ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 47496-2026

Cybersecurity technology - Security technical specification for computer BIOS

网络安全技术 计算机基本输入输出系统（BIOS）安全技术规范

Issued on: April 30, 2026 **Implemented on: November 1, 2026**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

5 General Rules

5.1 Architecture The BIOS is typically stored in non-volatile memory on the computer's motherboard and is responsible for the hardware initialization and configuration of the computing device, providing a basis for operation. The system provides a hardware abstraction interface to manage hardware resources and shield platform differences; it is responsible for booting the operating system and providing hardware support during operating system runtime. BIOS access services. The BIOS occupies a crucial position between the hardware platform and system software. During the computer startup process, the BIOS needs to access... Integrity measurement or signature verification methods are used to perform security verification on critical software such as loaded component drivers and operating system loader, achieving [the goal of] [security]. The security of the computer boot process. Security verification methods include, but are not limited to, trusted boot or secure boot. Figure 1 illustrates the BIOS in a computer. Location of hardware and software and their main functional modules.

5.2 Classification This document divides BIOS security requirements into Basic and Enhanced levels. Compared to the Basic level, the Enhanced level requires the addition of... The content is indicated in bold Song typeface within the main text. The BIOS security specification classification should comply with Appendix A, and user rights should comply with Appendix B.

6.1 Safety Function Requirements

6.1.1 Access Control Access control functions meet the following requirements.

a) The BIOS should not contain any functionality that allows access to computer resources by bypassing the BIOS security mechanisms; security mechanisms include, but are not limited to, [the following]. Limited to power-on passwords, access control, etc.

b) The BIOS should support setting a power-on password. If the power-on password verification fails, the operating system should not be booted.

c) In the context of internal computer use within an organization, the BIOS should at least support setting up two roles. system administrator and ordinary user. 1) The permissions for regular users are as follows:

---Should support viewing BIOS information, motherboard information, processor information, memory information, and hard drive information in the BIOS configuration interface. Information, system date and time;

---It should support setting and modifying the current password and power-on password for regular users;

---Users should not have permission to modify the log records of current regular users;

---Permission to modify the device's boot priority options should not be available. 2) The system administrator's permissions are as follows:

---Should support viewing BIOS information, motherboard information, processor information, memory information, and hard drive information in the BIOS configuration interface. Information, system date and time, and supports setting the system date and time.

---Should support viewing and setting device startup priority options.

---Should support setting and clearing the power-on password.

---Should support setting, modifying, and clearing system administrator passwords.

---It should support setting and clearing passwords for ordinary users.

---Where the hardware supports it, the computer terminal should support setting, modifying and clearing hard drive passwords.

6.2 Safety Assurance Requirements

6.2.1 Design and Development BIOS providers are designed and developed to meet the following requirements.

a) Coding principles such as minimum attack surface and minimum privileges should be followed;

b) Configuration management should be implemented for design documents, development documents, etc., and a configuration management list or corresponding procedure should be established to process changes to configuration items. Authorization and control;

c) Security flaws and vulnerabilities discovered should be patched during the development phase;

d) An emergency remediation security management process should be developed and implemented to promptly fix security defects and vulnerabilities that were not discovered during the development phase.

6.2.2 Production and Delivery The production and delivery of BIOS providers meet the following requirements.

a) The user-related human-computer interaction and access interfaces in the BIOS should be described;

b) All preset user types and their corresponding permissions should be described in the user manual;

c) A BIOS product manufacturing and service delivery process should be in place, with security checks and verifications implemented at critical stages;

d) A method for verifying the integrity of the delivered BIOS software should be provided;

e) User guides and other instructional documents should be provided.

6.2.3 Operation and Maintenance The operation and maintenance of the BIOS provider must meet the following requirements.

a) It should have a response mechanism for BIOS security flaws and vulnerabilities. Within the specified or contractually agreed period, it should address any BIOS product exposures. Respond to security flaws and vulnerabilities, and take timely remedial measures, including but not limited to vulnerability patching and security hardening solutions; and The relevant security risks should be promptly communicated to the BIOS supplier. (b) Within the stipulated or contractually agreed period, BIOS operation and maintenance work shall be carried out to ensure the BIOS itself during operation and maintenance. Data security is crucial for preventing data leaks, tampering, and damage.

c) Users should be informed of the update content, including changes, related security risks, and risk mitigation measures, before the BIOS update is implemented, and they should obtain the necessary information. Updates can only be implemented after the user grants their authorization and consent, and users can choose not to accept updates.

7.1.1 Test Environment

7.1.1.1 Hardware Environment The following hardware is required when performing BIOS testing.

a) Deploy the computer on which the BIOS to be tested is located. Important components required include, but are not limited to, the motherboard, CPU, memory, and storage devices. Peripherals, etc.

b) Firmware programmers, oscilloscopes, etc.

7.1.1.2 Software Environment The following software is required for BIOS testing.

a) Programming software;

b) Log capture and recording software, etc.

7.1.2 Access Control Testing Methods The testing methods, expected results, and result determination for access control are as follows:

a) The testing method is as follows: 1) Test whether the BIOS has access control enabled; if access control is enabled, unauthorized users should not be able to access the system. The BIOS is set not to boot the operating system. 2) Test if the BIOS can be set with a BIOS boot password. Using an incorrect BIOS boot password will prevent the operating system from booting. start up. 3) Test whether the BIOS can be configured with both system administrator and regular user roles. 4) Test whether the following conditions are met after logging in as a regular user.

---It should be able to display BIOS information, motherboard information, processor information, memory information, hard drive information, system date and time;

---Should be able to successfully set and modify the current power-on password and regular user password;

---Should only allow viewing of logs from the current regular user; When a regular user enters the BIOS configuration interface, they should only be able to view the device boot priority options and should not be able to modify them. The order of movement. 5) Test whether the following conditions are met after logging in as an administrator.

---It should be able to display BIOS information, motherboard information, processor information, memory information, hard drive information, system date and time.

---It should be possible to set the system date and time, and be able to modify them successfully.

---It should be possible to set a power-on password, and to modify and clear it.