THE NATIONAL ASSEMBLY	THE SOCIALIST REPUBLIC OF VIETNAM
No. 86/2015/QH13	Independence - Freedom - Happiness

Law on Cyberinformation Security

Pursuant to the Constitution of the Socialist Republic of Vietnam;

The National Assembly promulgates the Law on Cyberinformation Security.

Chapter I

GENERAL PROVISIONS

Article 1. Scope of regulation

This Law prescribes cyberinformation security activities, and rights and responsibilities of agencies, organizations and individuals in ensuring cyberinformation security; civil cryptography; standards and technical regulations on cyberinformation security; trading in the field of cyberinformation security; development of human resources for cyberinformation security; and state management of cyberinformation security.

Article 2. Subjects of application

This Law applies to Vietnamese agencies, organizations and individuals and foreign organizations and individuals directly involved in or related to cyberinformation security activities in Vietnam.

Article 3. Interpretation of terms

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

1. *Cyberinformation security* means the protection of information and information systems in cyberspace from being illegally accessed, utilized, disclosed, interrupted, altered or sabotaged in order to ensure the integrity, confidentiality and usability of information.

2. *Cyberspace* means an environment where information is provided, transmitted, collected, processed, stored and exchanged over telecommunications networks and computer networks.

3. *Information system* means a combination of hardware, software and databases established to serve the creation, provision, transmission, collection, processing, storage and exchange of information in cyberspace.

4. *National important information system* means an information system which, when being sabotaged, will cause extremely serious harms to national defense and security.

5. *Managing body of an information system* means an agency, organization or individual competent to directly manage an information system.

6. *Infringement upon cyberinformation security* means an act of illegally accessing, utilizing, disclosing, interrupting, altering or sabotaging information or information systems.

7. *Cyberinformation security incident* means an incident that harms information or an information system, affecting the integrity, confidentiality or usability of information.

8. *Cyberinformation security risk* means a subjective factor or an objective factor that is likely to affect the status of cyberinformation security.

9. *Cyberinformation security risk assessment* means the detection, analysis and estimation of levels of harm and threats to information or information systems.

10. *Cyberinformation security risk management* means the introduction of measures to minimize cyberinformation security risks.

11. *Malicious software* (malware) means software that is likely to cause abnormal operation to part or the whole of an information system or that illegally copies, alters or deletes information stored in such information system.

12. *Malware filtering system* means a combination of hardware and software connected to a network to detect, prevent, filter, and collect statistics of, malware.

13. *Electronic address* means an address used to send and receive information in cyberspace, including email address, telephone number, internet address and other similar forms.

14. *Information-related conflict* means two or more domestic and foreign organizations using communication technological or technical measures to harm information or information systems in cyberspace.

15. *Personal information* means information associated with the identification of a specific person.

16. *Owner of personal information* means a person identified based on such information.

17. *Processing of personal information* means the performance of one or some operations of collecting, editing, utilizing, storing, providing, sharing or spreading personal information in cyberspace for commercial purpose.

18. *Civil cryptography* means cryptographic techniques and products used to keep secret or authenticate information not classified as state secret.

19. *Cyberinformation security product* means hardware or software functioning to protect information and information systems.

20. *Cyberinformation security service* means the service of protecting information and information systems.

Article 4. Principles of ensuring cyberinformation security

1. All agencies, organizations and individuals shall ensure cyberinformation security. Cyberinformation security activities must comply with law and ensure national defense and security and state secrets, firmly maintain political stability and social order and safety, and promote socio-economic development.

2. Organizations and individuals may not infringe upon cyberinformation security of others.

3. The response to cyberinformation security incidents must guarantee lawful rights and interests of organizations and individuals and may not infringe upon privacy, personal and family secrets of individuals and private information of organizations.

4. Cyberinformation security activities shall be conducted in a regular, continuous, prompt and effective manner.

Article 5. State policies on cyberinformation security

1. To step up training and development of human resources for cyberinformation security and construction of cyberinformation security technical infrastructure to meet the requirements of political stability, socio-economic development, and assurance of national defense and security and social order and safety.

2. To encourage the research, development and application of technical, technological, export support and market expansion measures for domestically produced cyberinformation security products and services; to facilitate the import of modern products and technologies that cannot be domestically produced or provided yet.

3. To ensure a fair competitive environment for the provision of cyberinformation security products and services; to encourage and create conditions for organizations and individuals to participate in investment, research, development and provision of cyberinformation security products and services.

4. The State shall allocate funds for ensuring cyberinformation security for state agencies and national important information systems.

Article 6. International cooperation on cyberinformation security

1. International cooperation on cyberinformation security must adhere to the following principles:

a/ Respect for national independence, sovereignty and territorial integrity, non-intervention into one another's internal affairs, equality, and mutual benefit;

b/ Compliance with Vietnamese law and treaties to which the Socialist Republic of Vietnam is a contracting party.

2. Contents of international cooperation on cyberinformation security include:

a/ International cooperation in training in, and research and application of cyberinformation security sciences, techniques and technologies;

b/ International cooperation in prevention and control of violations of the law on cyberinformation security; investigation of and response to cyberinformation security incidents, and preclusion of the taking advantage of cyberspace for terrorist purposes;

c/ Other activities of international cooperation on cyberinformation security.

Article 7. Prohibited acts

1. Blocking the transmission of information in cyberspace, or illegally intervening, accessing, harming, deleting, altering, copying or falsifying information in cyberspace.

2. Illegally affecting or obstructing the normal operation of information systems or the users' accessibility to information systems.

3. Illegally attacking, or nullifying cyberinformation security protection measures of, information systems; attacking, seizing the right to control, or sabotaging, information systems.

4. Spreading spams or malware or establishing fake and deceitful information systems.

5. Illegally collecting, utilizing, spreading or trading in personal information of others; abusing weaknesses of information systems to collect or exploit personal information.

6. Hacking cryptographic secrets and lawfully enciphered information of agencies, organizations or individuals; disclosing information on civil cryptographic products or information on clients that lawfully use civil cryptographic products; using or trading in civil cryptographic products of unclear origin.

