Measures for Cyberspace Security Supervision and Inspection by Public Security Organs[1]

Issuing Authority: **Ministry of Public Security of the People's Republic of China**

Document Number: **Ministry of Public Security Order No. 176**

Adoption Date: **1 July 2026**

Promulgation Date: **6 August 2026**

Publication Date: **7 August 2026**

Effective Date: **1 October 2026**

Order of the Ministry of Public Security of the People's Republic of China No. 176

The Measures for Cyberspace Security Supervision and Inspection by Public Security Organs, adopted at the second executive meeting of the Ministry of Public Security on 1 July 2026, are hereby promulgated and shall enter into force on 1 October 2026.

Wang Xiaohong, Minister

6 August 2026

[1] Translated by Health Law Asia – Pharmaceutical, Medical Device, and Cosmetics Law.

Measures for Cyberspace Security Supervision and Inspection by Public Security Organs

Article 1

These Measures are formulated in accordance with the People's Police Law of the People's Republic of China, the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, the Regulations on the Security Protection of Critical Information Infrastructure, the Regulations on Network Data Security Management, the Measures for the Administration of Internet Information Services and other relevant laws and administrative regulations, in order to safeguard national security and the public interest, protect the lawful rights and interests of citizens, legal persons and other organisations, regulate cyberspace security supervision and inspection by public security organs, and prevent and combat cyber-related violations of law and crimes.

Article 2

These Measures apply to supervision and inspection conducted by public security organs in accordance with the law concerning the performance by network operators, data processors, personal information processors and other persons or entities of their cybersecurity, data security and information security obligations prescribed by laws and regulations.

For the purposes of these Measures, cyberspace security includes cybersecurity, data security and information security.

Article 3

Public security organs shall conduct cyberspace security supervision and inspection under the leadership of the Central Cyberspace Affairs Commission and other relevant bodies, adhere to the policy of law-based and scientifically grounded administration and of safeguarding and promoting development, strictly observe their statutory powers and procedures, improve law enforcement methods, and work with the relevant competent departments to establish and improve mechanisms for cooperation and coordination in cyberspace security supervision and inspection. Where a competent sectoral department exists, routine on-site inspections shall, in principle, be conducted primarily by that department.

Public security organs shall establish and implement a cyberspace security supervision and inspection system in accordance with the principles of tiered and categorised administration and other relevant principles, and shall voluntarily accept supervision by those subject to inspection and by the public.

Article 4

Public security organs shall conduct online patrols of the cyberspace security of persons and entities subject to inspection within their jurisdiction, using methods such as patrols of online information, testing of content review capabilities and vulnerability scanning that do not affect normal business operations or cyberspace security, in order to identify risks and vulnerabilities. Where content review capabilities are to be tested, the person or entity subject to inspection shall be notified of the timing, scope and other relevant matters three working days in advance.

Public security organs at the level of a city divided into districts or above may conduct remote testing of network facilities and information systems within their jurisdiction, other than critical information infrastructure, through vulnerability probing, penetration testing and other methods. They shall notify the person or entity subject to inspection of the timing, scope and other relevant matters three working days in advance, shall not interfere with or disrupt the normal operation of its network facilities or information systems, and shall inform the cyberspace affairs department and the competent sectoral department at the same level. Vulnerability probing, penetration testing and similar activities involving basic telecommunications networks shall be conducted in accordance with the Regulations on the Security Protection of Critical Information Infrastructure and other relevant provisions.

Risks and vulnerabilities identified through online patrols or remote testing shall be verified. Where necessary, offline verification shall be conducted through on-site inspections or other means.

Article 5

On-site cyberspace security inspections shall be conducted by public security organs at or above the county level at the location of the operating organisation of the person or entity subject to inspection. Where the person subject to inspection is an individual, the inspection shall be conducted by the public security organ at the individual's habitual residence.

The location of the operating organisation referred to in the preceding paragraph means the operator's actual principal place of operation, the location of its management organisation or network facilities, its place of business registration, or another such location. Where public security organs dispute jurisdiction over supervision and inspection, their common superior public security organ shall designate the organ responsible.

