

# 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 ..... 4

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..... 11

    5.3 选配检查工具功能..... 16

    5.4 辅助检查设备功能..... 18

6 界面要求 ..... 19

    6.1 工具管理系统界面要求..... 19

    6.2 检查工具界面要求..... 22

7 性能要求 ..... 23

    7.1 工具管理系统性能..... 23

    7.2 安全通用要求检查工具性能..... 23

    7.3 选配检查工具性能..... 24

8 安全要求 ..... 26

    8.1 工具管理系统安全..... 26

    8.2 U 口检查工具安全 ..... 28

    8.3 网口检查工具安全..... 29

    8.4 无线 WIFI 检查工具安全..... 29

9 兼容性要求 ..... 29

附录 A （规范性附录） 党政机关和行业主管部门检查指标..... 31

附录 B （规范性附录） 备案单位检查指标..... 35

附录 C （规范性附录） 安全通用要求检查指标..... 39

    C.1 第一级安全通用要求检查指标..... 39

    C.2 第二级安全通用要求检查指标..... 43

    C.3 第三级安全通用要求检查指标（含关键信息基础设施） ..... 53

    C.4 第四级安全通用要求检查指标（含关键信息基础设施） ..... 68

附录 D （规范性附录） 政府网站安全检查指标..... 84

    D.1 政府网站安全检查指标..... 84

    D.2 政府网站漏洞情况检查内容..... 87

附录 E （规范性附录） 网络安全等级保护检查工具总体架构..... 88

|                                         |     |
|-----------------------------------------|-----|
| E.1 检查工具的总体架构.....                      | 88  |
| 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.....        | 88  |
| 附录 F （规范性附录） 安全检查工作流程概述.....            | 90  |
| F.1 安全检查工作流程.....                       | 90  |
| F.2 网络安全等级保护备案表.....                    | 91  |
| 附录 G （规范性附录） 检查工具与重要信息系统基础数据库的接口规范..... | 98  |
| G.1 交互数据加密方式.....                       | 98  |
| G.2 交互数据的数据元素集及数据元素代码集.....             | 98  |
| 附录 H （资料性附录） 检查工具规格要求.....              | 99  |
| H.1 等级保护检查专用工具规格要求.....                 | 99  |
| H.2 辅助检查设备规格要求.....                     | 103 |
| 参考文献 .....                              | 107 |

## 前 言

GA/T ××××《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 ××××的第1部分。

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息安全标准化技术委员会归口。

本标准起草单位：公安部网络安全保卫局、公安部第三研究所。

本标准主要起草人：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 ××××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的一体化专用便携式检查装备，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。

##### 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

**检查指标库** inspection index library

由具体的网络安全等级保护检查指标所组成。

##### 3.1.4

**检查知识库** inspection knowledge library

由具体的检查知识（包括检查方法、检查结果判定依据和风险提示）所组成。

##### 3.1.5

**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。

**3.1.6****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。

**3.2 缩略语**

下列缩略语适用于本文件。

PID: 进程唯一标识 (ProcessID)

TCP: 传输控制协议 (Transmission Control Protocol)

UDP: 用户数据报协议 (User Datagram Protocol)

ASP: 动态服务器页面 (Active Server Pages)

ASPX: 动态服务XML格式Web页面 (Active Server Pages XML docx)

JSP: java服务器页面 (Java Server Pages)

PHP: 超文本预处理器 (Professional Hypertext Preprocessor)

CSS: 层叠样式表 (Cascading Style Sheets)

IIS: 互联网信息服务 (Internet Information Services)

SNMP: 简单网络管理协议 (Simple Network Management Protocol)

SSH: 安全外壳协议 (Secure Shell)

CDP: CISC0发现协议 (Cisco Discovery Protocol)

SMB: 客户端与服务器之间的信息沟通协议 (Server Message Block)

FTP: 文件传输协议 (File Transfer Protocol)

RDP: 远程桌面协议 (Remote Desktop Protocol)

POP3: 邮局协议版本3 (Post Office Protocol - Version 3)

HTTP: 超文本传输协议 (HyperText Transfer Protocol)

VNC: 虚拟网络控制台 (Virtual Network Console)

CGI: 通用网关接口 (Common Gateway Interface)

URL: 统一资源定位符 (Uniform/Universal Resource Locator)

CVE: 公共漏洞和暴露 (Common Vulnerabilities & Exposures)

CNNVD: 中国国家信息安全漏洞库 (China National Vulnerability Database of Information Security)

CVSS: 通用漏洞评分系统 (Common Vulnerability Scoring System)

IPV6: 互联网协议第六版 (Internet Protocol Version 6)

WIFI: 无线保真 (Wireless Fidelity )

WAPI: 无线局域网鉴别和保密基础结构 (Wireless LAN Authentication and Privacy Infrastructure)

SSID: 服务集标识 (Service Set Identifier)

SSD: 固态硬盘 (Solid State Drives)

HDMI: 高清晰度多媒体接口 (High Definition Multimedia Interface)

BD: 蓝光光碟 (Blue-ray Disc)

DVD: 高密度数字视频光盘 (Digital Video Disc)

CD: 光盘 (Compact Disc)

VGA: 视频图形阵列 (Video Graphics Array)

4 总体要求

4.1 检查工具设计原则

4.1.1 便携性、易用性

检查工具应便于携带和现场使用，界面友好，操作方式简捷，易于操作使用，检查任务可以并行。

4.1.2 专业性、标准性

工具检查指标库应严格依据等级保护政策和标准研发，应涵盖公安机关开展网络安全检查工作的检查指标全集。检查指标应严格依据有关国家网络安全政策和标准进行研发，可以由检查人员自行维护和选择使用，形成检查模板，确保检查数据的格式统一。

4.1.3 规范性、扩展性

工具检查知识库应封装专业检查知识和专业分析模型，可按照内置的分析模型对检查数据进行分类、统计、关联、分析和比对。可根据检查工作的需要，对检查内容进行扩展。检查工具的升级维护方式应简捷，易于维护。

4.1.4 安全性、保密性

检查专用工具应安全可靠，不得影响检查对象的稳定运行，不得影响检查对象所在网络的正常通讯。检查数据应采用国家商密办批准的国产商用密码产品加密，并具有检查数据的痕迹清除能力，确保检查数据的安全性和保密性。

4.1.5 专用性、可维护性

检查工具为警用执法装备，应拥有唯一编码，便于核对检查工具的生产厂商和使用单位。生产厂商应对检查工具的出厂情况留有详细记录，并指定售后技术支持部门负责检查工具的售后维护与技术支持。未经允许，生产厂商不得擅自提供该装备。

4.2 检查工具的组成

4.2.1 检查工具总体要求

检查工具由网络安全等级保护检查专用工具和辅助检查设备组成。网络安全等级保护检查专用工具集成了人机交互界面、检查指标库、检查知识库、工具管理模块、系统管理模块和专用接口。技术检测工具库是网络安全等级保护检查专用工具的重要组成部分，包括通用要求检查工具、选配工具和新技术新应用检查工具等。

检查工具组成如图1所示。

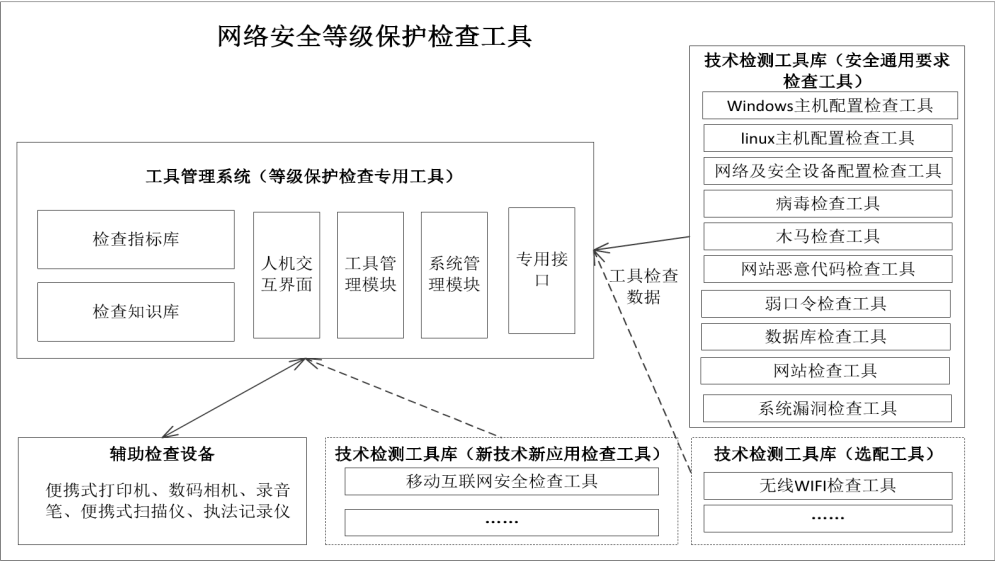


图1 网络安全等级保护检查工具组成示意图

#### 4.2.2 工具管理系统

工具管理系统是网络安全等级保护检查专用工具的重要组成部分，包括：人机交互界面、检查指标库、检查知识库、工具管理模块、系统管理模块、专用接口。

人机交互界面用于展示重要信息系统基础数据库管理系统下发的检查计划等内容，以及技术检测工具库导入的工具检查数据，并为公安机关提供检查知识引导和检查数据录入的功能。

检查指标库包括：备案单位网络安全工作开展情况检查（备案单位网络安全工作的组织部署、各项工作开展情况、网络安全责任制落实、信息系统运维情况等）、信息系统定级备案检查（网络安全定级工作情况、网络安全备案工作情况及定级备案调整情况等）、等级测评和安全建设整改工作情况、网络安全自查和整改工作情况、信息系统关键技术措施落实情况、信息系统网络安全管理制度落实情况、网络安全事件应急与案事件调查处置等检查内容和检查指标。检查指标库中的指标可以全选、部分选取和新增等方式形成检查模板，以便调用。详见附录A、附录B、附录C和附录D。

工具管理模块提供检查工具的使用帮助说明，升级管理和检查结果管理等功能。

系统管理模块为工具管理系统提供运行维护支撑，包括系统配置、用户管理和日志管理等功能。

专用接口用于检查工具之间的检查数据交互、检查工具的数据导入，以及与重要信息系统基础数据库管理系统之间的数据交互。

#### 4.2.3 技术检测工具库

技术检测工具库包括安全通用要求检查工具、选配工具和新技术新应用检查工具。

安全通用要求检查工具是检查工具应配置的工具，选配工具为各地公安机关根据检查工作的需要而选配的工具，新技术新应用检查工具是预留的扩展工具。检查工具知识库可以对通用要求检查工具的检查结果进行自动分析。通用要求检查工具包括以下检查工具：Windows主机配置检查工具、Linux主机配置检查工具、网络及安全设备配置检查工具、病毒检查工具、木马检查工具、网站恶意代码检查工具、弱口令检查工具、数据库安全检查工具、网站安全检查工具、系统漏洞检查工具。选配工具包括如下检查工具：协同工作处理机、网络设备信息侦测工具、无线WIFI检查工具、网站监测预警工具。

技术检测工具库中的工具在启动时应给出相应的提示信息，用于说明使用该工具进行现场检查时可能对被检查设备运行造成的影响，经被检查单位确认同意后，方可用工具执行现场检查。

### 4.3 升级和接口要求

#### 4.3.1 扩展要求

检查工具中的检查指标库、知识库应涵盖GB/T 22239中所列的相关安全要求。

检查工具应支持GB/T 22239的通用安全要求，并支持云计算、移动互联、物联网和工业控制系统等安全扩展要求。

检查工具应支持自定义检查指标，并可导入到检查指标库中。

检查工具应支持公安机关根据开展网络安全检查工作的需要，从检查指标库中选择合适指标生成检查表的功能。

#### 4.3.2 安全可靠和风险提示

网络安全等级保护检查工具应安全可靠，若因公安机关正确使用工具而导致被检查对象发生故障，检查工具的供应厂商应及时提供相应的技术支持和应急响应，并由检查工具的供应厂商承担相应的经济赔偿责任。

在进行现场检查时，工具管理系统启动时应给出相应的风险提示。只有当公安机关和被检查单位共同确认并接受风险提示所指出的各项风险后，才可以进行现场检查。

#### 4.3.3 升级维护

检查工具应提供升级和维护管理功能，应支持工具管理系统、技术检测工具、指标库、知识库的升级和维护。

5 功能要求

5.1 工具管理系统功能

5.1.1 业务功能

5.1.1.1 业务功能总体要求

工具管理系统应能支持公安机关相关部门的日常工作和检查工作。其中日常工作是指公安机关的检查人员从重要信息系统基础数据库管理系统下载相应的电子文档和电子表单,检查人员通过工具管理系统导入并使用这些电子文档和电子表单为信息系统运营使用单位提供指导的工作;检查工作是指公安机关的检查人员从重要信息系统基础数据库管理系统下载相应的检查计划,检查人员通过工具管理系统导入检查计划并根据检查计划对信息系统运营使用单位进行检查的工作。

检查工具的总体架构,以及与重要信息系统基础数据库管理系统的关系详见附录E。

5.1.1.2 日常工作业务功能

工具管理系统应支持公安机关检查人员的日常工作业务,应满足如下要求:

- a) 支持重要信息系统基础数据库管理系统下发的所有模板(包括电子文档、电子表单)的展示;
- b) 支持下发模板(包括电子文档、电子表单)的数据录入;
- c) 支持将数据录入完毕的电子文档和电子表单上报到重要信息系统基础数据库管理系统中。

5.1.1.3 检查工作业务功能

工具管理系统应支持公安机关检查人员的检查工作业务,应满足如下要求:

- a) 检查准备工作支持:
  - 1) 独立创建检查计划;
  - 2) 导入检查计划;
  - 3) 编辑与打印检查通知书;
  - 4) 生成检查记录表单。
- b) 现场检查支持:
  - 1) 执行检查;
  - 2) 打印现场检查记录;
  - 3) 检查任务导出;
  - 4) 检查任务多人协同工作;
  - 5) 检查数据汇总到等级保护检查专用工具中。
- c) 数据汇总工作支持:
  - 1) 编辑反馈意见功能;
  - 2) 检查结果导出与刻录等功能。

安全检查工作的检查准备、现场检查和数据汇总三个工作阶段的详细内容如图2所示。

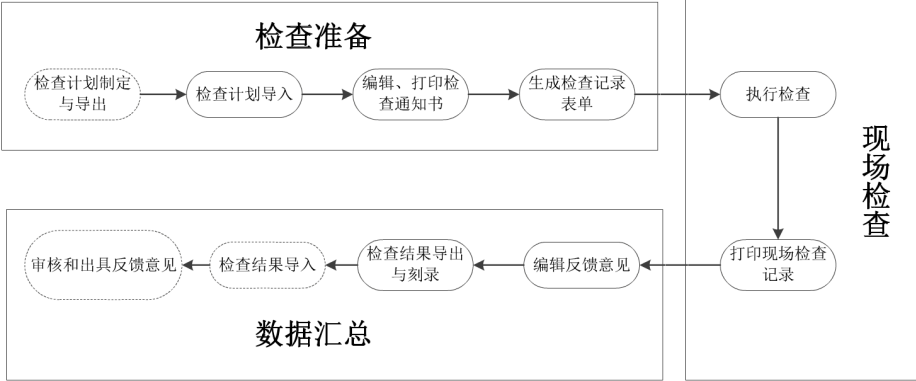


图2 网络安全等级保护检查工具检查工作流程图

如图2所示，工具管理系统提供独立创建检查计划、导入检查计划、编辑与打印检查通知书、生成检查记录表单、执行检查、打印现场检查记录、编辑反馈意见、检查结果导出与刻录等功能；重要信息系统基础数据库管理系统提供检查计划制定与导出、检查结果导入、审核和出具反馈意见等功能。详细的检查流程如附录F中F.1所示。

工具管理系统应支持检查任务导出、检查任务并发执行和检查数据汇总功能，方便检查人员进行检查任务分配和多人协作，便于现场检查，提升检查工作效率。

#### 5.1.1.4 检查计划导入

检查计划由重要信息系统基础数据库管理系统制定和导出，导出的检查计划应能导入到工具管理系统中。

检查计划导入是将重要信息系统基础库导出的内容全部导入到检查工具中，检查计划内容包括：

- a) 被检查单位基本状况（含已经发布的行业网络安全文件和标准、上次检查工作中发现的问题等）；
- b) 公安机关开展此次安全检查的工作背景材料等；
- c) 网络安全等级保护备案表相关数据：用于核对被检查单位的备案信息有无变化，该备案信息来自于重要信息系统基础数据库管理系统，若无备案信息，则需提供备案信息表模板并由被检查单位填写。网络安全等级保护备案表模板详见附录F.2；
- d) 检查表单（包括检查任务信息、检查指标信息、检查人员信息、检查指标版本信息等）：
  - 1) 检查任务信息：检查单位信息、检查计划名称、检查计划起止时间等；
  - 2) 检查指标信息：行业主管部门（含中央国家机关）检查指标、备案单位检查指标、信息系统（含政府网站）检查指标等相关信息（相关检查指标详见附录A、附录B、附录C、附录D）；
  - 3) 检查人员信息：检查人员单位、职务、警号、警衔、联系方式等；
  - 4) 检查指标版本信息：工具管理系统对检查计划中的检查指标版本与检查工具内置指标库中的检查指标版本进行比对，当版本不符时给出检查指标版本的升级提醒；
  - 5) 工具管理系统版本信息：工具管理系统对检查计划中的检查工具版本信息与检查工具自身版本进行比对，当版本不符时给出工具管理系统版本升级提醒。
- e) 重要信息系统基础数据库管理系统下发的其他电子文档（例如，word文档形式的执法文书模板）；
- f) 重要信息系统基础数据库管理系统下发的其他电子表单（例如，excel表单形式的IT资产信息调查表模板）。

工具管理系统应提供独立创建检查计划的功能，应支持检查人员自行选择检查指标并执行检查功能。

#### 5.1.1.5 编辑、打印检查通知书

工具管理系统应提供编辑、打印检查通知书的功能，包括：

- a) 编辑、打印检查通知书，用于书面通知被检查单位进行网络安全检查的时间、地点、检查人员等相关信息，以便被检查单位提前做好准备所需材料及接受检查；
- b) 导出网络安全等级保护备案数据（详见附录F.2），将其提交给被检查单位，用于核对被检查单位备案信息有无变化，若无备案信息或备案信息有变更，可要求被检查单位修改核对，并返回给检查单位，检查单位将备案数据导入到工具管理系统用于现场检查，后续在检查结果导入阶段将变更的备案信息上报并更新到重要信息系统基础数据库管理系统；
- c) 打印是否同意使用工具检查的纸质材料，以便让被检查单位书面确认是否同意采用工具进行现场检查。

#### 5.1.1.6 生成检查记录单

工具管理系统应根据检查计划生成相应的检查记录单，检查记录单应列出本次安全检查所使用的检查指标，包括检查范围、检查内容、检查项、检查要点和检查结果录入类型等信息：

- a) 检查范围：是确定行业主管部门、备案单位、重要信息系统、政府网站这四类检查对象的基本情况、定级备案、监测预警等事项；
- b) 检查内容：是对检查范围的细化，例如，系统定级情况、岗位设置情况、安全审计情况等检查事项；
- c) 检查项：是对检查内容的细化，例如，信息系统定级指导情况、信息系统定级执行情况等检查事项；
- d) 检查要点：是对检查项的细化，以确保检查结果记录的惟一性。例如，是否有定级指导的专家名单，是否有同级公安机关等级保护工作办公室的联系人；
- e) 检查结果录入类型：包括选择型、文本型、复合型。选择型是最常用的录入类型，检查人员可以直接选择检查结果记录为“是”、“否”和“不适用”。文本型是需要检查人员录入检查结果记录的录入类型，例如，操作系统国产化率。复合型是在选择型的基础上，录入相关的文本内容。例如，检查要点为“行业主管部门是否发布行业网络安全标准规范？”，如果行业发布了网络安全标准规范，则检查人员选择检查结果记录为“是”，并进一步录入行业标准规范名称、发布时间及发布单位等相关信息。

#### 5.1.1.7 检查执行

工具管理系统应提供检查执行功能，用于将检查过程中通过人员访谈、配置查看、工具检查等方式得到的检查结果录入到工具管理系统中。检查执行应包含如下具体功能：

- a) 针对每个检查要点提供相关的检查方法、检查结果判定依据等检查知识，以便引导检查人员进行现场检查；
- b) 提供检查结果录入功能，要求检查结果录入的类型包括选择型、文本型和复合型；
- c) 提供检查工具检查结果导入功能，要求能自动关联到检查指标并给出判定结果；
- d) 提供检查过程中具体检查对象（例如，主机、网络设备等）的新增、修改和删除功能，要求可以选择已有的检查对象或录入新的检查对象；
- e) 提供检查证据录入和管理功能，将扫描仪、照相机、录音笔等辅助设备采集的证据资料（例如，图片文件、声音文件等）作为检查数据的附件，分类别存储，并且可以根据需要调取查看；执法记录仪的影像文件由检查人员按照公安机关的有关规定处理；
- f) 支持将检查任务导出成检查模板，检查人员能够根据被检查单位情况，灵活分配各自的检查任务，也可以导出检查记录单，提供给被检查单位进行自查，检查人员经现场检查核对无误之后，可以直接将检查记录单数据导入到检查工具中，提高检查效率；
- g) 提供检查结果查询功能，针对检查结果状态（例如，是、否、不适用、未记录）进行查询；
- h) 支持检查工具检查结果信息的展示功能；
- i) 如果检查指标可采用工具进行自动检查，但被检查单位不允许使用工具检查时，可支持以人工填报方式记录检查结果。

#### 5.1.1.8 打印检查结果汇总情况

现场检查完成后应可对检查结果进行汇总统计。检查结果汇总情况应经过检查组组长审核后，方可打印。检查结果汇总情况打印后，应经被检查单位相关人员确认、签字，然后在公安机关留存。

检查结果汇总情况应包含如下信息：被检查单位名称、检查时间、检查地点、检查人员（签名）、被检查单位人员（签名）、检查要点的检查结果记录等相关信息：

- a) 检查结果汇总情况包括检查的统计信息和详细信息，分别供被检查单位的部门负责人和具体负责人员参考；
- b) 检查的统计信息包含此次检查的范围、检查要点数量、检查结果的统计、存在安全风险的检查要点数量等内容。若检查结果汇总情况中无安全风险，则要给出提示说明，待检查人员确认后 方可打印；

- c) 检查的详细信息包含所有检查要点的合规性详细列表。若采用了工具进行检查,则还要包含工具检查的详细内容;
- d) 提示检查人员让被检查单位书面确认,检查工作未对检查对象造成不良影响,检查对象工作正常;
- e) 提示检查人员让被检查单位书面确认,检查结果记录内容真实完整。

#### 5.1.1.9 编辑反馈意见

反馈意见是检查人员根据现场检查情况和检查记录给被检查单位反馈的意见,用于指出被检查单位在重要信息系统和政府网站安全保护工作中的成绩和存在的不足,并给出下一步工作意见和建议等:

- a) 反馈意见包括:反馈意见书、整改通知书、通报书、约谈通知书、行政处罚决定书、停机整顿通知书等;
- b) 反馈意见的文书模板由重要信息系统基础数据库管理系统统一下发到检查工具中,工具管理系统支持对反馈意见进行在线编辑(文书编号支持手工编辑),并将编辑完毕的反馈意见上报到重要信息系统基础数据库管理系统;
- c) 工具管理系统对反馈意见文书的打印操作进行日志记录。

#### 5.1.1.10 检查结果导出与刻录

检查结果导出是指将检查结果记录等相关信息(包括网络安全等级保护备案表数据,以及工具管理系统的版本信息和检查指标的版本信息)导出,以支持后续导入到重要信息系统基础数据库管理系统中进行汇总分析。检查结果导出应包含如下具体功能:

- a) 要求采用国家商密办批准的国产商用密码产品对检查数据进行加密后导出,以确保检查数据的保密性;
- b) 导出的检查数据按照指定的接口规范导出,接口规范详见附录G;
- c) 工具管理系统根据不同类型检查任务自动生成该任务类型的检查报告。检查报告包含不符合项和风险描述等信息。

### 5.1.2 检查指标库

#### 5.1.2.1 检查指标库要求

检查指标库是网络安全等级保护检查工作的检查依据,检查人员依据检查指标库选择具体的检查指标执行检查任务,检查指标库的层级结构为:检查范围、检查内容、检查项、检查要点和检查结果录入类型。检查范围由多个检查内容组成,检查内容由多个检查项组成,检查项由多个检查要点组成,检查要点可以有多种检查结果录入类型。

检查指标库须按照检查范围、检查内容、检查项和检查要点这四个层级来细分,以确保检查结果的惟一性。指标库的逻辑结构如图3所示。

检查指标库的具体要求如下:

- a) 应按照检查范围、检查内容、检查项、检查要点和检查结果录入类型的层级结构提供党政机关和行业主管部门的所有检查指标(详见附录A);
- b) 应按照检查范围、检查内容、检查项、检查要点和检查结果录入类型的层级结构提供备案单位的所有检查指标(详见附录B);
- c) 应按照检查范围、检查内容、检查项、检查要点和检查结果录入类型的层级结构提供信息系统的所有检查指标(详见附录C);
- d) 应按照检查范围、检查内容、检查项、检查要点和检查结果录入类型的层级结构提供政府网站的所有检查指标(详见附录D);
- e) 应能在公安部发布年度检查方案的两个月内完成新增指标的更新。



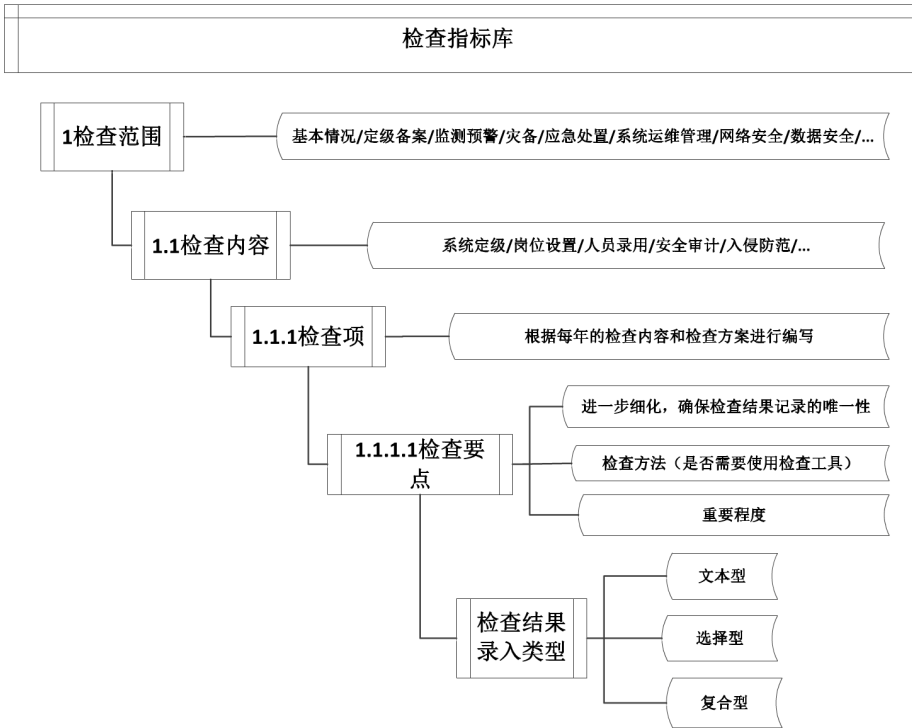


图3 指标库的逻辑结构图

5.1.2.2 检查指标库升级维护

检查指标库应定期升级，当检查指标变更时，应及时升级最新的指标库，以符合当前检查的具体要求。提供以下具体功能：

- a) 检查指标库升级功能，可以对检查指标库进行手动更新；
- b) 升级检测和提醒功能；
- c) 检查指标库升级留有日志记录；
- d) 检查指标库的查询和浏览功能。

5.1.3 检查知识库

5.1.3.1 检查知识库要求

检查知识库中应封装重要信息系统安全检查工作实施经验、专家知识和分析模型，使工具管理系统的检查内容和检查记录可以按照知识库内置的知识、模型和规则进行自动化分析，为重要信息系统安全检查工作提供检查方法、检查结果判定依据、工具检查结果自动分析、不符合项的风险提示，并且针对不同类型检查任务可以自动生成相应的检查结果判定记录。

检查知识库的具体要求如下：

- a) 可对党政机关和行业主管部门的所有检查指标（详见附录A）提供相应的检查方法、检查结果判定依据和不符合项的风险提示；
- b) 可对备案单位的所有检查指标（详见附录B）提供相应的检查方法、检查结果判定依据和不符合项的风险提示；
- c) 可对信息系统的所有检查指标（详见附录C）提供相应的检查方法、检查结果判定依据和不符合项的风险提示；
- d) 可对政府网站的所有检查指标（详见附录D）提供相应的检查方法、检查结果判定依据和不符合项的风险提示；
- e) 可对安全通用要求检查工具（安全通用要求检查工具的功能见5.2）的检查结果进行自动分析，并给出相应检查指标的判定结果（例如，是、否、不适用）；
- f) 可针对不同类型检查任务，对检查结果进行自动分析，并自动生成相应的检查结果判定记录；

- g) 可针对不同类型检查任务,自动生成安全检查结论,安全检查结论包括存在的安全风险点数量;
- h) 知识库定期更新,至少每年进行一次知识库更新;
- i) 当检查指标库或检查工具发生变更时,要同步更新知识库,应在公安部发布年度检查方案的两个月内或检查工具更新后的两个月内完成知识库的更新。

#### 5.1.3.2 检查知识库升级维护

检查知识库应定期升级,当检查指标变更或者检查知识库更新时,应及时升级,使检查知识库匹配最新的检查指标。提供以下具体功能:

- a) 提供检查知识库升级功能,可对检查知识库进行手动更新;
- b) 提供升级检测和提醒功能;
- c) 检查知识库升级留有日志记录。

#### 5.1.4 工具管理

##### 5.1.4.1 使用帮助说明

使用帮助说明应包含以下具体内容:

- a) 提供检查工具的使用风险说明;
- b) 提供检查工具的使用环境说明;
- c) 明确给出检查工具不能在工控系统环境中使用的说明;
- d) 提供工具适用范围的查看功能,用于检查人员在检查之前了解检查工具,引导检查人员选择使用;
- e) 提供工具使用操作的查看功能,便于检查人员了解检查工具的使用操作步骤,并作为使用参考。

##### 5.1.4.2 升级管理

升级管理应包含如下功能:

- a) 检查工具供应商通过技术支持网站提供检查工具升级提示功能,当检查工具有更新时,用户可以进行检查工具的升级操作;
- b) 检查工具升级操作在工具管理系统中留有日志记录。

##### 5.1.4.3 结果管理

结果管理应包括如下功能:

- a) 提供结果导入功能,可由检查人员将工具检查结果导入到工具管理系统中;
- b) 结果导入操作留有日志记录;
- c) 提供结果分析,依据内置知识库自动对工具检查结果进行分析,自动判别相应检查指标的检查结果。

#### 5.1.5 系统管理

##### 5.1.5.1 配置管理

配置管理用于对工具管理系统进行系统参数配置。保证工具管理系统正常运行。

##### 5.1.5.2 用户管理

用户管理用于对工具管理系统的用户进行管理,组长可以添加组员用户,用户可以自行修改密码。

##### 5.1.5.3 日志管理

日志管理应包括如下功能:

- a) 日志查看功能,可查看操作日期、操作用户、操作对象等日志记录;
- b) 日志筛选功能;
- c) 日志导出备份功能。

##### 5.1.5.4 系统升级

工具管理系统应提供如下系统升级管理功能:

- a) 升级功能,升级操作简单易用;
- b) 技术支持网站提供升级提示功能;

- c) 升级操作留存日志记录。

### 5.1.6 数据加密保护

工具管理系统应对系统数据进行加密保护，系统数据加密应采用国产商用密码产品并满足如下要求：

- 工具管理系统通过USB接口对国产商用密码产品进行调用；
- 工具管理系统通过调用存放在国产商用密码产品中的密钥来对重要信息系统基础数据库管理系统的导出文件进行解密；
- 工具管理系统通过调用存放在国产商用密码产品中的密钥来对要导入到重要信息系统基础数据库管理系统的文件进行加密；
- 国产商用密码产品支持密钥的离线更新；
- 检查工具研发厂商在每年的3月份及时将国产商用密码产品的密钥升级包提供给公安部网络安全保卫相关主管部门，并完成检查工具使用单位的国产商用密码产品的密钥的更新。

## 5.2 安全通用要求检查工具功能

### 5.2.1 检查工具通用要求

安全通用要求检查工具为网络安全等级保护检查工具的基本配置工具，包括U口检查工具和网口检查工具，安全通用要求检查工具操作应简捷友好，检查结果采用国产商用密码算法对检查数据自动加密。

U口检查工具和网口检查工具在启动时应给出相应的风险提示信息，说明使用工具检查时可能对被检查设备运行造成的影响，经被检查单位确认同意后，方可执行检查。

### 5.2.2 U口检查工具库

#### 5.2.2.1 Windows 主机配置检查工具

Windows主机配置检查工具是用于对安装Windows操作系统的主机进行配置信息自动化采集的工具。该工具需要通过专用USB转换线连接到被检查的Windows主机USB接口上，然后自动对Windows操作系统的配置信息进行采集。该工具的功能及适用范围如表1所示。

表1 Windows主机配置检查工具功能

| 序号 | 功能模块   | 功能要求                                                                                    |
|----|--------|-----------------------------------------------------------------------------------------|
| 1  | 系统信息   | 可检测到被检测主机的计算机名、操作系统类型、版本、开机时间、可用内存大小、磁盘大小、操作系统所在路径、共享目录                                 |
| 2  | 硬件信息   | 可检测到 CPU、内存、主板、硬盘、网卡等硬件信息                                                               |
| 3  | 启动项    | 可显示当前系统启动项的所有程序、进程、路径、运行方式                                                              |
| 4  | 异常服务   | 用于检测当前系统不必要的多余服务（默认仅检测 Remote Registry、Task Sheduler、Print Spooler、Terminal Services）服务 |
| 5  | 安全策略   | 显示账户和口令有关的安全策略，包含口令最长使用期限，长度最小值、锁定时间阈值等                                                 |
| 6  | 账户信息   | 显示当前系统内所有的账户，包含隐藏（影子）账户及活动状态                                                            |
| 7  | 审计策略   | 显示审核策略更改、审核登录事件、审核对方访问、审核进程跟踪、审核目录服务访问、审核特权使用、审核系统事件、审核账户登录事件、审核账户管理等                   |
| 8  | 系统安全补丁 | 显示已安装的更新程序、其中包含了补丁名称、补丁发布日期、补丁安装日期、严重级别、补丁描述                                            |
| 9  | 软件安装   | 显示已安装的软件，软件总数，并针对软件进行了分类，同时支持智能识别系统安装的反病毒软件、病毒库升级日期                                     |
| 10 | 进程扫描   | 显示了系统当前活的的进程、PID                                                                        |
| 11 | 活动端口   | 显示当前开放的 TCP/UDP 端口、连接状态、进程对应路径                                                          |
| 12 | 用户权限   | 显示用户、访问权限与操作系统安全相关的状态                                                                   |

