Translation

The following document is a draft PRC government plan for the near-term development of China's cybersecurity industry. The plan names a host of specific cybersecurity technologies that the Chinese government is encouraging PRC companies to pursue. China allowed the public to comment on this draft plan, but only for a four-day period in July 2021.

Title
Open Solicitation of Opinions on the *Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021-2023) (Draft for Solicitation of Opinions)*
公开征求对《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》的意见

Author
Cybersecurity Administration (网络安全管理局) of the PRC Ministry of Industry and Information Technology (MIIT; 工业和信息化部; 工信部)

Source
MIIT website, July 12, 2021.

The Chinese source text for the announcement of the opinion solicitation period is available online at:
https://www.miit.gov.cn/gzcy/yjzj/art/2021/art_34f89fff961b4862bf0c393532e2bf63.html
The Chinese source text of the draft plan itself is available online at:
https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20217/0e5071815ec641be9e2154566c09fe33.wps
U.S. $1 ≈ 6.5 Chinese Yuan Renminbi (RMB), as of July 27, 2021.

Translation Date	**Translator**	**Editor**
July 27, 2021	Etcetera Language Group, Inc.	Ben Murphy, CSET Translation Lead

In order to thoroughly implement the strategic decisions and deployments of the Chinese Communist Party (CCP) Central Committee and the State Council on [making China into] a manufacturing powerhouse (制造强国) and a cyber powerhouse (网络强国),[1] implement the relevant requirements of the *Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and*

[1] Translator's note: The Chinese word *qiángguó* (强国) is translated as "powerhouse" throughout this translation. *Qiángguó* literally means "strong nation"; an alternative translation is "superpower." Alternate translations of the term *wǎngluò qiángguó* (网络强国)—translated throughout as "cyber powerhouse"—include "cyber superpower," "internet powerhouse," "internet superpower," "network powerhouse," and "network superpower." For a more thorough discussion in English of the terms *qiángguó* and *wǎngluò qiángguó*, see:
https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/

Long-Range Objectives for 2035,[2] accelerate the promotion of the high-quality development of the cybersecurity industry, and enhance the comprehensive strength of the cybersecurity industry, the Ministry of Industry and Information Technology (MIIT) has drafted the *Three-Year Action Plan for the High-Quality Development of the Cybersecurity*[3] *Industry (2021-2023) (Draft for Solicitation of Opinions)*. In order to hear further opinions of all sectors of society, it is hereby publicized. If you have any comments or suggestions, please provide feedback before (Friday) July 16, 2021.

Fax: 010-66069561

E-mail: xiaojunfang@miit.gov.cn

Address: Cybersecurity Administration, Ministry of Industry and Information Technology, 13 West Chang'an Street, Xicheng District, Beijing (Postal Code: 100804). On the envelope, please indicate "Feedback on the *Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021-2023) (Draft for Comments)*."

Ministry of Industry and Information Technology

July 12, 2021

Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry

(2021-2023)

(Draft for Solicitation of Opinions)

As an emerging digital industry, the cybersecurity industry encompasses the cybersecurity technology, product production, and service activities that safeguard national cybersecurity (网络空间安全) and development interests, and it is a basic guarantee for building [China into] a manufacturing powerhouse and a cyber powerhouse. In recent years, China's cybersecurity industry has made positive progress, especially with the rapid development of new technologies, new lines of business (新业务), and new models, such as 5G, big data, artificial intelligence (AI), the

[2] Translator's note: CSET's English translation of China's 14th Five-Year Plan Outline is available online at: https://cset.georgetown.edu/publication/china-14th-five-year-plan/

[3] Translator's note: For consistency, the Chinese term *wǎngluò ānquán* (网络安全) is translated as "cybersecurity" throughout this translation. Depending on context, *wǎngluò ānquán* can also mean "network security" or "internet security."

Internet of Vehicles (IoV), the Industrial Internet, and the Internet of Things (IoT), and with the vigorous growth of technologies, products, and services such as cybersecurity and data security. This action plan has been formulated in order to thoroughly implement General Secretary Xi Jinping's important thinking on [building China into] a cyber powerhouse, implement the *Cybersecurity Law of the People's Republic of China*, *Data Security Law of the People's Republic of China*, and the *Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035*, accelerate the construction of an ecosystem for healthy and orderly industrial development with strong innovation capabilities and an optimized industrial structure, high supply quality, and a sufficient release of pent-up demand, in-depth industry integration and collaboration, and a cadre of professional talent, propel the cybersecurity industry towards achieving the high-quality development goals of advanced technology and developed industries, and to continuously improve national cybersecurity assurance capabilities.

