THE PRESIDENT	**THE SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness**
No. 06/2018/L-CTN	*Hanoi, June 25, 2018*

ORDER

On the promulgation of law[1]

Pursuant to Articles 88 and 91 of the Constitution of the Socialist Republic of Vietnam;

Pursuant to Article 80 of the Law on Promulgation of Legal Documents,

PROMULGATES:

The Law on Cyber Security,

which was passed on June 12, 2018, by the XIVth National Assembly of the Socialist Republic of Vietnam at its 5th session.

President of the Socialist Republic of Vietnam
TRAN DAI QUANG

[1] Công Báo Nos 775-776 (14/7/2018)

THE NATIONAL ASSEMBLY	THE SOCIALIST REPUBLIC OF VIETNAM Independence - Freedom - Happiness

No. 24/2018/QH14

LAW ON CYBER SECURITY[2]

Pursuant to the Constitution of the Socialist Republic of Vietnam;

The National Assembly promulgates the Law on Cyber Security.

Chapter I
GENERAL PROVISIONS

Article 1. Scope of regulation

This Law prescribes activities of protecting national security and ensuring social order and safety in cyberspace; and responsibilities of related agencies, organizations and individuals.

Article 2. Interpretation of terms

In this Law, the terms below are construed as follows:

1. *Cyber security* means the assurance that activities in cyberspace do not harm national security, social order and safety, and lawful rights and interests of agencies, organizations and individuals.

2. *Cyber security protection* means the prevention, detection, stopping and handling of acts of infringing upon cyber security.

3. *Cyberspace* means a network connecting information technology infrastructure facilities, including telecommunications networks, the Internet, computer networks, information systems, information processing and control systems and databases, where people socially interact without any space and time limitations.

4. *National cyberspace* means a cyberspace established, managed and controlled by the Government.

5. *National cyberspace infrastructure facilities* means a system of technical and physical facilities serving the creation, transmission and conveyance, collection, processing, storage, and exchange of information in the national cyberspace, including:

[2] Công Báo Nos 775-776 (14/7/2018)

a/ Transmission systems, including the national transmission system, internationally connected transmission systems, satellite systems, and transmission systems of enterprises providing services in telecommunications networks or the Internet or providing value-added services in cyberspace;

b/ Core service systems, including the national information channeling and routing system, the national domain name system (DNS), the national certification system (PKI/CA) and systems providing Internet connection and access services of enterprises providing services in telecommunications networks or the Internet or providing value-added services in cyberspace;

c/ Information technology services and applications, including online services, online-connected information technology applications serving management and administration work of important agencies, organizations and economic and financial groups, and national databases.

Online services include e-government, e-commerce, websites, online forums, social networks, and blogs;

d/ Information technology infrastructure facilities of smart cities, the Internet of things, mixed reality systems, cloud computing, big data systems, fast data systems, and artificial intelligence systems.

6. *International gateway* means the place where network signals are transmitted and received between Vietnam and other countries and territories.

7. *Cybercrime* means acts of using cyberspace, information technology or electronic devices to commit crimes prescribed in the Penal Code.

8. *Cyber-attack* means acts of using cyberspace, information technology or electronic devices to jeopardize or interrupt the operation of a telecommunications network, the Internet, a computer network, an information system, an information processing and control system, a database or an electronic device.

9. *Cyber terrorism* means the use of cyberspace, information technology or electronic devices to commit terrorism or terrorism financing.

10. *Cyber espionage* means the act of deliberately bypassing warnings, login codes, passwords, or firewalls, using others' administration right, or employing other methods to illegally acquire and collect information or information resources in telecommunications networks, the Internet, computer networks, information systems,

information processing and control systems, databases or electronic devices of agencies, organizations and individuals.

11. *Digital account* means information used to certify, authenticate and grant the right to use applications and services in cyberspace.

12. *Cyber security threat* means the appearance in cyberspace of signs of threat of infringing upon national security or causing serious harms to social order and safety or lawful rights and interests of agencies, organizations and individuals.

13. *Cyber security incident* means an unexpected event occurring in cyberspace which infringes upon national security, social order and safety or lawful rights and interests of agencies, organizations and individuals.

14. *Dangerous cyber security circumstance* means an event occurring in cyberspace which involves acts of seriously infringing upon national security or causing extremely serious harms to social order and safety or lawful rights and interests of agencies, organizations and individuals.

Article 3. The State's policies on cyber security

1. To prioritize the protection of cyber security in national defense, security, socio-economic development, science, technology, and foreign affairs.

2. To build a sound cyberspace without prejudicing national security, social order and safety, and lawful rights and interests of agencies, organizations and individuals.

3. To prioritize resources for building professional cyber security protection forces; to raise capacity of these forces and organizations and individuals engaged in cyber security protection; to prioritize investment in research into and development of science and technology for cyber security protection.

4. To encourage and create conditions for organizations and individuals to participate in cyber security protection and response to cyber security threats; research and develop cyber security protection technologies, products, services and applications; and cooperate with functional agencies in cyber security protection.

5. To increase international cooperation in cyber security.

Article 4. Principles of cyber security protection

1. To abide by the Constitution and laws; to ensure interests of the State and lawful rights and interests of agencies, organizations and individuals.

2. To be placed under the leadership of the Communist Party of Vietnam and the unified management of the State; to mobilize the combined strength of the political system and entire nation; and to bring into play the key role of professional cyber security protection forces.

3. To closely combine cyber security protection and protection of information systems of national security importance with socio-economic development, guarantee of human rights and citizens' rights, and facilitation of operations of agencies, organizations and individuals in cyberspace.

4. To proactively prevent, detect, stop, fight and spoil any activities of using cyberspace to infringe upon national security, social order and safety, or lawful rights and interests of agencies, organizations and individuals; to stay ready to avert cyber security threats.

5. To carry out cyber security protection activities for national cyberspace infrastructure facilities; to apply measures to protect information systems of national security importance.

6. To appraise and certify the satisfaction of cyber security conditions of information systems of national security importance before putting them into operation and use; to regularly conduct cyber security inspection and supervision throughout the operation process, and to promptly respond to and remedy cyber security incidents.

