

GOVERNMENT OF VIETNAM

SOCIALIST REPUBLIC OF VIETNAM

Independence - Freedom – Happiness

No. 332/2026/ND-CP

Hanoi, August 19, 2026

DECREE

ON PROVISION OF CYBERSECURITY PRODUCTS AND SERVICES

Pursuant to Law on Government Organization No. 63/2025/QH15;

Pursuant to Law on Cybersecurity No. 116/2025/QH15;

Pursuant to Law on Investment No. 143/2025/QH15;

Pursuant to Law on Foreign Trade Management No. 05/2017/QH14;

At the request of the Minister of Public Security;

The Government of Vietnam hereby promulgates a Decree on provision of cybersecurity products and services

Chapter I

GENERAL PROVISIONS

Article 1. Scope

1. This Decree provides for Clause 3 Article 28 and Clause 3 Article 29 of the Law on Cybersecurity No. 116/2025/QH15, including:

- a) Cybersecurity products/services;
- b) Cybersecurity product/service provision: conditions for product/service provision; issuance, modification, reissuance, extension, temporary suspension, and revocation of licenses for product/service provision;
- c) Import and export of cybersecurity products: Conditions for the issuance and revocation of export and import licenses for cybersecurity products;
- d) Inspection of provision of cybersecurity products/services; export and import of cybersecurity products;

dd) Responsibilities of relevant agencies, organizations, enterprises, and individuals relevant to cybersecurity product/service provision.

2. This Decree does not apply to provision of commercial cryptographic products and services.

Article 2. Regulated entities and principles of application

1. This Decree applies to organizations and enterprises engaged in cybersecurity product/service provision; licensing and governing agencies of cybersecurity product/service provision; and agencies, organizations, and individuals relevant to cybersecurity product/service provision.

2. The Ministry of National Defense shall manage cybersecurity for military and defense; the Ministry of Public Security shall manage cybersecurity for Military units engaged in civil and economic activities within its authority; for overlapping areas (if any), the Ministry of Public Security and the Ministry of National Defense shall agree on a coordination mechanism.

Article 3. Cybersecurity products

Cybersecurity products provided under this Decree include:

1. Cybersecurity testing and evaluation products: hardware devices and software with features or designed to integrate features including: scanning, testing, analyzing configurations, status, and log data of information systems and electronic devices; detecting vulnerabilities and weaknesses; and providing cybersecurity risk assessments.

2. Cybersecurity supervision products: hardware devices and software with features or designed to integrate features including: monitoring and analyzing data, network addresses, and network traffic; collecting and analyzing log data in real time; detecting and issuing alerts on abnormal events posing risks of cybersecurity breaches.

3. Anti-attack and intrusion prevention products: hardware devices and software featuring or designed to integrate features preventing attacks and intrusions into information systems.

4. Other cybersecurity products falling under any of the following categories:

a) Covert information-gathering products, including: hardware devices and software covertly collecting information in cyberspace, within electronic means and devices;

b) Cyber information suppression products, including: specialized hardware devices and software to block, insert, jam, or disrupt wireless Internet transmission in protected areas and targets;

c) Digital forensics and digital investigation products, including: specialized hardware devices and software for collecting, extracting, recovering, analyzing electronic data, and conducting digital forensics examinations from electronic data sources;

d) Network suppression products, including: specialized hardware devices and software to suppress or alter the operation of telecommunications networks, Internet networks, computer networks, information systems, information processing and control systems, databases, and electronic means;

dd) IP address masking products: products connecting networks between devices and cyberspace through remote servers to mask the real IP address of devices in cyberspace.

