关键信息基础设施安全保护条例

(征求意见稿)

Regulation on the Protection of the Security of Critical Information Infrastructure

(Draft for the Solicitation of Comment)

第一章 总则

Chapter 1 General

第一条 为了保障关键信息基础设施安全，根据《中华人民共和国网络安全法》，制定本条例。

Article 1 This Regulation has been drawn up in accordance with the *P.R.C. Cybersecurity Law* for the purpose of safeguarding the security of critical information infrastructure.

第二条 在中华人民共和国境内规划、建设、运营、维护、使用关键信息基础设施，以及开展关键信息基础设施的安全保护，适用本条例。

Article 2 This Regulation applies to the planning, construction, operation, maintenance and use of critical information infrastructure, and to the protection of the security of critical information infrastructure, within the territory of the People's Republic of China.

第三条 关键信息基础设施安全保护坚持顶层设计、整体防护，统筹协调、分工负责的原则，充分发挥运营主体作用，社会各方积极参与，共同保护关键信息基础设施安全。

Article 3 The protection of the security of critical information infrastructure will uphold the principles of top-level design, integrated protection, overall planning and coordination, and division of individual responsibility. It will fully bring to bear the actions of the operating entity, and the affirmative participation of each member of society, to jointly protect the security of critical information infrastructure.

第四条 国家行业主管或监管部门按照国务院规定的职责分工，负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。

Article 4 The national industry regulatory or supervisory departments will have the responsibility to guide and oversee the protection of the security of critical information

infrastructure within their own industry sectors and their own fields, in accordance with the division of duty stipulated by the State Council.

国家网信部门负责统筹协调关键信息基础设施安全保护工作和相关监督管理工作。国务院公安、国家安全、国家保密行政管理、国家密码管理等部门在各自职责范围内负责相关网络安全保护和监督管理工作。

The national network information departments will undertake responsibility to coordinate the protection of the security, and related supervision and management, of critical information infrastructure. Agencies such as the public security, national security, national secrets management administration, and national password management of the State Council will within the scope of their respective official responsibilities undertake responsibility for the relevant protection of the security of networks and supervision and administration.

县级以上地方人民政府有关部门按照国家有关规定开展关键信息基础设施安全保护工作。

Relevant agencies of the local People's Governments at the county level or higher will launch the protection of the security of critical information infrastructure in accordance with relevant national stipulations.

第五条 关键信息基础设施的运营者（以下称运营者）对本单位关键信息基础设施安全负主体责任，履行网络安全保护义务，接受政府和社会监督，承担社会责任。

Article 5 Operators of critical information infrastructure (hereinafter referred to as operators) will bear principal responsibility for the safety of the critical information infrastructure of their own Entity (*danwei*), perform the duties of network security protection, accept the oversight of the government and society, and shall undertake responsibility for the overall well-being of society.

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

The State encourages network operators that are not operating critical information infrastructure to voluntarily participate in the system for the protection of critical information infrastructure.

第六条 关键信息基础设施在网络安全等级保护制度基础上，实行重点保护。

Article 6 Protection will be implemented with an emphasis on critical information infrastructure on the basis of the multi-level protection system for network security.

第七条 任何个人和组织发现危害关键信息基础设施安全的行为，有权向网信、电信、公安等部门以及行业主管或监管部门举报。

Article 7 Any individual or organization has the right, when discovering acts that threaten the security of critical information infrastructure, to make a report to agencies such as the network information, telecommunications and public security agencies, and to industry regulatory or supervisory agencies.

收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

The agency which receives the report should handle it promptly and in accordance with law; where it does not fall within the official responsibility of that agency, it should promptly transfer it to the agency that has the authority to handle it.

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

The relevant agencies should maintain the related information of the reporting person in confidentiality, and protect the lawful interests of the reporting person.

第二章 支持与保障

Chapter 2 Support and Safeguards

第八条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动。

Article 8 The State will adopt measures, monitoring and defenses, dispose of risks and threats to network safety that originate from within and outside the territory of the People’s Republic of China, protect critical information infrastructure from attacks, intrusions, interference and destruction, and in accordance with law mete out punishment of activities on the Internet that offend and violate the law.