7. To promptly and severely handle all violations of the law on cyber security.

Article 5. Cyber security protection measures

1. Cyber security protection measures include:

a/ Conducting cyber security appraisal;

b/ Assessing cyber security conditions;

c/ Conducting cyber security inspection;

d/ Conducting cyber security supervision;

dd/ Responding to and remedying cyber security incidents;

e/ Taking actions to protect cyber security;

g/ Using cryptography to protect cyber information;

h/ Blocking, or requesting the suspension or termination of, provision of online information; terminating or suspending the establishment, supply and use of telecommunications networks or the Internet, production and use of radio transmitters and receivers in accordance with law;

i/ Requesting the removal of, or logging in to remove, unlawful or false information in cyberspace which infringes upon national security, social order and safety, or lawful rights and interests of agencies, organizations and individuals;

k/ Collecting electronic data relating to activities in cyberspace which infringe upon national security, social order and safety, or lawful rights and interests of agencies, organizations and individuals;

l/ Blocking or restricting operation of information systems; terminating, suspending or requesting the cessation of operation of information systems or revocation of domain names in accordance with law;

m/ Initiating criminal cases, carrying out, investigation, prosecution and trial activities in accordance with the Criminal Procedure Code;

n/ Other measures prescribed by the law on national security and law on handling of administrative violations.

2. The Government shall prescribe the order and procedures for taking cyber security protection measures, except those referred to at Points m and n, Clause 1 of this Article.

Article 6. Protection of the national cyberspace

The State shall apply measures for protecting the national cyberspace, preventing and handling acts in cyberspace which infringe upon national security, social order and safety, or lawful rights and interests of agencies, organizations and individuals.

Article 7. International cooperation in cyber security

1. International cooperation in cyber security shall be implemented on the basis of respect for independence, sovereignty, and territorial integrity, non-intervention into internal affairs, equality, and mutual benefits.

2. International cooperation in cyber security covers:

a/ Research and analysis of cyber security trends;

b/ Creation of mechanisms and policies to boost cooperation between Vietnamese organizations and individuals and foreign organizations and individuals as well as international organizations engaged in cyber security;

c/ Sharing of information and experiences; assistance in training, equipment and technology in cyber security protection;

d/ Prevention of and fighting against cybercrime and infringements upon cyber security; averting cyber security threats;

dd/ Provision of counseling on, training and developing human resources for cyber security;

e/ Organization of international conferences, seminars and forums on cyber security;

g/ Entry into, and implementation of, treaties and international agreements on cyber security;

h/ Implementation of, international cooperation programs and projects on cyber security.

i/ Other activities of international cooperation in cyber security.

3. The Ministry of Public Security shall take responsibility before the Government for assuming the prime responsibility for and coordinating international cooperation in cyber security, except activities of the Ministry of National Defense.

The Ministry of National Defense shall take responsibility before the Government for international cooperation in cyber security under its management.

The Ministry of Foreign Affairs shall coordinate with the Ministry of Public Security and Ministry of National Defense in implementing international cooperation in cyber security.

International cooperation in cyber security involving the responsibilities of more than one ministry or sector shall be decided by the Government.

4. Except for international cooperation activities of the Ministry of National Defense, other ministries, sectors and localities shall obtain written opinions of the Ministry of Public Security before carrying out activities of international cooperation in cyber security.

Article 8. Prohibited acts in cyber security

1. Using cyberspace to commit the following acts:

a/ The acts prescribed in Clause 1, Article 18 of this Law;

b/ Organizing or carrying out activities, colluding with, instigating, buying off, deceiving, enticing or training people to carry out activities against the State of the Socialist Republic of Vietnam;

c/ Distorting history, denying revolutionary achievements, sabotaging the national great solidarity bloc, offending religions or committing gender or racial discrimination;

d/ Providing false information causing public anxiety, harming socio-economic activities or causing difficulties to operation of state

agencies or persons on official duty, or infringing upon lawful rights and interests of other agencies, organizations and individuals;

dd/ Prostitution or other social evils, trafficking in humans; posting obscene, debauched or cruel information; undermining fine traditions and customs of the nation, social ethics and community well-being;

e/ Instigating, inducing or provoking other people to commit crime.

2. Committing cyber-attacks, cyber terrorism, cyber espionage or cybercrime; causing incidents to, attacking, breaking into, taking control of, disrupting, paralyzing or sabotaging information systems of national security importance.

3. Manufacturing, producing or using instruments, equipment or software or obstructing or disrupting the operation of telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, or electronic devices; spreading malware harmful to the operation of telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, or electronic devices; unauthorizedly breaking (hacking) into telecommunications networks, computer networks, information systems, information processing and control systems, databases, or electronic devices of others.

4. Opposing or obstructing operations of cyber security protection forces; illegally attacking and counteracting cyber security protection measures.

5. Taking advantage of or abusing cyber security protection activities to infringe upon national sovereignty, interests or security, social order and safety, or lawful rights and interests of agencies, organizations or individuals or for gaining illicit profits.

6. Other acts violating this Law.

Article 9. Handling of violations of the law on cyber security

Any violators of this Law shall, depending on the nature and severity of their violations, be disciplined, administratively handled or examined for penal liability; if causing damage, they shall pay compensation in accordance with law.

Chapter II

PROTECTION OF CYBER SECURITY OF INFORMATION SYSTEMS OF NATIONAL SECURITY IMPORTANCE

Article 10. Information systems of national security importance

1. An information system of national security importance is an information system which, if encountering incidents, being hacked, taken control of, disrupted, interrupted, paralyzed or sabotaged, will cause serious harm to cyber security.

2. Information systems of national security importance include:

a/ Information systems of the military, public security, diplomacy and cipher sectors;

b/ Information systems storing and processing information classified as state secrets;

c/ Information systems serving the retention and preservation of objects or documents of particularly important value;

d/ Information systems serving the preservation of materials and substances which are extremely dangerous to humans and the eco-environment;

dd/ Information systems serving the preservation, manufacture and management of other particularly important physical foundations related to national security;

e/ Important information systems serving the operation of central agencies and organizations;

g/ National information systems in the energy, finance, banking, telecommunications, transport, natural resources and environment, chemicals, health, culture and mass media sectors;

h/ Automatic control and surveillance systems in important works related to national security or targets of national security importance.

3. The Prime Minister shall promulgate and revise the list of information systems of national security importance.

4. The Government shall prescribe the coordination among the Ministry of Public Security, Ministry of National Defense, Ministry of Information and Communications, Government Cipher Committee and other ministries and related sectors in appraising, assessing, inspecting, supervising, and responding to and remedying incidents to, information systems of national security importance.