Article 4. Cybersecurity services

Cybersecurity services provided under this Decree include:

1. Cybersecurity testing and evaluation services: services for scanning, testing, analyzing configurations, status, and log data of information systems and electronic devices; detecting vulnerabilities and weaknesses; and providing cybersecurity risk assessments.
2. Information security services not using commercial cryptography: services supporting users in ensuring the confidentiality of information and information systems not using commercial cryptographic products.
3. Cybersecurity consulting services: services supporting consultation, testing, evaluation, implementation, design, and construction of cybersecurity solutions.
4. Cybersecurity monitoring services: services for monitoring and analyzing data traffic transmitted on information systems; collecting and analyzing log data in real time; and detecting and issuing alerts on abnormal events posing risks of cybersecurity breaches.
5. Cybersecurity incident response services: services for promptly handling and remediating cybersecurity incidents occurring on information systems.
6. Data recovery services: services for restoring data within electronic devices or information systems that has been deleted or damaged.
7. Cyberattack prevention/mitigation services: services for blocking acts of attack and intrusion into information systems through monitoring, collecting, and analyzing ongoing events on information systems.
8. Other cybersecurity services, including:
 - a) Cybersecurity protection platform provision services: services connecting experts and the cyberspace community to participate in cybersecurity and data security protection;
 - b) Cybersecurity protection training and drill services;
 - c) IP address masking services: services providing network connections between devices and cyberspace via remote servers to mask the real IP address of devices in cyberspace;

d) Vulnerability hunting and reporting services: services providing platforms to receive reports on detected security vulnerabilities within information systems of agencies, organizations, and individuals from security experts and the cybersecurity community.

Article 5. Cybersecurity product/service provision

1. An organization/enterprise must hold a license for cybersecurity product/service provision to provide cybersecurity products and services specified in Article 3 and Article 4 of this Decree.
2. A license for cybersecurity product/service provision shall have a validity period of 10 years.
3. The applicant for issuance of a license for cybersecurity product/service provision shall pay fees in accordance with laws on fees and charges.

Chapter II

CONDITIONS FOR CYBERSECURITY PRODUCT/SERVICE PROVISION

Article 6. General conditions for cybersecurity product provision

A cybersecurity product/service provider shall be issued a license for cybersecurity product/service provision upon fully satisfying the following conditions:

1. It is established under Vietnamese law and not in contrary with regulations on cybersecurity product/service provision. A foreign-invested economic organization must have its investment duration in Vietnam remained valid for more than 5 years as from the date of issuance of the license for cybersecurity product/service provision.

2. Personnel requirements:

a) The legal representative, manager, or person authorized by the legal representative or manager does not fall under any of the following cases:

He/she is a Vietnamese citizen who has been criminally prosecuted and is undergoing investigation, prosecution, or trial by Vietnamese or foreign competent authorities; or has a criminal record for offenses against national security; or has been identified by competent authorities as engaging in activities against national security; or has criminal records for other intentional offenses that have not been expunged; or is currently serving a suspended sentence; or is under the mandatory supervision, or the prohibition from residence or holding certain position or running a business line subject to security and order requirements upon the court's decision; or is subject to compulsory educational measures at communes, wards, or special zones; or is suspended from the compliance with a decision on serving a sentence in correctional institution or rehabilitation center.

He/she is an overseas Vietnamese holding foreign passports and foreign nationals who has not been granted residence and work permit in Vietnam by the competent Vietnamese authority.

b) The cybersecurity product/service provider has technical personnel appropriate for the type of products and services, who must hold a bachelor's degree or higher or possess specialized certifications in cybersecurity, information security, information technology, or electronics and telecommunications.

3. Technical requirements: It has system equipment, facilities, and technology appropriate for investment and provision of the registered cybersecurity products and services.

Article 7. Conditions for production, purchase, sale, exchange, import, and export of cybersecurity products

1. A cybersecurity product manufacturer must satisfy the conditions specified in Article 6 of this Decree and the following conditions:

a) The product categories and production scale conform to the development strategy of the cybersecurity industry;

b) It has an appropriate business plan, comprising: Scope and target users of product supply; types of products intended for production; compliance with relevant technical standards and regulations of each product; basic technical features of products;

c) It has appropriate means and equipment to inspect and monitor technical parameters for product quality control during manufacturing, ensuring compliance with technical standards and regulations on cybersecurity protection;

d) The cybersecurity products specified in points a, b, c, and d, Clause 4, Article 3 of this Decree shall only be manufactured for national security purposes by manufacturers of the Ministry of Public Security or the Ministry of National Defense upon written task assignments or commissioning or by manufacturers executing contracts with competent authorities of the Ministry of Public Security or the Ministry of National Defense that fully satisfy the prescribed manufacturing conditions.

