

ICS 35.020
CCS L 09

GA

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

GA/T 708-2007

**Information security technology--Architecture framework of
security classification protection for information system**

信息安全技术 信息系统安全等级保护体系框架

(English Translation)

Issued on: August 13, 2007

Implemented on: October 1, 2007

Issued by: Ministry of Public Security

Table of Contents

Foreword
Introduction
1 Scope
2 Normative references
3 Terms and definitions

Foreword

Appendix A and Appendix B of this standard are informative annexes.

This standard is proposed and managed by the Information System Security Standardization Technical Committee of the Ministry of Public Security.

This standard was drafted. Beijing Jiangnan Tianan Technology Co., Ltd., Beijing Siyuan Xinchuang Information Security Information Co., Ltd.

Introduction

Information System Security Level Protection Information created and used by countries, societies, groups and individuals through three major functions and five links the system implements the necessary security protection hierarchically.

The three major functions to achieve information system security level protection are.

---Prevention and protection functions. from the physical, network, system, application and management components to achieve overall prevention and protection;

--- Supervision and inspection functions. the self-inspection of each unit is combined with the supervision and inspection of government functional departments, from the technical and management aspects, Ensure that the security of the information system meets the requirements for determining the level of security;

---Response and Disposal Function. The information system owner should have the ability to respond quickly and dispose of the security incidents of the system and discover when major problems are raised, they can be promptly reported to the competent authorities and communicate with relevant units.

The five links to achieve information system security level protection are.

---Policy and regulations. Establish a sound information security level protection policy and regulations, establish a special management organization, and clearly implement

Procedures and methods.

---Standardization of technology and management links. the development of information system security level protection technology and management standards in line with national conditions, and according to the standard Seek to implement safety management and conduct research and development of safety technologies and products.

--- System construction process control link. According to the requirements of who is responsible for the responsibility, the security information system construction process is fully controlled and through the strict testing and evaluation of the testing organization to ensure that the constructed safety information system meets the required safety requirements.

--- System operation process control link. According to the requirements of who operates and who is responsible, the operation process of the safety information system is fully controlled.

And through the supervision and inspection of functional departments to ensure that the safety information system in operation meets the designed safety requirements.

--- System supervision and inspection links. Information security related functional departments, in accordance with laws, regulations and standards, develop and improve information security supervision Rules and regulations, carry out special management of information security level protection. Supervise the implementation of the safety level protection responsibility system, supervision and inspection Investigate and guide the construction and management of the information system security level protection of the departments and units of the information system, and the security technology products.

Implement supervision and implement supervision over safety inspection agencies. Establish non-profit coverage of national security level protection law enforcement inspection with the inspection support system, use the unified standard to inspect, test and evaluate the operational safety information system to ensure its actual operation.

The security during the process meets the design goals.

This standard is a description of the various components of the information system security level and their relationship, first of all to the information system security level the main content of the components of the protection and their interrelationships are briefly explained, and then the main content of each component is compared in more detail.

instruction of.

Information security technology Information System Security Level Protection System Framework

1 Scope

This standard specifies the system for implementing security level protection for information systems from a technical perspective in accordance with the requirements of information security level protection.

frame.

This standard applies to the implementation of the security system according to the requirements of the five security protection levels specified in the information system security level protection.

Level protection The technical activities carried out and their associated management activities.

2 Normative references

The terms in the following documents become the terms of this standard by reference to this standard. All dated references, followed by all Modifications (not including errata content) or revisions do not apply to this standard, however, parties to agreements based on this standard are encouraged to study is it possible to use the latest version of these files? For undated references, the latest edition applies to this standard.

GB 17859-1999 Computer Information System Security Protection Level Division Guidelines

3 Terms and definitions

The following terms and definitions established in GB 17859-1999 apply to this standard.

Systematic approach to design and implementation of information security products, information security technologies and management measures with appropriate security strength/grade Now, according to the requirements of the information system security level protection, there is an information system with primary/secondary/third/fourth/five security.

Abbreviation for Information System Security Subsystem. The security subsystem of an information system is composed of all security devices in the information system.

system. In GB 17859-1999, the overall protection of the system is referred to as TCB (Trusted Computing Base). Information security here the title of the system is to emphasize that the security of the information system should be designed in a systematic way.

An information product with a defined security strength/grade for building a secure information system. Information security products are divided into information technology security products Product and information security products. Information technology security products are products that are supplemented by corresponding security

technologies and mechanisms for information technology products.

(such as secure routers); information security products are information security products developed specifically to enhance the security of information systems (such as fire protection) wall).

Consisting of one or more computer systems (hosts/servers) to store and process data information in an information system.

A computing environment with a clear purpose and a clear boundary. A local computing environment can consist of one computer system or multiple computers the system consists of a LAN connection.

A local computing environment with a defined level of security protection.