze overall market trends of NEV, EV infrastructure, ICV, automotive cybersecurity, value chains and shared-mobility that indirectly highlight increasing requirements and scale for security industry.

2.6.1 NEV Market Trends

China's EV sales are expected to reach 6 million units by 2025. As per China Automobile Association 2019 Q1, passenger car (NEV) new sales occupied 91.3% (563,000) and commercial vehicles (NEV) 8.7% (54,000) respectively of the total NEV market share. NEV market trends:

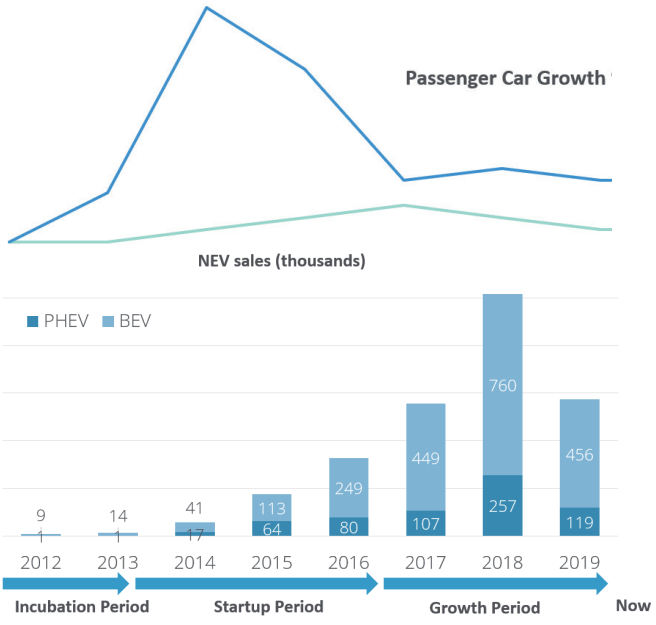
1. BEV and HEV shall still be choice in mid-term. Pure EV and Fuel cell vehicles will jointly direct future development. Emerging trend of EVs at large-scale and high-end models. Private purchase will be the main leader for NEVs.

2. More than cruising range and charging convenience, intelligent (smart), networked (connected), and humanized functional design competition among Chinese and foreign OEM will be key to differentiated competition in China's NEV industry.

3. The transformation of new retail (including direct sales model) is the general trend of industry development. Balance between user withdrawal and cost efficiency would be the key. Sales concentrate in first, second tier and restricted-licensing cities, and gradually will increase in third tier and non-restricted-licensing cities.

4. NEVs will greatly extend the value chain upstream and downstream. Upstream power batteries and smart technology, and downstream end-market user services will become important profit pools.

Figure 3: Growth and Sales of NEV's (2009-19)[50]



50 Nielsen: New Energy Market and Automotive Demand Research Report-Oct 2019

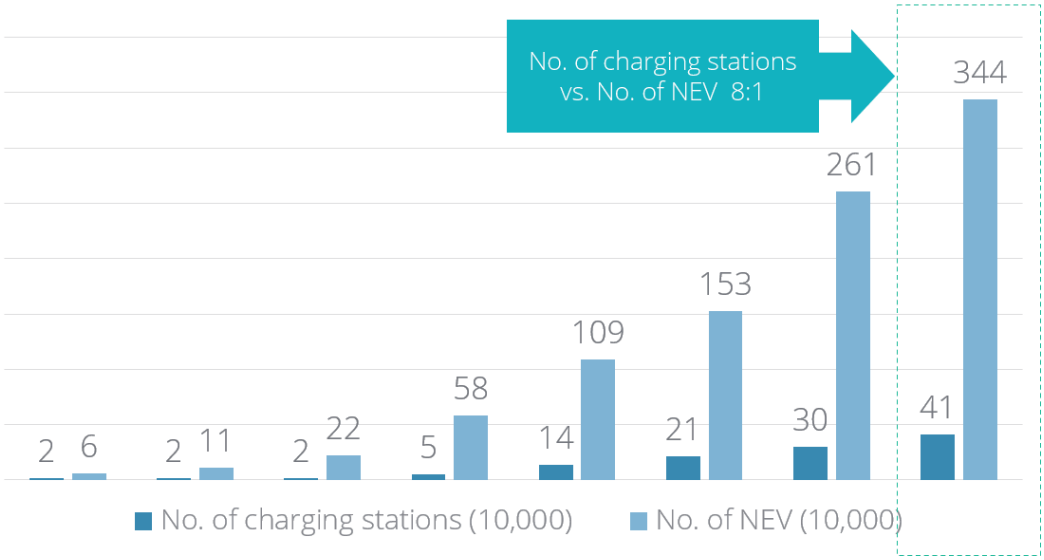
Figure 4, shows collation of members of China's current NEV safety value chain.

Figure 4: New energy vehicle safety value-chain[51]

2.6.2 EV Infrastructure Market Trends

At the end of 2018, optimised ratio of charging stations (included private charging stations) and EVs in China was relatively low around 1:3.2. Installed EV charging stations in China are expected to surpass 20 million units by 2025. End of 2018, 63.3% charging piles were AC and 36.5% DC and with increasing proportion of DC charging.

Figure 5: Comparison of number of charging stations vs NEV's



51 Interpretation of 2019 White Paper on Automotive Safety Trends

The following figure 6 represents collation of members of China's EV infrastructure value chain.

Figure 6: Electric Vehicle Charging Pile Industry Chain[52]

2.6.3 ICV Market Trends

ICV sales estimated to be ~30% of overall automotive industry in 202530:

1. Industrial development: transformation from single manufacturing industry to deep integration of multiple industrial chain is key.

2. Supply: scalability has increased; OEMs are upgrading from manufacturing to travel services.

3. Service: towards forming a service system with ICV's as the service carrier and increasing interaction between end-user and vehicle as smart mobile partner.

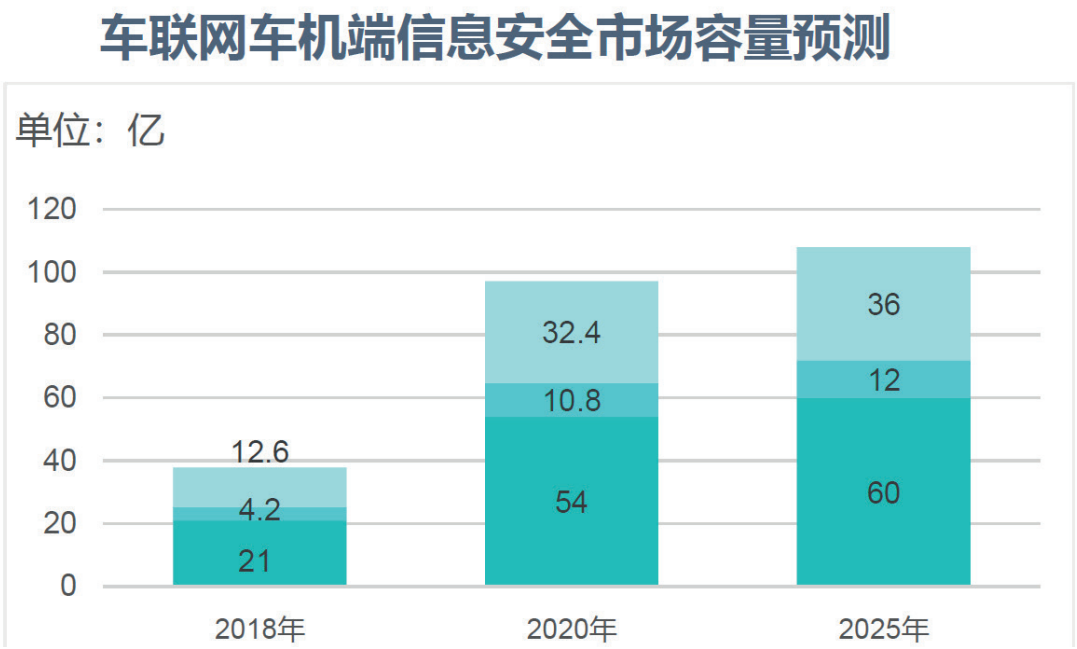
4. Presently, in the autonomous vehicle development direction, China has ability to develop and test vehicles of L2 and above, and its commercialization and application landing are also in exploratory stage. L2 assisted driving is still the main focus, L3 and above autonomous driving functions have not yet been applied in mass-produced vehicles. Autonomous driving technical solutions are becoming mainstream and relevant laws, regulations for autonomous driving application scenarios, standards in V2X, data security, information security, and personal information protection are underway.

52 2019, China electric car charging pile Industry Research Report

2.6.4 Automotive Cyber Security Market Trends

Automotive vehicle-side security market is estimated 10.8 billion Yuan in 2025.

Figure 7: Automotive Cybersecurity Vehicle-Side market estimation



The following figure (Figure 8) presents collation of members as part of China's present automotive cyber security value chain. The respective labels are further explained in Table 2.

Figure 8: Automotive Cybersecurity value chain

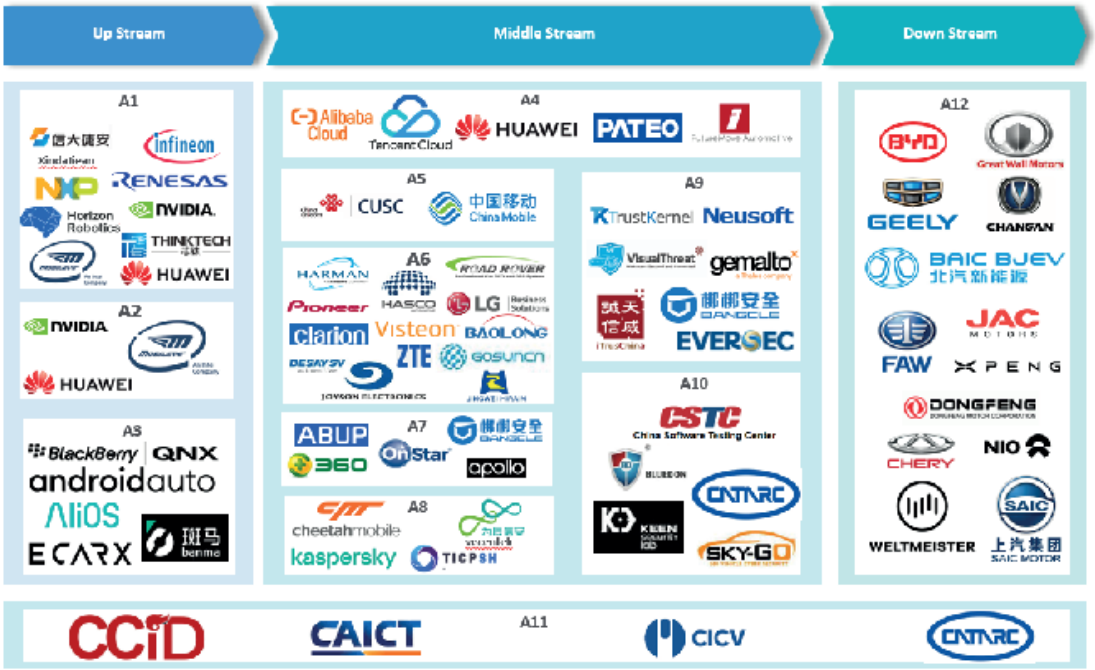


Table 2: Term of Labels in Figure 8

Value-chain	Label	Term
Upstream	A1	Security chip and microcontroller
	A2	Security algorithms
	A3	Secure operating system
Middle Stream	A4	Cloud security
	A5	Communication security
	A6	In-vehicle hardware security
	A7	In-vehicle software security
	A8	Mobile App - Smartphone app security
	A9	Information security solutions
	A10	Information security testing and services
Downstream	A11	Information security integration services (security consultant, process services)
Government Layer	A12	Vehicle security

2.6.5 Shared Mobility Market Trends

Shared mobility has emerged as an important and developing market for automobile and travel industries and as an approach to provide for, in medium and long term, China's high levels of transportation demands. China is moving from its statistics-based travel demand services, online shared car-hailing, and time based rental towards travel-as-supply service using EVs.

Shared mobility is driving up EV demand in China. With improving cost-effectiveness in shared travel scenarios, higher demand for environmental protection and air quality, some cities like Shenzhen, Guangzhou, Foshan, Huizhou, Dongguan, Kunming, Zhengzhou, Haikou, Shenyang, Liuzhou have already proposed mandatory use of EV for car-sharing.

At the end of June 2019, 967,000 pure electric vehicles were registered on the DiDi platform, China largest shared mobility platform. This accounted for more than 30% of pure EVs in China. In 2040, under the optimistic scenario, it is estimated that 80% of mileage will be completed by car-sharing.

Shared EV Charging Station: As the sharing economy becomes more popular in the Chinese market, its application range has gradually expanded and enriched. Till June 2019, there were approximately 591,000 private charging stations built in China. Even assuming that only a quarter of charging stations can be shared, charging stations have the potential to become another emerging sharing economy industry.

III China NEV and ICV Cybersecurity Law and Standardization Activities (2015-2020)

3 China NEV and ICV Cybersecurity Law and Standardization Activities (2015-2020)

This section provides information on NEV/ICV cybersecurity related law and standards, including China cryptography system, laws and its standards. It gives an overview of relevant NEV security standards from TC114 and TC260 and background of its organization. China standardization process and other industry standards from important industry associations are also described.

3.1 National Cybersecurity and Cryptography Law

Chinese cybersecurity laws and regulations have a general, overarching legal effect within the country. Also, within China cryptographic compliance, some laws and regulations are applicable depending on the detailed project (case by case basis). China Cybersecurity Law and Cryptography Law, are most important high-level laws applicable to NEV/ICV industry.

3.1.1 China Cybersecurity Law (CSL June 2017)

China has adopted National Cybersecurity Law that came into effect on 1 June 2017. Following is description of five relevant points that are applicable to EV security context.

I. The wide range of "network service providers" are subject to regulation.

Article 76 (1) "Networks" refers to systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing.

-from <China's Cybersecurity Law>

According to Article 76 (1), a network must have a certain physical form to gather, store, transmit information. The term "network" in China must rely on the network of physical facilities located in China (including the use of the network for its own business purposes).

II. Network operation security:

Article 21: The State implements a tiered system of network security protections. Network operators shall perform the following security protection duties according to the requirements of the tiered network security protection system to ensure the network avoids interference, damage or unauthorized visits, and to prevent network data leaks, theft or falsification:

1. Formulate internal security management systems and operating rules, determine persons responsible for network security, and implement network security protection responsibility;

2. Adopt technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering network security;

3. Adopt technological measures for monitoring and recording network operational statuses and network security incidents, and follow relevant provisions to store network logs for at least six months;

4. Adopt measures such as data classification, back-up of important data, and encryption;

5. Other obligations provided by law or administrative regulations.

-from <China's Cybersecurity Law>

Article 21 clearly specifies "network security level protection system". Network security will be divided into 5 levels. However, China's Cybersecurity Law does not further clarify the meaning of this protection system. It also does not explain how to implement this protection system and how to divide and identify the "network security level" in details.

Before China's Cybersecurity Law, China already established two types of protection systems (by law and regulations) involving cybersecurity, "**computer information system** information security level protection"[53] and "**communication network** unit security rating protection"[54]. Network security level defined by China's Cybersecurity Law has no clear relationship with the two protection systems above. According to these, the second level (up to the fifth level) of the computer information system only need to be recorded at the public security department from 2011. Up to the third level of the **computer information system** or beyond the second level of **communication network** is required to carry out regular security self-assessment or periodic security checks.

In Cybersecurity Law, the translation is "operator", but for understanding we use "provider". That is a paid service run by network service "provider" will be regulated, whereas service with no earning will not be regulated. For example, consider "Internet Information Service", the Internet "provider" of information services need to apply for ICP certificate, whereas provider giving free service only needs ICP record. To re-phrase, "Business" means that the providers (providers) of paid Internet information services need to apply for an ICP certificate, while "non-business" providers (operators) of free services only need ICP record. For example, the former could be an e-commerce platform, and the latter is a website where a company is only used to publicly release corporate information and does not involve any paid information.

Insight: The "network security level protection system" in not clear. For further detailed information, please refer to the revised China **MLPS** (Multilevel Protection Scheme) 2.0 series of regulations[55].

III. Security of Critical information infrastructure:

Article 31: The State implements key protection of public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure that if destroyed, losing function or leaking data might seriously endanger national security, national welfare and the people's livelihood, or the public interest, on the basis of their tiered protection system. The State Council will formulate the specific scope and security protection measures for critical information infrastructure.

Article 38: At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks security and risks that might exists either personally, or through retaining a network security services establishment; and submit a network security report on the circumstances of the inspection and assessment as well as improvement measures, to be sent to the relevant department responsible for critical information infrastructure security protection efforts.

-from <China's Cybersecurity Law>

The critical information infrastructure covers important sectors and areas such as "public communications and information services, energy, traffic, water, finance, public services, e-government, etc." The provisions of the China State Council need to further clarify whether these are critical and if any other areas/sectors (not listed above) are critical. Cybersecurity Law does not clearly state which areas/sectors are critical, which leaves the margin for Chinese government to give detailed information in the future. The suggestion is to monitor if **traffic** will be included in the future detailed regulations/rules.

53 <Regulations of the People's Republic of China for Safety Protection of Computer Information Systems (Revised in 2011)> Article 9 and <Administrative Measures for the Graded Protection of Information Security (22.06.2007)> by the Ministry of Public Security, the State Secrecy Bureau, the State Cipher Code Administration and the Information Office of the State Council.

54 <Measures for the Administration of Communication Network Security Protection> effected from 1st March 2010.

55 Information MLPS 2.0 - Dec 2019

Article 31 clearly elaborates the critical information infrastructure needs to be protected according to the network security level protection system.

Article 38 requires the critical information infrastructure operators to conduct, at least once a year, a security risk inspection and evaluation by itself or by a professional organization (at their own expense).

Insight: The law proposes security of CII for the first time, but its definition is not clear.

IV. Personal information protection:

Article 41: Network operators collecting and using personal information shall abide by the principles of legality, propriety and necessity; make public rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtaining the consent of the person whose data is gathered.

Network operators must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations and agreements with users to process personal information they have stored.

Article 42: Network operators must not disclose, tamper with, or destroy personal information they gather; and, absent the consent of the person whose information was collected, must not provide personal information to others. Except, however, where it has been processed so that the specific individual is unidentifiable and cannot be recovered.

Network operators shall adopt technological measures and other necessary measures to ensure the security of personal information they gather, and prevent personal information from leaking, being destroyed or lost. When the leak, destruction or loss of personal information occur, or might occur, remedial measures shall be immediately taken, and provisions followed to promptly inform users and to make report to the competent departments in accordance with regulations.

Article 43: Where individuals discover that network operators have violated the provisions of laws, administrative regulations or agreements between the parties to gather or use their personal information, they have the right to request the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to request the network operators make corrections. Network operators shall employ measures for deletions and corrections.

Article 44: Individuals or organizations must not steal or use other illegal methods to acquire personal information and must not unlawfully sell or unlawfully provide others with personal information.
Article 45: Departments lawfully having network security supervision and management duties, and their staffs, must keep personal information, private information and commercial secrets, which they learn of in performing their duties, strictly confidential, and must not leak, sell, or unlawfully provide it to others.