Article 11. Cyber security appraisal of information systems of national security importance

1. Cyber security appraisal means the consideration and evaluation of cyber security issues so as to provide grounds for making decision on building or upgrading an information system.

2. Subject to cyber security appraisal of an information system of national security importance are:

a/ Pre-feasibility study report and construction design dossier of the investment project to build the information system before they are approved;

b/ Scheme on upgrading the information system before it is approved.

3. Cyber security appraisal of an information system of national security importance covers:

a/ Compliance of the system's design with cyber security regulations and conditions;

b/ Conformity with plans on cyber security protection, incident response and remediation and cyber security protection personnel.

4. The competence to appraise cyber security of information systems of national security importance is as follows:

a/ The Ministry of Public Security's professional cyber security protection force shall appraise cyber security of information systems of national security importance, except those referred to at Points b and c of this Clause;

b/ The Ministry of National Defense's professional cyber security protection force shall appraise cyber security of military information systems;

c/ The Government Cipher Committee shall appraise cyber security of its cryptographic information systems.

Article 12. Assessment of cyber security conditions of information systems of national security importance

1. Assessment of cyber security conditions means the consideration of the satisfaction of cyber security requirements by information systems before they are put into operation and use.

2. An information system of national security importance must meet conditions regarding:

a/ Cyber security regulations, processes and plans; and system operation and administration staffs;

b/ Cyber security of equipment, devices, hardware and software which are parts of the information system;

c/ Technical measures to supervise and protect cyber security; measures to protect automatic control and supervision systems; the

Internet of things, mixed reality system, cloud computing, big data system, fast data system, and artificial intelligence system;

d/ Measures to ensure physical security, including special isolation, data leak prevention, information collection prevention, and entry and exit control.

3. The competence to assess cyber security conditions of information systems of national security importance is prescribed as follows:

a/ The Ministry of Public Security's professional cyber security protection force shall assess and certify the satisfaction of cyber security conditions for information systems of national security importance, except those referred to at Points b and c of this Clause;

b/ The Ministry of National Defense's professional cyber security protection force shall assess and certify the satisfaction of cyber security conditions for military information systems;

c/ The Government Cipher Committee shall assess and certify the satisfaction of cyber security conditions by its cryptographic information systems.

4. Information systems of national security importance may be put into operation and use only after they are certified as meeting cyber security conditions.

5. The Government shall detail Clause 2 of this Article.

Article 13. Cyber security inspection of information systems of national security importance

1. Cyber security inspection means activities of determining the actual cyber security state of information systems, information system infrastructure facilities or information stored, processed and transmitted in information systems in order to prevent, detect and handle cyber security threats and put forward plans and measures to ensure their normal operation.

2. Cyber security inspection of an information system of national security importance shall be carried out in the following cases:

a/ Electronic devices and cyber information security services are introduced in the information system;

b/ There is a change in the current state of the information system;

c/ On an annual basis;

d/ On an unscheduled basis upon occurrence of cyber security incidents, acts infringing upon cyber security; requirement for state

management of cyber security; expiration of the time limit for remedying security weaknesses and vulnerabilities as recommended by professional cyber security protection forces.

3. Subject to cyber security inspection of an information system of national security importance are:

a/ Hardware, software and digital devices used in the information system;

b/ Cyber security protection regulations and measures;

c/ Information stored, processed and transmitted in the information system;

d/ Cyber security incident response and remediation plan of the information system manager;

dd/ Measures to protect state secrets and prevent disclosure and loss of state secrets via technical channels;

e/ Cyber security protection staffs.

4. Managers of information systems of national security importance shall inspect cyber security of their information systems in the cases prescribed at Points a, b and c, Clause 2 of this Article; notify the inspection result in writing before October every year to the Ministry of Public Security's professional cyber security protection force or to the Ministry of National Defense's professional cyber security protection force, for military information systems.

5. An unscheduled cyber security inspection of an information system of national security importance is prescribed as follows:

a/ Before conducting the inspection, the professional cyber security protection force shall notify in writing the inspection to the information system manager at least 12 hours in advance in case of occurrence of a cyber security incident or an act of infringing upon cyber security; at least 72 hours in advance in case of requirement for state management of cyber security or expiration of the time limit for remedying security weaknesses and vulnerabilities as recommended by a professional cyber security protection force;

b/ Within 30 days after the end of the inspection, the professional cyber security inspection force shall notify the inspection result and its requests to the information system manager, in case of detecting security weaknesses and vulnerabilities; guide or participate in the remediation of incidents if so requested by the information system manager;

c/ The Ministry of Public Security's professional cyber security protection force shall carry out unscheduled cyber security inspections of

information systems of national security importance, except military information systems managed by the Ministry of National Defense, cryptographic information systems of the Government Cipher Committee, and cryptographic products provided by the Government Cipher Committee serving the protection of information classified as state secrets.

The Ministry of National Defense's professional cyber security protection force shall carry out unscheduled cyber security inspections of military information systems.

The Government Cipher Committee shall carry out unscheduled cyber security inspections of its cryptographic information systems and cryptographic products provided by the Government Cipher Committee serving the protection of information classified as state secrets.

d/ Managers of information systems of national security importance shall collaborate with cyber security protection forces performing unscheduled cyber security inspections.

6. Cyber security inspection results shall be kept confidential in accordance with law.

Article 14. Cyber security supervision of information systems of national security importance

1. Cyber security supervision means the collection and analysis of information in order to identify, warn of, remedy and handle cyber security threats and incidents, security weaknesses and vulnerabilities, malware and malicious hardware.

2. Managers of information systems of national security importance shall assume the prime responsibility for, and coordinate with a competent professional cyber security protection force in, regularly supervising cyber security of information systems under their management; create mechanisms for self-warning and receiving warnings about cyber security threats and incidents, security weaknesses and vulnerabilities, malware and malicious hardware, and work out emergency response and remediation plans.

3. Professional cyber security protection forces shall supervise cyber security of information systems of national security importance under their respective management; warn of and coordinate with information system managers in remedying and handling cyber security threats and incidents, security weaknesses and vulnerabilities, malware and malicious hardware in information systems of national security importance.

Article 15. Response to and remediation of cyber security incidents for information systems of national security importance

1. Response to and remediation of cyber security incidents for information systems of national security importance include:

a/ Detecting and identifying cyber security incidents;

b/ Protecting scenes and collecting evidence;

c/ Blocking or limiting the scope of, and minimizing damage caused by, cyber security incidents;

d/ Identifying targets in need and scope of response;

dd/ Verifying, analyzing, assessing and classifying cyber security incidents;

e/ Implementing cyber security incident response and remediation plans;

g/ Identifying causes and sources of incidents;

h/ Investigating and handling in accordance with law.

