ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 42583-2023

Information security technology - Technical specifications for government network security monitoring platform

信息安全技术 政务网络安全监测平台技术规范

Issued on: May 23, 2023 **Implemented on: December 1, 2023**

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

Table of Contents

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 contents of this document may refer to patents: The issuing agency of this document assumes no responsibility for identifying patents: This document is proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260): This document was drafted by: State Information Center, Beijing Guoxin Jingning Information Security Technology Co:, Ltd:, the Third Research Institute of the Ministry of Public Security, and State Information Technology Co:, Ltd: Information Technology Security Research Center, China Information Security Evaluation Center, Institute of Information Engineering, Chinese Academy of Sciences, AsiaInfo Technology (Chengdu) Co:, Ltd:, Huawei Technologies Co:, Ltd:, Qi Anxin Technology Group Co:, Ltd:, Beijing Weibu Online Technology Co:, Ltd:, Sangfor Technology Co:, Ltd: Company, Beijing Tianrongxin Network Security Technology Co:, Ltd:, New H3C Technology Co:, Ltd:, Hangzhou Anheng Information Technology Co:, Ltd:, Beijing Qihoo Technology Co:, Ltd:, Venustech Information Technology Group Co:, Ltd:, Hengan Jiaxin (Beijing) Technology Co:, Ltd:, Guangdong Yingshiji Computer Technology Co:, Ltd:, Inspur Cloud Information Technology Co:, Ltd:, Beijing Zhongke Security Technology Co:, Ltd:, Beijing Zhongce Anhua Technology Co:, Ltd: company: The main drafters of this document: Lu Kai, Liu Bei, Yan Guixun, Cheng Hao, Zhao Ruibin, Wu Aming, Wen Bo, Yuan Zhiqian, Ren Weihong, Wu Xian, Yao Jiaming, Li Juan, Ma Hongxia, Wang Zhenlei, Yang Qingze, Wang Wei, Zhang Erming, Xue Feng, Zhang Kuan, Ye Runguo, An Gaofeng, Wan Xiaolan, Su Qibo, Zhang Yi, Du Yu, Shi Shuai, Lin Yanzhong, Dong Shu, Jia Bochao, Yao Yuangang: Information Security Technology Technical specifications for government network security monitoring platform

1 Scope

GB/T 42583-2023 specifies what the monitoring platform watching over a government network has to be able to do. Public administration networks are an attractive target and an awkward one to defend: they span many agencies, run systems of very different ages, and hold data whose loss is measured in public consequence rather than in revenue. A monitoring platform is the layer that is supposed to notice, and its usefulness depends entirely on parts that are easy to specify badly. This document sets out the platform's technical architecture, the scope and objects it monitors, and the classification of its requirements, then divides those requirements into general and extended. The general requirements follow the path the data actually takes - collection and preprocessing, storage, the data bus, analysis, and display and application - and the extended requirements cover what is added on top. For each it gives the corresponding testing and evaluation method, so that conformance can be demonstrated rather than declared. It applies to the design, construction, operation and maintenance, and test evaluation of such platforms. Under ICS 35.030 and CCS L80, it is written for the agencies procuring these systems, the vendors building them and the laboratories testing them.

This document specifies the general technical requirements, extended technical requirements, and testing and evaluation methods of the government network security monitoring platform: This document is applicable to the design, construction, operation and maintenance, and test evaluation of the government network security monitoring platform:

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text: Among them, dated references For documents, only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to this document:

GB/T 25069 Information Security Technical Terms

GB/T 32924 Information Security Technology Network Security Early Warning Guidelines

3 Terms and Definitions

The following terms and definitions defined in GB/T 25069 and GB/T 32924 apply to this document: 3:1 government network governmentnetwork A dedicated network that carries non-secret government affairs:

Note: Including the basic network, as well as information technology facilities and resources such as government cloud, government application and government data deployed on the basic network, mainly divided into Government WAN, government MAN and government

LAN: 3:2 A government affairs network that realizes interconnection among various government affairs departments in the same city: 3:

3 It connects the government affairs LAN or government affairs metropolitan area network in different regions to realize the government affairs network of remote communication: 3:

4 Through real-time collection, monitoring and analysis of network traffic, security logs, threat intelligence and other data, network risks can be dynamically identified and discovered: Attack threats, asset vulnerabilities, and security events, as well as a system for early warning notification and visual display: 3:5 alarm alert Analyze network security elements, and when an attack or intrusion is found, the platform will automatically send a notification to the relevant personnel: 3:6 warning warning For upcoming or ongoing network security incidents or threats, security warnings issued in advance or in time: [Source: GB/T 32924-2016, 3:5]