ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/Z 42885-2023

Information security technology - Guidance for cyber security information sharing

信息安全技术 网络安全信息共享指南

Issued on: August 6, 2023 **Implemented on: March 1, 2024**

Issued by: State Administration for Market Regulation;
Standardization Administration of China

Table of Contents

Foreword

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: National Industrial Information Security Development Research Center, China Electronics Technology Standardization Institute, National Computer Network Emergency Technology Coordination Center, China Information Security Evaluation Center, Institute of Information Engineering, Chinese

Academy of Sciences, Hangzhou Anheng Information Technology Co., Ltd. Co., Ltd., Beijing Shenzhou Green League Technology Co., Ltd., Sichuan University, Beijing Tianrongxin Network Security Technology Co., Ltd., China Electronic Information Industry The Sixth Research Institute of Industrial Group Co., Ltd., Electric Power Research Institute of State Grid Xinjiang Electric Power Co., Ltd., China Aerospace Science and Industry Aviation Technology Research Institute, Guoneng Information Technology Co., Ltd., China Southern Power Grid Digital Grid Group Co., Ltd., Tencent Cloud Computing (Beijing) Co., Ltd., Shaanxi Provincial Network Network and Information Security Assessment Center. The main drafters of this document. Zhang Ge, Zhang Zheyu, Wang Shirui, Sun Jun, Yu Meng, Xiao Junfang, Hao Zhiqiang, Wang Huili, Guo Jing, Du Yuge, Jiang Zhengwei, Liang Wei, Wu Hao, Wang Junfeng, Tang Binhui, An Gaofeng, Yang Peng, Guo Li, Liu Zhilei, Li Mingxuan, Pei Yanchun, Zhang Liguang, Han Pengjun, Lu Huahui, Li Yang, Cheng Xi, Yang Zitao, Fan Kai, Qin Xiaowei, Ren Zejun, Wang Rui, Wang Zun, Xie Chengyun, Gao Rui, Jiang Jun. Information Security Technology Cybersecurity Information Sharing Guide

1 Scope

This document gives guidance on sharing cyber security information: what kinds of information are shared, between whom, in what form, and with what safeguards on the sharing itself. Threat intelligence only works if it moves faster than the attacker, and it only moves if the organisations holding it trust the channel. The hard part is not the format but the conditions - what may be attributed, what must be redacted, what an organisation is exposed to by admitting it was hit. This document is China's attempt to set those conditions down. Issued on 6 August 2023 by SAMR and SAC as a guiding technical document, in force from 1 March 2024. It belongs to the series, the body of Chinese information security standards that any company operating data infrastructure in China has to work within.

This document establishes the elements and basic principles of network security information sharing activities, and describes the scope and process of sharing activities. This document applies to network security information sharing activities between various organizations or individuals.

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 25069-2022 Information security technical terms

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2022 and the following apply to this document.

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

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

3.2 sharing activities sharing activities By adopting effective organizational mechanisms and technical means, network security information can be reused among participants.

Note. Network security information in sharing activities can be shared one-way, two-way or multi-way.

3.3 sharingmodesharingmode Behavioral patterns of information sharing among participants.

Note. Sharing modes are mainly divided into central sharing mode, point-to-point sharing mode, hybrid sharing mode and group sharing mode.

4 Abbreviations

The following abbreviations apply to this document. P2P. peer-to-peer technology (peer-to-peer)