ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 24294.1-2026

Cybersecurity technology - Implementation guide for the information security of internet-based e-government - Part 1: General

网络安全技术 基于互联网电子政务信息安全实施指南 第1部分：总则

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

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1.Structure and Drafting Rules of Standardization Documents". Drafting. This document is Part 1 of GB/T 24294 "Information Security Technology - Implementation Guidelines for Internet-based E-government Information Security". The "Information Security Technology Implementation Guidelines for Internet-based E-Government Information Security" has been released, including the following sections.

1.General Provisions;

2.Access Control and Security Switching;

3.Identity Authentication and Authorization Management;

4.Endpoint Security Protection. This document replaces GB /Z 24294.1-2018 "Information Security Technology - Implementation Guidelines for Internet-based E-government Information Security (Part 1)". Part. General Provisions. Compared with GB /Z 24294.1-2018, apart from structural adjustments and editorial changes, the main technical changes are as follows:

a) The Internet-based e-government information security reference model has been modified (see Chapter 5, Chapter 5 of the.2018 version);

b) The Internet-based e-government information security technology system has been

revised (see Chapter 6, Chapter 6 of the.2018 edition);

c) The implementation principles of the system have been changed (see Chapter 7, Chapter 7 of the.2018 edition);

d) The implementation architecture of the system was changed (see Chapter 8, Chapter 8 of the.2018 edition);

e) Added Chapter 9, "Cryptography Use and Security Responsibilities" (see Chapter 9);

f) The risk assessment for the system has been removed (see Chapter 10 of the.2018 edition). Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents. This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260). This document was drafted by: Information Engineering University of the Cyberspace Force of the Chinese People's Liberation Army, National Information Center, and Beijing Municipal Bureau of Economy and Information Technology. The Cybersecurity Management Center of the Bureau of Natural Resources, Zhengzhou Yunzhixin Security Technology Co., Ltd., Beijing Topsec Network Security Technology Co., Ltd., and Huazhong University of Science and Technology Technical University, Beijing Shenzhou Green Alliance Technology Co., Ltd., Zhengzhou Xinda Jiean Information Technology Co., Ltd., Wuhan Minwei Technology Co., Ltd. Guangzhou Zhuoteng Technology Co., Ltd. The main drafters of this document are. Chen Xingyuan, Du Xuehui, Ren Zhiyu, Wang Na, Cao Lifeng, Wang Wenjuan, Zhang Dongwei, Sun Yi, Shan Dibin, and Liu Aodi. Liu Yingying, Liu Bei, Yan Guixun, Li Yuan, Zhang Qiankun, Zhang Nan, Gao Junwei, Peng Ming, Wang Yu, Chen Zhuo, Liu Yao, Jing Hongli, Luo Yuan, Xie Qin, Zhang Chao Wang Haoyu, Dong Feng, Zhao Yanjie, Ye Xiaohu, Fan Dunqiu, Huang Jun, Ye Jianwei, Liao Zhengyun, Mei Guangming, Cao Wanyu. The release history of this document and the document it replaces is as follows:

---First published in.2009 as GB /Z 24294-2009;

---First revised in.2018 as GB /Z 24294.1-2018;

1 Scope

GB/T 24294.1-2026 is the Chinese national standard covering securing government services delivered over the public internet - the general part: the boundary between the internet-facing systems and the internal ones, the identity and access, the data classification and the incident response. Part 1 of the series, first edition, in force since 1 November 2026. It was issued on 30 April 2026 and takes effect on 1 November 2026, as a first edition. The document is under the responsibility of the Standardization Administration of China. This page is published from the official record of the 2026 edition; the clause text of a standard this recent is not yet in circulation, and the figures, limits and tables it contains are those of the document itself, delivered in full with the English translation.

1.Scope This document provides a reference model, cybersecurity technology system, system implementation principles, and system framework for internet-based e-government information security. Implement frameworks and cryptographic usage and security confidentiality responsibilities. This document applies to the construction and operation of internet e-government network security for municipal (and below) government units, and is for municipal (and below) level government units. (Below) Provide a basis for government agencies to carry out the construction and security of integrated government service platforms.

4.Abbreviations The following abbreviations apply to this document. App. Application API. Application Programming Interface DDoS. Distributed Denial of Service IPSec. IP Security Protocol PKI. Public Key Infrastructure SSL. Secure Sockets Layer VPN. Virtual Private Network

2 Internet e-government network security technology system

6.2 Boundary Protection Border protection includes the following.

a) It should have policy-based network access control functionality, implementing network-level access control based on the scope of government application services, and blocking incoming... Internet security threats;

b) When deploying virtual networks and devices in a cloud computing environment, it is advisable to deploy a virtual firewall to manage multi-tenant networks within the government cloud. To achieve isolation and control, it is advisable to implement isolation of government services based on container isolation rules, and to realize the virtualization of business resources. East-west data flow control, see GB/T 31168;

c) Network intrusion prevention is recommended, with real-time monitoring and alerting capabilities for typical malicious behaviors such as SYNFlood, DDoS, and webshell attacks. The alarm and tracing functions support both intrusion prevention capabilities for traditional government service deployment architectures and for government virtualization cloud environments. The ability to prevent intrusion;

d) A reliable and trustworthy isolation and exchange mechanism should be established between the internet-based government service area and the public government business area to prevent data transmission from the internet. The risks in the government service area have spread to the public government affairs area.

6.3 Device access security and secure communication network Device access to secure communication networks includes the following.

a) When user equipment accesses the network, it is advisable to implement equipment access protection. Specific access requirements are detailed in GB/T 31168.

b) Relying on internet infrastructure, it is advisable to adopt cryptographic technology,

security policy management, secure tunnel management, security audit management, and dynamic evaluation. For technologies such as estimation, IPSec or SSL protocols should be adopted for communication between remote government agencies and government service centers, and between remote government office users and... Secure interconnection is established between government service centers to build a virtualized secure communication network between remote users and the government service platform;

c) It is advisable to use technologies such as user authentication, virtual security domain construction, access terminal status assessment, data encryption and decryption, and cloud environment micro-segmentation. Technology to ensure the security of government data transmission;

d) Network device connectivity should be achieved through technologies such as network device identification, user account management, network identity authentication, and network login control. Safety of connection;

e) Network architecture should be improved through methods such as subnetting and segmenting, redundant deployment of network devices, and enhancement of network bandwidth performance. Safety.

6.4 Security of Government Cloud Services Government cloud service security includes the following.

a) Internet-based government cloud platforms should have malicious code protection functions; specific requirements are detailed in GB/T 31168.

b) Internet-based government cloud platforms should possess functions such as virtual machine image security, resource isolation of the virtualization platform, and virtual machine security isolation. Specifically... Requirements are specified in GB/T 31168;

5 Reference Model

5.1 Model Framework The reference model framework for internet-based e-government cybersecurity is shown in Figure 1. Figure

1 Reference Model Framework The Internet-based e-government cybersecurity reference model consists of "requirements identification, security design, security implementation, operation and evaluation, and system". The model comprises five phases. "migration and deprecation." Centered on security policy, it identifies, designs, implements, evaluates, and deprecates internet-based security measures. The network security system for e-government is built and maintained throughout its entire lifecycle.

5.2 Security Strategy A security policy is a set of rules used for all security-related activities. It occupies a central position in the reference model and should be adaptable to the system's needs. We dynamically adjust and optimize our approach to address the risks and needs we face in order to adapt to the ever-changing cybersecurity landscape. It includes