-from <China's Cybersecurity Law>

Article 41 to Article 45 of the law states that "personal information and other important data gathered or produced by critical information infrastructure network operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China." It also stipulates the requirements of protection of personal information especially avoiding disclosure, damage or loss of personal information.

Use case: Any company that operates a wholly foreign-owned enterprise (WFOE) in China collects personal information about its employees. China's new cybersecurity law defines personal information as "all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses, telephone numbers, and so forth."

It is still best practice for foreign company employers in China, to follow the basic rules. In the consumer context, China imposes more generally, on the collection and

maintenance of personal information, including the following,

Be sure the disclosing party (your employee) is aware that the company collects and maintains personal information. The company should have a written policy (in Chinese and in English) on how long that information is maintained, and that policy should be revealed to the employee.

Company should not collect more personal information than necessary.
Company should maintain the confidentiality of the personal information collected. That means company should limit internal access to that information and should take proper security measures to prevent a data breach of the company's online systems.

Company should not sell or otherwise transfer the personal information to any third party. Stated more bluntly, do not sell employee personal information to marketers or spammers.

Insight: Restrictions on the transmission of specific personal information abroad.

V. Specific requirements for "network critical equipment and network security products"

Article 23: Critical network equipment and specialized network security products shall follow the national standards and mandatory requirements, and be security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided. The state network information departments, together with the relevant departments of the State Council, formulate and release a catalog of critical network equipment and specialized network security products, and promote reciprocal recognition of safety certifications and security inspection results to avoid duplicative certifications and inspections.

-from <China's Cybersecurity Law>

Article 23: Critical network equipment and specialized network security products shall follow the national standards and mandatory requirements. These equipment and products need to be certified and evaluated to meet certain security requirements by a qualified agency before being sold or provided. The Chinese network information departments, together with the relevant departments of China State Council, will formulate and release a catalog of critical network equipment and specialized network security products (**foreign companies must follow up this release in the future**).

An enterprise that is not a network operator, but as long as it has engaged in "selling" or "providing" in the business of network security equipment and products, also requires to be compliant with the relevant regulations of the China's Cybersecurity Law.

3.1.2 China Cybersecurity Review Measures (June 2020)

China Cybersecurity Review Measures **effected at 1st June 2020.** Following are relevant implications brought about by these measures,
According to China Cybersecurity Law:

"Article 35: Critical information infrastructure operators purchasing network products and services that might impact national security shall go through a national security review organized by the State network information departments and relevant departments of the State Council. "

"Article 59: Where network operators do not perform network security protection duties provided for in articles 21 and 25 of this law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to endangerment of network security or other such consequences, a fine of between RMB 10,000 and 100,000 is given; and the directly responsible management personnel are fined between RMB 5,000 and 50,000.

Where critical information infrastructure operators do not perform network security protection duties provided for in articles 33, 34, 36 and 38 of this law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to endangerment of network security or other such consequences, a fine of

between RMB 100,000 and 1,000,000 is give; and the directly responsible management personnel is fined between RMB 10,000 and 100,000. "

One of the key principles of the China Cybersecurity Law provided that the procurement of network products and services (which may affect national security interests) must be subject to an official cybersecurity review. Following the release of the measures, there is now greater clarity regarding the procedures and timing of this cybersecurity assessment.

Under the new Measures, operators of critical information infrastructure in China are required to perform a cybersecurity review when they procure network products and services that may impact China's national security interests. Network products and services include core network equipment, high-performance computers and servers, mass storage equipment, large-scale databases and application software, cybersecurity equipment, cloud computing services as well as other network products and services that have a significant impact on critical information infrastructure security.

Importantly, the Measures require that operators of critical information infrastructure identified by the authorities:

- anticipate potential national security risks brought about by the procurement;
- if the procurement may have an impact on national security, declare to the Office for Cybersecurity Review about the need for a cybersecurity review; and
- obtain via contractual means, the right to request the vendors' cooperation in the review process as well as undertakings from the vendors prohibiting: (i) the illegal solicitation of users' data, (ii) the control or manipulation of users' equipment, and (iii) the suspension of the supply of products or necessary technical support services without justification

The Office of Cybersecurity Review will respond on whether a cybersecurity review will be required within 10 business days following its receipt of the operator's declaration. Any initial cybersecurity review is expected to be completed within 30 working days.

Contravention of the Measures may be subject to a fine of up to ten times the procurement price, along with individual fines of up to RMB100,000 for the personnel involved.

Operators of critical information infrastructure should commence preparatory work in relation to cybersecurity assessments which will be relevant for any upcoming procurement of network products and services, which may require updates to their procurement contract templates.

3.1.3 China Cryptography (Encryption) Law (CEL – Oct 2019)

October 2019, China passed the Cryptography Law[56]. The law seeks to provide a unified approach to the regulation of cryptography, including its production, sale, import, export, testing, certification and use. The law consolidates various aspects of the existing cryptography regime (which has been in place since 1999).

The stated purpose of the Law is as follows:
(Article 1)

1. to regulate encryption application and management;
2. to facilitate the development of the encryption industry;
3. to protect network and information security;
4. to safeguard national security and public interest;
5. to protect the legal rights of citizens, legal persons, and other organizations.

Below mentioned are certain relevant aspects of the Law, in group of seven points, short comparison between CSL and CEL. For reference, also provide published list of security products and cryptography products.

56 China Cryptography Law - Oct 2019

I. Align with "China Foreign Investment Law"

Article 21: The state encourages research and development, academic exchange, achievement transformation, and spreading the use of commercial cryptography, to complete a unified, open, competitive, and orderly market system for commercial cryptography, encouraging **the development of the commercial cryptography** industry.

All levels of people's government and their relevant departments shall follow the principle of non-discrimination to lawfully give equal treatment to units, **including foreign investment enterprises**, such as those researching, producing, selling, servicing, or importing or exporting, commercial cryptography (hereinafter jointly referred to as "commercial cryptography work units"). The state encourages technological cooperation on commercial cryptography to be conducted in the course of foreign investment and on the basis of the voluntariness principle and business rules. Administrative organs and their employees must not force the transfer of commercial cryptography technology through administrative measures.

Research, production, sale, service, import, and export of commercial cryptography must not endanger national security, the societal public interest, or the lawful rights and interests of others.

-from <China's Cryptography Law>

In terms of market access, foreign-invested enterprises must not be discriminated against. This is in the same inline as the "Foreign Investment Law"[57] passed earlier in 2020. If the previous "China Foreign Investment Law" provided for the protection of the legal rights and interests of foreign investment from the general framework, then the second paragraph of Article 21 directly clarifies the strengthening of the protection of the legal rights and interests of foreign investment in the field of commercial encryption.

II. China Promotes Development of National, Industry, Group Commercial Cryptography Standards with International Standards

Article 22: The state is to **establish** and improve a system of standards for **commercial** cryptography.
On the basis of their individual responsibilities, the State Council administrative department for standardization and the State Cryptography Administration are to organize the drafting of relevant national and industry standards for commercial cryptography.

The state supports social groups and enterprises use of their own innovative technologies and drafting group **or enterprise cryptography standards** that exceed the state and industry standards' requirements.

Article 23: The state promotes participation in activities for the international standardization of **commercial** cryptography, participation **in drafting international standards on commercial cryptography**, and advancing conversion for use between Chinese and foreign standards on commercial cryptography.

The state encourages enterprises and social groups, and educational and research bodies, etc., to participate in activities for the international standardization of commercial cryptography.

Article 24: Commercial cryptography work units launching commercial cryptography activities shall comply with the technical requirements of relevant laws, administrative regulations, compulsory state standards on commercial cryptography, as well as the unit's public standards.

The state encourages commercial cryptography work units to employ **recommended** state and industry standards on commercial cryptography, increasing the defensive capacity of commercial cryptography and preserving users' lawful rights and interests.

-from <China's Cryptography Law>

Articles 22, 23, and 24 specifies that in addition to national standards and industry standards, commercial encryption group standards and corporate standards can also be formulated.

Although there are a large number of commercial encryption companies in China, due to differences in

57 Foreign Investment Law - Jan 2020 [Last Visited:05/07/2021]

domestic and foreign standards, no Chinese commercial companies have opened up overseas business and neither foreign commercial encryption companies have entered China. The promulgation of the "Cryptography Law" has provided support for Chinese companies. There are no regulations that object use of international cryptographic standards in China. The introduction of cryptographic products based on national cryptographic algorithms and international algorithms to the international market has paved the way for foreign companies that support national cryptographic algorithms and international cryptographic products to enter the Chinese market.

III. Compulsory Testing Requirements of "Critical Network Equipment and Network Security Special Product"

Article 25: The state is to advance the establishment of systems for **testing and certification** of **commercial** cryptography, drafting technical regulations and rules for testing and certification of commercial cryptography, and encouraging commercial cryptography work units to accept testing and certification to increase their market competitiveness.

Commercial cryptography testing and certification bodies shall obtain credentials in accordance with law and carry out commercial cryptography testing and certification in accordance with laws, administrative regulations, and technical regulations for commercial cryptography testing and certification.

Commercial cryptography testing and certification bodies shall bear an obligation to maintain the secrecy of state secrets and commercial secrets that they learn of in the course of commercial cryptography testing and certifications.

Article 26: Commercial cryptography products that involve national security, the national welfare and the people's livelihood, or the societal public interest, shall be lawfully entered into the catalogs of critical network equipment and specialized cybersecurity products, and **must pass** testing and certification by qualified bodies before being sold or provided. Testing and certification of commercial cryptography products is to apply the relevant provisions of the "People's Republic of China Cybersecurity Law", to avoid repetitive testing.

Where commercial cryptography services use critical network equipment and specialized cybersecurity products, it **shall be after** that commercial cryptography service is certified as up to standards by a commercial cryptography certification body.

-from <China's Cryptography Law>

Articles 25 and 26 are regulations for testing and certification systems of commercial cryptography products. According to Article 9 of the "Regulations on the Administration of Commercial Encryption"[58]: All cryptographic products must be tested by a designated cryptographic testing agency before they can be sold to the market and provided to users. After the "Cryptography Law" is promulgated, commercial cryptographic products related to national security, national economy, people's livelihood, and social public interest will be included in the list of "Critical Network Equipment "and "Network Security Special Product Catalog", and approved according to the regulatory system or market access system corresponding to the catalog. Only after the testing and certification are qualified, commercial cryptographic products that are mentioned in the catalog can be sold with this testing certification.

IV. Adopt Cryptographic Protection and Security Assessments for Critical Information Infrastructure

Article 27: Where laws, administrative regulations, and relevant state provisions require that critical information infrastructures use **commercial** cryptography **protections**, their operators shall use commercial cryptography protections and carry out commercial cryptography application **security assessments** either on their own or by retaining a commercial cryptography testing body. Security assessments of commercial cryptography applications shall be connected to critical information infrastructure security testing assessments and network security classification level assessments to avoid repetitive assessments and evaluations.

58 Regulations on the Administration of Commercial Encryption

Where operators of critical information infrastructure purchase network products or services that involve commercial cryptography, and might impact national security, they shall follow the provisions of the "People's Republic of China Cybersecurity Law" to pass national security review organized by the State Internet Information Department, together with the State Cryptography Administration, and other relevant departments.

-from <China's Cryptography Law>

Article 27 stipulates that for critical information infrastructure, it is required to use commercial cryptography for protection, and it is necessary to entrust corresponding institutions to conduct security assessments.

V. Import and Export Rules for Commercial Cryptography Products

Article 28: The State Council department for commercial affairs and the State Cryptography Administration are to lawfully carry out **import permitting** for commercial cryptography that involves national security or the societal public interest that have cryptographic protection functions, and carry out **export controls** on commercial cryptography that involves national security, the societal public interest, or international obligations that China has undertaken. The lists of import permits and export controls for commercial cryptography are to be drafted and published by the State Council department for commercial affairs together with the State Cryptography Administration and General Customs Administration.

Import permitting and export control systems are **not** implemented for commercial cryptography for mass consumption.

-from <China's Cryptography Law>

Article 28 is a regulation for the commercial cryptography products import and export management system. Article 13 of the "Regulations on the Administration of Commercial Encryption"61 stipulates that the import of cryptographic products and equipment containing cryptographic technology or the export of commercial cryptographic products must be reported to the national cryptographic management agency for approval. No unit or individual may sell overseas cryptographic products. It can be seen that **before** the promulgation of the "Cryptography Law," commercial cryptographic products produced by foreign manufacturers must obtain corresponding import licenses if they are to be provided to users in China

After the "Cryptography Law" was promulgated, all products **included** in the list of commercial encryption import licenses can be imported after obtaining a license, and commercial encryption used in **mass consumer products are not** subject to import license and export control systems.

The detailed process for obtaining a license is difficult to find and it is only listed in the government website. The time period is around 3-6 months. The products included in the list of import/export are not clear, that is those that fall within the scope of "products for mass consumption" and therefore can be freely imported into China. Thus licensing requirement of individual backend/production line cryptographic equipment or direct import of cryptographic material from IT servers is not known as this point. The commercial encryption import permit list and export control list are formulated and published by the Ministry of Commerce in conjunction with the SCA[59]. Those engaged in the import of cryptographic products and equipment containing cryptographic technology shall be handled in accordance with the State Secrets Bureau Announcement No. 18 and No. 27 jointly issued by the SCA and the General Administration of Customs. In Dec 2020, Ministry of Commerce, SCA and the General Administration of Customs announced update of import permit and export control lists and application procedures to procure licenses 63.

VI. Management of Commercial Cryptography

Article 29: The State Cryptography Administration is to **conduct certification of entities** using commercial cryptography technology to engage in e-governance e-certification services, and collaborate with relevant departments responsible for managing the use of electronic signatures and data messaging in government activities.

59 State Cryptography Administration Import/Export Rules -Dec 2019

Article 30: Industry associations for the commercial cryptography field and other organizations are to follow laws, administrative regulations, and their charters to provide services such as information, technology, and training to commercial cryptography work units, guiding and urging them to lawfully carry out commercial cryptography activities, strengthen industry self-discipline, promote the establishment of industry creditworthiness, and promote the healthy development of the industry.

-from <China's Cryptography Law>

Articles 29 and 30 stipulate the management organization of commercial cryptography business units. SCA shall identify agencies that engage in electronic authentication services using commercial cryptography and administer its management in conjunction with relevant departments. The industry associations in the field of commercial cryptography must guide and supervise the commercial cryptography activities carried out by practicing business units.

VII. Certification of Commercial Encryption Product based on Volunteer Basis

Article 31: Cryptography management departments and relevant departments are to establish systems for regulation of commercial cryptography, during and after the fact, that combine routine oversight and random sampling inspections, establish a unified platform for commercial cryptography oversight and management information, advance the establishment of connections between regulation during and after the fact and the social credit system, and strengthen commercial cryptography work units' self-discipline and public oversight.

Cryptography management departments and relevant departments, as well as their staffs, must not require commercial cryptography work units and commercial cryptography testing and certification bodies to disclose source code and other proprietary information related to cryptography; and are to strictly preserve the secrecy of commercial secrets and personal private information learned of in the performance of their duties, and must not leak or illegally provide it to other people.

-from <China's Cryptography Law>

As per China's regulations, manufacturers were required to submit the **source code** of the product to the cryptographic product testing and certification agency when submitting commercial cryptographic products for inspection. This has caused some manufacturers' concerns. After the "Cryptography Law" is promulgated, the Cryptographic management department and relevant departments and their staff shall **not require** commercial cryptography practitioners and commercial cryptography testing and certification agencies to disclose source code and other proprietary cryptographic information to them, and be aware of them in the performance of their duties. The business secrets and personal privacy of the company shall be kept strictly confidential, and shall not be disclosed or illegally provided to others. This provides legal protection for the confidentiality of commercial cryptographic products, which can greatly alleviate the concerns of manufacturers, especially foreign manufacturers.

In summary, China Cryptography Law struck a conciliatory tone on the commercial end of things with the intention to boost Chinese economy with foreign investment and engagement. However, the Law also reveals an existing security gap in China's cryptography apparatus that needs regulation. In the near future, cryptographic systems in the national security realm will be more regulated and professionalized. Greater cooperation between foreign and Chinese entities in cryptography research and development is expected, yet one must also anticipate additional Chinese state support for domestic cryptography enterprises to become more competitive.

A short comparison between China Cybersecurity Law and China Cryptography Law is provided in Appendix Table 16. List of security products mentioned in CSL is provided in Table 17 of the Appendix. Commercial cryptography products in CEL are listed in Table 18.

3.2 Standardization Layers and Procedure

This section describes the different group of standards in China and the course for standard publishing.

3.2.1 Standardization Layers

There are four layers of Chinese standardization: National layer, Industrial layer, Local layer and Enterprise layer.

Table 3: Layers of Chinese Standardization

	National	Industrial	Local	Enterprise
Who	SAC	OSCCA (e.g.)	Province/City	Corporate
Scope	National	Specific industrial technologies	Local	Corporate
Effectiveness	National	Specific area (It will be abolished once national standardization comes into effect)	No national and industrial standardization are available (It will be abolished once national standardization comes into effect)	Enterprise standardization for company
Requirement	Mandatory/ Recommend	Mandatory/ Recommend	Mandatory/ Recommend	N.A.
Priority (high to low)	1	2	3	4

Both national layer and industrial layer are equally important. Industrial layer focuses on detailed technology to supplement the national layer standard, if national layer does not cover the topic. For example, national layer standard will require to use cryptography in certain product, but it will not mention which cryptographic algorithm is used. On the contrary, the industrial layer will focus on which algorithm need to be applied, e.g. Chinese cryptography algorithms.

3.2.2 Publishing Procedure

There are some procedures to publish Chinese national standards.

Table 4: Requirements for Publishing National Standard

Required Documents for Standards Approval		No. of copies
National Standard Approval Signing Form		1
Standard Declaration (National Standard Application form)		2
Standard Draft (National Standard Approval Document)		4
Instructions for preparing standard drafts for approval (National Standard Approval Preparation Instruction)		2
Summary of Processing Table of Comments of Draft Version of National Standard Document		2
Audit Meeting Minutes	Annex: Audit of summary of comments table	Member signature form
	Annex: Name list of review representatives	
Standard Draft (National Standard Manuscript)		1
Publication Figures, Original CAS Figures		1
Electronic Version of Approval Document		1

Critical steps of standardization procedure with timeline as follows:

Note:

1. All standards need to be established complying with the standards developing requirements like GB/T 1.1 and GB/T 20000 series;
2. The projects should be carefully named to avoid complicated renaming processes;
3. The relative documents need to be prepared based on SAC's requirements and submitted on time (such as Draft for comments, Inspection draft, etc.).

3.3 NEV and ICV Security Standards

It is expected that till 2025 there will be around 30+ Chinese Cybersecurity standards for automotive. In the future, most ECUs in vehicle, which have information exchange with government infrastructures, would potentially have to communicate using both international cryptographic algorithms and Chinese cryptographic algorithms. By government infrastructure it is meant those built by the government only. Government infrastructures (backend) will prefer to use Chinese cryptographic algorithm. CEL and CSL take precedence over standards, in case of ambiguity.

