Technical Review Guidelines for Cybersecurity of Medical Devices (Second Edition) [1]

Authority: **Center for Medical Device Evaluation (CMDE), National Medical Products Administration (NMPA)**

Promulgation Date: September 8, 2020

Effective Date: September 8, 2020

These Guidelines are intended to assist registrants in standardizing the cybersecurity lifecycle processes of medical devices and in preparing cybersecurity-related registration documents. They also aim to standardize the technical review requirements for medical device cybersecurity and provide reference for system audits of medical device software and quality management software.

These Guidelines set forth general requirements for the cybersecurity of medical devices. Registrants shall submit cybersecurity registration materials based on the specific characteristics of their medical device products and assess the applicability of the specific contents of these Guidelines. If certain contents are deemed not applicable, the reasons shall be stated in detail. Registrants may also adopt alternative approaches that meet regulatory requirements, provided that comprehensive supporting research materials are submitted.

These Guidelines are formulated based on current understanding and technological capabilities, taking into account relevant international regulations, standards, and technical reports within the existing regulatory framework. As understanding and technological capabilities continue to improve, and as the regulatory framework evolves, relevant content will be revised accordingly.

These Guidelines serve as a reference for registrants, reviewers, and inspectors. They do not include administrative matters involved in the review and approval process and are not legally binding regulations. They shall be applied on the premise of compliance with relevant regulatory requirements.

These Guidelines are to be used as a supplement to the *Technical Review Guidelines for Medical Device Software* (hereinafter referred to as the "Software Guidelines") and should be applied in conjunction with the relevant requirements of the Software Guidelines. These Guidelines provide general principles for the cybersecurity of medical devices. Other product-specific cybersecurity guidance documents may adjust, revise, and supplement these Guidelines as appropriate.

Chapter I. Scope of Application

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

These Guidelines apply to cybersecurity registration submissions for medical devices, including Class II and Class III standalone software products and medical devices containing software components that possess functionalities such as electronic data exchange, remote control, or user access.

"Network" herein includes wired and wireless networks. "Electronic data exchange" refers to one-way or two-way data transmission over networks or storage media. "Remote control" includes real-time or non-real-time control via network. "User access" includes software user interfaces (including standalone software and software components) and human-machine interaction via electronic interfaces (including network and electronic data exchange interfaces).

Chapter II. Cybersecurity Fundamentals

(1) Basic Concepts of Cybersecurity

1. Cybersecurity of Medical Devices

Cybersecurity for medical devices refers to the state in which the device and its associated data are protected from unauthorized activities, with associated risks to confidentiality, integrity, and availability (commonly known as the CIA triad) maintained at acceptable levels throughout the product lifecycle.

Confidentiality refers to the characteristic whereby information is not accessed or disclosed to unauthorized entities (including individuals or organizations), i.e., only authorized users may access and use the device and related data at authorized times in authorized ways.

Integrity refers to the characteristic whereby data are not modified (including deleted or added) in an unauthorized manner during creation, transmission, storage, or display. This ensures that device data are accurate, complete, and untampered.

Availability refers to the characteristic whereby information can be accessed and used in a timely manner by authorized entities, i.e., the device and its data are available for use as intended.

In addition to the CIA triad, cybersecurity for medical devices also encompasses authenticity, non-repudiation, accountability, and reliability:

Authenticity ensures that an entity is what it claims to be.

Non-repudiation ensures that entities cannot deny having performed certain actions or events.

Accountability refers to the traceability of actions and outcomes performed by entities.

Reliability means that the operations and outcomes of an entity are consistent with expectations.

The CIA characteristics are interdependent and can be mutually constraining. Enhancing one attribute may weaken another. For instance, increasing availability may reduce confidentiality or integrity. Registrants shall balance these attributes in accordance with the device's intended use, usage scenarios, and core functions to determine specific cybersecurity requirements.

Although distinctions exist among the concepts of information security, cybersecurity, and data security in terms of definitions and scope, this document does not distinguish them strictly.

From the perspective of medical device software, all such concerns are collectively addressed under the term "cybersecurity," which integrates considerations of information and data security.

2. Medical Device-Related Data

Medical device-related data may be categorized into medical data and device data.

Medical data refers to data (including logs) used or generated by the medical device in connection with medical activities. From the perspective of personal information protection, medical data are divided into:

Sensitive medical data: containing personally identifiable information.

Non-sensitive medical data: containing no personally identifiable information.