第九条 国家制定产业、财税、金融、人才等政策，支持关键信息基础设施安全相关的技术、产品、服务创新，推广安全可信的网络产品和服务，培养和选拔网络安全人才，提高关键信息基础设施的安全水平。

Article 9 The State will formulate policies relating to industry, fiscal and tax matters, finance, training and qualification and so forth, to support innovation in technology, products and services that relate to the safety of critical information infrastructure, promote secure and

reliable network products and services, select and train competent network security personnel, and raise the level of security of critical information infrastructure.

第十条 国家建立和完善网络安全标准体系，利用标准指导、规范关键信息基础设施安全保护工作。

Article 10 The State will establish a system of standards for network security and will bring it to its completion. It will make good use of the standards to provide direction and regulation to the protection of the security of critical information infrastructure.

第十一条 地市级以上人民政府应当将关键信息基础设施安全保护工作纳入地区经济社会发展总体规划，加大投入，开展工作绩效考核评价。

Article 11 Local People's Governments above the municipal levels should incorporate the protection of the security of critical information infrastructure into the overall regional economic and social development planning, increasing their inputs, and implementing the evaluation and assessment of the performance of the work.

第十二条 国家鼓励政府部门、运营者、科研机构、网络安全服务机构、行业组织、网络产品和服务提供者开展关键信息基础设施安全合作。

Article 12 The State encourages governmental departments, operators, scientific research agencies, network safety service agencies, industry organizations, and providers of network products and services to cooperate on the safety of critical information infrastructure.

第十三条 国家行业主管或监管部门应当设立或明确专门负责本行业、本领域关键信息基础设施安全保护工作的机构和人员，编制并组织实施本行业、本领域的网络安全规划，建立健全工作经费保障机制并督促落实。

Article 13 National industry regulatory or supervisory departments should set up or make clear agencies and personnel that specially undertake responsibility for the protection of the security of critical information infrastructure in their own industry sectors or their own fields; formulate and implement the network security plan in their own industry sectors or their own fields; and establish and improve mechanism to assure funding for the work, and urge its implementation.

第十四条 能源、电信、交通等行业应当为关键信息基础设施网络安全事件应急处置与网络功能恢复提供电力供应、网络通信、交通运输等方面的重点保障和支持。

Article 14 Industry sectors such as energy, telecommunications and transportation should provide priority safeguards and support in aspects such as electricity supply, network connectivity, transport and shipping, for emergency responses to network security incidents and network function recovery of critical information infrastructure.

第十五条 公安机关等部门依法侦查打击针对和利用关键信息基础设施实施的违法犯罪活动。

Article 15 Departments such as the public security agencies will in accordance with law investigate and strike down illegal and criminal activities that are directed towards and make use of critical information infrastructure.

第十六条 任何个人和组织不得从事下列危害关键信息基础设施的活动和行为：

Article 16 No person or organization shall engage in the following activities and acts which jeopardize critical information infrastructure:

（一）攻击、侵入、干扰、破坏关键信息基础设施；

（1）attacking, intruding upon, interfering with or destroying critical information infrastructure;

（二）非法获取、出售或者未经授权向他人提供可能被专门用于危害关键信息基础设施安全的技术资料等信息；

（2）Unlawfully obtaining, selling or providing to other persons without authorization information such as technical materials that could be specifically used to jeopardize the security of critical information infrastructure;

（三）未经授权对关键信息基础设施开展渗透性、攻击性扫描探测；

（3）Launching unauthorized scanning and diagnostics, that infiltrates or attacks, at critical information infrastructure;

（四）明知他人从事危害关键信息基础设施安全的活动，仍然为其提供互联网接入、服务器托管、网络存储、通讯传输、广告推广、支付结算等帮助；

（4）Providing such assistance as Internet connections, server hosting, network storage, communication transmissions, advertising and promotion, or payment settlement to another person while still having clear knowledge that that person is engaged in activities that jeopardize the security of critical information infrastructure;

（五）其他危害关键信息基础设施的活动和行为。

（5）Other activities and acts which jeopardize critical information infrastructure.

