

ICS 35.240
CCS A 90

GA

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

GA/T 1717.2-2020

**Information security technology - Notification and warning of
cyber security incidents - Part 2: Specifications for procedure
for notification and warning**

信息安全技术 网络安全事件通报预警 第2部分：通报预警流程规范
(English Translation)

Issued on: March 24, 2020

Implemented on: August 1, 2020

Issued by: Ministry of Public Security

Table of Contents

- Foreword
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Classification of cyber security incidents
 - 4.1 Classification elements
 - 4.2 Classification of network security incident notification
 - 4.3 Early warning levels of network security incidents
- 5 Notification process
 - 5.1 Publication of notification
 - 5.2 Disposal of notification
 - 5.3 Filing of notifications
- 6 Early warning process
 - 6.1 Issuance of warning
 - 6.2 Disposal of early warning
 - 6.3 Upgrade or downgrade of warning
 - 6.4 Releasing the warning
- 7 Evaluation Index
- Appendix A (normative appendix) Network security incident notification content, report and classification example
 - A.1 Cybersecurity incident notification content
 - A.2 Network security incident analysis report
 - A.3 Summary report of cyber security incidents
 - A.4 Example of classification of network security incident notification
- Reference

Foreword

GA/T 1717 "Information Security Technology Cybersecurity Incident Notification and Early Warning" is divided into three parts.

---Part 1: Terminology;

---Part 2: Notification and early warning process specifications;

---Part 3: Data classification coding and labeling system technical specifications.

This part is part 2 of GA/T 1717.

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

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

This part is proposed and managed by the Public Security Information System Security Standardization Technical Committee.

Drafting organizations of this section. Network Security Bureau of the Ministry of Public Security, Network Security Detachment of Public Security Bureau of Longyan City, Fujian Province, China Science and Technology Co., Ltd.

1 Scope

This part of GA/T 1717 specifies the classification and processing procedures for notification and early warning of cyber security incidents.

This section applies to public security organs and other relevant functional institutions or organizations to carry out cybersecurity incident notification and early warning work.

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

GB/Z 20986-2007 Information Security Technology Information Security Incident Classification and Classification Guidelines GB/T 22240 Information Security Technology Information System Security Level Protection Rating Guidelines GB/T 25069-2010 Information Security Technical Terms GB/T 32924-2016 Information Security Technology Network Security Early Warning Guide GA/T 1717.1-2020 Information Security Technology Cybersecurity Incident Notification and Early Warning Part 1: Terminology

3 Terms and definitions

The terms and definitions defined in GA/T 1717.1-2020 apply to this document.

4.1.1 Overview

The classification of network security incidents mainly considers two elements. the importance of network security protection objects and the degree of possible damage.

4.1.2 The importance of network security protection objects the importance of network security protection objects is based on the importance of the business they carry to national

security, economic construction, and social activities, Comprehensive factors such as the level of network security protection, the importance and sensitivity of data, are divided into three levels. particularly important, and general.

Specifically.

a) Particularly important objects of protection, including.

- 1) Network security protection objects during major events;
- 2) Information systems rated as Level 4 and above in accordance with the provisions of GB/T 22240;
- 3) Important Internet applications with hundreds of millions of users or tens of millions of daily active users;
- 4) Electronic trading platform with daily trading volume of 100 million yuan;
- 5) The top five important Internet applications in the industry;
- 6) Systems involving personal information of citizens above one million;