Personal information includes data that can identify a specific natural person alone or in combination with other information, such as name, date of birth, ID number, biometric data (including facial images), address, and phone number. Sensitive medical data falls under the broader category of health data, which encompasses private data reflecting an individual's physical and psychological condition across healthcare and wellness domains.

Device data refers to information describing the operational status of the medical device, used for monitoring, controlling, or maintaining the device. Such data shall not contain personal information.

Registrants shall determine cybersecurity requirements for medical device data based on data types, functionalities, and purposes, ensuring sensitive data is protected against leakage, misuse, or tampering, and that medical and device data are effectively segregated.

3. Electronic Interfaces

Electronic interfaces of medical devices include network interfaces and electronic data exchange interfaces.

Network interface: enables electronic data exchange or remote control via networks. Relevant technical parameters include network type (wired or wireless), physical interface (e.g., electrical or optical ports), data protocols (standard or proprietary), remote control mode (real-time or non-real-time), and performance indicators (e.g., port specifications, transmission rate, bandwidth). Wireless networks may include Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), RF, infrared, etc. Wireless medical devices not using general-purpose communication technologies must comply with Chinese radio frequency management regulations.

Electronic data exchange interface: enables data exchange via non-network electronic interfaces (e.g., serial, parallel, USB, video, or audio interfaces) or storage media (e.g., CDs, external hard drives, USB drives).

Technical specifications for other electronic interfaces may refer to those for network interfaces. Data storage parameters include medium type, file format (standard or proprietary), compression method (lossy or lossless), and performance indicators (e.g., transmission speed,

capacity). Standard formats refer to widely accepted data storage specifications, with considerations for file integrity.

Registrants shall determine cybersecurity requirements for both internal and external electronic interfaces, based on interface type, method, and technical attributes.

(2) Cybersecurity Capabilities

In accordance with relevant cybersecurity standards and technical reports, the cybersecurity capabilities of medical devices include:

1-Automatic Logout – Prevents unauthorized access during idle periods.

2-Audit – Allows auditability of user activity.

3-Authorization – Confirms user authorization status.

4-Cybersecurity Configuration – Configurable security features based on user needs.

5-Patch Updates – Authorized personnel can install or upgrade security patches.

6-Data De-identification – Supports anonymization or removal of personal identifiers.

7-Backup & Disaster Recovery – Enables recovery from data/hardware/software damage.

8-Emergency Access – Allows access in predefined emergency scenarios.

9-Data Integrity & Authenticity – Ensures data are unaltered and from legitimate sources.

10-Malware Protection – Detects and mitigates malicious software threats.

11-Node Authentication – Authenticates network nodes.

12-User Authentication – Authenticates authorized users.

13-Physical Protection – Prevents unauthorized physical access.

14-COTS Software Maintenance – Maintains cybersecurity for commercial off-the-shelf software throughout lifecycle.

15-System Hardening – Defends against network attacks and malware.

16-Cybersecurity Guidance – Provides users with guidance on secure usage.

17-Storage Confidentiality & Integrity – Protects stored data from unauthorized access.

18-Transmission Confidentiality & Integrity – Secures data during transmission.

19-Remote Access & Control Security – Secures remote functionalities.

20-Denial-of-Service Resistance – Withstands DoS attacks.

Registrants shall assess the applicability of these capabilities to their product. If applicable, they shall specify implementation methods and define the strength level based on the device's risk profile (e.g., stronger authentication methods like biometrics for high-risk devices). If not applicable, clear rationale shall be documented.

(3) Cybersecurity Incident Response

Design and development can only address known vulnerabilities. Post-market, devices remain susceptible to unknown cybersecurity threats, potentially resulting in loss of access, data breaches, or data tampering — posing risks to patient safety or privacy.

Given the complexity, scope, propagation, and suddenness of such events, stringent post-market surveillance is essential. Registrants shall establish a cybersecurity incident response mechanism aligned with applicable standards to ensure product safety and patient privacy.

Registrants shall:

1-Develop an incident response plan covering planning, detection/reporting, assessment/decision-making, implementation, and improvement.

2-Establish a response team comprising management, planning, monitoring, response, execution, and analysis groups; external experts may be engaged as needed.

3-Classify incidents based on severity, urgency, and impact scope.

4-Validate response measures via risk management and maintain documentation.

5-Promptly notify users of response measures during incidents.

6-Report severe incidents to regulatory authorities per adverse event or recall regulations, and if applicable, report to national cybersecurity authorities.

