GA

PUBLIC SECURITY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.40

L 80

GA/T 1389-2017

Information Security Technology - Guidelines for Grading of Classified Protection of Cyber Security

信息安全技术

网络安全等级保护定级指南

Issued on: May 8, 2017 **Implemented on: May 8, 2017**

Issued by: The Ministry of Public Security of the People's Republic of China.

Table of Contents

Information Security Technology - Guidelines for Grading of Classified Protection of Cyber Security

1 Scope

This Standard stipulates the grading method and grading process for classified protection of cyber security.

This Standard is applicable to the guidance of the grading of the target of classified protection.

2 Normative References

The following documents are indispensable to the application of this document. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB 17859-1999 *Classified Criteria for Security protection of Computer Information System*

GB/T 25069-2010 *Information Security Technology - Glossary*

3 Terms and Definitions

What is defined in GB 17859-1999 and GB/T 25069-2010, and the following terms and definitions are applicable to this document.

3.1 Target of Classified Protection

Target of classified protection refers to the object of cyber security classified protection work, which mainly includes basic information network, information system (such as: industrial control system, cloud computing platform, Internet of Things, information system using mobile Internet technology and other information systems) and big data, etc.

3.2 Basic Information Network

Basic information network refers to information networks that play a basic supporting role for information circulation and the operation of information system, including telecommunication network, broadcast and television transmission network, the Internet, private business network and other network facilities.

c) Grade-3: after the target of classified protection is damaged, it would cause extremely severe damage to the legitimate rights and interests of citizens, juridical persons and other organizations, or cause severe damage to the social order and public interests, or cause damage to the national security;

d) Grade-4: after the target of classified protection is damaged, it would cause extremely severe damage to the social order and public interests, or cause severe damage to the national security;

e) Grade-5: after the target of classified protection is damaged, it would cause extremely severe damage to the national security.

4.2 Grading Elements

4.2.1 An overview of grading elements

The grade of the target of classified protection is determined by two grading elements:

a) The object being infringed;

b) The degree of infringement on the object.

4.2.2 The object being infringed

When the target of classified protection is damaged, the object being infringed includes the following three aspects:

a) Legitimate rights and interests of citizens, juridical persons and other organizations;

b) Social order and public interests;

c) National security.

The infringement of the legitimate rights and interests of citizens, juridical persons and other organizations means certain social rights and interests enjoyed by citizens, juridical persons and other organizations confirmed and protected by law are impaired.

The infringement of the social order includes the following aspects:

a) Affect the work order of social management and public services of state organs;

b) Affect the order of various types of economic activities;

c) Affect the order of scientific research and production in various industries;

d) Affect the normal life of the public under legal constraints and ethics;

e) Other effects on the social order.

The infringement of the public interests includes the following aspects:

a) Affect social members' use of public facilities;

b) Affect social members' acquisition of public information resources;

c) Affect social members' reception of public services;

d) Other effects on the public interests.

The infringement of the national security includes the following aspects:

a) Affect the steadiness of state power and national defense strength;

b) Affect national unity, ethnic unity and social stability;

c) Affect national political and economic interests in foreign activities;

d) Affect important national security defense work;

e) Affect national economic competitiveness and technological strength;

f) Other effects on the national security.

4.2.3 The degree of infringement on the object

The degree of infringement on the object is comprehensively determined by different external manifestations of the objective aspects. Since the infringement on the object is implemented by destroying the target of classified protection, the external manifestation of the infringement on the object is the damage to the target of classified protection, which is described through the mode of damage, the consequence of damage and the degree of damage.

The degrees of infringement on the object, after the target of classified protection is destroyed are attributed as: general damage, severe damage and extremely severe damage. The description of the three degrees of infringement is as follows:

a) General damage: job function is partially affected, and service capability is decreased, but it does not affect the execution of the main functions; there are relatively slight legal problems, relatively low property loss, limited adverse social influence, and relatively low damage to other organizations and individuals;

b) Severe damage: job function is severely affected, and service capability is significantly decreased, the execution of the main functions is severely affected; there are relatively severe legal problems, relatively high property loss, a relatively wide sphere of adverse social influence, and relatively severe

management layer is shown in 5.2.5. The field equipment layer, the field control layer and the process monitoring layer shall be considered as a whole target for grading. The elements of each layer shall not be individually graded.