第十七条 国家立足开放环境维护网络安全，积极开展关键信息基础设施安全领域的国际交流与合作。

Article 17 The State will base itself upon an open environment in maintaining network security, and will affirmatively launch international exchanges and cooperation in the field of critical information infrastructure security.

第三章 关键信息基础设施范围

Chapter 3 Scope of Critical Information Infrastructure

第十八条 下列单位运行、管理的网络设施和信息系统，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，应当纳入关键信息基础设施保护范围：

Article 18 Network facilities and information systems which are operated and managed by the Entities (*danwei*) listed below, which once having suffered destruction, loss of functionality or leakage of data, could severely endanger national security, the national economy and the people's livelihood and the public interest, should be brought into the scope of the protection of critical information infrastructure:

（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；

（1）Governmental agencies and Entities (*danwei*) which are in industry sectors and fields such as energy, finance, transportation, water conservancy, hygiene and medical care, education, social insurance, environmental protection, and public utilities;

（二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；

（2）Information networks such as telecommunications networks, television broadcast networks and the Internet, and Entities (*danwei*) which provide cloud computing, big data and other large-scale public information network services;

（三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；

（3）R&D and manufacturing Entities (*danwei*) which are in industry sectors and fields such as science and technology for national defense, large equipment manufacturing, chemicals, and food and drug;

（四）广播电台、电视台、通讯社等新闻单位；

（4）News organizations (*danwei*), such as broadcasting stations, television stations and news agencies; and

（五）其他重点单位。

（5）Other critical organizations (*danwei*).

第十九条 国家网信部门会同国务院电信主管部门、公安部门等部门制定关键信息基础设施识别指南。

Article 19 The national cyberspace administration departments will, acting jointly with departments such as the telecommunications authority and the public security department of the State Council, formulate a handbook for identifying critical information infrastructure.

国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施，并按程序报送识别结果。

The national industry regulatory or supervisory departments will, in accordance with the handbook for identifying critical information infrastructure, identify critical information infrastructure within their own industry sectors and their own fields, and report the results of their identification in accordance with procedures.

关键信息基础设施识别认定过程中，应当充分发挥有关专家作用，提高关键信息基础设施识别认定的准确性、合理性和科学性。

In the course of identifying and recognizing critical information infrastructure, the role of relevant experts should be fully taken into account, to make the identification and recognition of critical information infrastructure more accurate, reasonable and scientific.

第二十条 新建、停运关键信息基础设施，或关键信息基础设施发生重大变化的，运营者应当及时将相关情况报告国家行业主管或监管部门。

Article 20 Operators of critical information infrastructure which has been newly constructed or the operation of which has been suspended, or where a major change to the critical information infrastructure has occurred, should promptly report the relevant circumstances to the national industry regulatory or supervisory departments.

国家行业主管或监管部门应当根据运营者报告的情况及时进行识别调整，并按程序报送调整情况。

The national industry regulatory or supervisory departments should promptly carry out an adjustment of their identification on the basis of the circumstances reported by the operator, and report the results of their adjustment in accordance with procedures.

第四章 运营者安全保护

Chapter 4 Operator Safety Protection

第二十一条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

Article 21 The construction of critical information infrastructure should ensure that it possesses stable supporting operations and operational continuity capabilities, and guarantee that safety technology measures will be planned in step, constructed in step, and put into use in step.

第二十二条 运营者主要负责人是本单位关键信息基础设施安全保护工作第一责任人，负责建立健全网络安全责任制并组织落实，对本单位关键信息基础设施安全保护工作全面负责。

Article 22 The person with principal responsibility for an operator is the person who bears first responsibility for protection of the security of critical information infrastructure of that Entity (*danwei*), and has responsibility for establishing, improving and bringing into actual practice a system of responsibility for network security, and has overall responsibility for the protection of the security of the critical information infrastructure of his or her own Entity (*danwei*).

