In order to implement the "Cybersecurity Law of the People's Republic of China", vigorously develop the cybersecurity industry, the Ministry of Industry and Information Technology has drafted the "Guiding Opinions concerning Stimulating the Development of the Cybersecurity Industry (Opinion-seeking Draft)" (see below), which is hereby published to society for the solicitation of opinions, please provide feedback before 11 October 2019.

Contact telephone: 010-66022774
E-mail: wangmeifang@miit.gov.cn

Guiding Opinions concerning Stimulating the Development of the Cybersecurity Industry (Opinion-seeking Draft)

Without cybersecurity, there is no national security, there will be no stable functioning of the economy and society, and the interests of the broad popular masses will be difficult to protect. At present, cyber attacks, hacking intrusions, malicious code and security vulnerabilities of all kinds and forms emerge one after another, constituting a grave threat against the security of critical information infrastructure, the security of data, and the security of personal information. The essence of cybersecurity is technological opposition, and guaranteeing cybersecurity cannot be separated from powerful support of cybersecurity technology and industry. In recent years, our country's cybersecurity industry has grown rapidly in scale, products and systems have become correspondingly perfected, innovative capabilities have progressively strengthened, and the development environment has clearly improved, but in comparison with cybersecurity protection requirements, problems such as deficiencies in core technology, the fact that the industry scale is relatively small, that market demand is insufficient and industrial coordination is not enough still exist. In order to vigorously develop the cybersecurity industry, enhance cybersecurity technology support and protection levels, these Guiding Opinions are formulated.

I, General requirements

(1) Guiding ideology

With Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era as guidance, deeply implement the spirit of the series of General Secretary Xi Jinping's speeches on cybersecurity, uphold new development ideas, establish correct cybersecurity views, implement the "Cybersecurity Law", take serving the national cyberspace security strategy requirements as guidance, actively respond to new risks emerging on the Internet, in big data, artificial intelligence and the deep integration with the real economy, vigorously respond to new challenges brought by new technologies and new applications such as 5G, the industrial Internet, next-generation Internet, persist in market guidance and government leadership, strive to make breakthroughs in critical technologies, building industrial ecologies and optimizing development atmospheres, promote our country's cybersecurity industry to develop at high quality, and provide powerful industrial support for safeguarding national cyberspace security and protecting the construction of a strong cyber power.

(2) Basic principles

Innovation-driven. Forcefully promote technological and product innovation, make breakthroughs in technological bottlenecks, and strive to enhance core cybersecurity technology capabilities. Innovate cybersecurity service models, enhance specialized

cybersecurity services levels, and realize the progressive transformation of industrial development from being product-led to being services-led.

Coordinated development. Fully muster forces from all sides, strengthen cooperation between industry, education and research, encourage the transformation of technological achievements, promote links between various strong elements and tackling strategic junctures in a coordinated manner, build an industrial ecological system with participation from many sides, mutually supporting advantages, and integrated development. Promote asset cooperation, and guide social capital to participate in the development of the cybersecurity industry.

Demand-led. Promote all sectors and all areas to continue to expand cybersecurity input, persist in being problem-oriented, strengthen supply-demand linkages, spur the industry to satisfy the cybersecurity demands of finance, energy, telecommunications, transportation, e-government and other such focus areas ever better.

Openness and cooperation. Promote international exchange and cooperation in the cybersecurity industry, study and learn from foreign industry development models, stimulate technology and talent exchange as well as information sharing, vigorously participate in the construction of the "Belt-Road Initiative" and enhance the international competitiveness of the industry.

(3) Development objectives

Cybersecurity technology innovation capabilities are to strengthen clearly, cybersecurity product and services systems are to become ever more complete, cybersecurity professional talent ranks are to grow daily, a cybersecurity industry structure with coordinated development between government, industry, education, research, users and finance is to become incessantly more consolidated, industrial development environments are to improve more, the cybersecurity industry's supporting ability in safeguarding national cyberspace security and protecting the construction of a strong cyber power are to increase substantially. By 2025, a batch of cybersecurity enterprises with annual revenues in excess of 2 billion are to be fostered and created, some cybersecurity backbone enterprises with international competitiveness are to be created, and the scale of the cybersecurity industry is to exceed 200 billion.

