사이버정보 보안에 관한 법률

국 가	베트남
원 법 률 명	Law on Cyberinformation Security
제 정	2015.11.15 86/2015/QH13
수 록 자 료	사이버정보 보안에 관한 법률, pp.1-39
발 행 사 항	전남 : 행정안전부 개인정보보호 국제협력센터, 2019

Law on Cyberinformation Security
(사이버정보 보안에 관한 법률)

※ 해당 법률 및 한국어 번역 자료는 참고 사항이며, 해당 내용 혹은 이를 사용하여 발생한 결과에 대하여 한국인터넷진흥원은 책임이 없음을 알려드립니다.
※ 오류 등 의견이 있으실 경우 iprivacy@kisa.or.kr로 보내 주시면 검토하여 반영하겠습니다.

영어	한국어
THE NATIONAL ASSEMBLY No. 86/2015/QH13 Law on Cyberinformation Security Pursuant to the Constitution of the Socialist Republic of Vietnam; The National Assembly promulgates the Law on Cyberinformation Security	베트남국회 제86/2015/QH13호 사이버정보 보안에 관한 법률 베트남사회주의공화국 국회는 베트남사회주의공화국 헌법에 의거하여 “사이버정보 보안에 관한 법률”을 공표한다.
Chapter I GENERAL PROVISIONS	제1장 총칙
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.	제1조 범위 본 법률은 사이버정보 보안의 보장; 민간 암호화; 사이버정보 보안에 관한 표준 및 기술 규정; 사이버정보 보안 분야의 거래; 사이버정보 보안을 위한 인적자원 개발; 및 국가 사이버정보 보안 관리와 관련하여 개인, 조직 및 기관의 사이버정보 보안 활동 및 권리와 책임을 규정한다.
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.	제2조 적용대상 본 법률은 국내에서의 사이버정보 보안 활동에 직접적으로 관여하거나 또는 연관이 있는 국내의 기관, 조직 및 개인 그리고 외국의 조직 및 개인에게 적용된다.
Article3.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	제3조 용어의 정의 본 법률의 해석에 있어, 각 용어는 아래와 같은 의미를 갖는다: 1. 사이버정보 보안이란 불법적인 열람, 활용, 공개, 방해, 변조 또는 파괴부터 사이버공간의 정보 및 정보시스템을 보호함으로써, 정보의 무결성, 기밀성 및 가용성을 유지함을 의미한다.

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.	2. 사이버공간이란 전기통신네트워크 및 컴퓨터네트워크를 통하여 정보가 제공, 전송, 수집, 처리, 저장 및 교환되는 환경을 의미한다.
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.	3. 정보시스템이란 사이버공간에서 정보를 생산, 제공, 전송, 수집, 처리, 저장 및 교환하기 위한 하드웨어, 소프트웨어 및 데이터베이스의 결합을 의미한다.
4. National important information system means an information system which, when being sabotaged, will cause extremely serious harms to national defense and security.	4. 국가 중요 정보시스템이란 파괴 대상이 될 경우, 국가 안보와 보안을 심각하게 저해할 수 있는 정보시스템을 의미한다.
5. Managing body of an information system means an agency, organization or individual competent to directly manage an information system.	5. 정보시스템 관리 주체란 정보시스템을 직접적으로 관리하는 기관, 조직 또는 개인을 의미한다.
6. Infringement upon cyberinformation security means an act of illegally accessing, utilizing, disclosing, interrupting, altering or sabotaging information or information systems.	6. 사이버정보 보안침해란 정보 또는 정보시스템에 불법적으로 접속, 활용, 공개, 방해, 변조 또는 파괴하는 행위를 의미한다.
7. Cyberinformation security incident means an incident that harms information or an information system, affecting the integrity, confidentiality or usability of information.	7. 사이버정보 보안 사고란 정보의 무결성, 기밀성 또는 가용성에 악영향을 유발함으로써, 정보 또는 정보시스템을 훼손하는 사고를 의미한다.
8. Cyberinformation security risk means a subjective factor or an objective factor that is likely to affect the status of cyberinformation security.	8. 사이버정보 보안위험이란 사이버정보 보안에 악영향을 미칠 소지가 있는 주관적 요인 또는 객관적 요인을 의미한다.
9. Cyberinformation security risk assessment means the detection, analysis and estimation of levels of harm and threats to information or information systems.	9. 사이버정보 위험평가란 정보 또는 정보시스템에 대한 훼손 및 훼손위협 수준을 탐지, 분석 및 평가하는 것을 의미한다.
10. Cyberinformation security risk management means the introduction of measures to minimize cyberinformation security risks.	10. 사이버정보 보안 위험관리란 사이버정보 보안 위험을 최소화하기 위한 조치의 도입을 의미한다.
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	11. 악성 소프트웨어(맬웨어)란 정보시스템의 일부 또는 전부가 비정상적으로 작동하도록 유발하거나, 그러한 정보시스템에 저장된 정보를 불법적으로 복제, 변조 또는 삭제할 수 있는 소프트웨어를 의미한다.

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 personalinformation 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.	12. 맬웨어 필터링 시스템이란 맬웨어를 탐지, 예방, 필터링하고 관련 통계를 수집하도록 네트워크에 연결된 하드웨어와 소프트웨어의 결합을 의미한다. 13. 전자주소란 전자우편주소, 전화번호, 인터넷 주소 및 기타 유사한 형태의 주소 등 사이버공간에서 정보를 발신 및 수신하는데 이용되는 주소를 의미한다. 14. 정보 관련 분쟁이란 복수의 국내외 조직이 통신기술 또는 기술적 조치를 이용하여 사이버공간에서 정보 또는 정보시스템을 훼손하는 것을 의미한다. 15. 개인정보란 특정 개인의 신원과 관련된 정보를 의미한다. 16. 개인정보 소유자란 그러한 정보를 기반으로 식별된 자를 의미한다. 17. 개인정보처리란 영리목적을 갖고 사이버공간에서 개인정보를 수집, 편집, 활용, 저장, 제공, 공유 또는 유포하는 행위를 의미한다. 18. 민간 암호화란 국가기밀로 분류되지 아니한 정보를 비밀로 유지하거나 인증하는데 사용되는 암호화 기법과 제품을 의미한다. 19. 사이버정보 보안 제품이란 정보 및 정보시스템을 보호하는 기능이 있는 하드웨어 또는 소프트웨어를 의미한다. 20. 사이버정보 보안 서비스란 정보 및 정보시스템을 보호하는 서비스를 의미한다.
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.	제4조 사이버정보 보안 기본원칙 1. 기관, 조직 및 개인은 사이버정보 보안을 보장해야 한다. 사이버정보 보안 활동은 관련 법률을 준수해야 하고, 국가 안보와 보안 및 국가기밀 보호를 보장하고, 정치적 안정 및 사회 질서와 안전을 유지하며, 또한 사회-경제적 발전을 도모해야 한다.

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.	2. 조직과 개인은 타인의 사이버정보 보안을 침해하지 않아야 한다. 3. 사이버정보 보안 사고에 대한 대응은 조직 및 개인의 법적 권리와 이익을 보장하고, 개인의 프라이버시, 사적 비밀 및 가족의 비밀 그리고 조직의 사적 정보를 침해하지 않아야 한다. 4. 사이버정보 보안 활동은 정기적이고 지속적이며 신속하고 효과적인 방식으로 수행되어야 한다.
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.	제5조 사이버정보 보안에 관한 국가정책 1. 정치적 안정과 사회-경제적 발전을 도모하며, 국가 안보와 보안 그리고 사회 질서와 안전을 보장할 수 있도록 사이버정보 보안을 위한 인적자원을 교육 및 개발하고, 사이버정보 보안기술 인프라를 구축한다. 2. 국산 사이버정보 보안 제품과 서비스를 위한 기술의 연구, 개발 및 응용을 장려하고, 수출을 지원하며, 시장 확대 방안을 마련한다. 국내에서 생산할 수 없거나 아직 국내에 도입되지 아니한 첨단 제품과 기술의 수입을 촉진한다. 3. 사이버정보 보안 제품과 서비스 시장의 공정한 경쟁 환경을 보장하고, 조직과 개인이 사이버정보 보안 제품과 서비스에 대한 투자, 연구, 개발 및 보급에 참여하도록 장려하며 적절한 여건을 조성한다. 4. 국가는 국가기관 및 국가 중요 정보시스템의 사이버정보 보안을 보장하기 위한 예산을 할당한다.
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	제6조 사이버정보 보안에 관한 국제협력 1. 사이버정보 보안에 관한 국제협력은 아래의 원칙을 준수해야 한다: a) 상대국의 독립과 자주, 그리고 영토를 존중하며, 내정에 간섭하지 않고, 평등과 호혜를 추구한다;

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.	b) 베트남의 법률과 베트남이 체결한 국제조약을 준수한다. 2. 사이버정보 보안에 관한 국제협력의 내용은 아래를 포함한다: a) 사이버정보 보안에 관한 과학, 기법 및 기술의 교육, 연구 및 응용 분야의 국제협력; b) 사이버정보 보안에 관한 법률 위반 행위의 예방 및 통제; 사이버정보 보안 사고에 대한 조사 및 대응, 그리고 테러를 목적으로 한 사이버공간 악용 예방 분야의 국제협력; c) 기타 사이버정보 보안에 관한 국제협력 활동.
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.	제7조 금지 행위 1. 사이버공간에서의 정보 전송 차단, 또는 사이버공간 정보에 대한 불법적인 방해, 열람, 훼손, 삭제, 변조, 복제 또는 위조하는 행위를 금지한다. 2. 정보시스템의 정상적인 작동 또는 사용자의 정보시스템 접근성에 불법적으로 악영향을 미치거나 방해하는 행위를 금지한다. 3. 정보시스템의 사이버정보 보안 보호조치를 불법적으로 공격하거나 무력화하는 행위; 정보시스템에 대한 공격이나 통제권 억제, 또는 파괴하는 행위를 금지한다. 4. 스팸 또는 맬웨어를 유포하는 행위, 또는 위/변조 정보시스템을 구축하는 행위를 금지한다. 5. 타인의 개인정보를 불법적으로 수집, 활용, 유포 또는 거래하는 행위; 개인정보를 수집하거나 부당하게 사용할 목적으로 정보시스템의 취약점을 악용하는 행위를 금지한다. 6. 기관, 조직 또는 개인의 암호화된 비밀 및 합법적으로 암호화된 정보를 해킹하는 행위; 민간 암호화 제품 제품에 관한 정보 또는 합법적으로 민간 암호화 제품을 사용하는 고객의 정보를 공개하는 행위; 출처가 불분명한 민간 암호화 제품을 사용하거나 거래하는 행위를 금지한다.
Article 8. Handling of violations of the law on cyberinformation security	제8조 사이버정보 보안에 관한 법률 위반자 처벌