表1 (续)

| 序号 | 功能模块   | 功能要求                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13 | 安全选项   | 显示与操作系统安全相关的安全策略状态                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 14 | 组策略    | 显示为管理员设置各种软件、计算机系统设置相关的策略                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 15 | 运行保护   | 显示系统当前防护措施                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 16 | 升级方式   | 支持离线升级方式                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 17 | 支持运行平台 | 包括但不限于以下主流操作系统：<br><div> <div>Windows XP Professional</div> <div>32/64bit</div> </div> <div> <div>Windows7 Professional</div> <div>32/64bit</div> </div> <div> <div>Windows7 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows7 Ultimate</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2003 Standard</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2003 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2008 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2008 Standard</div> <div>32/64bit</div> </div> <div> <div>Windows 8</div> <div>32/64bit</div> </div> |

### 5.2.2.2 病毒检查工具

病毒检查工具是用于检查Windows操作系统是否存在病毒的工具。该工具需要通过专用USB转换线连接到被检查Windows主机的USB接口上，然后自动对Windows主机中相关目录和文件进行病毒检查。该工具的功能及适用范围如表2所示。

表2 病毒检查工具功能

| 序号 | 功能模块   | 功能要求                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 快速扫描   | 指快速扫描系统关键目录，发现关键目录中(例如：system32)是否存在病毒                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 2  | 全盘扫描   | 指对系统所有文件进行全面深度检查，发现系统中是否存在的病毒                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 3  | 自定义扫描  | 对选择的目录进行全面的检查，发现指定检查的目录中是否含有病毒程序，支持快速选择桌面、文档、系统关键目录、U口等目录和分区                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 4  | 升级方式   | 支持离线升级方式                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 5  | 支持运行平台 | 包括但不限于以下主流操作系统：<br><div> <div>Windows XP Professional</div> <div>32/64bit</div> </div> <div> <div>Windows7 Professional</div> <div>32/64bit</div> </div> <div> <div>Windows7 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows7 Ultimate</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2003 Standard</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2003 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2008 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2008 Standard</div> <div>32/64bit</div> </div> <div> <div>Windows 8</div> <div>32/64bit</div> </div> |

### 5.2.2.3 木马检查工具

木马检查工具是用于检查Windows操作系统是否存在木马的工具。该工具需要通过专用USB转换线连接到被检查Windows主机的USB接口上，然后自动对Windows主机中相关目录和文件进行木马检查。该工具的功能及适用范围如表3所示。

表3 木马检查工具功能

| 序号 | 功能模块   | 功能要求                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 快速扫描   | 快速扫描系统关键目录，扫描和发现关键目录中是否存在的木马程序                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 2  | 全盘扫描   | 对系统所有文件进行全面深度检查，发现系统中是否存在木马程序                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 3  | 自定义扫描  | 对指定的目录进行全面检查，发现是否含有木马等程序。支持快速选择桌面、文档、系统关键目录、U口等目录或分区                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 4  | 升级方式   | 支持离线升级方式                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 5  | 支持运行平台 | 包括但不限于以下主流操作系统：<br><div> <div>Windows XP Professional</div> <div>32/64bit</div> </div> <div> <div>Windows7 Professional</div> <div>32/64bit</div> </div> <div> <div>Windows7 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows7 Ultimate</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2003 Standard</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2003 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2008 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2008 Standard</div> <div>32/64bit</div> </div> <div> <div>Windows 8</div> <div>32/64bit</div> </div> |

### 5.2.2.4 网站恶意代码检查工具

网站恶意代码检查工具是用于检查WEB服务器目录路径中ASP、ASPX、JSP、PHP、CSS等文件是否感染或存在恶意代码的工具。该工具需要通过专用USB转换线连接到被检查WEB服务器的USB接口上，然后自动对WEB服务器中相关目录进行恶意代码检查。该工具的功能及适用范围如表4所示。

表4 网站恶意代码检查工具功能

| 序号 | 功能模块      | 功能要求                                                                                                                                                                                                                                                                                                                                                                             |
|----|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 快速扫描      | 对指定检查的 WEB 服务器目录路径，按照扫描策略自动进行恶意代码检查。快速扫描是根据文件类型匹配对应的扫描策略                                                                                                                                                                                                                                                                                                                         |
| 2  | 全盘扫描      | 对指定检查的 WEB 服务器目录路径，进行全面检查，扫描所有默认 ASP、ASPX、JSP、PHP、CSS 等类型的文件                                                                                                                                                                                                                                                                                                                     |
| 3  | 自定义扫描     | 对指定检查的 WEB 服务器目录路径，自定义扫描文件类型和扫描策略等                                                                                                                                                                                                                                                                                                                                               |
| 4  | WEB 服务器支持 | IIS、Apache、nginx、weblogic、Websphere、Tomcat 等                                                                                                                                                                                                                                                                                                                                     |
| 5  | 升级方式      | 支持离线升级方式                                                                                                                                                                                                                                                                                                                                                                         |
| 6  | 支持运行平台    | 包括但不限于以下主流操作系统：<br><div> <div>Windows Server 2003 Standard</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2003 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2008 Enterprise</div> <div>32/64bit</div> </div> <div> <div>Windows Server 2008 Standard</div> <div>32/64bit</div> </div> <div> <div>Windows 8</div> <div>32/64bit</div> </div> |

## 5.2.3 网口检查工具库

### 5.2.3.1 Linux 主机配置检查工具

Linux主机配置检查工具是用于对安装Linux操作系统的主机进行配置信息自动化采集的工具。该工具通过局域网连接到被检查的Linux主机，然后自动对Linux操作系统的配置信息进行采集。该工具的功能及适用范围如表5所示。

表5 Linux主机配置检查工具功能

| 序号 | 功能模块     | 功能要求                                        |
|----|----------|---------------------------------------------|
| 1  | 系统信息     | 可以检测到被检测主机的计算机名、操作系统类型、版本、内存、网卡、IP 地址等信息    |
| 2  | 账户信息     | 显示当前系统内所有的账户，包括了 root 级账户，普通账户，以及检查弱口令账户等情况 |
| 3  | 账户口令策略   | 检查系统配置是否配置了口令复杂度、定期更换、登录失败、锁定时间、超时时间等状态     |
| 4  | 活动端口、服务  | 显示当前开放的 TCP/UDP 端口、连接状态、进程对应路径、以及端口对应服务     |
| 5  | 用户权限     | 显示用户、访问权限与操作系统安全相关的状态                       |
| 6  | 安全审计     | 检查系统是否开启了审计策略、同时是否配备了 SYSLOG 服务器            |
| 7  | SNMP 服务  | 检查是否开启了 SNMP 服务，并检查 SNMP 是否采用加密的协议          |
| 8  | SSH 协议   | 检查当前 SSH 版本                                 |
| 9  | 升级方式     | 支持离线升级方式                                    |
| 10 | 支持检查目标对象 | 包括主流的 Linux 操作系统                            |

### 5.2.3.2 网络及安全设备配置检查工具

网络及安全设备配置检查工具是用于对网络设备和安全设备的配置信息进行自动化采集的工具。该工具通过局域网连接到被检查对象（例如，路由器、交换机和防火墙等），然后自动采集被检查对象的配置信息。该工具的功能及适用范围如表6所示。

表6 网络及安全设备配置检查工具功能

| 序号 | 功能模块     | 功能要求                                                         |
|----|----------|--------------------------------------------------------------|
| 1  | 系统信息     | 检查设备厂商名称、版本、型号                                               |
| 2  | 不必要的服务端口 | 检查系统是否开启了不必要且存在安全隐患的相关服务和端口                                  |
| 3  | 账户和口令策略  | 指检查 CONSOLE、TELNET 等方式登录是否需要输入口令、以及账户和口令的安全策略情况              |
| 4  | 远程访问管理   | 检查是否设置了相关策略仅允许授权的 IP 地址采用 TELNET、SSH 等协议远程登录管理               |
| 5  | SNMP 协议  | 检查 SNMP 是否开启，SNMP 是否存在弱口令，并检查 SNMP 团体名称是否采取了相关加密措施           |
| 6  | 日志审计策略   | 检查是否开启了系统自带的日志审计功能，以及检查是否指定了 SYSLOG 服务器                      |
| 7  | 防火墙检查项   | 账户安全、安全审计、入侵防护、访问控制、网络日志、安全日志、网络报警、安全防护报警、安全策略、自身安全防护策略、攻击防护 |
| 8  | IOS 版本   | 读取当前 IOS 版本信息                                                |
| 9  | 支持目标设备   | 主流的路由器、交换机通用系列；主流的防火墙通用系列                                    |
| 10 | 升级方式     | 支持离线升级方式                                                     |
| 11 | 口令安全     | 在检查时，如果需要在工具中输入被检查对象（例如，路由器、防火墙等）的用户名和口令，输入的用户名和口令不允许落地      |

5.2.3.3 弱口令检查工具

弱口令检查工具是用于检查SMB、MSSQL、FTP、MYSQL、Oracle 、RDP、POP3、SSH、HTTP、Telnet、VNC和SyBase等应用服务是否存在弱口令的工具。该工具需要通过局域网连接到被检查对象，然后可以根据用户选择自动对本地、远程主机及相关协议进行弱口令检查。该工具的技术规格要求如表7所示。

表7 弱口令检查工具功能

| 序号 | 功能模块   | 功能要求                                                                               |
|----|--------|------------------------------------------------------------------------------------|
| 1  | 支持协议类型 | 应用服务支持类型：SMB、MSSQL、FTP、MYSQL、Oracle、RDP、POP3、SSH、HTTP、Telnet、VNC 和 SyBase 等协议弱口令检查 |
| 2  | 内置字典   | 内置常见弱口令字典，并支持自定义账户、口令字典                                                            |
| 3  | 支持加密   | 支持通过 SSL 方式进行检查                                                                    |
| 4  | 端口自定义  | 支持自定义应用协议 TCP 端口                                                                   |
| 5  | 批量支持   | 支持本地、远程主机及多协议同时检查                                                                  |
| 6  | 升级方式   | 支持离线升级方式                                                                           |

5.2.3.4 数据库安全检查工具

数据库安全检查工具是用于检查数据库是否存在安全弱点的工具。该工具需要通过局域网连接到被检查数据库，然后自动对数据库进行安全弱点检查。该工具的技术规格要求如表8所示。

表8 数据库安全检查工具功能

| 序号 | 功能要求                                                               |
|----|--------------------------------------------------------------------|
| 1  | 支持对数据库“弱点、不安全配置、弱口令、补丁”深层次安全检测及准确评估                                |
| 2  | 支持远程方式扫描数据库的配置信息、安全策略、参数、账号口令安全、远程服务、端口和漏洞情况                       |
| 3  | 支持业界主流的数据库类型（包括国产数据库）                                              |
| 4  | 扫描引擎应确保系统工作时对数据库及服务器性能无明显影响                                        |
| 5  | 支持授权扫描,使用具有 DBA 权限的数据库用户，执行选定的安全策略实现对目标数据库的检测                      |
| 6  | 支持非授权扫描,用户在没有授权的情况下（即：不需要数据库的用户名和密码），依据数据库版本号并根据选定的安全策略对目标数据库进行的检测 |
| 7  | 策略自定义,提供扫描策略可自定义模式，操作者可以灵活选择默认策略的同时也可以自定义添加策略                      |
| 8  | 支持离线升级方式                                                           |
| 9  | 支持导出 word、pdf 等常见格式                                                |
| 10 | 在检查时，如果需要在工具中输入被检查对象的用户名和口令，输入的用户名和口令不允许落地                         |

5.2.3.5 网站安全检查工具

网站安全检查工具是用于检查Web应用系统是否存在漏洞的工具。该工具需要通过互联网或局域网连接到被检查Web应用系统（网站），然后自动对Web应用系统（网站）进行漏洞检查。该工具的技术规格要求如表9所示。

表9 网站安全检查工具功能

| 序号 | 功能要求                           |
|----|--------------------------------|
| 1  | 支持 WEB2.0，支持各类 JavaScript 脚本解析 |
| 2  | 支持 WAP 站点扫描和 FLASH 解析          |
| 3  | 支持手动配置高级扫描参数和选项                |
| 4  | 支持基于 HTTPS 应用系统的扫描             |

表9 （续）

| 序号 | 功能要求                                                                                                                                                                      |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5  | 支持 ERP 等复杂的 Web 应用系统检查                                                                                                                                                    |
| 6  | 支持验证码录制功能                                                                                                                                                                 |
| 7  | 支持 JSP、CGI、ASP、.NET 等类型动态页面                                                                                                                                               |
| 8  | 支持当前 URL、当前子域名、当前域名、任何 URL 扫描                                                                                                                                             |
| 9  | 支持 IP 地址、域名地址扫描                                                                                                                                                           |
| 10 | 支持主动扫描、被动扫描 两种模式的深度扫描                                                                                                                                                     |
| 11 | 支持实时存储扫描项目文件、断点续扫                                                                                                                                                         |
| 12 | 支持 HTTP 1.0 和 1.1 标准的 Web 应用系统                                                                                                                                            |
| 13 | 支持基于证书认证的系统扫描（如：网银）                                                                                                                                                       |
| 14 | 支持主流的数据库类型                                                                                                                                                                |
| 15 | 支持主流的 WEB 应用程序漏洞扫描                                                                                                                                                        |
| 16 | 支持对 SQL 注入、XSS 跨站脚本、伪造跨站点请求、网页木马、隐藏字段、表单绕过、AJAX 注入、弱配置、敏感信息泄漏、HI-JACK 攻击、弱口令、Xpath 注入、LDAP 注入、框架注入、操作系统命令注入、Flash 源代码泄漏、Flash 跨域攻击、Cookies 注入、敏感文件、第三方软件、其他各类 CGI 等漏洞进行扫描 |
| 17 | 支持离线升级方式                                                                                                                                                                  |
| 18 | 支持导出 word、pdf 等常见格式                                                                                                                                                       |

### 5.2.3.6 系统漏洞检查工具

系统漏洞检查工具是用于检查操作系统、常用软件和应用系统是否存在安全漏洞的工具。该工具需要通过局域网连接到被检查对象，然后自动对被检查对象进行漏洞扫描。该工具的技术规格要求如表10所示。

表10 漏洞检查工具功能

| 序号 | 功能要求                                                                                                                     |
|----|--------------------------------------------------------------------------------------------------------------------------|
| 1  | 支持进行漏洞扫描的操作系统类型包括但不限于：Microsoft Windows XP/2003/Vista/2008/7、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD                  |
| 2  | 可对 Web、FTP、电子邮件等应用系统以及 Office、Apache 等常用软件进行漏洞扫描                                                                         |
| 3  | 可对网络设备、Windows 主机、类 Unix 主机等目标对象进行漏洞扫描                                                                                   |
| 4  | 扫描和检测方式：远程访问方式                                                                                                           |
| 5  | 支持多种扫描策略，包括不同强度的扫描策略，方便用户快速选择                                                                                            |
| 6  | 可自动统计总体漏洞数量、统计不同操作系统类型的主机数量、统计所有开放端口、可用帐户、列出每一个漏洞所存在的主机、详细描述与修补建议。漏洞详细描述包括：漏洞名称、详述、修补方案、CVE/Bugtraq/CNVE/CNNVD编号、CVSS评分等 |
| 7  | 支持离线升级方式                                                                                                                 |
| 8  | 支持导出word、pdf等常见格式                                                                                                        |

## 5.3 选配检查工具功能



### 5.3.1 选配工具通用要求

选配检查工具应操作简捷，应采用国产商用密码算法对检查结果数据进行加密，以确保检查数据的保密性。

选配检查工具功能要求由各地公安机关根据检查工作的需要而自行制定，相关选配工具的技术规格要求可以参考以下技术规格要求。

### 5.3.2 协同工作处理机

协同工作处理机用于检查人员进行多人协作执行检查任务，提升检查工作效率。协同工作处理机的功能要求包括：

- a) 可导入等级保护检查专用工具导出的检查任务；
- b) 可进行安全检查任务的多人协同工作；
- c) 可将检查数据汇总到等级保护检查专用工具中。

### 5.3.3 网络设备信息侦测工具

网络设备信息侦测工具用来探测目标信息系统网络环境内的活动主机、网络设备和安全设备信息，包括端口探测、操作系统类型探测、服务和版本信息探测，并能够根据探测到的信息，生成目标主机、网络设备、安全设备的网络拓扑图。该工具需要通过局域网连接到被检查对象，然后对目标网络进行侦测。该工具的技术规格要求如表11所示。

表11 网络设备信息侦测工具功能

| 序号 | 网络设备信息侦测工具                                                                               |
|----|------------------------------------------------------------------------------------------|
| 1  | 设备发现功能：探测指定 IP 范围内活动的主机、网络设备和安全设备；支持快速扫描（ICMP 方式）和深度扫描（采用 SNMP、telnet、SSH、CDP 等方式采集设备信息） |
| 2  | 支持 IPV6 类型网络环境侦测                                                                         |
| 3  | 端口探测功能：探测指定 IP 范围内的活动主机上的若干个端口状态，并支持自定义端口和自定义探测方式功能                                      |
| 4  | 操作系统探测功能：支持获取被探测目标的操作系统类型，系统版本和设备类型（如主机、路由器、交换机、防火墙等），并给出设备的品牌                           |
| 5  | 服务类型和版本探测功能：支持探测端口的服务的类型和版本功能                                                            |
| 6  | 网络拓扑生成功能：支持根据探测到的信息，生成针对指定目标主机、网络设备和安全设备的网络拓扑图功能                                         |

### 5.3.4 无线 WIFI 检查工具

无线WIFI检查工具用来探测目标信息系统网络环境内部署的无线WIFI访问节点、以及通过无线WIFI上网的终端的信息，包括定位无线WIFI访问节点、终端的物理位置，分析无线WIFI访问节点、终端的地址、通讯流量等设备信息。该工具独立运行，不接入目标网络。该工具的技术规格要求如表12所示。

表12 无线WIFI检查工具功能

| 序号 | 无线 WIFI 检查工具                                                  |
|----|---------------------------------------------------------------|
| 1  | 发现目标信息系统网络中活动的无线WIFI/WAPI访问节点、通过无线WIFI/WAPI上网的终端              |
| 2  | 显示侦测到的无线WIFI/WAPI访问节点的详细信息，包括SSID、MAC地址、频道、加密方式、信号强度          |
| 3  | 统计侦测到的无线WIFI/WAPI访问节点的出现频率，包括首次出现时间、最近出现时间                    |
| 4  | 可以分析每个无线WIFI/WAPI访问节点下面连接的终端个数和详细信息，包括MAC地址、设备厂商、信道、出现时间等相关信息 |
| 5  | 能通过无线WIFI/WAPI访问节点和终端的无线信号强度变化定位其物理位置                         |
| 6  | 可发现隐藏的无线WIFI/WAPI访问节点                                         |
| 7  | 可对发现的无线WIFI/WAPI访问节点进行弱口令检测                                   |

5.3.5 网站监测预警工具

网站监测预警工具用来检查目标网站的业务连续性，并监测目标网站的内容（文字、链接、图片）是否被篡改。该工具需要通过互联网或局域网连接到目标网站，然后自动对目标网站进行监测。该工具的技术规格要求如表13所示。

表13 网站监测预警工具功能

| 序号 | 网站监测预警工具                                                  |
|----|-----------------------------------------------------------|
| 1  | 内容监测：监测网站时间、名称和文字、链接、源码、图片是否被篡改的持续监测                      |
| 2  | 暗链检测：检测出暗链所在网页的位置，以及暗链的详细定位                               |
| 3  | 敏感词监测：根据自定义的非法信息，系统将自动监测出包含非法信息的所有信息                      |
| 4  | 敏感词搜索：根据键入的非法信息，搜索出包含非法信息的所有信息                            |
| 5  | 漏洞监测：能够持续监测网站是否存在漏洞                                       |
| 6  | 挂马监测：能持续监测网站上是否出现挂马，以及通过脚本变更，实时监测是否有变种挂马出现                |
| 7  | 网站拓扑：以拓扑形式展现出网络链接结构，方便观察连接和断开情况                           |
| 8  | 首页实时监测：监测出每一站点的链接，连接时间，连接状态，对网站的健康状态进行实时监测                |
| 9  | 域名解析监测：监测出每站点域名解析响应时间，网页响应时间，连接时间，下载时间，总时间                |
| 10 | 站点可用性：根据站点访问情况，统计出查找次数，可用次数，不能用次数，可用率，不可用率                |
| 11 | 错误页面：每个站点的错误页面和错误数                                        |
| 12 | 内外部链接错误：根据监测连接状况，统计出内部错误数，内部连接数，内部错误比率，外部错误数，外部连接数，外部错误比率 |

5.4 辅助检查设备功能

5.4.1 便携式打印机

便携式打印机应支持如下功能（包括但不限于）：

- a) A4纸打印；
- b) USB接口；
- c) 彩色/黑白打印。

5.4.2 数码相机

数码相机应支持如下功能（包括但不限于）：

- a) 全自动拍照模式和摄像模式；
- b) 光学防抖；
- c) 夜间拍摄；
- d) 连拍；
- e) SD存储；
- f) 通过USB接口导出数据。

5.4.3 录音笔

录音笔应支持如下功能（包括但不限于）：

- a) 长时间录音和标准录音模式；
- b) 内置闪存；
- c) 内置麦克风；
- d) 自动录音；
- e) 通过USB接口导出数据；
- f) 分段录音。

5.4.4 扫描仪

扫描仪应支持如下功能（包括但不限于）：

- a) 对照片、文本页面、图纸等对象进行扫描；
- b) 文件格式包括但不限于以下格式：JPG、BMP；
- c) 通过USB接口导出数据。

5.4.5 执法记录仪

执法记录仪应支持如下功能（包括但不限于）：

- a) 高清摄像；
- b) 高分辨率拍照；
- c) 录音；
- d) 回放，可对摄录的视频、音频、图片资料进行现场回放；
- e) 红外，确保在弱光环境下有效拍摄。

6 界面要求

6.1 工具管理系统界面要求

6.1.1 界面总体要求

6.1.1.1 界面通用要求

工具管理系统应满足如下要求：

- a) 界面风格一致，操作简洁；
- b) 所有界面颜色的主基调为蓝色；
- c) 网络安全等级保护检查专用工具开机后，自动显示工具管理系统的登录界面。

6.1.1.2 登录界面

登录界面布局如图4所示。

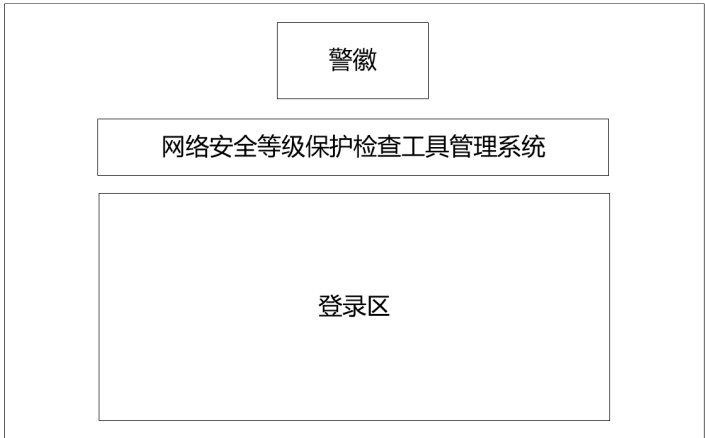


图4 工具管理系统登录界面布局示意图

在图4中，登录界面布局分为上部、中部、下部三个区域，其中：

- a) 上部：用于展示警徽的区域；
- b) 中部：用于展示工具管理系统名称的区域；
- c) 下部：用于用户输入用户名、密码的区域，包含确定和取消按钮等。

6.1.1.3 主界面

登录后主界面布局如图5所示。



图5 工具管理系统主界面布局示意图

在图5中，主界面布局分为：

- a) 标题区：用于展示警徽和工具管理系统名称、版本的区域，并用于显示当前日期时间、当前登录用户和用户角色等；
- b) 按钮区：用于展示检查计划管理、检查计划执行、检查结果分析、检查知识库管理、通知通报管理、检查工具管理、系统管理和退出按钮，要求如下：
  - 1) 检查计划管理：包含检查计划管理的业务，用于展示计划列表、创建检查计划、修改检查计划、删除检查计划、导入检查计划、导出检查计划等；
  - 2) 检查计划执行：包含检查计划执行的业务，用于检查表填报、工具检查、检查附件管理、日常工作等；
  - 3) 检查结果分析：包含检查结果分析的业务，用于等保合规性分析、输出报告、工具检查结果分析等；
  - 4) 检查知识库管理：包含检查知识库管理的业务，用于检查表管理、检查指标库管理等；
  - 5) 通知通报管理：用于编辑通知、通报等模板内容；
  - 6) 检查工具管理：用于对检查工具的升级管理等；
  - 7) 系统管理按钮：用于对工具管理系统进行管理；
  - 8) 退出按钮：点击退出按钮回到登录界面。

6.1.1.4 业务界面

主界面中按钮区中除了系统管理和退出按钮外，点击其他按钮均进入业务界面，业务界面布局如图6所示。

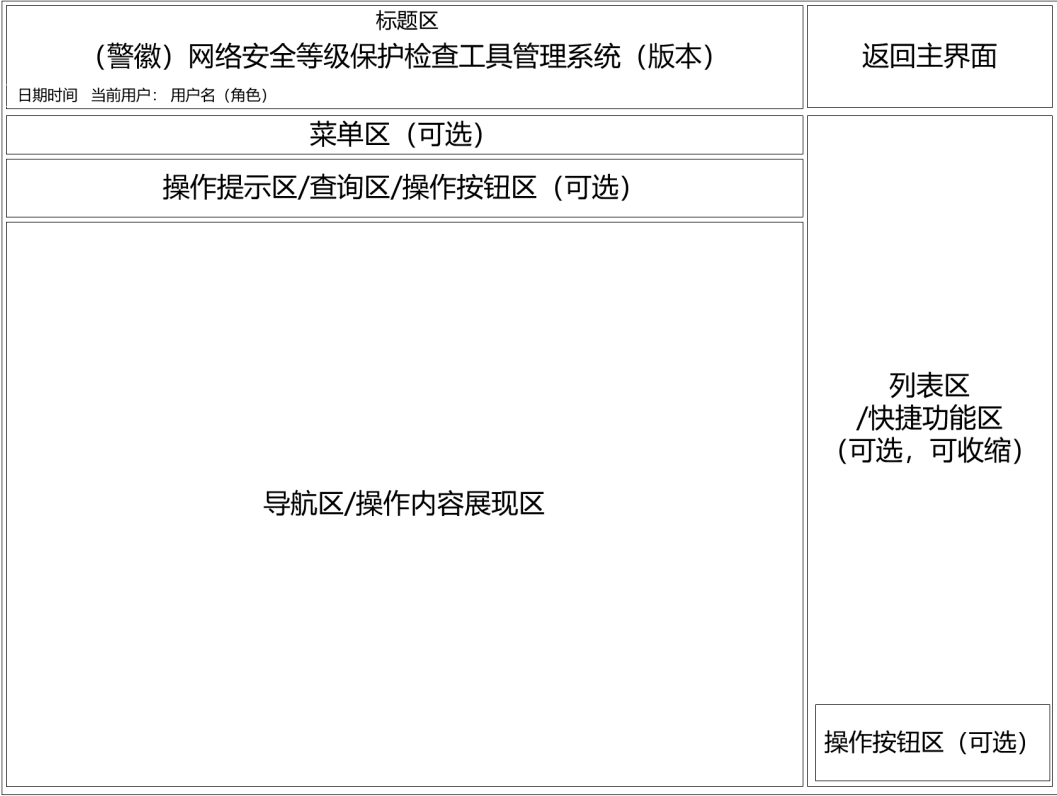


图6 工具管理系统业务操作主界面布局示意图

在图6中，工具管理系统业务主界面布局分为：

- a) 标题区：参见主界面标题区；
- b) 菜单区：为可选区域，用于放置一个或多个按钮形式菜单（例如，计划导入、计划新建等）的区域；
- c) 操作提示区/查询区/操作按钮区：为可选区域，用于放置操作内容展现区操作时的提示内容，或者是用于放置操作内容展现区的操作按钮，或者是用于放置查询所需的输入框和按钮等的区域；
- d) 操作按钮区：为可选区域，用于放置操作时所需按钮（例如，保存、导入、删除等）的区域；
- e) 列表区/快捷功能区：为可选区域，应可以收缩，用于放置快捷功能，或用于放置列表（例如，检查计划列表、检查表单列表等）的区域；
- f) 导航区/操作内容展现区：在首页时，该区域应为导航区，用于查看和选择检查计划，并可以查看当前检查计划的检查工作流程进展情况，可以通过点击检查工作流程的步骤进入到相应的工作界面中；在其他页面时，该区域为操作内容展现区，用于显示操作内容（例如，展现计划列表，进行检查表填报等）。

6.1.1.5 系统管理界面

点击主界面中的系统管理按钮，进入系统管理界面，系统管理界面布局如图7所示。



图7 工具管理系统-系统管理界面布局示意图

系统管理界面应包含如下按钮:

- a) 配置管理: 功能要求参见5.1.5.1内容;
- b) 用户管理: 功能要求参见5.1.5.2内容;
- c) 日志管理: 功能要求参见5.1.5.3内容;
- d) 系统升级: 功能要求参见5.1.5.4内容;
- e) 密码修改: 用于用户修改个人密码;
- f) 使用帮助: 用于查看帮助文档;
- g) 根据需要添加的其他功能按钮。

6.1.2 提示要求

工具管理系统在以下关键步骤时应给出提示:

- a) 在进行现场工作之前, 提示检查人员在现场检查时全程开启执法记录仪;
- b) 在进行现场工作之前, 提示检查人员在现场检查时全程进行屏幕录像;
- c) 在进行现场工作之前, 提示检查人员是否要对工具管理系统进行初始化操作;
- d) 在使用帮助界面, 明确说明检查工具的使用环境以及使用风险;
- e) 在打印检查结果汇总情况时, 若检查结果汇总情况中无安全风险, 提示检查人员不允许打印检查结果汇总情况;
- f) 在打印检查结果汇总情况时, 提示检查人员让被检查单位书面确认, 检查工作未对检查对象造成不良影响, 检查对象工作正常;
- g) 在打印检查结果汇总情况时, 提示检查人员让被检查单位书面确认, 检查结果记录内容真实完整。

6.2 检查工具界面要求

6.2.1 界面布局要求

检查工具界面应简洁, 应尽量采用“一键式”操作方式, 减少不必要的输入。输入内容仅能是:

- a) 必需的IP地址或URL地址;
- b) 被检查设备的账户和口令。

### 6.2.2 提示要求

检查工具在以下关键步骤时应给出以下提示:

- a) 在检查工具执行前,提示检查人员确认执法记录仪处于开启状态;
- b) 在检查工具执行前,明确说明检查工具不能用在工控系统中进行检查;
- c) 在检查工具执行前,明确说明该检查工具的使用环境以及使用风险;
- d) 在检查工具执行前,提示检查人员让被检查单位书面同意使用工具检查;
- e) 在检查工具执行前,提示检查人员确认检查对象工作正常;
- f) 在检查工具执行前,提示检查人员确认U盘工具的数据存储区经过工具管理系统的检测,无任何数据;
- g) 在检查工具执行前,提示该工具的接入方式(例如,网络及安全设备配置检查工具提示该工具的接入方式为接入目标对象所在局域网的核心交换机上,网站安全检查工具提示该工具的接入方式为接入目标所在的广域网/局域网中)。

## 7 性能要求

### 7.1 工具管理系统性能

#### 7.1.1 启动时间

启动时间指从用户启动工具管理系统到用户成功登录系统为止所使用的时间。

工具管理系统的启动时间应小于60s。

#### 7.1.2 操作响应时间

操作响应时间指从用户触发操作开始到系统完成相应操作并完整显示结果为止所使用的时间。

工具管理系统的操作响应时间应小于5s。

#### 7.1.3 工具检查结果自动分析时间

工具检查结果自动分析时间指从导入工具检查结果开始到工具检查结果自动分析完毕为止所使用的时间。

单个工具检查结果自动分析时间应小于60s。

### 7.2 安全通用要求检查工具性能

#### 7.2.1 U口检查工具

##### 7.2.1.1 Windows 主机配置检查工具

Windows主机配置检查工具使用过程中应最小化占用检查目标系统的资源,防止影响检查目标系统业务的正常运行,该工具应满足以下性能要求:

- a) 检测时间小于100s;
- b) CPU占用小于30%;
- c) 内存占用小于25%。

##### 7.2.1.2 病毒检查工具

病毒检查工具使用过程中应最小化占用检查目标系统的资源,防止影响检查目标系统业务的正常运行,该工具应满足以下性能要求:

- a) CPU平均占用量小于50%;
- b) 内存占用小于40%。

##### 7.2.1.3 木马检查工具

木马工具使用过程中应最小化占用检查目标系统的资源，防止影响检查目标系统业务的正常运行，该工具应满足以下性能要求：

- a) CPU平均占用量小于50%；
- b) 内存占用小于40%。

#### 7.2.1.4 网站恶意代码检查工具

网站恶意代码检查工具使用过程中应最小化占用检查目标系统的资源，防止影响检查目标系统业务的正常运行，该工具应满足以下性能要求：

- a) CPU平均占用量小于50%；
- b) 内存占用小于30%。

### 7.2.2 网口检查工具

#### 7.2.2.1 Linux 主机配置检查工具

Linux主机配置检查工具使用过程中应最小化占用检查目标系统的系统资源，防止影响检查目标系统业务的正常运行，该工具应满足以下性能要求：

- a) 检测时间小于100s；
- b) CPU占用小于30%；
- c) 内存占用小于25%；
- d) 平均带宽占用量小于128KB/s。

#### 7.2.2.2 网络及安全设备配置检查工具

网络及安全设备配置检查工具使用过程中应最小化占用检查目标系统所属网络的网络资源，防止影响检查目标系统业务和网络的正常运行，该工具应满足以下性能要求：

- a) 单台设备检测速度小于50s；
- b) 带宽占用小于30KB/s。

#### 7.2.2.3 弱口令检查工具

弱口令检查工具使用过程中应最小化占用检查目标系统的资源或所属网络的网络资源，防止影响检查目标系统业务和网络的正常运行，该工具应满足以下性能要求：

- a) CPU平均占用量小于30%；
- b) 内存占用小于30%；
- c) 平均带宽占用量小于128KB/s。

#### 7.2.2.4 数据库安全检查工具

数据库安全检查工具使用过程中应最小化占用检查目标系统资源和其所属网络的网络资源，防止影响检查目标系统业务和网络的正常运行，该工具应满足以下性能要求：平均带宽占用量小于3MB/s。