2. Managers of information systems of national security importance shall prepare cyber security incident response and remediation plans for these information systems; implement the plans when cyber security incidents occur and promptly report them to a competent professional cyber security protection force.

3. The coordination of the response to and remediation of cyber security incidents for information systems of national security importance is prescribed as follows:

a/ The Ministry of Public Security's professional cyber security protection force shall assume the prime responsibility for coordinating the response to and remediation of cyber security incidents occurring in information systems of national security importance, except those prescribed at Points b and c of this Clause; participate in the response to and remediation of cyber security incidents occurring in information systems of national security importance when so requested; and notify information system managers when detecting cyber-attacks or cyber security incidents;

b/ The Ministry of National Defense's professional cyber security protection force shall assume the prime responsibility for coordinating the response to and remediation of cyber security incidents occurring in military information systems;

c/ The Government Cipher Committee shall assume the prime responsibility for coordinating the response to and remediation of cyber security incidents occurring in its cryptographic information systems.

4. Agencies, organizations and individuals shall participate in the response to and remediation of cyber security incidents occurring in information systems of national security importance when so requested by the forces in charge of coordinating these activities.

Chapter II

PREVENTION AND HANDLING OF ACTS OF INFRINGING UPON CYBER SECURITY

Article 16. Prevention and handling of information in cyberspace with propaganda contents opposing the State of the Socialist Republic of Vietnam; instigating riots or disrupting security or public order; humiliating or slandering; or infringing upon economic management order

1. Information in cyberspace with propaganda contents against the State of the Socialist Republic of Vietnam includes:

a/ Information distorting and defaming the people's administration;

b/ Psychological warfare, information provoking wars of aggression, sowing division and hatred among people of different ethnic groups or religions or people of different nations;

c/ Information offending the nation, desecrating the national flag, emblem or anthem, great personalities, leaders, famous people and national heroes.

2. Information in cyberspace instigating riots or disruption of security or disturbance of public order includes:

a/ Information calling for, mobilizing, instigating, threatening, sowing division, carrying out armed activities or using violence to oppose the people's administration;

b/ Information calling for, mobilizing, instigating, threatening, enticing people to gather in masses to cause public disturbances, offend persons on official duty or obstruct activities of agencies and organizations, thus causing insecurity and disorder.

3. Information in cyberspace with disgracing or slandering contents includes:

a/ Information seriously offending the honor, prestige or dignity of others;

b/ Fabricated or false information harming the honor, prestige or dignity of other people or harming lawful rights and interests of other agencies, organizations or individuals.

4. Information in cyberspace infringing upon economic management order includes:

a/ Fabricated or false information on products, goods, banknotes, bonds, treasury bills, government bonds, checks and other valuable papers;

b/ Fabricated or false information concerning finance, banking, e-commerce, e-payment, monetary trading, capital raising, multi-level marketing, and securities.

5. Fabricated or false information in cyberspace causing public anxiety, damaging socio-economic activities, causing difficulties to activities of state agencies or persons on official duty, or infringing upon lawful rights and interests of other agencies, organizations or individuals.

6. Information system managers shall apply managerial and technical measures to prevent, detect, stop and remove the information prescribed in Clauses 1, 2, 3, 4 and 5 of this Clause in their information systems when so requested by professional cyber security protection forces.

7. Professional cyber security protection forces and competent agencies shall apply the measures prescribed at Points h, i, and l, Article 5 of this Law to handle the information in cyberspace prescribed in Clause 1, 2, 3, 4 or 5 of this Article.

8. Enterprises providing services on telecommunications networks or the Internet or providing value-added services in cyberspace and information system managers shall coordinate with functional agencies in handling the information in cyberspace prescribed in Clauses 1, 2, 3, 4 and 5 of this Article.

9. Organizations and individuals that create, publish and spread in cyberspace the information prescribed in Clause 1, 2, 3, 4 or 5 of this Article shall remove such information when so requested by cyber security protection forces and take responsibility in accordance with law.

Article 17. Prevention and combat of cyber espionage; protection of information classified as state secrets, work secrets, business secrets, personal secrets, family secrets and privacy in cyberspace

1. Cyber espionage and infringement upon state secrets, work secrets, business secrets, personal secrets, family secrets and privacy in cyberspace include:

a/ Acquiring, trading in, collecting and deliberately disclosing information classified as state secrets, work secrets, business secrets, personal secrets, family secrets or privacy, thus affecting the honor, prestige, dignity, or lawful interests of agencies, organizations or individuals;

b/ Deliberately deleting, damaging, mislaying or altering information classified as state secrets, working secrets, business secrets, personal secrets, family secrets or privacy, which is transmitted or stored in cyberspace;

c/ Deliberately modifying, annulling or neutralizing technical measures developed and applied to protect information classified as state secrets, work secrets, business secrets, personal secrets, family secrets or privacy;

d/ Illegally posting in cyberspace information classified as state secrets, work secrets, business secrets, personal secrets, family secrets or privacy;

dd/ Deliberately eavesdropping or illegally audio or video recording conversations;

e/ Other acts of deliberately infringing upon state secrets, work secrets, business secrets, personal secrets, family secrets or privacy.

2. Information system managers shall:

a/ Conduct cyber security inspection in order to detect and remove malicious codes and hardware, remedy security weaknesses and vulnerabilities; detect, prevent and cope with illegal intrusions or other cyber security threats;

b/ Apply managerial and technical measures to prevent, detect and stop acts of cyber espionage and infringement upon state secrets, work secrets, business secrets, personal secrets, family secrets or privacy in information systems and timely remove information relating to these acts;

c/ Cooperate with and comply with requests of professional cyber security protection forces regarding prevention and combat of cyber espionage and protection of information being state secrets, working secrets, business secrets, personal secrets or family secrets or relating to private life in cyberspace.

3. Agencies creating and storing information and documents classified as state secrets shall protect state secrets created and stored in computers and other devices or shared in cyberspace in accordance with the law on protection of of state secrets.