第二十三条 运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障关键信息基础设施免受干扰、破坏或者未经授权的访问，防止网络数据泄漏或者被窃取、篡改：

Article 23 Operators should, in accordance with the requirements of the multi-level network protection system, perform the following security protection obligations, to ensure that critical information infrastructure is safe from interference, destruction or unauthorized access, and to prevent the leakage, theft or falsification of internet data:

（一）制定内部安全管理制度和操作规程，严格身份认证和权限管理；

（1）Formulate an internal security management system and operating procedures, and adopt strict authentication and authorization management;

（二）采取技术措施，防范计算机病毒和网络攻击、网络侵入等危害网络安全行为；

（2）Adopt technological measures, to prevent computer viruses and actions which jeopardize network security such as network attacks and network intrusions;

（三）采取技术措施，监测、记录网络运行状态、网络安全事件，并按照规定留存相关的网络日志不少于六个月；

（3）Adopt technological measures, for monitoring and recording of operational status and network security incidents, and in accordance with stipulations retain relevant network logs for not less than six months;

（四）采取数据分类、重要数据备份和加密认证等措施。

（4）Adopt measures such as data classification, backing up of important data, and encryption and authentication.

第二十四条 除本条例第二十三条外，运营者还应当按照国家法律法规的规定和相关国家标准的强制性要求，履行下列安全保护义务：

Article 24 Other than Article 23 of this Regulation, operators still should in accordance with the stipulations of national laws and regulations and the mandatory requirements of relevant national standards, perform the following security protection obligations:

（一）设置专门网络安全管理机构和网络安全管理负责人，并对该负责人和关键岗位人员进行安全背景审查；

（1）Establish specialized network security management departments and persons who bear responsibility for network security management, and carry out security background investigations on such responsible persons and personnel in key positions;

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（2）Carry out periodic network security education, technological training and skills evaluation for working personnel;

（三）对重要系统和数据库进行容灾备份，及时对系统漏洞等安全风险采取补救措施；

（3）Implement disaster recovery backups for important systems and databases, and promptly adopt remedial measures for network risks such as system leakages;

（四）制定网络安全事件应急预案并定期进行演练；

（4）Formulate contingency plans for network security incidents and carry out periodic drills;

（五）法律、行政法规规定的其他义务。

（5）Other obligations stipulated under law or administrative regulation.

第二十五条 运营者网络安全管理负责人履行下列职责：

Article 25 Persons bearing responsibility for an operator's network security management will perform the following responsibilities:

（一） 组织制定网络安全规章制度、操作规程并监督执行；

（1） Formulate regulations, systems and operational procedures for network security, and oversee the implementation;

（二）组织对关键岗位人员的技能考核；

（2）Conduct evaluations of the skills of personnel in key positions;

（三）组织制定并实施本单位网络安全教育和培训计划；

（3）Formulate and implement a program for network security training and education in their own Entity (*danwei*);

（四）组织开展网络安全检查和应急演练，应对处置网络安全事件；

（4）Launch network security inspection and emergency response drills for the response to and handling of network security incidents; and

（五）按规定向国家有关部门报告网络安全重要事项、事件。

（5）Report important network safety issues and incidents to relevant departments of the State in accordance with regulations.

第二十六条 运营者网络安全关键岗位专业技术人员实行执证上岗制度。

Article 26 An "employment with certificate" system will be adopted for specialized technical personnel in key network security positions of operators.

执证上岗具体规定由国务院人力资源社会保障部门会同国家网信部门等部门制定。

The specific provisions of the "employment with certificate" system will be formulated by departments such as the human resources and social security departments of the State Council acting jointly with the national cyberspace administration departments.

第二十七条 运营者应当组织从业人员网络安全教育培训，每人每年教育培训时长不得少于 1 个工作日，关键岗位专业技术人员每人每年教育培训时长不得少于 3 个工作日。

Article 27 Operators should organize network security education and training for their working personnel. The duration of the education and training must not be less than one

working day per person per year. The duration of the education and training for specialized technical personnel in key positions must not be less than three working days per person per year.

第二十八条 运营者应当建立健全关键信息基础设施安全检测评估制度，关键信息基础设施上线运行前或者发生重大变化时应当进行安全检测评估。

Article 28 Operators should establish and improve a system for security diagnostics and evaluation of critical information infrastructure. Before taking critical information infrastructure into operation, or when a major change has taken place, security diagnostics and evaluation should be carried out.

