

ICS 35.240
CCS A 90

GA

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

GA/T 1717.1-2020

**Information security technology - Notification and warning of
cyber security incidents - Part 1: Terminology**

信息安全技术 网络安全事件通报预警 第1部分：术语

(English Translation)

Issued on: March 24, 2020

Implemented on: August 1, 2020

Issued by: Ministry of Public Security

Table of Contents

Preface
Introduction
1 Scope
2 General concept
3 Technology
4 Business
Chinese Pinyin Index
English Correspondence Index
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 1 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 under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

Drafting organizations of this section. Cyber Security Bureau of Ministry of Public Security, Third Research Institute of Ministry of Public Security, Institute of Software, Chinese Academy of Sciences, Taiji Computer Co., Ltd., Venus Star Information Technology Group Co., Ltd., Qi Anxin Technology Group Co., Ltd., State Grid Net Security (Beijing) Technology Co., Ltd.

Introduction

At present, the network security situation is becoming increasingly severe, security threats are becoming more diversified, vulnerabilities are frequently occurring, and the impact of

security incidents is becoming more and more profound.

Seriously endanger national security, public safety and people's interests.

Network security incident notification and early warning is an important part of the national network security guarantee system and an important work content required by national laws and regulations.

In order to further clarify the standardized description language system, work process specification, classification coding method and marking of network security incident notification and early warning Labeling system to standardize the notification and early warning of cybersecurity incidents, effectively maintain the security of the country's critical information infrastructure, and protect the interests of the people, for public safety and national security, GA/T 1717 is specially formulated.

GA/T 1717 is divided into three parts, which can carry out network security monitoring and analysis, notification and early warning, and emergency response for network security functional departments Provide basis and reference. Part 1 clarifies the key terms and meanings needed in the notification and early warning work of cybersecurity incidents, and unified standards the interactive language of all parties in the notification and early warning work; Part 2 regulates the grading method, notification process and early warning process of cybersecurity incidents.

Effectively improve the efficiency of notification and early warning; Part 3 regulates the classification method and coding method of relevant data in the notification and early warning of cyber security incidents.

The law and labeling system can provide support for the mechanized, intelligent and digital development of network security notification and early warning.

Information security technology, network security incident notification and early warning
Part 1: Terminology

1 Scope

This part of GA/T 1717 specifies the terms and definitions involved in the notification and early warning of cybersecurity incidents.

This part is applicable to network security incident monitoring and analysis, notification and early warning, investigation and disposal, and related management and technical research work.

And express related concepts.

2 General concepts

attacker

Intentionally exploiting the vulnerabilities of technical and non-technical security control measures to steal or damage information systems and networks, or damage information. Anyone with the availability of system and network resources to legitimate users.

attack

Attempt to destroy, leak, tamper with, damage, steal, unauthorized access or unauthorized use of assets.

[GB/T 29246-2017, definition 2.3] 2.3 Invade Unauthorized access to the network or networked system, that is, intentional or unintentional unauthorized access to information systems, including information systems. Malicious activities or unauthorized use of resources in the information system.

Cybersecurity incident Causes harm to the network or information system or to society due to natural or man-made defects or failures of the software and hardware itself. Negatively impacted events.

[GB/T 32924-2016, definition 3.4] Note. Refer to GB/T 20986-2007, network security incidents include harmful program incidents, network attack incidents, information destruction incidents, information content security incidents, Equipment failures, catastrophic events and other events.

3 Technology

Harmful program

Malicious program

A program specifically designed to damage or destroy the system, to attack confidentiality, integrity or availability.

Note: Harmful programs include viruses, Trojan horses, backdoors, worms, etc.

virus

Insert a set of computer instructions in a computer program that destroys computer functions or data, affects the use of the computer and can copy itself