#### 7.2.2.5 网站安全检查工具

网站安全检查工具使用过程中应最小化占用检查目标系统所属网络的网络资源，防止影响检查目标系统业务和网络的正常运行，该工具应满足以下性能要求：平均带宽占用量小于3MB/s。

#### 7.2.2.6 系统漏洞检查工具

系统漏洞检查工具使用过程中应最小化占用检查目标系统资源和其所属网络的网络资源，防止影响检查目标系统业务和网络的正常运行，该工具应满足以下性能要求：

- a) 检查目标系统CPU平均占用量小于30%；
- b) 检查目标系统内存占用小于10%；
- c) 平均带宽占用量小于512KB/s。

注：目标对象的CPU平均占用量按照CPU i5进行测算；目标对象的内存占用量按照内存4G进行测算。

### 7.3 选配检查工具性能

#### 7.3.1 协同工作处理机



### 7.3.1.1 主机配置

主机配置应满足如下要求：

- a) CPU类型为不低于第四代智能英特尔酷睿i7处理器；
- b) CPU型号为不低于i7-4500u；
- c) CPU主频为不低于1.8GHz；
- d) 内存容量不低于8GB；
- e) 内存类型不低于DDR3；
- f) 硬盘容量不低于240GB；
- g) 硬盘类别不低于SSD固态硬盘。

### 7.3.1.2 显卡

显卡应满足如下要求：

- a) 独立显卡；
- b) 显示芯片不低于AMD Radeon HD 8670M；
- c) 显存容量不低于独立2GB。

### 7.3.1.3 显示器

显示器应满足如下要求：

- a) 屏幕规格为不低于14英寸；
- b) 显示比例为16:9；
- c) 屏幕物理分辨率不低于1366像素×768像素；
- d) 屏幕类型为14英寸HD LED背光显示屏；
- e) 屏幕类型为多点触控屏。

### 7.3.1.4 通信

通信应满足如下要求：

- a) 内置蓝牙；
- b) 局域网通信支持10/100/1000Mbps；
- c) 支持无线局域网。

### 7.3.1.5 端口

端口应满足如下要求：

- a) 音频端口：耳机、麦克风二合一接口；
- b) 显示端口：HDMI接口；
- c) RJ45端口：RJ45；
- d) USB3.0：不少于2个USB3.0端口。

### 7.3.1.6 音效系统

音效系统应满足如下要求：

- a) 内置扬声器；
- b) 支持杜比音效；
- c) 内置麦克风。

### 7.3.1.7 输入设备

应配备如下输入设备：

- a) 全尺寸背光键盘；
- b) 五键合一多点触控板。

### 7.3.1.8 其他设备

应配备如下设备：

- a) 有摄像头；

- b) 支持指纹识别;
- c) 有四合一读卡器。

#### 7.3.1.9 电源

电源应满足如下要求:

- a) 电池续航时间不低于4h, 具体视使用环境而定;
- b) 100V~240V自适应交流电源适配器。

#### 7.3.1.10 硬件规格

协同工作处理机硬件规格应满足如下要求:

- a) 尺寸不大于333mm×225mm×21mm;
- b) 净重不大于2Kg。

#### 7.3.1.11 操作系统

操作系统为安全可靠操作系统。

### 7.3.2 网络设备侦测检查工具

网络设备侦测检查工具使用过程中应最小化占用检查目标系统的资源或所属网络的资源, 防止影响检查目标系统业务和网络的正常运行, 平均带宽占用量小于3MB/s。

### 7.3.3 无线 WIFI 检查工具

无线WIFI检查工具使用过程中不能占用检查目标系统的资源或所属网络的资源, 防止影响检查目标系统业务和网络的正常运行, 该工具应满足以下性能要求:

- a) 不接入目标网络, 不占用目标网络带宽;
- b) 扫描频段覆盖2.4G、5.8G两个频段;
- c) 定位扫描频率在每秒50次以上;
- d) 无障碍物的情况下, 可侦测并定位半径不小于300m内活动的无线WIFI设备;
- e) 定位误差小于3m;
- f) 设备采用专用手持设备形式, 方便携带。

### 7.3.4 网站监测预警工具

网站监测预警工具使用过程中应最小化占用检查目标系统的资源或所属网络的资源, 防止影响检查目标系统业务和网络的正常运行, 该工具应满足以下性能要求:

- a) 平均带宽占用量小于3MB/s;
- b) 可以按照正常外网用户访问速度(例如, 间隔4min访问一次)监测目标网站。

## 8 安全要求

### 8.1 工具管理系统安全

#### 8.1.1 数据安全

工具管理系统数据安全应满足以下要求:

- a) 采用国家商密办批准的国产商用密码产品对以下数据进行加解密:
  - 1) 检查数据(包括本地存放的文件类型的检查数据);
  - 2) 检查工具管理系统数据库中的检查数据的关键字段(例如, 设备IP地址、被检查单位名称等);
  - 3) 检查工具之间传递的任务数据;
  - 4) 检查工具导出到重要信息系统基础数据库管理系统的数据等。
- b) 密码产品与检查工具分开存放:
  - 1) 国产商用密码产品便于携带, 且与检查工具分开存放;
  - 2) 仅在使用工具管理系统时方可与检查工具进行连接。

### 8.1.2 痕迹清除

工具管理系统应具有清除业务数据的功能，当使用该痕迹清除功能后，检查工具上被清除的业务数据应无法恢复。

### 8.1.3 身份鉴别

工具管理系统身份鉴别应满足以下安全要求：

- a) 工具管理系统为每个用户角色规定与之相关的安全属性，包括用户角色标识、鉴别信息、隶属组、权限等；
- b) 工具管理系统提供使用默认值对创建的每个用户角色的属性进行初始化的能力；
- c) 只有授权用户才能登录工具管理系统，使用工具管理系统的相应功能；
- d) 系统提供两种以上认证方式对用户进行身份认证；
- e) 工具管理系统对身份鉴别数据进行加密存储；
- f) 工具管理系统提供登录尝试失败锁定功能。

### 8.1.4 访问控制

工具管理系统对用户访问控制应满足以下要求：

- a) 依据安全策略严格控制针对用户文件、数据库表等重要信息资源的操作；
- b) 不泄漏已注销用户的任何信息，如身份鉴别信息等。

### 8.1.5 安全审计

工具管理系统安全审计应满足以下要求：

- a) 工具管理系统应记录下列事件并生成审计记录：
  - 1) 指标库、知识库、检查工具等升级操作；
  - 2) 现场结果记录、反馈意见等文书材料打印事件；
  - 3) 用户登录和注销等事件；
  - 4) 数据导入、导出等事件。
- b) 确保只有授权用户才能读取和备份审计数据。

### 8.1.6 通信安全

工具管理系统通信安全应满足以下要求：

- a) 工具管理系统应采取措施确保导入和导出数据的完整性；
- b) 应保证数据交互时的保密性，应采用国产商用密码算法对以下数据进行加密：
  - 1) U口检查工具向检查工具提交的检查结果数据；
  - 2) 网口检查工具向检查工具提交的检查结果数据等。

### 8.1.7 软件容错

工具管理系统应提供数据有效性检验功能，保证输入的数据格式或长度符合系统设定要求。应包含以下数据的软件容错：

- a) 人机接口输入的数据；
- b) 检查工具输入的检查结果数据；
- c) 与重要信息系统基础数据库管理系统交互的数据。

### 8.1.8 资源控制

工具管理系统应对访问用户在一段时间内未作任何响应时，能够自动结束会话。

### 8.1.9 操作系统加固

工具管理系统运行依赖的操作系统环境应进行如下具体加固处理：

- a) 安装恶意代码防护软件；
- b) 为尽量减少系统安全漏洞被利用造成的安全隐患，保持系统功能最小化，至少禁用以下服务：
  - 1) World Wide Web Publishing；
  - 2) Wireless Zero Configuration；

- 3) Wired AutoConfig;
- 4) Windows Time;
- 5) Windows Audio;
- 6) Terminal Services;
- 7) Telephony;
- 8) TCP/IP NetBIOS Helper;
- 9) Simple Mail Transfer Protocol;
- 10) Shell Hardware Detection;
- 11) Remote Access Connection Manager;
- 12) Network Location Awareness (NLA);
- 13) Network Connections;
- 14) DNS Client;
- 15) DHCP Client;
- 16) Computer Browser;
- 17) Alerter;
- 18) Clipbook;
- 19) Computer Browser;
- 20) Fax Service;
- 21) FTP Publishing Service;
- 22) IIS Admin Service;
- 23) Internet Connection Sharing;
- 24) Messenger;
- 25) NetMeeting Remote Desktop Sharing;
- 26) Remote Registry Service;
- 27) Routing and Remote Access;
- 28) Simple Mail Transfer Protocol (SMTP);
- 29) Simple Network Management Protocol (SNMP) Service;
- 30) Simple Network Management Protocol (SNMP) Trap;
- 31) Telnet。

#### 8.1.10 恢复出厂设置

工具管理系统运行依赖的操作系统环境应提供恢复出厂设置的功能。

### 8.2 U口检查工具安全

#### 8.2.1 自身安全

U口检查工具自身安全应满足以下要求：

- a) 连续工作4h以上不会发生故障；
- b) 分为检查工具自身软件所在的存储区和检查结果存放的数据区；
- c) U口检查工具自身软件所在的存储区具有防止恶意代码感染能力，仅有授权软件可对该数据区进行数据的写入，在运行机器上显示为只读模式；
- d) U口检查工具数据区中的数据仅能读取。

#### 8.2.2 运行安全

U口检查工具在运行过程中应满足以下要求：

- a) 不改变检查对象当前配置；
- b) 不影响检查对象正常运行；

- c) 不影响检查对象所属网络正常运行；
- d) 不在检查对象中遗留数据。

### 8.2.3 数据安全

U口检查工具在数据安全方面应满足以下要求：

- a) U口检查工具对所有检查数据采用国产加密算法进行加密，防止检查数据被非法读取；
- b) U口检查工具对所有检查数据采取痕迹清除措施，以防信息泄露。

## 8.3 网口检查工具安全

### 8.3.1 自身安全

网口检查工具的运行环境应具有防止恶意代码感染能力。

### 8.3.2 运行安全

网口检查工具在运行过程中应满足以下要求：

- a) 不改变检查对象当前配置；
- b) 不影响检查对象正常运行；
- c) 不影响检查对象所属网络正常运行；
- d) 不在检查对象中遗留数据。

### 8.3.3 数据安全

网口检查工具在数据安全方面应满足以下要求：

- a) 网口检查工具对所有检查数据采用国产加密算法进行加密，防止检查数据被非法读取；
- b) 网口检查工具对所有检查数据采取痕迹清除措施，以防信息泄露。

## 8.4 无线 WIFI 检查工具安全

### 8.4.1 自身安全

检查工具独立运行，不接入目标网络系统。

### 8.4.2 运行安全

检查工具在运行过程中应满足以下要求：

- a) 不改变检查对象当前配置；
- b) 不影响检查对象正常运行；
- c) 不影响检查对象所属网络正常运行；
- d) 不在检查对象中遗留数据。

### 8.4.3 数据安全

无线WIFI检查工具在数据安全方面应满足以下要求：

- a) 无线WIFI检查工具对所有检查数据采用国产加密算法进行加密，防止检查数据被非法读取；
- b) 无线WIFI检查工具对所有检查数据采取痕迹清除措施，以防信息泄露。

## 9 兼容性要求

为保证检查数据的兼容性和可扩展性，工具管理系统与重要信息系统基础数据库管理系统之间数据的交互应满足指定的接口规范，具体要求如下：

- a) 工具管理系统与重要信息系统基础数据库管理系统之间按照指定的接口规范（详见附录G）进行数据交互；
- b) 工具管理系统与重要信息系统基础数据库管理系统交互数据采用国家商密办批准的国产商用密码产品进行数据加解密；

- c) 使用光盘介质作为工具管理系统和重要信息系统基础数据库管理系统之间的数据交换介质。数据以加密文件形式保存到光盘介质中，通过光盘介质完成数据导入导出操作。

## 附录 A

(规范性附录)

## 党政机关和行业主管部门检查指标

党政机关和行业主管部门检查指标如表A. 1所示。

表A. 1 党政机关和行业主管部门检查指标

| 检查范围        | 检查内容        | 检查项                  | 检查要点                                           |
|-------------|-------------|----------------------|------------------------------------------------|
| 网络安全工作的基本情况 | 网络安全工作的组织部署 | 检查行业网络安全协调领导机构运行情况   | 行业的等级保护联络员是否参加公安网安部门组织召开的联络员会议                 |
|             |             |                      | 联络员是否以书面形式向主管领导汇报公安网安部门在联络员会议上通报的内容            |
|             |             | 检查行业网络安全责任部门运行情况     | 行业网络安全责任部门是否对本行业的网络安全工作下发文件或召开会议等方式进行业务指导      |
|             |             |                      | 行业网络安全责任部门是否对本行业的网络安全工作听取汇报或现场检查等方式进行监督检查      |
|             |             | 检查行业网络安全工作的组织部署情况    | 是否明确行业各单位的信息系统的责任部门                            |
|             |             |                      | 是否明确信息系统责任部门的责任人                               |
|             |             | 检查行业网络安全工作文件执行情况     | 行业网络安全责任部门是否对本行业的网络安全工作文件或方案明确行业网络安全工作所需要执行的内容 |
|             |             |                      | 是否有网络安全工作文件或方案的执行情况的总结或汇报                      |
|             |             | 检查行业网络安全工作会议、业务培训情况  | 是否有组织人员培训的工作会议记录或文件                            |
|             |             |                      | 参训人员的业务水平是否提高                                  |
|             |             | 检查行业主要领导对网络安全工作的重视情况 | 行业是否将网络安全工作的执行情况纳入到年度考核指标                      |
|             |             |                      | 开展网络安全工作的经费是否纳入年度预算                            |
|             |             | 检查行业标准规范发布情况         | 是否发布或修订行业网络安全标准规范                              |
|             |             |                      | 是否对行业定级备案、测评、建设整改各环节网络安全相关标准的执行情况进行检查或审核       |
|             | 网络安全责任制落实情况 | 检查网络安全领导机构执行情况       | 是否有网络安全工作的领导责任制                                |
|             |             |                      | 对于网络安全领导是否有网络安全工作的考核指标                         |

表A.1 (续)

| 检查范围        | 检查内容        | 检查项               | 检查要点                                               |
|-------------|-------------|-------------------|----------------------------------------------------|
| 网络安全工作的基本情况 | 网络安全责任制落实情况 | 检查网络安全职能部门执行情况    | 是否对本部门/单位的网络安全工作发布文件或召开会议等方式进行业务指导                 |
|             |             |                   | 是否对本部门/单位的网络安全工作听取汇报或现场检查等方式进行监督                   |
|             |             | 检查网络安全责任追究制度执行情况  | 是否对所有的网络安全事故/事件有详细记录                               |
|             |             |                   | 是否按照网络安全责任追究制度进行处理                                 |
|             | 网络安全制度建设情况  | 检查人员安全管理制度执行情况    | 本单位人员录用、离岗、考核、安全保密、教育培训是否按照安全管理制度执行，并有详细记录         |
|             |             |                   | 外来人员管理是否按照安全管理制度执行，并有详细记录                          |
|             |             | 检查机房安全管理制度执行情况    | 本单位机房进出人员管理是否按照制度执行，并有详细记录                         |
|             |             |                   | 本单位机房日常监控是否按照制度执行，并有监控记录                           |
|             |             | 检查系统建设管理制度执行情况    | 本单位的产品采购、服务外包是否按照相关管理制度执行，并有相关记录                   |
|             |             |                   | 本单位的工程实施、验收交付等系统建设是否按照相关管理制度执行，并有相关记录              |
|             | 信息系统运维情况    | 检查开展日常网络安全监测和预警情况 | 本单位日常网络安全监测是否按照机制执行，并有网络安全监测记录                     |
|             |             |                   | 本单位日常网络安全预警是否按照机制执行，并有网络安全预警和处理记录                  |
|             |             | 检查安全事件的处置情况       | 本单位安全事件报告是否按照程序执行，并有相关报告记录                         |
|             |             |                   | 本单位安全事件响应处理是否按照程序执行，并有相关处置记录                       |
|             |             | 检查应急预案的制定、演练和完善情况 | 是否有应急预案，并有相应的预案文档                                  |
|             |             |                   | 否有应急保障队伍，并有人员名单和联系方式                               |
|             |             |                   | 是否定期应急演练，并有应急演练的文档记录                               |
|             |             |                   | 是否根据演练结果对应急预案进行完善，并有应急预案的修订记录                      |
| 信息系统定级备案情况  | 定级工作情况      | 检查信息系统定级指导执行情况    | 是否有定级指导的专家名单和联系方式                                  |
|             |             |                   | 是否有同级公安机关等级保护工作办公室的联系人和联系方式                        |
|             |             | 检查信息系统定级工作执行情况    | 是否梳理本行业/单位的信息系统数量和范围<br>信息系统的总数是                   |
|             |             |                   | 是否梳理本行业/单位的重要信息系统数量和范围<br>三级信息系统的数量是<br>四级信息系统的数量是 |
|             | 备案工作情况      | 检查信息系统备案工作执行情况    | 是否将本行业/单位的二级信息系统到同级公安机关进行备案<br>备案的二级信息系统数量是        |



表A.1 （续）

| 检查范围                              | 检查内容     | 检查项                 | 检查要点                                                        |
|-----------------------------------|----------|---------------------|-------------------------------------------------------------|
| 信息系统定级备案情况                        | 备案工作情况   | 检查信息系统备案工作执行情况      | 是否将本行业/单位的重要信息系统到同级公安机关进行备案<br>备案的三级信息系统数量是<br>备案的四级信息系统数量是 |
| 等级测评和安全建设整改工作部署和经费保障情况            | 测评工作情况   | 检查等级测评工作执行情况        | 是否制定年度等级测评计划                                                |
|                                   |          |                     | 计划本年度测评的信息系统数是                                              |
|                                   |          |                     | 正在进行测评的信息系统数是                                               |
|                                   | 建设整改工作情况 | 检查安全建设整改工作计划执行情况    | 完成等级测评的信息系统是                                                |
|                                   |          |                     | 是否制定年度安全建设整改计划                                              |
|                                   |          |                     | 计划本年度安全建设整改的信息系统数是                                          |
|                                   |          |                     | 正在进行安全建设整改的信息系统数是                                           |
|                                   | 经费保障情况   | 检查等级测评工作经费保障情况      | 完成安全建设整改的信息系统数是                                             |
|                                   |          |                     | 是否有年度等级测评经费预算，或专项经费预算                                       |
|                                   |          | 检查安全建设整改工作经费保障情况    | 是否按预算计划拨款                                                   |
|                                   |          |                     | 是否有年度安全建设整改经费预算，或专项经费预算                                     |
|                                   |          |                     | 是否按预算计划拨款                                                   |
|                                   | 机构选择     | 检查等级测评机构的选择情况       | 是否从《全国网络安全等级保护测评机构推荐目录》中选择测评机构开展等级测评                        |
| 网络安全自查和整改情况                       | 自查情况     | 检查行业网络安全检查工作的组织开展情况 | 行业网络安全责任部门是否对本行业的网络安全工作下发文件，并明确检查内容                         |
|                                   |          | 检查网络安全自查工作组织部署情况    | 是否有行业网络安全检查工作总结或报告                                          |
|                                   |          |                     | 是否有单位网络安全自查工作总结报告                                           |
|                                   | 整改情况     | 检查存在问题的整改工作完成情况     | 是否根据公安机关通报的整改意见进行整改，并及时反馈                                   |
| 信息系统使用国外信息技术产品和服务情况 <sup>注1</sup> | 软硬件情况    | 调查服务器和终端（含笔记本）使用情况  | 总台数                                                         |
|                                   |          |                     | 国外产品台数                                                      |
|                                   |          |                     | 国外产品使用率                                                     |
|                                   |          |                     | 使用国外 CPU 台数                                                 |
|                                   |          |                     | 使用 Windows 操作系统的台数                                          |
|                                   |          |                     | 使用 Linux 操作系统的台数                                            |
|                                   |          |                     | 使用其他国外类型操作系统的台数                                             |
|                                   |          | 调查核心路由器使用情况         | 总台数                                                         |
|                                   |          |                     | 国外产品台数                                                      |
|                                   |          |                     | 国外产品使用率                                                     |
|                                   |          | 调查交换机使用情况           | 总台数                                                         |
|                                   |          |                     | 国外产品台数                                                      |
|                                   |          |                     | 国外产品使用率                                                     |

表A.1 （续）

| 检查范围                                       | 检查内容   | 检查项             | 检查要点                                           |
|--------------------------------------------|--------|-----------------|------------------------------------------------|
| 信息系统使用国外信息技术产品和服务情况 <sup>注1</sup>          | 软硬件情况  | 调查防火墙使用情况       | 总台数                                            |
|                                            |        |                 | 国外产品台数                                         |
|                                            |        |                 | 国外产品使用率                                        |
|                                            |        | 调查字处理软件使用情况     | 安装字处理软件的终端计算机台数                                |
|                                            |        |                 | 安装国外字处理软件的终端计算机台数                              |
|                                            |        |                 | 国外字处理软件使用率(%)                                  |
|                                            |        | 调查防病毒产品使用情况     | 安装国外防病毒产品的终端计算机台数                              |
|                                            | 安全服务情况 | 调查运维服务情况        | 日常运维管理服务是否由社会第三方提供（若由社会第三方提供，则需填写受托单位名称）       |
|                                            |        |                 | 是否与受托单位签订了保密协议                                 |
|                                            |        |                 | 受托的单位是否没有外资参与                                  |
|                                            |        | 调查数据存储、信息处理服务情况 | 数据存储、信息处理服务是否由社会第三方提供（若是社会第三方提供，则需填写提供服务单位的名称） |
|                                            |        |                 | 是否与提供服务的单位签订了安全保密协议                            |
|                                            |        |                 | 提供服务的单位是否没有外资参与                                |
| 注：检查范围为“信息系统使用国外信息技术产品和服务情况”的所有检查结果数据为调查数据 |        |                 |                                                |

## 附录 B

(规范性附录)

## 备案单位检查指标

备案单位检查指标如表B.1所示。

表B.1 备案单位检查指标

| 检查范围       | 检查内容        | 检查项                | 检查要点                                       |
|------------|-------------|--------------------|--------------------------------------------|
| 网络安全工作基本情况 | 网络安全工作的组织部署 | 检查网络安全协调领导机构运行情况   | 等级保护联络员是否参加公安网安部门组织召开的联络员会议                |
|            |             |                    | 联络员是否以书面形式向主管领导汇报公安网安部门在联络员会议上通报的内容        |
|            |             | 检查网络安全责任部门运行情况     | 网络安全责任部门是否对本单位的网络安全工作下发文件或召开会议等方式进行业务指导    |
|            |             |                    | 网络安全责任部门是否对本单位的网络安全工作听取汇报或现场检查等方式进行监督检查    |
|            |             | 检查网络安全工作文件执行情况     | 网络安全责任部门是否对本单位的网络安全工作文件或方案明确网络安全工作所需要执行的内容 |
|            |             |                    | 是否有网络安全工作文件或方案的执行情况的总结或汇报                  |
|            |             | 检查网络安全工作会议、业务培训情况  | 是否有组织人员培训的工作会议记录或文件                        |
|            |             |                    | 参训人员的业务水平是否提高                              |
|            |             | 检查主要领导对网络安全工作的重视情况 | 是否将网络安全工作的执行情况纳入到年度考核指标                    |
|            |             |                    | 开展网络安全工作的经费是否纳入年度预算                        |
|            | 网络安全责任制落实情况 | 检查网络安全领导机构执行情况     | 是否有网络安全工作的领导责任制                            |
|            |             |                    | 对于网络安全领导是否有网络安全工作的考核指标                     |
|            |             | 检查网络安全职能部门的执行情况    | 是否对本单位的网络安全工作发布文件或召开会议等方式进行业务指导            |
|            |             |                    | 是否对本单位的网络安全工作听取汇报或现场检查等方式进行监督              |
|            |             | 检查网络安全责任追究制度执行情况   | 是否对所有的网络安全事故/事件有详细记录                       |
|            |             |                    | 是否按照网络安全责任追究制度进行处理                         |

表 B.1 (续)

| 检查范围               | 检查内容           | 检查项                       | 检查要点                                                     |
|--------------------|----------------|---------------------------|----------------------------------------------------------|
| 网络安全<br>工作基本<br>情况 | 网络安全制度建设<br>情况 | 检查人员安全管理<br>制度执行情况        | 本单位人员录用、离岗、考核、安全保密、教育培训是否按照安全管理制度执行，并有详细记录               |
|                    |                |                           | 外来人员管理是否按照安全管理制度执行，并有详细记录                                |
|                    |                | 检查机房安全管理<br>制度执行情况        | 本单位机房进出人员管理是否按照制度执行，并有详细记录                               |
|                    |                |                           | 本单位机房日常监控是否按照制度执行，并有监控记录                                 |
|                    |                | 检查系统建设管<br>理制度执行情况        | 本单位的产品采购、服务外包是否按照相关管理制度执行，并有相关记录                         |
|                    |                |                           | 本单位的工程实施、验收交付等系统建设是否按照相关管理制度执行，并有相关记录                    |
|                    | 信息系统运维情况       | 检查开展日常网<br>络安全监测和预<br>警情况 | 本单位日常网络安全监测是否按照机制执行，并有网络安全监测记录                           |
|                    |                |                           | 本单位日常网络安全预警是否按照机制执行，并有网络安全预警和处理记录                        |
|                    |                | 检查安全事件的<br>处置情况           | 本单位安全事件报告是否按照程序执行，并有相关报告记录                               |
|                    |                |                           | 本单位安全事件响应处理是否按照程序执行，并有相关处置记录                             |
|                    |                | 检查应急预案的<br>制定、演练和完善<br>情况 | 是否有应急预案，并有相应的预案文档                                        |
|                    |                |                           | 是否有应急保障队伍，并有人员名单和联系方式                                    |
|                    |                |                           | 是否定期应急演练，并有应急演练的文档记录                                     |
|                    |                |                           | 是否根据演练结果对应急预案进行完善，并有应急预案的修订记录                            |
| 信息系统<br>定级备案<br>情况 | 定级工作情况         | 检查信息系统定<br>级指导执行情况        | 是否有定级指导的专家名单和联系方式                                        |
|                    |                |                           | 是否有同级公安机关等级保护工作办公室的联系人和联系方式                              |
|                    |                | 检查信息系统定<br>级工作执行情况        | 是否梳理本单位的信息系统数量和范围<br>信息系统的总数是                            |
|                    |                |                           | 是否梳理本单位的重要信息系统数量和范围<br>三级信息系统的数量是<br>四级信息系统的数量是          |
|                    | 备案工作情况         | 检查信息系统备<br>案工作执行情况        | 是否将本单位的二级信息系统到同级公安机关进行备案<br>备案的二级信息系统数量是                 |
|                    |                |                           | 是否将本单位的重要信息系统到同级公安机关进行备案<br>备案的三级信息系统数量是<br>备案的四级信息系统数量是 |

表 B.1 (续)

| 检查范围                              | 检查内容     | 检查项                | 检查要点                       |
|-----------------------------------|----------|--------------------|----------------------------|
| 等级测评和安全建设整改工作部署和经费保障情况            | 测评工作情况   | 检查等级测评工作执行情况       | 是否制定年度等级测评计划               |
|                                   |          |                    | 计划本年度测评的信息系统数是             |
|                                   |          |                    | 正在进行测评的信息系统数是              |
|                                   |          |                    | 完成等级测评的信息系统数是              |
|                                   | 建设整改工作情况 | 检查安全建设整改工作计划执行情况   | 是否制定年度安全建设整改计划             |
|                                   |          |                    | 计划本年度安全建设整改的信息系统数是         |
|                                   |          |                    | 正在进行安全建设整改的信息系统数是          |
|                                   |          |                    | 完成安全建设整改的信息系统数是            |
|                                   | 经费保障情况   | 检查等级测评工作经费保障情况     | 是否有年度等级测评经费预算, 或专项经费预算     |
|                                   |          | 检查安全建设整改工作经费保障情况   | 是否按预算计划拨款                  |
|                                   |          |                    | 是否有年度安全建设整改经费预算, 或专项经费预算   |
| 网络安全自查和整改情况                       | 自查情况     | 检查网络安全自查工作组织部署情况   | 是否有单位网络安全自查工作总结报告          |
|                                   | 整改情况     | 检查存在问题的整改工作情况      | 是否根据公安机关通报的整改意见进行整改, 并及时反馈 |
| 信息系统使用国外信息技术产品和服务情况 <sup>注2</sup> | 软硬件情况    | 调查服务器和终端(含笔记本)使用情况 | 总台数                        |
|                                   |          |                    | 国外产品台数                     |
|                                   |          |                    | 国外产品使用率                    |
|                                   |          |                    | 使用国外 CPU 台数                |
|                                   |          |                    | 使用 Windows 操作系统的台数         |
|                                   |          |                    | 使用 Linux 操作系统的台数           |
|                                   |          |                    | 使用其他国外类型操作系统的台数            |
|                                   |          | 调查核心路由器使用情况        | 总台数                        |
|                                   |          |                    | 国外产品台数                     |
|                                   |          |                    | 国外产品使用率                    |
|                                   |          | 调查交换机使用情况          | 总台数                        |
|                                   |          |                    | 国外产品台数                     |
|                                   |          |                    | 国外产品使用率                    |
|                                   |          | 调查防火墙使用情况          | 总台数                        |
|                                   |          |                    | 国外产品台数                     |
|                                   |          |                    | 国外产品使用率                    |
|                                   |          | 调查字处理软件使用情况        | 安装字处理软件的终端计算机台数            |
|                                   |          |                    | 安装国外字处理软件的终端计算机台数          |

表 B.1 （续）

| 检查范围                                        | 检查内容   | 检查项             | 检查要点                                           |
|---------------------------------------------|--------|-----------------|------------------------------------------------|
| 信息系统使用国外信息技术产品和服务情况 <sup>注2</sup>           | 软硬件情况  | 调查防病毒产品使用情况     | 安装国外防病毒产品的终端计算机台数                              |
|                                             | 安全服务情况 | 调查运维服务情况        | 日常运维管理服务是否由社会第三方提供(若由社会第三方提供, 则需填写受托单位名称)      |
|                                             |        |                 | 是否与受托单位签订了保密协议                                 |
|                                             |        |                 | 受托的单位是否没有外资参与                                  |
|                                             |        | 调查数据存储、信息处理服务情况 | 数据存储、信息处理服务否由社会第三方提供(若是社会第三方提供, 则需填写提供服务单位的名称) |
|                                             |        |                 | 是否与提供服务的单位签订了安全保密协议                            |
|                                             |        |                 | 提供服务的单位是否没有外资参与                                |
| 注: 检查范围为“信息系统使用国外信息技术产品和服务情况”的所有检查结果数据为调查数据 |        |                 |                                                |

## 附录 C

## (规范性附录)

## 安全通用要求检查指标

## C.1 第一级安全通用要求检查指标

安全保护等级为第一级的安全通用要求检查指标如表C.1所示。

表C.1 第一级安全通用要求检查指标

| 检查范围   | 检查内容                 | 检查项                                                  | 检查要点                                               |
|--------|----------------------|------------------------------------------------------|----------------------------------------------------|
| 安全物理环境 | 物理访问控制               | 机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员                  | 是否在机房出入口安排专人值守或配置了电子门禁系统                           |
|        |                      |                                                      | 是否对进入机房的人员信息进行了记录                                  |
|        | 防盗窃和防破坏              | 应将设备或主要部件进行固定，并设置明显的不易除去的标记                          | 是否将设备或主要部件进行固定，并设置明显的不易除去的标记                       |
|        | 防雷击                  | 应将各类机柜、设施和设备等通过接地系统安全接地                              | 是否将各类机柜、设施和设备等通过接地系统安全接地                           |
|        | 防火                   | 机房应设置灭火设备                                            | 是否在机房设置了灭火设备                                       |
|        | 防水和防潮                | 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透                              | 是否采取措施防止雨水通过机房窗户、屋顶和墙壁渗透                           |
|        | 温湿度控制                | 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内                  | 是否设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内               |
|        | 电力供应                 | 应在机房供电线路上配置稳压器和过电压防护设备                               | 是否在机房供电线路上配置了稳压器和过电压防护设备                           |
| 电磁防护   | 电源线和通信线缆应隔离铺设，避免互相干扰 | 是否将电源线和通信线缆隔离铺设                                      |                                                    |
| 安全通信网络 | 通信传输                 | 应采用校验技术保证通信过程中数据的完整性                                 | 是否采用校验技术保证通信过程中数据的完整性                              |
|        | 可信验证                 | 可基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，在检测到其可信性受到破坏后进行报警     | 是否基于可信根对通信设备的系统引导程序、系统程序等进行可信验证                    |
|        |                      |                                                      | 在检测到其可信性受到破坏后是否进行报警                                |
| 安全区域边界 | 边界防护                 | 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信                      | 是否保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信                   |
|        | 访问控制                 | a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信 | 是否在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信 |
|        |                      | b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化           | 是否删除了多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化          |
|        |                      | c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出           | 是否对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出           |

