

ICS 35.240
CCS A 90

GA

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

GA/T 1394-2017

**Information security technology - Security technical
requirements for security operation and maintenance
management products**

信息安全技术 运维安全管理产品安全技术要求
(English Translation)

Issued on: April 19, 2017

Implemented on: April 19, 2017

Issued by: Ministry of Public Security

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Operation and Maintenance Safety Management Product Description	
5 General Description	
5.1 Safety Technical Requirements Classification	
5.2 Security classification	
6 Safety function requirements	
6.1 Single sign-on	
6.2 Access Control	
6.3 Operational Audit	
6.4 Session Monitoring	
6.5 Session playback	
6.6 Alarm	
6.7 Illegal operations blocked	
6.8 High Availability	
6.9 Identification and Identification	
6.10 Safety Management	
6.11 Audit Log	
7 Security Requirements	
7.1 Development	
7.2 Guidance Document	
7.3 Life Cycle Support	
7.4 Test	
7.5 Vulnerability Assessment	
8 Grade division requirements	
8.1 Overview	
8.2 Classification of safety function requirements	
8.3 Security Assurance Requirements Classification	

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard proposed by the Ministry of Public Security Network Security Bureau.

This standard by the Ministry of Public Security Information System Safety Standardization Technical Committee.

1 Scope

This standard specifies the safety function requirements of operation and maintenance safety management products, safety protection requirements and classification requirements.

This standard applies to the operation and maintenance safety management product design, development and testing.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version applies to this article Pieces. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 18336.3-2015 Information Technology Security Technology Information Technology Security Assessment Guidelines Part 3. Security components Information technology - Security terminology

3 Terms and definitions

GB/T 18336.3-2015 and GB/T 25069-2010 defined by the following terms and definitions apply to this document.

Operation and maintenance user on the server, network equipment and databases and other important information systems operating and maintenance personnel.

Operation and maintenance security management products
securityoperationandmaintenancemanagementproduct the maintenance of key assets of the information system to achieve single sign-on, centralized authorization, centralized management and audit of the product.

Operation and maintenance object Assets protected by O & M safety management products.

4 Operation and maintenance safety management product description

Operation and maintenance security management products provide a unified authentication interface for operation and maintenance users, a variety of remote operation and maintenance management, the assets and their accounts such as centralized management and authorization, monitoring and auditing operation and maintenance operations, and illegal operation of the alarm, blocking. This type of product protection the object is a server, network equipment, security products, databases, application systems and other important information system assets. In addition, operation and maintenance safety management production the product itself and its internal important data is also the object of protection.

O & M safety management products are usually deployed by-pass. Operation and maintenance safety management products typical operating environment shown in Figure 1.