In accordance with system functions, control target and manufacturer, large-scale industrial control system may be divided into multiple grading targets.

5.2.2 Cloud computing platform

In the cloud computing environment, the cloud computing platform on the cloud server side shall be considered as an individual grading target for grading. The target of classified protection on the cloud tenant side shall also be considered as an individual grading target for grading.

In terms of large-scale cloud computing platform, cloud computing infrastructures and relevant auxiliary service systems shall be divided into different grading targets.

5.2.3 Internet of Things

As a whole target for grading, the Internet of Things mainly includes elements like perception layer, network transmission layer and processing application layer, etc.

5.2.4 Information system adopting mobile Internet technology

The target of classified protection that adopts mobile Internet technology shall be considered as a whole target for grading, which mainly includes mobile terminals, mobile applications, wireless networks and relevant application systems, etc.

5.2.5 Other information systems

Other information systems, which are considered as the grading target, shall have the following basic characteristics:

a) Have a determined main security responsibility unit. As the grading target, the information system shall be able to clarify its main security responsibility unit;

b) Undertake relatively independent business applications. As the grading target, the information system shall undertake relatively independent business applications. Multiple information systems that complete different business goals, or support different units or different department functions shall be divided into different grading targets;

c) Have the basic elements of an information system. As the grading target, the information system shall be a multi-resource collection composed of related and supporting equipment and facilities in accordance with certain application goals and rules. An individual device (such as: server, terminal and network equipment, etc.) shall not be separately graded.

3) Preliminarily determine the higher one between the grade of security protection for business information and the grade of security protection for system service as the grade of security protection for the grading target.

The schematic diagram of the process of the grading methods is shown in Appendix B.

In terms of grading targets like big data, factors such as data scale and data value shall be comprehensively considered. In accordance with its importance in the national security, economic construction and social life, and the damage to the national security, social order, public interests, and the legitimate rights and interests of citizens, juridical persons and other organizations after data resources are damaged, determine the grade of security protection. In principle, the grade of security protection for big data shall be above Grade-3.

In terms of grading targets like basic information network and cloud computing platform, in accordance with the importance of targets of classified protection that they undertake or will undertake, determine the grade of security protection. In principle, the grade of security protection shall be not lower than the grade of security protection for the targets that they undertake.

The grade of security protection for national critical information infrastructure shall be not lower than Grade-3.

6.2 Determine the Object Being Infringed

When the grading target is damaged, the object being infringed includes national security, social order, public interests, and legitimate rights and interests of citizens, juridical persons and other organizations.

In the determination of the object being infringed, firstly, judge whether the national security is infringed; then, judge whether the social order or public interests is infringed. Finally, judge whether the legitimate rights and interests of citizens, juridical persons and other organizations are infringed.

6.3 Determine the Degree of Infringement on the Object

6.3.1 Objective aspect of infringement

In the objective aspect, the external manifestation of infringement on the object is the damage to the grading target. The mode of infringement is expressed in the damage to the business information security and the system service security. Specifically speaking, business information security refers to ensuring the confidentiality, integrity and availability of information in the information system. System service security refers to ensuring that the grading targets can provide services in a timely and effective manner, so as to complete the pre-determined business goals. When the business

7 Expert Review

The organization operating and using the grading target shall organize information security experts and business experts to review the rationality of the preliminary grading result and issue expert review opinions.

8 Competent Department’s Review

The organization operating and using the grading target shall report the preliminary grading result to the industrial competent department or superior competent department for review.

9 Public Security Organ’s Recording and Review

The organization operating and using the grading target shall, in accordance with the relevant management regulations, submit the preliminary grating result to the public security organ for recording and review. If the review fails, the organization operating and using the grading target shall organize a re-grading. After passing the review, he organization operating and using the grading target shall finally determine the grade of security protection for the grading target.

10 Grade Variation

When the information, business status and system service range processed by the target of classified protection change, after the business information security or the system service security are damaged, the object being infringed and the degree of infringement on the object might significantly change. Under this circumstance, in accordance with the requirements of this Standard, re-determine the grading target and the grade of security protection.

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------