TC114 automotive and TC260 information security committees consists of the most important WG's from EV security context in China. These presently draft and published the most important EV security standards. Following, presented are both, the committee and their relevant EV security standards, as well as standards from important NGOs like CEC and CCSA.

3.3.1 TC114 NEV Security Standards

Figure 9: Overview of Working Groups in TC 114

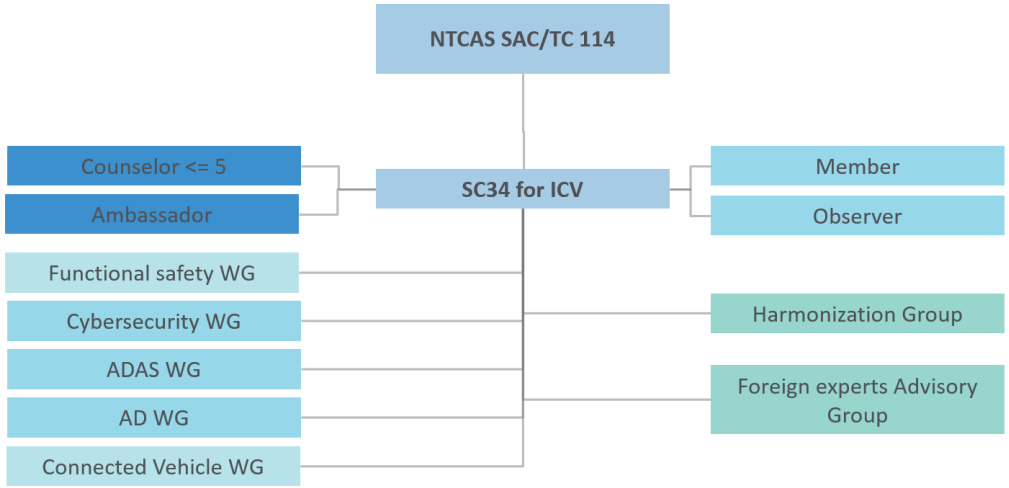


Figure 9 gives the structure of TC114. TC114 comes under the aegis of CATARC. CATARC[60] is the national centralized technical administration of automotive standardization and regulations. It has the following roles:

1. Secretariat of National Technical Committee of Automotive Standardization (SAC/TC114)
2. Secretariat of Automotive Branch of China Association for Standardization

60 National Technical Committee for Auto Standardization TC114

3. Secretariat of China WP.29 Workgroup (C-WP.29)

4. Organize the industry to research the Chinese automotive standard system and enforce the annual automotive standard revising plans

5. Formulate the automotive standards and technical regulations in the key areas as energy conservation, safety, environmental protection, NEV (new energy vehicle) etc.

6. Participate in the formulation of international standards and international automotive technical regulation, harmonization such as ISO/TC22, UNECE/WP.29.

Table 5 provides the list of TC114/SC34 NEV Security Standards (February 2020). Overview of all cybersecurity standards of various working groups of SC34 are listed in Table 19 of Appendix. The standards/plan number marked in bold, are among the more important standards from NEV security context.

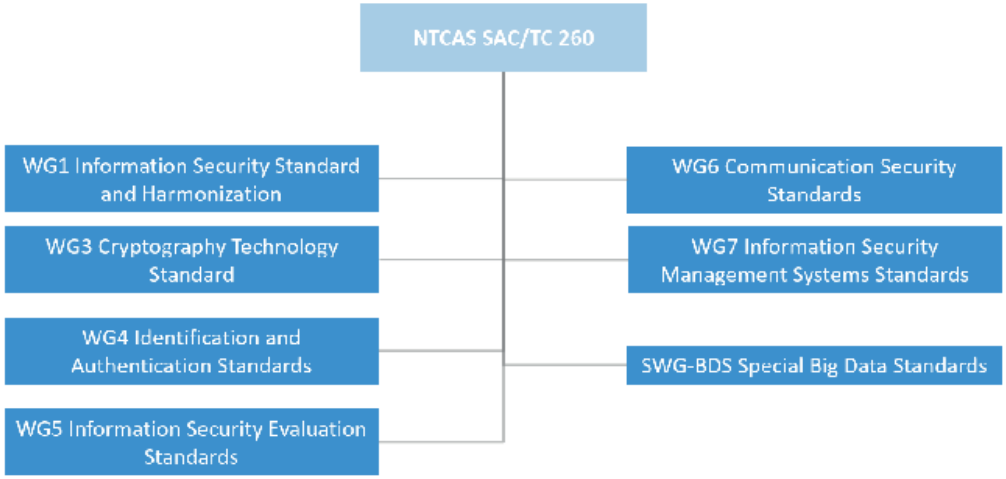
Table 5: TC114/SC34 NEV Cybersecurity Standards

	No	Standard	Status
First Batch	1	General technical requirements for Cybersecurity vehicles (20191065-T-339)	Solicit comments within WG
	2	Cyber-Security Technical specifications of remote service and management system for electrical vehicles (**20191066-T-339**) Note: Supplement to GB/T 32960, concerning security on NEV remote monitoring	Solicit comments within WG
	3	Technical security requirements of vehicle-mounted information interactive system (**20191069-T-339**)	Solicit comments within WG
	4	Information security of automobile gateway (20191070-T-339)	Solicit comments within WG
	5	Technical requirements of information security of electric vehicles charging systems (**20192313-T-339**). Concerning charging security on vehicle side	Project approval
Second Batch	6	Technical requirements of vehicle software update	Draft
	7	Information security technology requirement of OBD interface	Draft
	8	Guidance on emergency response management of automobile information safety	Draft
	9	Specification for risk assessment of vehicle information security	Draft

Third Batch	10	**Test methods of vehicle information safety**	Pre – research
	11	Road vehicles – Cybersecurity engineering (adoption/localization of **ISO 21434**)	Pre – research
Project under Evaluation	12	Requirements for standardization of on-board computing platforms research	Pre – research
	13	Technical requirements for information safety of on-board ECU	Pre – research

3.3.2 TC260 NEV Information Protection Standards

Figure 10: Overview of Working Groups under SAC/TC260



CESI[61] hosts the Secretariat of National Technical Committee of Information Security Standardization SAC/TC260. CESI is an institute for standardization in electronics and IT industry authorized by the MIIT for adoption and enforcement of national information standards. The Information Security Research Center under CESI mainly engages in information security standardization, information security attacking/ countermeasure theory and evaluation methods, information security assessment and consulting services, etc.

Table 6 lists TC260 relevant NEV cyber security standards. Detailed landscape of TC260 standards is listed in Appendix Table 20. Its includes 25 catalogues of Information Security standards from TC260. Note, WG3 forms China cryptography system in TC260. It is difficult for members from foreign company to join WG3. The Cryptography standards listed in Table 6, are very important from NEV context.

61 National Information Security Standardization Technical Committee 260

Table 6: Relevant NEV cyber security standards from TC260

Project/Standard No.	Comment	Title	Status
GB/T 22240-2020	Classified Protection 2.0	Information security technology-Classification guide for classified protection of cybersecurity	published
GB/T 25058-2019		Information security technology-Implementation guide for classified protection of cybersecurity	published
GB/T 28448-2019		Information security technology-Evaluation requirement for classified protection of cybersecurity	published
GB/T 22239-2019		Information security technology-Baseline for classified protection of cybersecurity	published
GB/T 25070-2019		Information security technology-Technical requirements of security design for classified protection of cybersecurity	published
GB/T 36958-2018		Information security technology-Technical requirements of security management center for classified protection of cybersecurity	published
GB/T 35273-2020	PI Protection	Information security technology-Personal information security specification	published
20194267-T-469		Information security technology-Basic specification for collecting personal information in mobile internet applications	request for comment
GB/T 37092-2018	Crypto	Information security technology-Security requirements for cryptographic modules	published
GB/T 38625-2020		Information security technology-Security test requirements for cryptographic modules	published
20190902-T-469		Information Security Technology-General requirements for information system cryptography application	request for approval

3.3.3 CEC EV Charging Security Standards

China Electricity Council (CEC)[62], is a non-profit, NGO, and self-disciplinary national trade association joined by China's power enterprises and institutions on a voluntary basis. CEC is among the most important NGOs, when it comes to EV charging standards. The leadership of the CEC Board consists of the 17 presidential members, with State Grid Corporation of China as president member, 15 major power corporations and North China Electric Power University as vice president members. CEC has formed a functional, coordinating, complementary and orderly service network covering the nation-wide power industry. CEC represent the interest and rights of enterprises, the industry, society, whilst functioning as a bridge between the government and power enterprises.

Table 7 lists 6 of 10 important CEC series of standards for EV charging and EV.

Table 7: Important CEC Series of Standards for EV charging and EV

No.	Title	Status
1	Charging and battery swap service information exchange for electric vehicles Part 1 : General	Request for Comments
2	Interactive of charging and battery swap service information for electric vehicle Part 4 : Data transmission and Security	Request for Comments
3	Interactive of charging and battery swap service information for electric vehicle Part 5 : charging service credential technical specification and information exchange	Proposal
4	Interactive information of charging and battery swap service for electric vehicles Part 6: Technical specification for the access of the charging and battery swap equipment to service platform	Request for Comments
5	Interactive information of charging and battery swap service for electric vehicle Part 7: The electric vehicle services information exchange	Proposal
6	Interactive of charging and battery swap service information for electric vehicles Part 8: Supervise information interface specification	Request for Comments

62 China Electricity Council

3.3.4 CCSA Communications Security Standards

The China Communications Standards Association (CCSA) was established in Beijing on December 18, 2002. CCSA[63] conducts standardization activities in the field of ICT under the guidance of the other government authorities. It is among the most important NGOs related to EV standardization. It is responsible for organizing the preparation and revision of national standards, industry standards, and group standards. CCSA TC8 is the Network & Information Security Technical Committee that oversees communication security standards and has four working groups. WG1: Wired Network Security, WG2: Wireless Network Security, WG3: Security Management Workgroup, WG4: Security Infrastructure

Present status of important automotive wireless communications security standards under WG2 are as follows

- Researches (Finished)
  - security of co-system of vehicle and road
  - security for LTE-V2X
- Draft ready standards
  - Technical requirement of user data application and protection in automotive based on mobile network
  - Protection assessment of user data application and protection based on mobile network
  - Technical requirement of Security Certificate Management System for LTE-based Vehicular Communication

Table 8 lists some of relevant communications security standards.

Table 8: CCSA communications security standards

No	Document	Title	Publish Date	Status
1	YD/T 3628-2019	5G mobile telecommunication network-Technical requirement of 5G security	2019-12-24	In force
2	YD/T 3530-2019	Technical requirements for Security capability of mobile internet wireless access equipment	2019-11-11	In force
3	YD/T 3572-2019	Test methods for security capability of mobile internet wireless access equipment	2019-11-11	In force
4	YD/T 3584-2019	Requirements for wireless access security configuration and enhancement of smart mobile device in heterogeneous wireless network environment	2019-11-11	In force
5	YD/T 3456-2019	Technical requirements for electronic identity carrier security	2019-08-27	In force
6	YD/T 3458-2019	Technical requirements of secure operations of resource public key infrastructure (RPKI) - Threat model of data security	2019-08-27	In force

63 China Communication Standards Association

3.4 China Cryptography Standards

Most of China Cryptography is administered by Office of State Commercial Cryptography Administration (OSCCA), also called the State Cryptography Administration (SCA) which publishes the industrial layer standards (GM/TXXX). **China cryptography system comes under SAC/TC260 WG3 (Cryptography Technology Standards).**

This section introduces SCA, gives overview of Chinese cryptography system, China cryptographic algorithms and finally, two use cases are provided.

3.4.1 State Cryptography Administration

The SCA system in China, runs from the central level to provinces, municipalities, and counties and its roles are bound to cryptography policy formulation, coordination, and implementation.

The SCA's official mandate mentions:

1. Implementation of party and state guidelines and policies on cryptography, and propose suggestions for solving major problems in cryptographic work;

2. Provide development plans on cryptographic work, draft cryptographic work regulations and be responsible for the interpretation of cryptography regulations, and organize the development of cryptography-related standards;

3. Perform lawful cryptography administration duties, manage cryptography research, production, sales, evaluation, and application, investigate and deal with leaks of confidential cryptography-related information, investigate illegal development and use of cryptography, and be responsible for cryptographic work relating to foreign entities, provide overall leadership in cryptographic work;

4. Handle the planning and management of cryptographic systems in networks and information systems, in addition to planning, building and managing national cryptographic infrastructure; and

5. Guide professional cryptography education and exchange, organize education and training of professional cryptographers, and guide research and exchange of basic cryptography theory and applied technology at institutions of higher learning, scientific research institutions, and academic organizations.

SCA also leads in formulating and publishing industrial layer standards related to cryptography. **Some of its industrial standard proposals are submitted to TC260 to upgrade to national layer standards.**

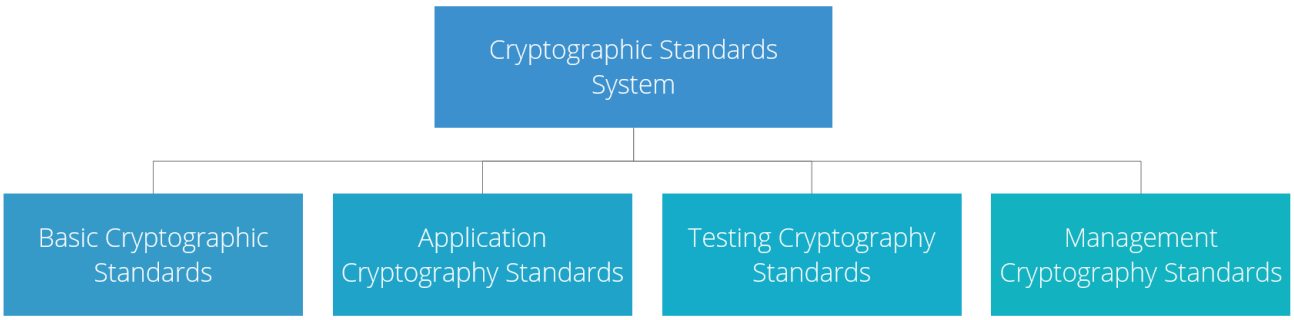
3.4.2 Cryptography Standards System

According to new standard system established by the new "China Standardization Law 2018", encryption standards can also be classified according to national standards, industry standards, and group standards. The national cryptographic standards are under the centralized management of the National Information Security Standardization Technical Committee. The specific standardization work, as mentioned previously, is under the responsibility of the WG3 cryptographic working group of TC 260.

So far, **16 national cryptographic standards** have been issued. Under the leadership and management of SCA, the encryption industry standard has been developing steadily since its inception in 2006. The establishment of the encryption industry standardization technical committee in 2011 led to official incorporation of its standardization work into the national standard management system and embarked on institutionalization, systematic development path. So far, **68 cryptographic industry standards** have been released, forming a relatively complete cryptographic industry standard system. Cryptographic group standards

are a new, and their status has just been clarified in the new "Chinese Standardization Law". At present, some group standardization organizations have carried out exploration and practice of cryptographic group standards in accordance with the requirements of the "Provisions for the Administration of Group Standards (Trial)".

Figure 11: Overview of China Cryptography Standards System



Basic Cryptography Standards:

These standards mainly regulate general cryptographic technology. It is the basic specification within the framework of the cryptographic system. It mainly covers cryptographic term standards, cryptographic identification standards, cryptographic algorithm and protocol standards, cryptographic product standards, etc. These universal basic standards are the basis and foundation for application standards, testing standards and management standards.

Application Cryptography Standards:

These are based on the basic cryptography standards. They use cryptographic technology to achieve certain security functions. They are used to standardize cryptographic applications and cryptographic services under different security goals, different application scenarios, and different business application systems to ensure completion of specific cryptographic functions, compliance and standardization of functions.

Testing Cryptography Standards:

These are corresponding testing standards prepared for the standards. They evaluate and test the compliance, interoperability, security, availability, and reliability of cryptographic algorithms, cryptographic products, and cryptographic systems. Password detection standards are the main basis for password detection and password system security assessment. They are integrated, supported and interacted with basic standards, application standards, and management standards to form an organic whole.

Management Cryptography Standards:

These support basic, application and testing standards. They are non-technical means to ensure and regulate the security of commercial cryptographic algorithms, cryptographic products, cryptographic systems, and cryptographic services. It mainly includes password product naming management, institutional qualification and quality management, password project management, password system operation and maintenance management, and password project construction implementation management. These are important means for the administrative management function to be scientific, standardized, and refined.

Summary of cryptographic standards of SCA is listed in Appendix Table 21.

3.4.3 Chinese Cryptographic Algorithms

Brief description of Chinese cryptographic algorithms:

- **SM2** is a public key cryptography algorithm based on elliptic curve cryptography, including digital signature, key exchange and public key encryption. It is used to replace international algorithms such as RSA / Diffie-Hellman / ECDSA / ECDH.
- **SM3** is password hash algorithm.
- **SM4** is a block cipher used to replace DES / AES and other international algorithms.
- **SM9** is an identity-based cryptographic algorithm that can replace PKI / CA based on digital certificate.

With the effectiveness of China Cybersecurity Law and China Cryptography Law from January 2020, there are more trends of China using Chinese Cryptographic algorithms e.g. SM2, SM3, SM4, SM9 etc. These algorithms are not presently compulsory for private business, but those concerned are suggested to continue monitor the regulations and law for detailed rules.

At the international level, several Chinese cryptographic algorithms have been included in the ISO standards:

- **SM2** Chinese Cryptographic algorithm (Digital Signature Mechanism) is finalized in ISO/IEC 14888-3:2016/DAmd.[64]
- **SM3** Cryptographic Hash Function SM3 has been included in ISO/IEC 10118-3:2018(en) IT Security Techniques - Hash-functions - Part 3: dedicated hash-functions.[65]
- **SM9** ID based cryptography equaling to RSA signature has been included in ISO/IEC 14888-3:2016 Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms.[66]
- **SM9** ID based encryption algorithm included in ISO/IEC 18033-5:2015/AMD 1:202170

3.4.4 Comparisons: China and International Cryptography Standards

In this section, are mentioned two use-cases, relevant to EV security context, security chip and cryptographic module. Both these products are published in list of Commercial Encryption Products of Table 19 and require GM/T 0008 and the GM/T 0028 industrial layer standards respectively for certification in China. Below they are compared with compatible international standards.

Table 9: Comparison for GM/T 0008 vs. FIPS-140-2 and GM/T 0028 vs ISO/IEC 19790

	GM/T 0008 Cryptography test criteria for security IC	GM/T 0028 Security Requirements for cryptographic modules
Objects	Security Chips	Cryptographic Module
Chinese National Standard	Not yet	GB/T 37092-2018

64 SM2 Digital Signature and SM9 (Chinese IBS) in ISO/IEC 14888-3:2018

65 SM3 hash function in ISO/IEC 10118-3:2018

66 SM9 ID based encryption (Chinese IBE) in ISO/IEC 18033-5:2015

Mapping to International standards	FIPS-140-2	ISO/IEC 19790: 2012 Information technology - Security techniques -Security requirements for cryptographic modules
Security Levels Classifications	OSCCA level 1; OSCCA level 2; OSCCA level 3	Security Level1; Security Level 2; Security Level 3; Security Level 4
Mapping to Automotive	Independent HSM	HSM embedded with MCU

For detailed comparisons between the Chinese and International standards refer Appendix Table 23 and Table 24.