(4) Cybersecurity Updates

Fundamental Concepts

-Cybersecurity updates for medical devices include:

-Functional updates (enhancements)

-Patch updates (corrections)

Updates are categorized based on their impact:

1-Major cybersecurity updates: Affect device safety or effectiveness. These require a formal change application.

2-Minor cybersecurity updates: Do not affect safety or effectiveness (including minor functional updates or patches). These are managed under the quality management system and do not require regulatory change applications, though they must be reported in the next application cycle.

Note: All updates related to recalls are considered major and handled under applicable recall regulations.

The most conservative principle applies — if a major and minor update occur simultaneously, treat the update as major. Software versioning rules must reflect update types and distinguish between major and minor updates accordingly.

Chapter III. Fundamental Principles

(1) Cybersecurity Positioning

With the development of network technologies, an increasing number of medical devices now feature network connectivity to enable electronic data exchange or remote control. While these capabilities enhance the quality and efficiency of healthcare services, they also expose the devices to cybersecurity threats. Cybersecurity issues in medical devices not only risk compromising patient privacy but may also result in unintended device operations, potentially leading to patient or user injury or even death. Therefore, cybersecurity is a critical component of the safety and effectiveness of medical devices.

Information sharing is a fundamental principle in ensuring medical device cybersecurity. Timely access to information on cybersecurity vulnerabilities, incidents, and related matters aids in the identification, assessment, and mitigation of cybersecurity risks, thus ensuring the safety and effectiveness of medical devices and the continuity of medical operations. All stakeholders are encouraged to proactively share cybersecurity-related information throughout the entire lifecycle of medical devices. Registrants should actively utilize vulnerability disclosure mechanisms to strengthen cybersecurity in device design, development, and post-market monitoring. They should also conduct regular cybersecurity risk management activities based on vulnerability information disclosed by the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and the National Vulnerability Database of Information Security (CNVD).

Medical device cybersecurity requires the joint efforts and close collaboration of registrants, users (including medical institutions and individuals), IT service providers, and other stakeholders. Although medical devices are often connected with unintended equipment or systems during actual use—posing challenges for registrants in ensuring cybersecurity—this does not absolve registrants of their cybersecurity responsibilities. Registrants must ensure the cybersecurity of the devices themselves, clearly define the expected network environment and electronic interface requirements, and continually monitor, assess, respond to, and share cybersecurity risks. They must work closely with other stakeholders to maintain the safety and effectiveness of medical devices.

Medical device cybersecurity also constitutes a key part of the national cybersecurity strategy. Therefore, it must comply with relevant laws, regulations, and departmental rules. Registrants must continuously monitor legislative and regulatory developments and ensure compliance with applicable requirements.

(2) Risk-Oriented Approach

Taking into account industry development levels and risk-based management principles, different levels of cybersecurity risk for medical devices correspond to different quality control requirements throughout the product lifecycle and different registration documentation requirements.

Although cybersecurity risks differ from software risks, cybersecurity risk is a significant subset of software risk. In general, cybersecurity risk levels may refer to software safety levels; that is, the cybersecurity risk level of a medical device is usually aligned with the safety level of its

associated software. In exceptional cases, the cybersecurity risk level may be lower than the software risk level, in which case the rationale must be clearly explained, and relevant registration documentation must be submitted in accordance with the revised software safety level.

Cybersecurity risk assessments for medical devices should consider the intended use, usage scenarios, and core functions of the devices—particularly the usage scenarios. Network environments vary significantly across different usage scenarios, which may impact cybersecurity differently. Therefore, for devices intended for multiple usage scenarios, registrants must ensure cybersecurity in each individual scenario.

Typical cybersecurity risk management activities for medical devices include:

-Identifying assets (physical or digital entities of value to individuals or organizations),

-Identifying threats (potential causes of unwanted incidents that may harm individuals or organizations),

-Identifying vulnerabilities (weaknesses in assets or safeguards that may be exploited by threats),

-Assessing the impact and likelihood of threats and vulnerabilities affecting medical devices and patients,

-Determining the risk level and implementing adequate, effective, and appropriate risk control measures.

The remaining risks should be evaluated against risk acceptance criteria. Registrants may refer to relevant standards and technical reports on both medical device and cybersecurity risk management to perform effective risk control.

(3) Lifecycle Management

Like software, registrants should maintain continued focus on cybersecurity throughout the entire lifecycle of medical devices, including but not limited to design and development, manufacturing, distribution, deployment, maintenance, and post-market surveillance.