4. The Ministry of Public Security has the following responsibilities, except those prescribed in Clauses 5 and 6 of this Article:

a/ To conduct cyber security inspection of information systems of national security importance in order to detect and remove malicious codes and hardware, remedy security weaknesses and vulnerabilities; to detect, prevent and handle illegal intrusions;

b/ To conduct cyber security inspection of information and communication equipment, products and services, and digital and electronic equipment before they are used in information systems of national security importance;

c/ To conduct cyber security supervision of information systems of national security importance in order to detect and handle the illegal collection of information classified as state secrets;

d/ To detect and handle acts of illegally posting, storing and exchanging information and documents classified as state secrets in cyberspace;

dd/ To participate in the research into and production of products serving the storage and transmission of information and contents classified as state secrets, and cryptographic products in cyberspace according to its assigned functions and tasks;

e/ To inspect and examine the protection of state secrets in cyberspace by state agencies and protection of cyber security by managers of information systems of national security importance;

g/ To organize training courses to raise cyber security protection forces' awareness and knowledge about protection of state secrets in cyberspace, prevention and combat of cyber-attacks, and protection of cyber security under Clause 2, Article 30 of this Law.

5. The Ministry of National Defense shall implement the provisions of Points a, b, c, d, dd and e, Clause 4 of this Article regarding military information systems.

6. The Government Cipher Committee shall organize the implementation of the law on encryption to protect information classified as state secrets stored and exchanged in cyberspace.

Article 18. Prevention and combat of acts of using cyberspace, information technology or electronic devices in violation of the law on national security and social order and safety

1. Acts of using cyberspace, information technology or electronic devices in violation of the law on national security or social order and safety include:

a/ Posting or spreading in cyberspace the information prescribed in Clauses 1, 2, 3, 4, and 5, Article 16, or committing the acts prescribed in Clause 1, Article 17, of this Law;

b/ Appropriating property; organizing gambling or gambling via the Internet; committing theft of Internet-based international telecommunications services; infringing upon copyright and intellectual property rights in cyberspace;

c/ Creating fake websites; forging, distributing, stealing, trading in, collecting or exchanging illegally information on others' credit cards and bank accounts; illegally issuing, supplying and using payment instruments;

d/ Promoting, advertising and trading in goods and services banned by law;

dd/ Guiding how to commit illegal acts;

e/ Other acts of using cyberspace, information technology or electronic devices in violation of the law on national security or social order and safety.

2. Professional cyber security protection forces shall take responsibility for preventing and combating acts of using cyberspace, information technology or electronic devices in violation of the law on national security or social order and safety.

Article 19. Prevention and combat of cyber-attacks

1. Cyber-attacks and acts related to cyber-attacks include:

a/ Spreading computer programs harmful to telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases or electronic devices;

b/ Obstructing, disrupting, paralyzing, interrupting or delaying the operation of, or illegally blocking the transmission of data by, telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, or electronic devices;

c/ Accessing, damaging or obtaining data stored or transmitted via telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases or electronic devices;

d/ Accessing, creating or exploiting security weaknesses or vulnerabilities and system services to obtain information and gain illicit profits;

dd/ Producing, trading in, exchanging or donating instruments, equipment or software having a feature of attacking telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases or electronic devices for illegal purposes;

e/ Other acts affecting normal operation of telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases or electronic devices.

2. Information system managers shall apply technical measures to prevent and stop the acts prescribed at Points a, b, c, d and e, Clause 1 of this Article against their information systems.

3. Upon occurrence of cyber-attacks infringing or threatening to infringe upon national sovereignty, interests or security or seriously jeopardizing social order or safety, professional cyber security protection forces shall assume the prime responsibility for, and coordinate with information system managers and related organizations and individuals in, applying measures to identify the origins of these cyber-attacks and collect evidence; request enterprises providing services on telecommunications networks or the Internet and enterprises providing value-added services in cyberspace to block and filter information so as to prevent and eliminate cyber-attacks and sufficiently and promptly provide relevant information and documents.

4. The responsibility for preventing and combating cyber-attacks is prescribed as follows:

a/ The Ministry of Public Security shall assume the prime responsibility for, and coordinate with related ministries and sectors in preventing, detecting and handling the acts prescribed in Clause 1 of this Article which infringe or threaten to infringe upon national sovereignty, interests or security or seriously jeopardizing social order or safety nationwide, except the cases prescribed at Points b and c of this Clause;

b/ The Ministry of National Defense shall assume the prime responsibility for, and coordinate with related ministries and sectors in, preventing, detecting and handling the acts prescribed in Clause 1 of this Article for military information systems;

c/ The Government Cipher Committee shall assume the prime responsibility for, and coordinate with related ministries and sectors in,

preventing, detecting and handling the acts prescribed in Clause 1 of this Article for its cryptographic information systems.

Article 20. Prevention and combat of cyber terrorism

1. Competent state agencies shall apply measures prescribed by this Law, Article 29 of the Law on Cyberinformation Security and the anti-terrorism law to combat cyber-terrorism.

2. Information system managers shall regularly review and inspect their information systems so as to eliminate the danger of cyber terrorism.

3. Any signs or acts of cyber terrorism shall be promptly reported to cyber security protection forces. Agencies which receive information and reports on cyber terrorism shall promptly notify them to professional cyber security protection forces.

4. The Ministry of Public Security shall assume the prime responsibility for, and coordinate with related ministries and sectors in, preventing and combating cyber terrorism, applying measures to neutralize sources of cyber terrorism, and deal with cyber terrorism and minimize consequences to information systems, except the cases prescribed in Clauses 5 and 6 of this Article.

5. The Ministry of National Defense shall assume the prime responsibility for, and coordinate with related ministries and sectors in, preventing and combating cyber terrorism and applying measures to deal with cyber terrorism occurring in military information systems.

6. The Government Cipher Committee shall assume the prime responsibility for, and coordinate with related ministries and sectors in, preventing and combating cyber terrorism and applying measures to deal with cyber terrorism occurring in its cryptographic information systems.

Article 21. Prevention and handling of dangerous cyber security circumstances

1. Dangerous cyber security circumstances include:

a/ Provocative information in cyberspace, posing risks of riot, security disruption or terrorism;

b/ Attacks against information systems of national security importance;

c/ Large-scale and intense attacks against multiple information systems;

d/ Cyber-attacks aiming at destroying a work or target of national security importance;

dd/ Cyber-attacks seriously infringing upon national sovereignty, interests or security; seriously disturbing social order or safety or infringing upon lawful rights and interests of agencies, organizations and individuals.