I. Overall Requirements

(1) Guiding Ideology

Guided by Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, fully implement the spirit of the 19th Party Congress and the Second, Third, Fourth, and Fifth Plenums of the 19th CCP Central Committee. Be firmly grounded in the new stage of development (新发展阶段), implement the new development concept (新发展理念), and construct the new development pattern (新发展格局). Coordinate development with security. Actively grasp the development opportunities of digital industrialization and industrial digitalization and accelerate the advancement of supply-side structural reform with the goal of promoting the high-quality development of the cybersecurity industry. Take as the main thread driving high-quality supply with effective demand, and fully stimulate the vitality of technological innovation. Give full play to the supporting roles of various forms of capital and strengthen support and assurance for multiple levels of talent. Promote the coordinated development of innovation chains, production chains, and value chains, cultivate a healthy and orderly industrial ecosystem, and lay a solid foundation for building a manufacturing powerhouse and a cyber powerhouse.

(2) Basic Principles

Driven by innovation, lay a solid foundation. Strengthen basic, universal, and forward-looking security technology research, accelerate research on key and core technologies (关键核心技术), spur corporate innovation, effectively promote the

conversion of technological achievements into practical applications (技术成果转化), strengthen basic industrial capabilities, and improve the level of the production chain.

Insist on the pulling force of demand and transform supply. Encourage key industries to increase investment in cybersecurity so as to drive supply with effective demand. Guide cybersecurity products to service-oriented and high-end-oriented transformations and create high-level demand with high-quality supply.

Integrate deeply, and advance in unison. Persist in the development of cybersecurity education, technology, and industry integration, and strengthen industry-academia-research institute-user (产学研用) cooperation. Support the establishment of innovative consortia and increase the role of capital and highlight the effectiveness of collaborative advancement.

The market leads, and the government guides (市场主导、政府引导). Give full play to the role of various market players and encourage differentiated development and competition. Give better play to the role of government planning and guidance, policy support, standard formulation, and market supervision, and urge enterprises to carry out the main responsibilities of cybersecurity and data security and thereby foster an environment that is conducive to development.

(3) Development Objectives

By 2023, cybersecurity technology innovation capabilities will be significantly improved, product and service levels will continue to improve, economic and social cybersecurity demand will be unleashed faster, production integration will be precise and efficient, the cadre of cybersecurity talent will improve daily, and the industry's basic capabilities and comprehensive strength will continue to increase. The structural layout will be more optimized, and the industrial development ecosystem will be healthy and orderly.

– **Scale of the industry:** The scale of the cybersecurity industry will exceed 250 billion [Chinese] yuan [Renminbi (RMB)], with a compound annual growth rate of over 15%.

– **Technological innovation:** A number of key and core cybersecurity technologies will have achieved breakthroughs and reached an advanced level. The integration and innovation of emerging technologies and cybersecurity will have accelerated significantly, and the ability to create new cybersecurity products and services will have been further enhanced.

– **Enterprise development:** A group of flagship enterprises (领航企业) with significant advantages in quality brands and effective operations with the ability to lead

the cybersecurity ecosystem will be initially formed, and a group of “professional, meticulous, specialized, and innovative” (“专精特新”) small- and medium-size enterprises (SMEs) will have rapidly grown through new development tracks such as IoV, the Industrial Internet, IoT, and smart city, and the number of niche champions in cybersecurity products, services, and solutions will have gradually grown.

– **Unleash demand:** Cybersecurity investments in key industries such as telecommunications will account for 10% of investments in informatization (信息化). The speed at which security is applied in key industries and fields will have comprehensively increased, the cybersecurity capabilities of SMEs will have significantly improved, and the level of cybersecurity protection for infrastructure in key industries will have continued to improve.