表 C.1 (续)

| 检查范围      | 检查内容   | 检查项                                                 | 检查要点                                         |                           |
|-----------|--------|-----------------------------------------------------|----------------------------------------------|---------------------------|
| 安全区域边界    | 可信验证   | 可基于可信根对边界设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警   | 是否基于可信根对边界设备的系统引导程序、系统程序等进行可信验证              |                           |
|           |        |                                                     | 在检测到其可信性受到破坏后是否进行报警                          |                           |
| 安全计算环境    | 身份鉴别   | a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换    | 是否对登录的用户进行身份标识和鉴别                            |                           |
|           |        |                                                     | 登录的用户身份标识是否具有唯一性                             |                           |
|           |        |                                                     | 登录用户身份鉴别信息是否具有复杂度要求并定期更换                     |                           |
|           |        | b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施 | 是否具有登录失败处理功能                                 |                           |
|           | 访问控制   | a) 应对登录的用户分配账户和权限                                   | 是否对登录的用户分配账户和权限                              |                           |
|           |        |                                                     | b) 应重命名或删除默认账户，修改默认账户的默认口令                   | 是否重命名或删除默认账户              |
|           |        |                                                     | 是否修改默认账户的默认口令                                |                           |
|           |        | c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在                      | 是否及时删除或停用多余的、过期的账户，避免共享账户的存在                 |                           |
|           | 入侵防范   | a) 应遵循最小安装的原则，仅安装需要的组件和应用程序                         | 是否遵循最小安装的原则，仅安装需要的组件和应用程序                    |                           |
|           |        | b) 应关闭不需要的系统服务、默认共享和高危端口                            | 是否关闭不需要的系统服务、默认共享和高危端口                       |                           |
|           | 恶意代码防范 | 应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库             | 是否安装防恶意代码软件或配置具有相应功能的软件                      |                           |
|           |        |                                                     | 是否定期进行升级和更新防恶意代码库                            |                           |
|           | 可信验证   | 可基于可信根对计算设备的系统引导程序、系统程序等进行可信验证，在检测到其可信性受到破坏后进行报警    | 是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和是应用程序等进行可信验证 |                           |
|           |        |                                                     | 是否在检测到应用程序可信根的可信性受到破坏后进行报警                   |                           |
|           | 数据完整性  | 应采用校验技术保证重要数据在传输过程中的完整性                             | 是否采用校验码技术保证重要数据在传输过程中的完整性                    |                           |
|           | 数据备份恢复 | 应提供重要数据的本地数据备份与恢复功能                                 | 是否提供重要数据的本地数据备份与恢复功能                         |                           |
|           | 安全管理制度 | 管理制度                                                | 应对安全管理活动中的各类管理内容建立安全管理制度                     | 是否对安全管理活动中的各类管理内容建立安全管理制度 |
|           | 安全管理机构 | 岗位设置                                                | a) 应设立系统管理员等岗位，并定义各个工作岗位的职责                  | 是否设立系统管理员岗位               |
| 是否明确各岗位职责 |        |                                                     |                                              |                           |
| 人员配备      |        | a) 应配备一定数量的系统管理员                                    | 是否配备系统管理员                                    |                           |
|           |        |                                                     | 是否明确系统管理员人员配备情况                              |                           |
| 授权和审批     |        | a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等                  | 是否明确各部门和岗位的职责和授权范围                           |                           |
|           |        | 是否明确针对审批事项、审批部门和批准人等内容与相关制度一致                       |                                              |                           |



表 C.1 (续)

| 检查范围       | 检查内容      | 检查项                                                            | 检查要点                                                                   |
|------------|-----------|----------------------------------------------------------------|------------------------------------------------------------------------|
| 安全管理<br>人员 | 人员录用      | 应指定或授权专门的部门或人员负责人员录用                                           | 是否由专门的部门或人员负责人员的录用工作                                                   |
|            | 人员离岗      | a) 应及时终止离岗人员的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备               | 是否及时终止离岗人员的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备                         |
|            | 安全意识教育和培训 | a) 应对各类人员进行安全意识教育和岗位技能培训, 并告知相关的安全责任和惩戒措施                      | 是否建立相关制度对各类人员进行安全意识教育和岗位技能培训                                           |
|            |           |                                                                | 是否告知相关的安全责任和惩戒措施                                                       |
|            | 外部人员访问管理  | a) 应保证在外部人员访问受控区域前得到授权或审批                                      | 是否建立相关制度明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等<br>外部人员访问受控区域前是否先提出书面申请 |
| 安全建设<br>管理 | 定级和备案     | 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由                                | 是否有书面材料说明保护对象的安全保护等级及确定等级的方法和理由                                        |
|            | 安全方案设计    | 应根据安全保护等级选择基本安全措施, 依据风险分析的结果补充和调整安全措施                          | 是否根据安全保护等级选择基本安全措施, 依据风险分析的结果补充和调整安全措施                                 |
|            | 产品采购和使用   | 应确保网络安全产品采购和使用符合国家的有关规定                                        | 网络安全产品采购是否符合国家的有关规定                                                    |
|            |           |                                                                | 网络安全产品使用是否符合国家的有关规定                                                    |
|            | 工程实施      | 应指定或授权专门的部门或人员负责工程实施过程的管理                                      | 是否指定或授权专门的部门或人员负责工程实施过程的管理                                             |
|            | 测试验收      | 应进行安全性测试验收                                                     | 是否进行安全性测试验收                                                            |
|            | 系统交付      | a) 应制定交付清单, 并根据交付清单对所交接的设备、软件和文档等进行清点                          | 是否根据交付清单对所交接的设备、软件和文档等进行清点                                             |
|            |           | b) 应对负责运行维护的技术人员进行相应的技能培训                                      | 是否对负责运行维护的技术人员进行相应的技能培训                                                |
| 安全运维<br>管理 | 环境管理      | a) 应确保服务供应商的选择符合国家的有关规定                                        | 服务供应商是否符合国家的有关规定                                                       |
|            |           |                                                                | 是否与选定的服务供应商签订相关协议, 明确明确约定相关责任                                          |
|            |           | b) 应与选定的服务供应商签订相关协议, 明确约定相关责任                                  | 是否指定专门的部门或人员负责机房安全                                                     |
|            |           |                                                                | 指定的部门或人员是否对机房出入进行管理                                                    |
|            | 介质管理      | a) 应指定专门的部门或人员负责机房安全, 对机房出入进行管理, 定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理 | 是否定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理                                        |
|            |           |                                                                | 是否建立机房安全管理规范, 对有关物理访问、物品进出和环境安全等方面的管理作出规定                              |
|            |           | b) 应对机房的安全管理做出规定, 包括物理访问, 物品进出和环境安全等方面                         | 是否将介质存放在安全的环境中, 各类介质进行控制和保护                                            |
|            |           |                                                                | 是否实行存储环境专人管理                                                           |
| 安全运维<br>管理 | 介质管理      | 应将介质存放在安全的环境中, 对各类介质进行控制和保护, 实行存储环境专人管理, 并根据存档介质的目录清单定期盘点      | 是否根据存档介质的目录清单定期盘点                                                      |
|            |           |                                                                |                                                                        |
|            |           |                                                                |                                                                        |

表 C.1 (续)

| 检查范围   | 检查内容      | 检查项                                                 | 检查要点                                              |
|--------|-----------|-----------------------------------------------------|---------------------------------------------------|
| 安全运维管理 | 设备维护管理    | 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理             | 是否指定专门的部门或人员定期进行维护管理各种设备（包括备份和冗余设备）、线路等           |
|        | 漏洞和风险管理   | 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补    | 是否采取必要的措施识别安全漏洞和隐患                                |
|        |           |                                                     | 对发现的安全漏洞和隐患是否及时进行修补或评估可能的影响后进行修补                  |
|        | 网络和系统安全管理 | a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限             | 是否划分了不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限            |
|        |           | b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制           | 是否指定专门的部门或人员进行账户管理                                |
|        |           |                                                     | 是否对申请账户、建立账户、删除账户等进行控制                            |
|        | 恶意代码防范管理  | a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等        | 是否有相关措施提高所有用户的防恶意代码意识                             |
|        |           |                                                     | 是否对外来计算机或存储设备接入系统前进行恶意代码检查等                       |
|        | 备份与恢复管理   | b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等 | 是否对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等 |
|        |           | a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等                      | 是否识别需要定期备份的重要业务信息、系统数据及软件系统等                      |
|        | 安全事件处置    | b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等                      | 是否规定备份信息的备份方式、备份频度、存储介质、保存期等                      |
|        |           | a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件                        | 是否及时向安全管理部门报告所发现的安全弱点和可疑事件                        |
|        |           | b) 应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责       | 是否制定了安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责      |

## C.2 第二级安全通用要求检查指标

安全保护等级为第二级的安全通用要求检查指标如表C.2所示。

表C.2 第二级安全通用要求检查指标

| 检查范围   | 检查内容    | 检查项                                  | 检查要点                                 |
|--------|---------|--------------------------------------|--------------------------------------|
| 安全物理环境 | 物理位置选择  | a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内         | 机房场地是否选择在具有防震能力的建筑内                  |
|        |         |                                      | 机房场地是否选择在具有防风能力的建筑内                  |
|        |         |                                      | 机房场地是否选择在具有防雨等能力的建筑内                 |
|        |         | b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施  | 机房场地是否未设在建筑物的顶层或地下室                  |
|        |         |                                      | 机房场地设在建筑物的顶层或地下室，是否加强防水和防潮措施         |
|        | 物理访问控制  | 机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员  | 是否在机房出入口安排专人值守或配置了电子门禁系统             |
|        |         |                                      | 是否对进入机房的人员信息进行了记录                    |
|        | 防盗窃和防破坏 | a) 应将设备或主要部件进行固定，并设置明显的不易除去的标记       | 是否将设备或主要部件进行固定，并设置明显的不易除去的标记         |
|        |         | b) 应将通信线缆铺设在隐蔽安全处                    | 是否将通信线缆铺设在隐蔽安全处                      |
|        | 防雷击     | 应将各类机柜、设施和设备等通过接地系统安全接地              | 是否将各类机柜、设施和设备等通过接地系统安全接地             |
|        | 防火      | a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火 | 机房是否设置火灾自动消防系统                       |
|        |         |                                      | 火灾自动消防系统是否能够自动检测火情、自动报警，并自动灭火        |
|        |         | b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料      | 机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料        |
|        | 防水和防潮   | a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透           | 是否采取措施防止雨水通过机房窗户、屋顶和墙壁渗透             |
|        |         | b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透        | 是否采取措施防止机房内水蒸气结露和地下积水的转移与渗透          |
|        | 防静电     | 应采用防静电地板或地面并采用必要的接地防静电措施             | 是否安装防静电地板或地面并采用必要的接地防静电措施            |
|        | 温湿度控制   | 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内  | 是否设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内 |
|        | 电力供应    | a) 应在机房供电线路上配置稳压器和过电压防护设备            | 是否在机房供电线路上配置了稳压器和过电压防护设备             |
|        |         | b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求  | 是否提供了短期的备用电力供应设备，以满足设备在断电情况下的正常运行要求  |
|        | 电磁防护    | 电源线和通信线缆应隔离铺设，避免互相干扰                 | 是否将电源线和通信线缆隔离铺设                      |

表 C.2 (续)

| 检查范围   | 检查内容        | 检查项                                                                                   | 检查要点                                                |
|--------|-------------|---------------------------------------------------------------------------------------|-----------------------------------------------------|
| 安全通信网络 | 网络架构        | a) 应划分不同的网络区域, 并按照方便管理和控制的原则为各网络区域分配地址                                                | 是否划分不同的网络区域                                         |
|        |             |                                                                                       | 是否按照方便管理和控制的原则为各网络区域分配地址                            |
|        |             | b) 应避免将重要网络区域部署在网络边界处, 重要网络区域和其他网络区域之间应采取可靠的技术隔离手段                                    | 是否避免将重要网络区域部署在网络边界处                                 |
|        |             |                                                                                       | 重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段                        |
|        | 通信传输        | a) 应采用校验技术保证通信过程中数据的完整性                                                               | 是否采用校验技术保证通信过程中数据的完整性                               |
|        | 可信验证        | 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证, 在检测到其可信性受到破坏后进行报警, 并将验证结果形成审计记录送至安全管理中心 | 是否基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证       |
|        |             |                                                                                       | 在检测到其可信性受到破坏后进行报警                                   |
|        |             |                                                                                       | 是否将验证结果形成审计记录送至安全管理中心                               |
| 安全区域边界 | 边界防护        | a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信                                                    | 是否保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信                    |
|        | 访问控制        | a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则, 默认情况下除允许通信外受控接口拒绝所有通信                                 | 是否在网络边界或区域之间根据访问控制策略设置访问控制规则, 默认情况下除允许通信外受控接口拒绝所有通信 |
|        |             | b) 应删除多余或无效的访问控制规则, 优化访问控制列表, 并保证访问控制规则数量最小化                                          | 是否删除了多余或无效的访问控制规则, 优化访问控制列表, 并保证访问控制规则数量最小化         |
|        |             | c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查, 以允许/拒绝数据包进出                                           | 是否对源地址、目的地址、源端口、目的端口和协议等进行检查, 以允许/拒绝数据包进出           |
|        |             | d) 应根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力                                                     | 是否能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力                    |
|        | 入侵防范        | a) 应在关键网络节点处监视网络攻击行为                                                                  | 是否在关键网络节点处监视网络攻击行为                                  |
|        | 恶意代码和垃圾邮件防范 | a) 应在关键网络节点处对恶意代码进行检测和清除, 并维护恶意代码防护机制的升级和更新                                           | 是否在关键网络节点处对恶意代码进行检测和清除                              |
|        |             |                                                                                       | 是否维护恶意代码防护机制的升级和更新                                  |
|        | 安全审计        | a) 应在网络边界、重要网络节点进行安全审计, 审计覆盖到每个用户, 对重要的用户行为和重要安全事件进行审计                                | 是否在网络边界进行安全审计                                       |
|        |             |                                                                                       | 是否在重要网络节点进行安全审计                                     |
|        |             |                                                                                       | 审计是否覆盖到每个用户, 是否对重要的用户行为和重要安全事件进行审计                  |
|        |             | b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息                                          | 审计记录是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息          |
|        |             | c) 应对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等                                                | 是否对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等                |

表 C.2 (续)

| 检查范围   | 检查内容 | 检查项                                                                                   | 检查要点                                            |
|--------|------|---------------------------------------------------------------------------------------|-------------------------------------------------|
| 安全区域边界 | 可信验证 | 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证,在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心 | 是否基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证 |
|        |      |                                                                                       | 在检测到其可信性受到破坏后是否进行报警                             |
|        |      |                                                                                       | 是否将验证结果形成审计记录送至安全管理中心                           |
| 安全计算环境 | 身份鉴别 | a) 应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定期更换                                      | 是否对登录的用户进行身份标识和鉴别                               |
|        |      |                                                                                       | 登录的用户身份标识是否具有唯一性                                |
|        |      |                                                                                       | 登录用户身份鉴别信息是否具有复杂度要求并定期更换                        |
|        |      | b) 应具有登录失败处理功能,应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施                                   | 是否具有登录失败处理功能                                    |
|        |      |                                                                                       | 是否配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施           |
|        |      | c) 当进行远程管理时,应采取必要措施防止鉴别信息在网络传输过程中被窃听                                                  | 当进行远程管理时,是否采取必要措施防止鉴别信息在网络传输过程中被窃听              |
|        | 访问控制 | a) 应对登录的用户分配账户和权限                                                                     | 是否对登录的用户分配账户和权限                                 |
|        |      | b) 应重命名或删除默认账户,修改默认账户的默认口令                                                            | 是否重命名或删除默认账户                                    |
|        |      |                                                                                       | 是否修改默认账户的默认口令                                   |
|        |      | c) 应及时删除或停用多余的、过期的账户,避免共享账户的存在                                                        | 是否及时删除或停用多余的、过期的账户,避免共享账户的存在                    |
|        | 安全审计 | d) 应授予管理用户所需的最小权限,实现管理用户的权限分离                                                         | 是否授予管理用户所需的最小权限,实现管理用户的权限分离                     |
|        |      | a) 应启用安全审计功能,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计                                            | 是否启用安全审计功能                                      |
|        |      |                                                                                       | 审计是否覆盖到每个用户,以及对重要的用户行为和重要的安全事件进行审计              |
|        |      | b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息                                          | 审计记录是否包括事件的日期和时间、事件类型、事件是否成功及其他与审计相关的信息         |
|        |      | c) 应对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等                                                  | 是否对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等              |
|        | 入侵防范 | a) 应遵循最小安装的原则,仅安装需要的组件和应用程序                                                           | 是否遵循最小安装的原则,仅安装需要的组件和应用程序                       |
|        |      | b) 应关闭不需要的系统服务、默认共享和高危端口                                                              | 是否关闭不需要的系统服务、默认共享和高危端口                          |
|        |      | c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制                                               | 是否通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制           |
|        |      | d) 应提供数据有效性检验功能,保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求                                        | 是否提供数据有效性检验功能,保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求    |
|        |      | e) 应能发现可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞                                                   | 是否具备已知漏洞发现的能力                                   |
|        |      |                                                                                       | 是否充分测试评估后,及时修补漏洞                                |

表 C.2 (续)

| 检查范围   | 检查内容   | 检查项                                                                                | 检查要点                                                                                  |
|--------|--------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 安全计算环境 | 恶意代码防范 | 应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库                                            | 是否安装防恶意代码软件或配置具有相应功能的软件                                                               |
|        |        |                                                                                    | 是否定期进行升级和更新防恶意代码库                                                                     |
|        | 可信验证   | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 | 是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和是应用程序等进行可信验证                                          |
|        |        |                                                                                    | 是否在检测到应用程序可信根的可信性受到破坏后进行报警                                                            |
|        |        |                                                                                    | 是否将验证结果形成审计记录，并将审计记录送至安全管理中心，进行动态关联感知                                                 |
|        | 数据完整性  | 应采用校验码技术保证重要数据在传输过程中的完整性                                                           | 是否采用校验码技术保证重要数据在传输过程中的完整性                                                             |
|        | 数据备份恢复 | a) 应提供重要数据的本地数据备份与恢复功能                                                             | 是否提供重要数据的本地数据备份与恢复功能                                                                  |
|        |        | b) 应提供异地备份功能，利用通信网络将重要数据定时批量备份至备份场地                                                | 是否提供异地备份功能，利用通信网络将重要数据定时批量备份至备份场地                                                     |
| 安全管理中心 | 剩余信息保护 | 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除                                                      | 是否保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除                                                        |
|        | 个人信息保护 | a) 应仅采集和保存业务必需的用户个人信息                                                              | 是否仅采集和保存业务必需的用户个人信息                                                                   |
|        |        | b) 应禁止未授权访问和非法使用用户个人信息                                                             | 是否禁止未授权访问和非法使用用户个人信息                                                                  |
|        | 系统管理   | a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计                               | 安全管理中心是否对系统管理员进行身份鉴别                                                                  |
|        |        |                                                                                    | 安全管理中心是否只允许系统管理员通过特定命令或操作界面进行系统管理操作                                                   |
|        |        |                                                                                    | 系统管理员在安全管理中心中的操作是否进行审计                                                                |
|        | 审计管理   | b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等        | 是否只有系统管理员可以通过安全管理中心对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等操作 |
|        |        |                                                                                    | 安全管理中心是否对审计管理员进行身份鉴别？                                                                 |
|        |        |                                                                                    | 安全管理中心是否只允许审计管理员通过特定命令或操作界面进行系统管理操作                                                   |
|        |        |                                                                                    | 审计管理员在安全管理中心中的操作是否进行审计                                                                |
|        |        | b) 应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等                       | 是否只有审计管理员可以通过安全管理中心对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等操作                |

表 C.2 (续)

| 检查范围       | 检查内容  | 检查项                                                          | 检查要点                                                       |
|------------|-------|--------------------------------------------------------------|------------------------------------------------------------|
| 安全管理<br>制度 | 安全策略  | 应制定网络安全工作的总体方针和安全策略, 阐明机构安全工作的总体目标、范围、原则和安全框架等               | 检查信息安全工作的总体方针和安全策略文件, 查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等      |
|            | 管理制度  | a) 应对安全管理活动中的各类管理内容建立安全管理制度                                  | 是否对安全管理活动中的各类管理内容建立安全管理制度                                  |
|            |       | b) 应对管理人员或操作人员执行的日常管理操作建立操作规程                                | 是否对管理人员或操作人员执行的日常管理操作建立操作规程                                |
|            | 制定和发布 | a) 应指定或授权专门的部门或人员负责安全管理制度的制定                                 | 是否有专门的部门或人员负责制定安全管理制度                                      |
|            |       | b) 安全管理制度应通过正式、有效的方式发布, 并进行版本控制                              | 安全管理制度制、修订人员, 是否按照统一的格式标准或要求制定                             |
|            | 评审和修订 | 应定期对安全管理制度的合理性和适用性进行论证和审定, 对存在不足或需要改进的安全管理制度进行修订             | 是否定期对安全管理制度的合理性和适用性进行论证和审定, 对存在不足或是否改进的安全管理制度进行修订          |
| 安全管理<br>机构 | 岗位设置  | a) 应设立网络安全管理工作的职能部门, 设立安全主管、安全管理各个方面的负责人岗位, 并定义各负责人的职责       | 是否划分网络安全管理职能部门<br>是否设立安全主管、安全管理各个方面的负责人岗位, 并定义各负责人的职责      |
|            |       | b) 应设立系统管理员、审计管理员和安全管理员等岗位, 并定义部门及各个工作岗位的职责                  | 是否划分网络安全管理岗位                                               |
|            |       |                                                              | 是否明确部门及各岗位职责                                               |
|            |       |                                                              |                                                            |
|            | 人员配备  | a) 应配备一定数量的系统管理员、审计管理员和安全管理员等                                | 是否配备系统管理员、审计管理员和安全管理员                                      |
|            |       |                                                              | 是否明确各岗位人员配备情况                                              |
|            | 授权和审批 | a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等                           | 是否明确各部门和岗位的职责和授权范围<br>是否明确针对审批事项、审批部门和批准人等内容与相关制度一致        |
|            |       | b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程                           | 系统变更、重要操作、物理访问和系统接入等事项是否进行审批                               |
|            | 沟通和合作 | a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通, 定期召开协调会议, 共同协作处理网络安全问题 | 是否加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通, 定期召开协调会议, 共同协作处理网络安全问题 |
|            |       | b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通                        | 是否建立与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通机制                      |
|            |       |                                                              | 是否与网络安全职能部门、各类供应商、业界专家及安全组织开展合作与沟通                         |
|            |       | c) 应建立外联单位联系列表, 包括外联单位名称、合作内容、联系人和联系方式等信息                    | 是否建立外联单位联系列表                                               |
|            | 审核和检查 | a) 应定期进行常规安全检查, 检查内容包括系统日常运行、系统漏洞和数据备份等情况                    | 是否定期进行常规安全检查, 检查内容包括系统日常运行、系统漏洞和数据备份等情况                    |

表 C.2 (续)

| 检查范围       | 检查内容      | 检查项                                                | 检查要点                                           |
|------------|-----------|----------------------------------------------------|------------------------------------------------|
| 安全管理<br>人员 | 人员录用      | a) 应指定或授权专门的部门或人员负责人员录用                            | 是否由专门的部门或人员负责人员的录用工作                           |
|            |           | b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查                    | 是否对被录用人员的身份、安全背景、专业资格或资质等进行审查                  |
|            | 人员离岗      | a) 应及时终止离岗人员的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备   | 是否及时终止离岗人员的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备 |
|            | 安全意识教育和培训 | a) 应对各类人员进行安全意识教育和岗位技能培训, 并告知相关的安全责任和惩戒措施          | 是否建立相关制度对各类人员进行安全意识教育和岗位技能培训                   |
|            |           |                                                    | 是否告知相关的安全责任和惩戒措施                               |
|            | 外部人员访问管理  | a) 应在外部人员物理访问受控区域前提出书面申请, 批准后由专人全程陪同, 并登记备案        | 是否建立相关制度明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等 |
|            |           |                                                    | 外部人员物理访问受控区域前是否先提出书面申请                         |
|            |           |                                                    | 是否由专人全程陪同, 并登记备案                               |
|            |           | b) 应在外部人员接入受控网络访问系统前提出书面申请, 批准后由专人开设账户、分配权限, 并登记备案 | 是否建立相关制度明确外部人员接入网络前的申请审批流程                     |
|            |           |                                                    | 外部人员接入受控网络访问系统前是否先提出书面申请                       |
|            |           |                                                    | 是否由专人开设账户、分配权限, 并登记备案                          |
|            |           | c) 外部人员离场后应及时清除其所有的访问权限                            | 外部人员离场后是否及时清除其所有的访问权限                          |
| 安全建设<br>管理 | 定级和备案     | a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由                 | 是否有书面材料说明保护对象的安全保护等级及确定等级的方法和理由                |
|            |           | b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定            | 是否组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定          |
|            |           | c) 应保证定级结果经过相关部门的批准                                | 定级结果是否经过相关部门的批准                                |
|            |           | d) 应将备案材料报主管部门和相应公安机关备案                            | 备案材料是否报主管部门和相应公安机关备案                           |
|            | 安全方案设计    | a) 应根据安全保护等级选择基本安全措施, 依据风险分析的结果补充和调整安全措施           | 是否根据安全保护等级选择基本安全措施, 依据风险分析的结果补充和调整安全措施         |
|            |           | b) 应根据保护对象的安全保护等级进行安全方案设计                          | 是否根据保护对象的安全保护等级进行安全方案设计                        |
|            |           | c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定, 经过批准后才能正式实施 | 是否组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定            |
|            |           |                                                    | 安全方案是否经过批准                                     |
|            | 产品采购和使用   | a) 应确保网络安全产品采购和使用符合国家的有关规定                         | 网络安全产品采购是否符合国家的有关规定                            |
|            |           |                                                    | 网络安全产品使用是否符合国家的有关规定                            |



表 C.2 (续)

| 检查范围   | 检查内容    | 检查项                                          | 检查要点                                       |
|--------|---------|----------------------------------------------|--------------------------------------------|
| 安全建设管理 | 产品采购和使用 | b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求           | 密码产品与服务的采购是否符合国家密码管理主管部门的要求                |
|        |         |                                              | 密码产品与服务的使用是否符合国家密码管理主管部门的要求                |
|        | 自行软件开发  | a) 应将开发环境与实际运行环境物理分开, 测试数据和测试结果受到控制          | 是否将开发环境与实际运行环境物理分开, 测试数据和测试结果受到控制          |
|        |         | b) 应在软件开发过程中对安全性进行测试, 在软件安装前对可能存在的恶意代码进行检测   | 是否在软件开发过程中对安全性进行测试                         |
|        |         |                                              | 是否在软件安装前进行恶意代码检测                           |
|        | 外包软件开发  | a) 应在软件交付前检测其中可能存在的恶意代码                      | 开发单位是否在软件交付前进行了恶意代码检测                      |
|        |         | b) 应保证开发单位提供软件设计文档和使用指南                      | 开发单位是否提供软件设计文档和使用指南                        |
|        | 工程实施    | a) 应指定或授权专门的部门或人员负责工程实施过程的管理                 | 是否指定或授权专门的部门或人员负责工程实施过程的管理                 |
|        |         | b) 应制定安全工程实施方案控制工程实施过程                       | 是否制定安全工程实施方案                               |
|        |         |                                              | 是否按照安全工程实施方案进行工程实施                         |
|        | 测试验收    | a) 应制订测试验收方案, 并依据测试验收方案实施测试验收, 形成测试验收报告      | 是否制订测试验收方案                                 |
|        |         | b) 应进行上线前的安全性测试, 并出具安全测试报告                   | 是否依据测试验收方案实施测试验收, 形成测试验收报告                 |
|        |         |                                              | 是否进行上线前的安全性测试验收                            |
|        | 系统交付    | a) 应制定交付清单, 并根据交付清单对所交接的设备、软件和文档等进行清点        | 是否根据交付清单对所交接的设备、软件和文档等进行清点                 |
|        |         | b) 应对负责运行维护的技术人员进行相应的技能培训                    | 是否对负责运行维护的技术人员进行相应的技能培训                    |
|        |         | c) 应提供建设过程文档和运行维护文档                          | 是否提供建设过程文档和运行维护文档                          |
|        | 等级测评    | a) 应定期进行等级测评, 发现不符合相应等级保护标准要求的及时整改           | 是否定期进行等级测评                                 |
|        |         |                                              | 是否对不符合项进行了及时整改                             |
|        |         | b) 应在发生重大变更或级别发生变化时进行等级测评                    | 在重大变更或级别发生变化时是否进行等级测评                      |
|        | 服务供应商选择 | c) 应确保测评机构的选择符合国家有关规定                        | 测评机构是否符合国家有关规定                             |
|        |         | a) 应确保服务供应商的选择符合国家的有关规定                      | 服务供应商是否符合国家的有关规定                           |
|        |         | b) 应与选定的服务供应商签订相关协议, 明确整个服务供应链各方需履行的网络安全相关义务 | 是否与选定的服务供应商签订相关协议, 明确整个服务供应链各方需履行的网络安全相关义务 |

表 C.2 (续)

| 检查范围   | 检查内容      | 检查项                                                               | 检查要点                                             |
|--------|-----------|-------------------------------------------------------------------|--------------------------------------------------|
| 安全运维管理 | 环境管理      | a) 应指定专门的部门或人员负责机房安全, 对机房出入进行管理, 定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理    | 是否指定专门的部门或人员负责机房安全                               |
|        |           |                                                                   | 指定的部门或人员是否对机房出入进行管理                              |
|        |           |                                                                   | 是否定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理                  |
|        |           | b) 应对机房的安全管理做出规定, 包括物理访问, 物品进出和环境安全等                              | 是否建立机房安全管理规范, 对有关物理访问、物品进出和环境安全等方面的管理作出规定        |
|        |           | c) 应不在重要区域接待来访人员, 不随意放置含有敏感信息的纸档文件和移动介质等                          | 是否避免了在重要区域接待来访人员? 如何避免                           |
|        | 资产管理      |                                                                   | 是否避免了桌面等开放或者明显位置上包含敏感信息的纸档文件、移动介质等               |
|        |           | 应编制并保存与保护对象相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容                         | 是否编制并保存了与保护对象相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容      |
|        | 介质管理      | a) 应将介质存放在安全的环境中, 对各类介质进行控制和保护, 实行存储环境专人管理, 并根据存档介质的目录清单定期盘点      | 是否将介质存放在安全的环境中, 各类介质进行控制和保护                      |
|        |           |                                                                   | 是否实行存储环境专人管理                                     |
|        |           |                                                                   | 是否根据存档介质的目录清单定期盘点                                |
|        |           | b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制, 并对介质的归档和查询等进行登记记录              | 是否对介质在物理传输过程中的人员选择、打包、交付等情况进行控制                  |
|        |           |                                                                   | 是否对介质的归档和查询等进行登记记录                               |
|        | 设备维护管理    | a) 应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理                        | 是否指定专门的部门或人员定期进行维护管理                             |
|        |           | b) 应对配套设施、软硬件维护管理做出规定, 包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等            | 是否对配套设施、软硬件维护管理做出规定                              |
|        |           |                                                                   | 是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等                  |
|        | 漏洞和风险管理   | 应采取必要的措施识别安全漏洞和隐患, 对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补                 | 是否采取必要的措施识别安全漏洞和隐患                               |
|        |           |                                                                   | 对发现的安全漏洞和隐患是否及时进行修补或评估可能的影响后进行修补                 |
|        | 网络和系统安全管理 | a) 应划分不同的管理员角色进行网络和系统的运维管理, 明确各个角色的责任和权限                          | 是否划分了不同的管理员角色进行网络和系统的运维管理, 明确各个角色的责任和权限          |
|        |           | b) 应指定专门的部门或人员进行账户管理, 对申请账户、建立账户、删除账户等进行控制                        | 是否指定专门的部门或人员进行账户管理                               |
|        |           |                                                                   | 是否对申请账户、建立账户、删除账户等进行控制                           |
|        |           | c) 应建立网络和系统安全管理制度, 对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定 | 是否对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定 |
|        |           | d) 应制定重要设备的配置和操作手册, 依据手册对设备进行安全配置和优化配置等                           | 是否制定重要设备的配置和操作手册                                 |
|        |           |                                                                   | 是否依据手册对设备进行安全配置和优化配置等                            |

表 C.2 (续)

| 检查范围   | 检查内容     | 检查项                                                                   | 检查要点                                                                 |
|--------|----------|-----------------------------------------------------------------------|----------------------------------------------------------------------|
| 安全运维管理 |          | e) 应详细记录运维操作日志, 包括日常巡检工作、运行维护记录、参数的设置和修改等内容                           | 是否详细记录运维操作日志, 包括日常巡检工作、运行维护记录、参数的设置和修改等内容                            |
|        | 恶意代码防范管理 | a) 应提高所有用户的防恶意代码意识, 对外来计算机或存储设备接入系统前进行恶意代码检查等                         | 是否有相关措施提高所有用户的防恶意代码意识<br>是否对外来计算机或存储设备接入系统前进行恶意代码检查等                 |
|        |          | b) 应对恶意代码防范要求做出规定, 包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等                  | 是否对恶意代码防范要求做出规定, 包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等                   |
|        |          | c) 应定期检查恶意代码库的升级情况, 对截获的恶意代码进行及时分析处理                                  | 是否定期检查恶意代码库的升级情况                                                     |
|        |          |                                                                       | 是否对截获的恶意代码进行及时分析处理                                                   |
|        | 配置管理     | 应记录和保存基本配置信息, 包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等       | 基本配置信息是否包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等            |
|        | 密码管理     | a) 应遵循密码相关国家标准和行业标准                                                   | 是否遵循密码相关国家标准和行业标准                                                    |
|        |          | b) 应使用国家密码管理主管部门认证核准的密码技术和产品                                          | 是否使用国家密码管理主管部门认证核准的密码技术和产品                                           |
|        | 变更管理     | 应明确变更需求, 变更前根据变更需求制定变更方案, 变更方案经过评审、审批后方可实施                            | 变更前是否明确变更需求                                                          |
|        |          |                                                                       | 变更前是否根据变更需求制定变更方案                                                    |
|        |          |                                                                       | 变更方案是否经过评审                                                           |
|        | 备份与恢复管理  | a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等                                        | 是否识别需要定期备份的重要业务信息、系统数据及软件系统等                                         |
|        |          | b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等                                        | 是否规定备份信息的备份方式、备份频度、存储介质、保存期等                                         |
|        |          | c) 应根据数据的重要性和数据对系统运行的影响, 制定数据的备份策略和恢复策略、备份程序和恢复程序等                    | 是否根据数据的重要性和数据对系统运行的影响, 制定数据的备份策略和备份程序                                |
|        |          |                                                                       | 是否根据数据的重要性和数据对系统运行的影响, 制定数据的恢复策略和恢复程序                                |
|        | 安全事件处置   | a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件                                          | 是否及时向安全管理部门报告所发现的安全弱点和可疑事件                                           |
|        |          | b) 应制定安全事件报告和处置管理制度, 明确不同安全事件的报告、处置和响应流程, 规定安全事件的现场处理、事件报告和后期恢复的管理职责等 | 是否制定了安全事件报告和处置管理制度, 明确不同安全事件的报告、处置和响应流程, 规定安全事件的现场处理、事件报告和后期恢复的管理职责等 |
|        |          | c) 应在安全事件报告和响应处理过程中, 分析和鉴定事件产生的原因, 收集证据, 记录处理过程, 总结经验教训               | 是否在安全事件报告和响应处理过程中, 分析和鉴定事件产生的原因, 收集证据, 记录处理过程, 总结经验教训                |
|        | 应急预案管理   | a) 应制定重要事件的应急预案, 包括应急处理流程、系统恢复流程等内容                                   | 是否制定重要事件的应急预案, 包括应急处理流程、系统恢复流程等内容                                    |