3.5 Summary

In this chapter, summaries of some of important points for Chinese cybersecurity and cryptography law, from EV security perspective were described. List of important NEV and ICV security standards from TC114, TC260, CEC, CCSA are provided.

IV China Data Security and Personal Information Protection Regulations

4 China Data Security and Personal Information Protection Regulations

Data Security and Personal Information Protection Law are recently introduced and mark an important development in China's data protection framework. They build upon foundation and framework laid by China Cybersecurity Law and related security regulations.

However, both these laws are still available as drafts. Unlike effected law, draft law has no enforcement in China and certain rules within the present drafts, may change, and thus may not be applicable once the laws take effect. Its impact and application to NEV and ICV industry is not completely discernible and is still evolving. Thus these laws will require continued monitoring from time to time. However, for awareness, an early introduction and some insights on these draft versions are provided.

4.1 Data Security: Law and Standards

4.1.1 China Data Security Law (2020 – Draft)

Data Security Law (Draft) was released in July 2020[67]. The law provides rules around markets for data, government data collection and handling, and classification of different types of data. It specifies new responsibilities and authorities for government offices and private actors. The draft law features a total of 51 articles, divided in seven chapters: (i) general rules; (ii) data security and development; (iii) data security systems; (iv) obligations for data security protection; (v) government data security and openness; (vi) legal liability; and (vii) supplementary provisions. The draft Data Security Law marks the elevation of data security to national security level. Following is summary of five key aspects, from within the Law,

1. Data **security management measures**: For regulating the use of networks to carry out data collection, storage, transfer and processing activities, and data security protection.
2. Measures for regulating **cross-border transfer** and security assessment of personal information
3. Protection regulations on **critical information infrastructure** (CII): These relate to definition, scope and security protection measures of CII's
4. Regulations on cybersecurity **grade protection**: Regulating applicable scope of grade protection, classification of network grade, and review of grading;
5. Competent authorities of various industries can also formulate and issue regulations or drafts for comments on cybersecurity, data security protection and personal information protection applicable to their industries in accordance with the Cybersecurity Law.

Table 10 below mentions relevant articles from the Data Security Law.

67 NPC Standing Committee Seeks Public Comments on Draft Data Security Law - July 2020

Table 10: Important Articles from the draft Data Security Law

No.	Key Points	Related Article/s in the Data Security Law Draft
1	Data Security Grading	**Article 19:** The state is to implement graded and categorical data protections based on the level of importance of data in economic and social development and the extent of harm that can be caused to national security, the public interest, or the lawful rights and interests of citizens and organizations, if the data were altered, destroyed, leaked, or illegally obtained or used. Each region and each department shall follow relevant state provisions to designate a catalog of important data for protection in the corresponding region, departments, or industry, and carry out key protections for data included in the catalog.
2	Data Security Responsibility	**Article 25:** Those conducting data activities shall, according to the provisions of laws and administrative regulations as well as the mandatory requirements in national standards, establish and complete a data security management system across the entire workflow, organize and conduct data security education and training, and adopt corresponding technical measures and other necessary measures to ensure data security. Article 25: Those conducting data activities shall, according to the provisions of laws and administrative regulations as well as the mandatory requirements in national standards, establish and complete a data security management system across the entire workflow, organize and conduct data security education and training, and adopt corresponding technical measures and other necessary measures to ensure data security. **Article 28:** Those organizations processing important data shall follow provisions, to periodically carry out risk assessments of their data activities, and send risk assessment reports to the relevant regulatory departments. The risk assessment report shall include: the categories and quantities of important data controlled by said organization; how data is collected, stored, processed and used; the data security risks faced and countermeasures;
3	Data Transaction	**Article 5:** The state protects citizens and organizations rights and interests related to data; encourage reasonable and effective use of data in accordance with law; ensure lawful and orderly free flow of data; and promote the lawful development of the digital economy with data as a key element. **Article 17:** The state is to establish, develop and complete systems, for data transactions and management, regulating data transaction conduct, and fostering the data transaction market. **Article 30:** Bodies engaging in data transaction intermediary services shall, when providing trading intermediary services, require that the data providing party explain the source of the data, examine and verify the identity of both sides, and retain examination, verification, and transaction records. **Article 31:** Businesses specializing in providing services such as online data handling shall lawfully obtain business operation permits or make filings. The specific measures will be formulated by the State Council's department for telecommunications in conjunction with relevant departments.

4	National Data Security System	**Article 4:** In ensuring data security, the overall national security concept shall be upheld, data security governance systems shall be established and completed, and data security protection capabilities increased. **Article 20:** The state is to establish a uniform, highly effective, and authoritative data security risk assessment, reporting, information sharing, monitoring, and early warning system to strengthen the acquisition, analyses, assessment, and early warnings for information on data security risks.
	(Emergency Response)	**Article 21:** The state is to establish data security emergency response mechanisms. Where data security threat occurs, the relevant regulatory departments shall initiate the emergency response plan and employ corresponding emergency response measures, eliminate security threats, and prevent the harms from expanding, and promptly publish relevant warning information to the public.
	(Data security review)	**Article 22:** The state is to establish systems for data security reviews and conduct national security reviews of data activities that impact or might impact national security. Security review decisions made in accordance with law are final decisions.
	(Export controls)	**Article 23:** The State implements export controls according to law on data belonging to controlled categories to carry out international duties and safeguard national security.
5	Enforcement Assistance	**Article 32:** Public security organs and state security organs collecting data, as necessity to lawfully preserve national security or investigate crimes, shall follow relevant state provisions and complete strict approval formalities to do so, and relevant organizations and individuals shall cooperate. **Article 33:** If entities are requested by overseas law enforcement agencies to access data in China, such entities are required to report to relevant competent authorities in China and obtain approval before disclosing to overseas law enforcement agencies. These are subject to provisions set out in international treaties and agreements acceded to or by China

4.1.2 Data Security Standards

Following are selection of some of important data security standards formulated by different technical committee such as TC260, TC28, under SAC and NGOs such as CCSA.

Table 11: Data Security Standards

Project/Standard No.	Title	Status
GB/T 37932-2019	Information security technology - Security requirements for data transaction service (SAC/TC 260)	published
GB/T 37728-2019	Information technology - Data transaction service platform. General functional requirements (SAC/TC 28)	published
GB/T 36343-2018	Information technology - Data transaction service platform. Transaction data description (SAC/TC 28)	Published
GB/T 37988-2019	Information security technology - Data security capability maturity model (SAC/TC 260)	Published
GB/T 36073-2018	Data management capability maturity assessment model (SAC/TC 28)	Published
20111693-T-469	Intelligent transport - Data security service (SAC/TC 268)	Published
YD/T 3644-2020	Internet-oriented data security capability technical framework (Communication Industry Standard /CCSA)	Published
YD/T 3458-2019	Technical requirements for safe operation of Internet code number resource public key infrastructure (RPKI) data security threat model (Communication Industry Standard/ CCSA)	Published

4.1.3 Map Data Security

For foreign companies, rigid restrictions apply to the collection, storage and processing of map data. According to the Surveying and Mapping Law[68], foreign-invested entities are not eligible for the highest-level license allowing for wide-ranging data collection and processing for survey and mapping activities.

Moreover, under the Cybersecurity Law, personal information collected or generated in China must be assessed before being transferred overseas. This creates an effective restriction for foreign companies seeking to transfer data outside of China.

Companies require special licenses, from the National Administration of Surveying, Mapping, and Geo-Information (NASG), to collect data about road conditions and the height or weight limits of bridges. In particular, they are forbidden to collect any road data around military districts.

4.2 Measures for Security Assessment of Cross-border Transfer of Personal Information (Draft for Comments 2019)

June 2019, the National Internet Information Office issued the draft of "Measures for the Security Assessment for Cross-border Transfer of Personal Information"[69]. The "Security Assessment Measures" is the implementation of Article 37 of the "Cyber Security Law". Its purpose is not to restrict the active exit behaviour of individual users, but to strengthen data localization and localization in the current global flow of data and in many countries and regions. In summary:

1. **Network operators need to report for evaluation whenever personal information is exported abroad**

   Article 3: Network operators shall report to the provincial cybersecurity administration for the completion of the personal information security assessment before any cross-border transfer of personal information. The transfer of personal information to different recipients shall require a separate security assessment for each recipient. Multiple or continuous transfers of personal information to the same recipient does not require multiple assessments.

   As long as network operators need to export personal information abroad, they need to report to the local provincial network information department for security assessment.

2. **Clarified the key security assessment content**

   Article 6: The security assessment of the cross-border transfer of personal information shall focus on the following aspects:

   - Whether the transfer complies with relevant laws and administrative regulations;
   - Whether the contractual terms with the recipient can fully protect the legal rights and interests of the personal information subject;
   - Whether the contract can be carried out effectively;
   - Whether the network operator or the recipient has a history of abusing the legal rights and interests of the personal information subject, and whether any significant network security incident has previously occurred;
   - Whether the network operator obtained the personal information in a lawful and legitimate way; and
   - Other aspects that shall be evaluated.

   This draft of 2019 distinguishes between personal information and important data compared to its 2017 draft. Article 6 stipulates the content of security assessment. It focuses

68 China Survey and Mapping Law - Apr 2017

69 Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China June 2019

more on the review and enforcement requirements of the content of the contract signed between network operators and personal information recipients, as well as past personal information protection and network security performance requirements, emphasizing the legitimacy of personal information sources and the protection of the rights and interests of personal information subjects. It no longer emphasizes the necessity of exiting the country.

3. **Fully stipulates the specific content of the contract signed by the network operator and the overseas recipient**

   The 2019 Security Assessment Draft Measures specifies specific provisions on the content of the contract, including the purpose, type, storage time limit, recipients' responsibilities, and rights of the subject of personal information. It involves many new obligations for network operators and receivers, including special institutional arrangements such as "network operators pay in advance on behalf of receivers" and "provide a copy of the contract at the request of the subject of personal information".

4. **Strengthen the supervision of overseas recipients through series design**

   In practice, for overseas recipients, due to jurisdictional issues, it is often difficult for cybersecurity and information departments to perform their supervisory duties, which is not conducive to the implementation of supervisory rules. In this draft, the supervision has been strengthened of overseas recipients through a series of designs.

5. **Clarified the guarantee for the fulfilment of the rights of personal information subjects**

   The export of personal information will affect the control of subjects, of their personal information. Therefore, regulating the rights of subjects in the situation of personal information exits can not only alleviate the concerns of subjects about the security of their personal information, but also realize personal information exit security.

4.3 Personal Information Protection: Laws, Standards

4.3.1 China Personal Information Protection Law (Expert Proposal 2019 - Draft)

In October 2019, China published a revised draft of its 2017 draft of the Personal Information Protection Law, as the **Expert Proposal**. The 2019 Expert Proposal draft integrated other Chinese personal information protection legislative regulations, such as "2013 Decision on Strengthening Information Protection on Networks", the 2009 VII Amendment to China Criminal Law, the 2015 IX Amendment China Criminal Law, the 2013 Amendment of Protection of Consumer Rights and Interests Law, 2017 China Cybersecurity Law. In addition, it is also majorly inspired from EU's GDPR, Japan's 2015 revised "Personal Information Protection Law" and other advanced foreign legal systems, responded to technological, economic and social changes, and effectively balanced the interests of multiple parties.

Summary of the law (2019 Expert Proposal Draft):

1. Chapters 1, 2, and 3 are about the general provisions, the basic regulations, the basic principles (such as informed consent and purpose limitation) and basic systems of personal information (PI) protection (such as the establishment of a PI protection standard system, certification and marking system, risk assessment, and de-identification processing), clarifying the framework for the government, enterprises, industry, society and other parties to jointly construct and maintain the order of PI protection

2. Chapters 4 and 5 are the code of conduct and stipulate the PI processing rules of information industry operators and government affairs departments respectively. Although both the information industry and the state agencies have requirements for the use of PI, their legal status, purpose of use, and usage scenarios are quite different and should not

be uniformly regulated. Therefore, two separate chapters are used for parallel regulations.

3. Chapters 6, 7, and 8 are the implementation and guarantee of PI protection. Chapter 6 is based on the concept of social co-governance. While adhering to the core position of the national cybersecurity and informatization sector, it also gives full play to the role of news supervision, social supervision and public participation. Chapter 7 establishes a dispute resolution system of PI protection led by multiple competent cybersecurity and informatization departments, through mediation, complaints, public interest litigation, negotiation, arbitration and administrative relief. Chapter 8 consists of 12 articles, that specify, the legal responsibilities of information companies, personal information protection service agencies, data transaction service agencies, network product service providers, state agencies, and regulatory agencies.

4. Chapter 9 is about supplementary provisions, which mainly defines the terms used in this draft proposal.

   However, a new draft of the Law was released recently on Oct 21st 2020. A reference translation[70] and preliminary information are provided here[71].

4.3.2 Personal Information Protection Standards

Following are some of important personal information protection standards formulated by different technical committee such as TC260, TC 543, under SAC and NGOs such as CESI.

Table 12: Personal Information Protection Standards

Project/Standard No.	Title	Status
GB/T 35273-2020	Information security technology-Personal information security specification (TC 260)	Published
20194267-T-469	Information security technology-Basic specification for collecting personal information in mobile internet applications (TC 260)	Request for comment
GB/T 37964-2019	Information security technology-Guide for de-identifying personal information (TC 260)	Published
GB/T 28828-2012	Information security technology-Guideline for personal information protection within information system for public and commercial services (TC 260)	Published
GB/T 29841.3-2013	Satellite positioning personal position information service system (PPISS)-Part 3: Information security specification (CESI)	Published
GB/T 34978-2017	Information security technology-Technology requirements for personal information protection of smart mobile terminal (TC 260)	Published

70 China's Draft 'Personal Information Protection Law' (Full Translation) - Oct 2020

71 Explanation of Personal Information Protection Law (Draft) Oct 2020

20190914-T-469	Information security technology-Guidelines for Personal information security engineering (TC 260)	Seek for approval
20173806-T-339	Telecom and Internet service User personal information protection requirements (TC 543)	Published
20180840-T-469	Information security technology - Guidance for personal information security impact assessment (TC 260)	Approval for publish

4.3.3 Overview of International PI Protection Laws

Europe

The EU PI protection model is a unified legislative model that includes a comprehensive personal information protection law to regulate the collection, processing and use of personal information. The law is uniformly applicable to public and non-public sectors, and a comprehensive supervision department is set up to concentrate supervision. In 1995, the EU passed the classic "General Data Protection Regulation". This personal information protection legislation was implemented throughout Europe, covering a wide range of aspects and a clear implementation mechanism. By virtue of this law, the EU made Europe a model of global personal information protection in terms of information protection for foreign companies entering the EU.

U.S.A.

The American model is based on the right to privacy and is a model that combines decentralized legislation and industry self-discipline. In the public domain, the United States takes privacy as the basis of its constitution and administrative law and adopts a decentralized legislation model to legislate one by one. In the private sector, the United States relies on self-discipline mechanisms (including corporate codes of conduct, private certification systems, and alternative dispute resolution mechanisms) to protect personal information. According to the specific content of personal information, it is supervised by corresponding regulatory agencies.

Japan

Considering the information protection model of Europe and the USA, Japan passed the "Personal Information Protection Act" in 2005, and achieved personal information protection in all aspects through this law. At the same time, Japan also pays attention to industry self-discipline and community participation, thus forming a unique Japanese personal information protection model which is neither the European nor the U.S.A standard.

China

As of March 2020, China Internet users have reached 900 million, with more than 4 million Internet websites, and more than 3 million applications. The collection and use of personal information is more extensive. The China laws on the protection of personal information are currently composed of myriad of specific laws, administrative regulations, local regulations and rules, various normative documents and departmental rules, etc., forming a multi-level, multi-field, sparse content, and complex system of personal information protection mode.

As China's personal information protection is not as strong as that of Europe and the United States, Chinese companies are not allowed to process personal information of European and American customers in international economic and trade transactions. Foreign financial institutions in China choose to transfer personal information of domestic customers to Singapore and the European Union for processing. On the other hand, when personal data protection is not perfected, some enterprises, foreign institutions can also obtain large-scale personal data through legal or illegal channels, such as Chinese biometric information, medical record information, etc., not only to obtain artificial industrial advantages such as intelligence and big data, but can also get subtle insights into national security, posing a potential threat to national security.

China recently revised draft of "Personal Information Protection Law", is being eagerly looked forward, to address these issues, effectively manage and fulfil different necessities of personal information protection.

4.3.4 Personal Information Protection in Mobile Apps

Summary of personal information protection in Apps[72]:

1. Measures taken to **establish** app data security and personal information protection system:

- The "China Cyber Security Law" clarifies Chinese basic principles and framework of individual information protection, strengthen the protection obligations and responsibilities of network operators.

- The Ministry of Industry and Information Technology specially formulated the "Provisions on the Protection of Personal Information of Telecommunications and Internet Users", which clearly specified the scope of protection of personal information of telecommunications and Internet users in the industry, principles and rules for the collection and use of users' personal information, security measures, and supervision and inspection systems.

- The Cyberspace Administration of China issued "Regulations on the Management of Mobile Internet Application Information Services" in June 2016, which clearly requires mobile app providers to establish and improve user information security protection mechanisms; not to collect geographic locations without expressly indicating to users; only with user consent , read the address book, access the camera, enable recording and other functions; not open mobile functions not related to service, and do not bundle and install unrelated applications.

- The Ministry of Industry and Information Technology also issued the "Interim Provisions on the Pre-setting and Distribution Management of Mobile Smart Terminal Application Software" in December 2016.

2. Measures for **enhancement** measures for app data security and personal information protection supporting standard:

- The Basic Requirements for Information Security Technology -Network Security Level Protection was issued in May 2019. The requirements for app level protection were put forward for the first time in its request.

- The "Required Information Specifications for Basic Business Functions of Mobile Internet Applications" released in June 2019, focuses on the basic business functions of 16 commonly used apps such as **map navigation, online ride-hailing,** instant messaging, **online payment**, news information, online shopping, and short videos; defines the scope of personal information necessary to ensure its normal operation, and provides practical guidelines for the collection of personal information.

- The "Information Security Technology and Technology Mobile Internet Application Basic Specifications for the Collection of Personal Information (Draft)" released in August 2019, put forward more detailed management and technical requirements for the collection of personal information by apps. The promulgation of relevant standard documents regulates the various behaviors of the app's collection, use, storage, transmission, and destruction of personal information, and provides evaluation standards and basis for relevant agencies.