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.	본 법률을 위반한 자는 그러한 위반의 성질과 정도에 따라 행정 처분 또는 형사 책임에 처해지며, 손해가 발생한 경우에는 법률에 따라 배상해야 한다.
Chapter II ASSURANCE OF CYBERINFORMATION SECURITY	제2장 사이버정보 보안의 보장
Section 1 CYBERINFORMATION PROTECTION	제1절 사이버정보 보호
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.	제9조 정보의 분류 1. 정보를 소유한 기관과 조직은 적절한 정보보호 대책을 강구하기 위하여 기밀성을 기준으로 정보를 분류해야 한다. 2. 국가기밀로 간주되는 정보는 국가 기밀 보호에 관한 법률에 따라 분류 및 보호되어야 한다. 각자의 업무 분야에서 기밀정보와 일반정보를 모두 사용하는 기관 및 조직은 정보처리에 관한 규정과 절차를 개발하고; 인가된 기밀정보 열람 이력을 기록하기 위한 범위와 방법을 결정해야 한다.
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	제10조 정보 발신 관리 1. 사이버공간으로 정보를 발신할 때, 아래의 요건을 준수해야 한다: a) 정보 발신자 원천을 위조하지 아니한다; b) 본 법률 및 기타 관련 법률을 준수한다. 2. 수신자가 법률에 따른 정보 수신 의무를 갖지 아니하는 한, 수신에 동의하지 않았거나 수신을 거부한 수신자의 전자주소로 상업적 정보를 발신하지 않아야 한다. 3. 정보를 발신하는 전기통신사업자, 전기통신응용서비스사업자 및 정보기술서비스사업자는: a) 개인의 개인정보 및 조직의 사적 정보 보유와 보호에 관한 법률을 준수한다; b) 불법 정보 발신에 관한 조직 또는 개인의 통보를 접수한 즉시, 적절한 차단 및 처리 조치를 시

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.	행한다; c) 수신자가 정보 수신 거부 여부를 선택할 수 있도록 한다; d) 사이버정보 보안을 관리 및 보장하는 관할 국가기관의 요청에 따라, 필요한 기술적, 전문적 여건을 제공한다.
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.	제11조 맬웨어 예방, 탐지, 차단 및 취급 1. 기관, 조직 및 개인은 관할 국가기관의 지도 또는 요청에 따라 맬웨어를 예방 및 차단해야 한다. 2. 국가 중요 정보시스템 관리 주체는 맬웨어를 예방, 탐지, 차단하고 신속하게 처리할 수 있도록 기술적이고 전문적인 시스템을 운용해야 한다. 3. 전자우편 서비스 또는 정보 전송 저장 서비스를 제공하는 사업자는 자사의 시스템을 통하여 정보를 발신, 수신 및 저장하는 과정 전반에 걸쳐 맬웨어 필터링 시스템을 운용하고, 관련 법률에 따라 관할 국가기관에게 보고서를 제출해야 한다. 4. 인터넷 서비스를 제공하는 사업자는 맬웨어를 관리, 예방, 삭제하고 맬웨어 확산을 차단하기 위한 조치를 시행하며, 관할 국가기관의 요청에 따라 이를 처리해야 한다. 5. 정보통신부는 주무기관으로서, 국방부, 공안부 및 기타 유관부처와 협조하여, 국가 안보와 보안에 악영향을 미치는 맬웨어를 예방, 탐지, 차단 및 처리할 책임을 진다.
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	제12조 전기 통신 자원의 보안 보장 1. 전기 통신 자원의 사용자는: a) 사용자의 주파수, 저장된 번호, 도메인 이름 및 인터넷 주소로부터 발생하는 사이버정보 위험을 예방하기 위한 관리적, 기술적 조치를 시행한다. b) 관할 국가기관에 협조하고, 그러한 기관의 요청에 따라 전기 통신 자원 보안에 관한 정보를 제공한다.

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.	 2. 인터넷에서 서비스를 제공하는 사업자는 자사의 인터넷 자원과 자사 고객으로부터 발생하는 사이버정보 위험을 관리 및 예방하고; 관할 국기가관의 요청에 따라 적절한 정보를 제공하며; 베트남 국가 도메인네임서버(DNS) 시스템의 안정적 운용을 위하여 연결 및 라우팅 업무에 협조해야 한다. 3. 정보통신부는 베트남 국가 도메인서버 시스템의 사이버정보 보안 상태를 보장해야 한다.
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.	제13조 사이버정보 보안 사고에 대한 대응 1. 사이버정보 보안 사고에 대한 대응이란 사이버 보안 위험을 일으키는 사고를 처리하고 피해를 구제하기 위한 활동을 의미한다. 2. 사이버정보 보안 사고에 대한 대응은 아래의 원칙을 준수해야 한다: a) 신속, 정확하고, 즉각적, 동시적이며 또한 효과적인 대응을 취한다; b) 사이버정보 보안 사고 대응 조율에 관한 법률을 준수한다; c) 국내외 기관, 조직 및 사업자 간 업무 협조를 보장한다. 3. 중앙부처, 정부산하기관, 성급인민위원회, 전기통신사업자 및 국가 중요 정보시스템 관리 주체는 사이버정보 보안 사고에 대응할 전담부서를 설치하거나 지정해야 한다. 4. 정보통신부는 국가차원의 사이버정보 보안 사고 대응을 조율하고, 사이버정보 보안 사고대응 조율에 관한 세칙을 제정해야 한다.
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	제14조 국가 사이버정보 보안 보장을 위한 긴급 대응 1. 국가 사이버정보 보안 보장을 위한 긴급 대응이란 국가 재난 사태 발생 시, 또는 관할 국가기관의 요청에 따라, 국가 사이버정보 보안을 보장

request of competent state agencies with a view to ensuring national cyberinformation security.	하기 위하여 수행하는 사고 대응 활동을 의미한다.
2. Emergency response to ensure national cyberinformation security must adhere to the following principles:	2. 국가 사이버정보 보안 보장을 위한 긴급 대응은 아래의 원칙을 준수해야 한다:
a/ Organizing response according to decentralized competence;	a) 분산된 역량에 따라 대응 조치를 기획한다;
b/ Conducting response on the spot, rapidly, strictly and with close coordination;	b) 긴밀한 협조를 바탕으로, 현장에서 신속하고 엄격한 대응 조치를 수행한다.
c/ Applying effective and feasible technical measures.	c) 효과적이고 실행 가능한 기술적 조치를 적용한다.
3. Emergency response plans to ensure national cyberinformation security include:	3. 국가 사이버정보 보안 보장을 위한 비상 대응 계획은 아래를 포함한다:
a/ Emergency response plan to ensure national cyberinformation security;	a) 국가 사이버정보 보안을 보장하기 위한 비상 대응 계획;
b/ Emergency response plan to ensure cyberinformation security for state agencies, political organizations and socio-political organizations;	b) 국가기관, 정치조직 및 사회-정치단체의 사이버정보 보안을 보장하기 위한 비상 대응 계획;
c/ Emergency response plan to ensure cyberinformation security for localities;	c) 지방자치단체의 사이버정보 보안을 보장하기 위한 비상 대응 계획;
d/ Emergency response plan to ensure cyberinformation security for telecommunications enterprises.	d) 전기통신사업자의 사이버정보 보안을 보장하기 위한 비상 대응 계획.
4. Responsibilities to ensure national cyberinformation security are prescribed as follows:	4. 국가 사이버정보 보안을 보장하기 위한 책임은 아래와 같다:
a/ The Prime Minister shall decide on emergency response plans to ensure national cyberinformation security;	a) 총리는 국가 사이버정보 보안을 보장하기 위한 비상 대응 계획을 결정해야 한다;
b/ The Ministry of Information and Communications shall coordinate emergency response to ensure national cyberinformation security;	b) 정보통신부는 국가 사이버정보 보안을 보장하기 위한 비상 대응을 조율한다;
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;	c) 중앙부처, 각급 인민위원회, 유관기관 및 조직은 부여 받은 책무와 권한 내에서 국가 사이버정보 보안을 보장하기 위한 비상 대응 활동을 조율 및 지시한다.
d/ Telecommunications enterprises shall take emergency response measures and coordinate with the Ministry of Information and Communications and related ministries, sectors	d) 전기통신사업자는 국가 사이버정보 보안을 보장하기 위한 비상 대응 조치를 시행하고, 정보통신부, 유관부처, 및 각급 인민위원회와 협조한다.