表 C.2 （续）

| 检查范围   | 检查内容   | 检查项                                     | 检查要点                                  |
|--------|--------|-----------------------------------------|---------------------------------------|
| 安全运维管理 | 应急预案管理 | b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练       | 是否定期对系统相关的人员进行应急预案培训                  |
|        |        |                                         | 是否进行应急预案的演练                           |
|        | 外包运维管理 | a) 应确保外包运维服务商的选择符合国家的有关规定               | 是否能确保外包运维服务商的选择符合国家的有关规定              |
|        |        | b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容 | 是否与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容 |

## C.3 第三级安全通用要求检查指标（含关键信息基础设施）

安全保护等级为第三级的安全通用要求检查指标如表C.3所示。

表C.3 第三级安全通用要求检查指标

| 检查范围   | 检查内容                            | 检查项                                  | 检查要点                              |
|--------|---------------------------------|--------------------------------------|-----------------------------------|
| 安全物理环境 | 物理位置选择                          | a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内         | 机房场地是否选择在具有防震能力的建筑内               |
|        |                                 |                                      | 机房场地是否选择在具有防风能力的建筑内               |
|        |                                 |                                      | 机房场地是否选择在具有防雨等能力的建筑内              |
|        |                                 | b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施  | 机房场地是否未设在建筑物的顶层或地下室               |
|        |                                 |                                      | 机房场地设在建筑物的顶层或地下室，是否加强防水和防潮措施？具体措施 |
|        | 物理访问控制                          | 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员         | 是否在机房出入口配置了电子门禁系统                 |
|        |                                 |                                      | 是否对进入机房的人员信息进行了记录                 |
|        | 防盗窃和防破坏                         | a) 应将设备或主要部件进行固定，并设置明显的不易除去的标记       | 是否将设备或主要部件进行固定，并设置明显的不易除去的标记      |
|        |                                 | b) 应将通信线缆铺设在隐蔽安全处                    | 是否将通信线缆铺设在隐蔽安全处                   |
|        |                                 | c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统        | 是否设置机房防盗报警系统或设置有专人值守的视频监控系统       |
|        | 防雷击                             | a) 应将各类机柜、设施和设备等通过接地系统安全接地           | 是否将各类机柜、设施和设备等通过接地系统安全接地          |
|        |                                 | b) 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等      | 是否采取措施防止感应雷                       |
|        | 防火                              | a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火 | 机房是否设置火灾自动消防系统                    |
|        |                                 |                                      | 火灾自动消防系统是否能够自动检测火情、自动报警，并自动灭火     |
|        |                                 | b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料      | 机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料     |
|        |                                 |                                      | c) 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施   |
|        | 区域和区域之间是否设置隔离防火措施               |                                      |                                   |
|        |                                 | 防水和防潮                                | a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透        |
|        | b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透   |                                      | 是否采取措施防止机房内水蒸气结露和地下积水的转移与渗透       |
|        | c) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警 |                                      | 是否安装对水敏感的检测仪表或元件                  |
|        |                                 |                                      | 检测仪表或元件，是否可对机房进行防水检测和报警           |
|        | 防静电                             | a) 应采用防静电地板或地面并采用必要的接地防静电措施          | 是否安装防静电地板或地面并采用必要的接地防静电措施         |
|        |                                 | b) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等   | 是否采取措施防止静电的产生                     |

表 C.3 (续)

| 检查范围   | 检查内容  | 检查项                                                                                                       | 检查要点                                                |
|--------|-------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| 安全物理环境 | 温湿度控制 | 应设置温湿度自动调节设施,使机房温湿度的变化在设备运行所允许的范围之内                                                                       | 是否设置温湿度自动调节设施,使机房温湿度的变化在设备运行所允许的范围之内                |
|        | 电力供应  | a) 应在机房供电线路上配置稳压器和过电压防护设备                                                                                 | 是否在机房供电线路上配置了稳压器和过电压防护设备                            |
|        |       | b) 应提供短期的备用电力供应,至少满足设备在断电情况下的正常运行要求                                                                       | 是否提供了短期的备用电力供应设备,以满足设备在断电情况下的正常运行要求                 |
|        |       | c) 应设置冗余或并行的电力电缆线路为计算机系统供电                                                                                | 是否设置了冗余或并行的电力电缆线路为计算机系统供电                           |
|        | 电磁防护  | a) 电源线和通信线缆应隔离铺设,避免互相干扰                                                                                   | 是否将电源线和通信线缆隔离铺设                                     |
|        |       | b) 应对关键设备实施电磁屏蔽                                                                                           | 是否对关键设备实施了电磁屏蔽                                      |
| 安全通信网络 | 网络架构  | a) 应保证网络设备的业务处理能力满足业务高峰期需要                                                                                | 网络设备的业务处理能力是否满足业务高峰期需要                              |
|        |       | b) 应保证网络各个部分的带宽满足业务高峰期需要                                                                                  | 网络各个部分的带宽是否满足业务高峰期需要                                |
|        |       | c) 应划分不同的网络区域,并按照方便管理和控制的原则为各网络区域分配地址                                                                     | 是否划分不同的网络区域                                         |
|        |       |                                                                                                           | 是否按照方便管理和控制的原则为各网络区域分配地址                            |
|        |       | d) 应避免将重要网络区域部署在网络边界处,重要网络区域和其他网络区域之间应采取可靠的技术隔离手段                                                         | 是否避免将重要网络区域部署在网络边界处<br>重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段 |
|        |       | e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余,保证系统的可用性                                                                    | 是否提供通信线路、关键网络设备的硬件冗余                                |
|        |       |                                                                                                           | 是否提供关键计算设备的硬件冗余                                     |
|        | 通信传输  | a) 应采用校验技术或密码技术保证通信过程中数据的完整性                                                                              | 是否采用校验技术或密码技术保证通信过程中数据的完整性                          |
|        |       | b) 应采用密码技术保证通信过程中数据的保密性                                                                                   | 是否采用密码技术保证通信过程中数据的保密性                               |
|        | 可信验证  | 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证,并在应用程序的所有执行环节进行动态可信验证,在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心 | 是否基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证       |
|        |       |                                                                                                           | 是否在应用程序的所有执行环节进行动态可信验证                              |
|        |       |                                                                                                           | 在检测到其可信性受到破坏后进行报警                                   |
|        |       |                                                                                                           | 是否将验证结果形成审计记录送至安全管理中心                               |
| 安全区域边界 | 边界防护  | a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信                                                                        | 是否保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信                    |
|        |       | b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制                                                                            | 是否能够对非授权设备私自联到内部网络的行为进行检查或限制                        |

表 C.3 (续)

| 检查范围       | 检查内容        | 检查项                                                    | 检查要点                                                     |
|------------|-------------|--------------------------------------------------------|----------------------------------------------------------|
| 安全区域<br>边界 | 边界防护        | c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制                         | 是否能够对内部用户非授权联到外部网络的行为进行检查或限制                             |
|            |             | d) 应限制无线网络的使用, 保证无线网络通过受控的边界设备接入内部网络                   | 是否限制无线网络的使用, 保证无线网络通过受控的边界设备接入内部网络                       |
|            | 访问控制        | a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则, 默认情况下除允许通信外受控接口拒绝所有通信  | 是否在网络边界或区域之间根据访问控制策略设置访问控制规则, 默认情况下除允许通信外受控接口拒绝所有通信      |
|            |             | b) 应删除多余或无效的访问控制规则, 优化访问控制列表, 并保证访问控制规则数量最小化           | 是否删除了多余或无效的访问控制规则, 优化访问控制列表, 并保证访问控制规则数量最小化              |
|            |             | c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查, 以允许/拒绝数据包进出            | 是否对源地址、目的地址、源端口、目的端口和协议等进行检查, 以允许/拒绝数据包进出                |
|            |             | d) 应根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力                      | 是否根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力                          |
|            |             | e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制                        | 是否对进出网络的数据流实现基于应用协议和应用内容的访问控制                            |
|            | 入侵防范        | a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为                       | 是否在关键网络节点处检测、防止或限制从外部发起的网络攻击行为                           |
|            |             | b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为                       | 是否在关键网络节点处检测、防止或限制从内部发起的网络攻击行为                           |
|            |             | c) 应采取技术措施对网络行为进行分析, 实现对网络攻击特别是新型网络攻击行为的分析             | 是否采取技术措施对网络行为进行分析, 实现对网络攻击特别是新型网络攻击行为的分析                 |
|            |             | d) 当检测到攻击行为时, 记录攻击源 IP、攻击类型、攻击目标、攻击时间, 在发生严重入侵事件时应提供报警 | 当检测到攻击行为时, 是否记录攻击源 IP、攻击类型、攻击目标、攻击时间<br>在发生严重入侵事件时是否提供报警 |
|            | 恶意代码和垃圾邮件防范 | a) 应在关键网络节点处对恶意代码进行检测和清除, 并维护恶意代码防护机制的升级和更新            | 是否在关键网络节点处对恶意代码进行检测和清除<br>是否维护恶意代码防护机制的升级和更新?            |
|            |             | b) 应在关键网络节点处对垃圾邮件进行检测和防护, 并维护垃圾邮件防护机制的升级和更新            | 是否在关键网络节点处对垃圾邮件进行检测和防护                                   |
|            |             |                                                        | 是否维护垃圾邮件防护机制的升级和更新                                       |
|            | 安全审计        | a) 应在网络边界、重要网络节点进行安全审计, 审计覆盖到每个用户, 对重要的用户行为和重要安全事件进行审计 | 是否在网络边界进行安全审计                                            |
|            |             |                                                        | 是否在重要网络节点进行安全审计                                          |
|            |             |                                                        | 审计是否覆盖到每个用户, 是否对重要的用户行为和重要安全事件进行审计                       |
|            |             | b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息           | 审计记录是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息               |

表 C.3 (续)

| 检查范围   | 检查内容 | 检查项                                                                                                            | 检查要点                                            |
|--------|------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| 安全区域边界 | 安全审计 | c) 应对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等                                                                         | 是否对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等            |
|        |      | d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析                                                                       | 是否对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析           |
|        | 可信验证 | 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证, 并在应用程序的所有执行环节进行动态可信验证, 在检测到其可信性受到破坏后进行报警, 并将验证结果形成审计记录送至安全管理中心 | 是否基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证 |
|        |      |                                                                                                                | 是否在应用程序的所有执行环节进行动态可信验证                          |
| 安全计算环境 | 身份鉴别 | a) 应对登录的用户进行身份标识和鉴别, 身份标识具有唯一性, 身份鉴别信息具有复杂度要求并定期更换                                                             | 是否对登录的用户进行身份标识和鉴别                               |
|        |      |                                                                                                                | 登录的用户身份标识是否具有唯一性                                |
|        |      |                                                                                                                | 登录用户身份鉴别信息是否具有复杂度要求并定期更换                        |
|        |      | b) 应具有登录失败处理功能, 应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施                                                           | 是否具有登录失败处理功能                                    |
|        |      |                                                                                                                | 是否配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施           |
|        |      | c) 当进行远程管理时, 应采取必要措施防止鉴别信息在网络传输过程中被窃听                                                                          | 当进行远程管理时, 是否采取必要措施防止鉴别信息在网络传输过程中被窃听             |
|        | 访问控制 | d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别, 且其中一种鉴别技术至少应使用密码技术来实现                                              | 是否采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别        |
|        |      |                                                                                                                | 鉴别技术是否使用密码技术来实现                                 |
|        |      | a) 应对登录的用户分配账户和权限                                                                                              | 是否对登录的用户分配账户和权限                                 |
|        |      | b) 应重命名或删除默认账户, 修改默认账户的默认口令                                                                                    | 是否重命名或删除默认账户                                    |
|        |      |                                                                                                                | 是否修改默认账户的默认口令                                   |
|        |      | c) 应及时删除或停用多余的、过期的账户, 避免共享账户的存在                                                                                | 是否及时删除或停用多余的、过期的账户, 避免共享账户的存在                   |
|        |      | d) 应授予管理用户所需的最小权限, 实现管理用户的权限分离                                                                                 | 是否授予管理用户所需的最小权限, 实现管理用户的权限分离                    |
|        |      | e) 应由授权主体配置访问控制策略, 访问控制策略规定主体对客体的访问规则                                                                          | 是否由授权主体配置访问控制策略, 访问控制策略规定主体对客体的访问规则             |
|        |      | f) 访问控制的粒度应达到主体为用户级或进程级, 客体为文件、数据库表级                                                                           | 访问控制的粒度是否达到主体为用户级或进程级, 客体为文件、数据库表级              |
|        |      | g) 应对重要主体和客体设置安全标记, 并控制主体对有安全标记信息资源的访问                                                                         | 是否对主体、客体设置安全标记                                  |
|        |      |                                                                                                                | 是否依据安全标记控制主体对有安全标记信息资源的访问                       |



表 C.3 (续)

| 检查范围   | 检查内容   | 检查项                                                                                                        | 检查要点                                                                     |
|--------|--------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| 安全计算环境 | 安全审计   | a) 应启用安全审计功能, 审计覆盖到每个用户, 对重要的用户行为和重要安全事件进行审计                                                               | 是否启用安全审计功能<br>审计是否覆盖到每个用户, 以及对重要的用户行为和重要的安全事件进行审计                        |
|        |        | b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息                                                               | 审计记录是否包括事件的日期和时间、事件类型、事件是否成功及其他与审计相关的信息                                  |
|        |        | c) 应对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等                                                                     | 是否对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等                                     |
|        |        | d) 应对审计进程进行保护, 防止未经授权的中断                                                                                   | 是否应对审计进程进行保护, 防止未经授权的中断                                                  |
|        | 入侵防范   | a) 应遵循最小安装的原则, 仅安装需要的组件和应用程序                                                                               | 是否遵循最小安装的原则, 仅安装需要的组件和应用程序                                               |
|        |        | b) 应关闭不需要的系统服务、默认共享和高危端口                                                                                   | 是否关闭不需要的系统服务、默认共享和高危端口                                                   |
|        |        | c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制                                                                    | 是否通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制                                    |
|        |        | d) 应提供数据有效性检验功能, 保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求                                                            | 是否提供数据有效性检验功能, 保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求                            |
|        |        | e) 应能发现可能存在的已知漏洞, 并在经过充分测试评估后, 及时修补漏洞                                                                      | 是否具备已知漏洞发现的能力                                                            |
|        |        |                                                                                                            | 是否充分测试评估后, 及时修补漏洞                                                        |
|        |        | f) 应能够检测到对重要节点进行入侵的行为, 并在发生严重入侵事件时提供报警                                                                     | 是否能够检测到对重要节点进行入侵的行为                                                      |
|        |        |                                                                                                            | 是否能对发生严重入侵事件时提供报警                                                        |
|        | 恶意代码防范 | 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为, 并将其有效阻断                                                            | 是否采用免受恶意代码攻击的技术措施或主动免疫可信验证机制                                             |
|        |        |                                                                                                            | 是否能及时识别入侵和病毒行为                                                           |
|        |        |                                                                                                            | 是否具备有效阻断入侵和病毒行为的能力                                                       |
|        | 可信验证   | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证, 并在应用程序的关键执行环节进行动态可信验证, 在检测到其可信性受到破坏后进行报警, 并将验证结果形成审计记录送至安全管理中心 | 是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和是应用程序等进行可信验证                             |
|        |        |                                                                                                            | 是否在应用程序的关键环节进行动态可信验证                                                     |
|        |        |                                                                                                            | 是否在检测到应用程序可信根的可信性受到破坏后进行报警                                               |
|        |        |                                                                                                            | 是否将验证结果形成审计记录, 并将审计记录送至安全管理中心, 进行动态关联感知                                  |
|        | 数据完整性  | a) 应采用密码技术保证重要数据在传输过程中的完整性, 包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等                                 | 是否采用密码技术保证重要数据在传输过程中的完整性, 包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等 |

表 C.3 (续)

| 检查范围   | 检查内容   | 检查项                                                                          | 检查要点                                                                                   |
|--------|--------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| 安全计算环境 | 数据完整性  | b) 应采用密码技术保证重要数据在存储过程中的完整性, 包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等   | 是否采用密码技术保证重要数据在存储过程中的完整性, 包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等               |
|        | 数据保密性  | a) 应采用密码技术保证重要数据在传输过程中的保密性, 包括但不限于鉴别数据、重要业务数据和重要个人信息等                        | 是否采用密码技术保证重要数据在传输过程中的保密性, 包括但不限于鉴别数据、重要业务数据和重要个人信息等                                    |
|        |        | b) 应采用密码技术保证重要数据在存储过程中的保密性, 包括但不限于鉴别数据、重要业务数据和重要个人信息等                        | 是否采用密码技术保证重要数据在存储过程中的保密性, 包括但不限于鉴别数据、重要业务数据和重要个人信息等                                    |
|        | 数据备份恢复 | a) 应提供重要数据的本地数据备份与恢复功能                                                       | 是否提供重要数据的本地数据备份与恢复功能                                                                   |
|        |        | b) 应提供异地实时备份功能, 利用通信网络将重要数据实时备份至备份场地                                         | 是否提供异地实时备份功能, 利用通信网络将重要数据实时备份至备份场地                                                     |
|        |        | c) 应提供重要数据处理系统的冗余, 保证系统的高可用性                                                 | 是否提供重要数据处理系统的冗余, 保证系统的高可用性                                                             |
|        | 剩余信息保护 | a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除                                             | 是否保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除                                                         |
|        |        | b) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除                                             | 是否保证存有敏感数据的存储空间被释放或重新分配前得到完全清除                                                         |
|        | 个人信息保护 | a) 应仅采集和保存业务必需的用户个人信息                                                        | 是否仅采集和保存业务必需的用户个人信息                                                                    |
|        |        | b) 应禁止未授权访问和非法使用用户个人信息                                                       | 是否禁止未授权访问和非法使用用户个人信息                                                                   |
| 安全管理中心 | 系统管理   | a) 应对系统管理员进行身份鉴别, 只允许其通过特定的命令或操作界面进行系统管理操作, 并对这些操作进行审计                       | 安全管理中心是否对系统管理员进行身份鉴别                                                                   |
|        |        |                                                                              | 安全管理中心是否只允许系统管理员通过特定命令或操作界面进行系统管理操作                                                    |
|        |        |                                                                              | 系统管理员在安全管理中心中的操作是否进行审计                                                                 |
|        | 审计管理   | b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理, 包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等 | 是否只有系统管理员可以通过安全管理中心对系统的资源和运行进行配置、控制和管理, 包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等操作 |
|        |        |                                                                              | 安全管理中心是否对审计管理员进行身份鉴别                                                                   |
|        |        |                                                                              | 安全管理中心是否只允许审计管理员通过特定命令或操作界面进行系统管理操作                                                    |
|        |        | a) 应对审计管理员进行身份鉴别, 只允许其通过特定的命令或操作界面进行安全审计操作, 并对这些操作进行审计                       | 审计管理员在安全管理中心中的操作是否进行审计                                                                 |

表 C.3 (续)

| 检查范围   | 检查内容  | 检查项                                                                    | 检查要点                                                                             |
|--------|-------|------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| 安全管理中心 | 审计管理  | b) 应通过审计管理员对审计记录应进行分析, 并根据分析结果进行处理, 包括根据安全审计策略对审计记录进行存储、管理和查询等         | 是否只有审计管理员可以通过安全管理中心对审计记录应进行分析, 并根据分析结果进行处理, 包括根据安全审计策略对审计记录进行存储、管理和查询等操作         |
|        | 安全管理  | a) 应对安全管理员进行身份鉴别, 只允许其通过特定的命令或操作界面进行安全管理操作, 并对这些操作进行审计                 | 安全管理中心是否对安全管理员进行身份鉴别                                                             |
|        |       |                                                                        | 安全管理中心是否只允许安全管理员通过特定命令或操作界面进行系统管理操作                                              |
|        |       |                                                                        | 安全管理员在安全管理中心中的操作是否进行审计                                                           |
|        | 集中管控  | b) 应通过安全管理员对系统中的安全策略进行配置, 包括安全参数的设置, 主体、客体进行统一安全标记, 对主体进行授权, 配置可信验证策略等 | 是否只有安全管理员可以通过安全管理中心对系统中的安全策略进行配置, 包括安全参数的设置, 主体、客体进行统一安全标记, 对主体进行授权, 配置可信验证策略等操作 |
|        |       | a) 应划分出特定的管理区域, 对分布在网络中的安全设备或安全组件进行管控                                  | 网络中是否划分出特定的管理区域, 对分布在网络中的安全设备或安全组件进行管控                                           |
|        |       | b) 应能够建立一条安全的信息传输路径, 对网络中的安全设备或安全组件进行管理                                | 对网络中的安全设备或安全组件进行管理时, 是否通过具有安全保护的通信方式                                             |
|        |       | c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测                                    | 安全管理中心是否对系统中的网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测                                      |
|        |       | d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析, 并保证审计记录的留存时间符合法律法规要求                    | 是否对分散在各个设备上的审计数据进行收集汇总和集中分析                                                      |
|        |       | e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理                                       | 是否对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理                                                   |
|        |       | f) 应对网络中发生的各类安全事件进行识别、报警和分析                                            | 是否应对网络中发生的各类安全事件进行识别、报警和分析                                                       |
| 安全管理制度 | 安全策略  | 应制定网络安全工作的总体方针和安全策略, 阐明机构安全工作的总体目标、范围、原则和安全框架等                         | 检查信息安全工作的总体方针和安全策略文件, 查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等                            |
|        | 管理制度  | a) 应对安全管理活动中的各类管理内容建立安全管理制度                                            | 是否对安全管理活动中的各类管理内容建立安全管理制度                                                        |
|        |       | b) 应对管理人员或操作人员执行的日常管理操作建立操作规程                                          | 是否对管理人员或操作人员执行的日常管理操作建立操作规程                                                      |
|        |       | c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系                              | 机构是否形成全面的信息安全管理制度体系, 制度体系是否由总体方针、安全策略、管理制度、操作规程等构成                               |
|        | 制定和发布 | a) 应指定或授权专门的部门或人员负责安全管理制度的制定                                           | 是否有专门的部门或人员负责制定安全管理制度                                                            |
|        |       | b) 安全管理制度应通过正式、有效的方式发布, 并进行版本控制                                        | 安全管理制度制、修订人员, 是否按照统一的格式标准或要求制定                                                   |

表 C.3 (续)

| 检查范围   | 检查内容  | 检查项                                                           | 检查要点                                                     |
|--------|-------|---------------------------------------------------------------|----------------------------------------------------------|
| 安全管理制度 | 评审和修订 | 应定期对安全管理制度的合理性和适用性进行论证和审定,对存在不足或需要改进的安全管理制度进行修订               | 是否定期对安全管理制度的合理性和适用性进行论证和审定,对存在不足或是否改进的安全管理制度进行修订         |
| 安全管理机构 | 岗位设置  | a) 应成立指导和管理网络安全工作的委员会或领导小组,其最高领导由单位主管领导担任或授权                  | 是否成立指导和管理网络安全工作的委员会或领导小组                                 |
|        |       |                                                               | 网络安全工作委员会的最高领导是否由单位主管领导担任或授权                             |
|        |       | b) 应设立网络安全管理工作的职能部门,设立安全主管、安全管理各个方面的负责人岗位,并定义各负责人的职责          | 是否划分网络安全管理职能部门                                           |
|        |       |                                                               | 是否设立安全主管、安全管理各个方面的负责人岗位,并定义各负责人的职责                       |
|        |       | c) 应设立系统管理员、审计管理员和安全管理员等岗位,并定义部门及各个工作岗位的职责                    | 是否划分网络安全管理岗位                                             |
|        |       |                                                               | 是否明确部门及各岗位职责                                             |
|        | 人员配备  | a) 应配备一定数量的系统管理员、审计管理员和安全管理员等                                 | 是否配备系统管理员、审计管理员和安全管理员                                    |
|        |       |                                                               | 是否明确各岗位人员配备情况                                            |
|        |       | b) 应配备专职安全管理员,不可兼任                                            | 是否配备专职安全管理员                                              |
|        | 授权和审批 | a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等                            | 是否明确各部门和岗位的职责和授权范围                                       |
|        |       |                                                               | 是否明确针对审批事项、审批部门和批准人等内容与相关制度一致                            |
|        |       | b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序,按照审批程序执行审批过程,对重要活动建立逐级审批制度 | 系统变更、重要操作、物理访问和系统接入等事项是否明确建立逐级审批程序                       |
|        |       |                                                               | 审批记录、操作记录是否与相关制度一致                                       |
|        |       | c) 应定期审查审批事项,及时更新需授权和审批的项目、审批部门和审批人等信息                        | 是否对各类审批事项进行更新                                            |
|        | 沟通和合作 | a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通,定期召开协调会议,共同协作处理网络安全问题    | 是否加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通,定期召开协调会议,共同协作处理网络安全问题 |
|        |       | b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通                         | 是否建立与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通机制                    |
|        |       |                                                               | 是否与网络安全职能部门、各类供应商、业界专家及安全组织开展合作与沟通                       |
|        |       | c) 应建立外联单位联系列表,包括外联单位名称、合作内容、联系人和联系方式等信息                      | 是否建立外联单位联系列表                                             |
|        | 审核和检查 | a) 应定期进行常规安全检查,检查内容包括系统日常运行、系统漏洞和数据备份等情况                      | 是否定期进行常规安全检查,检查内容包括系统日常运行、系统漏洞和数据备份等情况                   |

表 C.3 (续)

| 检查范围       | 检查内容      | 检查项                                                           | 检查要点                                                        |
|------------|-----------|---------------------------------------------------------------|-------------------------------------------------------------|
| 安全管理机构     | 审核和检查     | b) 应定期进行全面安全检查, 检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等 | 是否定期进行全面安全检查, 检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等 |
|            |           | c) 应制定安全检查表格实施安全检查, 汇总安全检查数据, 形成安全检查报告, 并对安全检查结果进行通报          | 是否制定安全检查表格实施安全检查                                            |
| 安全管理<br>人员 | 人员录用      | a) 应指定或授权专门的部门或人员负责人员录用                                       | 是否由专门的部门或人员负责人员的录用工作                                        |
|            |           | b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查, 对其所具有的技术技能进行考核               | 是否对被录用人员的身份、安全背景、专业资格或资质等进行审查                               |
|            |           |                                                               | 是否对被录用人员所具有的技术技能进行考核                                        |
|            |           | c) 应与被录用人员签署保密协议, 与关键岗位人员签署岗位责任协议                             | 是否与被录用人员签署保密协议                                              |
|            |           |                                                               | 是否与关键岗位人员签署岗位责任协议                                           |
|            | 人员离岗      | a) 应及时终止离岗人员的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备              | 是否及时终止离岗人员的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备              |
|            |           |                                                               | 管理文档中是否规定人员调离手续和离岗要求等                                       |
|            |           | b) 应办理严格的调离手续, 并承诺调离后的保密义务后方可离开                               | 是否具有按照离岗程序办理调离手续的记录                                         |
|            |           |                                                               | 保密承诺文档是否有调离人员的签字                                            |
|            | 安全意识教育和培训 | a) 应对各类人员进行安全意识教育和岗位技能培训, 并告知相关的安全责任和惩戒措施                     | 是否建立相关制度对各类人员进行安全意识教育和岗位技能培训                                |
|            |           |                                                               | 是否告知相关的安全责任和惩戒措施                                            |
|            |           | b) 应针对不同岗位制定不同的培训计划, 对安全基础知识、岗位操作规程等进行培训                      | 是否建立相关制度针对不同岗位制定不同的培训计划, 包括安全基础知识、岗位操作规程等内容                 |
|            |           | c) 应定期对不同岗位的人员进行技术技能考核                                        | 是否定期对不同岗位的人员进行技术技能考核                                        |
|            | 外部人员访问管理  | a) 应在外部人员物理访问受控区域前提出书面申请, 批准后由专人全程陪同, 并登记备案                   | 是否建立相关制度明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等              |
|            |           |                                                               | 外部人员物理访问受控区域前是否先提出书面申请                                      |
|            |           |                                                               | 是否由专人全程陪同, 并登记备案                                            |
|            |           | b) 应在外部人员接入受控网络访问系统前提出书面申请, 批准后由专人开设账户、分配权限, 并登记备案            | 是否建立相关制度明确外部人员接入网络前的申请审批流程                                  |
|            |           |                                                               | 外部人员接入受控网络访问系统前是否先提出书面申请                                    |
|            |           |                                                               | 是否由专人开设账户、分配权限, 并登记备案                                       |
|            |           | c) 外部人员离场后应及时清除其所有的访问权限                                       | 外部人员离场后是否及时清除其所有的访问权限                                       |

表 C.3 (续)

| 检查范围       | 检查内容         | 检查项                                                                     | 检查要点                                                                 |
|------------|--------------|-------------------------------------------------------------------------|----------------------------------------------------------------------|
| 安全管理<br>人员 | 外部人员<br>访问管理 | d) 获得系统访问授权的外部人员应签署保密协议, 不得进行非授权操作, 不得复制和泄露任何敏感信息                       | 获得系统访问授权的外部人员是否签署保密协议                                                |
| 安全建设<br>管理 | 定级和备<br>案    | a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由                                      | 是否有书面材料说明保护对象的安全保护等级及确定等级的方法和理由                                      |
|            |              | b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定                                 | 是否组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定                                |
|            |              | c) 应保证定级结果经过相关部门的批准                                                     | 定级结果是否经过相关部门的批准                                                      |
|            |              | d) 应将备案材料报主管部门和相应公安机关备案                                                 | 备案材料是否报主管部门和相应公安机关备案                                                 |
|            | 安全方案<br>设计   | a) 应根据安全保护等级选择基本安全措施, 依据风险分析的结果补充和调整安全措施                                | 是否根据安全保护等级选择基本安全措施, 依据风险分析的结果补充和调整安全措施                               |
|            |              | b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计, 设计内容应包含密码技术相关内容, 并形成配套文件 | 是否根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计, 设计内容是否包含密码相关内容, 并形成配套文件 |
|            |              | c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定, 经过批准后才能正式实施              | 是否组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定                          |
|            |              |                                                                         | 安全整体规划及配套文件是否经过批准                                                    |
|            | 产品采购<br>和使用  | a) 应确保网络安全产品采购和使用符合国家的有关规定                                              | 网络安全产品采购是否符合国家的有关规定                                                  |
|            |              |                                                                         | 网络安全产品使用是否符合国家的有关规定                                                  |
|            |              | b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求                                      | 密码产品与服务的采购是否符合国家密码管理主管部门的要求                                          |
|            |              |                                                                         | 密码产品与服务的使用是否符合国家密码管理主管部门的要求                                          |
|            |              | c) 应预先对产品进行选型测试, 确定产品的候选范围, 并定期审定和更新候选产品名单                              | 是否预先对产品进行选型测试, 确定产品的候选范围                                             |
|            |              |                                                                         | 是否定期审定和更新候选产品名单                                                      |
|            | 自行软件<br>开发   | a) 应将开发环境与实际运行环境物理分开, 测试数据和测试结果受到控制                                     | 是否将开发环境与实际运行环境物理分开, 测试数据和测试结果受到控制                                    |
|            |              | b) 应制定软件开发管理制度, 明确说明开发过程的控制方法和人员行为准则                                    | 是否制定软件开发管理制度, 明确说明开发过程的控制方法和人员行为准则                                   |
|            |              | c) 应制定代码编写安全规范, 要求开发人员参照规范编写代码                                          | 是否制定代码编写安全规范, 要求开发人员参照规范编写代码                                         |
|            |              | d) 应具备软件设计的相关文档和使用指南, 并对文档使用进行控制                                        | 是否具备软件设计的相关文档和使用指南, 并对文档使用进行控制                                       |

表 C.3 (续)

| 检查范围   | 检查内容    | 检查项                                                | 检查要点                                    |
|--------|---------|----------------------------------------------------|-----------------------------------------|
| 安全建设管理 | 自行软件开发  | e) 应在软件开发过程中对安全性进行测试, 在软件安装前对可能存在的恶意代码进行检测         | 是否在软件开发过程中对安全性进行测试                      |
|        |         |                                                    | 是否在软件安装前进行恶意代码检测                        |
|        |         | f) 应对程序资源库的修改、更新、发布进行授权和批准, 并严格进行版本控制              | 是否对程序资源库的修改、更新、发布进行授权和批准, 并严格进行版本控制     |
|        |         | g) 应保证开发人员为专职人员, 开发人员的开发活动受到控制、监视和审查               | 开发人员是否为专职人员                             |
|        |         |                                                    | 开发人员的开发活动是否受到控制、监视和审查                   |
|        | 外包软件开发  | a) 应在软件交付前检测其中可能存在的恶意代码                            | 开发单位是否在软件交付前进行了恶意代码检测                   |
|        |         | b) 应保证开发单位提供软件设计文档和使用指南                            | 开发单位是否提供软件设计文档和使用指南                     |
|        |         | c) 应保证开发单位提供软件源代码, 并审查软件中可能存在的后门和隐蔽信道              | 开发单位是否提供软件源代码                           |
|        |         |                                                    | 是否审查了软件中可能存在的后门和隐蔽信道                    |
|        | 工程实施    | a) 应指定或授权专门的部门或人员负责工程实施过程的管理                       | 是否指定或授权专门的部门或人员负责工程实施过程的管理              |
|        |         | b) 应制定安全工程实施方案控制工程实施过程                             | 是否制定安全工程实施方案                            |
|        |         |                                                    | 是否按照安全工程实施方案进行工程实施                      |
|        |         | c) 应通过第三方工程监理控制项目的实施过程                             | 是否通过第三方工程监理控制项目的实施过程                    |
|        | 测试验收    | a) 应制订测试验收方案, 并依据测试验收方案实施测试验收, 形成测试验收报告            | 是否制订测试验收方案                              |
|        |         |                                                    | 是否依据测试验收方案实施测试验收, 形成测试验收报告              |
|        |         | b) 应进行上线前的安全性测试, 并出具安全测试报告, 安全测试报告应包含密码应用安全性测试相关内容 | 是否进行上线前的安全性测试验收                         |
|        | 系统交付    | a) 应制定交付清单, 并根据交付清单对所交接的设备、软件和文档等进行清点              | 安全测试报告是否包含密码应用安全性测试相关内容                 |
|        |         | b) 应对负责运行维护的技术人员进行相应的技能培训                          | 是否根据交付清单对所交接的设备、软件和文档等进行清点              |
|        |         | c) 应提供建设过程文档和运行维护文档                                | 是否对负责运行维护的技术人员进行相应的技能培训                 |
|        | 等级测评    | a) 应定期进行等级测评, 发现不符合相应等级保护标准要求的及时整改                 | 是否提供建设过程文档和运行维护文档                       |
|        |         |                                                    | 是否定期进行等级测评                              |
|        |         | b) 应在发生重大变更或级别发生变化时进行等级测评                          | 是否对不符合项进行了及时整改                          |
|        |         | c) 应确保测评机构的选择符合国家有关规定                              | 在重大变更或级别发生变化时是否进行等级测评                   |
|        | 服务供应商选择 | a) 应确保服务供应商的选择符合国家的有关规定                            | 测评机构是否符合国家有关规定                          |
|        |         | b) 应与选定的服务供应商签订相关协议, 明确整个服务供应链各方需履行的网络安全相关义务       | 服务供应商是否符合国家的有关规定                        |
|        | 服务供应链   |                                                    | 是否与服务供应商签订相关协议, 明确整个服务供应链各方需履行的网络安全相关义务 |