Before market launch, cybersecurity quality control should be conducted in accordance with quality management system requirements and the characteristics of the medical device to ensure its safety and effectiveness. After launch, registrants should evaluate update requests, conduct verification and validation, manage risks, and inform users in line with cybersecurity update developments to maintain continued safety and effectiveness. Additionally, registrants should establish an incident response process for cybersecurity events, conduct regular vulnerability risk assessments, and promptly inform users of relevant information and response measures.

Moreover, good engineering practices from the field of information security may be adopted to further improve medical device cybersecurity management and ensure device safety and effectiveness.

Chapter IV. Cybersecurity Lifecycle Process

The cybersecurity lifecycle process, as an important component of the software lifecycle process, should take into account the quality control requirements for medical device cybersecurity within the medical device software lifecycle process. Specific requirements can be found in Chapter 6 of the Software Guiding Principles as well as the *Medical Device Production Quality Management Practice Appendix for Standalone Software* and the *On-Site Inspection Guiding Principles for Standalone Software under the Medical Device Production Quality Management Practice*.

The registrant may refer to relevant standards and technical reports in the field of information security to improve the quality control requirements of the cybersecurity lifecycle process.

Chapter V. Technical Considerations

(1) Off-the-shelf Software

Off-the-shelf software also presents cybersecurity issues. The registrant should establish a cybersecurity update and maintenance process for off-the-shelf software in accordance with the requirements of the quality management system, and promptly inform users of cybersecurity-related information and corresponding measures related to the off-the-shelf software.

At the same time, cybersecurity quality control work should be carried out based on the type of relationship between the off-the-shelf software and the medical device software. For off-the-shelf software components—that is, off-the-shelf software that constitutes a part of the medical device software—the focus should be on the impact of its cybersecurity issues on the effectiveness of the medical device's use. For external software environments—that is, off-the-shelf software that constitutes a part of the operating environment of the medical device software—the focus should be on the impact of its cybersecurity patches on the safety and effectiveness of the medical device. It should be noted that cybersecurity patches are considered design changes and must undergo verification and validation.

(2) Cross-border Transfer of Medical Data

According to relevant provisions of the *Cybersecurity Law of the People's Republic of China*, personal information and important data collected and generated within the territory of China must be stored within the territory of China. If it is truly necessary to provide such data overseas due to business needs, a security assessment must be conducted in accordance with the measures formulated by the national cybersecurity authority in conjunction with relevant departments under the State Council. The *Administrative Measures for Population Health Information (Trial)* also stipulates that population health information must not be stored on servers located outside of China, nor be hosted or leased on overseas servers.

Medical data is classified as important data—especially sensitive medical data that contains personal information—and therefore, cross-border transfer of medical data must comply with the relevant provisions of the *Measures for the Security Assessment of Personal Information and Important Data Outbound Transfer*.

(3) Remote Maintenance

Medical devices with remote maintenance functions are capable of accessing and using device data. Although they may not directly involve medical data, if effective separation between device data and medical data is not achieved, there is a possibility of unauthorized access, use, and tampering of medical data. Meanwhile, the electronic interfaces used for remote maintenance are also subject to cybersecurity threats, which may affect the normal operation of the medical device and lead to harm or death of the patient as well as violation of privacy. In addition, if the medical device is unattended during the remote maintenance process, there may be a risk of unauthorized access and use of the medical device.

Therefore, the registrant should specify the implementation method of remote maintenance, the conditions of the electronic interfaces used, the content contained in the device data, the method of separation between device data and medical data, the cybersecurity assurance measures during the maintenance process, and other technical characteristics, and provide corresponding research materials and risk management documentation.

(4) Obsolete Equipment

The obsolete equipment referred to in this guiding principle refers to medical devices that cannot resist current cybersecurity threats through patch updates, compensatory controls, or other reasonable risk control measures. Because obsolete equipment cannot cope with current cybersecurity threats, the overall residual risk of the product cannot be reduced to an acceptable level, thereby reducing the safety and effectiveness of the medical device. Therefore, they should be promptly decommissioned and withdrawn from the market.

Given the extreme complexity of actual use conditions of medical devices, generally the determination of whether they fall under obsolete equipment can be based on two time points: discontinuation of sales and discontinuation of after-sales service:

-Medical devices that are still on the market are not considered obsolete equipment;

-Medical devices that are discontinued but after-sales service has not stopped:

If they cannot resist current cybersecurity threats through reasonable risk control measures, they are considered obsolete equipment;

If they can, they are not considered obsolete;

Medical devices for which after-sales service has stopped are all considered obsolete equipment.