II, Main tasks

(1) Strive to make breakthroughs in critical cybersecurity technology

With building advanced and complete cybersecurity product systems as the objective, focus on demands in segments such as ex0-ante cybersecurity prevention, monitoring in medias res and response ex post, forcefully promote the gradual upgrading of cybersecurity products such as asset identification, vulnerability detection, virus scanning and killing, boundary protection, intrusion defence, source code monitoring, data protection, tracing to the source, etc., strive to enhance risk investigation, situation sensing, emergency response processing and source tracing capabilities. Strengthen cybersecurity threat and risk analysis in emerging areas such as 5G, next-generation Internet, industrial Internet, the Internet of Things, the Internet of Cars, etc., forcefully promote the research and development of cybersecurity technologies and products in relevant settings. Support the application of technologies such as cloud computing, big data, artificial intelligence and quantum computing in the area of cybersecurity, strive to enhance threat intelligence analysis, smart monitoring and waning, encrypted telecommunications and other such cybersecurity de-

fence capabilities. Vigorously explore new cybersecurity concepts and new frameworks such as mimicry defence, trusted computing, zero-trust security, etc., and promote innovation in cybersecurity theories and technologies.

(2) Vigorously innovate cybersecurity service models

Countering cybersecurity's characteristics of being strongly specialized, technology evolving rapidly and the difficulty of application is great, initiate "security and service" concepts, cybersecurity enterprises are encouraged to transform from providing security products to providing security services and solutions. Support specialized bodies and enterprises to engage in security services such as cybersecurity planning and consulting, threat intelligence, risk assessment, monitoring and certification, security integration, emergency response, etc., standardize activities such as vulnerability scanning, disclosure, etc. Support lawfully established certification bodies to launch cybersecurity certification according to the law. Forcefully develop cloud model-based cybersecurity public service platforms, provide long-distance real-time online vulnerability discovery, website protection, resistance services against attacks, domain name security and other such services. Basic telecommunications enterprises and cloud service providers are encouraged to give their advantages in network resources full rein, and provide cybersecurity monitoring and warning, attack prevention, emergency response protection and other such value-added services to users. Encourage the development of integrated cybersecurity operations outsourcing services aimed at smart city construction, e-government and other such areas. Explore the launch of cybersecurity insurance services.

(3) Join forces to forge a cybersecurity industry ecology

Support leading and backbone enterprises in integrating cybersecurity innovation chains, industry chains and value chains, establish open cybersecurity technology research and development, standards and testing, and achievement transformation platforms, unblock channels for the linkage and transformation of innovation capabilities, realize multi-dimensional and multi-contact point innovation capability sharing, innovation achievement transformation and brand coordination between large, mid-size and small enterprises. Strive to foster small and mid-size cybersecurity enterprises with prominent operational activities, strong competitiveness and good growth prospects, encourage mutual cooperation with large enterprises through such means as specialized division of labour, service outsourcing, shared research and development, etc., create coordinated and mutually beneficial structures. Fully muster the vigour and initiative of subjects from all kinds of parks, enterprises, scientific research institutions, financial bodies, etc., encourage their collected, intensive, interconnected, interlinked and collaborative development. Foster and build a batch of new innovation platforms and labs with coordinated cybersecurity technologies and products, launch joint research on important questions of a public nature and in the direction of urgent market demand, give full rein to the supporting and guiding role of science and technology, promote research, development, popularization and application of industrial technology of a public nature, and guide the concentration of innovation resources. Encourage enterprises, research bodies, higher education institute and sectoral organizations to vigorously participate in the formulation of cybersecurity-related national standards and sectoral standards.