表 C.3 (续)

| 检查范围   | 检查内容    | 检查项                                                                   | 检查要点                                        |
|--------|---------|-----------------------------------------------------------------------|---------------------------------------------|
| 安全建设管理 | 服务供应商选择 | c) 应定期监督、评审和审核服务供应商提供的服务, 并对其变更服务内容加以控制                               | 是否定期监督、评审和审核服务供应商提供的服务                      |
|        |         |                                                                       | 是否对服务供应商变更服务内容加以控制                          |
| 安全运维管理 | 环境管理    | a) 应指定专门的部门或人员负责机房安全, 对机房出入进行管理, 定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理        | 是否指定专门的部门或人员负责机房安全                          |
|        |         |                                                                       | 指定的部门或人员是否对机房出入进行管理                         |
|        |         |                                                                       | 是否定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理             |
|        |         | b) 应建立机房安全管理制度, 对有关物理访问、物品进出和环境安全等方面的管理作出规定                           | 是否建立机房安全管理制度, 对有关物理访问、物品进出和环境安全等方面的管理作出规定   |
|        |         | c) 应不在重要区域接待来访人员, 不随意放置含有敏感信息的纸档文件和移动介质等                              | 是否避免了在重要区域接待来访人员? 如何避免                      |
|        |         |                                                                       | 是否避免了桌面等开放或者明显位置上包含敏感信息的纸档文件、移动介质等          |
|        | 资产管理    | a) 应编制并保存与保护对象相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容                          | 是否编制并保存了与保护对象相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容 |
|        |         | b) 应根据资产的重要程度对资产进行标识管理, 根据资产的价值选择相应的管理措施                              | 是否根据资产的重要程度对资产进行标识管理                        |
|        |         |                                                                       | 是否根据资产的价值选择相应的管理措施                          |
|        |         | c) 应对信息分类与标识方法作出规定, 并对信息的使用、传输和存储等进行规范化管理                             | 是否对信息分类与标识方法作出规定                            |
|        | 介质管理    |                                                                       | 是否对信息的使用、传输和存储等进行规范化管理                      |
|        |         | a) 应将介质存放在安全的环境中, 对各类介质进行控制和保护, 实行存储环境专人管理, 并根据存档介质的目录清单定期盘点          | 是否将介质存放在安全的环境中, 各类介质进行控制和保护                 |
|        |         |                                                                       | 是否实行存储环境专人管理                                |
|        |         |                                                                       | 是否根据存档介质的目录清单定期盘点                           |
|        |         | b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制, 并对介质的归档和查询等进行登记记录                  | 是否对介质在物理传输过程中的人员选择、打包、交付等情况进行控制             |
|        |         |                                                                       | 是否对介质的归档和查询等进行登记记录                          |
|        | 设备维护管理  | a) 应对各种设备 (包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理                           | 是否指定专门的部门或人员定期进行维护管理                        |
|        |         | b) 应建立配套设施、软硬件维护方面的管理制度, 对其维护进行有效的管理, 包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等 | 是否对配套设施、软硬件维护管理做出规定                         |
|        |         |                                                                       | 是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等             |
|        |         | c) 信息处理设备应经过审批才能带离机房或办公地点, 含有存储介质的设备带出工作环境时其中重要数据应加密                  | 信息处理设备带离机房或办公地点前是否经过审批                      |
|        |         |                                                                       | 含有存储介质的设备带出工作环境时其中重要数据是否加密                  |



表 C.3 (续)

| 检查范围   | 检查内容      | 检查项                                                                          | 检查要点                                                      |
|--------|-----------|------------------------------------------------------------------------------|-----------------------------------------------------------|
| 安全运维管理 | 设备维护管理    | d) 含有存储介质的设备在报废或重用前, 应进行完全清除或被安全覆盖, 保证该设备上的敏感数据和授权软件无法被恢复重用                  | 含有存储介质的设备在报废或重用前, 是否进行完全清除或被安全覆盖, 保证该设备上的敏感数据和授权软件无法被恢复重用 |
|        | 漏洞和风险管理   | a) 应采取必要的措施识别安全漏洞和隐患, 对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补                         | 是否采取必要的措施识别安全漏洞和隐患                                        |
|        |           |                                                                              | 对发现的安全漏洞和隐患是否及时进行修补或评估可能的影响后进行修补                          |
|        |           | b) 应定期开展安全测评, 形成安全测评报告, 采取措施应对发现的安全问题                                        | 是否定期开展安全测评                                                |
|        |           |                                                                              | 是否形成安全测评报告                                                |
|        |           |                                                                              | 是否采取措施应对发现的安全问题                                           |
|        | 网络和系统安全管理 | a) 应划分不同的管理员角色进行网络和系统的运维管理, 明确各个角色的责任和权限                                     | 是否划分了不同的管理员角色进行网络和系统的运维管理, 明确各个角色的责任和权限                   |
|        |           | b) 应指定专门的部门或人员进行账户管理, 对申请账户、建立账户、删除账户等进行控制                                   | 是否指定专门的部门或人员进行账户管理                                        |
|        |           |                                                                              | 是否对申请账户、建立账户、删除账户等进行控制                                    |
|        |           | c) 应建立网络和系统安全管理制度, 对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定            | 是否对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定          |
|        |           | d) 应制定重要设备的配置和操作手册, 依据手册对设备进行安全配置和优化配置等                                      | 是否制定重要设备的配置和操作手册                                          |
|        |           |                                                                              | 是否依据手册对设备进行安全配置和优化配置等                                     |
|        |           | e) 应详细记录运维操作日志, 包括日常巡检工作、运行维护记录、参数的设置和修改等内容                                  | 是否详细记录运维操作日志, 包括日常巡检工作、运行维护记录、参数的设置和修改等内容                 |
|        |           | f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计, 及时发现可疑行为                                  | 是否指定专门的部门或人员对日志、监测和报警数据等进行分析、统计, 及时发现可疑行为                 |
|        |           | g) 应严格控制变更性运维, 经过审批后才可改变连接、安装系统组件或调整配置参数, 操作过程中应保留不可更改的审计日志, 操作结束后应同步更新配置信息库 | 是否严格控制变更性运维, 经过审批后才可改变连接、安装系统组件或调整配置参数                    |
|        |           |                                                                              | 操作过程中是否保留不可更改的审计日志                                        |
|        |           |                                                                              | 操作结束后是否同步更新配置信息库                                          |
|        |           | h) 应严格控制运维工具的使用, 经过审批后才可接入进行操作, 操作过程中应保留不可更改的审计日志, 操作结束后应删除工具中的敏感数据          | 是否严格控制运维工具的使用, 经过审批后才可接入进行操作                              |
|        |           |                                                                              | 操作过程中是否保留不可更改的审计日志                                        |
|        |           |                                                                              | 操作结束后是否删除工具中的敏感数据                                         |
|        |           | i) 应严格控制远程运维的开通, 经过审批后才可开通远程运维接口或通道, 操作过程中应保留不可更改的审计日志, 操作结束后应立即关闭接口或通道      | 是否严格控制远程运维的开通, 经过审批后才可开通远程运维接口或通道                         |
|        |           |                                                                              | 操作过程中是否保留不可更改的审计日志                                        |
|        |           |                                                                              | 操作结束后是否立即关闭接口或通道                                          |

表 C.3 (续)

| 检查范围   | 检查内容      | 检查项                                                                 | 检查要点                                                               |
|--------|-----------|---------------------------------------------------------------------|--------------------------------------------------------------------|
| 安全运维管理 | 网络和系统安全管理 | j) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为                  | 是否保证所有与外部的连接均得到授权和批准<br>是否定期检查违反规定无线上网及其他违反网络安全策略的行为               |
|        | 恶意代码防范管理  | a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等                        | 是否有相关措施提高所有用户的防恶意代码意识<br>是否对外来计算机或存储设备接入系统前进行恶意代码检查等               |
|        |           | b) 应定期验证防范恶意代码攻击的技术措施的有效性                                           | 是否定期验证防范恶意代码攻击的技术措施的有效性                                            |
|        | 配置管理      | a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等   | 基本配置信息是否包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等          |
|        |           | b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库                       | 是否将基本配置信息改变纳入变更范畴                                                  |
|        |           |                                                                     | 是否及时更新基本配置信息库                                                      |
|        | 密码管理      | a) 应遵循密码相关国家标准和行业标准                                                 | 是否遵循密码相关国家标准和行业标准                                                  |
|        |           | b) 应使用国家密码管理主管部门认证核准的密码技术和产品                                        | 是否使用国家密码管理主管部门认证核准的密码技术和产品                                         |
|        | 变更管理      | a) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施                         | 变更前是否明确变更需求<br>变更前是否根据变更需求制定变更方案<br>变更方案是否经过评审                     |
|        |           |                                                                     | 是否建立了变更的申报和审批控制程序                                                  |
|        |           |                                                                     | 是否依据程序控制所有的变更<br>是否记录变更实施过程                                        |
|        |           | b) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程                             | 是否建立了变更的申报和审批控制程序                                                  |
|        |           |                                                                     | 是否依据程序控制所有的变更<br>是否记录变更实施过程                                        |
|        |           | c) 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练                   | 是否建立中止变更并从失败变更中恢复的程序，以明确过程控制方法和人员职责                                |
|        |           |                                                                     | 是否规定了在必要时对恢复过程进行演练                                                 |
|        | 备份与恢复管理   | a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等                                      | 是否识别需要定期备份的重要业务信息、系统数据及软件系统等                                       |
|        |           | b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等                                      | 是否规定备份信息的备份方式、备份频度、存储介质、保存期等                                       |
|        |           | c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等                   | 是否根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和备份程序                               |
|        |           |                                                                     | 是否根据数据的重要性和数据对系统运行的影响，制定数据的恢复策略和恢复程序                               |
|        | 安全事件处置    | a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件                                        | 是否及时向安全管理部门报告所发现的安全弱点和可疑事件                                         |
|        |           | b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等 | 是否制定了安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等 |

表 C.3 (续)

| 检查范围   | 检查内容   | 检查项                                                                      | 检查要点                                              |
|--------|--------|--------------------------------------------------------------------------|---------------------------------------------------|
| 安全运维管理 | 安全事件处置 | c) 应在安全事件报告和响应处理过程中,分析和鉴定事件产生的原因,收集证据,记录处理过程,总结经验教训                      | 是否在安全事件报告和响应处理过程中,分析和鉴定事件产生的原因,收集证据,记录处理过程,总结经验教训 |
|        |        | d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序                                  | 对造成系统中断和造成信息泄漏的重大安全事件是否采用不同的处理程序和报告程序             |
|        | 应急预案管理 | a) 应规定统一的应急预案框架,包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容                       | 是否规定统一的应急预案框架包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容   |
|        |        | b) 应制定重要事件的应急预案,包括应急处理流程、系统恢复流程等内容                                       | 是否制定重要事件的应急预案,包括应急处理流程、系统恢复流程等内容                  |
|        |        | c) 应定期对系统相关的人员进行应急预案培训,并进行应急预案的演练                                        | 是否定期对系统相关的人员进行应急预案培训                              |
|        |        |                                                                          | 是否进行应急预案的演练                                       |
|        |        | d) 应定期对原有的应急预案重新评估,修订完善                                                  | 是否定期对原有的应急预案重新评估,修订完善                             |
|        | 外包运维管理 | a) 应确保外包运维服务商的选择符合国家的有关规定                                                | 是否能确保外包运维服务商的选择符合国家的有关规定                          |
|        |        | b) 应与选定的外包运维服务商签订相关的协议,明确约定外包运维的范围、工作内容                                  | 是否与选定的外包运维服务商签订相关的协议,明确约定外包运维的范围、工作内容             |
|        |        | c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力,并将能力要求在签订的协议中明确          | 是否能保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力     |
|        |        |                                                                          | 是否将能力要求在签订的协议中明确                                  |
|        |        | d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求,对IT基础设施中断服务的应急保障要求等 | 是否在与外包运维服务商签订的协议中明确所有相关的安全要求                      |

## C.4 第四级安全通用要求检查指标（含关键信息基础设施）

安全保护等级为第四级的安全通用要求检查指标如表C.4所示。

表C.4 第四级安全通用要求检查指标

| 检查范围   | 检查内容    | 检查项                                  | 检查要点                          |
|--------|---------|--------------------------------------|-------------------------------|
| 安全物理环境 | 物理位置选择  | a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内         | 机房场地是否选择在具有防震能力的建筑内           |
|        |         |                                      | 机房场地是否选择在具有防风能力的建筑内           |
|        |         |                                      | 机房场地是否选择在具有防雨等能力的建筑内          |
|        |         | b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施  | 机房场地是否未设在建筑物的顶层或地下室           |
|        |         |                                      | 机房场地设在建筑物的顶层或地下室，是否加强防水和防潮措施  |
|        | 物理访问控制  | a) 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员      | 是否在机房出入口配置了电子门禁系统             |
|        |         |                                      | 是否对进入机房的人员信息进行了记录             |
|        |         | b) 重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员    | 是否在重要区域配置了第二道电子门禁系统           |
|        |         |                                      | 是否对进入重要区域的人员信息进行了记录           |
|        | 防盗窃和防破坏 | a) 应将设备或主要部件进行固定，并设置明显的不易除去的标记       | 是否将设备或主要部件进行固定，并设置明显的不易除去的标记  |
|        |         | b) 应将通信线缆铺设在隐蔽安全处                    | 是否将通信线缆铺设在隐蔽安全处               |
|        |         | c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统        | 是否设置机房防盗报警系统或设置有专人值守的视频监控系统   |
|        | 防雷击     | a) 应将各类机柜、设施和设备等通过接地系统安全接地           | 是否将各类机柜、设施和设备等通过接地系统安全接地      |
|        |         | b) 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等      | 是否采取措施防止感应雷                   |
|        | 防火      | a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火 | 机房是否设置火灾自动消防系统                |
|        |         |                                      | 火灾自动消防系统是否能够自动检测火情、自动报警，并自动灭火 |
|        |         | b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料      | 机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料 |
|        |         |                                      | 是否对机房划分区域进行管理                 |
|        | 防水和防潮   | a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透           | 是否采取措施防止雨水通过机房窗户、屋顶和墙壁渗透      |
|        |         |                                      | 是否采取措施防止机房内水蒸气结露和地下积水的转移与渗透   |
|        |         | c) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警      | 是否安装对水敏感的检测仪表或元件              |
|        |         |                                      | 检测仪表或元件，是否可对机房进行防水检测和报警       |

表 C.4 (续)

| 检查范围   | 检查内容  | 检查项                                                | 检查要点                                  |
|--------|-------|----------------------------------------------------|---------------------------------------|
| 安全物理环境 | 防静电   | a) 应采用防静电地板或地面并采用必要的接地防静电措施                        | 是否安装防静电地板或地面并采用必要的接地防静电措施             |
|        |       | b) 应采取措施防止静电的产生, 例如采用静电消除器、佩戴防静电手环等                | 是否采取措施防止静电的产生                         |
|        | 温湿度控制 | 应设置温湿度自动调节设施, 使机房温湿度的变化在设备运行所允许的范围之内               | 是否设置温湿度自动调节设施, 使机房温湿度的变化在设备运行所允许的范围之内 |
|        | 电力供应  | a) 应在机房供电线路上配置稳压器和过电压防护设备                          | 是否在机房供电线路上配置了稳压器和过电压防护设备              |
|        |       | b) 应提供短期的备用电力供应, 至少满足设备在断电情况下的正常运行要求               | 是否提供了短期的备用电力供应设备, 以满足设备在断电情况下的正常运行要求  |
|        |       | c) 应设置冗余或并行的电力电缆线路为计算机系统供电                         | 是否设置了冗余或并行的电力电缆线路为计算机系统供电             |
|        |       | d) 应提供应急供电设施                                       | 是否提供了应急供电设施                           |
|        | 电磁防护  | a) 电源线和通信线缆应隔离铺设, 避免互相干扰                           | 是否将电源线和通信线缆隔离铺设                       |
|        |       | b) 应对关键设备或关键区域实施电磁屏蔽                               | 是否对关键设备或关键区域实施了电磁屏蔽                   |
| 安全通信网络 | 网络架构  | a) 应保证网络设备的业务处理能力满足业务高峰期需要                         | 网络设备的业务处理能力是否满足业务高峰期需要                |
|        |       | b) 应保证网络各个部分的带宽满足业务高峰期需要                           | 网络各个部分的带宽是否满足业务高峰期需要                  |
|        |       | c) 应划分不同的网络区域, 并按照方便管理和控制的原则为各网络区域分配地址             | 是否划分不同的网络区域                           |
|        |       |                                                    | 是否按照方便管理和控制的原则为各网络区域分配地址              |
|        |       | d) 应避免将重要网络区域部署在网络边界处, 重要网络区域和其他网络区域之间应采取可靠的技术隔离手段 | 是否避免将重要网络区域部署在网络边界处                   |
|        |       |                                                    | 重要网络区域与其他网络区域之间是否采取可靠的技术隔离手段          |
|        |       | e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余, 保证系统的可用性            | 是否提供通信线路、关键网络设备的硬件冗余                  |
|        |       |                                                    | 是否提供关键计算设备的硬件冗余                       |
|        |       | f) 应可按照业务服务的重要程度分配带宽, 优先保障重要业务                     | 是否按照业务服务的重要程度分配带宽, 优先保障重要业务           |
|        | 通信传输  | a) 应采用密码技术保证通信过程中数据的完整性                            | 是否采用密码技术保证通信过程中数据的完整性                 |
|        |       | b) 应采用密码技术保证通信过程中数据的保密性                            | 是否采用密码技术保证通信过程中数据的保密性                 |
|        |       | c) 应在通信前基于密码技术对通信的双方进行验证或认证                        | 是否在通信前基于密码技术对通信的双方进行验证或认证             |
|        |       | d) 应基于硬件密码模块对重要通信过程进行密码运算和密钥管理                     | 是否基于硬件密码模块对重要通信过程进行密码运算和密钥管理          |

表 C.4 (续)

| 检查范围   | 检查内容 | 检查项                                                                                                                 | 检查要点                                               |
|--------|------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| 安全通信网络 | 可信验证 | 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知 | 是否基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证      |
|        |      |                                                                                                                     | 是否在应用程序的所有执行环节进行动态可信验证                             |
|        |      |                                                                                                                     | 在检测到其可信性受到破坏后进行报警                                  |
|        |      |                                                                                                                     | 是否将验证结果形成审计记录送至安全管理中心，并进行动态关联感知                    |
| 安全区域边界 | 边界防护 | a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信                                                                                  | 是否保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信                   |
|        |      | b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制                                                                                      | 是否能够对非授权设备私自联到内部网络的行为进行检查或限制                       |
|        |      | c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制                                                                                      | 是否能够对内部用户非授权联到外部网络的行为进行检查或限制                       |
|        |      | d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络                                                                                 | 是否限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络                  |
|        |      | e) 应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断                                                                | 是否能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断 |
|        |      | f) 应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信                                                                          | 是否采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信           |
|        | 访问控制 | a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信                                                                | 是否在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信 |
|        |      | b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化                                                                          | 是否删除了多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化          |
|        |      | c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出                                                                          | 是否对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出           |
|        |      | d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力                                                                                  | 是否能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力                   |
|        |      | e) 应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换                                                                                   | 是否在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换                    |
|        | 入侵防范 | a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为                                                                                    | 是否在关键网络节点处检测、防止或限制从外部发起的网络攻击行为                     |
|        |      | b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为                                                                                    | 是否在关键网络节点处检测、防止或限制从内部发起的网络攻击行为                     |

表 C.4 (续)

| 检查范围   | 检查内容        | 检查项                                                                                                                   | 检查要点                                            |
|--------|-------------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| 安全区域边界 | 入侵防范        | c) 应采取技术措施对网络行为进行分析,实现对网络攻击特别是新型网络攻击行为的分析                                                                             | 是否采取技术措施对网络行为进行分析,实现对网络攻击特别是新型网络攻击行为的分析         |
|        |             | d) 当检测到攻击行为时,记录攻击源 IP、攻击类型、攻击目标、攻击时间,在发生严重入侵事件时应提供报警                                                                  | 当检测到攻击行为时,是否记录攻击源 IP、攻击类型、攻击目标、攻击时间             |
|        |             |                                                                                                                       | 在发生严重入侵事件时是否提供报警                                |
|        | 恶意代码和垃圾邮件防范 | a) 应在关键网络节点处对恶意代码进行检测和清除,并维护恶意代码防护机制的升级和更新                                                                            | 是否在关键网络节点处对恶意代码进行检测和清除                          |
|        |             |                                                                                                                       | 是否维护恶意代码防护机制的升级和更新                              |
|        |             | b) 应在关键网络节点处对垃圾邮件进行检测和防护,并维护垃圾邮件防护机制的升级和更新                                                                            | 是否在关键网络节点处对垃圾邮件进行检测和防护                          |
|        | 安全审计        |                                                                                                                       | 是否维护垃圾邮件防护机制的升级和更新                              |
|        |             | a) 应在网络边界、重要网络节点进行安全审计,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计                                                                  | 是否在网络边界进行安全审计                                   |
|        |             |                                                                                                                       | 是否在重要网络节点进行安全审计                                 |
|        |             | b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息                                                                          | 审计是否覆盖到每个用户,是否对重要的用户行为和重要安全事件进行审计               |
|        | 可信验证        | c) 应对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等                                                                                  | 审计记录是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息      |
|        |             |                                                                                                                       | 是否对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等              |
| 安全计算环境 | 身份鉴别        | 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证,并在应用程序的所有执行环节进行动态可信验证,在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心,并进行动态关联感知 | 是否基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证 |
|        |             |                                                                                                                       | 是否在应用程序的所有执行环节进行动态可信验证                          |
|        |             |                                                                                                                       | 在检测到其可信性受到破坏后进行报警                               |
|        |             |                                                                                                                       | 是否将验证结果形成审计记录送至安全管理中心,并进行动态关联感知                 |
|        |             | a) 应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定期更换                                                                      | 是否对登录的用户进行身份标识和鉴别                               |
|        |             |                                                                                                                       | 登录的用户身份标识是否具有唯一性                                |
|        |             |                                                                                                                       | 登录用户身份鉴别信息是否具有复杂度要求并定期更换                        |
|        |             | b) 应具有登录失败处理功能,应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施                                                                   | 是否具有登录失败处理功能                                    |
|        |             |                                                                                                                       | 是否配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施           |

表 C.4 (续)

| 检查范围   | 检查内容 | 检查项                                                               | 检查要点                                          |
|--------|------|-------------------------------------------------------------------|-----------------------------------------------|
| 安全计算环境 | 身份鉴别 | c) 当进行远程管理时, 应采取必要措施防止鉴别信息在网络传输过程中被窃听                             | 当进行远程管理时, 是否采取必要措施防止鉴别信息在网络传输过程中被窃听           |
|        |      | d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别, 且其中一种鉴别技术至少应使用密码技术来实现 | 是否采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别      |
|        |      |                                                                   | 鉴别技术是否使用密码技术来实现                               |
|        | 访问控制 | a) 应对登录的用户分配账户和权限                                                 | 是否对登录的用户分配账户和权限                               |
|        |      | b) 应重命名或删除默认账户, 修改默认账户的默认口令                                       | 是否重命名或删除默认账户                                  |
|        |      |                                                                   | 是否修改默认账户的默认口令                                 |
|        |      | c) 应及时删除或停用多余的、过期的账户, 避免共享账户的存在                                   | 是否及时删除或停用多余的、过期的账户, 避免共享账户的存在                 |
|        |      | d) 应授予管理用户所需的最小权限, 实现管理用户的权限分离                                    | 是否授予管理用户所需的最小权限, 实现管理用户的权限分离                  |
|        |      | e) 应由授权主体配置访问控制策略, 访问控制策略规定主体对客体的访问规则                             | 是否由授权主体配置访问控制策略, 访问控制策略规定主体对客体的访问规则           |
|        |      | f) 访问控制的粒度应达到主体为用户级或进程级, 客体为文件、数据库表级                              | 访问控制的粒度是否达到主体为用户级或进程级, 客体为文件、数据库表级            |
|        |      | g) 应对主体、客体设置安全标记, 并依据安全标记和强制访问控制规则确定主体对客体的访问                      | 是否对主体、客体设置安全标记                                |
|        |      |                                                                   | 是否依据安全标记和强制访问控制规则确定主体对客体的访问                   |
|        | 安全审计 | a) 应启用安全审计功能, 审计覆盖到每个用户, 对重要的用户行为和重要安全事件进行审计                      | 是否启用安全审计功能                                    |
|        |      |                                                                   | 审计是否覆盖到每个用户, 以及对重要的用户行为和重要的安全事件进行审计           |
|        |      | b) 审计记录应包括事件的日期和时间、事件类型、主体标识、客体标识和结果等                             | 审计记录是否包括事件的日期和时间、事件类型、主体标识、客体标识和结果等           |
|        |      | c) 应对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等                            | 是否对审计记录进行保护, 定期备份, 避免受到未预期的删除、修改或覆盖等          |
|        | 入侵防范 | d) 应对审计进程进行保护, 防止未经授权的中断                                          | 是否应对审计进程进行保护, 防止未经授权的中断                       |
|        |      | a) 应遵循最小安装的原则, 仅安装需要的组件和应用程序                                      | 是否遵循最小安装的原则, 仅安装需要的组件和应用程序                    |
|        |      | b) 应关闭不需要的系统服务、默认共享和高危端口                                          | 是否关闭不需要的系统服务、默认共享和高危端口                        |
|        |      | c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制                           | 是否通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制         |
|        |      | d) 应提供数据有效性检验功能, 保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求                   | 是否提供数据有效性检验功能, 保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求 |
|        |      | e) 应能发现可能存在的已知漏洞, 并在经过充分测试评估后, 及时修补漏洞                             | 是否具备已知漏洞发现的能力                                 |
|        |      |                                                                   | 是否充分测试评估后, 及时修补漏洞                             |



表 C.4 (续)

| 检查范围   | 检查内容   | 检查项                                                                                                               | 检查要点                                                                    |
|--------|--------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| 安全计算环境 | 入侵防范   | f) 应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警                                                                             | 是否能够检测到对重要节点进行入侵的行为                                                     |
|        |        |                                                                                                                   | 是否能够对发生严重入侵事件时提供报警                                                      |
|        | 恶意代码防范 | 应采用主动免疫可信验证机制及时识别入侵和病毒行为,并将其有效阻断                                                                                  | 是否采用主动免疫可信验证机制                                                          |
|        |        |                                                                                                                   | 是否能及时识别入侵和病毒行为                                                          |
|        |        |                                                                                                                   | 是否具备有效阻断入侵和病毒行为的能力                                                      |
|        | 可信验证   | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证,并在应用程序的所有执行环节进行动态可信验证,在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心,并进行动态关联感知 | 是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和是应用程序等进行可信验证                            |
|        |        |                                                                                                                   | 是否在应用程序的所有执行环节进行动态可信验证                                                  |
|        |        |                                                                                                                   | 是否在检测到应用程序可信根的可信性受到破坏后进行报警                                              |
|        |        |                                                                                                                   | 是否将验证结果形成审计记录,并将审计记录送至安全管理中心,进行动态关联感知                                   |
|        | 数据完整性  | a) 应采用密码技术保证重要数据在传输过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等                                         | 是否采用密码技术保证重要数据在传输过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等 |
|        |        | b) 应采用密码技术保证重要数据在存储过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等                                         | 是否采用密码技术保证重要数据在存储过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等 |
|        |        | c) 在可能涉及法律责任认定的应用中,应采用密码技术提供数据原发证据和数据接收证据,实现数据原发行为的抗抵赖和数据接收行为的抗抵赖                                                 | 在可能涉及法律责任认定的应用中,是否采用密码技术提供数据原发证据和数据接收证据,实现数据原发行为的抗抵赖和数据接收行为的抗抵赖         |
|        | 数据保密性  | a) 应采用密码技术保证重要数据在传输过程中的保密性,包括但不限于鉴别数据、重要业务数据和重要个人信息等                                                              | 是否采用密码技术保证重要数据在传输过程中的保密性,包括但不限于鉴别数据、重要业务数据和重要个人信息等                      |
|        |        | b) 应采用密码技术保证重要数据在存储过程中的保密性,包括但不限于鉴别数据、重要业务数据和重要个人信息等                                                              | 是否采用密码技术保证重要数据在存储过程中的保密性,包括但不限于鉴别数据、重要业务数据和重要个人信息等                      |
|        | 数据备份恢复 | a) 应提供重要数据的本地数据备份与恢复功能                                                                                            | 是否提供重要数据的本地数据备份与恢复功能                                                    |
|        |        | b) 应提供异地实时备份功能,利用通信网络将重要数据实时备份至备份场地                                                                               | 是否提供异地实时备份功能,利用通信网络将重要数据实时备份至备份场地                                       |
|        |        | c) 应提供重要数据处理系统的热冗余,保证系统的高可用性                                                                                      | 是否提供重要数据处理系统的热冗余,保证系统的高可用性                                              |
|        |        | d) 应建立异地灾难备份中心,提供业务应用的实时切换                                                                                        | 是否建立异地灾难备份中心,提供业务是否用的实时切换                                               |

表 C.4 (续)

| 检查范围   | 检查内容   | 检查项                                                                          | 检查要点                                                                                   |
|--------|--------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| 安全计算环境 | 剩余信息保护 | a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除                                             | 是否保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除                                                         |
|        |        | b) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除                                             | 是否保证存有敏感数据的存储空间被释放或重新分配前得到完全清除                                                         |
|        | 个人信息保护 | a) 应仅采集和保存业务必需的用户个人信息                                                        | 是否仅采集和保存业务必需的用户个人信息                                                                    |
|        |        | b) 应禁止未授权访问和非法使用用户个人信息                                                       | 是否禁止未授权访问和非法使用用户个人信息                                                                   |
| 安全管理中心 | 系统管理   | a) 应对系统管理员进行身份鉴别, 只允许其通过特定的命令或操作界面进行系统管理操作, 并对这些操作进行审计                       | 安全管理中心是否对系统管理员进行身份鉴别                                                                   |
|        |        |                                                                              | 安全管理中心是否只允许系统管理员通过特定命令或操作界面进行系统管理操作                                                    |
|        |        |                                                                              | 系统管理员在安全管理中心中的操作是否进行审计                                                                 |
|        |        | b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理, 包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等 | 是否只有系统管理员可以通过安全管理中心对系统的资源和运行进行配置、控制和管理, 包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等操作 |
|        | 审计管理   | a) 应对审计管理员进行身份鉴别, 只允许其通过特定的命令或操作界面进行安全审计操作, 并对这些操作进行审计                       | 安全管理中心是否对审计管理员进行身份鉴别                                                                   |
|        |        |                                                                              | 安全管理中心是否只允许审计管理员通过特定命令或操作界面进行系统管理操作                                                    |
|        |        |                                                                              | 审计管理员在安全管理中心中的操作是否进行审计                                                                 |
|        |        | b) 应通过审计管理员对审计记录应进行分析, 并根据分析结果进行处理, 包括根据安全审计策略对审计记录进行存储、管理和查询等               | 是否只有审计管理员可以通过安全管理中心对审计记录应进行分析, 并根据分析结果进行处理, 包括根据安全审计策略对审计记录进行存储、管理和查询等操作               |
|        | 安全管理   | a) 应对安全管理员进行身份鉴别, 只允许其通过特定的命令或操作界面进行安全管理操作, 并对这些操作进行审计                       | 安全管理中心是否对安全管理员进行身份鉴别                                                                   |
|        |        |                                                                              | 安全管理中心是否只允许安全管理员通过特定命令或操作界面进行系统管理操作                                                    |
|        |        |                                                                              | 安全管理员在安全管理中心中的操作是否进行审计                                                                 |
|        |        | b) 应通过安全管理员对系统中的安全策略进行配置, 包括安全参数的设置, 主体、客体进行统一安全标记, 对主体进行授权, 配置可信验证策略等       | 是否只有安全管理员可以通过安全管理中心对系统中的安全策略进行配置, 包括安全参数的设置, 主体、客体进行统一安全标记, 对主体进行授权, 配置可信验证策略等操作       |
|        | 集中管控   | a) 应划分出特定的管理区域, 对分布在网络中的安全设备或安全组件进行管控                                        | 网络中是否划分出特定的管理区域, 对分布在网络中的安全设备或安全组件进行管控                                                 |
|        |        | b) 应能够建立一条安全的信息传输路径, 对网络中的安全设备或安全组件进行管理                                      | 对网络中的安全设备或安全组件进行管理时, 是否通过具有安全保护的通信方式                                                   |

表 C.4 (续)

| 检查范围   | 检查内容  | 检查项                                                    | 检查要点                                                     |
|--------|-------|--------------------------------------------------------|----------------------------------------------------------|
| 安全管理中心 | 集中管控  | c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测                    | 安全管理中心是否对系统中的网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测              |
|        |       | d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析, 并保证审计记录的留存时间符合法律法规要求    | 是否对分散在各个设备上的审计数据进行收集汇总和集中分析<br>是否审计数据的留存时间符合法律法规要求       |
|        |       | e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理                       | 是否对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理                           |
|        |       | f) 应能对网络中发生的各类安全事件进行识别、报警和分析                           | 是否能对网络中发生的各类安全事件进行识别、报警和分析                               |
|        |       | g) 应保证系统范围内的时间由唯一确定的时钟产生, 以保证各种数据的管理和分析在时间上的一致性        | 系统范围内的时间是否由唯一确定的时钟产生, 以保证各种数据的管理和分析在时间上的一致性              |
| 安全管理制度 | 安全策略  | 应制定网络安全工作的总体方针和安全策略, 阐明机构安全工作的总体目标、范围、原则和安全框架等         | 检查信息安全工作的总体方针和安全策略文件, 查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等    |
|        | 管理制度  | a) 应对安全管理活动中的各类管理内容建立安全管理制度                            | 是否对安全管理活动中的各类管理内容建立安全管理制度                                |
|        |       | b) 应对管理人员或操作人员执行的日常管理操作建立操作规程                          | 是否对管理人员或操作人员执行的日常管理操作建立操作规程                              |
|        |       | c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系              | 机构是否形成全面的信息安全管理制度体系, 制度体系是否由总体方针、安全策略、管理制度、操作规程等构成       |
|        | 制定和发布 | a) 应指定或授权专门的部门或人员负责安全管理制度的制定                           | 是否有专门的部门或人员负责制定安全管理制度                                    |
|        |       | b) 安全管理制度应通过正式、有效的方式发布, 并进行版本控制                        | 安全管理制度制、修订人员, 是否按照统一的格式标准或要求制定                           |
|        | 评审和修订 | 应定期对安全管理制度的合理性和适用性进行论证和审定, 对存在不足或需要改进的安全管理制度进行修订       | 是否定期对安全管理制度的合理性和适用性进行论证和审定, 对存在不足或是否改进的安全管理制度进行修订        |
| 安全管理机构 | 岗位设置  | a) 应成立指导和管理网络安全工作的委员会或领导小组, 其最高领导由单位主管领导担任或授权          | 是否成立指导和管理网络安全工作的委员会或领导小组<br>网络安全工作委员会的最高领导是否由单位主管领导担任或授权 |
|        |       |                                                        | 是否划分网络安全管理职能部门                                           |
|        |       | b) 应设立网络安全管理工作的职能部门, 设立安全主管、安全管理各个方面的负责人岗位, 并定义各负责人的职责 | 是否设立安全主管、安全管理各个方面的负责人岗位, 并定义各负责人的职责                      |
|        |       |                                                        | 是否划分网络安全管理岗位                                             |
|        |       | c) 应设立系统管理员、审计管理员和安全管理员等岗位, 并定义部门及各个工作岗位的职责            | 是否明确部门及各岗位职责                                             |
|        | 人员配备  | a) 应配备一定数量的系统管理员、审计管理员和安全管理员等                          | 是否配备系统管理员、审计管理员和安全管理员<br>是否明确各岗位人员配备情况                   |
|        |       |                                                        |                                                          |