2. A cybersecurity product trader/importer/exporter must satisfy the conditions specified in Article 6 of this Decree and the following conditions:

a) The product categories and scale conform to the development strategy of the cybersecurity industry;

b) It has an appropriate business plan, comprising: Purpose of import; types of products intended for production; compliance with relevant technical standards and regulations of each product; detailed basic technical features of products;

c) It has appropriate means and equipment for preservation and quality assurance of cybersecurity products in accordance with technical standards and regulations on cybersecurity protection;

d) Only entities specified in Point d Clause 1 of this Article are permitted to trade, import, or export the cybersecurity products specified in Points a, b, c, and d Clause 4 Article 3 of this Decree;

dd) Export and import of cybersecurity products must have clear purposes and users, provided that it shall not harm national security.

Article 8. Conditions for provision of cybersecurity services

A cybersecurity service provider must satisfy the conditions specified in Article 6 of this Decree and the following conditions:

1. For cybersecurity testing services and cybersecurity consulting services: (i) the technical team must comprise at least 05 individuals holding a bachelor's degree or higher or certificates in cybersecurity and having specific residential addresses in Vietnam; (ii) the legal representative must be a Vietnamese national.
2. For cybersecurity supervision services: (i) there must be at least 12 individuals holding a bachelor's degree or higher or certificates in cybersecurity; (ii) there must be a person responsible for system administration and information security; and (iii) the legal representative must be a Vietnamese national.
3. It has a technical plan that satisfies the requirements for cybersecurity protection according to the services to be provided, which is made using Form No. 07 in Appendix I enclosed herewith.
4. It has a contingency plan to ensure continuous and safe operation maintenance and incident recovery when an incident occurs.
5. It has an overall description of the technical features of the cybersecurity supervision system; operating procedures for cybersecurity supervision.
6. It has an appropriate business plan, comprising: Scope, service users, types of services to be provided, customer information security plan, and service quality assurance plan.

Article 9. Issuance of license for cybersecurity product/service provision

1. An organization or enterprise shall be granted a license for cybersecurity product/service provision when satisfying the conditions specified in Article 6, Article 7, and Article 8 of this Decree.
2. An application for issuance of a license for cybersecurity product/service provision includes:
 - a) An application form made using Form No. 03 in Appendix I enclosed herewith;
 - b) Curricula vitae accompanied by personal papers of the legal representative, managers of the applicant, where the information cannot be retrieved from the information system, including:

Copies of ID card/citizen ID card/passport, permanent residence card/temporary residence card/visa with valid duration of stay in Vietnam; declarations of personnel of the organization/enterprise made using Form No. 05, Form No. 06 in Appendix I enclosed herewith;

c) Diplomas, certificates, or equivalent documents proving the satisfaction of personnel conditions in accordance with the law on education and training;

d) Explanatory documents on system, equipment, facilities, and technology appropriate for investment and provision of the registered cybersecurity products and/or services.

dd) Technical plan and business plan made using Form No. 07 and Form No. 08 in Appendix I enclosed herewith;

e) For manufacturers of products specified in points a, b, c, and d, Clause 4, Article 3 hereof for national security purposes: written task assignments or commissioning or contracts with competent authorities of the Ministry of Public Security or the Ministry of National Defense are required.

3. The application for issuance of a license for cybersecurity product/service provision shall be prepared in 01 set and submitted in person, via postal service, or online through the public service portal of the Ministry of Public Security. The application must be in Vietnamese, comprising 01 original set. In case of direct submission or submission via postal service, the original set must bear full signatures and seals of the applicant; any documents consisting of at least 02 pages must bear a cross-page seal. The applicant shall be held accountable for the legitimacy of the application. In case of online submission, the applicant must use a digital signature in accordance with the law on digital signatures.