运营者应当自行或委托网络安全服务机构对关键信息基础设施的安全性和可能存在的风险隐患每年至少进行一次检测评估，对发现的问题及时进行整改，并将有关情况报国家行业主管或监管部门。

Operators should, acting on their own behalf or entrusting a network security services agency, conduct diagnostics and evaluation at least one time per year of the security and possible hidden risks of critical information infrastructure. They shall promptly carry out corrections of any problems which are discovered, and report relevant circumstances to the national industry regulatory or supervisory departments.

第二十九条 运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照个人信息和重要数据出境安全评估办法进行评估；法律、行政法规另有规定的，依照其规定。

Article 29 Personal information and important data which an operator collects or generates in the course of its operations within the territory of the People's Republic of China should be stored within that territory. When there is a veritable need to provide it overseas for reasons of business necessity, they should conduct an assessment in accordance with the *Measures for the Security Assessment of Personal Information and Important Data Leaving the Country*. Where law or administrative regulations provide otherwise, such provisions shall prevail.

第五章 产品和服务安全

Chapter 5 Security of Products and Services

第三十条 运营者采购、使用的网络关键设备、网络安全专用产品，应当符合法律、行政法规的规定和相关国家标准的强制性要求。

Article 30 Key network equipment and specialized network security products which an operator procures or uses should comply with the provisions of law and administrative regulations, and the mandatory requirements of relevant national standards.

第三十一条 运营者采购网络产品和服务，可能影响国家安全的，应当按照网络产品和服务安全审查办法的要求，通过网络安全审查，并与提供者签订安全保密协议。

Article 31 When an operator procures a network product or service which could have an influence on national security, it should pass a network security examination in accordance with the requirements of the *Measures for the Security Review of Network Products and Services*, and execute a security and confidentiality agreement with the provider.

第三十二条 运营者应当对外包开发的系统、软件，接受捐赠的网络产品，在其上线应用前进行安全检测。

Article 32 Operators should carry out security diagnostics before putting systems and software which were developed by subcontractors, or network products which were accepted as a donation, into operation.

第三十三条 运营者发现使用的网络产品、服务存在安全缺陷、漏洞等风险的，应当及时采取措施消除风险隐患，涉及重大风险的应当按规定向有关部门报告。

Article 33 When an operator discovers that there exist risks such as security deficiencies or vulnerabilities in the network products or services which it uses, it should promptly adopt measures to eliminate the risks or hidden dangers. Where major risks are involved, it should make a report to relevant departments in accordance with regulations.

第三十四条 关键信息基础设施的运行维护应当在境内实施。因业务需要，确需进行境外远程维护的，应事先报国家行业主管或监管部门和国务院公安部门。

Article 34 The operation and maintenance of critical information infrastructure should be carried out within the territory of China. When there is a veritable need to carry out remote overseas maintenance for reasons of business necessity, they should report it in

advance to the national industry regulatory or supervisory departments and to the public security department of the State Council.

第三十五条 面向关键信息基础设施开展安全检测评估，发布系统漏洞、计算机病毒、网络攻击等安全威胁信息，提供云计算、信息技术外包等服务的机构，应当符合有关要求。

Article 35 Organizations that provide security diagnostics and evaluation, publicize information on a security threat such as system vulnerabilities, computer viruses or network attacks and provide services such as cloud computing and information technology outsourcing aimed at critical information infrastructure should comply with relevant requirements.

具体要求由国家网信部门会同国务院有关部门制定。

The specific requirements will be formulated by the national cyberspace administration departments, acting jointly with relevant departments of the State Council.

第六章 监测预警、应急处置和检测评估

Chapter 6 Monitoring and Early Warning, Emergency Response and Handling and Diagnostics and Evaluation

第三十六条 国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度，组织指导有关机构开展网络安全信息汇总、分析研判和通报工作，按照规定统一发布网络安全监测预警信息。

Article 36 The national cyberspace administration departments will make the overall plans and establish a network security monitoring and warning system and an information publication system for critical information infrastructure, will instruct relevant agencies in the implementation of the gathering, analyzing, studying, assessing and publication of network security information, and will promulgate uniform information about network security monitoring and warning in accordance with regulations.