Article 8. Handling of violations of the law on cyberinformation security

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

Chapter II

ASSURANCE OF CYBERINFORMATION SECURITY

Section 1

CYBERINFORMATION PROTECTION

Article 9. Classification of information

1. Information-owning agencies and organizations shall classify information based on its secrecy in order to take appropriate protection measures.

2. Information regarded as state secret shall be classified and protected in accordance with the law on protection of state secrets.

Agencies and organizations that use classified and unclassified information in activities within their fields shall develop regulations and procedures for processing information; determine contents and methods of recording authorized accesses to classified information.

Article 10. Management of sending of information

1. The sending of information in cyberspace must meet the following requirements:

a/ Not forging the information sender source;

b/ Complying with this Law and other relevant laws.

2. Commercial information may not be sent to electronic addresses of recipients when the latter has not yet consented or has refused to receive, unless the recipients are obliged to receive information under law.

3. Telecommunications enterprises, enterprises providing telecommunications application services and enterprises providing information technology services that send information shall:

a/ Comply with the law on storage of information and protection of personal information and private information of organizations and individuals;

b/ Take blocking and handling measures upon receiving notices of organizations or individuals that the sending of information is illegal;

c/ Offer recipients to refuse to receive information;

d/ Provide necessary technical and professional conditions upon request for competent state agencies to manage and ensure cyberinformation security.

Article 11. Prevention, detection, stoppage and handling of malware

1. Agencies, organizations and individuals shall prevent and stop malware as guided or requested by competent state agencies.

2. The managing body of a national important information system shall put into operation technical and professional systems for preventing, detecting, stopping and promptly handling malware.

3. Enterprises providing email services or transmitting and storing information must have malware filtering systems in the course of sending, receiving and storing information via their systems and shall send reports to competent state agencies in accordance with law.

4. Internet service-providing enterprises shall take measures to manage, prevent, detect, and stop the spread of, malware and handle it at the request of competent state agencies.

5. The Ministry of Information and Communications shall assume the prime responsibility for, and coordinate with the Ministry of National Defense, the Ministry of Public Security and related ministries and sectors in, preventing, detecting, stopping and handling malware that affects national defense and security.

Article 12. Security assurance for telecommunications resources

1. Users of telecommunications resources shall:

a/ Apply managerial and technical measures to prevent cyberinformation insecurity arising from their frequencies, number stores, domain names and internet addresses;

b/ Coordinate with, and provide information relating to telecommunications resource security for, competent state agencies upon request.

2. Enterprises providing services on the internet shall manage, and coordinate in preventing cyberinformation insecurity arising from, internet resources and their clients; provide adequate information at the request of competent state agencies; coordinate in connection and routing to ensure secure and stable operation of Vietnam's system of national domain name servers.

3. The Ministry of Information and Communications shall ensure cyberinformation security for Vietnam's system of national domain name servers.

Article 13. Response to cyberinformation security incidents

1. Response to a cyberinformation security incident means activities aiming to handle and remedy an incident that causes cyberinformation insecurity.

2. Response to cyberinformation security incidents must adhere to the following principles:

a/ Being prompt, rapid, accurate, synchronous and effective;

b/ Complying with the law on coordination of response to cyberinformation security incidents;

c/ Ensuring coordination among domestic and foreign agencies, organizations and enterprises.

3. Ministries, ministerial-level agencies, government-attached agencies, provincial-level People's Committees, telecommunications enterprises and managing bodies of national important information systems shall establish or appoint a specialized division to respond to cyberinformation security incidents.

4. The Ministry of Information and Communications shall coordinate response to cyberinformation security incidents nationwide, and prescribe in detail coordination of response to cyberinformation security incidents.

Article 14. Emergency response to ensure national cyberinformation security

1. Emergency response to ensure national cyberinformation security means incident response activities in catastrophic circumstances or at the request of competent state agencies with a view to ensuring national cyberinformation security.

2. Emergency response to ensure national cyberinformation security must adhere to the following principles:

a/ Organizing response according to decentralized competence;

b/ Conducting response on the spot, rapidly, strictly and with close coordination;

c/ Applying effective and feasible technical measures.

3. Emergency response plans to ensure national cyberinformation security include:

a/ Emergency response plan to ensure national cyberinformation security;

b/ Emergency response plan to ensure cyberinformation security for state agencies, political organizations and socio-political organizations;

c/ Emergency response plan to ensure cyberinformation security for localities;

d/ Emergency response plan to ensure cyberinformation security for telecommunications enterprises.

4. Responsibilities to ensure national cyberinformation security are prescribed as follows:

a/ The Prime Minister shall decide on emergency response plans to ensure national cyberinformation security;

b/ The Ministry of Information and Communications shall coordinate emergency response to ensure national cyberinformation security;

c/ Ministries, sectors, People's Committees at all levels, and related agencies and organizations shall, within the ambit of their tasks and powers, coordinate and direct emergency response to ensure national cyberinformation security;

d/ Telecommunications enterprises shall take emergency response measures and coordinate with the Ministry of Information and Communications and related ministries, sectors and People's Committees at all levels in ensuring national cyberinformation security.

Article 15. Responsibilities of agencies, organizations and individuals in ensuring cyberinformation security

1. Agencies, organizations and individuals engaged in cyberinformation security activities shall coordinate with competent state agencies and other organizations and individuals in ensuring cyberinformation security.

2. Agencies, organizations and individuals using services in cyberspace shall promptly notify service-providing enterprises or specialized incident response units of cyberinformation security sabotaging acts or incidents.

Section 2

PROTECTION OF PERSONAL INFORMATION

Article 16. Principles of protecting personal information in cyberspace

1. Individuals shall themselves protect their personal information and comply with the law on provision of personal information when using services in cyberspace.

2. Agencies, organizations and individuals that process personal information shall ensure cyberinformation security for the information they process.

3. Organizations and individuals that process personal information shall develop and publicize their own measures to process and protect personal information.

4. The protection of personal information must comply with this Law and other relevant laws.

5. The processing of personal information for the purpose of ensuring national defense and security and social order and safety or for non-commercial purposes must comply with other relevant laws.