4. The time of application receipt is the time the application-receiving official receives the application from the applicant (for direct submission), or receives it from a postal employee (for submission via postal service), or the date the application-receiving official records the application in the public service portal system and confirms receipt to the applicant (for online submission). Within 03 working days from the date of receipt, the receiving agency shall review and notify the applicant of the validity of the application:

a) If the application is satisfactory: Receive and process such application; prepare a written confirmation (Form No. 10 in Appendix I enclosed herewith) and send it to the applicant or confirm via the account on the public service portal or via email address (if any);

b) If supplementary documents are required: Provide a guidance to supplement the application and send a notice (using Form No. 11 in Appendix I enclosed herewith) to the applicant in writing, via the applicant's account on the public service portal, or via email address (if any). Within 10 working days from the date of receiving the notice, the applicant must complete and re-submit the application as notified. If the applicant fails to re-submit the complete application within the prescribed time limit, such application shall be deemed unsatisfactory.

c) If the application is unsatisfactory: Refuse to receive and process the application; a refusal and reasons for refusal (Form No. 11 in Appendix I enclosed herewith) shall be sent to the applicant in writing, via the account on the public service portal, or via email address (if any);

5. Within 28 working days from the date of receiving a satisfactory application, the Ministry of Public Security shall appraise the application. If it contains sufficient information to demonstrate eligibility prescribed in this Decree, the Ministry of Public Security shall consider issuing the license for cybersecurity product/service provision according to Form No. 01 in Appendix I enclosed herewith; otherwise, a written refusal according to Form No. 12 in Appendix I enclosed herewith shall be provided.

Article 10. Replacement of license for cybersecurity product/service provision

1. An organization or enterprise shall request the replacement of its license for cybersecurity product/service provision in cases where there is a modification of its name, its legal representative, or an addition or change to cybersecurity products and services; or when an unexpired license for cybersecurity product/service provision is lost or damaged.

2. An application for replacement of a license for cybersecurity service provision includes:

a) An application form made using Form No. 03 in Appendix I enclosed herewith;

b) Curriculum vitae accompanied by personal papers of the legal representative;

c) A detailed description of the content to be replaced;

d) Documents proving satisfaction of conditions for the corresponding type of cybersecurity product/service as requested by the applicant (in cases of modification of the applicant's name or legal representative, or changes of cybersecurity products and services).

3. Information safety products and services shall be converted into cybersecurity products and services as follows:

a) Information safety testing and evaluation products shall be replaced with cybersecurity testing and evaluation products;

b) Information safety supervision products shall be replaced with cybersecurity supervision products;

c) Anti-attack and anti-intrusion products shall remain unchanged;

d) Other information safety products shall be removed;

dd) Information safety supervision services shall be replaced with cybersecurity supervision services;

- e) Anti-attack and anti-intrusion services shall remain unchanged;
 - g) Information safety consulting services shall be replaced with cybersecurity consulting services;
 - h) Information safety incident response services shall be replaced with cybersecurity incident response services;
 - i) Information safety testing and evaluation services shall be replaced with cybersecurity testing and evaluation services;
 - k) Data recovery services shall remain unchanged;
 - l) Information security services not using civil cryptography shall remain unchanged;
 - m) Other information safety services shall be removed;
4. An application for replacement of a license for cybersecurity product/service provision shall be submitted in accordance with Clause 3 Article 9 hereof.
5. The Ministry of Public Security shall review the validity of the application as specified in Clause 4, Article 9 of this Decree.
6. Within 05 working days from the date of receiving a satisfactory application, the Ministry of Public Security shall consider replacing the license for cybersecurity product/service provision; in case of refusal, a written explanation shall be provided.
7. The validity period of the new license for cybersecurity product/service provision shall correspond to that of the former license.

Article 11. Reissuance of a license for cybersecurity service provision

1. An organization or enterprise shall apply for the reissuance of its license for cybersecurity product/service provision in cases where its unexpired license is lost or damaged.
2. An application for reissuance of a license for cybersecurity service provision includes:
- a) An application form made using Form No. 03 in Appendix I enclosed herewith;
 - b) Curriculum vitae accompanied by personal papers of the legal representative;
 - c) A detailed description of the content to be reissued;
3. An application for reissuance of a license for cybersecurity product/service provision shall be submitted in accordance with Clause 3 Article 9 hereof.

