ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43557-2023

Information security technology - Guidelines for cyber security information submission

信息安全技术 网络安全信息报送指南

Issued on: December 28, 2023 **Implemented on: July 1, 2024**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document was issued on 28 December 2023 by the State Administration for Market Regulation; Standardization Administration of the PRC and takes effect on 1 July 2024.

It is a GB/T standard: recommended rather than compulsory, but it is the text a Chinese reviewer applies when assessing a submission.

It is classified under ICS 35.030, Chinese classification L80.

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.

Please note that some content in this document may be subject to patents. The publisher of this document assumes no responsibility for identifying patents.

This document is proposed and coordinated by the National Information Security Standardization Technical Committee (SAC/TC260).

This document was drafted by. Zhejiang Branch of the National Computer Network Emergency Response Technology Coordination Center, National Computer Network Emergency Technology Division

Coordination Center, China Electronics Technology Standardization Institute, National Computer Network Emergency Response Technology Coordination Center Jiangsu Branch, China Information Technology

Information Security Research Institute Co., Ltd., Shanghai Guanan Information Technology Co., Ltd., Venus Information Technology Group Co., Ltd., Beijing

Antiy Network Security Technology Co., Ltd., Beijing Dongfangtong Network Technology Co., Ltd., Hangzhou Hikvision Digital Technology Co., Ltd., Harbin

Erbin Engineering University, Xi'an Jiaotong University Jabil Network Technology Co., Ltd., Sangfor Technology Co., Ltd., Yuanjiang Shengbang (Beijing) Network Security

Technology Co., Ltd., Nanjing Juming Network Technology Co., Ltd., Shaanxi Provincial Network and Information Security Evaluation Center, Shanghai 30 Guardian Information

Security Co., Ltd., Beijing Tianrongxin Network Security Technology Co., Ltd., Institute of Information Engineering, Chinese Academy of Sciences, Third Research Institute of the Ministry of Public Security, Shanxi

Shuling Network Technology Co., Ltd., Huaxin Consulting and Design Institute Co., Ltd., Beijing China Green League Technology Co., Ltd., Zhejiang University Computer

Innovation Technology Research Institute, Zhijiang Laboratory, AsiaInfo Technology (Chengdu) Co., Ltd., Hangzhou Anheng Information Technology Co., Ltd., Hengan Jiaxin

(Beijing) Technology Co., Ltd.

The main drafters of this document. Yan Hanbing, Guo Jing, Luo Liang, Long Quan, Ding Li, He Nengqiang, Wen Senhao, Lei Jun, Ma Yang, Zhong Sichao, Li Zhong,

Xie Jiang, Lu Ming, Wang Cambridge, Cui Tingting, Wan Li, Zhuang Zhuang, He Jianfeng, Chen Yangguo, Wang Jing, Chen Hu, Ju Tengfei, Gan Lu, Yang Jian, Liu Song, Chen Yan,

Bai Xiaoyu, Sun Xiaoping, Zhang Yuna, Jiang Bowen, Wu Shaoyong, He Zhongxu, Li Yujia, Han Xiaozhe, Li Guangli, Ma Minyan, Wang Lihua, Wang Xiaolong,

Liao Shuangxiao, Miao Chunyu, Zhang Yu.

Information Security Technology Network Security Information Submission Guide

1 Scope

GB/T 43557-2023 covers what one organization sends another when it reports network security information, and how that reporting is carried out. The first half deals with content: the types of information that get submitted and, for each type, the elements a submission is expected to carry. The second half deals with the reporting activity itself - the parties involved and the relationships between them, the basic process running from the production of the information to its receipt, and the methods by which a submission can be made. Terms are taken from existing information security standards rather than restated, so the vocabulary lines up with risk assessment and vulnerability work already in use. The problem behind it is practical. Notices about incidents, vulnerabilities and threats travel

between organizations that structure them differently, so a receiving party can get a report it cannot match against anything it already holds, or one missing the fields it would need to act, and has to go back and ask while the window to respond closes. A shared element list and an agreed process make submissions from different senders comparable without that round of clarification. Guidance rather than a conformance document, aimed at security operations and incident response teams, industry reporting bodies, and the people building the interfaces through which reports are exchanged.

This document gives the information types and elements for network security information reporting, as well as the elements, relationships, and basics of network security information reporting activities.

This process, submission method, etc.

This document is applicable to network security information reporting activities between various organizations.

2 Normative reference documents

The contents of the following documents constitute essential provisions of this document through normative references in the text. Among them, the dated quotations

For undated referenced documents, only the version corresponding to that date applies to this document; for undated referenced documents, the latest version (including all amendments) applies to

this document.

GB/T 20984 Information Security Technology Information Security Risk Assessment Method

GB/T 20986 Information Security Technology Network Security Incident Classification and Grading Guidelines

GB/T 25069-2022 Information security technical terms

GB/T 30279 Information Security Technology Network Security Vulnerability Classification and Grading Guidelines

GB/T 36643 Information security technology network security threat information format specification

3 Terms and definitions

GB/T 20984, GB/T 20986, GB/T 25069-2022, GB/T 30279, GB/T 36643 and the following terms

and definitions apply to this document.

3.1

Information describing network security (i.e. cyberspace security)-related situations.

Note. Network security information mainly includes threat information, vulnerability information, network security event information, network security situation information, etc.

[Source. GB /Z 42885-2023,3.1]

3.2

vulnerabilityvulnerability

A weakness in an asset or control that could be exploited by one or more threats.

[Source. GB/T 25069-2022,3.91]

3.3

Threat

Potential factors that could cause undesired events that could harm a system or organization.

[Source. GB/T 25069-2022,3.628]

3.4

Cybersecurity event cybersecurityevent

Indicates the occurrence of a possible information security breach or failure of certain controls.