– **Talent training:** A number of cybersecurity talent training bases, public service platforms, and training ranges (实训靶场) will have been established. The training of innovative, skilled, and battle-tested (实战型) talents will have been significantly increased, the multi-level cybersecurity talent training system will have become more robust, and the number and quality of cybersecurity talents will have continuously improved.

– **Ecosystem cultivation:** Industry-finance linking (产融对接) will be more precise and efficient, and the role of capital empowerment will continue to grow. The cybersecurity industry structure will be further optimized, and industrial clustering will be significantly enhanced. The healthy market order oriented by product and service capabilities will have continuously improved, and the industrial pattern of integration and development of large, medium-size, and small enterprises will have basically taken shape.

II. Key Tasks

(1) Actions to strengthen industrial supply

1. Accelerate the upgrading of traditional security products. Further improve the performance of traditional detection products such as intrusion detection systems, advanced threat detection, network auditing, host and terminal security, and content security, optimize rule extraction algorithms, and improve the quality of security detection. Promote the intensive development (集约化发展) of the security capabilities of traditional protection products such as firewalls, anti-denial-of-service (DoS) systems, and security gateways. Promote the intelligentized (智能化) development of traditional analysis products such as security operating platforms, network traffic analysis systems, and threat information analysis and traceability systems and improve

the level of application of big data, AI, and cryptography technology in the field of security.

2. Strengthen the supply of cybersecurity in key areas. For 5G, cloud computing, AI, and other emerging technology fields, accelerate the development and promotion of technology products such as native security (原生安全), intelligent orchestration (智能编排), endogenous security and safety (内生安全), dynamic access control (DAC), and trustworthy computing (可信计算). For the Industrial Internet, strengthen capabilities in heavy-traffic security analysis, vulnerability mining and management, data fusion analysis, and protocol identifier analysis (协议标识解析). For IoV and IoT, promote the endogenous combination of lightweight terminal security products or middleware and the application of protection solutions such as communications security, identity authentication, and platform security. Promote the research and application of data security technologies such as federated learning, multi-party security technology, privacy-preserving computation (隐私计算), confidential computing (密态计算), secure retrieval, and multi-threshold collaborative tracing (多阈协同追踪).

3. Strengthen research on and application of data security technology. In response to traditional data security requirements such as leak prevention, anti-tampering, and anti-theft, further optimize the functions and performance of products for data security management, categorized and hierarchical security protection, etc., and improve the level of intelligent protection and management of data security. In response to data security supervision requirements, further strengthen research on monitoring, early warning, and emergency response technology and improve capabilities for intelligent risk analysis, threat early warning, and automated incident handling. In response to the demand for data security sharing, vigorously promote research on and deployment of technologies such as secure multi-party computing, federated learning, and trustworthy computing to promote the safe and orderly flow of data factors of production (要素).

4. Create innovative security service models. Strengthen the cloud-based (云化) capabilities of security enterprise technology products, promote the application of cloud-based security products, and encourage security companies with strong comprehensive strength to develop flexible and agile cloud-based cybersecurity services. Develop intensive (集约化) security services and encourage enterprises to provide all-inclusive, integrated solutions including firewalls, user authentication, data security, and application security. Support the development of security trusts (安全托管) and consulting services such as threat management, detection, and response. Develop regional, city-level, and industry-level secure operation services and improve the level of operational automation, sequencing, and toolification (工具化). Encourage basic

telecommunications companies and large cloud service providers to give full play to the advantages of networks and basic resources to export security service capabilities while upgrading and transforming infrastructure to support security companies in embedding security service capabilities.

5. Develop innovative security technologies. Promote the endogenous and adaptive development of cybersecurity architecture and accelerate the development of cybersecurity system research and development based on frameworks such as development, security, and operations (DevSecOps), active immunity, and zero trust. Accelerate the development of dynamic perimeter defense (动态边界防护) technologies and encourage enterprises to deepen the application of technology products for micro-segmentation, software-defined perimeters (SDPs), secure access service edge frameworks, etc. Actively develop intelligent detection and response technology and improve the level of application of technologies such as user and entity behavior analytics (UEBA), security orchestration, automation, and response (SOAR), and extended detection and response (XDR). Promote the development of active security and defense (主动安全防御) technology and promote the implementation of technical products such as deception defense (欺骗防御), threat hunting, and mimic defense. Accelerate the application of blockchain-based protection technologies and promote the development of technical products such as multi-party authorization (MPA) and trusted data sharing. Strengthen research on security technology in the fields of satellite internet and quantum teleportation.

