ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 46820-2025

Cybersecurity technology - Cybersecurity experiment platform - Architecture

网络安全技术 网络安全试验平台 体系架构

Issued on: December 2, 2025 **Implemented on: July 1, 2026**

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

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 involve patents. The issuing organization of this document assumes no responsibility for identifying patents. This document was proposed and is under the jurisdiction of the National Cybersecurity Standardization Technical Committee (SAC/TC260). This document was drafted by: Pengcheng Laboratory, Guangzhou University, National Computer Network Emergency Response Technical Team/Coordination Center, and China Telecom Corporation Limited. Limited Company Research Institute, State Grid Jiangxi Electric Power Co., Ltd., China Automotive Technology and Research Center (Tianjin) Co., Ltd., China Automotive Innovation Technology Co., Ltd. Company, Chongqing Changan Automobile Co., Ltd., China Academy of Information and Communications Technology, Beijing Zhongguancun Laboratory, China Mobile Communications Group, China Mobile Dongtong Communication Group Design Institute Co., Ltd., Sichuan Yilan Technology Co., Ltd., Soft Extreme Network Technology (Beijing) Co., Ltd., Beijing Topsec Network Security Technology Co., Ltd., Qi An Xin Technology Group Co., Ltd., Beijing Antiy Network Security Technology Co., Ltd., Beijing University of Posts and Telecommunications Harbin Institute of Technology (Shenzhen), Beijing Institute of Technology, Tarim University, China Mobile IoT Co., Ltd., and China

Southern Power Grid Research Institute have the following institutions. Limited Liability Company, State Grid Xinjiang Electric Power Research Institute, Shandong Provincial Computing Center (National Supercomputing Center in Jinan), China Information Security Evaluation Center, National Industrial Information Security Development Research Center, State Grid Shandong Electric Power Research Institute, China Engineering The Institute of Computer Applications, Institute of Physics, Xingtang Communication Technology Co., Ltd., Digital Hunan Co., Ltd., and Sinopec Safety Engineering Research Institute have Limited Liability Company, H3C Technologies Co., Ltd., Hangzhou Anheng Information Technology Co., Ltd., Nanjing Saining Information Technology Co., Ltd., Yongxin Zhicheng Technology Group Co., Ltd., Beijing NSFOCUS Technology Co., Ltd., Beijing Times Newway Information Technology Co., Ltd., and Bozhi Security Technology Joint-stock company, Shaanxi Provincial Information Engineering Research Institute, Xi'an Jiaotong University Jabil Network Technology Co., Ltd., Guangdong Weichen Information Technology Co., Ltd. Company, Information Center of Guangdong Power Grid Co., Ltd., Guangdong Yingshi Computer Technology Co., Ltd., Shaanxi Provincial Network and Information Security Evaluation Center, CAS Information Security Common Technology National Engineering Research Center Co., Ltd., Blue Elephant Standard (Beijing) Technology Co., Ltd., Inner Mongolia University of Technology Venustech Information Technology Group Co., Ltd. and Beijing Hillstone Networks Technology Co., Ltd. The main drafters of this document are. Jia Yan, Li Shudong, Han Weihong, Hu Ning, Gu Zhaoquan, Xiang Wenli, Zheng Zhibin, Liu Xinran, Wang Shuai, and Jin Huamin. Qiu Rixuan, Wang Gang, Li Runheng, Wang Wenlei, Tian Zhihong, Yin Lihua, An Lun, Fu Yulong, Zhang Liwu, Xie Wei, Wang Dongbin, He Kexun, Yang Yanzhao Li Feng, Zhao Dawei, Zhang Jiawei, Chen Dewei, Qiu Xinyi, Jing Xiao, Mei Yangyang, Zheng Tao, Yu Tao, Xiang Xiayu, Meng Lingxiao, Luo Cui, Li Zongzhe, Tao Sha Cui Mufan, Dong Hang, Zhang Gaoshan, Yu Lei, Xu Peng, Wang Yan, Liu Lijun, Gao Kun, Liu Yong, Meng Nan, Wang Xiangyang, Sun Yaping, Guo Chao, Zhao Chao, Wei Shengjun Liang Zhihong, Liu Xin, Yang Yiwei, Shen Wuqiang, Feng Yongsheng, Yin Mingyong, Xie Jiajun, Wan Xiaolan, Yu Zhengchen, Zheng Yi, Hu Zhifeng, Zhang Yong, He Jianfeng Chen Lirong, Miao Chunyu, Zhang Chao, Hu Jianxun, Song Cheng, Lin Yanzhong, Hu Jixiang, Chen Jun, Meng Qi, Wang Guowei, Cao Deshun, Xiao Yanjun, Zhang Hongyan, Hu Yue Wu Jiang, Yan Wei, Yang Tianshi. Network security technology Network security test platform architecture

1 Scope

GB/T 46820-2025 is the Chinese national standard covering the cyber range - the isolated environment in which attacks are run against a replica of a real network for research, exercise and training, with the virtualisation, the traffic generation, the isolation that must not leak and the instrumentation that records what happened. First edition. It was issued on 2 December 2025 and has been in force since 1 July 2026, as a first edition. The document is under the responsibility of the Standardization Administration of China. This page is

published from the official record of the 2025 edition; the clause text of a standard this recent is not yet in circulation, and the figures, limits and tables it contains are those of the document itself, delivered in full with the English translation.

This document establishes the system architecture of the network security testing platform, including the overall architecture and component functions. This document applies to the design, development, and construction of network security testing platforms.

2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included. For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies. This document.

GB/T 20986 Information Security Technology - Guidelines for Classification and Grading of Network Security Incidents

GB/T 22239 Information Security Technology - Basic Requirements for Network Security Level Protection

GB/T 25069 Information Security Technical Terminology

GB/T 25070 Information Security Technology - Technical Requirements for Security Design of Network Security Level Protection

3 Terms and Definitions

The terms and definitions defined in GB/T 25069 and GB/T 20986, as well as the following terms and definitions, apply to this document.

3.1 Experimental activities such as network security technology verification, network security capability testing and evaluation, and network attack and defense training are conducted in a simulation environment.

Note. When used as a compound word in this document, it is also referred to as "experiment" or "experimental task".

3.2 Information systems that provide the necessary operating environment for conducting cybersecurity experiments.

3.3 target network A simulated network was constructed on a network security testing platform using virtual, physical, and simulation modeling technologies, based on the experimental requirements.

Note. Depending on the experimental requirements, the target network includes virtual or

physical target devices, attack devices, springboard devices, and defense devices used to support the experimental activities. And the network devices and network links connecting the various devices; the target network also includes the simulated network behavior.

4.Abbreviations The following abbreviations apply to this document.