and People's Committees at all levels in ensuring national cyberinformation security.	
Article 15. Responsibilities of agencies, organizations and individuals in ensuring cyberinformation security	제15조 사이버정보 보안 보장에 관한 기관, 조직 및 개인의 책임
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.	1. 사이버정보 보안 활동에 관여된 기관, 조직 및 개인은 사이버정보 보안을 보장하는 관할 국가기관, 기타 조직 및 개인의 활동에 협조해야 한다.
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.	2. 사이버공간에서 서비스를 이용하는 기관, 조직 및 개인은 사이버정보 보안을 파괴하는 행위 또는 사이버정보 보안 사고 발생 사실을 서비스 제공 사업자 또는 사고 대응 전담조직에게 즉시 통보해야 한다.
Section 2 PROTECTION OF PERSONAL INFORMATION	제2절 개인정보 보호
Article 16. Principles of protecting personal information in cyberspace	제16조 사이버공간에서의 개인정보보호 원칙
1. Individuals shall themselves protect their personal information and comply with the law on provision of personal information when using services in cyberspace.	1. 개인은 사이버공간에서 서비스를 이용함에 있어, 자신의 개인정보를 스스로 보호하고 개인정보 제공에 관한 법률을 준수해야 한다.
2. Agencies, organizations and individuals that process personal information shall ensure cyberinformation security for the information they process.	2. 개인정보를 처리하는 기관, 조직 및 개인은 처리대상 정보의 사이버정보 보안을 보장해야 한다.
3. Organizations and individuals that process personal information shall develop and publicize their own measures to process and protect personal information.	3. 개인정보를 처리하는 조직 및 개인은 개인정보를 처리하고 보호하기 위한 자체 대책을 개발 및 공표해야 한다.
4. The protection of personal information must comply with this Law and other relevant laws.	4. 개인정보보호는 본 법률 및 기타 관련 법률에 의거하여 수행되어야 한다.
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.	5. 비영리 목적 또는 국가 안보와 보안 및 사회 질서와 안전을 보장하기 위한 목적의 개인정보 처리는 여타 관련 법률에 의거하여 수행되어야 한다.
Article 17. Collection and use of personal information	제17조 개인정보의 수집 및 이용
1. Organizations and individuals that process personal information shall:	1. 개인정보를 처리하는 조직 및 개인은:
a/ Collect personal information only after obtaining the consent of its owners regarding the	a) 개인정보 소유자의 동의를 얻은 이후에만, 그러한 정보의 수집 및 이용 범위와 목적에 따라 개인

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.	정보를 수집한다; b) 개인정보 소유자의 동의를 얻은 이후에만, 개인정보 소유자가 당초에 동의하였던 목적 이외의 용도로 수집된 개인정보를 이용할 수 있다; c) 개인정보 소유자의 동의를 얻거나 관할 국가기관이 요청하지 않는 한, 개인정보를 처리하는 조직 또는 개인이 수집, 열람, 또는 통제하는 개인정보를 제3자에게 제공, 공유 또는 유포하지 않는다. 2. 국가기관은 수집한 개인정보를 안전하게 저장해야 한다. 3. 개인정보 소유자는 개인정보를 처리하는 조직 및 개인에게 그러한 조직 및 개인이 수집 및 저장한 자신의 개인정보를 제공하도록 요청할 수 있다.
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	제18조 개인정보의 갱신, 변경 및 폐기 1. 개인정보 소유자는 개인정보를 처리하는 조직 및 개인에게 그러한 조직 및 개인이 수집 및 저장한 자신의 개인정보를 갱신, 변경 또는 폐기하거나, 그러한 개인정보의 제3자 제공을 중지하도록 요청 할 수 있다. 2. 개인정보 소유자가 자신의 개인정보를 갱신, 변경 또는 폐기하도록 요구하거나 그러한 개인정보의 제3자 제공을 중지하도록 요청한 경우, 개인정보를 처리하는 조직 또는 개인은: a) 개인정보 소유자의 요청을 따르고, 개인정보 소유자에게 그러한 개인정보가 갱신, 변경 또는 폐기되었음을 통보하거나, 갱신, 변경 또는 폐기된 개인정보를 직접 확인할 수 있는 권한을 부여한다; b) 개인정보를 보호하기 위하여 적절한 조치를 시행하고, 만약 기술적 사유 또는 여타 사유로 인하여 그러한 요청을 따를 수 없는 경우, 개인정소유자에게 통보한다. 3. 법률에 달리 규정되지 않는 한, 이용 목적을 달성하였거나 보유기간이 만료된 경우, 개인정보를

use purposes or the storage time has expired and notify such to the owners of such personal information, unless otherwise prescribed by law.	처리하는 조직 및 개인은 저장된 개인정보를 삭제하고, 그러한 개인정보의 소유자에게 삭제 사실을 통보해야 한다.
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.	제19조 사이버공간에서의 개인정보 보안 보장 1. 개인정보를 처리하는 조직 및 개인은 수집 및 저장한 개인정보를 보호하기 위하여 적절한 관리적, 기술적 조치를 시행하고, 사이버정보 보안 보장에 관한 표준 및 기술 규정을 준수해야 한다. 2. 사이버정보 보안 사고가 발생하거나 그러한 사고발생 위협이 있는 경우, 개인정보를 처리하는 조직 및 개인은 가능한 신속하게 적절한 구제 및 차단조치를 시행해야 한다.
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.	제20조 사이버공간에서의 개인정보보호를 관리하는 국가기관의 책임 1. 사이버공간에서의 개인정보 보안 보장과 관련된 일반시민의 진정 및 신고를 접수할 수 있는 온라인정보채널을 구축한다. 2. 개인정보를 처리하는 조직 및 개인을 매년 점검 및 평가하고, 필요한 때마다 특별점검 및 평가를 수행한다.
Section 3 PROTECTION OF INFORMATION SYSTEMS	제3절 정보시스템의 보호
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	제21조 정보시스템 보안 등급의 분류 1. 정보시스템 보안 등급분류란 정보시스템을 보호하는 관리적, 기술적 대책을 기준으로 하여, 1등급부터 5등급까지 오름차순으로 정보시스템의 정보 보안 수준을 결정하는 것을 의미한다. 2. 아래의 기준에 따라 정보시스템의 보안 등급을 분류한다: a) 1등급: 정보시스템이 파괴된 경우, 조직 또는 개인의 합법적 권리와 이익을 저해하지만, 공익, 사회 질서와 안전 또는 국가 안보와 보안을 저해

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.	하지 않는다; b) 2등급: 정보시스템이 파괴된 경우, 조직 또는 개인의 합법적 권리와 이익을 심각하게 저해하거나 공익을 저해하지만, 사회 질서와 안전 또는 국가 안보와 보안을 저해하지 않는다; c) 3등급: 정보시스템이 파괴된 경우, 생산, 공익 및 사회 질서와 안전을 심각하게 저해하거나, 국가 안보와 보안을 저해한다; d) 4등급: 정보시스템이 파괴된 경우, 공익 및 사회 질서와 안전을 매우 심각하게 저해하거나, 국가 안보와 보안을 심각하게 저해한다; dd) 5등급: 정보시스템이 파괴된 경우, 국가 안보와 보안을 매우 심각하게 저해한다. 3. 정부는 정보시스템보안 등급 결정을 위한 세부 기준, 역량, 순서 및 절차, 그리고 각 등급별 정보시스템의 보안 보장 책임을 정해야 한다.
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.	제22조 정보시스템 보호 책무 1. 정보시스템의 보안 등급을 결정한다. 2. 정보시스템에 대한 보안위험을 평가 및 관리한다. 3. 정보시스템 보호대책을 요구, 감독 및 평가한다. 4. 정보시스템을 보호하기 위한 조치를 시행한다. 5. 보고체계를 준수한다. 6. 사이버정보 보안의식을 제고하기 위한 홍보 활동을 수행한다.
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.	제23조 정보시스템 보호조치 1. 정보시스템을 설계, 개발, 관리, 운용, 이용, 업그레이드 또는 폐기함에 있어, 사이버정보 보안을 보장하는 규정을 공표한다.

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.	2. 사이버정보 보안 사고 위험을 예방 및 차단하고 사고 피해를 구제하기 위하여, 사이버정보 보안 보장에 관한 표준 및 기술 규정에 따른 관리적, 기술적 조치를 시행한다. 3. 규정 준수 상태를 점검 및 감독하고, 정보시스템에 적용된 관리적, 기술적 조치의 효과성을 평가한다. 4. 정보시스템의 보안 상태를 감독 한다.
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.	제24조 정보시스템의 보안 관리 1. 정보시스템 보안 감독이란 감독 대상을 결정하고, 그러한 대상의 정보현황을 수집 및 분석함으로써 그러한 정보시스템의 보안에 악영향을 미치는 요인을 식별하고; 사이버정보 보안침해 행위 또는 그러한 정보시스템에 대한 사이버정보 보안 사고 위협 행위를 보고 및 경고하며; 사이버정보 보안 상태에 악영향을 미치는 핵심 요인을 분석하고; 또한 기술적 조치 변경을 제안하는 활동을 의미한다. 2. 정보시스템 보안 감독 대상은 방화벽, 접속 통제, 중요 정보 경로, 중요 서버, 중요 장비 및 중요 터미널장비를 포함한다. 3. 전기통신사업자, 정보기술서비스사업자 및 사이버 정보 보안 서비스 사업자는 관할 국가기관의 요청에 따라 정보시스템의 보안 상태를 감독함에 있어, 정보시스템 관리 주체와 협조한다.
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	제25조 정보시스템 관리 주체의 책임 1. 정보시스템 관리 주체는 본 법률 제22조, 제23조 및 제24조에 의거하여 정보시스템을 보호해야 한다. 2. 국가지원금을 받는 정보시스템 관리 주체는 본조 1항에 명시된 책임을 이행하고, 또한: a) 정보시스템을 구축, 확장 또는 업그레이드 할