6. Strengthen support for a common foundation. Continue to build a basic cybersecurity knowledge base of high-quality threat information, vulnerabilities, malicious code, malicious addresses, and attack behavior characteristics and strengthen the ability to support cybersecurity knowledge. Accelerate the development of low-level engines and tools such as malicious code detection, advanced threat monitoring and analysis, information processing, inverse analysis (逆向分析), vulnerability analysis, and password security analysis to improve the use of cybersecurity knowledge. Accelerate the development of software supply chain security tools such as source code analysis and component and composition analysis, and improve the security development level of cybersecurity products. Actively promote research on cyber range (网络靶场) technology, build a security twin testbed that combines a virtual environment with real equipment, and improve the testing and verification capabilities of cybersecurity technology products.

Focus 1: Security Technology and Product Improvement Projects for New Facilities (新设施) and New Factors of Production

5G Security: For 5G network infrastructure such as the 5G core network and edge computing platforms, promote the application of products such as security orchestration and automated response, in-depth traffic analysis, threat hunting, and signaling security (信令安全) and promote cloud-side collaborative security capabilities. For the technical characteristics of network slicing and network function virtualization (NFV), promote the deployment and application of virtualized security protection products such as container security and micro-segmentation and security products such as 5G air interface and signaling protection detection (信令防护检测) so as to improve 5G endogenous security capabilities and awareness of 5G network threats. For network construction models such as 5G virtual private networks (VPNs) and 5G joint construction and sharing (共建共享), actively promote the application of security resource pools, zero-trust security architecture, asset identification, and other security solutions to build security capabilities that are provided on demand.

Cloud Security: For new cloud computing architectures such as the multicloud, cloud native, the edge cloud, and the distributed cloud, develop multicloud identity management, cloud security management platforms, cloud security configuration management, cloud native security, cloud disaster recovery, and other technology products to promote the secure development of cloud architecture. For basic resources such as cloud servers, virtual hosts, and networks in the cloud environment, strengthen the level of basic information collection and improve the capabilities of security products such as dual-stack (IPv4 and IPv6) traffic visualization, micro-segmentation, SDPs, and cloud workload protection to ensure the security and reliability of resources on the cloud. For services such as cloud-based services and applications, improve the efficiency of security products such as the secure access service edge (SASE) model, cloud web application firewalls, and cloud data protection to ensure the secure operation of cloud-based services.

AI Security: Construct an AI security threat categorization system, confront the life cycle of AI systems, establish AI threat models, and formulate a standard system for AI system security detection and evaluation. Study security factors such as interpretability and privacy of AI systems, achieve breakthroughs in the key technologies of AI model attack and defense, design and implement automatic attack and defense platforms for AI systems, and build AI security ranges.

Data Security: Optimize data security management technology, improve the accuracy and level of intelligence of basic technology products such as data identification, categorization, and grading, quality control, and consanguinity analysis (血缘分析), improve the capabilities of quality control and consanguinity analysis technology, accurately grasp the data resource situation, and make data visualizable,

manageable, and controllable. Improve data application security protection technology, promote data desensitization, data leakage prevention, data encryption, data backup and recovery, granular access controls, and other technical product upgrades to ensure the security and controllability of data applications. Strengthen data security monitoring, early warning, and emergency response technology; improve the breadth, depth, and precision of data flow and abnormal behavior monitoring in terminal, network, cloud, and cross-border (跨境) scenarios, and improve the intelligentization and degree of automation of incident handling. Achieve breakthroughs in data sharing security technology, promote secure multi-party computation, federated learning, trustworthy computing, homomorphic encryption, differential privacy, blockchain, data watermarking, and other privacy protection and flow tracing (流向溯源) technologies and promote the practical deployment and popularization of Chinese-made commercial password applications to promote the secure and orderly flow of data factors of production.