第三十七条 国家行业主管或监管部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警和信息通报制度，及时掌握本行业、本领域关键信息基础设施运行状况和安全风险，向有关运营者通报安全风险和相关工作信息。

Article 37 The national industry regulatory or supervisory departments should establish and improve a monitoring and warning and information publication system for the

network security of critical information infrastructure within their own industry sectors and their own fields, promptly grasp the operational status and security risks pertaining to critical information infrastructure within their own industry sectors and their own fields, and publicize information on security risks and related works to relevant operators.

国家行业主管或监管部门应当组织对安全监测信息进行研判，认为需要立即采取防范应对措施的，应当及时向有关运营者发布预警信息和应急防范措施建议，并按照国家网络安全事件应急预案的要求向有关部门报告。

The national industry regulatory or supervisory departments should conduct study and assessment of security monitoring information, and where they are of the view that there is a need to immediately adopt preventive response measures, they should promptly promulgate warning information and suggestions for response and preventive measures to relevant operators, and report to the relevant departments in accordance with the requirements of national network security incident contingency plans.

第三十八条 国家网信部门统筹协调有关部门、运营者以及有关研究机构、网络安全服务机构建立关键信息基础设施网络安全信息共享机制，促进网络安全信息共享。

Article 38 The national cyberspace administration departments will coordinate the relevant departments and operators as well as relevant research organizations and network security service organizations, to establish mechanisms for the sharing of information about critical information infrastructure network security, and promote the sharing of network security information.

第三十九条 国家网信部门按照国家网络安全事件应急预案的要求，统筹有关部门建立健全关键信息基础设施网络安全应急协作机制，加强网络安全应急力量建设，指导协调有关部门组织跨行业、跨地域网络安全应急演练。

Article 39 The national cyberspace administration departments will, in accordance with the requirements of national network security incident contingency plans, coordinate the relevant departments to establish and improve emergency coordination mechanisms for critical information infrastructure network security, strengthen the construction of network security emergency capabilities, and guide and coordinate relevant departments in organizing cross-sector and cross-regional network security emergency drills.

国家行业主管或监管部门应当组织制定本行业、本领域的网络安全事件应急预案，并定期组织演练，提升网络安全事件应对和灾难恢复能力。发生重大网络安全事件或接到网信部门的预警信息后，应立即启动应急预案组织应对，并及时报告有关情况。

The national industry regulatory or supervisory departments should formulate network security incident contingency planning for their own industry sectors and their own fields, and periodically organize drills, to raise network security incident response and disaster recovery capabilities. After the occurrence of a major network security incident or after receiving warning information from cyberspace administration departments, they should immediately start up the contingency plans to respond, and promptly report the relevant status.

第四十条 国家行业主管或监管部门应当定期组织对本行业、本领域关键信息基础设施的安全风险以及运营者履行安全保护义务的情况进行抽查检测，提出改进措施，指导、督促运营者及时整改检测评估中发现的问题。

Article 40 The national industry regulatory or supervisory departments should periodically conduct spot-checking and examination for security risks of critical information infrastructure as well as the status of operators' performance of their obligations to protect security within their own industry sectors and their own fields, propose corrective measures, and guide operators and urge them to promptly rectify and improve problems discovered during the examination and evaluation.

国家网信部门统筹协调有关部门开展的抽查检测工作，避免交叉重复检测评估。

The national cyberspace administration departments will coordinate the spot-checking and examination conducted by relevant departments, to avoid overlapping examinations and evaluations.

第四十一条 有关部门组织开展关键信息基础设施安全检测评估，应坚持客观公正、高效透明的原则，采取科学的检测评估方法，规范检测评估流程，控制检测评估风险。

Article 41 In launching the security diagnostics and evaluation of critical information infrastructure, relevant departments should uphold the principles of objectivity, impartiality, efficiency and transparency, and adopt a scientific methodology for the diagnostics and evaluation and a standardized diagnostics and evaluation flow path, and control risks in the diagnostics and evaluation.

