

ICS 35.240
CCS A 90

GA

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

GA/T 1718-2020

**Information security technology - Security technology
requirements for security management products of big data
platform**

信息安全技术 大数据平台安全管理产品安全技术要求
(English Translation)

Issued on: April 2, 2020

Implemented on: June 1, 2020

Issued by: Ministry of Public Security

Table of Contents

- Foreword
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Big data platform security management product description
- 5 General description
 - 5.1 Classification of safety technical requirements
 - 5.2 Security classification
- 6 Safety function requirements
 - 6.1 Safe Operation and Maintenance
 - 6.2 Data security access
 - 6.3 Security incident management
 - 6.4 Identification and identification
 - 6.5 Security Management
 - 6.6 Security Audit
- 7 Security requirements
 - 7.1 Development
 - 7.2 Guidance Document
 - 7.3 Life Cycle Support
 - 7.4 Test
 - 7.5 Vulnerability assessment
- 8 Classification requirements
 - 8.1 Classification of safety function requirements
 - 8.2 Classification of safety assurance requirements

Foreword

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

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security.

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

Drafting organizations of this standard. the Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security, the Cyber Security Bureau of the Ministry of Public Security, the Third Research Institute of Abe.

1 Scope

This standard specifies the security function requirements, security assurance requirements and grading requirements of big data platform security management products.

This standard applies to the design, development and testing of security management products for big data platforms.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 18336.3-2015 Information Technology Security Technology Information Technology Security Evaluation Criteria Part 3: Security Assurance Components GB/T 25069-2010 Information Security Technical Terms

3 Terms and definitions

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

Big Data

Large-scale data sets have large, diverse, fast and/or changeable characteristics, and require a scalable architecture for effective storage, calculation and analysis.

Big data platform

Software and hardware systems for storing and processing big data.

Audit log

The big data platform securely manages the log data generated by the product's own audit record

The big data platform generates access, processing, analysis and other operations for big data, and is unified by the big data platform security management product Collect and centrally store log data.

4 Big data platform security management product description

Big data platform security management products (hereinafter referred to as "products") is a collection of various software and hardware systems that make up a big data platform Security management products whose main functions include status monitoring, configuration management, policy management, data security access and security auditing, etc., and can Secure data access through technologies such as access control.