表 C.4 (续)

| 检查范围   | 检查内容  | 检查项                                                             | 检查要点                                                        |
|--------|-------|-----------------------------------------------------------------|-------------------------------------------------------------|
| 安全管理机构 | 人员配备  | b) 应配备专职安全管理员, 不可兼任                                             | 是否配备专职安全管理员                                                 |
|        |       | c) 关键事务岗位应配备多人共同管理                                              | 关键事务岗位是否配备多人共同管理                                            |
|        | 授权和审批 | a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等                              | 是否明确各部门和岗位的职责和授权范围                                          |
|        |       |                                                                 | 是否明确针对审批事项、审批部门和批准人等内容与相关制度一致                               |
|        |       | b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序, 按照审批程序执行审批过程, 对重要活动建立逐级审批制度 | 系统变更、重要操作、物理访问和系统接入等事项是否明确建立逐级审批程序                          |
|        |       | c) 应定期审查审批事项, 及时更新需授权和审批的项目、审批部门和审批人等信息                         | 审批记录、操作记录是否与相关制度一致                                          |
|        | 沟通和合作 | a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通, 定期召开协调会议, 共同协作处理网络安全问题    | 是否对各类审批事项进行更新                                               |
|        |       | b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通                           | 是否加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通, 定期召开协调会议, 共同协作处理网络安全问题  |
|        |       |                                                                 | 是否建立与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通机制                       |
|        |       | c) 应建立外联单位联系列表, 包括外联单位名称、合作内容、联系人和联系方式等信息                       | 是否与网络安全职能部门、各类供应商、业界专家及安全组织开展合作与沟通                          |
|        | 审核和检查 | a) 应定期进行常规安全检查, 检查内容包括系统日常运行、系统漏洞和数据备份等情况                       | 是否建立外联单位联系列表                                                |
|        |       | b) 应定期进行全面安全检查, 检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等   | 是否定期进行常规安全检查, 检查内容包括系统日常运行、系统漏洞和数据备份等情况                     |
|        |       | c) 应制定安全检查表格实施安全检查, 汇总安全检查数据, 形成安全检查报告, 并对安全检查结果进行通报            | 是否定期进行全面安全检查, 检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等 |
| 安全管理人员 | 人员录用  | a) 应指定或授权专门的部门或人员负责人员录用                                         | 是否制定安全检查表格实施安全检查                                            |
|        |       | b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查, 对其所具有的技术技能进行考核                 | 是否由专门的部门或人员负责人员的录用工作                                        |
|        |       |                                                                 | 是否对被录用人员的身份、安全背景、专业资格或资质等进行审查                               |
|        |       | c) 应与被录用人员签署保密协议, 与关键岗位人员签署岗位责任协议                               | 是否对被录用人员所具有的技术技能进行考核                                        |
|        |       |                                                                 | 是否与被录用人员签署保密协议                                              |
|        |       |                                                                 | 是否与关键岗位人员签署岗位责任协议                                           |

表 C.4 (续)

| 检查范围       | 检查内容      | 检查项                                                | 检查要点                                           |
|------------|-----------|----------------------------------------------------|------------------------------------------------|
| 安全管理<br>人员 | 人员录用      | d) 应从内部人员中选拔从事关键岗位的人员                              | 是否从内部人员中选拔从事关键岗位的人员                            |
|            | 人员离岗      | a) 应及时终止离岗人员的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备   | 是否及时终止离岗人员的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备 |
|            |           | b) 应办理严格的调离手续, 并承诺调离后的保密义务后方可离开                    | 管理文档中是否规定人员调离手续和离岗要求等                          |
|            |           |                                                    | 是否具有按照离岗程序办理调离手续的记录                            |
|            | 安全意识教育和培训 | a) 应对各类人员进行安全意识教育和岗位技能培训, 并告知相关的安全责任和惩戒措施          | 是否建立相关制度对各类人员进行安全意识教育和岗位技能培训                   |
|            |           |                                                    | 是否告知相关的安全责任和惩戒措施                               |
|            |           | b) 应针对不同岗位制定不同的培训计划, 对安全基础知识、岗位操作规程等进行培训           | 是否建立相关制度针对不同岗位制定不同的培训计划, 包括安全基础知识、岗位操作规程等内容    |
|            |           | c) 应定期对不同岗位的人员进行技术技能考核                             | 是否定期对不同岗位的人员进行技术技能考核                           |
|            | 外部人员访问管理  | a) 应在外部人员物理访问受控区域前提出书面申请, 批准后由专人全程陪同, 并登记备案        | 是否建立相关制度明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等 |
|            |           |                                                    | 外部人员物理访问受控区域前是否先提出书面申请                         |
|            |           |                                                    | 是否由专人全程陪同, 并登记备案                               |
|            |           | b) 应在外部人员接入受控网络访问系统前提出书面申请, 批准后由专人开设账户、分配权限, 并登记备案 | 是否建立相关制度明确外部人员接入网络前的申请审批流程                     |
|            |           |                                                    | 外部人员接入受控网络访问系统前是否先提出书面申请                       |
|            |           |                                                    | 是否由专人开设账户、分配权限, 并登记备案                          |
|            |           | c) 外部人员离场后应及时清除其所有的访问权限                            | 外部人员离场后是否及时清除其所有的访问权限                          |
|            |           | d) 获得系统访问授权的外部人员应签署保密协议, 不得进行非授权操作, 不得复制和泄露任何敏感信息  | 获得系统访问授权的外部人员是否签署了保密协议                         |
|            |           | e) 对关键区域或关键系统不允许外部人员访问                             | 是否建立相关制度明确外部人员不允许访问关键区域或关键系统                   |
| 安全建设<br>管理 | 定级和备案     | a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由                 | 是否有书面材料说明保护对象的安全保护等级及确定等级的方法和理由                |
|            |           | b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定            | 是否组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定          |

表 C.4 (续)

| 检查范围   | 检查内容    | 检查项                                                                     | 检查要点                                                                 |
|--------|---------|-------------------------------------------------------------------------|----------------------------------------------------------------------|
| 安全建设管理 | 定级和备案   | c) 应保证定级结果经过相关部门的批准                                                     | 定级结果是否经过相关部门的批准                                                      |
|        |         | d) 应将备案材料报主管部门和相应公安机关备案                                                 | 备案材料是否报主管部门和相应公安机关备案                                                 |
|        | 安全方案设计  | a) 应根据安全保护等级选择基本安全措施, 依据风险分析的结果补充和调整安全措施                                | 是否根据安全保护等级选择基本安全措施, 依据风险分析的结果补充和调整安全措施                               |
|        |         | b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计, 设计内容应包含密码技术相关内容, 并形成配套文件 | 是否根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计, 设计内容是否包含密码相关内容, 并形成配套文件 |
|        |         | c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定, 经过批准后才能正式实施              | 是否组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定                          |
|        |         |                                                                         | 安全整体规划及配套文件是否经过批准                                                    |
|        | 产品采购和使用 | a) 应确保网络安全产品采购和使用符合国家的有关规定                                              | 网络安全产品采购是否符合国家的有关规定                                                  |
|        |         |                                                                         | 网络安全产品使用是否符合国家的有关规定                                                  |
|        |         | b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求                                      | 密码产品与服务的采购是否符合国家密码管理主管部门的要求                                          |
|        |         |                                                                         | 密码产品与服务的使用是否符合国家密码管理主管部门的要求                                          |
|        |         | c) 应预先对产品进行选型测试, 确定产品的候选范围, 并定期审定和更新候选产品名单                              | 是否预先对产品进行选型测试, 确定产品的候选范围                                             |
|        |         |                                                                         | 是否定期审定和更新候选产品名单                                                      |
|        |         | d) 应对重要部位的产品委托专业测评单位进行专项测试, 根据测试结果选用产品                                  | 是否对重要部位的产品委托专业测评单位进行专项测试, 根据测试结果选用产品                                 |
|        | 自行软件开发  | a) 应将开发环境与实际运行环境物理分开, 测试数据和测试结果受到控制                                     | 是否将开发环境与实际运行环境物理分开, 测试数据和测试结果受到控制                                    |
|        |         | b) 应制定软件开发管理制度, 明确说明开发过程的控制方法和人员行为准则                                    | 是否制定软件开发管理制度, 明确说明开发过程的控制方法和人员行为准则                                   |
|        |         | c) 应制定代码编写安全规范, 要求开发人员参照规范编写代码                                          | 是否制定代码编写安全规范, 要求开发人员参照规范编写代码                                         |
|        |         | d) 应具备软件设计的相关文档和使用指南, 并对文档使用进行控制                                        | 是否具备软件设计的相关文档和使用指南, 并对文档使用进行控制                                       |
|        |         | e) 应在软件开发过程中对安全性进行测试, 在软件安装前对可能存在的恶意代码进行检测                              | 是否在软件开发过程中对安全性进行测试                                                   |
|        |         |                                                                         | 是否在软件安装前进行恶意代码检测                                                     |
|        |         | f) 应对程序资源库的修改、更新、发布进行授权和批准, 并严格进行版本控制                                   | 是否对程序资源库的修改、更新、发布进行授权和批准, 并严格进行版本控制                                  |
|        |         | g) 应保证开发人员为专职人员, 开发人员的开发活动受到控制、监视和审查                                    | 开发人员是否为专职人员                                                          |
|        |         |                                                                         | 开发人员的开发活动是否受到控制、监视和审查                                                |

表 C.4 (续)

| 检查范围   | 检查内容    | 检查项                                                            | 检查要点                                       |
|--------|---------|----------------------------------------------------------------|--------------------------------------------|
| 安全建设管理 | 外包软件开发  | a) 应在软件交付前检测其中可能存在的恶意代码                                        | 开发单位是否在软件交付前进行了恶意代码检测                      |
|        |         | b) 应保证开发单位提供软件设计文档和使用指南                                        | 开发单位是否提供软件设计文档和使用指南?                       |
|        |         | c) 应保证开发单位提供软件源代码, 并审查软件中可能存在的后门和隐蔽信道                          | 开发单位是否提供软件源代码                              |
|        |         |                                                                | 是否审查了软件中可能存在的后门和隐蔽信道                       |
|        | 工程实施    | a) 应指定或授权专门的部门或人员负责工程实施过程的管理                                   | 是否指定或授权专门的部门或人员负责工程实施过程的管理                 |
|        |         | b) 应制定安全工程实施方案控制工程实施过程                                         | 是否制定安全工程实施方案                               |
|        |         |                                                                | 是否按照安全工程实施方案进行工程实施                         |
|        |         | c) 应通过第三方工程监理控制项目的实施过程                                         | 是否通过第三方工程监理控制项目的实施过程                       |
|        | 测试验收    | a) 应制订测试验收方案, 并依据测试验收方案实施测试验收, 形成测试验收报告                        | 是否制订测试验收方案                                 |
|        |         |                                                                | 是否依据测试验收方案实施测试验收, 形成测试验收报告                 |
|        |         | b) 应进行上线前的安全性测试, 并出具安全测试报告, 安全测试报告应包含密码应用安全性测试相关内容             | 是否进行上线前的安全性测试验收                            |
|        |         |                                                                | 安全测试报告是否包含密码应用安全性测试相关内容                    |
|        | 系统交付    | a) 应制定交付清单, 并根据交付清单对所交接的设备、软件和文档等进行清点                          | 是否根据交付清单对所交接的设备、软件和文档等进行清点                 |
|        |         | b) 应对负责运行维护的技术人员进行相应的技能培训                                      | 是否对负责运行维护的技术人员进行相应的技能培训                    |
|        |         | c) 应提供建设过程文档和运行维护文档                                            | 是否提供建设过程文档和运行维护文档                          |
|        | 等级测评    | a) 应定期进行等级测评, 发现不符合相应等级保护标准要求的及时整改                             | 是否定期进行等级测评                                 |
|        |         |                                                                | 是否对不符合项进行了及时整改                             |
|        |         | b) 应在发生重大变更或级别发生变化时进行等级测评                                      | 在重大变更或级别发生变化时是否进行等级测评                      |
|        |         | c) 应确保测评机构的选择符合国家有关规定                                          | 测评机构是否符合国家有关规定                             |
|        | 服务供应商选择 | a) 应确保服务供应商的选择符合国家的有关规定                                        | 服务供应商是否符合国家的有关规定                           |
|        |         | b) 应与选定的服务供应商签订相关协议, 明确整个服务供应链各方需履行的网络安全相关义务                   | 是否与选定的服务供应商签订相关协议, 明确整个服务供应链各方需履行的网络安全相关义务 |
|        |         | c) 应定期监督、评审和审核服务供应商提供的服务, 并对其变更服务内容加以控制                        | 是否定期监督、评审和审核服务供应商提供的服务                     |
|        |         |                                                                | 是否对服务供应商变更服务内容加以控制                         |
| 安全运维管理 | 环境管理    | a) 应指定专门的部门或人员负责机房安全, 对机房出入进行管理, 定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理 | 是否指定专门的部门或人员负责机房安全                         |
|        |         |                                                                | 指定的部门或人员是否对机房出入进行管理                        |
|        |         |                                                                | 是否定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理            |

表 C.4 (续)

| 检查范围   | 检查内容   | 检查项                                                                   | 检查要点                                                      |
|--------|--------|-----------------------------------------------------------------------|-----------------------------------------------------------|
| 安全运维管理 | 环境管理   | b) 应建立机房安全管理制度, 对有关物理访问、物品进出和环境安全等方面的管理作出规定                           | 是否建立机房安全管理制度, 对有关物理访问、物品进出和环境安全等方面的管理作出规定                 |
|        |        | c) 应不在重要区域接待来访人员, 不随意放置含有敏感信息的纸档文件和移动介质等                              | 是否避免了在重要区域接待来访人员<br>是否避免了桌面等开放或者明显位置上包含敏感信息的纸档文件、移动介质等    |
|        |        | d) 应对出入人员进行相应级别的授权, 对进入重要安全区域的人员和活动实时监控等                              | 是否对出入人员进行相应级别的授权                                          |
|        |        |                                                                       | 是否对进入重要安全区域的人员和活动实时监控                                     |
|        | 资产管理   | a) 应编制并保存与保护对象相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容                          | 是否编制并保存了与保护对象相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容               |
|        |        | b) 应根据资产的重要程度对资产进行标识管理, 根据资产的价值选择相应的管理措施                              | 是否根据资产的重要程度对资产进行标识管理                                      |
|        |        |                                                                       | 是否根据资产的价值选择相应的管理措施                                        |
|        |        | c) 应对信息分类与标识方法作出规定, 并对信息的使用、传输和存储等进行规范化管理                             | 是否对信息分类与标识方法作出规定                                          |
|        |        |                                                                       | 是否对信息的使用、传输和存储等进行规范化管理                                    |
|        | 介质管理   | a) 应将介质存放在安全的环境中, 对各类介质进行控制和保护, 实行存储环境专人管理, 并根据存档介质的目录清单定期盘点          | 是否将介质存放在安全的环境中, 各类介质进行控制和保护                               |
|        |        |                                                                       | 是否实行存储环境专人管理                                              |
|        |        |                                                                       | 是否根据存档介质的目录清单定期盘点                                         |
|        |        | b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制, 并对介质的归档和查询等进行登记记录                  | 是否对介质在物理传输过程中的人员选择、打包、交付等情况进行控制<br>是否对介质的归档和查询等进行登记记录     |
|        | 设备维护管理 | a) 应对各种设备 (包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理                           | 是否指定专门的部门或人员定期进行维护管理                                      |
|        |        | b) 应建立配套设施、软硬件维护方面的管理制度, 对其维护进行有效的管理, 包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等 | 是否对配套设施、软硬件维护管理做出规定                                       |
|        |        |                                                                       | 是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等                           |
|        |        | c) 信息处理设备应经过审批才能带离机房或办公地点, 含有存储介质的设备带出工作环境时其中重要数据应加密                  | 信息处理设备带离机房或办公地点前是否经过审批                                    |
|        |        |                                                                       | 含有存储介质的设备带出工作环境时其中重要数据是否加密                                |
|        |        | d) 含有存储介质的设备在报废或重用前, 应进行完全清除或被安全覆盖, 保证该设备上的敏感数据和授权软件无法被恢复重用           | 含有存储介质的设备在报废或重用前, 是否进行完全清除或被安全覆盖, 保证该设备上的敏感数据和授权软件无法被恢复重用 |



表 C.4 (续)

| 检查范围   | 检查内容      | 检查项                                                                       | 检查要点                                                   |
|--------|-----------|---------------------------------------------------------------------------|--------------------------------------------------------|
| 安全运维管理 | 漏洞和风险管理   | a) 应采取必要的措施识别安全漏洞和隐患,对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补                       | 是否采取必要的措施识别安全漏洞和隐患<br>对发现的安全漏洞和隐患是否及时进行修补或评估可能的影响后进行修补 |
|        |           | b) 应定期开展安全测评,形成安全测评报告,采取措施应对发现的安全问题                                       | 是否定期开展安全测评                                             |
|        |           |                                                                           | 是否形成安全测评报告                                             |
|        |           |                                                                           | 是否采取措施应对发现的安全问题                                        |
|        | 网络和系统安全管理 | a) 应划分不同的管理员角色进行网络和系统的运维管理,明确各个角色的责任和权限                                   | 是否划分了不同的管理员角色进行网络和系统的运维管理,明确各个角色的责任和权限                 |
|        |           | b) 应指定专门的部门或人员进行账户管理,对申请账户、建立账户、删除账户等进行控制                                 | 是否指定专门的部门或人员进行账户管理                                     |
|        |           |                                                                           | 是否对申请账户、建立账户、删除账户等进行控制                                 |
|        |           | c) 应建立网络和系统安全管理制度,对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定          | 是否对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定       |
|        |           | d) 应制定重要设备的配置和操作手册,依据手册对设备进行安全配置和优化配置等                                    | 是否制定重要设备的配置和操作手册                                       |
|        |           |                                                                           | 是否依据手册对设备进行安全配置和优化配置等                                  |
|        |           | e) 应详细记录运维操作日志,包括日常巡检工作、运行维护记录、参数的设置和修改等内容                                | 是否详细记录运维操作日志,包括日常巡检工作、运行维护记录、参数的设置和修改等内容               |
|        |           | f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计,及时发现可疑行为                                | 是否指定专门的部门或人员对日志、监测和报警数据等进行分析、统计,及时发现可疑行为               |
|        |           | g) 应严格控制变更性运维,经过审批后才可改变连接、安装系统组件或调整配置参数,操作过程中应保留不可更改的审计日志,操作结束后应同步更新配置信息库 | 是否严格控制变更性运维,经过审批后才可改变连接、安装系统组件或调整配置参数                  |
|        |           |                                                                           | 操作过程中是否保留不可更改的审计日志                                     |
|        |           |                                                                           | 操作结束后是否同步更新配置信息库                                       |
|        |           | h) 应严格控制运维工具的使用,经过审批后才可接入进行操作,操作过程中应保留不可更改的审计日志,操作结束后应删除工具中的敏感数据          | 是否严格控制运维工具的使用,经过审批后才可接入进行操作                            |
|        |           |                                                                           | 操作过程中是否保留不可更改的审计日志                                     |
|        |           |                                                                           | 操作结束后是否删除工具中的敏感数据                                      |
|        |           | i) 应严格控制远程运维的开通,经过审批后才可开通远程运维接口或通道,操作过程中应保留不可更改的审计日志,操作结束后应立即关闭接口或通道      | 是否严格控制远程运维的开通,经过审批后才可开通远程运维接口或通道                       |
|        |           |                                                                           | 操作过程中是否保留不可更改的审计日志                                     |
|        |           |                                                                           | 操作结束后是否立即关闭接口或通道                                       |
|        |           | j) 应保证所有与外部的连接均得到授权和批准,应定期检查违反规定无线上网及其他违反网络安全策略的行为                        | 是否保证所有与外部的连接均得到授权和批准                                   |
|        |           |                                                                           | 是否定期检查违反规定无线上网及其他违反网络安全策略的行为                           |

表 C.4 (续)

| 检查范围   | 检查内容     | 检查项                                                                   | 检查要点                                                                           |
|--------|----------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 安全运维管理 | 恶意代码防范管理 | a) 应提高所有用户的防恶意代码意识, 对外来计算机或存储设备接入系统前进行恶意代码检查等                         | 是否有相关措施提高所有用户的防恶意代码意识<br>是否对外来计算机或存储设备接入系统前进行恶意代码检查等                           |
|        |          | b) 应定期验证防范恶意代码攻击的技术措施的有效性                                             | 是否定期验证防范恶意代码攻击的技术措施的有效性                                                        |
|        | 配置管理     | a) 应记录和保存基本配置信息, 包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等    | 基本配置信息是否包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等                      |
|        |          | b) 应将基本配置信息改变纳入系统变更范畴, 实施对配置信息改变的控制, 并及时更新基本配置信息库                     | 是否将基本配置信息改变纳入系统变更范畴                                                            |
|        |          |                                                                       | 是否及时更新基本配置信息库                                                                  |
|        | 密码管理     | a) 应遵循密码相关的国家标准和行业标准                                                  | 是否遵循密码相关国家标准和行业标准                                                              |
|        |          | b) 应使用国家密码管理主管部门认证核准的密码技术和产品                                          | 是否使用国家密码管理主管部门认证核准的密码技术和产品                                                     |
|        |          | c) 应采用硬件密码模块实现密码运算和密钥管理                                               | 是否采用硬件密码模块实现密码运算和密钥管理                                                          |
|        | 变更管理     | a) 应明确变更需求, 变更前根据变更需求制定变更方案, 变更方案经过评审、审批后方可实施                         | 变更前是否明确变更需求<br>变更前是否根据变更需求制定变更方案<br>变更方案是否经过评审                                 |
|        |          |                                                                       |                                                                                |
|        |          |                                                                       |                                                                                |
|        |          | b) 应建立变更的申报和审批控制程序, 依据程序控制所有的变更, 记录变更实施过程                             | 是否建立了变更的申报和审批控制程序<br>是否依据程序控制所有的变更<br>是否记录变更实施过程                               |
|        |          |                                                                       |                                                                                |
|        |          | c) 应建立中止变更并从失败变更中恢复的程序, 明确过程控制方法和人员职责, 必要时对恢复过程进行演练                   | 是否建立中止变更并从失败变更中恢复的程序, 以明确过程控制方法和人员职责<br>是否规定了在必要时对恢复过程进行演练                     |
|        |          |                                                                       |                                                                                |
|        | 备份与恢复管理  | a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等                                        | 是否识别需要定期备份的重要业务信息、系统数据及软件系统等                                                   |
|        |          | b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等                                        | 是否规定备份信息的备份方式、备份频度、存储介质、保存期等                                                   |
|        |          | c) 应根据数据的重要性和数据对系统运行的影响, 制定数据的备份策略和恢复策略、备份程序和恢复程序等                    | 是否根据数据的重要性和数据对系统运行的影响, 制定数据的备份策略和备份程序<br>是否根据数据的重要性和数据对系统运行的影响, 制定数据的恢复策略和恢复程序 |
|        |          |                                                                       |                                                                                |
|        | 安全事件处置   | a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件                                          | 是否及时向安全管理部门报告所发现的安全弱点和可疑事件                                                     |
|        |          | b) 应制定安全事件报告和处置管理制度, 明确不同安全事件的报告、处置和响应流程, 规定安全事件的现场处理、事件报告和后期恢复的管理职责等 | 是否制定了安全事件报告和处置管理制度, 明确不同安全事件的报告、处置和响应流程, 规定安全事件的现场处理、事件报告和后期恢复的管理职责等           |

表 C.4 (续)

| 检查范围   | 检查内容   | 检查项                                                                      | 检查要点                                              |
|--------|--------|--------------------------------------------------------------------------|---------------------------------------------------|
| 安全运维管理 | 安全事件处置 | c) 应在安全事件报告和响应处理过程中,分析和鉴定事件产生的原因,收集证据,记录处理过程,总结经验教训                      | 是否在安全事件报告和响应处理过程中,分析和鉴定事件产生的原因,收集证据,记录处理过程,总结经验教训 |
|        |        | d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序                                  | 对造成系统中断和造成信息泄漏的重大安全事件是否采用不同的处理程序和报告程序             |
|        |        | e) 应建立联合防护和应急机制,负责处置跨单位安全事件                                              | 是否建立联合防护和应急机制,负责处置跨单位安全事件                         |
|        | 应急预案管理 | a) 应规定统一的应急预案框架,包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容                       | 是否规定统一的应急预案框架包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容   |
|        |        | b) 应制定重要事件的应急预案,包括应急处理流程、系统恢复流程等内容                                       | 是否制定重要事件的应急预案,包括应急处理流程、系统恢复流程等内容                  |
|        |        | c) 应定期对系统相关的人员进行应急预案培训,并进行应急预案的演练                                        | 是否定期对系统相关的人员进行应急预案培训                              |
|        |        |                                                                          | 是否进行应急预案的演练                                       |
|        |        | d) 应定期对原有的应急预案重新评估,修订完善                                                  | 是否定期对原有的应急预案重新评估,修订完善                             |
|        |        | e) 应建立重大安全事件的跨单位联合应急预案,并进行应急预案的演练                                        | 是否建立重大安全事件的跨单位联合应急预案                              |
|        |        |                                                                          | 是否针对重大安全事件跨单位联合应急预案进行演练                           |
|        | 外包运维管理 | a) 应确保外包运维服务商的选择符合国家的有关规定                                                | 是否能确保外包运维服务商的选择符合国家的有关规定                          |
|        |        | b) 应与选定的外包运维服务商签订相关的协议,明确约定外包运维的范围、工作内容                                  | 是否与选定的外包运维服务商签订相关的协议,明确约定外包运维的范围、工作内容             |
|        |        | c) 应保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力,并将能力要求在签订的协议中明确           | 是否能保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力     |
|        |        |                                                                          | 是否将能力要求在签订的协议中明确                                  |
|        |        | d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求,如可能涉及对敏感信息的访问、处理、存储要求,对IT基础设施中断服务的应急保障要求等 | 是否在与外包运维服务商签订的协议中明确所有相关的安全要求                      |

## 附录 D

(规范性附录)

## 政府网站安全检查指标

## D.1 政府网站安全检查指标

政府网站安全检查内容如表D.1所示。

表D.1 政府网站安全检查内容

| 检查范围        | 检查内容         | 检查项                  | 检查要点                                 |
|-------------|--------------|----------------------|--------------------------------------|
| 网络安全责任制落实情况 | 网站责任制落实情况    | 主要领导对政府网站网络安全工作的重视情况 | 是否将政府网站网络安全工作的执行情况纳入到年度考核指标          |
|             |              |                      | 开展政府网站网络安全工作的经费是否纳入年度预算              |
|             |              | 网络安全责任追究制度执行情况       | 是否对所有的网络安全事故/事件有详细记录                 |
|             |              |                      | 是否按照网络安全责任追究制度进行处理                   |
|             | 网站网络安全工作保障情况 | 关键岗位人员配备情况           | 是否有安全管理员，并签订保密协议                     |
|             |              |                      | 是否有内容管理员，并签订保密协议                     |
|             |              |                      | 是否有网络管理员，并签订保密协议                     |
|             |              |                      | 是否有系统管理员，并签订保密协议                     |
|             |              |                      | 是否有安全审计员，并签订保密协议                     |
|             |              | 政府网站系统定级指导执行情况       | 政府网站是否完成等级保护定级备案工作                   |
|             |              |                      | 是否有定级指导的专家名单和联系方式                    |
|             |              |                      | 是否有同级公安机关等级保护工作办公室的联系人和联系方式          |
|             |              | 等级测评情况               | 是否从《全国网络安全等级保护测评机构推荐目录》中选择测评机构开展等级测评 |
|             |              |                      | 是否对政府网站系统定期进行安全测评                    |
|             |              | 政府网站系统建设管理执行情况       | 政府网站的产品采购、服务外包是否按照相关管理制度执行，并有相关记录    |
|             |              |                      | 政府网站的工程实施、验收交付等建设是否按照相关管理制度执行，并有相关记录 |
|             |              |                      | 是否委托第三方测试单位对网站系统进行安全性测试验收，并出具安全性测试报告 |

表 D.1 (续)

| 检查范围       | 检查内容   | 检查项              | 检查要点                              |
|------------|--------|------------------|-----------------------------------|
| 安全管理措施落实情况 | 网站监测情况 | 安全事件报告处置         | 是否制定事件报告和处置制度                     |
|            |        |                  | 是否制定事件通报流程                        |
|            |        |                  | 是否有完整事件处置记录                       |
|            |        | 开展日常网络安全监测和预警情况  | 本单位日常网络安全监测是否按照机制执行，并有网络安全监测记录    |
|            |        |                  | 本单位日常网络安全预警是否按照机制执行，并有网络安全预警和处理记录 |
|            |        | 应急预案的制定、演练和完善情况  | 是否有应急预案，并有相应的预案文档                 |
|            |        |                  | 是否有应急保障队伍，并有人员名单和联系方式             |
|            |        |                  | 是否定期应急演练，并有应急演练的文档记录              |
|            |        |                  | 是否根据演练结果对应急预案进行完善，并有应急预案的修订记录     |
|            | 网站管理情况 | 网站内容管理           | 是否制定内容发布管理制度                      |
|            |        |                  | 是否制定内容发布流程                        |
|            |        |                  | 是否制定网站信息分类分级标准或制度                 |
|            |        |                  | 是否制定内容及完整性监控制度                    |
|            |        | 网站用户个人信息保护管理     | 是否制定用户个人信息保护制度                    |
|            |        |                  | 是否制定用户个人信息保护策略维护记录                |
|            |        | 机房安全管理制度执行情况     | 本单位机房进出人员管理是否按照制度执行，并有详细记录        |
|            |        |                  | 本单位机房日常监控是否按照制度执行，并有监控记录          |
|            |        | 网络安全安全检查工作组织部署情况 | 是否有政府网站系统网络安全自查工作总结报告             |
|            |        | 存在问题的整改工作情况      | 是否根据公安机关通报的整改意见进行整改，并及时反馈         |
|            | 网站边界情况 | 互联网接入链路          | 是否有互联网接入链路                        |
|            |        | 网络边界所部署的安全防护设备   | 是否部署防火墙                           |
|            |        |                  | 是否部署入侵检测（防护）设备                    |
|            |        |                  | 是否部署防病毒网关                         |
|            |        |                  | 是否部署抗拒服务攻击设备                      |
|            |        |                  | 是否部署其他设备                          |

表 D.1 (续)

| 检查范围       | 检查内容       | 检查项         | 检查要点              |
|------------|------------|-------------|-------------------|
| 安全管理措施落实情况 | 网站内容安全防护措施 | 网页防篡改       | 是否采用网页防篡改措施       |
|            |            | 漏洞扫描措施及补丁升级 | 是否定期进行漏洞扫描        |
|            |            |             | 是否进行过漏洞扫描         |
|            |            |             | 网站是否不存在网站木马       |
|            |            |             | 网站是否不存在网站暗链       |
|            |            |             | 网站是否不存在页面篡改       |
|            |            |             | 网站是否不存在 SQL 注入漏洞  |
|            |            |             | 网站是否不存在后台管理地址泄露漏洞 |
|            |            |             | 网站是否不存在攻击痕迹       |
|            |            |             | 网站是否不存在跨站脚本       |
|            |            |             | 网站是否不存在文件包含       |
|            |            |             | 网站是否不存在目录遍历       |
|            |            |             | 网站是否不存在危险端口       |
|            |            |             | 网站是否不存在信息泄露       |
|            |            |             | 网站是否不存在中间件漏洞      |
|            |            |             | 网站是否不存在第三方插件漏洞    |
|            |            |             | 网站是否不存在文件上传漏洞     |
|            |            |             | 网站是否不存在配置文件漏洞     |
|            |            |             | 网站是否不存在其他漏洞       |
|            |            |             | 发现的漏洞是否及时升级补丁     |
|            |            | 恶意代码防护      | 是否有网页挂马检测系统       |
|            |            | 内容安全防护措施    | 内容编辑、审核及发布权限是否分离  |
|            |            |             | 关键信息发布是否多级审核      |
|            |            |             | 网站发布内容是否过滤        |

表 D.1 （续）

| 检查范围       | 检查内容       | 检查项          | 检查要点                    |
|------------|------------|--------------|-------------------------|
| 安全管理措施落实情况 | 网站内容安全防护措施 | 管理终端安全防护措施   | 是否有控制措施（如地址绑定，网络接入控制等）  |
|            |            | 主要设备可用性      | 网站服务器和数据库服务器是否双机热备      |
|            |            |              | 网站服务器和数据库服务器是否采用冷备方式    |
|            |            | 网站前、后台系统隔离情况 | 是否采用逻辑隔离                |
|            |            |              | 是否采用物理隔离                |
|            |            | 应用远程管理       | 是否不允许远程管理政府网站的应用        |
|            |            |              | 应用远程管理时是否采用加密通道         |
|            |            | 内容远程维护       | 是否不允许远程维护政府网站内容         |
|            |            |              | 政府网站内容远程维护时是否采用加密通道     |
|            |            | 政府网站系统运维管理   | 是否对系统设备的运行状态进行集中管理和监控   |
|            |            |              | 是否对信息系统的网络流量进行集中管理和监控   |
|            |            |              | 是否对系统设备的用户行为进行集中管理和监控   |
|            |            |              | 是否对信息系统的恶意代码防范进行集中管理和监控 |
|            |            |              | 是否对信息系统的补丁升级进行集中管理和监控   |
|            |            |              | 是否对信息系统的安全审计进行集中管理和监控   |
|            |            |              | 是否对监测和报警记录进行分析          |