4. The Ministry of Public Security shall review the validity of the application as specified in Clause 4, Article 9 of this Decree.

5. Within 05 working days from the date of receiving a satisfactory application, the Ministry of Public Security shall consider reissuing the license for cybersecurity product/service provision; in case of refusal, a written explanation shall be provided.

6. The validity period of the new license for cybersecurity product/service provision shall correspond to that of the former license.

Article 12. Renewal of licenses for cybersecurity product/service provision

1. An organization or enterprise that has not committed any violations against regulations on cybersecurity product/service provision may have its license for cybersecurity product/service provision renewed once with the prolonged duration not more than 03 years. An application for the renewal of a license for cybersecurity product/service provision shall be submitted to the Ministry of Public Security at least 60 days prior to the expiration date of the license for cybersecurity product/service provision.

2. An application for renewal of a license for cybersecurity service provision includes:

a) An application form made using Form No. 03 in Appendix I enclosed herewith;

b) An operational report of the applicant for the most recent 02 years.

3. An application for renewal of a license for cybersecurity product/service provision shall be submitted in accordance with Clause 3 Article 9 hereof.

4. The Ministry of Public Security shall review the validity of the application as specified in Clause 4, Article 9 of this Decree.

5. Within 10 working days from the date of receiving a satisfactory application, the Ministry of Public Security shall consider the renewal of the license for cybersecurity product/service provision; in case of refusal, a written explanation shall be provided.

Article 13. Issuance of licenses for export and import of cybersecurity products

1. When exporting/importing cybersecurity products specified in the list of cybersecurity products subject to export/import licensing in the Appendix enclosed herewith, the exporter/importer must possess a license for export/import of cybersecurity products issued by the Ministry of Public Security. A license for export/import of cybersecurity products shall be issued separately on the consignment basis and is valid for 02 years. The applicant for issuance of license for export/import of cybersecurity products must possess a valid license for cybersecurity product/service provision and pay fees in accordance with regulations.

2. Conditions for issuance of licenses for export and import of cybersecurity products

- a) The applicant possesses a valid license for cybersecurity product/service provision;
 - b) Imported cybersecurity products conform to international standards or Vietnamese standards in cybersecurity in accordance with the law on standards and technical regulations;
 - c) The purpose and intended users of the cybersecurity products are specific and do not cause harm to national security.
3. An application for issuance of a license for export and import of cybersecurity products specified in Article 3 of this Decree includes:
- a) An application form for issuance of a license for export and import of cybersecurity products, which is made using Form No. 04 in Appendix I enclosed herewith;
 - b) Documents proving compliance with international standards or Vietnamese standards in cybersecurity;
 - c) Documents proving the purpose and subject of import, including commercial contracts with end users, documents proving the purpose of import to serve research or warranty services.
4. The list of exported and imported cybersecurity products and HS codes is specified in Appendix II enclosed herewith.
5. An application for issuance of license for export and import of cybersecurity products shall be submitted in accordance with Clause 3 Article 9 of this Decree.
6. The Ministry of Public Security shall review the validity of the application as specified in Clause 4, Article 9 of this Decree.
7. Within 05 working days from the date of receiving a satisfactory application, the Ministry of Public Security shall consider issuing the license for export and import of cybersecurity products; in case of refusal, a written explanation made using Form No. 12 in Appendix I enclosed herewith shall be provided.

Article 14. Suspension and revocation of licenses for cybersecurity product/service provision

1. Cases of indefinite revocation:

- a) Forged documents are used or false information is provided in the application for issuance of the license for cybersecurity product/service provision; the license for cybersecurity product/service provision is issued ultra vires as specified in this Decree;
- b) The cybersecurity product/service provider is detected that it fails to satisfy the conditions prescribed Articles 6, 7, and 8 hereof upon the inspection conducted by the competent authority,

but it still fails to perform remedial actions within 40 days from the day on which the written conclusion is made;

c) After 06 months from the day on which the license for cybersecurity product/service provision is issued, the enterprise is inactive;

d) The cybersecurity product/service provider is suspended from operation, dissolved, or declared bankrupt in accordance with law; or has its establishment registration documents revoked by the competent authority; or has a proposal for revocation of the license for cybersecurity product/service provision;

dd) The license for cybersecurity product/service provision is lent, leased or sold.