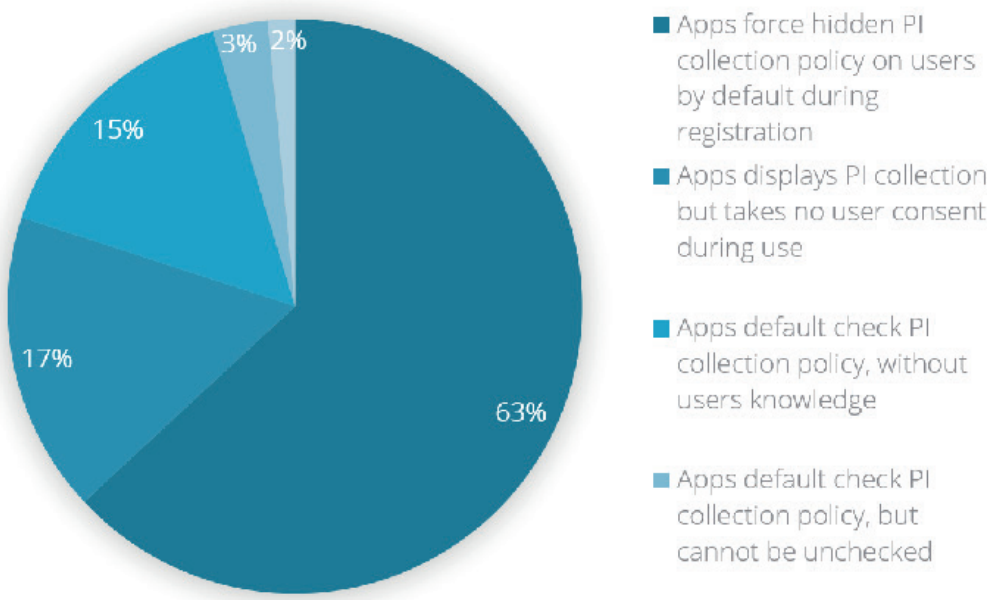
In Nov 2019, CAICT's, Security Research Institute, conducted research76, that selected and tested mobile apps from 20 categories such as social communications, food delivery, **map navigation**, live video, online shopping, **online car-hailing**, medical education, etc. from 10 Android app markets including App Store, Huawei App Market, and Xiaomi App Store. Among the 20 categories, around 200 apps with large downloads, wide impact, and typical problems, were tested, and a total of 1265 data security issues were detected. The risks related to the protection of users' personal information of the investigated apps are as follows:

72 CAICT Mobile Apps : Data Security and Personal information protection whitepaper Dec 2019

1. Many inquiries on personal information by default, risk of data collection violations:

   Although more than 90% of the apps have privacy policy, but more than half of the apps informed their privacy policies in concealed or vague manner, rather than explicit, when users log in for the first time. 63.1% apps force users to agree to their privacy policy by means of compulsory "logging in/registering" without providing a rejection option. If users want to continue to use, they have to passively agree to the privacy policy, which violated user's right to choose; 16.9% of the apps only displayed the privacy policy during use but did not ask for the user's consent, which violated the original intention of formulating the privacy policy; 15.4% of the apps provided a check box for whether to agree to the privacy policy, but there was a default check box problem.

Figure 12: Scenarios among apps investigated with implicit user PI collection



Above figure (Figure 12), 1.5% refers to apps that provide dis-agree option to policy.

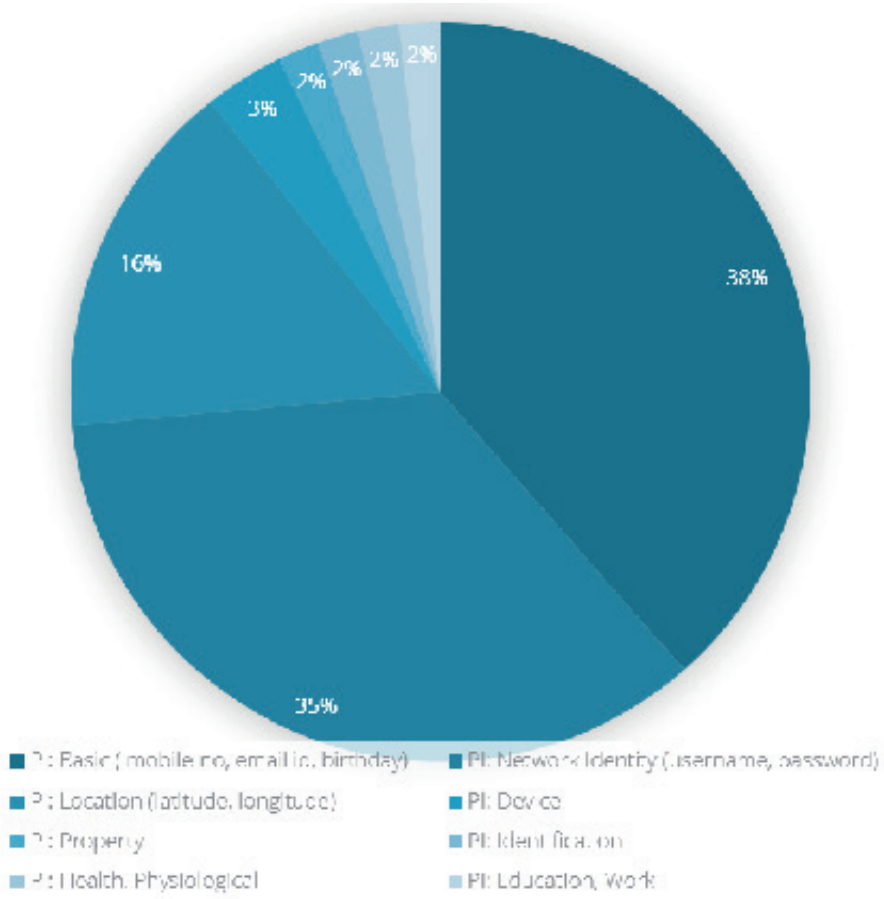
2. Excessive request for personal permissions, risk of malicious abuse of data:

   Nearly 30% of apps applied for more than 10 permissions related to the collection of personal information, and some financial apps had as many as 14-16 permissions, and the personal information collected far exceeded the guidelines set by the "Network Security Practice Guidelines-Scope of Necessary Information for Basic Business Functions of Mobile Internet Applications".

3. Personal information stored in plaintext, risk of illegal data acquisition:

   More than 90% of apps, store data such as operation logs, device information, and user information in the user phone, but 25% of them stored in plaintext. The types of personal information stored in plaintext included, network identity around 35%, which mostly included account and password; personal basic information around 38.6%, mainly including user mobile phone number, email address, birthday, etc.; accurate positioning information around 15.8%, mainly including latitude and longitude coordinates of the user's location.

Figure 13: Proportion of different user PI stored as plaintext in 25% of investigated apps



In above figure (Figure 13), remaining proportions of 1.8%, represent personal health and physiological information and personal education work information respectively.

4. Sharing user data, risk of malicious dissemination of data:

   In 40% of apps, it was found, when they jumped to third-party apps, users were not reminded of third-party personal information collection and use rules. The redirected third-party applications are mainly finance and online shopping, both taking up for 31%. Financial third-party apps are susceptible to virus infections, malicious counterfeiting and privacy stealing, which can easily lead to the leakage of user's sensitive personal information and even cause economic losses; online shopping third-party apps have excessive use of user personal information, tracking user behavior, and malicious scenarios such as theft of transaction information.

5. Restrictions on logging out, risk of data retention:

   20.5% apps do not provide logout function. 26.9% apps that provide a log-off function, but takes a long time and the process is tedious. Also, it was found necessary, to submit additional non-essential personal sensitive information, such as the user's real name, address, email address, ID photo, etc. The apps operator did not clarify whether the additional information will be deleted after logout. Compared with the simple registration process, a large number of unreasonable conditions are set for users to cancel their accounts, which prevents users from exercising their right to cancel.

4.3.5 Personal Information Protection in "Internet+"

In 2015, the State Council issued the "Guiding Intent on Actively Promoting the "Internet +" strategy3, driven by the new situation where the Internet has accelerated its penetration into traditional industries."Internet + e-commerce", "Internet + travel services", "Internet + smart home", "Internet + medical and health" and other new formats have developed rapidly and personal information protection has become increasingly prominent[73].

- With respect to automotive industry, in the field of "Internet + travel services", the Ministry of Transport and the Ministry of Industry and Information Technology published the "Interim Measures for the Administration of Online Taxi Reservation Service Management". It put forward relevant regulations on the protection of personal information of drivers and passengers. **Article 26** of Interim Measures clearly states that "online car- hailing platform" companies shall, through their service platforms, inform in a significant way the purpose, method and scope of the collection and use of personal information to drivers, car hirers, and passengers. Without, the subject's express agreement, the company shall not use the personal information for other businesses. The company shall not exceed the "personal information collection" scope, then necessary, to provide its services. Except for cooperating with state agencies to exercise supervision, inspection or criminal investigation, in accordance with the law, companies shall not provide any third party with the names, contact information, home addresses, bank accounts or payment accounts, geographic locations of drivers, car hirers and passengers. Personal information such as location, travel routes, etc., shall not disclose geographical coordinates, geographical landmarks and other sensitive information related to national security. After the information leakage occurs, the online car-hailing platform company shall promptly report to the relevant authorities and take timely and effective remedial measures.
- In addition, the transportation industry standard, JT/T 1068-2016 "Online Taxi Reservation Operation Service Specification" in Chapter 4.4 provides the requirements for the security of online car-hailing information, including the information security system, collection, use, and destruction.
- With respect to NEV, personal information protection is relatively new issue. It presently appears there are certain restrictions in place on collection of user personal information against collection of vehicle data.

In order to control the safety and rationality of their operations, the Chinese government will monitor some information such as vehicle repairs, maintenance, battery, motor and electric control system products, hereinafter referred to as the Electronic Instrument Cluster, EIC system. This is mandatory monitoring by the Chinese government, thus the OEMs have no right or control about it. For instance, it is understood that, some pure electric vehicles cannot be sold in Beijing and other regions without installing monitoring equipment such as driving recorders. The reason for the introduction of this regulation is for safety and to prevent fraudulent replenishment of pure electric vehicles.

In order to ensure safe production and operation, the state forces electric vehicles to upload daily use, repair, and maintenance data and vehicle dynamic monitoring data to the new energy vehicle data government collection/monitoring platform, but user accounts, user nicknames and other information will not be uploaded. The purpose of data use is also strictly controlled and is only used for national operation monitoring and enterprises to provide users with basic services.

73 CAICT's Internet + industry" personal information Protection Research Report – Mar 2020

Figure 14: Shanghai EV Public Data Collecting, Monitoring and Research Centre[74].

There has only been one reported scrutiny on OEMs vehicle PI protection. In October 2018, NIO E8S, concerns were raised, that its in-vehicle camera system and microphone are "spying at all times". NIO had to assure users, that the hardware worked only after the user activates. In addition, NIO also desensitized and encrypted the stored data, and assured expiration will never be traced back.

4.4 Summary

China Data Security and Personal Information Protection Law are shaping into national level laws and are complementary to Cybersecurity Law. Due to its evolving nature and in places, abstract content, it is difficult to discern and interpret its applications not only to NEV security and privacy, but also other use-cases. Where possible, legal help must be sought. Also, it is important to continuously monitor China's privacy landscape to get deeper clarity on its application and implications. This chapter was an attempt to introduce and cover relevant aspects and present insights where possible.

74 Financial Times - China demand for electric vehicle data raises privacy issues - Nov 2018

V China IoV Security – Academic Survey

5 China IoV Security – Academic Survey

At present, IoT, AI, 5G network, cloud computing, big data technologies are developing rapidly, and gradually being applied to EV and ICV's.

As EV and ICV's move from the present closed system to open internet, it brings out severe challenges of cyber security. Remote attack, malicious control, data privacy and other security risks become potential threat for the car, road, environment, and human life. The number of annual security incidents increased by 605% since 2016 and more than double in 2019[75]. In 2019, 57% of incidents were carried out by cybercriminals to disrupt business, steal property and request ransoms. 38% of the cases warned the companies and consumers for the bugs i.e. white ethical hacking.

In 2018, there were 14 information security incidents of ICV's worldwide, including 5 data leakage incidents and 9 car hacking incidents. Automobile information security has entered the era of "brushing vulnerabilities". In the past years, many automobile manufacturers have also been troubled with vulnerabilities. More and more automobile-related vulnerabilities have obtained CVE numbers. The attack surface has shifted from automobile terminals to the cloud. The business has had a sizeable impact, and the problems exposed are many. Example, data breaches, in July 2018, more than 100 confidential documents from automakers including Volkswagen, Tesla, Toyota, Ford, General Motors, Fiat Chrysler, etc. were exposed. It involved content ranging from car factory development blueprint planning, factory principles, manufacturing details, to customer contract materials, work plans, to various confidentiality agreement documents, and even private information such as scanned copies of employee driver licenses and passports, totaling 157 gigabytes, containing nearly 47,000 files.

Therefore, cyber and information security of EV or ICV has attracted great attention. Cyber security plays a fundamental role in protecting and guaranteeing and is a prerequisite for the integrated development the vehicles, transportation and smart cities system.

75 https://www.helpnetsecurity.com/2020/01/06/automotive-cybersecurity-incidents/

5.1 Domestic Summits and Conferences in Automotive Security (2017-2020)

There are quite a few local conferences, summits, seminars on automotive security. These are conducted and attended in large numbers by representatives of domestic and foreign OEM's, government and academia in China. A few notable ones are mentioned below.

Table 13: Local Summits and Conferences in Automotive Security (2015-2020)

Date	Organizer	Conference/Summit	Topic
Feb 2017	Shanghai Chuangshi Tuoyuan Investment Consulting Co. Ltd	2nd China Automotive Network Information Security Summit[76]	Security issues of vehicle communication interface and ECU exchange.
May 2017	Automotive Information Security Committee	China Automotive Security Evaluation Regulations Seminar[77]	Promote industry adoption of automotive security evaluation procedure and system
July 2018	MIIT and CAC	China Network and Information Security Conference[78]	National Security Talent Training, Cybersecurity Legal Risks and Compliance, IoT and IC Innovation and Security Development
Oct 2018	BaiDu	Autonomous Driving Information Security Seminar[79]	Emphasis strengthening automotive security to increasing vulnerabilities.
Jan 2019	Shanghai Suoya Automobile Technology Co. Ltd.	4th China Automotive Network Information Security Summit[80]	TEE, Vehicle E&E Security Architecture, Privacy Protection
Aug 2019	SAE International	SAE-AWC 2019 Autonomous Vehicle Safety Technology Conferenc[81]	Other than functional safety, addressed topics on autmotive network security

76 https://www.sohu.com/a/126920958_193867
77 https://www.sohu.com/a/145216411_696625
78 https://www.sohu.com/a/243201581_100160034
79 https://baijiahao.baidu.com/s?id=1613846062445028083&wfr=spider&for=pc
80 https://www.sohu.com/a/288820610_566219
81 https://www.sohu.com/a/337527946_297649

Sept 2019	China Software Evaluation/Test Center (CSTC)	Information Security of Internet of Vehicles[82]	Research progress on connected vehicle security
Sept 2019	CATARC, MIIT, CSTC	6th meeting of the Automobile Information Security Standards (CS) Standards WG[83]	Progress on the ten important EV security and EV charging security standards
Oct 2019	CATARC	2nd meeting of Automobile Security Regulations WG[84]	Domestic and international policies and regulations on automobile security, security management, risk assessment and ICV trust.
March 2020	Artisan Exhibition and NewCar	Smart Car Information Security Conference AutoCS 2020[85]	Commercialization challenges of the automotive security market
July 2020	SAE International	ICV Information Security Knowledge Seminar[86]	ICV security basics, SAE J3061 ICV Security Guidelines, Security Offense and Defense, Security SDLC, threat intelligence and situational awareness
Nov 2020	Shanghai Suoya Automobile Technology Co., Ltd.	China Automotive Network Information Security Summit[87]	Implementation of UN regulations in various countries, and the future outlook of ICV's.

82 https://wemp.app/posts/73946927-4309-4e75-9e2d-5062cb385dc5

83 https://www.gongkongke.com/posts/4yCufisRXWLR/

84 http://www.catarc.info/news/6714.cshtml [Last Visited:05/07/2021]

85 https://www.sohu.com/a/348393095_560056

86 https://www.sohu.com/a/385409959_297649

87 http://www.grccacss.com/

5.2 Industrial and Academic Initiatives to IoV Security Challenges (2015-2020)

OEM's in China are increasingly developing and having dedicated teams to address cyber security issues. The following table (Table 14), mentions some of the activities and responses, in the past 5 years, by major OEM's, Tier1 suppliers and internet security companies in China or their overseas subsidiaries, to address cyber security challenges in IoV's.[88]

Table 14: Industrial and Academic Initiatives on IoV security challenges

Organization Type	Name	Activity	Description
OEM	Tesla	Bug Bounty	Cash rewards for professionals and security companies that submit vulnerabilities. Established, a Security Hall of Fame.
	NIO	Platform Solution	Since 2017, NIO formed a large-scale information security team, and built a centralized, unified, complaint information sharing platform with secure identity authentication
	BYD	Partnership	In September 2018, BYD and 360 signed a strategic cooperation agreement to discuss and integrate relevant resources in automotive information security and network security of smart cars.
	DongFeng	System Security	In March 2019, DongFeng adopted, an IPD2R model (Identify, Protect, Detect, Response, Recovery) to address automotive security. It gradually established information security level protection test system to improve the layout of its security.
	XiaoPeng	Network Security	In 2019, XiaoPeng G3 model, adopted separation of the vehicle control network and the in-vehicle entertainment network as a security measure. Communication between its systems was subject to strict vehicle identity authentication and user authorization.
	Weltmeister	Partnership	In January 2019, Weimar Automobile and Baidu signed strategic partnership to develop security services, among other services, as a part of its autonomous driving solution and develop a joint smart car R&D center.
	GAC	T-Box Security	Since 2017, GAC introduced T-BOX intelligent vehicle-mounted terminals for its Trumpchi models. It provides a series of remote monitoring and operation functions including security services

88 Suggestions on Information Security and Development of Intelligent Connected Vehicles, Hou Xintan, Gao Hong, CATARC, 2020

TIER1 (overseas)	Continental	Network Security	In 2018, Continental Group with Argus and Elektrobit, released an end-to-end network security and wireless software update (OTA) solution.
	NXP	Hardware Security	NXP implemented several solutions to ensure information security viz. including cryptographic algorithm accelerators, key management, building a secure boot trust chain, runtime integrity checking, and instant encryption/decryption engines.
	Bosch	Network Security	In 2017, Bosch demonstrated the protection scheme of Escrypt intrusion detection based on the geographical isolation of the central network.
Internet and Security Company	360	Security Platform, Vulnerability Research	The company established an Intelligent Connected Automobile Security Department specializing in automobile security. In June 2018, it developed a security early warning system called the "Automotive Security Brain". 360 was included in Tesla's "Security Hall of Fame" three times, for its research in finding vulnerabilities.
	Baidu	Network and System Security	In November 2018, Baidu in its Apollo platform, developed an information security product called "Apollo Vehicle Security Defense system". Apollo presently provides complete range of automotive information security solutions, products and services.
	Tencent	Vulnerability Research	Tencent's, Keen Security Lab undertakes security research in Internet of Vehicles, focusing on vehicle network vulnerabilities.
	Venustech	Vulnerability Research	A provider of conventional cyber and network security products and solutions, promoted and developed an Internet of Vehicles Vulnerability Database.