For obsolete equipment, the registrant should carry out corresponding work in accordance with the requirements for software discontinuation/software withdrawal under the quality management system, as detailed in the *Medical Device Production Quality Management Practice Appendix for Standalone Software*.

For medical devices whose registration certificate has expired but after-sales service has not yet stopped, or those whose registration certificate is valid but have already been discontinued, the registrant should provide existing users with necessary cybersecurity-related information and countermeasures in accordance with the requirements of the quality management system,

to ensure the cybersecurity of the medical device. If the cybersecurity of the medical device cannot be ensured, it should be treated as obsolete equipment.

For medical devices with valid registration certificates and that are still on the market, if they cannot resist current cybersecurity threats through reasonable risk control measures, the registrant should formulate corresponding risk control measures in accordance with the requirements of the quality management system and apply for changes to the licensing items.

Chapter VI. Cybersecurity Research Documentation

(I) Cybersecurity Research Report for Self-Developed Software

The Cybersecurity Research Report for self-developed software applies to both initial release and redeployment. It must include basic information, implementation process, vulnerability assessment, and conclusion. The depth of each section depends on the software security level. If any requirement is not applicable, the reason must be stated. See Table 1.

1. Basic Information

(1) Software Information

Specify the name, model/specification, release version, and software security level of the medical device software. If the cybersecurity risk level is lower than the software risk level, provide the rationale and submit registration materials according to the revised security level.

(2) Data Architecture

For each usage scenario (including remote maintenance), provide the network environment and data flow diagrams, and describe the basic nature of device-related data and electronic interfaces. Indicate data types (sensitive or non-sensitive medical data, device data), details for each type (e.g., personal information, clinical data, device operational data), functions (e.g., uni- or bi-directional data exchange; real-time or non-real-time remote control), and purposes (e.g., clinical use, device maintenance). For electronic interfaces, describe for each network or data interface the intended user, usage scenario, purpose, data type, technical characteristics, and restrictions. Refer to Chapter II for technical detail requirements.

(3) Cybersecurity Capabilities

Based on the 20 cybersecurity capabilities in Chapter II, analyze applicability to each capability; where applicable, detail implementation; where not, explain why.

(4) Cybersecurity Patches

List all cybersecurity patches: specify name, full version, and release date for each.

(5) Security Software

List compatible or integrated security software (e.g., antivirus, firewall): name, model, full version, vendor, operating environment, and configuration requirements.

2. Implementation Process

(1) Risk Management

Provide cybersecurity risk analysis and risk management reports for the device (including remote maintenance), including original-language documents. Alternatively, medical device software risk docs may be used if they clearly note cybersecurity aspects.

(2) Requirements Specification

Provide original-language cybersecurity (and remote maintenance) requirements specification. If relying on general software specs, clearly mark cybersecurity-related requirements.

(3) Verification & Validation

Submit cybersecurity (and remote maintenance) test plans and reports, original-language. System-level software tests are acceptable if they clearly mark cybersecurity. – For security software compatibility, include compatibility test reports.– For standard protocols/formats, a declaration of conformity suffices; for proprietary protocols/formats, include integrity test summaries.– For real-time remote control, provide integrity and availability test reports.

– For medical wireless devices, include proof of compliance with telecommunications regulations.

(4) Traceability Analysis

Provide a traceability matrix linking cybersecurity capabilities, requirements, design specifications, test reports, and risk analysis.

(5) Update & Maintenance Plan

Minor risk level: include flowchart of cybersecurity update process with accompanying description.

Moderate or serious risk levels: in addition, include flowchart and description of incident response processes or submit a formal incident response plan.

If applicable, all risk levels must include remote maintenance process flowchart and description.

3. Vulnerability Assessment

-*Minor* risk: use CVSS to report total known vulnerabilities and residual vulnerabilities.

-*Moderate* risk: submit a self-assessment report on vulnerabilities using CVSS; specify known residual vulnerabilities with detail on content, impact, and risk acceptance, or provide a third-party vulnerability assessment.

-*Serious* risk: submit a report from a domestic third-party cybersecurity evaluation body, including a maintenance plan for any remaining vulnerabilities.