2. The responsibility for preventing dangerous cyber security circumstances is prescribed as follows:

a/ Professional cyber security protection forces shall work with managers of information systems of national security importance in implementing technical and professional solutions to prevent, detect and handle dangerous cyber security circumstances;

b/ Telecommunications, Internet and information technology enterprises, enterprises providing services on telecommunications networks or the Internet, enterprises providing value-added services in cyberspace, and related agencies, organizations and individuals shall coordinate with the Ministry of Public Security's professional cyber security protection force in preventing, detecting and handling dangerous cyber security circumstances.

3. Measures for handling dangerous cyber security circumstances include:

a/ Immediately implementing plans on prevention of and urgent response to cyber security incidents, preventing, eliminating or minimizing damage caused by dangerous cyber security circumstances;

b/ Notifying the circumstances to related agencies, organizations and individuals;

c/ Collecting relevant information; constantly monitoring and supervising dangerous cyber security circumstances;

d/ Analyzing and assessing information, forecasting the probability, scope of influence and extent of damage caused by dangerous cyber security circumstances;

dd/ Suspending the provision of cyber information in specific areas or disconnecting the international gateway;

e/ Arranging forces and means to prevent and eliminate dangerous cyber security circumstances;

g/ Other measures as prescribed in the Law on National Security.

4. The handling of dangerous cyber security circumstances is prescribed as follows:

a/ When detecting a dangerous cyber security circumstance, agencies, organizations and individuals shall promptly notify it to

professional cyber security protection forces and apply the measures prescribed at Points a and b, Clause 3 of this Article;

b/ The Prime Minister shall consider and decide or authorize the Minister of Public Security to consider, decide and handle dangerous cyber security circumstances nationwide or in each locality or for a specific target.

The Prime Minister shall consider and decide or authorize the Minister of National Defense to consider, decide and handle dangerous cyber security circumstances for military information systems and cryptographic information systems of the Government Cipher Committee;

c/ Professional cyber security protection forces shall assume the prime responsibility for, and coordinate with related agencies, organizations and individuals in, applying the measures prescribed in Clause 3 of this Article to handle dangerous cyber security circumstances;

d/ Related agencies, organizations and individuals shall coordinate with professional cyber security protection forces in applying measures for preventing and handling dangerous cyber security circumstances.

Article 22. Fighting to protect cyber security

1. Fighting to protect cyber security means organized activities carried out in cyberspace by professional cyber security protection forces in order to protect national security and ensure social order and safety.

2. Fighting to protect cyber security covers:

a/ Grasping information relating to national security protection;

b/ Preventing and combating attacks against, and protecting information systems of national security importance to ensure their stable operation;

c/ Paralyzing or restricting activities of using cyberspace to infringe upon national security or cause extremely serious harms to social order and safety;

d/ Taking the initiative in attacking and neutralizing targets in cyberspace in order to protect national security and ensure social order and safety.

3. The Ministry of Public Security shall assume the prime responsibility for, and coordinate with related ministries and sectors in, fighting to protect cyber security.

Chapter IV

CYBER SECUYRITY PROTECTION ACTIVITIES

Article 23. Implementation of cyber security protection activities by state agencies and political organizations at central and local levels

1. Cyber security protection activities include:

a/ Formulating and improving regulations on use of local computer networks and Internet-connected computer networks; plans on assurance of cyber security for information systems; and plans on response to and remediation of cyber security incidents;

b/ Applying and implementing plans, measures and technologies to protect cyber security for information systems under their management and information and documents stored, created and transmitted thereon;

c/ Organizing training in knowledge on cyber security for cadres, civil servants, public employees and workers; building cyber security protection capacity for cyber security protection forces;

d/ Protecting cyber security in the provision of public services in cyberspace; providing information to, exchanging information with and collecting information from agencies, organizations and individuals; sharing information within their agencies and with other agencies, or in other activities according to the Government's regulations;

dd/ Investing in and building appropriate physical infrastructure facilities to ensure implementation of cyber security protection activities for information systems;

e/ Conducting cyber security inspection of information systems; preventing and combating violations of the law on cyber security; responding to and remedying cyber security incidents.

2. Heads of agencies and units shall organize cyber security protection activities under their management.

Article 24. Cyber security inspection of agencies' and organizations' information systems outside the list of information systems of national security importance

1. Cyber security inspection of agencies' and organizations' information systems outside the list of information systems of national security importance shall be conducted in the following cases:

a/ There is an act of violating the law on cyber security, infringing upon national security or seriously jeopardizing social order and safety;

b/ There is a request of an information system manager.

2. Subject to cyber security inspection are:

a/ Hardware systems, software, and digital equipment used in information systems;

b/ Information stored, processed and transmitted in information systems;

c/ Measures for protecting state secrets and preventing and controlling disclosure and loss of state secrets via technical channels.

3. When detecting acts of violating the law on cyber security in their information systems, information system managers shall notify them the Ministry of Public Security's professional cyber security protection force.

4. The Ministry of Public Security's professional cyber security protection force shall conduct cyber security inspection of information systems of agencies and organizations in the cases prescribed in Clause 1 of this Article.

5. Professional cyber security protection forces shall notify information system managers in writing at least 12 hours before conducting cyber security inspection.

Within 30 days after finishing the inspection, professional cyber security protection forces shall notify inspection results and their requests to information system managers if detecting security weaknesses or vulnerabilities; guide or participate in the remediation of incidents if so requested by information system managers.

6. Cyber security inspection results shall be kept confidential in accordance with law.

7. The Government shall prescribe the order and procedures for cyber security inspection under this Article.

Article 25. Protection of cyber security for national network infrastructure facilities and international gateways

1. Protection of cyber security for national network infrastructure facilities and international gateways must ensure close combination between security protection and socio-economic development requirements; the location of international gateways in Vietnam's territory shall be encouraged; and organizations and individuals shall be encouraged to invest in and build national network infrastructure facilities.

2. Managers and users of national network infrastructure facilities and international gateways shall:

a/ Protect cyber security within their management; submit to the management, inspection and examination by competent state agencies and comply with their cyber security protection requests;

b/ Create conditions and apply necessary technical and professional measures for competent state agencies to protect cyber security when so requested by the latter.

Article 26. Assurance of information security in cyberspace

1. Websites, portals or social network pages of agencies, organizations and individuals may not provide, post or transmit the information prescribed in Clauses 1, 2, 3, 4 and 5, Article 16 of this Law and other information infringing upon national security.