运营者应当对有关部门依法实施的检测评估予以配合，对检测评估发现的问题及时进行整改。

Operators should cooperate with diagnostics and evaluations which are carried out lawfully by the relevant departments, and promptly carry out rectification and improvement of problems identified in the diagnostics and evaluations.

第四十二条 有关部门组织开展关键信息基础设施安全检测评估，可采取下列措施：

Article 42 When relevant departments launch diagnostics and evaluations of critical information infrastructure security, they may adopt the following measures:

（一）要求运营者相关人员就检测评估事项作出说明；

（1）Require relevant personnel of the operator to provide explanations of items in the diagnostics and evaluation;

（二）查阅、调取、复制与安全保护有关的文档、记录；

（2）Access and review, obtain, and copy documents and records which are relevant to the protection of security;

（三）查看网络安全管理制度制订、落实情况以及网络安全技术措施规划、建设、运行情况；

（3）Inspect the status of the formulation and implementation of the network security management system, and the status of the planning, construction and operation of the network security technological measures;

（四）利用检测工具或委托网络安全服务机构进行技术检测；

（4）Utilize diagnostic tools or engage a network security services agency to carry out technical diagnostics;

（五）经运营者同意的其他必要方式。

（5）Other necessary methods to which the operator has consented.

第四十三条 有关部门以及网络安全服务机构在关键信息基础设施安全检测评估中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

Article 43 Information which relevant departments and network security services agencies obtain during the diagnostics and evaluation of critical information infrastructure security can only be used for the maintenance of network security, and shall not be used for other purposes.

第四十四条 有关部门组织开展关键信息基础设施安全检测评估，不得向被检测评估单位收取费用，不得要求被检测评估单位购买指定品牌或者指定生产、销售单位的产品和服务。

Article 44 When relevant departments launch diagnostics and evaluations of critical information infrastructure security, they shall not collect a fee from the Entity (*danwei*) which is undergoing diagnostics and evaluation, shall not require the Entity (*danwei*) which is undergoing diagnostics and evaluation to purchase products or services of a designated brand name or produced or sold by a designated Entity (*danwei*).

第七章 法律责任

Chapter 7 Legal Liabilities

第四十五条 运营者不履行本条例第二十条第一款、第二十一条、第二十三条、第二十四条、第二十六条、第二十七条、第二十八条、第三十条、第三十二条、第三十三条、第三十四条规定的网络安全保护义务的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

Article 45 Where an operator does not perform the network security protection obligations as stipulated under Articles 20(1), 21, 23, 24, 26, 27, 28, 30, 32, 33 and 34 of this Regulation, the relevant competent departments acting in their official responsibilities will issue an order to effect corrections, and issue a warning; [if an operator] refuses to effect correction or jeopardization of network security occurs, it will be punished with a fine of more than RMB100,000 and less than RMB 1 million, and management personnel who bear direct responsibility will be punished with a fine of more than RMB10,000 and less than RMB100,000.

第四十六条 运营者违反本条例第二十九条规定，在境外存储网络数据，或者向境外提供网络数据的，由国家有关主管部门依据职责责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

Article 46 Where an operator violates the provisions of Article 29 of this Regulation, by storing network data outside the territory of China, or providing network data to a place outside the territory of China, the relevant competent departments of the State acting in their

official responsibilities will issue an order to effect corrections, issue a warning, confiscate illegal income, and impose a fine of more than RMB 50,000 and less than RMB 500,000. In addition, they may order temporary suspension of the related business, suspension of the business for internal rectification, shut down of the website, and revocation of the related business license; management personnel who bear direct responsibility and other directly responsible personnel will be punished with a fine of more than RMB10,000 and less than RMB100,000.

第四十七条 运营者违反本条例第三十一条规定，使用未经安全审查或安全审查未通过的网络产品或者服务的，由国家有关主管部门依据职责责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

Article 47 Where an operator violates the provisions of Article 31 of this Regulation, by using network products or services that have not undergone a security examination or have not passed a security examination, the relevant competent departments of the State acting in their official responsibilities will issue an order to cease usage, and impose a fine of more than one time and less than ten times the procurement amount; management personnel who bear direct responsibility and other directly responsible personnel will be punished with a fine of more than RMB10,000 and less than RMB100,000.