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.	경우, 관할 국가기관이 사이버정보 보안 상태를 심사할 수 있도록 계획을 수립한다; b) 사이버정보 보안업무를 주관하는 인원 또는 부서를 지정한다.
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.	제26조 국가 중요 정보시스템 1. 국가 중요 정보시스템을 구축, 확장 또는 업그레이드 한 경우, 그러한 시스템을 운영하여 시스템이 공격에 노출되기 전에, 정보 보안 상태를 점검해야 한다. 2. 정보통신부는 주무기관으로서, 국방부, 공안부 및 기타 유관부처와 협조하여, 공표권자인 총리에게 제출할 국가 중요 정보시스템 목록을 작성할 책임을 진다.
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	제27조 국가 중요 정보시스템의 사이버정보 보안 보장 책임 1. 국가 중요 정보시스템 관리 주체는: a) 본 법률 제25조 2항의 규정을 준수한다; b) 관할 국가기관이 지정한 전문기관을 통하여 사이버정보 보안위험을 평가한다; c) 예비 정보시스템을 마련한다; d) 국가 중요 정보시스템 보호에 관한 훈련을 계획 및 실시한다. 2. 정보통신부는: a) 본 조 3항 및 4항에 규정된 바를 제외하고, 주무기관으로서, 국가 중요 정보시스템 관리 주체, 공안부 및 기타 유관부처와 협조하여, 국가 중요 정보시스템의 사이버정보 보안 보호 활동을 지도, 촉구, 점검 및 평가할 책임을 진다; b) 전기통신사업자, 정보기술서비스사업자 및 사이버정보 보안서비스사업자가 기술 자문 및 기술 지

services and enterprises providing cyberinformation security services to provide technical advice and assistance and respond to cyberinformation security incidents for national important information systems.	원을 제공하고, 국가 중요 정보시스템 사이버정보 보안 사고 발생 시, 대응 조치를 취하도록 요청한다.
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.	3. 공안부는 공안부 관리하에 있는 국가 중요 정보시스템의 사이버정보 보안 보호 활동을 지도, 촉구, 점검 및 평가하고; 관할 국가기관의 요청에 따라, 정보통신부, 국가 중요 정보시스템 관리 주체, 유관부처 및 각급 인민위원회와 협조하여, 국가 중요 정보시스템을 보호한다.
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.	4. 국방부는 국방부가 관리 하에 있는 국가 중요 정보시스템의 사이버정보 보안 보호 활동을 지도, 촉구, 점검 및 평가한다.
5. The Government CipherCommittee 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.	5. 정부암호위원회는 국가기관, 정치조직 및 사회-경제단체의 국가 중요 정보시스템에서 정보를 보호하기 위한 암호체계를 기획하고; 국가 중요 정보시스템 관리 주체와 협조하여 관련 법률에 따른 사이버정보 보안 감독 활동을 수행한다.
Section 4 STOPPAGE OF INFORMATION-RELATED CONFLICTS IN CYBERSPACE	제4절 사이버공간 정보 관련 분쟁 대처
Article 28. Responsibilities of organizations and individuals for stopping information-related conflicts in cyberspace	제28조 사이버공간 정보 관련 분쟁에 대처하기 위한 조직 및 개인의 책임
1. Within the ambit of their tasks and powers, organizations and individuals shall:	1. 부여 받은 책무와 권한 내에서, 조직 및 개인은:
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;	a) 자신의 정보시스템에서 발생한 정보 파괴를 차단하고; 국내외 조직 및 개인의 정보시스템을 통하여 수행된 사이버 공격의 원천을 식별하고, 그러한 사이버 공격을 격퇴하며, 또한 사이버 공격으로 인하여 발생한 피해를 구제하는데 상호 협력한다;
b/ Stop acts of domestic and foreign organizations and individuals that aim to sabotage	b) 정보 네트워크 무결성을 파괴하려는 국내외 조직 및 개인의 행위를 차단한다;

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.	c) 국가 안보와 보안 또는 사회 질서와 안전에 심각한 악영향을 초래하는 국내외 조직 및 개인의 사이버공간 불법 활동을 차단한다. 2. 정부는 사이버공간에서의 정보 관련 분쟁에 대처하기 위한 세칙을 제정해야 한다.
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 web sites 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.	제29조 테러 목적의 사이버공간 악용 차단 1. 사이버공간이 테러 목적으로 악용되는 것을 차단하기 위하여 아래와 같은 조치를 시행한다: a) 테러 행위에 악용되는 인터넷 원천을 무력화한다; b) 테러 행위를 위하여 인터넷을 악용하는 신호, 인자, 수단 및 방법에 관한 정보, 그리고 테러조직의 목표 및 운영에 관한 정보의 공유 및 확산을 차단한다. c) 테러에 악용되는 인터넷 원천의 통제, 테러 목적 웹사이트 콘텐츠의 검색 및 통제에 관한 경험과 기법을 공유한다. 2. 정부는 본 조 1항에 명시된 테러 목적의 사이버공간 악용을 차단하기 위하여, 책임과 조치를 명시한 세칙을 제정해야 한다.
Chapter III CIVIL CRYPTOGRAPHY	제3장 민간 암호화
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.	제30조 민간 암호화 제품 및 서비스 1. 민간 암호화 제품은 국가기밀로 분류되지 아니한 정보를 보호하는데 이용되는 암호화 문서 및 기술적, 전문적 장비를 포함한다. 2. 민간 암호화 서비스는 민간 암호화 제품을 이용한 정보보호 서비스; 민간 암호화 제품에 관한 점검 및 평가; 그리고 민간 암호화 제품을 이용한 사이버정보 기밀성과 보안성 유지에 관한 상담을 포함한다.
Article 31. Trading in civil cryptographic products and services 1. An enterprise that wishes to trade in civil	제31조 민간 암호화 제품 및 서비스의 거래 1. 민간 암호화 제품 서비스목록에 등재된 민간

cryptographic products and services on the list of civil cryptographic products and services shall obtain a license for doing so.	암호화 제품 및 서비스를 거래하고자 하는 사업자는 그러한 제품 또는 서비스를 거래하는데 필요한 면허를 취득해야 한다.
2. An enterprise shall be granted a license for trading in civil cryptographic products and services when fully meeting the following conditions:	2. 민간 암호화 제품 서비스 거래 면허 증서는 아래의 모든 조건에 부합하는 사업자에게 교부된다:
a/ Having managerial, administration and technical staff members who meet professional requirements on information confidentiality and security;	a) 정보 기밀성과 보안성에 관한 전문적 요건을 준수하는데 필요한 경영직, 관리직 및 기술직 인력을 보유하고 있다;
b/ Having equipment and physical foundations suitable to the scale of provision of civil cryptographic products and services;	b) 민간 암호화 제품 및 서비스 제공 규모에 적합한 장비와 물적 토대를 보유하고 있다;
c/ Having a technical plan conformable with standards and technical regulations;	c) 관련 표준 및 기술 규정에 부합하는 기술 계획서를 보유하고 있다;
d/ Having a cyberinformation confidentiality and security plan in the course of management and provision of civil cryptographic products and services;	d) 민간 암호화 제품 및 서비스의 관리와 제공과정에서 사이버정보의 기밀성 및 보안성을 유지하기 위한 계획서를 보유하고 있다;
dd/ Having an appropriate business plan.	dd) 적절한 사업 계획서를 보유하고 있다.
3. Civil cryptographic products shall be inspected and certified as conformable with regulations before being marketed.	3. 민간 암호화 제품은 시판 전에, 관련 규정에 따른 점검 및 인증을 받아야 한다.
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.	4. 민간 암호화 제품 서비스 거래 면허 증서를 취득하고자 하는 사업자는 비용 및 수수료에 관한 법률에 따라, 해당 수수료를 납부해야 한다.
5. The Government shall promulgate a list of civil cryptographic products and services and detail this Article.	5. 정부는 민간 암호화 제품 서비스 목록을 공표하고, 본 조에 따른 세칙을 제정해야 한다.
Article 32. Order and procedures for grant of licenses for trading in civil cryptographic products and services	제32조 민간 암호화 제품 서비스 거래 면허 증서의 교부 순서와 절차
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.	1. 민간 암호화 제품 서비스 거래 면허 증서를 신청하는 사업자는 신청 구비서류를 정부암호위원회에게 제출해야 한다.
2. A dossier of application for a license for trading in civil cryptographic products and services shall be made in two sets, each comprising:	2. 민간 암호화 제품 서비스 거래 면허 증서를 신청하는 사업자는 아래와 같은 문서로 구성된 구비서류를 각 2부씩 제출해야 한다:
a/ An application for a license for trading in civil	a) 민간 암호화 제품 서비스 거래 면허 신청서;

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.	b) 사업자등록증, 투자등록증 또는 그에 준하는 서류의 사본; c) 경영직, 관리직 및 기술직 인력이 소지한 정보 기밀성 및 보안성 분야 학위증서 또는 기타 증서의 사본; d) 제품의 기술적 특징과 사양; 제품과 관련된 표준 또는 기술 규정; 서비스 표준 및 품질; 기술적 조치 및 솔루션; 그리고 제품 보증 및 유지 보수 계획에 관한 서류로 구성된 기술 계획서; dd) 민간 암호화 제품 및 서비스의 관리와 제공과정에서 사이버정보의 기밀성 및 보안성을 유지하기 위한 계획서; e) 제품 및 서비스의 제공 범위와 사용자 범위; 제품 및 서비스의 규모와 수량, 고객 서비스 네트워크 및 기술 보증에 관한 사항을 명시한 사업 계획서. 3. 정부암호위원회는 구비서류를 수취한 날로부터 30일 이내에, 신청서를 심사하여 민간 암호화 제품 서비스 거래 면허 증서를 교부한다. 면허 증서 교부를 거부할 경우, 정부암호위원회는 사업자에게 구체적인 거부 사유를 서면으로 통보한다. 4. 민간 암호화 제품 서비스 거래 면허 증서는 발행일로부터 10년간 유효하다.
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	제33조 민간 암호화 제품 서비스 거래 면허 증서의 수정, 보충, 재교부, 연장, 정지 및 취소 1. 사업자가 상호 명을 변경하거나, 법적 대표자를 변경하거나, 또는 민간 암호화 제품 및 서비스를 변경하거나 추가할 경우, 민간 암호화 제품 서비스 거래 면허 증서를 수정 및 보충해야 한다. 사업자는 아래와 같은 문서로 구성된 수정보충요청 구비서류를 각 2부씩 정부암호위원회에게 제출해야 한다:

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.	a) 면허 증서 수정 보충 요청서; b) 사업자등록증, 투자등록증 또는 그에 준하는 서류의 사본; c) 기존에 교부 받은 민간 암호화 제품 서비스 거래 면허 증서; d) 사업자가 민간 암호화 제품 및 서비스, 또는 사업 분야를 추가하고자 할 경우, 추가될 제품 및 서비스와 관련하여, 본 법률 제32조 2항 d)호, dd)호 및 e)호에 명시된 기술계획서, 사이버정보 기밀성 및 보안성 유지 계획서, 사업 계획서; 정부암호위원회는 구비서류를 수취한 날로부터 10일 이내에, 요청서를 심사하여 기존 면허 증서를 수정 및 보충한 후 사업자에게 재교부한다. 면허 증서 재교부를 거부할 경우, 정부암호위원회는 사업자에게 구체적인 거부사유를 서면으로 통보한다.
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.	2. 민간 암호화 제품 서비스 거래 면허 증서를 분실하거나 면허 증서가 훼손된 경우, 사업자는 재발급 사유를 명시한, 재교부요청서를 정부암호위원회에게 제출해야 한다. 정부암호위원회는 그러한 요청을 수취한 날로부터 5일 이내에, 요청서를 검토하여 사업자에게 면허 증서를 재교부한다.
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	3. 민간 암호화 제품 서비스 거래에 관한 법률을 위반하지 아니한 사업자는 민간 암호화 제품 서비스 거래 면허 증서의 유효기간을 1회에 한 하여, 1년 이하의 기간으로 연장할 수 있다. 사업자는 아래와 같은 문서로 구성된 연장요청 구비서류를 각 2부씩, 면허 증서 만료일로부터 60일 이전까지 정부암호위원회에게 제출해야 한다: a) 면허 증서 연장 요청서; b) 유효기간이 만료되지 아니한 민간 암호화 제품 서비스 거래 면허 증서; c) 사업자의 최근 2년간 운영 보고서.

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.	정부암호위원회는 구비서류를 수취한 날로부터 20일 이내에, 요청서를 심사하여 기존 면허 증서를 연장한 후 사업자에게 재교부한다. 면허 증서 연장을 거부할 경우, 정부암호위원회는 사업자에게 구체적인 거부사유를 서면으로 통보한다.
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.	4. 아래 각 호의 사유가 발생한 경우, 사업자의 민간 암호화 제품 서비스 거래 면허 증서는 최장 6개월까지 정지된다: a) 사업자가 면허 증서에 명시되지 아니한 제품 및 서비스를 제공한 경우; b) 사업자가 본 법률 제31조 2항에 명시된 조건을 충족하지 못한 경우; c) 기타 법률에서 정한 정지사유가 발생한 경우.
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.	5. 아래 각 호의 사유가 발생한 경우, 사업자의 민간 암호화 제품 서비스 거래 면허 증서는 취소된다: a) 사업자가 정당한 사유 없이, 면허 증서 교부일로부터 1년 이내에 서비스를 제공하지 아니할 경우; b) 면허 증서가 만료된 경우; c) 정지기간이 경과한 이후에도, 사업자가 본 조 4항에 명시된 문제를 해결하지 못한 경우.
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.	제34조 민간 암호화 제품의 수출입 1. 수출입 허가 대상 민간 암호화 제품 목록에 등재된 민간 암호화 제품을 수입 및 수출하고자 할 경우, 사업자는 관할 국가기관으로부터 민간 암호화 제품 수출입 허가 증서를 취득해야 한다.
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	2. 민간 암호화 제품 수출입 허가 증서는 아래의 모든 조건에 부합하는 사업자에게 교부된다: a) 민간 암호화 제품 서비스 거래 면허 증서를 소지하고 있다; b) 수입할 민간 암호화 제품이 본 법률 제39조에 따라 인증되었고 그러한 사실이 공표되었다; c) 민간 암호화 제품의 사용자 및 사용목적이 국

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.	가 안보와 보안 또는 사회 질서와 안전을 저해하지 않는다. 3. 민간 암호화 제품 수출입 허가 증서 신청 구비서류는 아래와 같은 문서로 구성된다: a) 민간 암호화 제품 수출입 허가 증서 신청서; b) 민간 암호화 제품 서비스 거래 면허 증서 사본; c) 수입할 민간 암호화 제품의 규제적합성인증서 사본. 4. 정부암호위원회는 구비서류를 수취한 날로부터 10일 이내에, 신청서를 심사하여 민간 암호화 제품 수출입 허가 증서를 사업자에게 교부한다. 허가증서 교부를 거부할 경우, 정부암호위원회는 사업자에게 구체적인 거부사유를 서면으로 통보한다. 5. 정부는 수출입 허가 대상 민간 암호화 제품 목록을 공표하고, 본 조에 따른 세칙을 제정해야 한다.
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	제35조 민간 암호화 제품 및 서비스를 거래하는 사업자의 책임 1. 제품의 기술 솔루션 및 기술에 관한 구비서류 및 문서를 관리한다. 2. 고객정보, 민간 암호화 제품 및 서비스의 명칭, 유형, 수량 및 사용목적을 수집, 저장 및 보호한다. 3. 매년 12월 31일까지 민간 암호화 제품 및 서비스의 수출입 거래내역을 정부암호위원회에게 보고하고, 고객정보를 개괄한다. 4. 민간 암호화 제품의 안전한 운송 및 보관을 보장하기 위한 조치를 시행한다. 5. 사용자가 민간 암호화 제품 및 서비스 이용에 관한 법률을 위반한 사실, 또는 사업자와 체결한 민간 암호화 제품 서비스 이용약관을 위반한 사실

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.	을 적발한 경우, 민간 암호화 제품 및 서비스 제공을 거부한다. 6. 관할 국가기관의 요청에 따라 국가 안보와 보안 및 사회 질서와 안전을 보장하기 위하여 민간 암호화 제품 및 서비스 제공을 보류 또는 중단한다. 7. 관할 국가기관의 요청에 따라, 그러한 기관이 전문적 조치를 취할 수 있는 여건을 조성하고, 조치 시행에 협조한다.
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.	제36조 민간 암호화 제품 및 서비스 사용자의 책임 1. 암호-키 이용 관리, 민간 암호화 제품 및 기타 관련 콘텐츠의 전송, 수리, 유지보수, 폐기 및 파기와 관련하여, 사업자와 체결한 민간 암호화 제품 서비스 약관을 준수한다. 2. 요청에 따라, 관할 국가기관에게 암호-키와 관련된 정보를 제공한다. 3. 관할 국가기관이 정보 또는 암호-키 절취범죄 및 불법적 목적의 민간 암호화 제품사용을 예방하기 위한 조치를 취할 수 있는 여건을 조성하고, 그러한 조치시행에 협조한다. 4. 베트남에 주재한 외국의 대사관, 영사관, 대표부 및 국제기구 사무소를 제외하고, 민간 암호화 제품 거래허가를 받지 아니한 자가 제공한 민간 암호화 제품을 사용하는 조직 및 개인은 그러한 제품의 사용사실을 정부암호위원회에게 신고해야 한다.
Chapter IV STANDARDS AND TECHNICAL REGULATIONS ON CYBERINFORMATION SECURITY	제4장 사이버정보 보안에 관한 표준 및 기술 규정
Article 37. Standards and technical regulations on cyberinformation security 1. Standards on cyberinformation security include	제37조 사이버정보 보안에 관한 표준 및 기술 규정

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.	1. 사이버정보 보안에 관한 표준은 베트남에서 적용되도록 공표 및 인정된 정보시스템, 하드웨어, 소프트웨어, 사이버정보의 관리와 안전한 운용을 위한 시스템에 관한 국제표준, 권역표준, 해외표준, 국가표준, 및 제조사표준을 포함한다.
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.	2. 사이버정보 보안에 관한 기술 규정은 베트남에서 개발, 공표 및 적용된 정보시스템, 하드웨어, 소프트웨어, 및 사이버정보의 관리와 안전한 운용을 위한 시스템에 관한 국가기술 규정 및 지방정부 차원의 기술 규정을 포함한다.
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.	제38조 사이버정보 보안에 관한 표준 및 기술 규정의 관리 1. 사이버정보 보안 규정 적합성 인증 주체란 하드웨어, 소프트웨어, 및 사이버정보의 관리와 안전한 운용을 위한 시스템이 사이버정보 보안에 관한 기술 규정에 부합함을 인증하는 적합성 인증기관을 의미한다.
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.	2. 사이버정보 보안 규정 적합성 공표 주체란 정보시스템, 하드웨어, 소프트웨어, 및 사이버정보의 관리와 안전한 운용을 위한 시스템이 사이버정보 보안에 관한 기술 규정에 부합함을 공표하는 조직 또는 사업자를 의미한다.
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.	3. 사이버정보 보안 표준 적합성 인증 주체란 하드웨어, 소프트웨어, 및 사이버정보의 관리와 안전한 운용을 위한 시스템이 사이버정보 보안에 관한 표준에 부합함을 인증하는 적합성인증기관을 의미한다.
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.	4. 사이버정보 보안 표준 적합성 공표 주체란 정보시스템, 하드웨어, 소프트웨어, 및 사이버정보의 관리와 안전한 운용을 위한 시스템이 사이버정보 보안에 관한 표준에 부합함을 공표하는 조직 또는 사업자를 의미한다