2. Domestic and foreign enterprises providing services on the telecommunications networks or the Internet or providing value-added services in cyberspace in Vietnam shall:

a/ Verify information when users register digital accounts; keep user information and accounts confidential; provide user information to the Ministry of Public Security's professional cyber security protection force when receiving the latter's written requests to serve the investigation and handling of violations of the law on cyber security;

b/ Block the sharing of information, remove the information prescribed in Clauses 1, 2, 3, 4, and 5, Article 16 of this Law on the service platforms or information systems under their direct management within 24 hours after receiving a request from the Ministry of Public Security's professional cyber security protection force or a competent agency of the Ministry of Information and Communications and keep a system log for a period prescribed by the Government to serve the investigation and handling of violations of the law on cyber security;

c/ Refrain from providing or stop providing services on telecommunications networks or the Internet or value-added services to organizations and individuals that publish in cyberspace the information prescribed in Clauses 1, 2, 3, 4, and 5, Article 16 of this Law when so requested by the Ministry of Public Security's professional cyber security protection force or a competent agency of the Ministry of Information and Communications.

3. Domestic and foreign enterprises providing services on telecommunications networks or the Internet or providing value-added services in cyberspace in Vietnam that collect, exploit, analyze and process personal information or data on relationships of service users and data created by service users in Vietnam shall store these data in Vietnam for a period prescribed by the Government.

Foreign enterprises referred to in this Clause shall establish branches or representative offices in Vietnam.

4. The Government shall detail Clause 3 of this Article.

Article 27. Cyber security research and development

1. Cyber security research and development cover:

a/ Developing cyber security protection software and equipment;

b/ Developing methods for appraising cyber security protection software and equipment in order to ensure that they are up to standards and restrict security weaknesses or vulnerabilities or malware;

c/ Developing methods for testing supplied hardware and software in order to ensure their proper operation;

d/ Developing methods for protecting state secrets, work secrets, business secrets, personal and family secrets and privacy; and for ensuring confidentiality upon transmission of information in cyberspace;

dd/ Identifying the origin of information transmitted in cyberspace;

e/ Handling cyber security threats;

g/ Building cyber ranges and environments for cyber security testing;

i/ Developing technical initiatives to improve cyber security awareness and skills;

i/ Forecasting cyber security developments;

k/ Conducting practical research and developing theories on cyber security.

2. Related agencies, organizations and individuals have the right to conduct cyber security research and development.

Article 28. Improvement of cyber security self-reliance

1. The State shall encourage and create conditions for agencies, organizations and individuals to improve their self-reliance in cyber security and build their capacity of production, testing, evaluation and appraisal of digital equipment, network services and network applications.

2. The Government shall apply the following measures to help agencies, organizations and individuals improve their self-reliance in cyber security:

a/ Promoting the transfer, research, command and development of cyber security protection technologies, products, services and applications;

b/ Promoting the application of new and advanced technologies related to cyber security;

c/ Organizing training, development and use of cyber security human resources;

d/ Improving the business environment and competition conditions to support enterprises to research and produce cyber security protection products, services and applications.

Article 29. Protection of children in cyberspace

1. Children have the right to be protected, access information, participate in social, recreational and entertainment activities, confidentiality of their personal secrets and privacy and other rights when participating in cyberspace.

2. Information system managers, enterprises providing services in telecommunications networks or the Internet and enterprises providing value-added services in cyberspace shall control the contents of information in the information systems or services they manage or provide so as to avoid causing harms to children, infringing upon children or children's rights; restrict the sharing of or remove information causing harms to children or infringing upon children or children's rights; promptly notify and cooperate with the Ministry of Public Security's professional cyber security protection force in handling such harmful information.

3. Agencies, organizations and individuals operating in cyberspace shall cooperate with competent agencies in guaranteeing children's rights in cyberspace and block information causing harms to children in accordance with this Law and the law on children.

4. Agencies, organizations, parents, teachers, child carers and other related individuals shall guarantee children's rights and protect children participating in cyberspace in accordance with the law on children.

5. Professional cyber security protection forces and competent agencies shall apply measures to prevent, detect, stop and strictly handle acts of using cyberspace to cause harms to children or infringe upon children or children's rights.

Chapter V

ASSURANCE OF CYBER SECURITY PROTECTION ACTIVITIES

Article 30. Cyber security protection forces

1. Professional cyber security protection forces shall be arranged at the Ministry of Public Security and the Ministry of National Defense.

2. Cyber security protection forces shall be arranged at ministries, sectors, provincial-level People's Committees, and agencies and organizations directly managing information systems of national security importance.

3. Organizations and individuals may be mobilized to participate in cyber security protection.

Article 31. Assurance of human resources for cyber security protection

1. Vietnamese citizens having knowledge about cyber security, cyberinformation security and information technology are the basic and major resource for cyber security protection.

2. The State shall adopt programs and plans on building and development of human resources for cyber security protection.

3. Upon occurrence of dangerous cyber security circumstances, cyber-attacks, cyber security incidents or cyber security threats, competent state agencies shall decide to mobilize human resources for cyber security protection.

The competence, responsibilities, order and procedures for mobilization of human resources for cyber security protection must comply with the Law on National Security, the Law on National Defense, the Law on the People's Public Security Force and other relevant laws.

Article 32. Recruitment, training and development of cyber security protection forces

1. Vietnamese citizens who satisfy all standards on ethics, health, and qualifications and knowledge about cyber security, cyberinformation security and information technology may be recruited into cyber security protection forces if they so wish.

2. To prioritize the training and development of high-quality cyber security protection forces.

3. To prioritize the development of cyber security training institutions up to international standards; encourage partnership and create opportunities for cooperation in cyber security between the state and private sectors and between domestic and foreign partners.

Article 33. Education and training in cyber security knowledge and operations

1. Cyber security knowledge education and training shall be included in the national defense and security education subject at schools and national defense and security knowledge training programs in accordance with the Law on National Defense and Security Education.

2. The Ministry of Public Security shall assume the prime responsibility for, and coordinate with related ministries and sectors in, organizing training in cyber security operations for cyber security protection forces and civil servants, public employees and workers engaged in cyber security protection.

The Ministry of National Defense and the Government Cipher Committee shall organize cyber security operations training for related people under their management.

Article 34. Dissemination of cyber security knowledge

1. The State shall adopt policies to disseminate cyber security knowledge nationwide, and encourage state agencies to coordinate with private organizations and individuals in implementing cyber security education and awareness raising programs.