(2) Initiatives to spur demand for security

7. Promote the upgrading of cybersecurity capabilities in the telecommunications and internet industries. Guide enterprises in key industries such as telecommunications and the internet to increase investment in cybersecurity, promote the simultaneous planning, construction, and use of cybersecurity and informatization (信息化), and improve cybersecurity management and technical support systems. Launch cybersecurity asset surveying and mapping, monitoring and early warning, detection and evaluation, and information sharing in an in-depth manner and improve measures for security monitoring and handling of abnormal behaviors such as network-side Trojan horses, malicious mobile programs, and advanced threat behaviors. Strengthen cybersecurity risk assessment and emergency drills in the fields of telecommunications and the internet, enhance cybersecurity threat prevention, hidden danger handling (隐患处理), and emergency response capabilities, and continue to improve the maturity level of security protection systems. Strengthen security protection of the entire data life cycle, implement categorized and hierarchical management (分类分级管理), carry out data security risk assessments, improve the level of security protection of personal data and important data, and protect the safety and personal privacy of the lives and property of the people.

8. Accelerate security applications in emerging convergent fields (新兴融合领域). Comprehensively promote the implementation of categorized and hierarchical cybersecurity for Industrial Internet companies and strengthen the construction of a categorization and protection system for cybersecurity for industries such as raw materials, equipment manufacturing, consumer goods, and electronic information. For

the security of the IoV, encourage vehicle companies to improve the security protection and detection capabilities of automobiles, key network equipment, and cloud platforms, strengthen the security of roadside networking facilities, and promote the testing and verification of security solutions in IoV demonstration area, pilot area, and test site demonstrations. Implement the IoT basic security "Hundreds of Enterprises and Thousands of Products" (“百企千款”) product cultivation initiative, with IoT terminals, gateways, and platforms for the key links of the IoT. Carry out IoT security detection, abnormality handling, and public services and create “Safe IoT Products” (“物联网安心产品”).

9. Promote the construction of key industry infrastructure to strengthen cybersecurity. Prompt energy, finance, transportation, water conservancy, health care, education, and other industries to strengthen the establishment of technological means such as asset identification, equipment protection, perimeter defense, identity authentication, data security, and application security, and improve the security protection capabilities of major systems, key nodes, and data. Support the establishment of security mechanisms and in-depth protection systems such as situational awareness, notification and early warning, emergency response, and security operations, and continuously improve risk prevention and emergency response capabilities. Promote the application of technologies such as zero trust and AI to enhance the effectiveness of protection systems.

10. Encourage SMEs to strengthen cybersecurity capacity building. Implement the SME “securely go to the cloud” (“安全上云”) special initiative, build a cybersecurity operations service center, and provide high-quality, low-cost, intensive cybersecurity products and services for SMEs. Guide SMEs towards flexibly deploying cybersecurity products and solutions through one-stop shopping, leasing, subscription, trusteeship (托管), cloud delivery, and other related cybersecurity products and services. Support the development of diversified cybersecurity awareness promotions and skills training and continuously improve the cybersecurity protection awareness and capabilities of SMEs.

Focus 2: Security Capability Building Project for New Digital Scenarios and New Services
IoV Security: Strengthen the establishment of IoV security capabilities, promote the application of key technologies and products such as lightweight identity authentication, vehicle security gateways, vehicle firewalls, and intrusion detection for connected vehicles and their key network equipment, and strengthen the establishment of defense-in-depth (DiD) technology capabilities. For

vehicle-to-everything (V2X) communications, promote public key infrastructure (PKI)-based security authentication and audit technology and accelerate the establishment of IoV identity authentication and secure trusted systems (安全信任体系). For IoV platforms and applications, build a security operations center to promote the implementation of technology products such as integrated cloud security protection, data compliance protection, and security detection, monitoring, and emergency response. Promote the application and deployment of cybersecurity technologies in key settings such as over-the-air (OTA) updates, remote monitoring, autonomous driving, and vehicle-road collaboration.

Industrial Internet and Industrial Control Security: For the entire business workflow of the Industrial Internet, focusing on equipment, control systems, networks, identifiers, platforms, and data security protection requirements, accelerate industrial host snapshot rollbacks, control system vulnerability discovery, control system endogenous security, and other industrial control security technology research, achieve breakthroughs in protocol inverse analysis, lightweight authenticated encryption, high-traffic security analysis, industrial cybersecurity threat information sharing analysis, and other Industrial Internet security technologies. Strengthen the promotion and application of security products such as industrial-grade protection equipment, trusted access for massively connected (海量联网) devices, platform security, identifier analysis security management, and industrial data full life cycle protection, and enhance Industrial Internet scenario-based security protection capabilities.