第四十八条 个人违反本条例第十六条规定，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款；构成犯罪的，依法追究刑事责任。

Article 48 Where an individual violates the provisions of Article 16 of this Regulation, and if such activities do not constitute a crime, the public security agencies will confiscate the illegal income, and impose detention of less than five days, and may impose a concurrent fine of more than RMB50,000 and less than RMB500,000; where the circumstances are relatively serious, they may impose detention of more than five days and less than fifteen days, and may impose a concurrent fine of more than RMB 10,000 and less than RMB 100,000; where a crime is constituted, criminal liability shall be prosecuted in accordance with law.

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

Where an Entity (*danwei*) has taken actions under the foregoing clause, the public security agencies will confiscate the illegal income, and impose a fine of more than RMB100,000 and less than RMB1,000,000, and management personnel who bear direct responsibility and other directly responsible personnel will be punished in accordance with the provisions of the preceding clause.

违反本条例第十六条规定，受到刑事处罚的人员，终身不得从事关键信息基础设施安全管理和网络运营关键岗位的工作。

Personnel who receive criminal punishment after having violated the provisions of Article 16 of this Regulation may not for the remainder of their lives engage in any work in key positions for the security management or network operation of critical information infrastructure.

第四十九条 国家机关关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接负责人员依法给予处分。

Article 49 Where an operator of critical information infrastructure of a State agency does not perform obligations to protection network security as provided under this Regulation, the agency at the higher level or relevant agencies will issue an order to effect corrections; management personnel who bear direct responsibility and other directly responsible personnel will be subject to disciplinary action in accordance with law.

第五十条 有关部门及其工作人员有下列行为之一的，对直接负责的主管人员和其他直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任：

Article 50 Where relevant departments and their working personnel have one of the actions listed below, management personnel who bear direct responsibility and other directly responsible personnel will be subject to disciplinary action in accordance with law; where a crime is constituted, criminal liability shall be prosecuted in accordance with law:

（一）在工作中利用职权索取、收受贿赂；

（1）Abusing their official authority to demand or receive a bribe in the course of their work;

（二）玩忽职守、滥用职权；

（2）Being in dereliction of duty, or misusing official authority;

（三）擅自泄露关键信息基础设施有关信息、资料及数据文件；

（3）Disclosing without authorization information, materials or data files relating to critical information infrastructure;

（四）其他违反法定职责的行为。

（4）Other actions that violate legal official responsibilities.

第五十一条 关键信息基础设施发生重大网络安全事件，经调查确定为责任事故的，除应当查明运营单位责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

Article 51 Where critical information infrastructure has undergone a major network security incident and an investigation has confirmed that it was an accident for which liability would attach, not only should the responsibility of the operating Entity (*danwei*) be brought to light and investigated in accordance with law, but also the responsibility of the relevant network security service agency and the relevant department should be brought to light, and where there has been a breach of duty, malfeasance or other unlawful actions, liability should be prosecuted in accordance with law.

第五十二条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门、国家安全机关和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

Article 52 Where agencies, organizations, or individuals outside the territory of China engage in activities that endanger the critical information infrastructure of the People’s Republic of China, such as attacks, intrusions, interference, and destruction, and this results in serious consequences, legal liability shall be pursued in accordance with law; the public security department of the State Council, national security agencies and relevant departments may determine to adopt measures to freeze the assets of such agency, organization or individual, or other necessary sanction measures.

第八章 附则

Chapter 8 Miscellaneous

第五十三条 存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

Article 53 The protection of the security of critical information infrastructure that stores and processes information that involves national secrets should also comply with the provisions of secrecy laws and administrative regulations.

关键信息基础设施中的密码使用和管理，还应当遵守密码法律、行政法规的规定。

The use and management of passwords within critical information infrastructure should also comply with the provisions of laws and administrative regulations on passwords.

第五十四条 军事关键信息基础设施的安全保护，由中央军事委员会另行规定。

Article 54 The Central Military Commission will separately formulate provisions for the protection of the security of military critical information infrastructure.

第五十五条 本条例自****年**月**日起施行。

Article 55 This Regulation will be put into effect from [***day, month and year***].