Article 17. Collection and use of personal information

1. Organizations and individuals that process personal information shall:

a/ Collect personal information only after obtaining the consent of its owners regarding the scope and purpose of collection and use of such information;

b/ Use the collected personal information for purposes other than the initial one only after obtaining the consent of its owners;

c/ Refrain from providing, sharing or spreading to a third party personal information they have collected, accessed or controlled, unless they obtain the consent of the owners of such personal information or at the request of competent state agencies.

2. State agencies shall secure and store personal information they have collected.

3. Owners of personal information may request personal information-processing organizations and individuals to provide their personal information collected and stored by the latter.

Article 18. Updating, alteration and cancellation of personal information

1. Owners of personal information may request personal information-processing organizations and individuals to update, alter or cancel their personal information collected or stored by the latter or to stop providing such personal information to a third party.

2. Upon receiving the request of an owner of personal information for update, alteration or cancellation of personal information or for stoppage of the provision of personal information to a third party, a personal information-processing organization or individual shall:

a/ Comply with the request and notify such owner or grant him/her/it the right to access information for the latter to update, alter or delete his/her/its personal information;

b/ Take appropriate measures to protect personal information; and notify such owner if it/he/she fails to comply with the request for technical or other reasons.

3. Personal information-processing organizations and individuals shall delete the stored personal information when they have accomplished their use purposes or the storage time has expired and notify such to the owners of such personal information, unless otherwise prescribed by law.

Article 19. Security assurance for personal information in cyberspace

1. Personal information-processing organizations and individuals shall take appropriate management and technical measures to protect personal information they have collected and stored; and comply with standards and technical regulations on assurance of cyberinformation security.

2. When a cyberinformation security incident occurs or threatens to occur, personal information-processing organizations and individuals shall take remedy and stoppage measures as soon as possible.

Article 20. Responsibilities of state management agencies in protecting personal information in cyberspace

1. To establish online information channels for receiving petitions and reports from the public which are related to security assurance for personal information in cyberspace.

2. To annually inspect and examine personal information-processing organizations and individuals; to conduct extraordinary inspection and examination when necessary.

Section 3

PROTECTION OF INFORMATION SYSTEMS

Article 21. Classification of security grades of information systems

1. Classification of information systems by security grade means the determination of information security grades of information systems in an ascending order from 1 to 5 for taking appropriate management and technical measures to properly protect information systems of each grade.

2. Information systems shall be classified by security grade as follows:

a/ Grade 1 means that when an information system is sabotaged, it will harm lawful rights and interests of organizations or individuals but will not harm public interests, social order and safety or national defense and security;

b/ Grade 2 means that when an information system is sabotaged, it will seriously harm lawful rights and interests of organizations or individuals or will harm public interests but will not harm social order and safety or national defense and security;

c/ Grade 3 means that when an information system is sabotaged, it will seriously harm production, public interests and social order and safety or will harm national defense and security;

d/ Grade 4 means that when an information system is sabotaged, it will cause extremely serious harms to public interests and social order and safety or will seriously harm national defense and security;

dd/ Grade 5 means that when an information system is sabotaged, it will cause extremely serious harms to national defense and security.

3. The Government shall prescribe in detail criteria, competence, order and procedures for determining security grades of information systems and responsibility for ensuring security for information systems of each grade.

Article 22. Tasks of protecting information systems

1. To determine security grades of information systems.

2. To assess and manage security risks to information systems.

3. To urge, supervise and examine the protection of information systems.

4. To take measures to protect information systems.

5. To comply with the reporting regime.

6. To conduct public information for raising awareness about cyberinformation security.

Article 23. Measures to protect information systems

1. To promulgate regulations on cyberinformation security assurance in designing, developing, managing, operating, using, updating or abolishing information systems.

2. To apply management and technical measures according to standards and technical regulations on cyberinformation security for preventing and combating risks and remedying incidents to cyberinformation security.

3. To examine and supervise the observance of regulations and assess the effectiveness of applied management and technical measures.

4. To supervise security of information systems.

Article 24. Security supervision of information systems

1. Security supervision of an information system means activities of choosing a to-be-supervised object, and collecting, and analyzing the status of, information of this object with a view to identifying factors that affect the security of such information system; reporting on and warning acts of infringing upon cyberinformation security or acts threatening to cause cyberinformation security incidents to such information system; analyzing key factors that affect the status of cyberinformation security; and proposing change of technical measures.

2. Subject to security supervision of an information system are firewall, access control, major routes of information, important servers, important equipment and important terminal equipment.

3. Telecommunications enterprises, enterprises providing information technology services and enterprises providing cyberinformation security services shall coordinate with managing bodies of information systems in supervising the security of information systems at the request of competent state agencies.

Article 25. Responsibilities of managing bodies of information systems

1. Managing bodies of information systems shall protect information systems in accordance with Articles 22, 23 and 24 of this Law.

2. State-funded managing bodies of information systems shall perform the responsibilities defined in Clause 1 of this Article and shall:

a/ Make plans to ensure cyberinformation security appraised by competent state agencies when establishing, expanding or upgrading their information systems;

b/ Appoint individuals or units to take charge of cyberinformation security.

Article 26. National important information systems

1. When establishing, expanding or upgrading a national important information system, information security shall be inspected before putting this system into operation and exploitation.

2. The Ministry of Information and Communications shall assume the prime responsibility for, and coordinate with the Ministry of National Defense, the Ministry of Public Security and related ministries and sectors in, making a list of national important information systems for submission to the Prime Minister for promulgation.

Article 27. Responsibility to ensure cyberinformation security for national important information systems

1. The managing body of a national important information system shall:

a/ Comply with the provisions of Clause 2, Article 25 of this Law;

b/ Periodically have cyberinformation security risks assessed by a specialized organization designated by a competent state agency;

c/ Take standby measures for information systems;

d/ Plan and conduct drills in the protection of national important information systems.

2. The Ministry of Information and Communications shall:

a/ Assume the prime responsibility for, and coordinate with managing bodies of national important information systems, the Ministry of Public Security and related ministries and sectors in, guiding, urging, inspecting and examining the protection of cyberinformation security for national important information systems, except those specified in Clauses 3 and 4 of this Article;

b/ Request telecommunications enterprises, enterprises providing information technology services and enterprises providing cyberinformation security services to provide technical advice and assistance and respond to cyberinformation security incidents for national important information systems.