5.3 Corp and Academic Labs: Research Highlights in IoV Security (2015-2020)

In order to strengthen the cyber security capability of Internet of vehicles, domestic enterprises and academic and research institutions established a number of security laboratories:

1) Keen Security Lab, Tencent[89]

Tencent's Keen Security Lab was established in January 2016, focusing on leading-edge security offensive and defensive technologies for operating systems, web and mobile applications, cloud computing, and IoT devices. In ICV security, the lab has discovered and assisted OEM's to repair multiple security vulnerabilities. One of its research highlights, it found two vulnerabilities in the wireless function module (Parrot module on Tesla Model S), one in the wireless chip firmware, and other in the chip driver and showcased a remote hack into the Tesla vehicle system. Vulnerabilities were reported to Tesla in 2019, and fixed subsequently. Marvell also fixed the reported vulnerability and subsequently issued a security bulletin.

89 Tencent Security Keen Lab

2) 360 ICV Security Center[90]

The 360 Internet of Vehicles Security Center was established in November 2016 by 360 in conjunction with universities and automotive companies. It is the first cross-industry cooperative center specializing in the security protection of automobiles and connected vehicles in China.
The Center has 2 research teams in attack and defense, 3 laboratories, 1 joint research institute, and a professional security service team. It has developed security and testing products like 360 automotive guards and CANPICK. Its "360-vehicle security operation platform", based on big data security, is the first comprehensive operation platform for automotive information security in China. The platform provides security threats to the automotive and the network security industry. One of its research highlight, it demoed hack on Tesla's autonomous driving system and presented at the World Hacking Conference DEFCON.

3) CATARC ICV Information Security Laboratory[91]

In March 2017, CATARC established an industry level laboratory in automotive security test and evaluation. The laboratory is owned by CATARC's subsidiary Automotive Data of China Co. Ltd. Relying on its strong scientific research strengths, the lab, implements China automotive security evaluation regulations and provides independent, third-party services to the automotive industry. Following are some of its undertaken work:

- Completed the first domestic automotive information security testing – Feb 2018
- Released "Automatic Driving Function Test Regulations for ICV's" – Apr 2018
- Won the SAE Best Paper Award for "Automobile Intelligent Index and Evaluation Method" – Aug 2018
- China Intelligent Network Automobile Industry Monitoring Report (Phase I & Phase II) – Oct 2018
- Automotive Information Security Blue Book Compilation – Nov 2018 at China Automotive Information Security Symposium
- "Automotive Automated Driving Technology Roadmap" – Feb 2019 at Information Security Technology Seminar

4) Apollo Information Security Lab (Baidu and CATARC, CAICT)[92]

In 2018, Baidu, CATARC and CAICT established Apollo Automotive Information Security Laboratory. China FAW Group, Chery Automobile, Beiqi New Energy, Tsinghua University, Beijing University of Aeronautics and Astronautics and Beijing Institute of Technology formed the first batch to jointly study related topics in intelligent driving information security and accelerate its development in China.

5) Automobile Information Security Lab (Baidu and Automotive Data of China Co. Ltd)[93]

In November 2018, Baidu and the Automotive Data of China Co. Ltd established the "Automobile Information Security Lab" in Tianjin. The laboratory focuses its research on offensive and defensive security and aims to become a key, industry-level laboratory for security testing and evaluation. Its research also focuses on developing security tools and products, vulnerabilities and penetration testing.

6) Automobile Security Lab (Baidu and BAIC New Energy)[94]

In December 2018, the Automobile Information Security Lab was jointly established by BAIC New Energy and Baidu. BAIC role is vehicle design and development, and Baidu provides for automotive information security solutions. The lab aims to develop security solutions for BAIC's autonomous driving L2.5, L3, and L4 level models.

90 360 ICV Security Center
91 CATARC Automotive Information Security Laboratory - Apr 2018
92 Apollo Information Security Lab
93 https://www.sohu.com/a/275816307_114771
94 http://www.caam.org.cn/chn/3/cate_79/con_5220931.html

7) ICV Security Lab (CAERI and CNCERT)[95]

In November 2019, ICV Security Laboratory was jointly established by China Automotive Engineering Research Institute (CAERI) and the National Computer Network Emergency Response Team, Coordination Center (CNCERT/CC) in Beijing. CNCERT has unique network security resource capabilities. It is presently improving the national-level IoV security emergency guarantee system and assessing industrial application scenarios. CNCERT has developed a comprehensive automotive security vulnerability database and efficient automated security testing platform.

8) ICV Information Security Training Laboratory (360 and Nanjing University of Science and Technology)[96]

In May 2020, 360 Enterprise Security Group reached a cooperation with Nanjing University of Science and Technology to establish a team of professionals focusing on teaching and research of ICV security. The lab assesses and trains talented students in ICV security, co-publishes security textbooks, provides technical services, supports research and innovation and building independent IPR rights and standards system in IoV security, and supports transformation of research prototypes into commercial products, and their subsequent promotion.

Ethical Hacking Works: Following are few of the published vulnerability, white ethical hacking works by domestic internet and security companies.

- Jul 2015, 360 published security vulnerabilities of BYD's vehicle model "Qin".
- Mar 2017, A hacker published analysis results (vulnerabilities) of OEM SAIC-VW's Navi "Tianbao 187A" on a hacker forum.[97]
- July 2019, 360 demonstrated relay attack on keyless system.[98]
- Aug 2019, Baidu made a speech in Black Hat US 2019 on general security issues of off-the-shelf 4G modules, used in vehicles.[99]
- Apr 2020, Tesla server certificate expiration caused customer's app to stop operating in China.[100]

5.4 ICV Non-Govermental Organizations

In this section, important NGO's for connected vehicle security are presented.

5.4.1 TIIA: Telematics Industrial Application Alliance

- **History:** TIAA established in February 2010, in Beijing, is a NGO committed to applying advanced electronic information technology to the fields of automobiles and transportation.
- **Supported by:** MIIT, MOT, MPS etc., 17 government bodies approve projects and provide guidance.
- **Members:** including over 300 members and nearly 200 observers in fields of OEM, agricultural machine, E-bike, electronic, software, communications and information service.
- **Organization:** 3 branches (unmanned agricultural union, E-bike union and smart charging & parking union);

95 CAERI-CNCERT/CC Vehicle Security Laboratory, Dec 2019
96 http://www.yangtse.com/content/933264.html
97 https://www.freebuf.com/geek/129160.html
98 https://zhuanlan.zhihu.com/p/28052451
99 https://www.blackhat.com/us-19/briefings/schedule/index.html#all-the-g-modules-could-be-hacked-16187
100 http://auto.ce.cn/auto/gundong/202005/15/t20200515_34910839.shtml

11 committees including Market service, Engineering application, Standard, IPR; Engineering application committee consists of 8 WGs including telecommunication, radar & sensor, micro-power. 2 institutions: Intelligent Automobile Research Institute (Chengdu) cluster and Anhui Province IoV Research center.

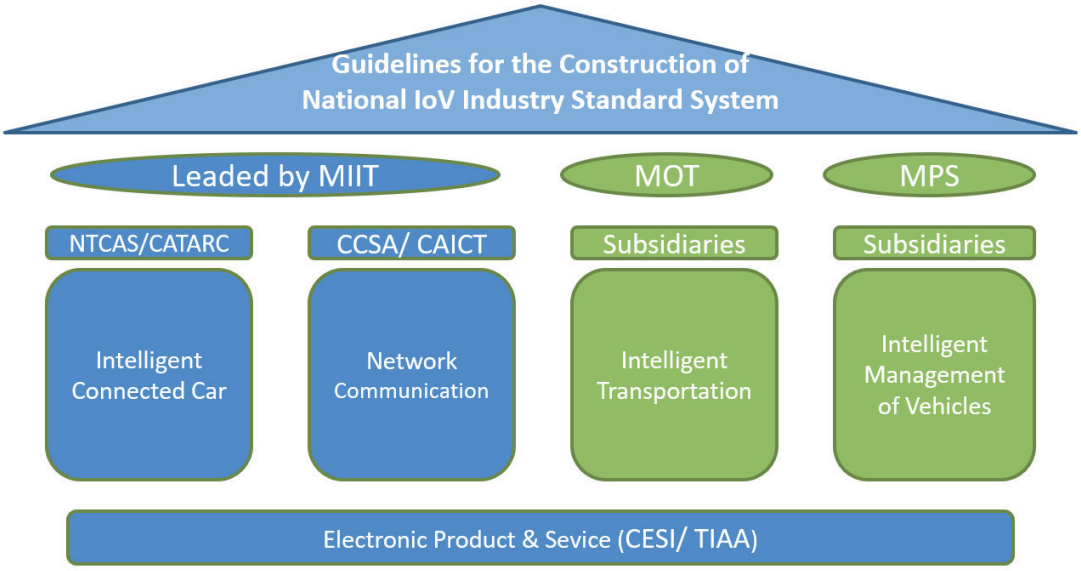
- **Achievements:** 50 state projects, 40 standards, the products which meet TIAA standards has been used in millions of vehicles.

In 2013, TIAA established an in-vehicle information security team, and yearly TIAA in-vehicle information security conference. It has issued "Internet of Vehicles Cyber Security White Paper" and "IoV Internet Security Implementation Guidelines" to actively promote the implementation of the IoV security. It actively supports the Chinese government's WTO/TBT related work to safeguard the sovereignty and security of China's Internet of Vehicles cyberspace.

Some of its relevant technical standard security projects include.

- Intelligent Vehicle and Intelligent Transportation Application Demonstration Based on Mobile Broadband IoT,
- Information Security of Official Vehicles,
- Commercial Vehicle Positive (Passive) Dynamic Security Integration Technology Program,
- Integrated Standardization of Electric Vehicles, Intelligent Traffic Radio Frequency Research and Testing,
- Networking Security of Electric Bicycle

Figure 15: TIAA: National Planning of IoV Industry in China



5.4.2 CAICV: China Intelligent Connected Vehicle Industry Innovation Alliance

The China Intelligent Connected Vehicle Industry Innovation Alliance (CAICV) was established in June 2017, and the Ministry of Industry and Information Technology served as the alliance's guidance unit. China Society of Automotive Engineers and China Association of Automobile Manufacturers are the governing units. The alliance has carried out work and achieved important results in policy and strategic research, research and development of key common technologies, standards and regulations, test demonstration, industrialization promotion, academic exchanges and international cooperation, and personnel training.

CAICV established the Automotive Information Security Working Group, which is committed to promoting automotive

information security strategy, management and organization implementation, technology and industry landing. The working group focuses on applications of traditional information security technology in automotive, roadmap of automobile information security, development process of automobile information security, architecture of automobile information security system, R&D of automobile information security testing tools, automobile information security standards and patent clusters. Its published a white paper on" Information Security of Intelligent Connected Vehicles", which established the methodology for information security of ICV's for the first time.

5.4.3 C-ITS: China Intelligent Transportation Industry

China Intelligent Transportation Industry Alliance (C-ITS) was formally established in September 2013. The alliance was led by the Highway Science Research Institute of the Ministry of Transport, large-scale intelligent transportation-related enterprises and universities, and standard committees at home and abroad. The composition of scientific research units aims to further promote the industrialization, standardization, testing services and applications of intelligent transportation systems. The Alliance is a member of the Asia-Pacific Intelligent Transportation Association and a member unit of the Intelligent Transportation World Congress. It is an international window in the field of intelligent transportation for China.

CITS established Transportation Information Security Working Group in 2018. The working group constitutes members from Beihang University, Highway Research Institute, Qihoo 360, China Telecom, and Huawei, among others. The working group focuses on the construction of transportation information security standard system.

5.5 Summary: ICV Security Standards and Roadmap

Till 2025, China will release the entire standards system (around 100 national standards) for ICV in cybersecurity (27 standards), V2X, functional safety, ADAS etc. Till 2020, China completed the first stage ICV cybersecurity standards to support driver assistance and low-level autonomous driving. Currently, 11 cybersecurity national standards have been either finalized or in the draft discussion stage and remaining 16 are to be developed in 5 years.

The roadmap of the Chinese government is as follows:

1. In 2017, MIIT and the National Standardization Management Committee jointly issued the "Guidelines for the Construction of the National Internet of Vehicles Industry Standard System (Intelligent Connected Vehicles)".
2. In 2018, MIIT issued the "Internet of Vehicles (Intelligent Connected Vehicles) Industry Development Action Plan", which mentioned three aspects of automotive information security: perfecting the security management system, enhancing the security protection capabilities, and promoting the development of security technology methods construction.
3. In April 2020, MIIT issued the "Key Points for Standardization of Intelligent Connected Vehicles in 2020", proposing to accelerate the improvement of the standard system for intelligent connected vehicles, and establish an ICV standard formulation and implementation evaluation mechanism.

5.6 Gaps in IoV Security: Academic Standpoint

With the deepening development of the IoV industry, need for security protection is common concern in academia and automotive industry. In 2017, the Chinese Academy of Information and Communications in cooperation with CATARC, and domestic OEM's, jointly published the Internet of Vehicles Network Security White Paper[101]. This white paper focused on the status of vehicle network security, provided threat analysis and protection strategies for ICV's, mobile applications, IoV service platform, communication security, data security and privacy protection. Below, mentioned are some of the broader gaps in IoV security ecosystem, from academic viewpoint,

1. Barriers in Laws, Policies and Standards

Due to the obstacles in policy and regulations, EV, EV charging and ICV enterprises are lagging in comprehensive system-level security solutions. Also, there is need to improve cyber and privacy security standards, further enhance national cyber security laws and regulations and establish strong privacy and data protection laws as soon possible.

2. Lack of Unified Supervision Platform

At present, the security testing methods and judging standards for EV/ICV have not yet been unified. The number of vulnerability database samples are not enough and threat intelligence cannot be communicated. OEMs and suppliers find it difficult to verify the security and reliability of their products, tools and services.

For vehicle operational security supervision, there is lack of credible security monitoring platform with rich data resources in China. The test results and monitoring data cannot be effectively recognized and shared. Therefore, there is need to increase investment in security supervision platform development.

3. Need for Multi-Layer Defense Solutions

Most of the cyber security protections are observed to be concentrated on the T-BOX, OBD or IVI. Some potential known security risks include malicious physical or wireless OBD port access, illegal access to vehicle RFID Tag, insecure external T-BOX communications, illegal access to TPMS, insecure on-board vehicle data storage methods, inefficient implementation of user identity authentication and access rights in IoV cloud.

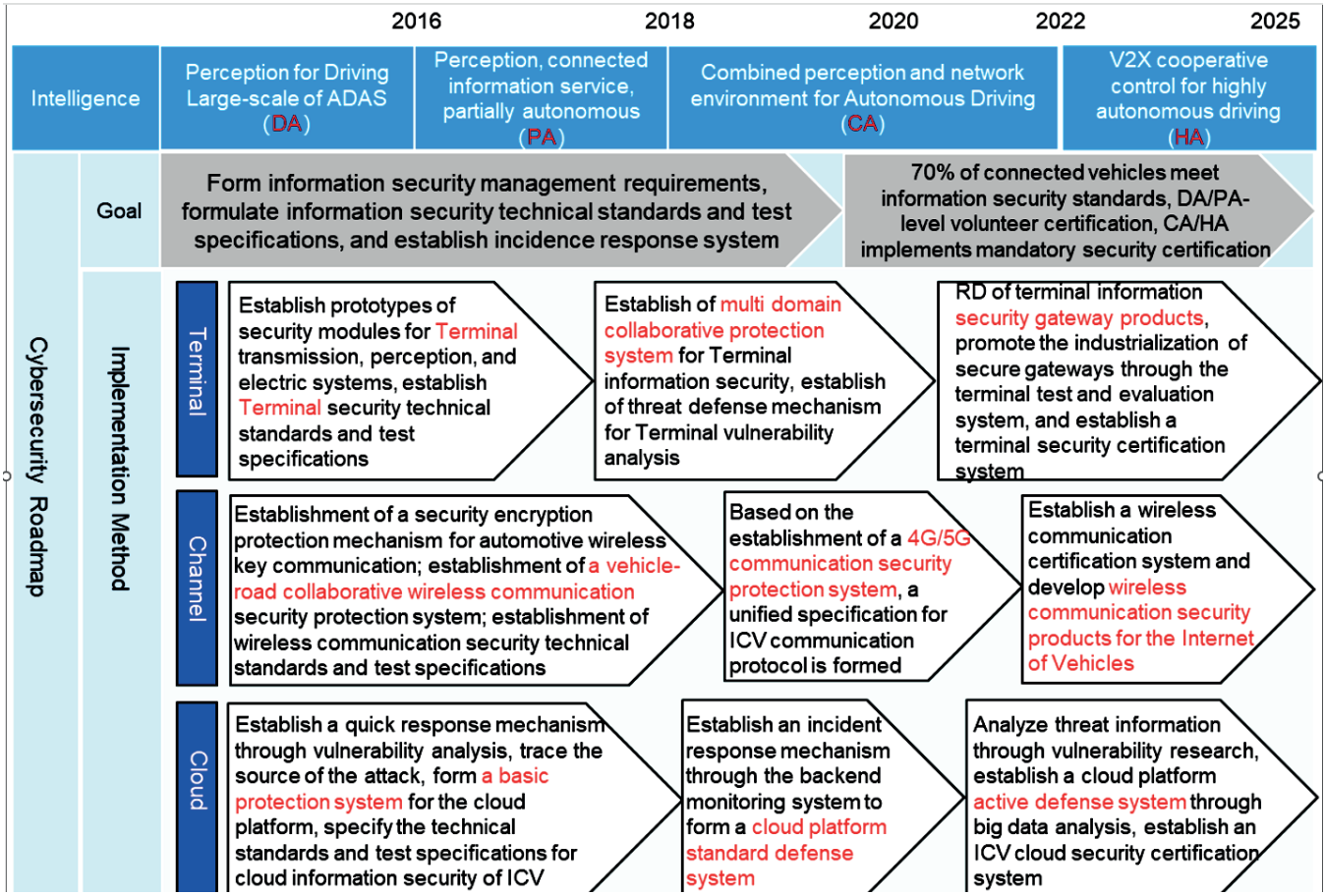
There is a need for a multi-level protection system (protections on IoV terminal layer, network layer, application layer). Increased adoption of protection measures is required to reliably acquire data of different data types from IoV node layer. Adoption and enforcement using authentication codes, hashes and IPSec, SSL like encryption, for integrity and confidentiality of data transmission from IoV network layer. Automotive firewalls and intrusion detection systems should be increasingly deployed in IoV application layer. Besides, the security level of stored user data in the vehicle database needs enhancement and management in an increasingly classified manner.

Based on above model (terminal-channel-cloud), a roadmap[102] for development Internet of Vehicles Security System was jointly developed by several state and industrial IoV companies.

