

ICS 35.040
CCS A 90

GA

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GA/T 671-2006

**Information security technology - Technology requirement for
terminal computer system of security classified protection
(English Translation)**

Issued on: December 28, 2006

Implemented on: February 1, 2007

**Issued by: The Ministry of Public Security of the People's Republic of
China**

Table of Contents

Foreword...	4
Introduction...	5
1 Scope...	6
2 Normative references...	6
3 Terms, definitions and abbreviations...	6
3.1 Terms and definitions...	6
3.2 Abbreviations...	9
4 Technology requirements for security function...	9
4.1 Physical security...	9
4.1.1 Equipment security availability...	9
4.1.2 Equipment protection against theft and destruction...	9
4.1.3 High reliability of equipment...	10
4.2 Operational security...	10
4.2.1 System security detection and analysis...	10
4.2.2 Security audit...	11
4.2.3 Trusted chains...	14
4.2.4 Protection during operation...	15
4.2.5 Backup and fault recovery...	16
4.2.6 Trusted time stamp...	17
4.2.7 I/O interface configuration...	17
4.3 Data security...	17
4.3.1 Password support...	17
4.3.2 Identification and discrimination...	18
4.3.3 Discretionary access control...	21
4.3.4 Marks...	22
4.3.5 Mandatory access control...	23
4.3.6 Data privacy protection...	24
4.3.7 Data integrity protection...	25
4.3.8 Trust service...	25
4.3.9 Trusted path...	26
5 Classified requirements for security technology of terminal computer system...	26
5.1 Level I. User discretionary protection level...	26

5.1.1 Security functional requirements...	26
5.1.2 Security assurance requirements...	29
5.2 Level II. System audit protection level...	30
5.2.1 Security functional requirements...	30
5.2.2 Security assurance requirements...	35
5.3 Level III. Security marking protection level...	37
5.3.1 Security functional requirements...	37
5.3.2 Security assurance requirements...	45
5.4 Level IV. Structured protection level...	46
5.4.1 Security functional requirements...	46
5.4.2 Security assurance requirements...	55
5.5 Level V. Access verification protection level...	57
5.5.1 Security functional requirements...	57
5.5.2 Security assurance requirements...	66
References...	69

1 Scope

This Standard specifies the security technology requirements needed for the security classified protection of terminal computer system, and makes different technology requirements for each security protection level.

This Standard applies to the design and realization of terminal computer system conducted according to the requirements for security protection level specified in the GB 17859-1999, and also provides a reference for the testing and management of terminal computer system conducted according to the requirements specified in the GB 17859-1999.

2 Normative references

The provisions in the following documents become the provisions of this

Standard through reference in this Standard. For dated references, the subsequent amendments (excluding corrections) or revisions do not apply to this Standard. However, parties who reach an agreement based on this

Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest versions apply to this Standard.

GB/T 17859-1999 Classified criteria for security protection of computer information system

GB/T 20271-2006 Information security technology - Common security techniques

requirement for information system

GB/T 20272-2006 Information security technology - Security techniques requirement for operating system

3.1 Terms and definitions

The terms and definitions established in the GB 17859-1999, GB/T 20271-2006 and GB/T 20272-2006 AND the following ones apply to this Standard.

equipment protection against theft and destruction of the terminal computer system is divided into.

- a) Equipment identification requirements. The equipment of the terminal computer system shall have obvious and non-removable identifications, so as to prevent the replacement and to facilitate the searching;
- b) Host physical security. The host of the terminal computer system shall have case encapsulation protection, so as to prevent the system damage caused by dropping and vibration;
- c) Requirements for equipment protection against theft and self-destruction.

The equipment of the terminal computer system shall provide owners with controllable anti-theft alarm and system self-destruction functions.

4.1.3 High reliability of equipment

According to the application requirements of special environments, the equipment's high reliability of the terminal computer system is divided into.

- a) Waterproof requirement. The terminal computer system shall have high sealing property, so as to prevent water drops from entering;
- b) Anti-dropping and anti-vibration requirements. The terminal computer system shall have reinforced protection, so as to prevent the system damage caused by dropping and vibration;
- c) Requirements for the resistance to high and low temperature and pressure.

The terminal computer system shall be able to adapt the environments with high and low temperature and pressure;

- d) Resistance to electromagnetic radiation and interference. The terminal computer system shall be able to resist the system security threats caused by electromagnetic interference and radiation.

4.2.1 System security detection and analysis

According to the different requirements of different security levels, the security detection and analysis of the terminal computer system is divided into.

a) Security detection and analysis of the operating system. ASSESS the file permission, file host, network service settings, account settings, program authenticity, and general user-related security points and intrusion signs as an administrator from the aspect of terminal computer operating system, so as to detect and analyze the security of the operating system, to discover the existing potential security hazards, and to put forward the remedial measures.

b) Security detection and analysis of the hardware system. CONDUCT the security detection to the hardware system supporting the terminal computer system operation. SCAN the specific security vulnerability related to the system operation and data protection in the hardware system, so as to analyze...

.....