3. The Ministry of Public Security shall guide, urge, inspect and examine the protection of cyberinformation security for national important information systems under its management; and coordinate with the Ministry of Information and Communications, managing bodies of national important information

systems and related ministries, sectors and People's Committees at all levels in protecting other national important information systems at the request of competent state agencies.

4. The Ministry of National Defense shall guide, urge, inspect and examine the protection of cyberinformation security for national important information systems under its management.

5. The Government Cipher Committee shall organize the use of ciphers for protecting information in national important information systems of state agencies, political organizations and socio-political organizations; and coordinate with managing bodies of national important information systems in supervising cyberinformation security in accordance with law.

Section 4

STOPPAGE OF INFORMATION-RELATED CONFLICTS IN CYBERSPACE

Article 28. Responsibilities of organizations and individuals for stopping information-related conflicts in cyberspace

1. Within the ambit of their tasks and powers, organizations and individuals shall:

a/ Stop sabotaging information originating from their information systems; collaborate with one another in identifying sources, and repulsing, and remedying consequences of, cyber-attacks carried out via information systems of domestic and foreign organizations and individuals;

b/ Stop acts of domestic and foreign organizations and individuals that aim to sabotage the integrity of information networks;

c/ Preclude the organization of illegal cyberspace activities of domestic and foreign organizations and individuals that seriously affect national defense and security or social order and safety.

2. The Government shall prescribe in detail the stoppage of information-related conflicts in cyberspace.

Article 29. Stoppage of use of cyberspace for terrorist purposes

1. Measures to stop the use of cyberspace for terrorist purposes include:

a/ Nullifying internet sources used to commit terrorist acts;

b/ Stopping the establishment and expansion of the exchange of information on signals, factors, methods and ways to use the internet for committing terrorist acts, and on objectives and operation of cyberterrorism organizations;

c/ Exchanging experiences and practices in controlling internet sources, and seeking and controlling contents of websites for terrorist purpose.

2. The Government shall prescribe in detail responsibilities and measures to stop the use of cyberspace for terrorist purposes prescribed in Clause 1 of this Article.

Chapter III

CIVIL CRYPTOGRAPHY

Article 30. Civil cryptographic products and services

1. Civil cryptographic products include cryptographic documents and technical and professional equipment used to protect information not classified as state secret.

2. Civil cryptographic services include services of protection of information using civil cryptographic products; inspection and assessment of civil cryptographic products; and counseling on cyberinformation confidentiality and security using civil cryptographic products.

Article 31. Trading in civil cryptographic products and services

1. An enterprise that wishes to trade in civil cryptographic products and services on the list of civil cryptographic products and services shall obtain a license for doing so.

2. An enterprise shall be granted a license for trading in civil cryptographic products and services when fully meeting the following conditions:

a/ Having managerial, administration and technical staff members who meet professional requirements on information confidentiality and security;

b/ Having equipment and physical foundations suitable to the scale of provision of civil cryptographic products and services;

c/ Having a technical plan conformable with standards and technical regulations;

d/ Having a cyberinformation confidentiality and security plan in the course of management and provision of civil cryptographic products and services;

dd/ Having an appropriate business plan.

3. Civil cryptographic products shall be inspected and certified as conformable with regulations before being marketed.

4. To obtain a license for trading in civil cryptographic products and services, an enterprise shall pay a fee in accordance with the law on charges and fees.

5. The Government shall promulgate a list of civil cryptographic products and services and detail this Article.

Article 32. Order and procedures for grant of licenses for trading in civil cryptographic products and services

1. An enterprise applying for a license for trading in civil cryptographic products and services shall submit a dossier of application for a license at the Government Cipher Committee.

2. A dossier of application for a license for trading in civil cryptographic products and services shall be made in two sets, each comprising:

a/ An application for a license for trading in civil cryptographic products and services;

b/ A copy of the enterprise registration certificate, investment registration certificate or another paper of equivalent validity;

c/ Copies of information confidentiality and security diplomas or certificates of managerial, administration and technical staff members;

d/ A technical plan, consisting of papers on technical characteristics and specifications of products; standards or technical regulations of products; standards and quality of services; technical measures and solutions; and product warranty and maintenance plan;

dd/ A cyberinformation confidentiality and security plan in the course of management and provision of civil cryptographic products and services;

e/ A business plan, indicating the scope of provision and recipients of products and services, scale and quantity of products and services, customer service networks, and technical assurance.

3. Within 30 days after receiving a complete dossier, the Government Cipher Committee shall appraise it and grant a license for trading in civil cryptographic products and services; if refusing to grant a license, it shall issue a written notice clearly stating the reason.

4. A license for trading in civil cryptographic products and services shall be valid for 10 years.

Article 33. Modification, supplementation, re-grant, extension, suspension and revocation of licenses for trading in civil cryptographic products and services

1. A license for trading in civil cryptographic products and services shall be modified and supplemented in case the enterprise possessing this license is renamed, replaces its at-law representative, or changes or adds civil cryptographic products and services.

An enterprise shall submit a dossier for license modification and supplementation at the Government Cipher Committee. Such dossier shall be made in two sets, each comprising:

a/ A written request for license modification and supplementation;

b/ A copy of the enterprise registration certificate, investment registration certificate or another paper of equivalent validity;

c/ The granted license for trading in civil cryptographic products and services;

d/ A technical plan, a cyberinformation confidentiality and security plan, and a business plan for products and services to be added as specified at Points d, dd and e, Clause 2, Article 32 of this Law, in case the enterprise wishes to add civil cryptographic products and services or business lines;

Within 10 working days after receiving a complete dossier, the Government Cipher Committee shall appraise it, modify and supplement the license and re-grant a license to the enterprise; if refusing to re-grant a license, it shall issue a written notice clearly stating the reason.

2. If its license for trading in civil cryptographic products and services is lost or damaged, an enterprise shall send a written request for re-grant, clearly stating the reason, to the Government Cipher Committee. Within 5 working days after receiving the request, the Government Cipher Committee shall consider it and re-grant a license to the enterprise.