101 Internet of Vehicles Network Security White Paper - 2017

102 http://www.its114.com/html/news/survey/2017_02_83937.html

Figure 16: Roadmap of IoV Security



4. Automotive Security Tools

More credible automotive security testing methods and tools, communication protocol analysis and threat warning tools need to be developed. Besides vehicle data is also not effectively used and applied.

At present, domestic enterprises are strengthening their own capabilities in threat warning, security protection and emergency response by mining bugs, establishing security knowledge base and issuing intelligence.

VI IoV Security and Privacy: Outlook and Trends

6 IoV Security and Privacy: Outlook and Trends

6.1 EV Charging: Trends and Gaps

6.1.1 EV Wireless Charging

Standards: Currently, China is in early phase of wireless charging for EV. In May 2020, SAC published four national standards for wireless charging of electric vehicles.[103]

1. "Electric Vehicle Wireless Charging System Part 1: General Requirements" (GB/T 38775.1)

2. "Electric Vehicle Wireless Charging System Part 2: Communication between Vehicle Chargers and Charging Equipment Agreement" (GB/T 38775.2)

3. "Electric Vehicle Wireless Charging System Part 3: Special Requirements" (GB/T 38775.3)

4. "Electric Vehicle Wireless Charging System Part 4: Electromagnetic Environment Limits and Test Methods" (GB/T 38775.3) T 38775.4).

These standards only fulfil the basic requirements for wireless charging technology in China. Till 2025, China will develop 10 national standards for wireless charging to promote the technology.

Presently, OEMs such as FAW, BAIC, GAC, SAIC and BYD have already carried out R&D. ZTE New Energy and Yutong had earlier launched China's first wireless test charging station[104]. In August 2018, the State Grid Corporation approved projects of "Development of key technologies and equipment for EV mobile wireless charging system" and "Experimental road section for EV mobile wireless charging". The length of the wireless charging road built was 181 meters, mobile wireless charging power 20kW and the conversion rate reached 80% and the driving speed 60km/h. This experiment also demonstrates feasibility of mobile wireless charging for electric buses.

6.1.2 C-V2X and 5G IoV Development in China

Chinese Internet of Vehicles market is increasingly seeing more activities in C-V2X (Cellular-V2X). China has already established policy for C-V2X Internet of Vehicles. Before 2019, the national standard was formulated, and the spectrum was allocated. Since 2020, China has also developed new infrastructure for 5G Internet of Vehicles and released "Smart car innovation development strategy" to support next 30 years of development. Volkswagen, FAW, Dongfeng, Changan, and SAIC vehicles, equipped with Huawei LTE-V2X in-vehicle terminals have demonstrated V2X smart transportation scenarios. Audi China, BAIC, Changan, Geely and Great Wall Motors have demonstrated V2V and V2I use-case scenarios based on the Qualcomm 9150 C-V2X chipset and Datang's LTE-V2X module DMD31. It is expected, that China C-V2X market will continue to have strong growth.[105] Summary,

1. One standard: C-V2X is the only car networking technology standard in China[106] and is increasingly getting support from the global industry.

103 https://www.greencarcongress.com/2020/05/20200508-witricity.html

104 http://news.ccidnet.com/2020/0528/10527302.shtml

105 Prospects of top ten application trends China, Jan 2020, International Electronic Business

106 Development and Prospects of 5G Internet of Vehicles, CAAM, July 2020

2. Integration: To promote autonomous driving; 5G and C-V2X integration, are considered complementary to create 5G car networking;

China is also speeding on development of V2X security standards, because

1. Government prefers development towards cryptographic and critical infrastructure security.

2. More and more industry activities are focusing on ICV-V2X applications and EV Charging Infrastructure.

6.1.3 5G and Bi-Directional Charging (V2G)

In 2019, China had successively started development of 5G networks, and the subsequent launch of its commercial services. For the charging pile industry, development of 5G is key technological upgrade, as it will speed up the development, efficiency of charging pile networks, and also improve the user experience of charging pile services and increase application scenarios. With 5G, V2X is set to become popular, including V2G, V2I, V2H, and V2V.

Due to absence of standards/regulations, Bi-Directional charging or V2G (Vehicle to Grid) is still in early phase in China. In June 2020, Weimar Motors and State Grid jointly began to promote the applications of V2G. Weimar Motors successfully passed the vehicle, pile and road test for V2G, and taken lead in developing its applications.

6.2 EV Charging Infrastructure Security Gaps

Some of the broader security gaps in China EV charging infrastructure:

Gaps	Description
Lacks cybersecurity testing	There is a lack of formal cybersecurity testing and assessment of EV charging infrastructure.
Insecure payment via mobile apps	Several risk points of mobile apps: No compilation, clear text transmission and storage of key data, etc.
Security risks in monitoring platform	No access control strategy, weak border protection measures, lack of security configuration strategies,
Standards and regulations not fully built	Chinese standards and regulations for EV Charging information security, doesn't yet provide clear picture of its security protection.

6.3 Vehicle Personal Information and Data Compliance[107]

OEMs need to address and pay closer attention to the following important requirements concerning personal information and data compliance with evolving Privacy and Data Security Protection laws and China Cybersecurity Law.

6.3.1 Personal Information Collection Compliance

Three requirements for judgment of necessary information collection in ICV:

1. The collected personal information should be directly related to the function of the product or service, that is, without the participation of this information, the function of the product or service cannot be realized.
2. The frequency of automatic collection of personal information should be the minimum frequency necessary to realize the function of the product or service.
3. The amount of personal information obtained indirectly should be the minimum amount necessary to realize the function of the product or service.

6.3.2 In-Vehicle Data Collection Compliance

There is wide range of data collection in Internet of Vehicles. In addition to conventional information, it may include information about the owner's activities in the vehicle. The built-in camera and microphone in the vehicle have the function of collecting user information in real time. Therefore, for the data collection behaviour of in-car microphones and in-car cameras, the principle of sensitive data collection should be strictly followed, and informed consent standard should be adopted, that is notified in a timely and separate manner, before data collection. Users should be given the option of blocking in-car information collection, at any time. According the above criteria above, following summarized are few suggestions to OEM's on certain products:

- Data collection directly required for vehicle driving functions:

  Such data collection is necessary data to realize the basic driving functions, and it is also necessary data for the vehicle manufacturer to provide product quality monitoring and safe driving functions. If the driver chooses to open the above-mentioned data to the manufacturer, there is generally no legal problems in terms of necessity.

- Data collected by driving assistance function and use of multimedia terminals (e.g., camera):

  It is relatively difficult to determine the necessity of the data collected by the driving assistance function and the multimedia terminal in the car. However, taking into account the factors of technological progress, for the data collection of this part, the overall judgment standard should be **appropriately loose.**

- Personal information collection:

  ICV companies should fully consider and evaluate the scope and rationality of the use of personal information in various applications, before personal information acquisition.

107 Research on Network and Data Compliance Issues of Internet of Vehicles (Part 2) – Jun 2019

6.3.3 In-Vehicle Personal Information Scope

Regarding personal privacy, China Cybersecurity Law states: "Personal information refers to various information recorded electronically or in other ways that can identify a natural person's personal identity alone or in combination with other information, including but not limited to the natural person's name, date of birth, ID, biometric information, address, telephone number, etc."

As example, OEM's should note, information available in chips used for communication, such as vehicle power control units, vehicle multimedia control systems, vehicle remote control systems, etc. comes under scope of personal information. In addition, unique vehicle identification number (VIN) will also come under scope of personal information.

6.4 Cross-Border Vehicle Data Transfer Requirements

In Aug 2017, National Information Security Standardization Committee issued "Guidelines for Data Transfer Security Assessment (Second Draft for Comment)". It includes geographic information as important information and states that it should be stored on domestic servers.

The guidelines document pointed out to the Dec 2015 'Regulations on Map Management' document (Order No. 664 of the State Council), that internet map service units should set up servers storing map data, within the territory of China and collect and use Internet map service units, provided user location-related information is stored in China.

Suggestions to OEM's:

1. Data classification: Classify data in a detailed manner for ease of evaluation. That is, classify general data, personal information, personal information that constitutes important data, and other important data, to provide a basis for the evaluation of data transfer and reduce the difficulty of evaluation.

2. Build data evaluation system: Enterprises are responsible for the results of their own data transfer evaluation. How to evaluate the necessity of data transfer and whether the data transfer will endanger national security and social public interests requires a complete evaluation method and system.

3. Build domestic data centers: For data that cannot be transferred, or cannot be determined whether it can be transferred, it should be stored in a server within China. Therefore, the establishment and management of domestic data centers is also an important arrangement in the cross-border data transfer strategy for OEMs.

VII Appendix

7 Appendix

7.1 Guidelines for National ICV Standard System

In order to promote and regulate development of the ICV information security industry, MIIT and the National Standards Committee of China, issued multiple guideline for the development of a "National Internet of Vehicles (IoV) Industry Standard System", since late 2017. The guidelines aim to accelerate development of generic, critical standards in the ICV industry, including autonomous driving, assisted driving, in-vehicle electronics, radio communications, LTE-V2X and 5G-V2X standards. In total, the guidelines, as of June 2018, cover almost 300 standards related to ICV. Aside from MIIT, CCSA, CESA, and CATARC were involved in drafting the guidelines. These guidelines were enumerated in section 2.5.1. Following, the various guidelines are summarized.

1. "Guidelines for the Development of the National Internet of Vehicles Industry Standard System (**Intelligent Connected Vehicles**)"[108] – Dec 2017

   Summary: ICV, is the second part of the guidelines, which includes 95 standards. The ICV standard system mainly outlines the basic directions for definition and classification in the ICV standard system, the general specification directions for human-machine interface, functional safety and evaluation, environmental perception, decision-making early warning, auxiliary control, automatic control, information interaction, etc. Also directions on standards related to product and technology applications. The development method combines the technical logic structure of the ICV with the physical structure of the product. ICV standard system framework is defined in four parts: basic, general specifications, product and technology applications, and related standards.

2. "Guidelines for the Development of the National Internet of Vehicles Industry Standard System (**General requirements**)"[109] - June 2018

   Summary: The overall requirements are the first part of the guidelines, constituting the top-level design. It mainly proposes the overall standard system structure and development of the IoV industry, list overall standardization work and promotes the gradual formation of a unified and coordinated national IoV industry standard system structure.

3. "Guidelines for the Construction of the National Internet of Vehicles Industry Standard System (**Information communication**)"[110] – June 2018

   Summary: This part mainly focuses on the design for the information and communication technology, network and equipment, and application services of the IoV's, focusing on research of LTE-V2X, 5G-V2X, and supporting the relevant standardization requirements and key directions of the development of IoV applications. The key standards related to information and communication are divided into three levels: perception layer (edge), network layer (management) and application layer (cloud) and use the "cloud-pipe-device" approach to divide the standard system structure.

4. " Guidelines for the Construction of the National Internet of Vehicles Industry Standard System (**Electronic products and services**)"[111] – June 2018

   Summary: The electronic product and service standard system aims at the standardization work related to automotive electronic products, on-board information

108 National ICV Industry Standard System Development Guide (ICV) - Dec 2017

109 National ICV Industry Standard System Development Guide (Overall Requirements) – Jun 2018

110 National Vehicle Networking Industry Standard System Construction guide (Information and Communication) – Jun 2018

111 National Vehicle Networking Industry Standard System Construction guide (Electronic Products and Services) - Jun 2018

systems, services and platforms supporting the IoV industry chain, and the direction of development of standardization of IoV electronic products and on-board information services. IoV electronic products and services include terminals, networks, platforms and services. Products and terminals, collect intelligent information of vehicles, perceive and process driving status and environment, and realize traffic information, navigation services, entertainment information, etc. On-board information services are for safe driving, online business, emission information, remote control, etc.

5. "Guidelines for the Construction of the National Internet of Vehicles Industry Standard System (**Intelligent vehicle management**)"[112] – April 2020

   Summary: The intelligent vehicle management standard system focuses on public security traffic management and safe operation of connected vehicles. The vehicle intelligent management standard system mainly includes five parts: basic standards, intelligent networked vehicle registration management, identity authentication and security, road operation management, vehicle-road collaborative management and control and service standards. A total of 66 standards are listed and will be developed as per demand, and updated from time to time.

7.2 Relevant ICV/IoV Security Industry Standards

Table 15: ICV/IoV Security Industry Standards

No.	Standard name	Schedule	Date
1	CSAE 101-2018 "Technical Requirements for Information Security of Vehicle-mounted ICV"[113]	Published	March 2018
2	"The Internet of Vehicles Network Security Emergency Response Specification"	Draft	Nov 2018
3	"Technical requirements of Security Certification of IoV Wireless Communication using LTE"	Drafting stage	Apr 2019
4	"Testing Method for Security Certification of IoV Wireless Communication using LTE"[114]	Drafting stage	Apr 2019
5	YD/T3737-2020 "Technical Requirements for Information Security of Connected Cars using Public Telecommunication Network"[115]	Published	Apr 2020
6	YD/T3751-2020 "Technical Requirements for Data Security of IoV Information Service"	Published	Apr 2020
7	YD/T3746-2020 "IoV Information Service User Personal Information Protection Requirements"	Published	Apr 2020

112 Interpretation of "Guidelines for the Construction of National Vehicle Networking Industry Standard System (Intelligent Vehicle Management) – Apr 2020

113 Notice on Soliciting Opinions on the "Technical Requirements for Information Security of Intelligent Connected Vehicles" – Mar 2018

114 Solicitation of opinions on 35 industry standards including LTE technical requirements and test methods for security certification in ICV's -MIIT Apr 2019

115 V2X standards announced by Ministry of Industry and Information Technology – Apr 2020

8	YD/T3750-2020 "Technical Guide for IoV Wireless Security"	Published	Apr 2020
9	YD/T3752-2020 "Requirements for Security Protection of IoV Information Service Platform"	Published	Apr 2020
10	"Security Requirements for In-Vehicle Applications and Service Software"	Consultation Draft	Apr 2020
11	"Technical Requirements for Virtual Car Key Information Security using Mobile Internet"	Consultation Draft	Apr 2020

7.3 Table Catalogue

Table 16: Outline of China Cybersecurity and Cryptography Law from OEM Perspective 2020

	Object	Application Scope	Details	Remarks
CSL	Any OEM or its subsidiaries in China involved in the project.	The security of information system	1) Security of information system. 2) Personal data protection. 3) Sales / provision of security products (CII)	Authority audit might be applied
CEL		Products / services / technologies with encryption function	Commercial encryption product (CEP) and related regulatory requirements for CEP.	No compulsory certification (volunteer basis)

7.3.1 Table17: List of Critical Network Equipment and Network Security Special Products (First Batch)[116]

Products mentioned in China Cybersecurity Law.

	Equipment or Product category	Range
Critical Information Infrastructure	Router	Overall system throughput (bidirectional) >=12Tbps The entire system routing table capacity >= 550,000
	Switch	Overall system throughput (bidirectional) >=30Tbps System packet forwarding rate>=10Gpps
	Server (rack type)	Number of CPUs >=8 Single CPU core number>=14 Memory capacity>=256GB
	Programmable Logic Controller (PLC Device)	Controller instruction execution time <=0.08us
Specialized Network Security Products	Data Backup Machine	Backup capacity >=20T Backup speed >=60MB/s Backup interval <=1hr
	Firewall (hardware)	Machine throughput>=80Gbps Maximum concurrent connections>=3 Million New connections per second>=250 Thousands
	WEB Application Firewall (WAF)	Machine application throughput >=6Gbps Maximum number of HTT concurrent connections>=2 Million
	Intrusion Detection System (IDS)	Full detection speed>=15Gbps Maximum concurrent connections>=5 Million
	Intrusion Prevention System (IPS)	Full detection speed>=20Gbps Maximum concurrent connections>=5 Million
	Secure isolation and information exchange products (gatekeepers)	Throughput >= 1Gbps System delay <=5ms
	Anti-spam products	Connection processing rate (connections / sec) > 100 Average delay time <100ms

116 Announcement on the issuance of the "Critical Network Equipment and Special Network Security Product Catalog (First Batch) - Jun 2017

	Network Integrated Audit System	Packet capture speed >= 5Gbps Recording time capability >=50 Thousands/second
	Network vulnerability scanning products	Maximum number of parallel scan IPs > = 60
	Secure database system	TPC-E tpsE (Transaction-able quantity per second) >=4500
	Web recovery product	Recovery time <=2ms The longest path of the site >=10

7.3.2 Table 18: Certification Catalog for Commercial Cryptographic Products (First Batch) and Certification Rules for Commercial Cryptographic Products[117]

Serial	Product	Product description	Certification Standard References
1	Smart token	Terminal cryptographic devices, which realize cryptographic operation and key management functions: normally using USB interface.	GM/T 0027 "Technical requirements for smart token" GM/T 0028 "Security requirements for cryptographic modules"
2	**Smart IC card**	Integrated circuit boards which realize cryptographic operations and key management functions including CPU, also applying to smart IC card in finance domains.	GM/T 0041 "Testing specifications for smart IC card" GM/T 0028 "Security requirements for cryptographic modules"
3	POS cryptographic application system; ATM cryptographic application system; Multifunctional cryptographic application in the internet terminal	Provides the cryptographic application systems for cryptographic services for the financial terminal devices.	GM/T 0028 "Security requirements for cryptographic modules" JR/T 0025-2018 "China financial integrated circuit card specifications part 7: Debit/credit application security specification"
4	PCI-E/PCI cryptographic card	PCI hardware board devices with the cryptographic operations and self-security protection functions.	"PCI Cryptographic Card Technology Specification" GM/T 0018 "Interface specification of cryptography device application" GM/T 0028 "Security requirements for cryptographic modules"

117 Announcement of the State Administration for Market Regulation and the State Cryptography Administration on issuing the Certification - May 2020.

