ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 45940-2025

Cybersecurity technology - Implementation guide of cybersecurity operation and maintenance

网络安全技术 网络安全运维实施指南

Issued on: August 1, 2025 **Implemented on: February 1, 2026**

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

Table of Contents

Preface III
1 Scope 1
2 Normative references 1
3 Terms and Definitions 1
4 Abbreviations 2
5 Overview 2
5.1 Network Security Operation and Maintenance Objectives 2
5.2 Network Security Operation and Maintenance Reference Framework 2
6 Network Security Operation and Maintenance Conditions 3
6.1 Network Security Operation and Maintenance Provider 3
6.2 Network Security Operation and Maintenance Personnel 3
6.3 Cybersecurity Operations Center 4
7 Establishment of network security operation and maintenance business 4
7.1 Network Security Operation and Maintenance Model 4
7.2 Network Security Operation and Maintenance Implementation Content 5
7.3 Network Security Operation and Maintenance Business Establishment Process 6
8 Network Security Operation and Maintenance Implementation 6
8.1 Operation and Maintenance Implementation Process 6
8.2 Operation and Maintenance Management 7
8.3 Identification 8
8.4 Protection 10
8.5 Monitoring and Analysis 11
8.6 Incident Handling 14
8.7 Collaboration 15
8.8 Operation and Maintenance Effectiveness Evaluation 16
Appendix A (Informative) Network Security Operation and Maintenance Capability Assessment 19
A.1 Evaluation Model 19
A.2 Assessment Content 20
A.3 Rating Methodology 21
Appendix B (Informative) Construction of Cybersecurity Operations Center 22
B.1 Construction Model 22

B.2 Site conditions 28
B.3 Platform and Tools 29
Reference 31

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents.

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

This document was drafted by: China Information Security Evaluation Center, Hangzhou Anheng Information Technology Co., Ltd., National Information Center, Beijing Shen Green Alliance Technology Co., Ltd., Beijing Changting Technology Co., Ltd., Qi'anxin Technology Group Co., Ltd., Beijing Bangbang Security Technology Co., Ltd.

Company, China Academy of Information and Communications Technology, Beijing Tianrongxin Network Security Technology Co., Ltd., 360 Digital Security Technology Group Co., Ltd., New Great Wall Technology Co., Ltd., Tsinghua University, China Unicom, Institute of Information Engineering, Chinese Academy of Sciences, Hangzhou Deepin Technology Co., Ltd., State Grid Siji Network Security Technology (Beijing) Co., Ltd., Huaneng Information Technology Co., Ltd., Sangfor Technologies Co., Ltd.

Company, Beijing CESI Technology Development Co., Ltd., Shanghai Sanling Guard Information Security Co., Ltd., China Welfare Lottery Technology Development (Beijing) Co., Ltd.

Company, Shenzhen Broadcom Intelligent Technology Co., Ltd., Rockwell Automation Technology Group Co., Ltd., Antiy Technology Group Co., Ltd., Zhouzhongruan Information Technology Co., Ltd., Beijing Zhiqi'an Technology Co., Ltd., Hangzhou NetEase Zhiqi Technology Co., Ltd., Beijing Winut Technology Co., Ltd.

Co., Ltd., Beijing Shengxin Network Technology Co., Ltd., Beijing Huidu Technology Co., Ltd., Tianyi Cloud Technology Co., Ltd., Guangdong Wangan Technology Co., Ltd.

Company, Ningbo Holly Information Security Research Institute Co., Ltd., Heilongjiang Anxin Yucheng Technology Development Co., Ltd.

The main drafters of this document are: Wang Yan, Yang Jingjing, Yuan Mingkun, Chen Xing, Tian Lidan, Liu Bei, Yang Ying, Cao Jia, Li Yunlei, Xu Yuna, Tian Baosong, Yang Kun,

Zhang Long, Ma Yu, Chen Xiangxi, Zhao Xiangnan, Fang Ning, Dai Hanglv, Yang Jiahai, Bai Jun, Wang Xinru, Wang Yuwei, Yun Han, Liu Jilin, Pan Zhongying, Cui Lei, Liu Biao, Wei Shiguang, Nie Jun, Wang Xiwei, Shen Dongsheng, Zhou Kai, Zhou Lingjun, Xie Meicheng, Zhou Sen, Dudu, Lu Zhigang, Li Wei, Xin Chen, Wei Shushan, Cao Jing, Cui Xin, and Yang Liang. Cybersecurity Technology Network Security Operations and Maintenance Implementation Guide

1 Scope

This document proposes a reference framework for network security operations and maintenance, the conditions for network security operations and maintenance providers and personnel, and the process for establishing operations and maintenance services.

The main work links of network security operation and maintenance, such as operation and maintenance management, identification, protection, monitoring and analysis, incident handling, coordination and effect evaluation, are given. Implementation content.

This document is applicable to network security operation and maintenance providers and demanders. It is used to provide guidance for the implementation of network security operation and maintenance, and to provide guidance for network security operation and maintenance.

It provides a reference for operation and maintenance demanders and third-party organizations to evaluate the implementation effect and capabilities of network security operation and maintenance.

2 Normative references

GB/T 20984

GB/T 20985.2

GB/T 20986-2023

GB/T 22239

GB/T 24363

GB/T 25069-2022

GB/T 28827.3

GB/T 32914-2023

GB/T 39204-2022

GB/T 39786

GB/T 42446

GB/T 43698-2024

GB/T 45577

3 Terms and Definitions

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

3.1 A network security service mode for handling, coordinating and other tasks

To resist cyberspace security threats, control network security risks, ensure business continuity and stable operation, and guarantee business and data Ensure the confidentiality, integrity and availability of data, coordinate technology, processes, personnel and other factors, and continuously carry out management, identification, protection, monitoring and analysis, and event