IoT Security: Actively promote cybersecurity applications in IoT scenarios such as smart energy, smart agriculture, smart home, and smart wearable devices, and encourage enterprises to develop end-to-end security protection solutions that suit heterogeneous IoT scenarios. For IoT platforms, develop platform security products based on technologies such as secure transmission, abnormal activity analysis, trusted identity, threat analysis, and data loss prevention (DLP). For the trusted access gateways of IoT devices, accelerate the development of identification, protocol analysis, and security detection and analysis technologies and encourage enterprises to integrate more security capabilities into gateways. For IoT terminals, strengthen vulnerability discovery for IoT devices and firmware, develop embedded intensive security products that integrate interface protection, security certification, application security, and sensitive data protection so as to create a safe IoT.

Smart City Security: Adapt to business scenarios such as smart city government affairs, transportation, energy, manufacturing, education, and healthcare, build a “one brain, three clouds” (“一脑，三云”) cybersecuritydefense capabilities cluster, strengthen the level of heterogeneous security capability linkages, and create

a dynamic security defense system. Encourage the creation of smart city security brains (安全大脑), the construction of cybersecurity "smart clouds," the establishment of panoramic security knowledge bases, cybersecurity monitoring and analysis engines, and big data centers so as to enhance cybersecurity awareness, analysis, response, and decision-making capabilities from a global perspective. Create cybersecurity “range clouds” (“靶场云”), build digital twin ranges (数字孪生靶场), and provide support for the verification of urban security capabilities. Build cybersecurity “service clouds” and gather service resources such as smart city security planning, construction, and operations to ensure the secure and orderly operation of cities.

(3) Initiatives for deepening industry integration

11. Increase investment in industrial funds. Guide government guidance funds such as the National Manufacturing Industry Transformation and Upgrading Fund (国家制造业转型升级基金) to tilt towards fields such as new cybersecurity technologies, new models, and integration and innovation, and promote the establishment of national-level cybersecurity industry guidance funds at an appropriate time to accelerate the mature implementation of new products and services in the market. Encourage local governments to include the cybersecurity industry in the investment categories for government guidance funds and to support the development of local cybersecurity enterprises.

12. Channel capital to accurately support enterprise development. Encourage various types of capital to establish S&T innovation funds, focus on industrial technological innovation and core technology research, explore “technological donation” (“科技捐赠”) and intellectual property and options-based financing models, guide the capital market to invest early with small investments, and help growth companies strengthen their technological advantages and thoroughly develop their market segments towards specialization and precision. Encourage cybersecurity companies with strong foundations to go public, support leading companies in integrating resources through strategic investment so that they may become bigger and stronger, and enhance their ability to lead the cybersecurity ecosystem.

13. Strengthen the construction of industry integration mechanisms. Encourage industry integration pilot cities to boost investment and deepen cybersecurity industry integration. Improve the dynamic monitoring systems of industry and finance and regularly carry out dynamic monitoring of venture capital, equity investment, corporate mergers and acquisitions, and the operation of listed companies in the field of cybersecurity so as to promote precision linking (精准对接) of industry and finance. Promote the establishment of an evaluation system suited to the

characteristics of the cybersecurity industry and targets different stages of enterprise development, support the evaluation of high-growth enterprises and high-value projects, and coordinate the transformation of achievements (成果转换) in information sharing and credit evaluation.