Superior public security organs shall provide guidance on and supervise inspections conducted by subordinate public security organs. Where necessary, they may conduct supervision and inspection at a higher level or organise the relevant public security organs to do so.

Article 6

As required to safeguard cyberspace security, public security organs shall conduct supervision and inspection of the following persons and entities in accordance with the law:

(1) Internet service providers providing Internet access, data centres, content delivery, domain name services, information services or other such services;

(2) Providers of public Internet access services;

(3) Network operators and those responsible for constructing and maintaining their networks;

(4) Critical information infrastructure operators and those responsible for constructing and maintaining their infrastructure;

(5) Providers of network products and services;

(6) Data processors;

(7) Personal information processors;

(8) Other persons and entities that may be subject to supervision and inspection in accordance with the law.

Priority shall be given to the supervision and inspection of persons and entities that have experienced cybersecurity, data security or other such incidents, or that have received administrative penalties for failure to perform statutory cybersecurity, data security or information security obligations and have not made the required rectifications.

Article 7

Public security organs shall supervise and inspect the performance of statutory cybersecurity, data security and information security obligations by persons and entities subject to inspection, focusing on the following matters:

(1) Whether network-connected organisations have completed the required filing formalities and reported basic information on connected organisations and users and changes thereto in accordance with the law;

(2) Whether cybersecurity, data security and information security management rules and operating procedures have been formulated and implemented in accordance with the law;

(3) Whether user registration information and Internet access logs have been recorded and retained in accordance with the law;

(4) Whether security protection obligations under the cybersecurity multi-level protection scheme, including classification and filing, level-based assessment, construction and rectification, and self-inspection, have been performed in accordance with the law;

(5) Whether critical information infrastructure security protection obligations have been performed in accordance with the law;

(6) Whether technical measures to prevent computer viruses, cyberattacks, network intrusions and other such threats have been adopted in accordance with the law;

(7) Whether appropriate rectification measures have been taken in accordance with the law to address cybersecurity vulnerabilities and weaknesses and eliminate risks;

(8) Whether preventive measures have been taken in accordance with the law in public information services against information whose publication or transmission is prohibited by laws or administrative regulations;

(9) Whether primary responsibility for algorithm security has been fulfilled and sound management rules and technical measures for algorithmic recommendations have been established in accordance with the law;

(10) Whether data security and personal information protection obligations have been performed in accordance with the law;

(11) Whether technical support and assistance have been provided in accordance with the law to public security organs in safeguarding national security, preventing and

investigating terrorist activities, investigating crimes and performing other such duties.

Article 8

During major national security protection operations, public security organs shall conduct targeted supervision and inspection of network operators, data processors and personal information processors associated with those operations, focusing on the following matters:

(1) Whether the work plans required for the major security protection operations have been formulated, responsibilities for security clearly allocated and security management personnel designated;

(2) Whether cybersecurity, data security and information security risk assessments have been organised in accordance with the law and corresponding risk control measures adopted to address security vulnerabilities and weaknesses;

(3) Whether cybersecurity, data security and information security emergency response plans have been formulated and emergency drills conducted, and whether relevant emergency response facilities are complete and effective;

(4) Whether other cybersecurity, data security and information security precautions required for the major security protection operations have been adopted in accordance with the law;

(5) Whether cybersecurity, data security and information security incidents and their handling have been reported in accordance with the law.

Cyberspace security supervision and inspection of key targets for protection against terrorist attacks shall be conducted in accordance with the preceding paragraph.

Article 9

Routine on-site cyberspace security inspections by public security organs shall be conducted under the overall coordination of the national cybersecurity, data security and other relevant mechanisms. Cooperation, coordination and information exchange shall be strengthened, and the frequency, scope and methods of on-site inspections shall be determined reasonably, avoiding duplicate and overlapping inspections and minimising the burden on those subject to inspection.

For network operators classified at Level 3 or above under the cybersecurity multi-level protection scheme and critical information infrastructure operators, one routine on-site inspection shall be conducted each year. Where another competent department has already conducted an on-site inspection during that year, public security organs shall reuse the relevant inspection results and shall not conduct a duplicate on-site inspection.