2. Cases of fixed-term suspension of the use of licenses for cybersecurity product/service provision from 03 months to 06 months:

a) The cybersecurity product/service provider fails to carry out procedures for license replacement when its name or legal representative is changed;

b) The cybersecurity product/service provider fails to carry out procedures for license reissuance when the license is lost or damaged;

c) The cybersecurity product/service provider fails to cease or suspend the provision of cybersecurity products and services upon request by competent authorities;

d) The cybersecurity product/service provider fails to report to the Ministry of Public Security on business, export, and import of cybersecurity products and services as required;

dd) The cybersecurity product/service provider has faced administrative penalties for violations against regulations on provision of cybersecurity products services 02 times or more per year.

3. During inspections, if an organization or enterprise is found to fall under any of the cases for license revocation or suspension specified in Clauses 1 and 2 of this Article, the inspecting authority shall prepare a record and submit it to the Ministry of Public Security. Within 15 working days from the date of receiving the record, the Ministry of Public Security shall consider deciding on the revocation or suspension of the license for cybersecurity product/service. Decisions on revocation or suspension shall be sent to business registration agencies and customs authorities.

4. In cases where the license for cybersecurity product/service is revoked or suspended, the license for export and import of cybersecurity products shall cease to be valid.

Article 15. Revocation of licenses for export and import of cybersecurity products

1. An exporter/importer shall have its license for export and import of cybersecurity products revoked in the following cases:

- a) Forged documents are used in the application for issuance of the license for export and import of cybersecurity products; or the license is altered;
 - b) The license for export and import of cybersecurity products is granted ultra vires or not following procedures provided in this Decree;
 - c) The importer has its business registration certificate or investment registration certificate revoked or suspended, terminates operations, no longer authorized by the owner or manufacturer of the cybersecurity products without transfer of import right to the replacing organization, or is dissolved, or declared bankrupt in accordance with law;
 - d) Circulation period of imported cybersecurity products expire according to notice of manufacturers, owners, or competent organizations or errors are found while cybersecurity products are in circulation on the market causing consequences for users and cannot be rectified.
2. During inspections, if an exporter/importer is found to fall under any of the cases for license revocation or suspension specified in Clause 1 of this Article, the inspecting authority shall prepare a record and submit it to the licensing police authority. Within 05 working days from the date of receiving the record, the Ministry of Public Security shall consider deciding on the revocation or suspension of the license for export and import of cybersecurity products. The revocation decision shall be sent to the customs authority. Upon the issuance of the revocation decision, the exporter/importer shall recall the cybersecurity products specified in the revocation decision and must not continue importing or exporting those products.

Chapter III

RESPONSIBILITIES OF MINISTRIES, MINISTERIAL AGENCIES, PROVINCIAL PEOPLE'S COMMITTEES, ORGANIZATIONS, AND ENTERPRISES

Article 16. Responsibility of enterprises, organizations

Enterprises and organizations have the responsibility to:

- 1. Regularly and continuously maintain the eligibility during the provision of cybersecurity products and services; for cybersecurity supervision service providers: maintain connection and exchange supervision information with the national cybersecurity protection system of the Ministry of Public Security during the provision of supervision services; for cybersecurity products specified in points a, b, c, and d, Clause 4, Article 3 of this Decree: organize the destruction when damaged or no longer used for the tasks of the Ministry of Public Security or the Ministry of National Defense.
- 2. Pay fees for the issuance of licenses for cybersecurity product/service provision and fees for the issuance of licenses for export/import of cybersecurity products in accordance with regulations.

3. Holders of licenses for cybersecurity product/service provision shall submit ad hoc reports upon request and annual reports on cybersecurity product/service provision to the Ministry of Public Security using Form No. 09 in Appendix I enclosed herewith. The reporting period for annual reports is from January 1 to December 31; the deadline for report submission is before January 31 of the following year.