Focus 3: Cybersecurity Industry Capital Empowerment Project
Improve cybersecurity industry integration mechanisms. Give full play to the role of MIIT as a platform for national industry integration, strengthen the exchange and sharing of information on fiscal, taxation, and financial policies, financing needs, and financial products and services, and promote the precision linking of cybersecurity, industry, and finance. **Actively develop secure industrial finance services.** Establish the "Cybersecurity Industry Capital Innovation Forum" (“网络安全产业资本创新论坛”), actively carry out multi-level industry-finance linkage and consulting services such as listing guidance, corporate roadshows, project promotions, financing training, and the like, and give full play to the role of the full application of financial capital in boosting and upgrading industrial development. **Explore the development of cybersecurity insurance.** Carry out cybersecurity insurance service pilot projects in areas such as telecommunications and the internet, the Industrial Internet, and IoV. Accelerate cybersecurity insurance policy guidance and standards formulation, monitor risk exposure through cybersecurity insurance services, encourage companies to build and improve their own cybersecurity risk management systems, and strengthen cybersecurity risk response capabilities. **Explore and carry out cybersecurity enterprise value assessments.** For the different stages of enterprises and their different cybersecurity segmentation tracks, encourage industry and capital to jointly establish value evaluation models and detailed indicators and to explore the release of high-growth enterprise lists and high-value project catalogs.

(4) Initiatives to build a cadre of talent

14. Give full play to the leading role of leading talents. Cultivate a group of leading talents with outstanding capabilities in theoretical research, technological innovation, the conversion of technical achievements into practical applications (成果转化), and application experience. Encourage enterprises, institutions of higher education, and scientific research institutions to improve incentive mechanisms for leading talents by establishing workspaces (工作室) and by providing scientific research funding,

equity incentives, and talent exchanges. Encourage institutions of higher education, scientific research institutions, and enterprises to attract high-level talents and innovative teams from around the world through various channels such as international cooperation.

15. Deepen the integration of industry and education with collaborative education. Prompt institutions of higher education to strengthen cybersecurity curricula and majors. Promote cybersecurity school-enterprise collaboration, support and prompt institutions of higher education, research institutions, and enterprises to jointly build cybersecurity training bases and joint laboratories to create a "double-teacher" faculty team and enhance the practical acumen of cybersecurity talents. Give full play to the role of industry-specific institutions of higher education and vocational colleges to develop more cybersecurity skills and service-oriented talents. Actively carry out cybersecurity education and training activities, encourage the holding of multi-level and diversified cybersecurity capability competitions, and cultivate high-quality cybersecurity talents.

16. Promote the evaluation of cybersecurity talents. Carry out industrial vocational skill improvement campaigns in the communications industry and train and select cybersecurity professionals through computer technology and software professional technical qualification (level) examinations, the China Industrial Internet Security Competition (全国工业互联网安全技术技能大赛), and other such methods. For key industries such as equipment manufacturing, raw materials, consumer products, and electronic information, build "X + Security" talent evaluation systems and establish sound cybersecurity talent selection and evaluation mechanisms.

(5) Industrial ecosystem optimization initiatives

17. Guide the clustering of the cybersecurity industry. Create cybersecurity industrial park layouts with "multi-point support, radiation across the country, complementary advantages, and coordinated development," actively promote the establishment of the Beijing and the Changsha, Hunan national cybersecurity industrial parks, and give full play to the industrial advantages of Chengdu, Chongqing, the Yangtze River Delta, and the Pearl River Delta to accelerate the layout of national cybersecurity industrial parks. Actively build a number of leading and inspiring advanced pilot areas for cybersecurity innovation applications.

18. Promote the establishment of innovation consortia. Prompt basic telecommunications operators, industry users, scientific research institutions, institutions of higher education, and security companies to establish cybersecurity joint innovation centers and joint laboratories, strengthen basic cybersecurity theoretical

research, promote the application and conversion of research results into commercial products (研究成果应用转化), and enhance our innovation capabilities for key and core technologies in the cybersecurity domain. Give full play to the role of corporate alliances and associations in cybersecurity-related industries, promote the flow of innovation factors of production, integrate technological advantages and resource advantages, and spur innovation through various forms such as technological research, project collaboration, talent training, and park construction.

19. Foster a fair and competitive market environment. Support the development of cybersecurity product and service capability evaluations, cybersecurity project building and system operations and maintenance (O&M) quality evaluations, and security assessments for new technologies and new lines of business. Integrate factors such as enterprise product and service quality, contributions to [identifying] vulnerabilities (漏洞贡献), threat information sharing, and malicious competition, strengthen corporate credit system establishment, gradually establish corporate "red lists and blacklists," continuously improve market transparency, and guide the formation of a market environment of healthy competition underpinned by product service capabilities.