(4) Forcefully promote the application of cybersecurity technology

Fully give rein to the role of Party and government bodies and related sectoral supervisory departments, promote the deployment and usage of advanced applied cybersecurity technologies, products and services in important areas such as finance, energy, telecommunications, transportation, e-government, etc., Strengthen management of the industrial Internet, the Internet of Cars and the Internet of Things, supervise and guide related enterprises to adopt the necessary technical cybersecurity measures. Forcefully stimulate the application of commercial encryption technology in cybersecurity protection. Government-invested informatization projects shall simultaneously provide complementary measures to build cybersecurity technology, and security verification will be conducted individually. Expand support for and dissemination of cybersecurity technology application pilots and demonstration projects, encourage demonstration enterprises to transform solutions and plans into standards and guidelines, and launch specialized publicity. Encourage the launch of cybersecurity technology forums and demonstration activities for products and services.

(5) Accelerate the construction of cybersecurity infrastructure

Stimulate related sectoral controlling departments and local governments to establish cybersecurity situation sensing platforms for their sectors and their localities, strive to enhance capabilities to support cybersecurity management and respond to organized and high-strength attacks. Focus sectors and backbone enterprises are encouraged to establish vulnerability databases, virus databases and other such basic cybersecurity resource bases, and stimulate information sharing between corresponding subjects. Comprehensively plan and construct national cybersecurity information sharing platforms and emergency command platforms, realize cross-enterprise, cross-sector and cross-regional information sharing and coordination linkages. Focus on new application scenes such as the industrial Internet, Internet of Cars and Internet of Things in building basic platforms of a public nature for cybersecurity testing and certification, training and practice, as well as equipment security testing, etc. Support the construction of network identity authentication systems based on commercial encryption, fingerprint recognition, facial recognition and other such technologies.

III, Guarantee measures

(1) Strengthen organizational leadership

All local related departments must fully understand the importance of the cybersecurity industry from the height of the strong cyber power strategy, strengthen organizational leadership and comprehensive planning, strengthen department cooperation, and jointly build a desirable environment beneficial to the development of the cybersecurity industry. Deeply implement the "Cybersecurity Law", accelerate the formulation of complementary regulations and policies, expand cybersecurity supervision and management forces, supervise network operators' implementation of technical cybersecurity measures, and drive cybersecurity market demand.

(2) Strengthen policy support

The Centre's Cyberspace Administration will guide and support the construction of national cybersecurity talent and innovation bases, together with relevant ministries and commissions, it will stimulate mutual recognition of certification for critical

network equipment and specialized cybersecurity products, and of security monitoring results, avoiding duplicate certification and monitoring. The Ministry of Industry and Information Technology will promote the construction of national cybersecurity industry parks, establish cybersecurity industry operational monitoring systems, organize the launch of cybersecurity technology application pilots and demonstrations, and guide the organization of the China Cybersecurity Industry Summit Forum. The National Development and Reform Commission will strengthen planning, policy research and formulation in the cybersecurity area. The central financial administration will plan the use of existing channels such as the China Internet Investment Fund, to guide and support the development of the cybersecurity industry. All localities may, in integration with their actual local circumstances, formulated targeted industrial support policies in areas such as finance, talent attraction, factor guarantees, etc.

(3) Complete talent training systems

Stimulate higher education institutes to establish cyberspace security academies or cybersecurity-related specializations, strengthen the construction of first-rate cybersecurity academies and qualified cybersecurity ranks. Strengthen cybersecurity vocational education and skills training, and foster ever more practically skilled talents. Promote the linkage of education and enterprises, support the establishment of joint cybersecurity labs. Encourage the organization of high-level cybersecurity skills competitions, complete talent discovery and promotion mechanisms. Support professional skills appraisal bodies and sectoral organizations to launch cybersecurity personnel skills appraisal and competence assessment work.

(4) Moving international exchange and cooperation forward

Use various kinds of multilateral and bilateral dialogue mechanisms or activity platforms to strengthen pragmatic cooperation and exchange concerning cybersecurity technology and industries. Powerful cybersecurity enterprises are encouraged to establish foreign research and development centres and joint laboratories, attract foreign high-end talents and advanced technologies. It is encouraged to participate in and organize influential international cybersecurity forums and exhibitions, and vigorously participate in international cybersecurity standard formulation and coordination. Promote related localities to give rein to their local advantages, to forge international and regional cybersecurity technology, industry and talent exchange platforms.