3. An enterprise that does not violate the law on trading in civil cryptographic products and services may have its license for trading in civil cryptographic products and services extended once for no more than one year.

A dossier for license extension shall be sent to the Government Cipher Committee at least 60 days before the license expires, and shall be made in two sets, each comprising:

a/ A written request for license extension;

b/ The license for trading in civil cryptographic products and services which remains valid;

c/ A report on the enterprise's operation over the latest 2 years.

Within 20 days after receiving a complete dossier, the Government Cipher Committee shall appraise it, decide to extend the license and re-grant a license to the enterprises; if refusing to re-grant a license, it shall issue a written notice clearly stating the reason.

4. An enterprise shall be suspended from trading in civil cryptographic products and services for up to 6 months in the following cases:

a/ It provides products and services not stated in the license;

b/ It fails to satisfy one of the conditions specified in Clause 2, Article 31 of this Law;

c/ Other cases provided for by law.

5. An enterprise will have its license for trading in civil cryptographic products and services revoked in the following cases:

a/ It fails to provide the services within one year after being granted the license without a plausible reason;

b/ The license expires;

c/ It is unable to remedy the problems mentioned in Clause 4 of this Article after the suspension period expires.

Article 34. Export and import of civil cryptographic products

1. If wishing to export and import civil cryptographic products on the list of civil cryptographic products subject to export and import permit, an enterprise must obtain a permit for export and import of civil cryptographic products from a competent state agency.

2. An enterprise shall be granted a permit for export and import of civil cryptographic products when fully meeting the following conditions:

a/ Possessing a license for trading in civil cryptographic products and services;

b/ Having to-be-imported civil cryptographic products certified and announced as conformable with regulations under Article 39 of this Law;

c/ Ensuring that users and use purposes of civil cryptographic products do not harm national defense and security or social order ad safety.

3. A dossier of application for a permit for export and import of civil cryptographic products must comprise:

a/ An application for a permit for export and import of civil cryptographic products;

b/ A copy of the license for trading in civil cryptographic products and services;

c/ A copy of the regulation conformity certificate, for civil cryptographic products to be imported.

4. Within 10 working days after receiving a complete dossier, the Government Cipher Committee shall appraise it and grant a permit for export and import of civil cryptographic products to the enterprise; if refusing to grant a license, it shall issue a written notice clearly stating the reason.

5. The Government shall promulgate a list of civil cryptographic products subject to export and import permit and detail this Article.

Article 35. Responsibilities of enterprises trading in civil cryptographic products and services

1. To manage dossiers and documents on technical solutions and technologies of the products.

2. To establish, store and secure customer information, and names, types, quantities and use purposes of civil cryptographic products and services.

3. To report to the Government Cipher Committee on the trading in and export and import of civil cryptographic products and services and summarize customer information before December 31 every year.

4. To take measures to ensure secure and safe transportation and preservation of civil cryptographic products.

5. To refuse to provide civil cryptographic products and services when detecting their users' violations of the law on use of civil cryptographic products and services or violations of agreed commitments on use of the products and services provided by the enterprises.

6. To suspend or stop providing civil cryptographic products and services in order to ensure national defense and security and social order and safety at the request of competent state agencies.

7. To coordinate with and create conditions for competent state agencies to take professional measures upon request.

Article 36. Responsibilities of users of civil cryptographic products and services

1. To comply with the commitments with enterprises providing civil cryptographic products and services regarding the use management of cryptographic keys, transfer, repair, maintenance, abandonment and destruction of civil cryptography products, and other relevant contents.

2. To provide necessary information relating to cryptographic keys for competent state agencies upon request.

3. To coordinate with and create conditions for competent state agencies to take measures to prevent crimes of stealing information or cryptographic keys and using civil cryptographic products for illegal purposes.

4. Except for diplomatic representative missions, foreign consular offices and representative missions of inter-governmental international organizations in Vietnam, organizations and individuals that use civil cryptographic products provided by those other than enterprises licensed to trade in civil cryptographic products shall declare such to the Government Cipher Committee.

Chapter IV

STANDARDS AND TECHNICAL REGULATIONS ON CYBERINFORMATION SECURITY

Article 37. Standards and technical regulations on cyberinformation security

1. Standards on cyberinformation security include international standards, regional standards, foreign standards, national standards and manufacturer standards on information systems, hardware, software, and systems for management and safe operation of cyberinformation which are announced and recognized for application in Vietnam.

2. Technical regulations on cyberinformation security include national technical regulations and local technical regulations on information systems, hardware, software, and systems for management and safe operation of cyberinformation which are developed, promulgated and applied in Vietnam.

Article 38. Management of standards and technical regulations on cyberinformation security

1. Cyberinformation security regulation conformity certification means a conformity certification organization certifying the conformity of information systems, hardware, software, and systems for management and safe operation of cyberinformation with technical regulations on cyberinformation security.

2. Cyberinformation security regulation conformity announcement means an organization or enterprise announcing the conformity of information systems, hardware, software, and systems for management and safe operation of cyberinformation with technical regulations on cyberinformation security.

3. Cyberinformation security standard conformity certification means a conformity certification organization certifying the conformity of information systems, hardware, software, and systems for management and safe operation of cyberinformation with standards on cyberinformation security.

4. Cyberinformation security standard conformity announcement means an organization or enterprise announcing the conformity of information systems, hardware, software, and systems for management and safe operation of cyberinformation with standards on cyberinformation security.

5. The Ministry of Science and Technology shall assume the prime responsibility for, and coordinate with related agencies in, appraising and announcing national standards on cyberinformation security in accordance with the law on standards and technical regulations.

6. The Ministry of Information and Communications shall:

a/ Draft national standards on cyberinformation security, except national standards mentioned in Clause 7 of this Article;

b/ Promulgate national technical regulations on cyberinformation security, except national technical regulations mentioned in Clause 7 of this Article; and stipulate cyberinformation security regulation conformity assessment;

c/ Manage the quality of cyberinformation security products and services, except civil cryptographic products and services;

d/ Register, designate, and manage the operation of, cyberinformation security conformity certification organizations, except conformity certification organizations for civil cryptographic products and services.