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.	5. 과학기술부는 주무기관으로서, 유관부처 및 기관과 협조하여, 표준 및 기술 규정에 관한 법률에 따라 사이버정보 보안에 관한 국가표준을 심사 및 공표할 책임을 진다.
6. The Ministry of Information and Communications shall:	6. 정보통신부는:
a/Draft national standards on cyberinformation security, except national standards mentioned in Clause 7 of this Article;	a) 본 조 7항에 명시된 국가표준을 제외한 사이버정보 보안에 관한 국가표준 초안을 작성한다;
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;	b) 본 조 7항에 명시된 국가표준을 제외한 사이버정보 보안에 관한 국가 기술 규정을 공표하고; 사이버정보 보안규정 적합성 평가에 관한 사항을 규정한다;
c/ Manage the quality of cyberinformation security products and services, except civil cryptographic products and services;	c) 민간 암호화 제품 및 서비스를 제외한 사이버정보 보안 제품 및 서비스의 품질을 관리한다;
d/ Register, designate, and manage the operation of, cyberinformation security conformity certification organizations, except conformity certification organizations for civil cryptographic products and services.	d) 민간 암호화 제품 및 서비스에 관한 적합성인증기관을 제외한 사이버정보 보안 적합성인증기관을 등록, 지정 및 관리한다.
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.	7. 정부암호위원회는 표준의 시행을 공표 및 지도하는 관할 국가기관에 제출할 민간 암호화 제품 및 서비스에 관한 국가표준 초안을 작성함에 있어, 국방부에 협조하고; 민간 암호화 제품 및 서비스에 관한 국가기술 규정을 개발하여 국방부에게 제출하며; 민간 암호화 제품 및 서비스에 관한 적합성인증기관을 지정 및 관리하고; 민간 암호화 제품 및 서비스의 품질을 관리한다.
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.	8. 성급 인민위원회는 사이버정보 보안에 관한 지방정부 차원의 기술 규정을 개발, 공표하고 그 시행을 지도하며; 지방자치단체의 사이버정보 보안 제품 및 서비스 품질을 관리한다.

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.	제39조 사이버정보 보안 표준 또는 기술 규정 적합성 평가 1. 아래 각 호의 경우, 사이버정보 보안 표준 또는 기술 규정 적합성 평가를 실시한다: a) 기술 규정적합성을 인증 또는 공표할 필요가 있고, 조직 또는 개인이 사이버정보 보안 제품을 시판하기 전에, 적합성 날인을 받아야 하는 경우; b) 국가 사이버정보 보안 관리를 위하여 필요한 경우. 2. 정보통신부가 지정한 적합성인증기관은 국가 중요 정보시스템 및 국가 사이버정보 보안 관리에 관한 사이버정보 보안 표준 또는 기술 규정 적합성 평가를 수행한다. 3. 국방부가 지정한 적합성인증기관은 민간 암호화 제품 및 서비스에 대한 사이버정보 보안 표준 또는 기술 규정 적합성 평가를 수행한다. 4. 베트남과 여타 국가 및 그 속령 간 사이버정보 보안 표준 또는 기술 규정 적합성 평가 결과, 그리고 베트남과 여타 국가 및 그 속령 간 적합성 인증기관에 관한 인정은 표준 및 기술 규정에 관한 법률을 따른다.
Chapter V TRADING IN THE FIELD OF CYBERINFORMATION SECURITY	제5장 사이버정보 보안 분야의 거래
Section 1 GRANT OF LICENSES FOR TRADING IN CYBERINFORMATION SECURITY PRODUCTS AND SERVICES	제1절 사이버정보 보안 제품 서비스 거래 면허 증서 교부
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	제40조 사이버정보 보안 분야의 거래 1. 사이버정보 보안 분야의 거래는 조건부이며, 사이버정보 보안 제품의 거래 및 사이버정보 보안서비스의 제공을 포함한다.

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.	2. 본 법률 제41조에 명시된 사이버정보 보안 제품 및 서비스를 거래하고자 하는 사업자는 관할 국가기관으로부터 사이버정보 보안 제품 서비스 거래 면허 증서를 취득해야 하며, 면허 증서는 발행일로부터 10년간 유효하다. 3. 사이버정보 보안 제품 및 서비스의 거래는 본 법률 및 기타 관련 법률을 준수해야 한다. 민간 암호화 제품 및 서비스의 면허 조건 및 거래 면허 증서 교부순서와 절차, 민간 암호화 제품의 수출입, 민간 암호화 제품 및 서비스를 거래하는 사업자의 책임, 민간 암호화 제품 및 서비스의 이용은 본 법률 제3장의 조항을 따른다. 전자서명 인증 서비스의 면허 조건 및 면허 증서 교부 순서와 절차는 전자거래에 관한 법률을 따른다.
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;	제41조 사이버정보 보안 제품 및 서비스 1. 사이버정보 보안 서비스는 아래를 포함한다: a) 사이버정보 보안 테스트 및 평가를 위한 서비스; b) 민간 암호화 기술을 사용하지 않는 정보 기밀성유지 서비스; c) 민간 암호화 서비스; d) 전자서명 인증 서비스; dd) 사이버정보 보안 상담서비스; e) 사이버정보 보안 감독 서비스; g) 사이버정보 보안 사고 대응서비스; h) 데이터 복구 서비스; i) 사이버 공격예방 및 대응서비스; k) 기타 사이버정보 보안 서비스. 2. 사이버정보 보안 제품은 아래를 포함한다: a) 민간 암호화 제품; b) 사이버정보 보안 테스트 및 평가를 위한 제품; c) 사이버정보 보안 감독을 위한 제품;

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.	d) 사이버 공격 및 해킹에 대응하기 위한 제품; dd) 기타 사이버정보 보안 제품. 3. 정부는 본 조 1항 k)호 및 2항 dd)호에 명시된 사이버정보 보안 제품 및 서비스의 세부목록을 공표해야 한다.
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	제42조 사이버정보 보안 제품 서비스 거래 면허 증서의 교부 조건 1. 본 법률 제41조 1항 a), b), c) 및 d)호, 2항 a)호에 명시된 제품 및 서비스를 제외하고, 사이버정보 보안 제품 및 서비스 거래를 위한 면허 증서는 아래의 모든 조건에 부합하는 사업자에게 교부된다: a) 사이버정보 보안 발전을 위한 국가전략, 종합계획 또는 일반계획에 따라 거래를 수행한다; b) 사이버정보 보안 제품 및 서비스 제공 규모에 적합한 장비와 물적 토대를 보유하고 있다; c) 정보 보안에 관한 전문적 요건을 준수하는데 필요한 경영직, 관리직 및 기술직 인력을 보유하고 있다; d) 적절한 사업 계획서를 보유하고 있다. 2. 사이버정보 보안 테스트 및 평가서비스 면허 증서는 아래의 모든 조건에 부합하는 사업자에게 교부된다: a) 본 조 1항에 명시된 조건을 충족한다; b) (외국인 투자기업을 제외하고) 베트남 법률에 따라 설립되었으며 베트남에서 합법적으로 사업을 영위하고 있다; c) 법적 대표자 그리고 경영직, 관리직 및 기술직 인력은 베트남에 영구 거주하는 베트남 국적자이다; d) 관련 표준 또는 기술 규정에 부합하는 기술계획서를 보유하고 있다; dd) 서비스 제공 과정에서 고객정보의 기밀성을 유지하기 위한 계획서를 보유하고 있다 e) 경영직, 관리직 및 기술직 인력이 정보 보안 테

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.	스트 및 평가 분야 학위 증서 또는 기타 증서를 소지하고 있다. 3. 민간 암호화 기술을 사용하지 않는 정보 기밀성유지 서비스 면허 증서는 아래의 모든 조건에 부합하는 사업자에게 교부된다: a) 본 조 제2항 a), b), c), d) 및 dd)호에 명시된 조건을 충족한다; b) 경영직, 관리직 및 기술직 인력이 정보 기밀성 분야 학위 증서 또는 기타 증서를 소지하고 있다. 4. 정부는 본 조에 따른 세칙을 제정해야 한다.
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	제43조 사이버정보 보안 제품 서비스 거래 면허 증서 신청을 위한 구비서류 1. 사이버정보 보안 제품 서비스 거래 면허 증서를 신청하는 사업자는 면허신청 구비서류를 정보통신부에게 제출해야 한다. 2. 사이버정보 보안 제품 서비스 거래 면허 증서를 신청하는 사업자는 아래와 같은 문서로 구성된 구비서류를 각 5부씩 제출해야 한다: a) 거래할 사이버정보 보안 제품 및 서비스의 종류를 명시한, 사이버정보 보안 제품 서비스 거래 면허 증서 신청서; b) 사업자등록증, 투자등록증 또는 그에 준하는 서류의 사본; c) 법률 요건에 부합하는 기술 장비 시스템에 관한 기술서; d) 제품 및 서비스의 제공 범위, 사용자, 및 관련 표준과 품질 기준을 명시한 사업 계획서; dd) 경영직, 관리직 및 기술직 인력이 소지한 정보 보안 분야 학위 증서 또는 기타 증서의 사본; 3. 민간 암호화 기술을 사용하지 않는 정보 보안 테스트 및 평가서비스 면허 증서를 신청할 경우, 본 조 2항에 명시된 구비서류 외에도 아래의 문서를 추가로 제출해야 한다: a) 법적 대표자, 경영직, 관리직 및 기술직 인력의

