



# 中华人民共和国公共安全行业标准

GA/T 1735.1—2020

---

## 网络安全等级保护检查工具技术规范 第 1 部分：安全通用检查工具

Technical specifications of inspection tools for cybersecurity classified protection—Part 1: General safety inspection tools

2020-08-04 发布

2020-12-01 实施

---

中华人民共和国公安部 发布

## 目 次

前言 .....	Ⅲ
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语、定义和缩略语 .....	1
3.1 术语和定义 .....	1
3.2 缩略语 .....	2
4 总体要求 .....	3
4.1 检查工具设计原则 .....	3
4.2 检查工具的组成 .....	3
4.3 升级和接口要求 .....	5
5 功能要求 .....	5
5.1 工具管理系统功能 .....	5
5.2 安全通用要求检查工具功能 .....	13
5.3 选配检查工具功能 .....	20
5.4 辅助检查设备功能 .....	22
6 界面要求 .....	23
6.1 工具管理系统界面要求 .....	23
6.2 检查工具界面要求 .....	27
7 性能要求 .....	27
7.1 工具管理系统性能 .....	27
7.2 安全通用要求检查工具性能 .....	27
7.3 选配检查工具性能 .....	29
8 安全要求 .....	31
8.1 工具管理系统安全 .....	31
8.2 U口检查工具安全 .....	34
8.3 网口检查工具安全 .....	34
8.4 无线 WIFI 检查工具安全 .....	35
9 兼容性要求 .....	35
附录 A (规范性附录) 党政机关和行业主管部门检查指标 .....	36
附录 B (规范性附录) 备案单位检查指标 .....	40
附录 C (规范性附录) 安全通用要求检查指标 .....	43
C.1 第一级安全通用要求检查指标 .....	43
C.2 第二级安全通用要求检查指标 .....	47

C.3 第三级安全通用要求检查指标(含关键信息基础设施) .....	56
C.4 第四级安全通用要求检查指标(含关键信息基础设施) .....	70
附录D(规范性附录) 政府网站安全检查指标 .....	87
D.1 政府网站安全检查指标 .....	87
D.2 政府网站漏洞情况检查内容 .....	90
附录E(规范性附录) 网络安全等级保护检查工具总体架构 .....	91
E.1 检查工具的总体架构 .....	91
E.2 检查工具与重要信息系统基础数据库管理系统的关系 .....	91
附录F(规范性附录) 安全检查工作流程概述 .....	93
附录G(资料性附录) 检查工具规格要求 .....	95
G.1 等级保护检查专用工具规格要求 .....	95
G.2 辅助检查设备规格要求 .....	100
参考文献.....	103

## 前 言

GA/T 1753《网络安全等级保护检查工具技术规范》已经或计划发布以下部分：

——第1部分：安全通用检查工具；

——第2部分：工控系统检查工具；

——第3部分：应急处置工具；

.....

本部分为 GA/T 1753 的第 1 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由公安部网络安全保卫局提出。

本部分由公安部信息安全标准化技术委员会归口。

本部分起草单位：公安部网络安全保卫局、公安部第三研究所。

本部分主要起草人：郭启全、范春玲、祝国邦、陶源、李末岩、郭俸明、张宇翔、罗铮、郑国刚、马思远。

# 网络安全等级保护检查工具技术规范

## 第 1 部分：安全通用检查工具

### 1 范围

GA/T 1753 的本部分规定了公安机关开展网络安全等级保护检查工作时所装备检查工具的技术规范。

本部分适用于网络安全等级保护检查工具(以下简称为“检查工具”)的开发、设计、检测、使用等环节的工作,有利于提高网络安全等级保护工作的规范化和标准化。

### 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GA/WA 1001—2013 网安数据元素集

GA/WA 1002—2013 网安数据元素代码集

### 3 术语、定义和缩略语

#### 3.1 术语和定义

GB 17859、GB/T 22239 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

##### 3.1.1

**网络安全等级保护检查工具** **inspection tool for cybersecurity classified protection**

公安机关开展网络安全检查工作,具有规范检查、工具调用、结果展示等功能,集成定制专门的安全检查工具,为公安机关网络安全执法检查提供专业检查知识和检查方法,并实现对获取数据的关联分析、统计比对、处理流转等功能的一体化专用便携式检查装备。

##### 3.1.2

**网络安全等级保护检查专用工具** **special inspection tool for cybersecurity classified protection**

由网络安全等级保护检查工具管理系统、检查指标库、检查知识库和技术检测工具库等组成的设备。

##### 3.1.3

**U 口检查工具** **inspection tool of USB port**

通过专用 USB 接口连接到检查对象上的检查工具。

##### 3.1.4

**网口检查工具** **inspection tool of network port**

通过网络接口连接到检查对象上的检查工具。