7. The Government Cipher Committee shall assist the Minister of National Defense in drafting national standards on civil cryptographic products and services for submission to competent state agencies for announcement and guidance for implementation; develop and submit to the Minister of National Defense for promulgation national technical regulations on civil cryptographic products and services; designate, and manage the operation of, conformity certification organizations for civil cryptographic products and services; and manage the quality of civil cryptographic products and services.

8. Provincial-level People's Committees shall develop, promulgate, and guide the implementation of, local technical regulations on cyberinformation security; and manage the quality of cyberinformation security products and services in localities.

Article 39. Assessment of cyberinformation security standard or regulation conformity

1. Assessment of cyberinformation security standard or regulation conformity shall be conducted in the following cases:

a/ Regulation conformity certification or announcement shall be conducted and regulation conformity stamps shall be used before an organization or individual markets cyberinformation security products;

b/ To serve the state management of cyberinformation security.

2. Assessment of cyberinformation security standard or regulation conformity serving national important information systems and serving the state management of cyberinformation security shall be conducted by conformity certification organizations designated by the Minister of Information and Communications.

3. Assessment of standard or regulation conformity for civil cryptographic products and services shall be conducted by conformity certification organizations designated by the Minister of National Defense.

4. The recognition of cyberinformation security standard or regulation conformity assessment results between Vietnam and other countries and territories and between conformity certification organizations of Vietnam and other countries and territories must comply with the law on standards and technical regulations.

Chapter V

TRADING IN THE FIELD OF CYBERINFORMATION SECURITY

Section 1

GRANT OF LICENSES FOR TRADING IN CYBERINFORMATION SECURITY PRODUCTS AND SERVICES

Article 40. Trading in the field of cyberinformation security

1. Trading in the field of cyberinformation security is conditional and covers trading in cyberinformation security products and provision of cyberinformation security services.

2. To trade in cyberinformation security products and services specified in Article 41 of this Law, an enterprise must obtain a license for trading in cyberinformation security products and services from a competent state agency. Such a license shall be valid for 10 years.

3. Trading in cyberinformation security products and services must comply with this Law and other relevant laws.

Conditions and the order and procedures for grant of licenses for trading in civil cryptography products and services, export and import of civil cryptography products, responsibilities of enterprises trading in civil cryptography products and services, and use of civil cryptographic products and services must comply with Chapter III of this Law.

Conditions and the order and procedures for grant of licenses for provision of e-signature certification services must comply with the law on e-transactions.

Article 41. Cyberinformation security products and services

1. Cyberinformation security services include:

a/ Cyberinformation security testing and evaluation services;

b/ Information confidentiality services without using civil cryptography;

c/ Civil cryptographic services;

d/ E-signature certification services;

dd/ Cyberinformation security counseling services;

e/ Cyberinformation security supervision services;

g/ Cyberinformation security incident response services;

h/ Data recovery services;

i/ Cyber-attack prevention and combat services;

k/ Other cyberinformation security services.

2. Cyberinformation security products include:

a/ Civil cryptographic products;

b/ Cyberinformation security testing and evaluation products;

c/ Cyberinformation security supervision products;

d/ Attack and hacking combat products;

dd/ Other cyberinformation security products.

3. The Government shall issue detailed lists of cyberinformation security products and services mentioned at Point k, Clause 1, and Point dd, Clause 2, of this Article.

Article 42. Conditions for grant of licenses for trading in cyberinformation security products and services

1. An enterprise shall be granted a license for trading in cyberinformation security products and services, except those mentioned at Points a, b, c and d, Clause 1, and Point a, Clause 2, Article 41 of this Law, when fully meeting the following conditions:

a/ Such trading complies with the national strategy, master plan or plan on cyberinformation security development;

b/ It has equipment and physical foundations suitable to the scale of provision of cyberinformation security products and services;

c/ It has managerial, administration and technical staff members meeting professional requirements on information security;

d/ It has a suitable business plan.

2. An enterprise shall be granted a license for provision of cyberinformation security testing and evaluation services when fully meeting the following conditions:

a/ The conditions specified in Clause 1 of this Article;

b/ It is established and operates lawfully in the Vietnamese territory, except foreign-invested enterprises;

c/ Its at-law representative and managerial, administration and technical staff members are Vietnamese citizens permanently residing in Vietnam;

d/ It has a technical plan conformable with relevant standards or technical regulations;

dd/ It has a customer information confidentiality plan in the course of service provision;

e/ Its managerial, administration and technical staff members possess information security testing and evaluation diplomas or certificates.

3. An enterprise shall be granted a license for provision of information confidentiality services without using civil cryptography when fully meeting the following conditions:

a/ The conditions specified at Points a, b, c, d and dd, Clause 2 of this Article;

b/ Its managerial, administration and technical staff members possess information confidentiality diplomas or certificates.

4. The Government shall detail this Article.

Article 43. Dossiers of application for licenses for trading in cyberinformation security products and services

1. An enterprise that applies for a license for trading in cyberinformation security products and services shall submit a dossier of application at the Ministry of Information and Communications.

2. A dossier of application for a license for trading in cyberinformation security products and services shall be made in five sets, each comprising:

a/ An application for a license for trading in cyberinformation security products and services, specifying types of cyberinformation security products and services to be traded;

b/ A copy of the enterprise registration certificate, investment registration certificate or another paper of equivalent validity;

c/ A written explanation of the technical equipment system compliant with law;

d/ A business plan specifying the provision scope, users and standards and quality of products and services;

dd/ Copies of information security diplomas or certificates of managerial, administration and technical staff members.

3. In addition to the papers and documents mentioned in Clause 2 of this Article, a dossier of application for a license for provision of information security testing and evaluation services or information confidentiality services without using civil cryptography must comprise:

a/ Judicial record cards of the enterprise's at-law representative and managerial, administration and technical staff members;

b/ A technical plan;

c/ A customer information confidentiality plan in the course of service provision.

Article 44. Appraisal of dossiers and grant of licenses for trading in cyberinformation security products and services

1. Within 40 days after receiving a complete dossier, the Ministry of Information and Communications shall assume the prime responsibility for, and coordinate with related ministries and sectors in, appraising the dossier, and

grant a license for trading in cyberinformation security products and services, except products and services mentioned at Points c and d, Clause 1, and Point a, Clause 2, Article 41 of this Law; if refusing to grant a license, it shall issue a written notice clearly stating the reason.