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.	범죄 경력 증명서(; b) 기술계획서; c) 서비스 제공 과정에서 고객정보의 기밀성을 유지하기 위한 계획서.
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.	제44조 사이버정보 보안 제품 서비스 거래 면허 증서 심사 및 교부 1. 정보통신부는 구비서류를 수취한 날로부터 40일 이내에, 주무기관으로서, 유관부처 및 기관과 협조하여, 신청서를 심사하고, (본 법률 제41조 1항 c)호 및 d)호 그리고 2항의 a)호에 명시된 제품 및 서비스를 제외한) 사이버정보 보안 제품 서비스 거래 면허 증서를 교부한다. 면허 증서 교부를 거부할 경우, 정보통신부는 사업자에게 구체적인 거부사유를 서면으로 통보한다. 2. 사이버정보 보안 제품 서비스 거래 면허 증서는 아래와 같은 중요사항을 명시해야 한다: a) 사업자의 상호명, 수출입거래에 사용하는 베트남어 및 (해당 시) 영어 명칭, 베트남에 소재한 주사무소의 주소; b) 법적 대표자의 성명; c) 면허 증서의 일련번호, 교부일자 및 만료일자; d) 거래가 허용된 사이버정보 보안 제품 및 서비스. 3. 사이버정보 보안 제품 서비스 거래 면허 증서를 교부 받은 사업자는 비용 및 수수료에 관한 법률에 따라, 해당 수수료를 납부해야 한다.
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	제45조 사이버정보 보안 제품 서비스 거래 면허 증서의 수정, 보충, 연장, 정지, 취소 및 재교부 1. 사업자가 상호명을 변경하거나, 법적 대표자를 변경하거나, 또는 사이버정보 보안 제품 및 서비

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.	스를 변경하거나 추가할 경우, 사이버정보 보안 제품 서비스 거래 면허 증서를 수정 및 보충해야 한다.
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.	사업자는 면허 증서 수정 보완 요청서, 수정 및 보완할 사항을 구체적으로 명시한 기술서 및 기타 관련 문서로 구성된 수정보충요청 구비서류를 각 2부씩 정보통신부에게 제출해야 한다:
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.	정보통신부는 구비서류를 수취한 날로부터 10일 이내에, 요청서를 심사하여 기존 면허 증서를 수정 및 보충한 후 사업자에게 재교부한다. 면허 증서 재교부를 거부할 경우, 정보통신부는 사업자에게 구체적인 거부사유를 서면으로 통보한다.
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.	2. 사이버정보 보안 제품 서비스 거래 면허 증서를 분실하거나 면허 증서가 훼손된 경우, 사업자는 재발급 사유를 명시한, 재교부 요청서를 정보통신부에게 제출해야 한다. 정보통신부는 그러한 요청을 수취한 날로부터 5일 이내에, 요청서를 검토하여 사업자에게 면허 증서를 재교부한다.
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:	3. 사이버정보 보안 제품 서비스 거래에 관한 법률을 위반하지 아니한 사업자는 사이버정보 보안 제품 서비스 거래 면허 증서의 유효기간을 1회에 한 하여, 1년 이하의 기간으로 연장할 수 있다. 사업자는 아래와 같은 문서로 구성된 연장요청 구비서류를 각 2부씩, 면허 증서 만료일로부터 60일 이전까지 정보통신부에게 제출해야 한다:
a/ A written request for license extension;	a) 면허 증서 연장 요청서;
b/ The license for trading in cyberinformation security products and services which remains valid;	b) 유효기간이 만료되지 아니한 사이버정보 보안 제품 서비스 거래 면허 증서;
c/ A report on the enterprise’s operation over	c) 사업자의 최근 2년간 운영 보고서.

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.	정보통신부는 구비서류를 수취한 날로부터 20일 이내에, 요청서를 심사하여 기존 면허 증서를 연장한 후 사업자에게 재교부한다. 면허 증서 연장을 거부할 경우, 정보통신부는 사업자에게 구체적인 거부사유를 서면으로 통보한다.
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.	4. 아래 각 호의 사유가 발생한 경우, 사업자의 사이버정보 보안 제품 서비스 거래 면허 증서는 최장 6개월까지 정지된다: a) 사업자가 면허 증서에 명시되지 아니한 서비스를 제공한 경우; b) 사업자가 본 법률 제42조에 명시된 조건을 충족하지 못한 경우; c) 기타 법률에서 정한 정지사유가 발생한 경우. 5. 아래 각 호의 사유가 발생한 경우, 사업자의 사이버정보 보안 제품 서비스 거래 면허 증서는 취소된다: a) 사업자가 정당한 사유 없이, 면허 증서 교부일로부터 1년이내에 서비스를 제공하지 아니할 경우; b) 면허 증서가 만료된 경우; c) 정지기간이 경과한 이후에도, 사업자가 본 조 4항에 명시된 문제를 해결하지 못한 경우.
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	제46조 사이버정보 보안 제품 및 서비스를 거래하는 사업자의 책임 1. 제품의 기술 솔루션 및 기술에 관한 구비서류 및 문서를 관리한다. 2. 고객정보를 수집, 저장 및 보호한다. 3. 매년 12월 31일까지 사이버정보 보안 제품의 수출입 거래내역을 정보통신부에게 보고한다. 4. 조직 또는 개인이 사이버정보 보안 제품 및 서비스 이용에 관한 법률을 위반한 사실, 또는 사업자와 체결한 사이버정보 보안 제품 서비스 이용약관을 위반한 사실을 적발한 경우, 사이버정보 보안 제품 및 서비스 제공을 거부한다. 5. 관할 국가기관의 요청에 따라 국가 안보와 보

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.	안 및 사회 질서와 안전을 보장하기 위하여 사이버정보 보안 제품 및 서비스 제공을 보류 또는 중단한다. 6. 관할 국가기관의 요청에 따라, 그러한 기관이 전문적 조치를 취할 수 있는 여건을 조성하고, 조치시행에 협조한다.
Section 2 MANAGEMENT OF IMPORT OF CYBERINFORMATION SECURITY PRODUCTS	제2절 사이버정보 보안 제품의 수입에 관한 관리
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.	제47조 사이버정보 보안 제품의 수입에 관한 관리 원칙 1. 사이버정보 보안 제품의 수입은 본 법률 및 기타 관련 법률에 따라 관리된다. 2. 외교면책과 특권을 갖는 기관, 조직 및 개인에 의한 사이버정보 보안 제품의 수입은 관세법 및 베트남주재 외국 대사관, 영사관, 대표부 및 국제기구 사무소의 면책과 특권에 관한 법률을 따른다. 3. 수입대상 사이버정보 보안 제품에 적용할 수 있는 사이버정보 보안에 관한 기술 규정이 국내에 없는 경우, 베트남사회주의공화국이 체결한 국제협약 또는 조약을 적용한다.
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	제48조 수입 허가 대상에 속하는 사이버정보 보안 제품 1. 정부가 제정한 수입 허가 대상 사이버정보 보안 제품 목록에 등재된 사이버정보 보안 제품을 수입하고자 할 경우, 사업자는 관할 국가기관으로부터 사이버정보 보안 제품 수입 허가 증서를 취득해야 한다. 2. 사이버보안 제품을 수입하기 전에, 조직 및 사업자는 본 법률 제39조에 따라 수입할 사이버보안 제품을 인증하고 그러한 사실을 공표해야 한다. 3. 사이버정보 보안 제품 수입 허가 증서는 아래의 모든 조건에 부합하는 조직 또는 사업자에게

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.	교부된다: a) 사이버정보 보안 제품 거래 면허 증서를 소지하고 있다; b) 사이버정보 보안 제품이 본 법률 제39조에 따라 인증되었고 그러한 사실이 공표되었다; c) 사이버정보 보안 제품의 사용자 및 사용목적이 국가 안보와 보안 또는 사회 질서와 안전을 저해하지 않는다. 4. 정보통신부는 사이버정보 보안 제품 수입 허가 증서 교부순서와 절차, 그리고 구비서류에 관한 세칙을 제정해야 한다.
Chapter VI DEVELOPMENT OF HUMAN RESOURCES FOR CYBERINFORMATION SECURITY	제6장 사이버정보 보안을 위한 인적자원 개발
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.	제49조 사이버정보 보안 분야 전문 교육 1. 정보시스템 관리 주체는 관리직 및 기술직 인력에게 사이버정보 보안에 관한 지식과 기술 교육을 제공해야 한다. 2. 상근 사이버정보 보안 담당자는 보유한 전문자격과 연관된 업무에 배정되어 그러한 업무수행에 협조하며, 사이버정보 보안 재교육에 우선적으로 참여해야 한다. 3. 국가는 조직 및 개인이 사이버정보 보안 분야의 인적자원 양성을 위한 고등교육기관 및 직업훈련기관 설립에 투자, 합작투자하거나 여타 조직과 협력하도록 권장한다. 4. 내무부는 주무기관으로서, 정보통신부 및 유관부처와 협조하여, 고위공무원 및 일반공무원을 위한 사이버정보 보안 지식 및 운용 기술 교육 계획을 수립하고 기획할 책임을 진다.

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.	제50조 사이버정보 보안 분야 학위 및 증서 1. 고등교육기관 및 직업훈련기관은 부여 받은 책무와 권한 내에서, 사이버정보 보안 분야 학위 증서 및 직업훈련증서를 수여할 수 있다. 2. 교육부는 주무기관으로서, 정보통신부 및 기타 유관부처와 협조하여, 해외에서 발행된 사이버정보 보안 분야 고등교육 학위 증서의 인정 업무에 관한 책임을 진다. 3. 노동보훈사회부는 주무기관으로서, 정보통신부 및 기타 유관부처와 협조하여, 해외에서 발행된 사이버정보 보안 분야 학위 증서 및 직업 훈련 증서의 인정 업무에 관한 책임을 진다.
Chapter VII STATE MANAGEMENT OF CYBERINFORMATION SECURITY	제7장 국가 사이버정보 보안 관리
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 nationalstandards 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.	제51조 국가 사이버정보 보안 관리 내용 1. 사이버정보 보안에 관한 국가전략, 종합계획, 일반계획 및 정책을 수립하고; 사이버정보 보안에 관한 국가프로그램을 수립하며 그 시행을 지시한다. 2. 사이버정보 보안에 관한 법적 문서(legal documents)를 공표하고 그 시행을 기획하며; 사이버정보 보안에 관한 국가표준을 개발 및 공표하고; 또한 사이버정보 보안에 관한 기술 규정을 공표한다. 3. 민간 암호화 기술 국가관리를 수행한다. 4. 사이버정보 보안에 관한 표준 및 기술 규정 적합성 평가와 공표를 관리한다. 5. 정보시스템 보안 감독을 관리한다. 6. 정보시스템 설계도서의 사이버정보 보안관련 콘텐츠를 심사한다.