Supervision and inspection conducted by public security organs to investigate and handle cyberspace security cases and incidents, or targeted supervision and inspection conducted for major security protection operations or other such purposes, shall be undertaken promptly in accordance with their statutory duties and procedures.

Article 10

Where the Ministry of Public Security arranges routine on-site inspections involving multiple industries and departments, it shall submit the arrangements to the Central Cyberspace Affairs Commission for approval. Matters involving data security shall be handled under the overall guidance of the national coordination mechanism for data security work and in accordance with the relevant requirements. Matters involving content orientation management, online ideological security or related work shall be handled under the overall guidance of the department responsible for ideological affairs and in accordance with the relevant requirements.

Routine on-site inspections of basic telecommunications networks shall be organised and conducted by public security organs at the level of a city divided into districts or above. For routine on-site inspections of cyberspace security in telecommunications, energy, transport, water conservancy, finance, defence-related science and technology industries and other such sectors, the cyberspace affairs department and the competent sectoral department shall be notified five working days in advance. Where those departments request a joint inspection, public security organs shall conduct the inspection jointly with them.

Public security organs shall promptly inform the cyberspace affairs department and the competent sectoral department at the same level of relevant circumstances concerning on-site inspections.

Article 11

On-site cyberspace security inspections by public security organs shall be conducted by no fewer than two people's police officers, who shall present their people's police identification cards and a supervision and inspection notice issued by a public security organ at or above the county level.

Article 12

In conducting on-site cyberspace security inspections, public security organs may take the following measures:

(1) Enter business premises, computer rooms and workplaces;

(2) Question the person in charge or cybersecurity, data security or information security management personnel of the person or entity subject to inspection, and require explanations concerning matters under supervision and inspection;

(3) Inspect and copy information relating to matters under supervision and inspection;

(4) Examine the operation of technical security protection measures;

(5) Conduct technical testing, including vulnerability probing and penetration testing.

Article 13

In conducting cyberspace security supervision and inspection, public security organs may engage cybersecurity service institutions or specialised personnel with the requisite technical capabilities to provide technical support and shall file the engagement with the public security organ at the next higher level. Those institutions or personnel shall conduct supervision and inspection under the direction of people's police officers and shall undertake, through written undertakings signed with the person or entity subject to inspection or other means, to keep confidential trade secrets, personal privacy, personal information and other such matters learned during the inspection.

Where a public security organ inspecting critical information infrastructure genuinely needs to engage a cybersecurity service institution or specialised personnel to provide technical support, it shall inform the competent sectoral department.

Public security organs shall conduct background checks on cybersecurity service institutions and their personnel participating in vulnerability probing and penetration testing and shall exercise security management throughout the process.

Article 14

Public security organs shall conduct cyberspace security supervision and inspection objectively and impartially. They shall not charge those subject to inspection or require them to purchase or use designated products or services.

Article 15

Public security organs conducting on-site cyberspace security inspections shall prepare a supervision and inspection record, which shall be signed by the people's police officers conducting the inspection and by the person in charge or cybersecurity management personnel of the person or entity subject to inspection. Where the latter objects to the record, it shall be permitted to provide an explanation. Where it refuses to sign, the officers shall note the refusal in the record.

Public security organs conducting remote testing, including vulnerability probing and penetration testing, shall prepare a supervision and inspection record, which shall be signed by the people's police officers conducting the inspection.

Where cybersecurity service institutions or specialised personnel are engaged to provide technical support, the technical support personnel shall also sign the record.

Documents and materials generated during supervision and inspection shall be compiled into files and archived in accordance with the applicable provisions.

Article 16

Where a public security organ discovers cyberspace security risks or vulnerabilities during supervision and inspection, it shall urge and guide the person or entity inspected to take measures to eliminate them and shall note this in the supervision and inspection record.

Where a person or entity inspected fails to perform cybersecurity, data security or information security obligations in accordance with the law or is otherwise in breach, the public security organ shall, within its remit, pursue legal liability in accordance with the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, the Regulations on the Security Protection of Critical Information Infrastructure, the Regulations on Network Data Security Management, the Measures for the Administration of Internet Information Services, the Measures for the

Administration of Security Protection of Computer Information Networks Connected to the Internet and other laws and regulations.

