

ICS 35.240
CCS A 90

GA

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

GA/T 1717.3-2020

**Information security technology - Notification and warning of
cyber security incident - Part 3: Technical specifications for
data classification coding and label system**

信息安全技术 网络安全事件通报预警 第3部分：数据分类编码与标记标签技术体系技术规范

(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 Formulating Principle
- 5 Network security data classification method
 - 5.1 Classification of cybersecurity data elements
 - 5.2 Network security data category classification
 - 5.3 Classification of network security data activity characteristics
 - 5.4 Network security data attribute classification
- 6 Network security data classification and coding method
 - 6.1 Coding method
 - 6.2 Code composition
 - 6.3 Code Rules of Line Classification
 - 6.4 Coding rules for face classification
- 7 Cybersecurity data tag label
 - 7.1 Cybersecurity data tag label category
 - 7.2 Network Security Data Marking Label Sample
- Appendix A (Normative Appendix) Classification and Coding Rules
 - A.1 Classification and coding rules
 - A.2 Network security data classification and coding
 - A.3 Network Security Service Code
- Appendix B (informative appendix) Network security data catalog code example
- Appendix C (Informative Appendix) Sample Marking Label
- 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 3 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.

1 Scope

This part of GA/T 1717 specifies the classification method, coding method, and method of network security data in the notification and early warning of network security incidents.

Mark label system.

This part is applicable to network security functional departments to carry out network security monitoring and analysis, notification and early warning, and emergency response.

2 Normative references

The following documents are indispensable for the quotation of this document. For dated reference documents, only the dated version applies to this article Pieces. For undated references, the latest version (including all amendments) applies to this document.

GB/T 4754 Classification of National Economic Industries GB 11714 National Organization Code Compilation Rules GB/T 25069 Information Security Technical Terms GB 32100 Legal persons and other organizations unified social credit code coding rules GA/T 1717.1 Information Security Technology Cybersecurity Incident Notification and Early Warning Part 1: Terminology

3 Terms and definitions

The following terms and definitions defined in GB/T 25069 and GA/T 1717.1 apply to this document.

Cybersecurity data classification According to the attributes or characteristics of network security data, it is distinguished and classified according to certain principles and methods, and a certain classification is established.

Class system and arrangement order in order to better manage and use the data process.

Network security data encoding on the basis of classification, the network security data is given symbols that have certain regularity and are easily recognized and processed by computers.

Authority

The unit that provides network security data and is responsible for the content of the data in business.

Data tag label

Cybersecurity data is contained in its own attributes, or marked by certain analysis and calculations, and is used to generalize and summarize the data or objects described by the data.

Abstract description of text data with a certain dynamic and timeliness.

4 Develop principles

The principles for formulating cybersecurity data classification methods are as follows.