Focus 4: Cybersecurity Industry Ecosystem Cultivation Project
Establish a cybersecurity product and service capability evaluation system. Gather together the technology products of key links upstream and downstream in the cybersecurity production chain, draw a map of the cybersecurity production chain, and continue to conduct research on and evaluation of major risks in the cybersecurity industry. For overall key functional performance, capability maturity, application efficacy, cybersecurity service levels, and other such factors for cybersecurity products, respectively formulate cybersecurity product and service capability evaluation specifications and publicly release evaluation results. **Improve cybersecurity threat information sharing service systems and mechanisms.** Establish rules and mechanisms for the discovery, disclosure, circulation, and utilization of threat information such as driver vulnerabilities, malicious programs, malicious addresses, and attack behaviors. Encourage cybersecurity companies, industry users, scientific research institutions, and universities to actively participate in information sharing and improve the level of aggregation of threat information service capabilities. **Strengthen the demonstration and promotion of advanced technology applications.** For key directions such as 5G, IoV, the Industrial Internet, and the IoT, carry out the selection of outstanding security products and solutions and push the

application and promotion of pilot demonstration projects in various key industries through exchanges and forums, competitions, and supply-demand linking, and continue to spur innovation and promote the conversion of technical achievements into practical applications.

Cultivate high-quality corporate benchmarks for cybersecurity. Encourage enterprises to increase investment in research and development (R&D) and strengthen intellectual property protection and technological innovation. Encourage enterprises with strong comprehensive strength and strong influence in domestic and foreign technology, standards, and markets to further integrate the production chain, supply chain, and innovation chain to become production chain leaders. For outstanding enterprises in the cybersecurity product market segment, strengthen support for technology research and development, product promotions, and supply-demand linking through policy guidance, leaning in to projects (项目倾斜), and talent cultivation, and accelerate the cultivation of cybersecurity single-product champions and professional, meticulous, specialized, and innovative "little giant" enterprises.

III. Assurance Measures

(1) Strengthen organization and leadership. Strengthen the organization and leadership of departments in charge of industry and information technology and telecommunications administrations at the local level, strengthen departmental coordination, and actively promote the inclusion of the cybersecurity industry in the local overall planning for the 14th Five-Year Plan and in the major contents of related special plans. Strengthen the categorized guidance of cybersecurity construction in different industries, different fields, and different entities, promote the differentiated layout of the development of the cybersecurity industry, establish and improve the cybersecurity assurance system, and create a sound environment conducive to the development of the cybersecurity industry.

(2) Strengthen policy guidance. Make full use of existing policies such as cybersecurity technology application pilot demonstrations, first units (sets) (手台（套）), and special projects, promote research and formulate targeted support policies in areas such as finance, talent cultivation, and industrial clustering for cybersecurity companies at different stages of development that suit actual local conditions. Formulate targeted support policies, strengthen government-enterprise coordination and ministry-province linkages, and form a joint force to promote the close integration of the cybersecurity industry and the development of local digital economies. Encourage local governments to simultaneously construct cybersecurity technical measures informatization projects

that they are supporting through fiscal investment and encourage them to strengthen the review of cybersecurity aspects in the project acceptance phase. Encourage enterprises in key industries to increase investment in cybersecurity, set separate budgets for cybersecurity, and promote the deployment and application of cybersecurity technologies, products, and services.

(3) Enhance industrial coordination. Establish the MIIT Expert Advisory Committee on the High-Quality Development of the Cybersecurity Industry (工业和信息化部网络安全产业高质量发展专家咨询委员会) to provide consultation and recommendations on major issues and policy implementation. Give full play to all forces of industry, academia, research, users, and capital (产学研用资), strengthen the connection between supply and demand, coordinate the development of standards, personnel training, and conversion of technical achievements into practical applications, strengthen industry self-discipline, and create an industry ecosystem conducive to healthy and orderly development.

(4) Promote international cooperation. Make full use of bilateral and multilateral mechanisms, actively participate in the formulation of international cybersecurity rules and international security standards in key areas, and strengthen cybersecurity policies, regulations, and industry exchanges and collaborations. Support enterprises that set up overseas R&D centers and joint laboratories, support various cybersecurity conferences, forums, exhibitions, and other exchange activities, and strive to build multi-level, normalized industrial collaboration and exchange mechanisms.