4. In the case where an organization/enterprise temporarily suspends its operations, it must submit a written notice to the authority licensing cybersecurity product/service provision within 10 working days from the date of temporary suspension.

5. Comply with inspections and the handling of violations by the police authority and competent regulatory bodies.

Article 17. Responsibilities of Ministry of Public Security

The Minister of Public Security shall be held accountable to the Government of Vietnam for performing unified state management of cybersecurity product and service provision as follows:

1. Lead and cooperate with ministries and central departments in managing business activities in cybersecurity products and services in accordance with this Decree and relevant legislative documents; decentralize and delegate authority in managing business activities in cybersecurity products and services in accordance with law.

2. Promulgate standards and technical regulations in cybersecurity; formulate an electronic information database system to serve the work and carry out administrative procedures related to business activities in cybersecurity products and services.

3. Lead and cooperate with ministries and agencies to carry out and guide inspection work in accordance with Article 19 of this Decree, settle complaints and denunciations, and prevent, detect, fight, and handle violations against regulations on business of cybersecurity products and services.

Article 18. Responsibilities of ministries, ministerial-level agencies, and People's Committees of provinces

Within the scope of their functions, tasks, and powers, ministries, ministerial-level agencies, and People's Committees of provinces are responsible for cooperating with the Ministry of Public Security in performing state management in provision of cybersecurity products and services.

Article 19. Inspection

1. The comprehensive inspections of compliance with regulations on cybersecurity product/service provision shall be conducted no more than once a year, including inter-agency inspections, except in cases of violation detection.

Ad hoc inspections shall be conducted when a business establishment is found to have committed or has signs of committing violations against regulations on cybersecurity product/service provision; when there are complaints or denunciations from organizations or individuals regarding violations against regulations on cybersecurity product/service provision; or to improve the security and order enforcement as directed by written instructions from competent authorities.

2. Inspection content:

- a) Inspect documents in the legal dossiers; compare the business scope stated in the license for cybersecurity product/service provision, license for export and import of cybersecurity products against its actual operational activities;
- b) Inspect compliance with regulations in this Decree and other relevant legislative documents;
- c) Upon conclusion of the inspection, a record must be made (according to the form prescribed by the Minister of Public Security), clearly stating the results, existing shortcomings, or violations (if any).

3. Inspection authority:

- a) The Ministry of Public Security shall conduct annual inspections and ad hoc inspections as specified in Clause 1 of this Article;
- b) People's Committees of provinces or higher shall conduct inspect organizations and enterprises within their management areas when detecting any violations/signs of violations against regulations on cybersecurity product/service provision; upon receiving complaints or denunciations from organizations or individuals related to security and order at organizations and enterprises within their management areas. After inspection, written notices of the inspection results and violation handling shall be sent to the Ministry of Public Security.

4. Violations detected during inspections shall be handled in accordance with the law.

Chapter IV

IMPLEMENTATION PROVISIONS

Article 20. Effect

This Decree comes into force as from August 19, 2026.

Article 21. Transitional provisions

1. For contracts for cybersecurity product/service provision that were signed and valid prior to the effective date of this Decree, enterprises may continue to execute the contents of such contracts.

2. Applications for issuance, replacement, amendments, reissuance, or renewal received by the Ministry of Public Security prior to July 01, 2026, but not yet settled, shall be processed in accordance with the procedures and conditions specified in this Decree.

Article 22. Implementation

1. The Minister of Public Security shall urge, inspect, and guide the implementation of this Decree.
2. Ministers, heads of ministerial-level agencies, and chairpersons of People's Committees of provinces shall implement this Decree.

**ON THE BEHALF OF THE
GOVERNMENT OF VIETNAM
PP. PRIME MINISTER
DEPUTY PRIME MINISTER**

Pham Gia Tuc

*This translation is made by **THƯ VIỆN PHÁP LUẬT**, Ho Chi Minh City, Vietnam and for reference purposes only. Its copyright is owned by **THƯ VIỆN PHÁP LUẬT** and protected under Clause 2, Article 14 of the Law on Intellectual Property. Your comments are always welcomed*