2. A license for trading in cyberinformation security products and services must have the following principal contents:

a/ Name of the enterprise and its transaction name in Vietnamese and a foreign language (if any); and its head office address in Vietnam;

b/ Name of the enterprise's at-law representative;

c/ Serial number, date of grant and expiry date of the license;

d/ Cyberinformation security products and services licensed for trading.

3. An enterprise that is granted a license for trading in cyberinformation security products and services shall pay a fee in accordance with the law on charges and fees.

Article 45. Modification, supplementation, extension, suspension, revocation and re-grant of licenses for trading in cyberinformation security products and services

1. A license for trading in cyberinformation security products and services shall be modified and supplemented in case the enterprise possessing this license is renamed or replaces its at-law representative, or changes or adds cyberinformation security products and services it provides.

The enterprise shall submit a dossier for license modification and supplementation at the Ministry of Information and Communications. Such dossier shall be made in two sets, each comprising a written request for license modification and supplementation, a detailed description of contents to be modified and supplemented, and other relevant papers.

Within 10 working days after receiving a complete dossier, the Ministry of Information and Communications shall appraise it, modify and supplement the license, and re-grant a license to the enterprise; if refusing to re-grant a license, it shall issue a written notice clearly stating the reason.

2. If its license for trading in cyberinformation security products and services is lost or damaged, an enterprise shall send a written request for re-grant, clearly stating the reason, to the Ministry of Information and Communications. Within 5 working days after receiving the request, the Ministry of Information and Communications shall consider it and re-grant a license to the enterprise.

3. An enterprise that does not violate the law on trading in cyberinformation security products and services may have its license for trading in cyberinformation security products and services extended once for no more

than one year. A dossier for license extension shall be sent to the Ministry of Information and Communications at least 60 days before the license expires, and made in two sets, each comprising:

a/ A written request for license extension;

b/ The license for trading in cyberinformation security products and services which remains valid;

c/ A report on the enterprise's operation over the latest 2 years.

Within 20 days after receiving a complete dossier, the Ministry of Information and Communications shall appraise it, decide on license extension, and re-grant a license to the enterprise; if refusing to re-grant the license, it shall issue a written notice clearly stating the reason.

4. An enterprise shall be suspended from trading in cyberinformation security products and services for up to 6 months in the following cases:

a/ It provides services not stated in the license;

b/ It fails to satisfy one of the conditions mentioned in Article 42 of this Law;

c/ Other cases prescribed by law.

5. An enterprise will have its license for trading in cyberinformation security products and services revoked in the following cases:

a/ It fails to provide services within one year after being granted the license without a plausible reason;

b/ The license expires;

c/ It fails to remedy the problems mentioned in Clause 4 of this Article after the suspension period expires.

Article 46. Responsibilities of enterprises trading in cyberinformation security products and services

1. To manage dossiers and documents on technical solutions and technologies of products.

2. To establish, store and secure customer information.

3. To report to the Ministry of Information and Communications on the trading in and export and import of cyberinformation security products and services before December 31 every year.

4. To refuse to provide cyberinformation security products and services when detecting organizations' or individuals' violations of the law on use of cyberinformation security products and services or violations of agreed commitments on use of products and services provided by the enterprises.

5. To suspend or stop providing cyberinformation security products and services in order to ensure national defense and security and social order and safety at the request of competent state agencies.

6. To coordinate with and create conditions for competent state agencies to take professional measures upon request.

Section 2

MANAGEMENT OF IMPORT OF CYBERINFORMATION SECURITY PRODUCTS

Article 47. Principles of management of import of cyberinformation security products

1. The import of cyberinformation security products shall be managed in accordance with this Law and other relevant laws.

2. The import of cyberinformation security products by agencies, organizations and individuals entitled to diplomatic privileges and immunities must comply with the customs law and the law on privileges and immunities for diplomatic representative missions, foreign consular offices and representative missions of inter-governmental international organizations in Vietnam.

3. In case Vietnam has no relevant technical regulations on cyberinformation security for imported cyberinformation security products, international agreements or treaties to which the Socialist Republic of Vietnam is a contracting party shall apply.

Article 48. Cyberinformation security products subject to import permit

1. To import cyberinformation security products on the Government-prescribed list of cyberinformation security products subject to import permit, an enterprise shall obtain a permit for import of cyberinformation security products from a competent state agency.

2. Before importing cyberinformation security products, organizations and enterprises must have them certified and announced as conformable with regulations under Article 39 of this Law.

3. An organization or enterprise shall be granted a permit for import of cyberinformation security products when fully meeting the following conditions:

a/ Possessing a license for trading in cyberinformation security products;

b/ Having cyberinformation security products certified and announced as conformable with regulations under Article 39 of this Law;

c/ Ensuring that users and use purposes of cyberinformation security products do not harm national defense and security or social order and safety.

4. The Ministry of Information and Communications shall prescribe in detail the order, procedures and dossier for grant of a permit for import of cyberinformation security products.

Chapter VI

DEVELOPMENT OF HUMAN RESOURCES FOR CYBERINFORMATION SECURITY

Article 49. Professional training in cyberinformation security

1. The managing body of an information system shall provide training in cyberinformation security knowledge and skills for managerial and technical staff members.

2. Full-time cyberinformation security officers shall be assigned with, and assisted in performing, tasks relevant to their professional qualifications, and prioritized in attending cyberinformation security refresher training.

3. The State shall encourage organizations and individuals to invest in, and enter into joint venture and association with other organizations in building, higher education institutions and vocational training institutions with a view to training human resources for cyberinformation security.

4. The Ministry of Home Affairs shall assume the prime responsibility for, and coordinate with the Ministry of Information and Communications and related ministries and sectors in, planning and organizing training in cyberinformation security knowledge and operations for cadres, civil servants and public employees.

Article 50. Cyberinformation security diplomas and certificates

1. Higher education institutions and vocational training institutions may grant cyberinformation security diplomas and certificates within the ambit of their tasks and powers.