4. Conclusion

Summarize the regulatory compliance of the cybersecurity implementation and the results of vulnerability assessment, and conclude whether the device's cybersecurity meets requirements.

Table 1: Framework for Self-Developed Software Cybersecurity Research Report

Section	Minor	Moderate	Serious
Basic Info	Software info, basic security level	Same as minor	Same as minor
Data Architecture	Provide network & data flow diagrams	Same as minor	Same as minor
Cybersecurity Capabilities	Analyze applicability of 20 capabilities	Same as minor	Same as minor
Cybersecurity Patches	List patch details	Same as minor	Same as minor
Security Software	List details of security software	Same as minor	Same as minor
Implementation	Risk mgmt, requirements, testing, traceability	Same as minor	Same as minor
Update Plan	Update process flowchart	+ Incident response flowchart and/or plan	+ Incident response
Vulnerability Assessment	CVSS summary	Self-assessment or third-party report with detail on residual risks	Third-party report + maintenance plan
Conclusion	Compliance summary	Same as minor	Same as minor

(II) Cybersecurity Update Research Report for Self-Developed Software

This applies to subsequent releases involving cybersecurity functional updates or patch updates. See Table 2.

The Cybersecurity Functional Update Report covers minor to major functional changes or combined patch updates.

The Cybersecurity Patch Update Report applies to patch updates of device software, essential software, or external software environments, and includes sections on software info, patches, risk management, verification, traceability, update plan, vulnerabilities, and conclusion.

Table 2: Framework for Cybersecurity Functional Update Research Report

Section	Minor	Moderate	Serious
Basic Info	Specify version and changes	Same	Same
Data Architecture	Describe architectural changes	Same	Same
Cybersecurity Capabilities	Describe changes in capabilities	Same	Same
Cybersecurity Patches	List new patches	Same	Same
Security Software	Describe changes	Same	Same
Implementation	Risk mgmt for updates	Same	Same
Requirements Specs	Provide specs for updates	Same	Same
Testing	Provide test plans/reports for updates	Same	Same
Traceability	Provide traceability for updates	Same	Same
Update Plan	Include user notification plan	+ user notification + incident response summary	Same
Vulnerability Assessment	Provide known and residual counts	Self-assessment report or third-party	Third-party report
Conclusion	Compliance summary	Same	Same

(III) Cybersecurity Documentation for Off-the-Shelf Software

1. Off-the-Shelf Software Component Report

(a) Partial Use

If only portions are used, no separate cybersecurity report is needed. Instead, address the off-the-shelf component in the self-developed software report under relevant sections (software info, architecture, capabilities, patches, risk management, specs, testing, traceability, update plan, vulnerabilities, and conclusion). For functional updates, describe changes to the off-the-shelf component within the self-developed update report, and explain non-applicable sections. Patch updates are treated the same as for self-developed software.

(b) Full Use

If the entire off-the-shelf component is used as the medical device software, submit a standalone cybersecurity research report with content and level requirements identical to those for self-developed software, based on the component's security level. For updates, follow the same process as self-developed software feature or patch updates, describing changes or explaining non-applicability.

2. Cybersecurity Evaluation for External Software Environments

Evaluate cybersecurity and updates of the external software environment as part of general external environment assessment; requirements mirror those in Chapter VIII of the Software Guidance Principles.

Chapter VII. Registration Submission Requirements

(1) Product Registration

1. Software Research Documentation

Submit the proprietary cybersecurity research report and the external software environment assessment report. If using off-the-shelf components, submit corresponding documentation as per usage mode (see Chapter 6).

2. Instructions for Use

Must include cybersecurity details: Access control mechanism, Electronic interfaces and data types/technical features, Security configuration features, Data backup and disaster recovery, Operating environment (hardware, external software, network), Compatibility with security software and Update requirements for external software and security software.

(2) Change of Licensed Items

1. Software Research Documentation

Submit the impact assessment materials based on the type of cybersecurity update:

Functional Update: Submit functional update report (or full research report), and external software assessment.

Patch Only: Submit patch update report.

No Update: Provide a declaration of authenticity.

If using off-the-shelf software components, submit corresponding materials as outlined in Chapter 6.

2. Instructions for Use

Should reflect the changes in cybersecurity, if applicable.

(3) Renewal Registration

Cybersecurity documentation is not required.

The “model/spec version classification” in the product technical specification should include version naming rules that distinguish major and minor cybersecurity updates. If previous registration materials lack this info, it should be clearly stated in the “unchanged product declaration.”