Article 17

Where a public security organ discovers cyberspace security risks or vulnerabilities during supervision and inspection that do not yet constitute a violation of law or a criminal offence, it may issue an advisory or public notice in accordance with the following procedures:

(1) A public security organ at or above the county level may issue a public security advisory letter to the person or entity inspected, urging it to take security precautions;

(2) A public security organ at the level of a city divided into districts or above may issue a public security advisory letter to the competent sectoral department at the same level, urging it to strengthen cybersecurity, data security and information security supervision and administration in its sector;

(3) A public security organ at or above the provincial level may issue a public security notice to the public that does not identify any particular person or entity inspected, advising of cyberspace security risks and vulnerabilities and urging the public to take preventive measures.

Article 18

Where, during cyberspace security supervision and inspection, a public security organ discovers major security risks or vulnerabilities affecting networks classified at Level 3 or above under the cybersecurity multi-level protection scheme, critical information infrastructure or important data, it shall promptly inform the competent sectoral department and the cyberspace affairs department.

Where major cyberspace security risks or vulnerabilities are discovered in an important sector or in the local area that seriously threaten national security, public security or the public interest, the public security organ shall report them to the people's government and the superior public security organ, and issue public security advisories or notices in accordance with the applicable provisions.

Article 19

Where a public security organ at or above the provincial level discovers relatively significant security risks or the occurrence of a security incident in performing its

cybersecurity or information security supervision and administration duties, it may summon the legal representative or principal person in charge of the network operator concerned for a regulatory interview.

Where a public security organ at or above the county level discovers relatively significant security risks in data processing or personal information processing activities, or the occurrence of a data security or personal information security incident, in performing its data security supervision and administration duties, it may summon the relevant organisations or individuals for a regulatory interview.

Those interviewed shall take rectification measures in accordance with the requirements of laws and administrative regulations to eliminate cyberspace security risks and vulnerabilities.

Article 20

Public security organs and their staff, and cybersecurity service institutions and specialised personnel engaged to provide technical support, shall keep confidential state secrets, work secrets, trade secrets, personal privacy and personal information learned during supervision and inspection, and shall not disclose, sell or unlawfully provide them to others.

Information and materials obtained during supervision and inspection may be used only as necessary to safeguard cyberspace security, shall not be used for any other purpose and shall not be unlawfully provided to other organisations or individuals. Upon completion of supervision and inspection, participating cybersecurity service institutions and their staff shall hand over the information and materials obtained to the public security organ for safekeeping, or delete or destroy them as required by that organ.

Article 21

Where public security organs or their staff neglect their duties, abuse their powers or practise favouritism or fraud in cyberspace security supervision and inspection, the persons directly in charge and other directly responsible persons shall be subject to disciplinary sanctions in accordance with the law. Where a criminal offence is constituted, criminal liability shall be pursued in accordance with the law.

Article 22

Cybersecurity service institutions or specialised personnel engaged by public security organs to provide technical support shall be subject to penalties in accordance with the law if they engage in activities that endanger cyberspace security, including unlawfully intruding into the networks of those subject to inspection, interfering with normal network functions or stealing network data, or if they steal or otherwise unlawfully obtain, sell or provide state secrets, work secrets, trade secrets, personal privacy or personal information learned in the course of their work. Where a criminal offence is constituted, criminal liability shall be pursued in accordance with the law.

Article 23

These Measures shall enter into force on 1 October 2026. The Provisions on Internet Security Supervision and Inspection by Public Security Organs, issued on 15 September 2018 under Ministry of Public Security Order No. 151, shall be repealed simultaneously.

Source: Ministry of Public Security Order No. 176; official reproduction by the Chifeng Municipal Public Security Bureau.

https://www.mps.gov.cn/n6557558/c10576497/content.html

https://gaj.chifeng.gov.cn/zwgk/zfxxgk/fdzdgknr/zcfg/202609/t20260902_2812754.html