5	IPSec VPN product/ Secure Gateway	Based on the IPSec protocol, the devices which build up secure communication channels.	IPSec VPN product: GM/T 0022 "IPSec VPN specification" GM/T 0028 "Security requirements for cryptographic modules"
			IPSec VPN Security Gateway: GM/T 0023 "IPSec VPN Gateway product specification" GM/T 0028 "Security requirements for cryptographic modules"
6	SSL VPN product/ Secure Gateway	Based on SSL/TLS protocol, the devices which build up secure communication channels.	SSL VPN product: GM/T 0024 "SSL VPN specification" GM/T 0028 "Security requirements for cryptographic modules"
			SSL VPN Security Gateway: GM/T 0025 "SSL VPN Gateway product specification" GM/T 0028 "Security requirements for cryptographic modules"
7	Secure Authentication Gateway	Devices used for providing user management, identity authentication, single log-in, transmission encryption, access control and security audit services.	GM/T 0026 "Security authentication gateway product specification" GM/T 0028 "Security requirements for cryptographic modules"
8	Cryptographic keyboard	Independent cryptographic module for protecting inputted PIN and encrypting inputted PIN, including POS machine as main device with external devices of encryption keyboard and unattended (Self Service) Terminal with encryption keyboard.	GM/T 0049 "Cryptography test specification for EPP" GM/T 0028 "Security requirements for cryptographic modules"
9	Financial data cryptographic machines	Cryptographic devices for ensuring financial data security compatible to the financial bar magnet card IC card, mainly for the PIN encryption, PIN to transfer encryption, MAC generation/check, data encryption and decryption, signatures verification and key management and other cryptographic service functions.	GM/T 0045 "Specifications of financial cryptographic server" GM/T 0028 "Security requirements for cryptographic modules"
10	Server cryptographic machines	Devices providing cryptographic operations, key management function for application entities independently or in parallel.	GM/T 0030 "Cryptographic server technical specification" GM/T 0028 "Security requirements for cryptographic modules"

11	Sign and verify server	Servers providing digital signature, verification signature etc. functions based on PKI and digital signature system for application entities at the server-side.	GM/T 0029 "Sign and verify server technical specification" GM/T 0028 "Security requirements for cryptographic modules"
12	Time stamp server	Devices related to time stamp service based on public key infrastructure application system	GM/T 0033 "Interface specifications of time stamp" GM/T 0028 "Security requirements for cryptographic modules"
13	Secure access control systems	Access control system for user identity and privileges based on cryptographic techniques	GM/T 0036 "Technical guidance of cryptographic application for access control system based on contactless smart card"
14	Dynamic token; Dynamic token authentication system	Dynamic token: Carrier to generate and demonstrate dynamic password; Dynamic token authentication System: systems for authenticating dynamic password and dynamic token.	Dynamic token: GM/T 0021 "One-time password application of cryptography algorithm" GM/T 0028 "Security requirements for cryptographic modules"
			Dynamic token authentication system: GM/T 0021 "One-time password application of cryptography algorithm"
15	Secure electronic seal system	Systems provide the electronic seal management and signature/verification of electronic seal.	GM/T 0031 "Secure electronic seal cryptography technical specification"
16	Digital document cryptographic application system	Application systems providing cryptographic operations, key management functions during file creation, modification, authorization, reading, signing, stamping, printing, enhancing watermarks, circulation, archiving and destroying operations for electronic file.	GM/T 0055 "File cryptographic technical specification"
17	Cryptographic platform for trusted computing	Using cryptography technology providing cryptographic supporting with integrity and identity creditability and data security for trusted computing The products are trusted cryptographic module and trusted cryptographic service module	GM/T 0011 "Trusted computing – functionality and interface specification of cryptographic support system" GM/T 0012 "Trusted computing – interface specification of trusted cryptography module" GM/T 0058 "Trusted computing- TCM service module interface specification" GM/T 0028 "Security requirements for cryptographic modules"

18	Certificate authentication system; Certificate authentication key management systems	Certificate authentication system: System to manage life cycle of signing, releasing, updating and withdrawing of digital certificates; Certificate authentication key management system: system to manage the entire processes of key of encrypted certificates during life cycle.	GM/T 0034 "Specifications of cryptograph and related security technology for certification system based on SM2 cryptographic algorithm"
19	Symmetric key management products	System and devices for producing, distributing and managing symmetric key in cryptographic applications.	GM/T 0051 "Cryptography device management- specifications of symmetric key management technology"
20	**Secure chip**	IC chips including cryptographic algorithm, security function and providing key management mechanism.	GM/T 0008 "Cryptography test criteria for security IC"
21	Digital tag chip	Radio frequency identification chips using cryptography technique with the electronic identification information of the intended applications	GM/T 0035.2 "Specifications of cryptographic application for RFID systems- part 2: specification of cryptographic application for RFID tag chip"
22	**Other cryptographic modules**	Software, hardware, firmware and their combination providing cryptographic operations, key management functions, including cryptographic module, hardware cryptographic module, etc.	GM/T 0028 "Security requirements for cryptographic modules"

Note:

1. Cryptographic algorithms used for the products above should comply with GM/T 0001 "ZUC stream cipher algorithms", GM/T 0002 "SM4 Block cipher algorithms", GM/T 0003 "SM2 Elliptic curve public-key cryptography Algorithms", GM/T 0004 "SM3 cryptography hash algorithms", GM/T 0009 "SM2 cryptography algorithm application specification", GM/T 0010 "SM2 Cryptography message syntax specification", GM/T0044 "Identity-based cryptographic algorithms-SM9" and other cryptographic algorithms required by the SCA.
2. Random number generator used for the products above comply with GM/T 0005 "Randomness test specification", GM/T 0062 "Random number test requirements for cryptographic modules".
3. Standards above shall execute with their latest version (including parameters modification) if there is no marking with year.

7.3.3 Table 19: Overview of Cybersecurity Standards of TC114/SC34

Note: Numbers are only for planning purpose and no relationship with the final number e.g. GB/TXXX. Implementation level indicates importance and priority level. E.g. H: high; M: Medium; L: Low

Projects and Categories		Implementation Level
Basic (100)		
Terminologies and Definitions (101)		
101-1	Terminologies and definitions for automobile cybersecurity	H
Concepts and Procedures (102)		
102-1	Road vehicles – cybersecurity engineering (adoption of ISO 21434)	M
General Standards (103)		
103-1	General technical requirements for cybersecurity of vehicles	H
103-2	Technical requirements for the security of ICV working environment	M
103-3	Technical requirements and test standards for the security of the terminal device passwords	M
General Technologies (200)		
Risk Evaluation (201)		
201-1	Specification for risk assessment of vehicle information security	H
Security Requirements (202)		
202-1	General requirements for the security and privacy protection of automotive data	M
202-2	Technical requirements for the security of automotive chips	L
202-3	Technical requirements for information safety of on-board ECU	M
202-4	Technical requirements for the security of automotive OP and APPs	M
Tests & Evaluations (203)		
203-1	Test methods of vehicle information safety	M

Critical Systems and Components (300)		
Internal Communications (301)		
301-1	Technical requirements for the security of automotive ethernet	L
301-2	Information security of automobile gateway	H
Vehicles and Extended Systems (302)		
302-1	Technical security requirements of vehicle-mounted information interactive system	H
302-2	Information security technology requirement of OBD interface	H
302-3	Technical requirements of information security of electric vehicles charging systems	H
Functional Applications and Administrations (400)		
400-1	Technical requirements for the driver & passengers identity authentication systems	M
400-2	Technical requirements of vehicle software update	H
400-3	Technical requirements for the security of automotive remote monitoring systems	M
400-4	Technical requirements for the security of automotive remote diagnostics	M
400-5	Cyber-Security technical specifications of remote service and management system for electrical vehicle	H
400-6	Administration guide for automotive cybersecurity loopholes	M
400-7	On emergency response management of automobile information safety	H
Relative Standards (500)		
Cyber Communications (501)		
501-1	Technical requirements for the security of cellular data and satellite communications	--
501-2	Technical requirements and test methods for the security of LTE-V2X	--
Platforms & Facilities (502)		
502-1	Technologies of Technologies of cybersecurity for charging points	--
502-2	Technical requirements for the security of automotive remote service platform	--

7.3.4 Table 20: Summary of SCA Cryptographic Standards (Industrial layer)

Standards No.	Title
GM/T 0001-2012	ZUC stream cipher algorithm
GM/T 0002-2012	SM4 block cipher algorithm
GM/T 0003-2012	Public key cryptographic algorithm SM2 based on elliptic curves
GM/T 0004-2012	SM3 cryptographic hash algorithm
GM/T 0005-2012	Randomness test specification
GM/T 0006-2012	Cryptographic application identifier criterion specification
GM/T 0008-2012	Cryptography test criteria for security IC
GM/T 0009-2012	SM2 cryptography algorithm application specification
GM/T 0010-2012	SM2 cryptography message syntax specification
GM/T 0011-2012	Trusted computing Functionality and interface specification of cryptographic support platform
GM/T 0012-2012	Trusted computing Interface specification of trusted cryptography module
GM/T 0013-2012	Trusted cryptography module interface compliance
GM/T 0014-2012	Digital certificate authentication system cryptography protocol specification
GM/T 0015-2012	Digital certificate format based on SM2 algorithm
GM/T 0016-2012	Smart token cryptography application interface specification
GM/T 0017-2012	Smart token cryptography application interface data format specification
GM/T 0018-2012	Interface specifications of cryptography device application
GM/T 0019-2012	Universal cryptography service interface specification
GM/T 0020-2012	Certificate application integrated service interface specification
GM/T 0021-2012	One time password application of cryptography algorithm

GM/T 0022-2014	IPsec VPN specification
GM/T 0023-2014	IPsec VPN gateway product specification
GM/T 0024-2014	SSL VPN specification
GM/T 0025-2014	SSL VPN gateway product specification
GM/T 0026-2014	Security authentication gateway product specifications
GM/T 0027-2014	Technique requirements for smart token
GM/T 0028-2014	Security requirements for cryptographic modules
GM/T 0029-2014	Sign and verify server technical specification
GM/T 0030-2014	Cryptographic server technical specification
GM/T 0031-2014	Secure electronic seal cryptography technical specification
GM/T 0032-2014	Specifications for role based privilege management and access control
GM/T 0033-2014	Interface specifications of time stamp
GM/T 0034-2014	Specifications of cryptograph and related security technology for certification system based on SM2 cryptographic algorithm
GM/T 0035-2014	Specifications of cryptographic application for RFID systems
GM/T 0036-2014	Technical guidance of cryptographic application for access control systems based on contactless smart card
GM/T 0037-2014	Certificate authority system test specification
GM/T 0038-2014	Key management of certificate authority system test specification
GM/T 0039-2015	Security test requirements for cryptographic modules
GM/T 0040-2015	Cipher test specification of radio frequency identification tag module
GM/T 0041-2015	Cryptographic test specification for smart card
GM/T 0042-2015	Test specification for cryptography and security protocol in tri-element peer architecture
GM/T 0043-2015	Test specification for digital certificate interoperability

GM/T 0044-2016	Identity-based cryptographic algorithms SM9
GM/T 0045-2016	Specifications of financial cryptographic server
GM/T 0046-2016	Test specification for financial cryptographic server
GM/T 0047-2016	Cryptography test specification for secure electronic seal
GM/T 0048-2016	Cryptography test specification for cryptographic smart token
GM/T 0049-2016	Cryptography test specification for EPP
GM/T 0050-2016	Cryptography device management-Specification of device management technology
GM/T 0051-2016	Cryptography device management-Specifications of symmetric key management technology
GM/T 0052-2016	Cryptographic equipment management-Monitoring management specification of VPN equipment
GM/T 0053-2016	Cryptographic equipment management-Data interface specification of remote monitoring and compliance testing

7.3.5 Table 22: ISO/IEC 19790 vs GM/T 0028 (Security Requirements for Cryptographic Modules)

Item	ISO/IEC19790	GM/T 0028
7.1 General	The security requirements cover areas related to the design and implementation of a cryptographic module	The security requirements cover areas related to the design, implementation operation and decommission of a cryptographic module
7.2.2 Type of cryptographic modules	For software modules executing in a modifiable environment, the physical security requirements found in 7.7 are optional and the applicable non-invasive security requirements in 7.8 shall apply	For software modules executing in a modifiable environment, the physical security requirements found in 7.7 and non-invasive security in 7.8 are optional
7.2.2 Type of cryptographic modules	For hybrid modules, all applicable requirement of 7.5, 7.6,7.7 and 7.8 shall apply	For hybrid modules, software and firmware components shall apply for all applicable requirements of 7.5, 7.6; hardware components shall apply for all applicable requirements of 7.7 and 7.8

7.2.4.1 Modes of operations general requirement	A non-approved cryptographic algorithm or non-approved generated key may be used to obfuscate data or CSPs, but the result is considered unprotected plaintext and provides no security relevant functionality until protected with a proved cryptographic algorithm	A non-approved cryptographic algorithm or non-approved generated key may be used to obfuscate data or CSPs, but the result is considered unprotected plaintext and provides no security relevant functionality
7.2.4.3 Degraded operation	A cryptographic module may be designed to support degraded functionality if the module enters the error stage	No degraded operation is allowed.
7.3.3 Definition of interfaces	The cryptographic module shall distinguish between data, control, information, and power for input, and data, control information, status information, and power for output	The cryptographic module shall distinguish between data, control, information, and power for input, and data, control information, status information
7.3.4 Trusted channel for security level 3	The physical ports used for the trusted channel shall be physically separated from all other ports or the logical interfaces used for the trusted channel shall be logically separated from all other interfaces	The physical ports used for the trusted channel shall be physically separated from all other ports and the logical interfaces used for the trusted channel shall be logically separated from all other interfaces.
7.4.3.3 Self-initiated cryptographic output capability	No extra requirements for security level 4	For security level 4, two independent internal action shall be performed by two independent operators to activate the capability
7.5 Software/ Firmware security (security level 1)	The expected referenced output of the integrity technique mechanism may be considered data and itself not subject to the integrity technique.	No such statement
7.5 Software/ Firmware security (security level 1)	A cryptographic mechanism using an approved integrity technique or an error detection code (EDC) shall be applied to all software and firmware components within the hardware module's defined cryptographic boundary or within disjoint hardware components of the hybrid module.	A cryptographic mechanism using an approved integrity technique shall be applied to all software and firmware components within the hardware module's defined cryptographic boundary
7.5 Software/ Firmware security (security level 1)	If the software or firmware that is loaded is associated, bound, modifies or is an executable requisite of the validated modules, then the software/firmware load test is applicable and shall be performed by the validated module with the following exceptions…	If the software or firmware that is loaded is associated, bound, modifies or is an executable requisite of the validated modules, then the software/firmware load test is applicable and shall be performed by the validated module. No exception is accepted

7.5 Software/ Firmware security (security level 2, 3, and 4)	For software and firmware modules and the software or firmware component of a hybrid module for security level 2(except for the software and firmware component within a disjoint hardware component of a hybrid module): An approved digital signature or keyed message authentication code shall be applied to all software and firmware within the module's defined cryptographic boundary	An approved digital signature or keyed message authentication code shall be applied to all software and firmware within the module's defined cryptographic boundary. No exception statement regarding to the software and firmware components within disjoint hardware component of a hybrid module
7.6.3 Operating system requirements for modifiable operational environment	No statement of modifiable operational environments under security level 3 and security level 4	Clearly state "This standard provides no requirement for modifiable optional environments under security level 3 and security level 4, thus modifiable operational environment cannot be certified under security level 3 and security level 4."
7.7.4.3 Environmental failure testing procedures	From a temperature within the normal operating temperature range to the highest (e.g. hottest) temperature that either (1) shuts down or goes into an error state or (2) zeroizes all unprotected SSPs	From a temperature within the normal operating temperature range to the highest (e.g. hottest) temperature that either (1) shuts down (2) zeroizes all unprotected SSPs
7.8 Non-invasive security	This sub clause is not applicable if the cryptographic module does not implement non-invasive attack mitigation techniques to protect the module's unprotected SSPs from non-invasive attacks referenced in Annex F.	
7.8 Non-invasive security at security level 3 and security level 4	The cryptographic modules shall be tested to meet the approved non-invasive attack mitigation test metrics for security level 3 or security level 4 as referenced in Annex F	For security level 3, beside the above requirement, documents shall provide the proof of the effectiveness for each mitigation method, as well as the testing methods. For security level 4, the cryptographic module shall be tested to meet the requirements of national relevant departments regarding the mitigation of non-invasive security
7.9.1 SSP management general requirements	CSP encrypted or obfuscated using non-approved security function are considered unprotected plaintext within the scope of this international standards	CSP encrypted using non-approved security function are considered unprotected plaintext within the scope of this international standards

7.9.2 Random bit generators	No extra requirements on the length of entropy	No matter whether the entropy is collected internally or externally, the min-entropy shall be no less than 256 bits for any of the CSPs. IF the entropy is collected internally, detailed design of random bit generator shall be provided.
7.9.7 SSP zeroization	SSPs need not meet these zeroization requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialization key)	Which means ALL unprotected SSPs shall be zeroized.
7.10.1 Self-test general requirements	All self-tests identified in underlying algorithmic standards (Annexes C through E) shall be implemented as applicable within the cryptographic module. All self-tests identified in addition or in lieu of those specified in the underlying algorithmic standards (Annexes C through E) shall be implemented as referenced in Annexes C through E for each approved security function, SSP establishment method and authentication mechanism.	All self-tests identified in underlying algorithmic standards (Annexes C through E) shall be implemented as applicable within the cryptographic module

7.3.6 Table 23: GM/T 008 vs FIPS-140-2 (cryptography test criteria for security IC)

	GM/T 0008 Vs. FIPS-140-2
Similarity	4 security levels Single chip, Multichip embedded, and Multichip standalone 10 security requirements
Differences	No implementation guidance, derived test requirements No software/firmware module defined Annex C: SM4 and SM1 as symmetric algorithms, SM2 as asymmetric algorithm, SM3 as hash function, ZUC as stream cipher, ISO/IEC 9797-2 as MAC, GM/T 0005-2012: Randomness Test Specification as RNG specification Annex D: SM2 part 3, ISO/IEC 11770-2 and ISO/IEC 11770-3 as key establishment scheme. – Annex E: Best practices for software development – Annex F: Samples of mitigation of other attacks

7.4 China Security Testing Centers

7.4.1 CATARC -Testing and Certification Division

CATARC[64] **Testing and Certification Division** has been conducting research on automotive security testing since 2017. It has established automotive security voluntary certification and evaluation system. The voluntary certification evaluation system includes three parts:

- vehicle security certification,
- automobile parts security certification, and
- security management system certification.

It has numerous automotive and EV testing centres across China.

7.4.2 CCID- China Software Testing Center (CSTC)

The China Software Testing Center (CSTC) is a national-level computer software, hardware, and network security quality testing agency under MIIT and the General Administration of Quality Supervision, Testing and Quarantine. The center has established a complete quality management system in accordance with ISO/IEC17025. **CCID (China Electronics Information Industry Development Research Institute)** Group is a scientific research institution, under CSTC, in Beijing. The test reports issued by the center have achieved mutual recognition in 39 countries and regions. CSTC is equipped with advanced and complete computer software, hardware and network system testing environment and tools, with national software quality assurance experts and a technical team engaged in software and hardware quality assurance for many years.

7.4.3 Apollo Cybersecurity Service – Cybersecurity Test

It provides customizable vehicle cyber security testing service. It combines automated testing and manual penetration, provide vehicle-level and component-level testing, software/ hardware architecture security testing, firmware security testing, communication security and data security testing. They have abundant test cases, covering T-BOX, gateway, IVI and other components.

7.4.4 China Tyre Laboratory - CAICT

CAICT was founded in 1957 and is a scientific research institution under the MIIT. As an authoritative testing organization in China, **China Tyre Laboratory** has long been conducting research on the security evaluation of intelligent connected vehicles. The evaluation scope covers vehicle terminal equipment, V2X and cloud platform. It provides a comprehensive assessment of the vehicle security capabilities.

7.4.5 China Intelligent and Connected Vehicles (CICV)

CICV – China Automotive Beijing Research Institute Co., Ltd. was jointly established by China Society of Automotive Engineers (China SAE), China Association of Automobile Manufacturers (CAAM) and CAICV. CICV security built an ICV security system and service platform called Ability. Ability has become one of basic platforms for the development and innovation of the ICV security industry