2. Ministries, sectors, agencies and organizations shall plan and implement activities of disseminating cyber security knowledge for their cadres, civil servants, public employees and workers.

3. Provincial-level People's Committees shall plan and implement activities of disseminating knowledge and raising awareness about cyber security for agencies, organizations and individuals in localities.

Article 35. Funds for cyber security protection

1. Funds for cyber security protection activities of state agencies and political organizations shall be allocated from the state budget in annual state budget estimates. The management and use of such funds must comply with the law on the state budget.

2. Agencies and organizations other than those prescribed in Clause 1 of this Article shall allocate their own funds for the cyber security protection of their information systems.

Chapter VI

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS

Article 36. Responsibilities of the Ministry of Public Security

The Ministry of Public Security shall take responsibility before the Government for performing the state management of cyber security and

has the following tasks and powers, except those falling under the responsibilities of the Ministry of National Defense and the Government Cipher Committee:

1. To promulgate or propose competent state agencies to promulgate legal documents on cyber security and guide the implementation thereof.

2. To formulate and propose strategies, policies and plans on cyber security protection.

3. To prevent and combat activities of using cyberspace to infringe upon national sovereignty, interests or security and social order and safety, and cyber-crimes.

4. To ensure information security in cyberspace; to create mechanisms for verifying information declared for registration of digital accounts; to give warnings about and share information on cyber security and cyber security threats.

5. To advise and propose the Government and the Prime Minister to consider and decide on the assignment and coordination of implementation of measures for protecting cyber security, preventing and handling acts of infringing upon cyber security if these measures are related to the state management of many ministries and sectors.

6. To organize cyber-attack prevention and fighting drills and cyber security incident response and remediation drills for information systems of national security importance.

7. To conduct examination and inspection, settle complaints and denunciations and handle violation of the law on cyber security.

Article 37. Responsibilities of the Ministry of National Defense

The Ministry of National Defense shall take responsibility before the Government for performing the state management of cyber security within the scope of its management and has the following tasks and powers:

1. To promulgate or propose competent state agencies to promulgate legal documents on cyber security under its management and guide the implementation thereof;

2. To formulate and propose strategies, policies or plans on protection of cyber security within the scope of its management.

3. To prevent and combat activities of using cyberspace infringing upon national security within the scope of its management.

4. To coordinate with the Ministry of Public Security in organizing cyber-attack prevention and fighting drills, cyber security incident response and remedy drills for information systems of national security importance, and organizing cyber security protection work.

5. To conduct examination and inspection, settle complaints and denunciations and handle violations of the law on cyber security within the scope of its management.

Article 38. Responsibilities of the Ministry of Information and Communications

1. To coordinate with the Ministry of Public Security and the Ministry of National Defense in cyber security protection work.

2. To coordinate with related agencies in refuting information opposing the State of the Socialist Republic of Vietnam prescribed in Clause 1, Clause 16 of this Law.

3. To request enterprises providing services in telecommunications networks or the Internet and value-added services in cyberspace and information system managers in removing information violating the law on cyber security on their services and information systems under their management.

Article 39. Responsibilities of the Government Cipher Committee

1. To advise and propose the Minister of National Defense to promulgate or propose competent agencies to promulgate legal documents, programs and plans on cryptography and organize the implementation thereof to protect cyber security under its management.

2. To protect cyber security for cryptographic information systems under the Committee and cryptographic products provided by the Committee in accordance with this Law.

3. To perform the unified management of scientific and technological research in cryptography; use and provision of cryptographic products to protect information classified as state secrets stored and exchanged in cyberspace.

Article 40. Responsibilities of ministries, sectors and provincial-level People's Committees

Within the ambit of their tasks and powers, ministries, sectors and provincial-level People's Committees shall conduct cyber security inspection of information and information systems under their management; and coordinate with the Ministry of Public Security in performing the state management of cyber security in their ministries, sectors and localities.

Article 41. Responsibilities of enterprises providing services in cyberspace

1. Enterprises providing services in cyberspace in Vietnam have the following responsibilities:

a/ To give warnings about cyber security risks in the use of the services they provide in cyberspace and guide preventive measures;

b/ To devise plans and solutions for quick reaction to cyber security incidents, immediately handle security weaknesses and vulnerabilities, malware, cyber-attacks, network intrusion and other security risks; upon occurrence of cyber security incidents, to immediately implement emergency plans and apply appropriate response measures and, at the same time, report such incidents to professional cyber security protection forces in accordance with this Law;

c/ To apply technical solutions and other necessary measures to ensure security throughout the process of information collection, prevent risks of data disclosure, leakage, damage or loss; upon occurrence of an incident or a risk involving disclosure, leakage, damage or loss of user information data, to immediately put forward response solutions, notify users and report such incident or risk to professional cyber security protection forces in accordance with this Law;

d/ To cooperate with and create conditions for professional cyber security protection forces in cyber security protection.

2. Enterprises providing services on telecommunications networks or the Internet and enterprises providing value-added services in cyberspace in Vietnam shall comply with the provisions in Clause 1, this Article, and Clauses 2 and 3, Article 26, of this Law.

Article 42. Responsibilities of agencies, organizations and individuals using cyberspace

1. To comply with the law on cyber security.

2. To promptly provide information relating to cyber security protection, cyber security threats, and acts of infringing upon cyber security to competent agencies and cyber security protection forces.

3. To comply with requirements and instructions of competent agencies in cyber security protection; to help and create conditions for responsible agencies, organizations and individuals to implement cyber security protection measures.

Chapter VII

IMPLEMENTATION PROVISIONS

Article 43. Effect

1. This Law takes effect on January 1, 2019.

2. Managers of operating information systems which are included in the list of information systems of national security importance shall, within 12 months from the effective date of this Law, fully meet the cyber security conditions; professional cyber security protection forces shall assess the cyber security conditions under Article 12 of this Law; the extension of such time limit, when necessary, shall be decided by the Prime Minister but must not exceed 12 months.

3. Managers of operating information systems which are added to the list of information systems of national security importance shall, within 12 months from the date of addition, fully meet the cyber security conditions; professional cyber security protection forces shall assess the cyber security conditions under Article 12 of this Law; the extension of such time limit, when necessary, shall be decided by the Prime Minister but must not exceed 12 months.

This Law was passed on June 12, 2018, by the XIVth National Assembly of the Socialist Republic of Vietnam at its 5th session.-

Chairwoman of the National Assembly
NGUYEN THI KIM NGAN