7. Disseminating the law on cyberinformation security.	7. 사이버정보 보안에 관한 법률을 전파한다.
8. Managing the trading in cyberinformation security products and services.	8. 사이버정보 보안 제품 및 서비스의 거래를 관리한다.
9. Organizing research and application of cyberinformation security science and technology; developing human resources for cyberinformation security; training full-time cyberinformation security officers.	9. 사이버정보 보안 분야 과학기술의 연구와 응용; 사이버정보 보안 분야 인적자원 개발; 및 상근 사이버정보 보안 관리자의 교육을 기획한다.
10. Conducting examination and inspection, settling complaints and denunciations, and handling violations of the law on cyberinformation security.	10. 평가 및 점검을 수행하고, 진정 및 불만 사항을 해결하며, 사이버정보 보안에 관한 법률 위반 사항을 처리한다.
11. Entering into international cooperation on cyberinformation security.	11. 사이버정보 보안에 관한 국제협력을 추진한다.
Article 52. Responsibilities for state management of cyberinformation security	제52조 국가 사이버정보 보안 관리 책임
1. The Government shall uniformly perform the state management of cyberinformation security.	1. 정부는 국가 사이버정보 보안 관리를 일률적으로 수행해야 한다.
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:	2. 정보통신부는 국가 사이버정보 보안 관리의 수행과 관련하여 정부에 대한 책임을 지며, 아래의 책무와 권한을 갖는다:
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;	a) 사이버정보 보안에 관한 법적 문서, 국가전략, 종합계획, 일반계획, 국가표준 및 국가기술 규정을 공표하거나, 작성 후 공표를 담당하는 관할 당국에게 제출한다;
b/ To appraise cyberinformation security-related contents in design dossiers of information systems;	b) 정보시스템 설계도서의 사이버정보 보안관련 콘텐츠를 심사한다;
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;	c) 본 조 3항 c)호 및 5항 b)호에 명시된 정보시스템을 제외하고, 국가차원의 정보시스템 보안 감독을 관리한다;
d/ To manage cyberinformation security assessment;	d) 사이버정보 보안 평가를 관리한다;
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;	dd) 민간 암호화 제품 및 서비스를 제외하고, 사이버정보 보안 제품 서비스 거래 면허 증서 및 정보 보안 제품 수입 허가 증서를 교부한다;

e/ To research and apply cyberinformation security science and technology; to train and develop human resources;	e) 사이버정보 보안 분야 과학기술을 연구 및 응용하고; 인적자원을 교육 및 개발한다.
g/ To manage and carry out international cooperation on cyberinformation security;	g) 사이버정보 보안에 관한 국제협력을 관리 및 추진한다;
h/ To conduct examination and inspection, settle complaints and denunciations, and handle violations of the law on cyberinformation security;	h) 평가 및 점검을 수행하고, 진정 및 불만사항을 해결하며, 사이버정보 보안에 관한 법률 위반사항을 처리한다;
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) 주무기관으로서, 유관부처, 성급 인민위원회, 및 사업자와 협조하여, 사이버정보 보안을 보장할 책임을 진다;
i/ To disseminate the law on cyberinformation security;	i) 사이버정보 보안에 관한 법률을 전파한다;
l/ To annually report on cyberinformation security activities to the Government.	l) 사이버정보 보안 활동 내역을 매년 정부에게 보고한다.
3. The Ministry of National Defense has the following tasks and powers:	3. 국방부는 아래의 책무와 권한을 갖는다:
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;	a) 국방부가 관리하는 분야의 사이버정보 보안에 관한 법적 문서, 국가전략, 종합계획, 일반계획, 국가표준 및 국가기술 규정을 공표하거나, 작성 후 공표를 담당하는 관할 당국에게 제출한다;
b/To conduct examination and inspection, settle complaints and denunciations, and handle violations in cyberinformation security assurance activities in the fields under its management;	b) 국방부가 관리하는 분야의 평가 및 점검을 수행하고, 진정 및 불만사항을 해결하며, 사이버정보 보안 보장활동에 관한 위반사항을 처리한다;
c/ To manage security supervision of its information systems.	c) 국방부의 정보시스템 보안 감독을 관리한다.
4. The Government Cipher Committee shall assist the Minister of National Defense in performing the state management of civil cryptography, having the following tasks:	4. 정부암호위원회는 민간 암호화 기술 국가관리 수행분야에서 국방부와 협조하고, 아래의 책무 갖는다:
a/ To formulate and submit to competent authorities for promulgation legal documents on managementof civil cryptography;	a) 민간 암호화 기술 관리에 관한 법적 문서를 작성하여 관할 당국에게 제출한다.
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 civilcryptographic	b) 주무기관으로서, 유관부처와 협조하여, 민간 암호화 제품 및 서비스에 관한 국가표준 및 국가기술 규정을 작성하여 관할 국가기관에게 제출한다;

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;	c) 민간 암호화 기술의 거래와 이용을 관리하고; 민간 암호화 제품 및 서비스의 품질을 관리하며; 민간 암호화 제품 및 서비스에 관한 표준 및 기술 규정 적합성 평가와 공표를 관리한다;
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;	d) 민간 암호화 제품 서비스목록 및 수출입 허가 대상 민간 암호화 제품 목록을 작성하여 관할 당국에게 제출한다;
dd/ To grant licensesfor trading in civil cryptographic products and services and permits for export and import of civil cryptography products;	dd) 민간 암호화 제품 서비스 거래 면허 증서 및 민간 암호화 제품 수출입 허가 증서를 교부한다;
e/ To conduct examination and inspection, settle complaints and denunciations, and handle violations in the trading in and use of civil cryptography;	e) 평가 및 점검을 수행하고, 진정 및 불만사항을 해결하며, 민간 암호화 기술의 거래 및 사용에 관한 위반사항을 처리한다;
g/ To enter into international cooperation on civil cryptography.	g) 민간 암호화 기술에 관한 국제협력을 추진한다.
5. The Ministry of Public Security has the following tasks and powers:	5. 공안부는 아래의 책무와 권한을 갖는다:
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;	a) 주무기관으로서, 유관부처와 협조하여, 국가기밀의 보호, 국가 안보와 보안 또는 사회 질서와 안전을 저해하는 사이버범죄와 사이버공간악용 예방 및 대응에 관한 법적 문서를 작성하여 관할 당국에게 제출하거나, 또는 직접 공표하고 그 시행을 지도한다;
b/ To manage security supervision of its information systems;	b) 공안부의 정보시스템 보안 감독을 관리한다;
c/ To organize and direct the crime prevention and combat, and organize investigation of cybercrimes and other violations in the field of cyberinformation security;	c) 범죄 예방 및 대응을 기획 및 지시하고, 사이버범죄와 사이버정보 보안 분야의 기타 위반 사항에 관한 조사를 기획한다;
d/ To coordinate with the Ministry of Information and Communications and related ministries and sectors in examining and inspecting cyberinformation security and handling violations	d) 정보통신부 및 유관부처와 협조하여, 사이버정보 보안 상태를 평가 및 점검하고 사이버정보 보안에 관한 법률 위반사항을 처리한다.

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.	6. 내무부는 고위공무원 및 일반공무원을 위한 사이버정보 보안 지식 및 운용 기술 교육 계획을 수립하고 기획할 책임을 진다.
7. The Ministry of Education and Training shall organize training in and dissemination of cyberinformation security knowledge in higher education institutions.	7. 교육부는 고등교육기관이 사이버정보 보안에 관한 지식을 교육 및 보급할 수 있도록 기획한다.
8. The Ministry of Labor, War Invalids and Social Affairs shall organize training in and dissemination of cyberinformation security knowledge in vocational training institutions.	8. 노동보훈사회부는 직업훈련기관이 사이버정보 보안에 관한 지식을 교육 및 보급할 수 있도록 기획한다.
9. The Ministry of Finance shall provide guidance on and allocate funds for performance of cyberinformation security assurance tasks in accordance with law.	9. 재무부는 법률에 따라 사이버정보 보안 보장을 수행하는데 소요되는 예산에 관한 지침을 제공하고, 그러한 예산을 할당한다.
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.	10. 중앙부처는 부여 받은 책무와 권한 내에서, 해당 부처 네트워크의 사이버정보 보안을 관리하고, 정보통신부와 협조하여 국가 사이버정보 보안 관리를 수행한다.
11. Provincial-level People’s Committees shall, within the ambit of theirtasks and powers, perform the state management of cyberinformation security in localities.	11. 성급 인민위원회는 부여 받은 책무와 권한 내에서, 지방자치단체에서의 국가 사이버정보 보안 관리를 수행한다.
Chapter VIII IMPLEMENTATION PROVISIONS	제8장 법률의 시행
Article 53. Effect This Law takes effect on July 1, 2016.	제53조 발효일 본 법률은 2016년 7월 1일부부터 효력을 발생한다.
Article 54.Detailing provision The Government and competent state agencies shall detail the articles and clauses in the Law as assigned.	제54조 세칙의 제정 베트남사회주의공화국의 정부 및 산하기관은 본 법률의 해당 조항에 의거하여 세칙을 제정한다.
This Law was passed on November 19, 2015, by the XIIIthNational Assembly of the Socialist Republic of Vietnam at its 10th session. Chairman of the National Assembly NGUYEN SINH HUNG	베트남사회주의공화국 제13대 국회 제10차 본회의 2015년 11월 19일 국회의장 응웬 신 흥