2. The Ministry of Education and Training shall assume the prime responsibility for, and coordinate with the Ministry of Information and Communications and related ministries and sectors in, recognizing diplomas of higher education in cyberinformation security granted by foreign organizations.

3. The Ministry of Labor, War Invalids and Social Affairs shall assume the prime responsibility for, and coordinate with the Ministry of Information and Communications and related ministries and sectors in, recognizing diplomas and certificates of vocational training in cyberinformation security granted by foreign organizations.

Chapter VII

STATE MANAGEMENT OF CYBERINFORMATION SECURITY

Article 51. Contents of state management of cyberinformation security

1. Formulating strategies, master plans, plans and policies on cyberinformation security; formulating, and directing the implementation of, the national program on cyberinformation security.

2. Promulgating, and organizing the implementation of, legal documents on cyberinformation security; developing and announcing national standards and promulgating technical regulations on cyberinformation security.

3. Performing the state management of civil cryptography.

4. Managing the assessment and announcement of conformity with standards or technical regulations on cyberinformation security.

5. Managing security supervision of information systems.

6. Appraising cyberinformation security-related contents in design dossiers of information systems.

7. Disseminating the law on cyberinformation security.

8. Managing the trading in cyberinformation security products and services.

9. Organizing research and application of cyberinformation security science and technology; developing human resources for cyberinformation security; training full-time cyberinformation security officers.

10. Conducting examination and inspection, settling complaints and denunciations, and handling violations of the law on cyberinformation security.

11. Entering into international cooperation on cyberinformation security.

Article 52. Responsibilities for state management of cyberinformation security

1. The Government shall uniformly perform the state management of cyberinformation security.

2. The Ministry of Information and Communications shall take responsibility before the Government for performing the state management of cyberinformation security, having the following tasks and powers:

a/ To promulgate or formulate and submit to competent authorities for promulgation legal documents, strategies, master plans, plans, national standards and national technical regulations on cyberinformation security;

b/ To appraise cyberinformation security-related contents in design dossiers of information systems;

c/ To manage security supervision of information systems nationwide, except information systems mentioned at Point c, Clause 3, and Point b, Clause 5, of this Article;

d/ To manage cyberinformation security assessment;

dd/ To grant licenses for trading in cyberinformation security products and services and permits for import of information security products, except civil cryptographic products and services;

e/ To research and apply cyberinformation security science and technology; to train and develop human resources;

g/ To manage and carry out international cooperation on cyberinformation security;

h/ To conduct examination and inspection, settle complaints and denunciations, and handle violations of the law on cyberinformation security;

i/ To assume the prime responsibility for, and coordinate with related ministries, sectors, provincial-level People's Committees and enterprises in, ensuring cyberinformation security;

i/ To disseminate the law on cyberinformation security;

l/ To annually report on cyberinformation security activities to the Government.

3. The Ministry of National Defense has the following tasks and powers:

a/ To promulgate or formulate and submit to competent authorities for promulgation legal documents, strategies, master plans, plans, national standards and national technical regulations on cyberinformation security in the fields under its management;

b/ To conduct examination and inspection, settle complaints and denunciations, and handle violations in cyberinformation security assurance activities in the fields under its management;

c/ To manage security supervision of its information systems.

4. The Government Cipher Committee shall assist the Minister of National Defense in performing the state management of civil cryptography, having the following tasks:

a/ To formulate and submit to competent authorities for promulgation legal documents on management of civil cryptography;

b/ To assume the prime responsibility for, and coordinate with related ministries and sectors in, formulating and submitting to competent state agencies for promulgation national standards and national technical regulations on civil cryptographic products and services;

c/ To manage the trading in and use of civil cryptography; to manage the quality of civil cryptographic products and services; to manage the assessment and announcement of standard or regulation conformity for civil cryptographic products and services;

d/ To formulate and submit to competent authorities for promulgation a list of civil cryptography products and services and a list of civil cryptographic products subject to export and import permit;

dd/ To grant licenses for trading in civil cryptographic products and services and permits for export and import of civil cryptography products;

e/ To conduct examination and inspection, settle complaints and denunciations, and handle violations in the trading in and use of civil cryptography;

g/ To enter into international cooperation on civil cryptography.

5. The Ministry of Public Security has the following tasks and powers:

a/ To assume the prime responsibility for, and coordinate with related ministries and sectors in, formulating and submitting to competent authorities for promulgation, or promulgate according to its competence and guide the implementation of legal documents on protection of state secrets, prevention and combat of cybercrime and abuse of cyberspace to infringe upon national security or social order and safety;

b/ To manage security supervision of its information systems;

c/ To organize and direct the crime prevention and combat, and organize investigation of cybercrimes and other violations in the field of cyberinformation security;

d/ To coordinate with the Ministry of Information and Communications and related ministries and sectors in examining and inspecting cyberinformation security and handling violations of the law on cyberinformation security within its competence.

6. The Ministry of Home Affairs shall organize training in cyberinformation security knowledge and skills for cadres, civil servants and public employees.

7. The Ministry of Education and Training shall organize training in and dissemination of cyberinformation security knowledge in higher education institutions.

8. The Ministry of Labor, War Invalids and Social Affairs shall organize training in and dissemination of cyberinformation security knowledge in vocational training institutions.

9. The Ministry of Finance shall provide guidance on and allocate funds for performance of cyberinformation security assurance tasks in accordance with law.

10. Ministries and ministerial-level agencies shall, within the ambit of their tasks and powers, manage cyberinformation security of their own networks and

coordinate with the Ministry of Information and Communications in performing the state management of cyberinformation security.

11. Provincial-level People's Committees shall, within the ambit of their tasks and powers, perform the state management of cyberinformation security in localities.

Chapter VIII

IMPLEMENTATION PROVISIONS

Article 53. Effect

This Law takes effect on July 1, 2016.

Article 54. Detailing provision

The Government and competent state agencies shall detail the articles and clauses in the Law as assigned.

This Law was passed on November 19, 2015, by the XIIIth National Assembly of the Socialist Republic of Vietnam at its 10th session.-

Chairman of the National Assembly
NGUYEN SINH HUNG