## D.2 政府网站漏洞情况检查内容

可以通过采用工具扫描与人工验证相结合的方法对政府网站进行检查，自动生成检查报告，检查报告内容应包括漏洞数量统计（按照威胁级别高、中、低进行统计），漏洞类型（网站木马、网站暗链、页面篡改、SQL注入、后台管理、攻击痕迹、跨站脚本、文件包含、目录遍历、危险端口、信息泄露、中间件、三方插件、文件上传、配置文件、其他漏洞）统计，并且漏洞验证地址应准确无误，网站存在的问题描述应清晰、准确。

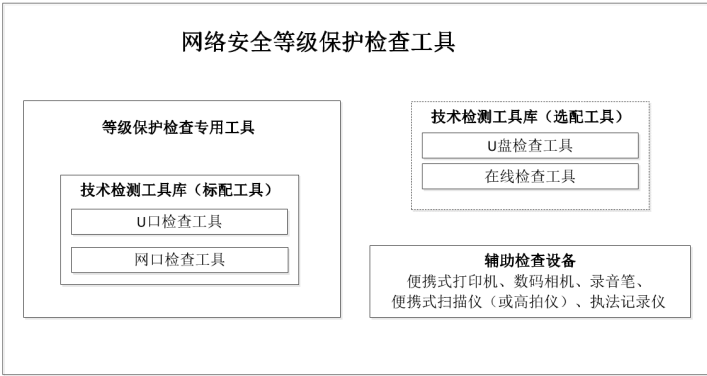
附录 E  
(规范性附录)

网络安全等级保护检查工具总体架构

E.1 检查工具的总体架构

网络安全等级保护检查工具由三部分组成：网络安全等级保护检查专用工具（以下简称为“等级保护检查专用工具”）、辅助检查设备和防护箱。其中，等级保护检查专用工具集成了网络安全等级保护检查工具管理系统（以下简称为“工具管理系统”）、技术检测工具库；辅助检查设备包括便携式打印机、数码相机、录音笔、便携式扫描仪和执法记录仪等设备；防护箱用于容纳所有的硬件设备。

检查工具总体架构示意图如图E. 1所示。



图E. 1 检查工具总体架构示意图

在图E. 1中，检查工具架构的各个功能如下：

- a) 等级保护检查专用工具：等级保护检查专用工具集成了工具管理系统和专用检查工具，以便检查人员在现场进行检查和记录。等级保护检查专用工具经过安全加固处理，安全加固要求详见本文的第8. 1。等级保护检查专用工具的硬件规格参数参见附录H中H. 1。技术检测工具库包括标配工具和选配工具。标配工具是集成在等级保护检查专用工具中的专项技术检查工具，包括U口检查工具和网口检查工具。选配工具为各地公安机关根据检查工作的需要而选配的检查工具；
- b) 辅助检查设备：辅助检查设备用于网络安全检查工作中的辅助管理工作，包括便携式打印机、数码相机、录音笔、便携式扫描仪、执法记录仪、打印纸、刻录光盘等。辅助检查设备的硬件规格要求参见附录H. 2。

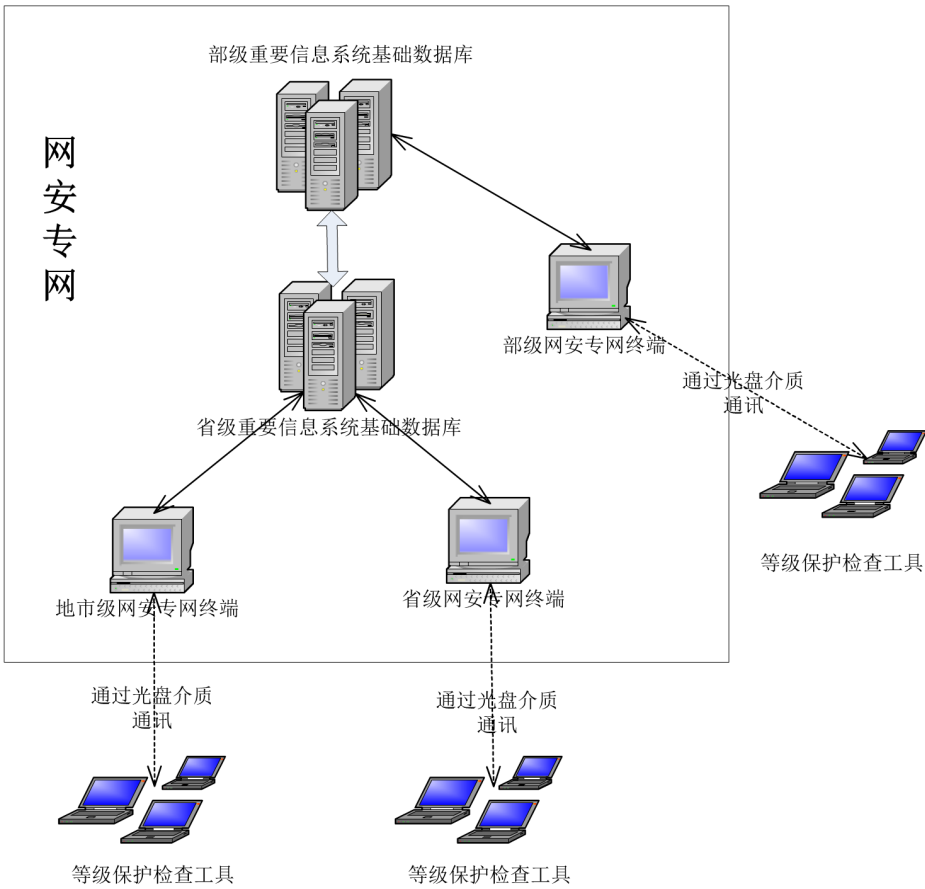
E.2 检查工具与重要信息系统基础数据库管理系统的关系

网络安全等级保护检查工具是公安机关开展网络安全检查工作的信息化工具，获取的检查数据可通过网安专网终端导入到重要信息系统基础数据库管理系统。

重要信息系统基础数据库管理系统是以网安专网为依托，部、省两级建设部署，采用专用终端访问，最终实现部省两级联网，部省市三级应用。有关数据格式应符合网安综合应用平台和网安业务专网的标准，最终可接入网安综合应用平台数据中心。

具体架构如图E. 2所示。





图E. 2 检查工具和重要信息系统基础数据库管理系统的关系示意图

## 附录 F

### （规范性附录）

#### 安全检查工作流程概述

##### F.1 安全检查工作流程

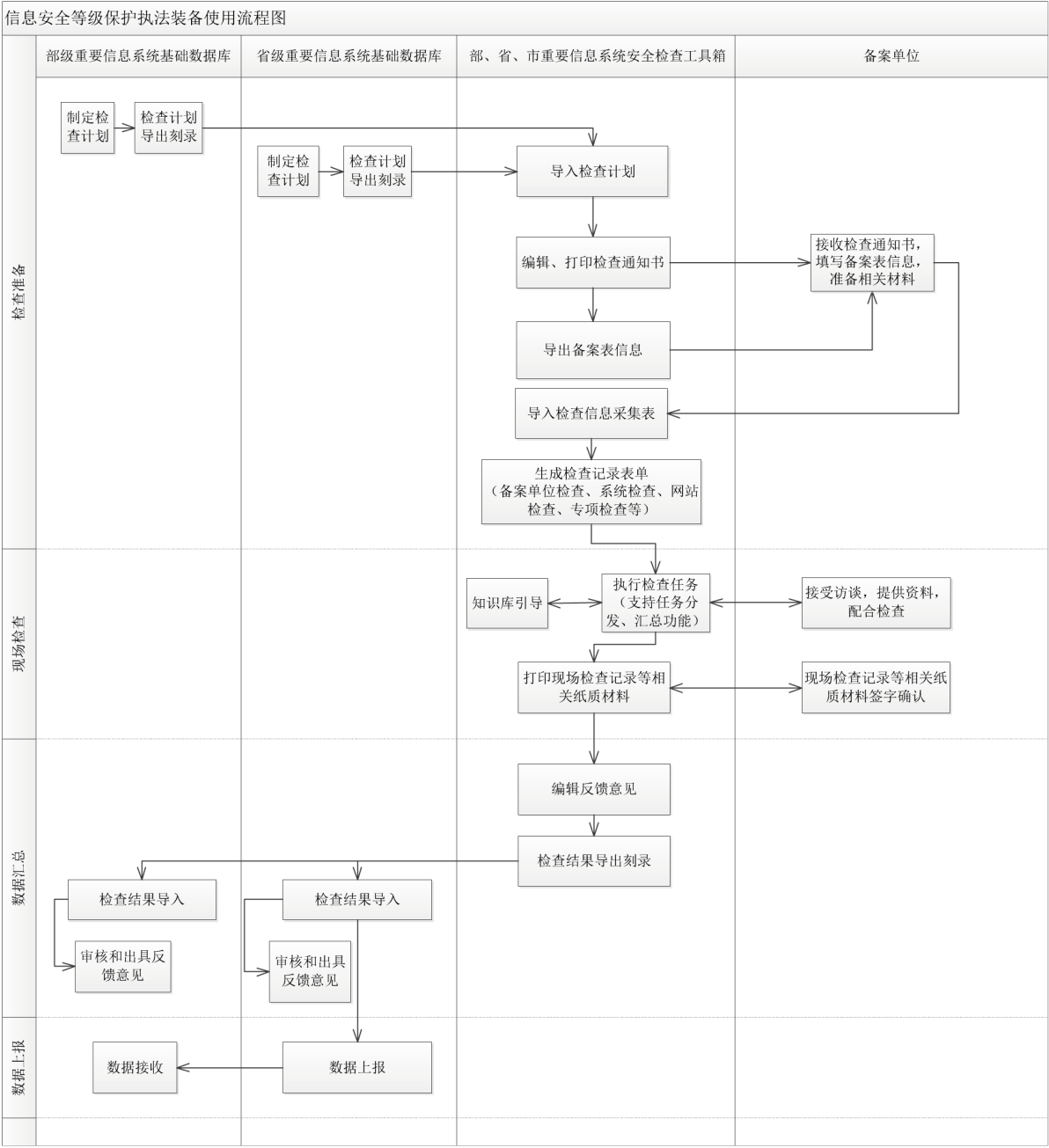
整个检查过程主要分为检查准备、现场检查和数据汇总三个工作阶段。

**检查准备：**检查准备的阶段是检查计划制定、检查信息收集和生成检查记录表单。其中检查计划的制定工作在重要信息系统基础数据库管理系统中进行；检查信息收集及生成检查记录表单在工具管理系统中进行。

**现场检查：**现场检查的阶段是在备案单位的检查现场进行访谈、查看、查阅，测试等相关的检查工作并将检查结果记录在工具管理系统中。检查过程可依据检查工具知识库提供的检查方法、检查结果判定依据等检查知识进行检查，也可使用检查工具提供的检查工具。在现场检查完成后，将检查结果进行汇总后，出具现场检查记录并请备案单位签字确认。

**数据汇总：**数据汇总的阶段主要为检查人员根据检查情况和现场检查记录使用工具管理系统编辑反馈意见，并将检查数据导出刻录，通过光盘将数据导入到重要信息系统基础数据库管理系统中，检查人员在重要信息系统基础数据库管理系统中审核和出具反馈意见。省厅级公安机关将本省的网络安全信息以及相关的检查数据同步到部级系统中。

整个检查过程流程图如图F.1所示。



图F. 1 安全检查工作流程图

F.2 网络安全等级保护备案表

网络安全等级保护备案表如图F.2所示。

备案表编号：

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

# 网络安全等级保护 备案表

备 案 单 位：\_\_\_\_\_（盖章）

备 案 日 期：\_\_\_\_\_

受理备案单位：\_\_\_\_\_（盖章）

受 理 日 期：\_\_\_\_\_

中华人民共和国公安部监制

图F.2 网络安全等级保护备案表

## 填 表 说 明

- 一、**制表依据。**根据《网络安全等级保护管理办法》（公通字[2007]43号）之规定，制作本表；
- 二、**填表范围。**本表由第二级以上信息系统运营使用单位或主管部门（以下简称“备案单位”）填写；本表由四张表单构成，表一为单位信息，每个填表单位填写一张；表二为信息系统基本信息，表三为信息系统定级信息，表二、表三每个信息系统填写一张；表四为第三级以上信息系统需要同时提交的内容，由每个第三级以上信息系统填写一张，并在完成系统建设、整改、测评等工作，投入运行后三十日内向受理备案公安机关提交；表二、表三、表四可以复印使用；
- 三、**保存方式。**本表一式二份，一份由备案单位保存，一份由受理备案公安机关存档；
- 四、本表中有选择的地方请在选项左侧“☐”划“☒”，如选择“其他”，请在其后的横线中注明详细内容；
- 五、**封面中备案表编号**（由受理备案的公安机关填写并校验）：分两部分共11位，第一部分6位，为受理备案公安机关代码前六位（可参照行标GA380-2002）。第二部分5位，为受理备案的公安机关给出的备案单位的顺序编号；
- 六、**封面中备案单位：**是指负责运营使用信息系统的法人单位全称；
- 七、**封面中受理备案单位：**是指受理备案的公安机关公共信息网络安全监察部门名称。此项由受理备案的公安机关负责填写并盖章；
- 八、**表一 04 行政区划代码：**是指备案单位所在的地（区、市、州、盟）行政区划代码；
- 九、**表一 05 单位负责人：**是指主管本单位信息安全工作的领导；
- 十、**表一 06 责任部门：**是指单位内负责信息系统安全工作的部门；
- 十一、**表一 08 隶属关系：**是指信息系统运营使用单位与上级行政机构的从属关系，须按照单位隶属关系代码（GB/T12404—1997）填写；
- 十二、**表二 02 系统编号：**是由运营使用单位给出的本单位备案信息系统的编号；
- 十三、**表二 05 系统网络平台：**是指系统所处的网络环境和网络构架情况；
- 十四、**表二 07 关键产品使用情况：**国产品是指系统中该类产品的研制、生产单位是由中国公民、法人投资或者国家投资或者控股，在中华人民共和国境内具有独立的法人资格，产品的核心技术、关键部件具有我国自主知识产权；
- 十五、**表二 08 系统采用服务情况：**国内服务商是指服务机构在中华人民共和国境内注册成立（港澳台地区除外），由中国公民、法人或国家投资的企事业单位；
- 十六、**表三 01、02、03 项：**填写上述三项内容，确定信息系统安全保护等级时可参考《网络安全等级保护定级指南》，信息系统安全保护等级由业务信息安全等级和系统服务安全等级较高者决定。01、02 项中每一个确定的级别所对应的损害客体及损害程度可多选；
- 十七、**表三 06 主管部门：**是指对备案单位信息系统负领导责任的行政或业务主管单位或部门。部级单位此项可不填；
- 十八、**解释：**本表由公安部网络安全保卫局监制并负责解释，未经允许，任何单位和个人不得对本表进行改动。

图F.2 （续）

表一 单位基本情况

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |             |  |  |  |   |       |             |  |  |  |   |  |  |  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--|--|--|---|-------|-------------|--|--|--|---|--|--|--|
| 01 单位名称        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |             |  |  |  |   |       |             |  |  |  |   |  |  |  |
| 02 单位地址        | _____省(自治区、直辖市) _____地(区、市、州、盟)<br>_____县(区、市、旗)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |             |  |  |  |   |       |             |  |  |  |   |  |  |  |
| 03 邮政编码        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |             |  |  |  |   |       | 04 行政区划代码   |  |  |  |   |  |  |  |
| 05 单位<br>负责人   | 姓 名                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |             |  |  |  |   | 职务/职称 |             |  |  |  |   |  |  |  |
|                | 办公电话                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |             |  |  |  |   | 电子邮件  |             |  |  |  |   |  |  |  |
| 06 责任部门        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |             |  |  |  |   |       |             |  |  |  |   |  |  |  |
| 07 责任部门<br>联系人 | 姓 名                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |             |  |  |  |   | 职务/职称 |             |  |  |  |   |  |  |  |
|                | 办公电话                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |             |  |  |  |   | 电子邮件  |             |  |  |  |   |  |  |  |
|                | 移动电话                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |             |  |  |  |   |       |             |  |  |  |   |  |  |  |
| 08 隶属关系        | <input type="checkbox"/> 1 中央 <input type="checkbox"/> 2 省(自治区、直辖市) <input type="checkbox"/> 3 地(区、市、州、盟)<br><input type="checkbox"/> 4 县(区、市、旗) <input type="checkbox"/> 9 其他_____                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |             |  |  |  |   |       |             |  |  |  |   |  |  |  |
| 09 单位类型        | <input type="checkbox"/> 1 党委机关 <input type="checkbox"/> 2 政府机关 <input type="checkbox"/> 3 事业单位 <input type="checkbox"/> 4 企业 <input type="checkbox"/> 9 其他_____                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |             |  |  |  |   |       |             |  |  |  |   |  |  |  |
| 10 行业类别        | <input type="checkbox"/> 11 电信 <input type="checkbox"/> 12 广电 <input type="checkbox"/> 13 经营性公众互联网<br><br><input type="checkbox"/> 21 铁路 <input type="checkbox"/> 22 银行 <input type="checkbox"/> 23 海关 <input type="checkbox"/> 24 税务<br><input type="checkbox"/> 25 民航 <input type="checkbox"/> 26 电力 <input type="checkbox"/> 27 证券 <input type="checkbox"/> 28 保险<br><br><input type="checkbox"/> 31 国防科技工业 <input type="checkbox"/> 32 公安 <input type="checkbox"/> 33 人事劳动和社会保障 <input type="checkbox"/> 34 财政<br><input type="checkbox"/> 35 审计 <input type="checkbox"/> 36 商业贸易 <input type="checkbox"/> 37 国土资源 <input type="checkbox"/> 38 能源<br><input type="checkbox"/> 39 交通 <input type="checkbox"/> 40 统计 <input type="checkbox"/> 41 工商行政管理 <input type="checkbox"/> 42 邮政<br><input type="checkbox"/> 43 教育 <input type="checkbox"/> 44 文化 <input type="checkbox"/> 45 卫生 <input type="checkbox"/> 46 农业<br><input type="checkbox"/> 47 水利 <input type="checkbox"/> 48 外交 <input type="checkbox"/> 49 发展改革 <input type="checkbox"/> 50 科技<br><input type="checkbox"/> 51 宣传 <input type="checkbox"/> 52 质量监督检验检疫<br><br><input type="checkbox"/> 99 其他_____ |             |  |  |  |   |       |             |  |  |  |   |  |  |  |
| 11 信息系统<br>总数  | 个                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 12 第二级信息系统数 |  |  |  | 个 |       | 13 第三级信息系统数 |  |  |  | 个 |  |  |  |
|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 14 第四级信息系统数 |  |  |  | 个 |       | 15 第五级信息系统数 |  |  |  | 个 |  |  |  |

图F.2 (续)

表二（ / ）信息系统情况

|                         |      |                                                                                                                                                                                                                                           |        |                                                       |                          |                          |                                 |  |  |  |  |
|-------------------------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|-------------------------------------------------------|--------------------------|--------------------------|---------------------------------|--|--|--|--|
| 01 系统名称                 |      |                                                                                                                                                                                                                                           |        |                                                       |                          | 02 系统编号                  |                                 |  |  |  |  |
| 03 系统<br>承载<br>业务<br>情况 | 业务类型 | <input type="checkbox"/> 1 生产作业 <input type="checkbox"/> 2 指挥调度 <input type="checkbox"/> 3 管理控制 <input type="checkbox"/> 4 内部办公<br><input type="checkbox"/> 5 公众服务 <input type="checkbox"/> 9 其他_____                                     |        |                                                       |                          |                          |                                 |  |  |  |  |
|                         | 业务描述 |                                                                                                                                                                                                                                           |        |                                                       |                          |                          |                                 |  |  |  |  |
| 04 系统<br>服务<br>情况       | 服务范围 | <input type="checkbox"/> 10 全国 <input type="checkbox"/> 11 跨省（区、市）跨_____个<br><input type="checkbox"/> 20 全省（区、市） <input type="checkbox"/> 21 跨地（市、区）跨_____个<br><input type="checkbox"/> 30 地（市、区）内<br><input type="checkbox"/> 99 其他_____ |        |                                                       |                          |                          |                                 |  |  |  |  |
|                         | 服务对象 | <input type="checkbox"/> 1 单位内部人员 <input type="checkbox"/> 2 社会公众人员 <input type="checkbox"/> 3 两者均包括 <input type="checkbox"/> 9 其他_____                                                                                                   |        |                                                       |                          |                          |                                 |  |  |  |  |
| 05 系统<br>网络<br>平台       | 覆盖范围 | <input type="checkbox"/> 1 局域网 <input type="checkbox"/> 2 城域网 <input type="checkbox"/> 3 广域网 <input type="checkbox"/> 9 其他_____                                                                                                           |        |                                                       |                          |                          |                                 |  |  |  |  |
|                         | 网络性质 | <input type="checkbox"/> 1 业务专网 <input type="checkbox"/> 2 互联网 <input type="checkbox"/> 9 其他_____                                                                                                                                         |        |                                                       |                          |                          |                                 |  |  |  |  |
| 06 系统互联情况               |      | <input type="checkbox"/> 1 与其他行业系统连接 <input type="checkbox"/> 2 与本行业其他单位系统连接<br><input type="checkbox"/> 3 与本单位其他系统连接 <input type="checkbox"/> 9 其他_____                                                                                  |        |                                                       |                          |                          |                                 |  |  |  |  |
| 07 关键产品使用情况             |      | 序号                                                                                                                                                                                                                                        | 产品类型   | 数量                                                    | 使用国产品率                   |                          |                                 |  |  |  |  |
|                         |      |                                                                                                                                                                                                                                           |        |                                                       | 全部使用                     | 全部未使用                    | 部分使用及使用率                        |  |  |  |  |
|                         |      | 1                                                                                                                                                                                                                                         | 安全专用产品 |                                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> _____% |  |  |  |  |
|                         |      | 2                                                                                                                                                                                                                                         | 网络产品   |                                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> _____% |  |  |  |  |
|                         |      | 3                                                                                                                                                                                                                                         | 操作系统   |                                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> _____% |  |  |  |  |
|                         |      | 4                                                                                                                                                                                                                                         | 数据库    |                                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> _____% |  |  |  |  |
|                         |      | 5                                                                                                                                                                                                                                         | 服务器    |                                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> _____% |  |  |  |  |
| 08 系统采用服务情况             |      | 序号                                                                                                                                                                                                                                        | 服务类型   |                                                       | 服务责任方类型                  |                          |                                 |  |  |  |  |
|                         |      |                                                                                                                                                                                                                                           |        |                                                       | 本行业（单位）                  | 国内其他服务商                  | 国外服务商                           |  |  |  |  |
|                         |      | 1                                                                                                                                                                                                                                         | 等级测评   | <input type="checkbox"/> 有 <input type="checkbox"/> 无 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>        |  |  |  |  |
|                         |      | 2                                                                                                                                                                                                                                         | 风险评估   | <input type="checkbox"/> 有 <input type="checkbox"/> 无 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>        |  |  |  |  |
|                         |      | 3                                                                                                                                                                                                                                         | 灾难恢复   | <input type="checkbox"/> 有 <input type="checkbox"/> 无 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>        |  |  |  |  |
|                         |      | 4                                                                                                                                                                                                                                         | 应急响应   | <input type="checkbox"/> 有 <input type="checkbox"/> 无 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>        |  |  |  |  |
|                         |      | 5                                                                                                                                                                                                                                         | 系统集成   | <input type="checkbox"/> 有 <input type="checkbox"/> 无 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>        |  |  |  |  |
|                         |      | 6                                                                                                                                                                                                                                         | 安全咨询   | <input type="checkbox"/> 有 <input type="checkbox"/> 无 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>        |  |  |  |  |
|                         |      | 7                                                                                                                                                                                                                                         | 安全培训   | <input type="checkbox"/> 有 <input type="checkbox"/> 无 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>        |  |  |  |  |
| 09 等级测评单位名称             |      |                                                                                                                                                                                                                                           |        |                                                       |                          |                          |                                 |  |  |  |  |
| 10 何时投入运行使用             |      | 年    月    日                                                                                                                                                                                                                               |        |                                                       |                          |                          |                                 |  |  |  |  |
| 11 系统是否是分系统             |      | <input type="checkbox"/> 是 <input type="checkbox"/> 否（如选择是请填下两项）                                                                                                                                                                          |        |                                                       |                          |                          |                                 |  |  |  |  |
| 12 上级系统名称               |      |                                                                                                                                                                                                                                           |        |                                                       |                          |                          |                                 |  |  |  |  |
| 13 上级系统所属单位名称           |      |                                                                                                                                                                                                                                           |        |                                                       |                          |                          |                                 |  |  |  |  |

图F.2 （续）

表三（ / ）信息系统定级情况

|                                                                                                       | 损害客体及损害程度                                                                                             | 级别                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| 01 确定<br>业务<br>信息<br>安全<br>保护<br>等级                                                                   | <input type="checkbox"/> 仅对公民、法人和其他组织的合法权益造成损害                                                        | <input type="checkbox"/> 第一级                                                                                                                     |
|                                                                                                       | <input type="checkbox"/> 对公民、法人和其他组织的合法权益造成 <b>严重</b> 损害<br><input type="checkbox"/> 对社会秩序和公共利益造成损害   | <input type="checkbox"/> 第二级                                                                                                                     |
|                                                                                                       | <input type="checkbox"/> 对社会秩序和公共利益造成 <b>严重</b> 损害<br><input type="checkbox"/> 对国家安全造成损害              | <input type="checkbox"/> 第三级                                                                                                                     |
|                                                                                                       | <input type="checkbox"/> 对社会秩序和公共利益造成 <b>特别严重</b> 损害<br><input type="checkbox"/> 对国家安全造成 <b>严重</b> 损害 | <input type="checkbox"/> 第四级                                                                                                                     |
|                                                                                                       | <input type="checkbox"/> 对国家安全造成 <b>特别严重</b> 损害                                                       | <input type="checkbox"/> 第五级                                                                                                                     |
|                                                                                                       | 02 确定<br>系统<br>服务<br>安全<br>保护<br>等级                                                                   | <input type="checkbox"/> 仅对公民、法人和其他组织的合法权益造成损害                                                                                                   |
| <input type="checkbox"/> 对公民、法人和其他组织的合法权益造成 <b>严重</b> 损害<br><input type="checkbox"/> 对社会秩序和公共利益造成损害   |                                                                                                       | <input type="checkbox"/> 第二级                                                                                                                     |
| <input type="checkbox"/> 对社会秩序和公共利益造成 <b>严重</b> 损害<br><input type="checkbox"/> 对国家安全造成损害              |                                                                                                       | <input type="checkbox"/> 第三级                                                                                                                     |
| <input type="checkbox"/> 对社会秩序和公共利益造成 <b>特别严重</b> 损害<br><input type="checkbox"/> 对国家安全造成 <b>严重</b> 损害 |                                                                                                       | <input type="checkbox"/> 第四级                                                                                                                     |
| <input type="checkbox"/> 对国家安全造成 <b>特别严重</b> 损害                                                       |                                                                                                       | <input type="checkbox"/> 第五级                                                                                                                     |
| 03 信息系统安全保护等级                                                                                         |                                                                                                       | <input type="checkbox"/> 第一级 <input type="checkbox"/> 第二级 <input type="checkbox"/> 第三级 <input type="checkbox"/> 第四级 <input type="checkbox"/> 第五级 |
| 04 定级时间                                                                                               | 年   月   日                                                                                             |                                                                                                                                                  |
| 05 专家评审情况                                                                                             | <input type="checkbox"/> 已评审 <input type="checkbox"/> 未评审                                             |                                                                                                                                                  |
| 06 是否有主管部门                                                                                            | <input type="checkbox"/> 有 <input type="checkbox"/> 无（如选择有请填下两项）                                      |                                                                                                                                                  |
| 07 主管部门名称                                                                                             |                                                                                                       |                                                                                                                                                  |
| 08 主管部门审批定级情况                                                                                         | <input type="checkbox"/> 已审批 <input type="checkbox"/> 未审批                                             |                                                                                                                                                  |
| 09 系统定级报告                                                                                             | <input type="checkbox"/> 有 <input type="checkbox"/> 无                      附件名称_____                  |                                                                                                                                                  |
| 填表人：                                                                                                  | 填表日期：   年   月   日                                                                                     |                                                                                                                                                  |

备案审核民警：

审核日期：

年   月   日

图F.2 （续）



表四（ / ）第三级以上信息系统提交材料情况

|                          |                            |                            |           |
|--------------------------|----------------------------|----------------------------|-----------|
| 01 系统拓扑结构及说明             | <input type="checkbox"/> 有 | <input type="checkbox"/> 无 | 附件名称_____ |
| 02 系统安全组织机构及管理制度         | <input type="checkbox"/> 有 | <input type="checkbox"/> 无 | 附件名称_____ |
| 03 系统安全保护设施设计实施方案或改建实施方案 | <input type="checkbox"/> 有 | <input type="checkbox"/> 无 | 附件名称_____ |
| 04 系统使用的安全产品清单及认证、销售许可证明 | <input type="checkbox"/> 有 | <input type="checkbox"/> 无 | 附件名称_____ |
| 05 系统等级测评报告              | <input type="checkbox"/> 有 | <input type="checkbox"/> 无 | 附件名称_____ |
| 06 专家评审情况                | <input type="checkbox"/> 有 | <input type="checkbox"/> 无 | 附件名称_____ |
| 07 上级主管部门审批意见            | <input type="checkbox"/> 有 | <input type="checkbox"/> 无 | 附件名称_____ |

图F. 2 （续）

## 附录 G

### （规范性附录）

#### 检查工具与重要信息系统基础数据库的接口规范

##### G.1 交互数据加密方式

工具管理系统与重要信息系统基础数据库管理系统的交互数据采用国产商用密码产品的sm1算法进行加解密。

##### G.2 交互数据的数据元素集及数据元素代码集

工具管理系统与重要信息系统基础数据库管理系统交互数据的数据元素集见GA/WA 1001-2013。

工具管理系统与重要信息系统基础数据库管理系统交互数据的数据元素代码集见GA/WA 1002-2013。

## 附录 H

### （资料性附录）

#### 检查工具规格要求

##### H.1 等级保护检查专用工具规格要求

###### H.1.1 主机配置

主机配置应满足如下要求：

- a) CPU类型为不低于英特尔酷睿i7处理器；
- b) CPU主频为不低于1.8GHz；
- c) 内存容量不低于8GB；
- d) 硬盘容量不低于240GB；
- e) 硬盘类别为SSD固态硬盘。

###### H.1.2 输入设备

应配备如下输入设备：

- a) 标准全尺寸键盘；
- b) 标准触摸板。

###### H.1.3 显示屏

显示屏应满足如下要求：

- a) 屏幕规格为14英寸；
- b) 显示比例为16:9；
- c) 屏幕物理分辨率不低于1366像素×768像素。

###### H.1.4 多媒体设备

应配备如下多媒体设备：

- a) 内置音效芯片和音频系统；
- b) 内置扬声器；
- c) 内置麦克风。

###### H.1.5 I/O 接口

应配备如下I/O接口：

- a) 专用接口：4个专用端口；
- b) 网络接口：1×RJ45千兆网口；
- c) 数据接口：3×USB 3.0端口，1×USB 2.0端口，串行端口；
- d) 视频接口：HDMI、VGA；
- e) 音频接口：音频输出端口、麦克风端口；
- f) 读卡器接口：1×SD读卡器端口；
- g) 其他接口：电源端口。

###### H.1.6 SATA 硬盘盒

配置SATA硬盘盒，应满足以下要求：

- a) 支持通过eSATA端口与专用工具进行连接；
- b) 支持2.5寸和3.5寸SATA硬盘热插拔。

H.1.7 蓝光刻录机

配置蓝光刻录机，应满足以下要求：

- a) 支持通过USB端口与专用工具进行连接；
- b) 支持BD、DVD、CD的读取和刻录。

H.1.8 电池及电源适配器

电池及电源适配器应满足如下要求：

- a) 内置电池的续航时间不低于4h，具体时间视使用环境而定；
- b) 外接电源适配器为100～240V自适应交流电源适配器。

H.1.9 整体尺寸

整体尺寸应满足如下要求：

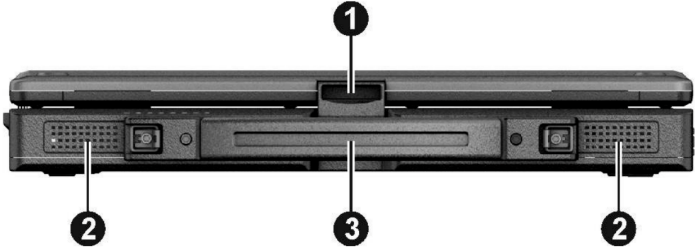
- a) 长：不超过360mm；
- b) 宽：不超过265mm；
- c) 高：不超过55mm。

H.1.10 专用工具组件布局

H.1.10.1 前侧面板

前侧面板上应有提手，以便进行提握。

前侧面板布局如图H. 1所示，各个组件的说明见表H. 1。



图H. 1 专用工具前侧面板布局示意图

表H. 1 专用工具前侧面板组件说明

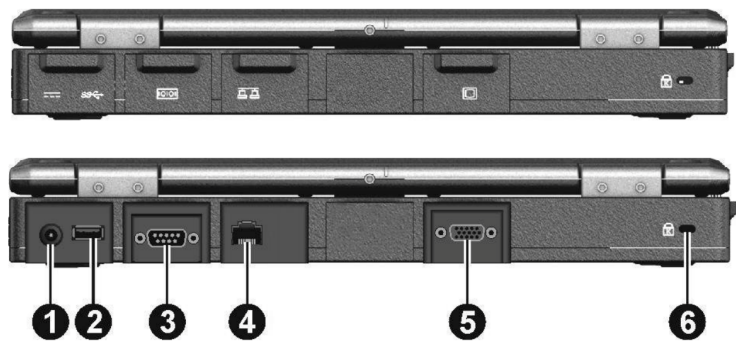
| 编号 | 组件     | 说明               |
|----|--------|------------------|
| ❶  | 上盖门闩   | 用来锁定上盖           |
| ❷  | 立体声扬声器 | 发出电脑的声音          |
| ❸  | 提手     | 为携带专用工具提供的一种便捷方式 |

H.1.10.2 后侧面板

后侧面板应有如下端口：

- a) 1个电源端口；
- b) 1个USB3. 0端口
- c) 1个串行端口；
- d) 1个千兆网口（RJ-45端口）；
- e) 1个VGA端口。

后侧面板布局如图H. 2所示，各个组件的说明见表H. 2。



图H. 2 专用工具后侧面板布局示意图

表H. 2 专用工具后侧面板组件说明

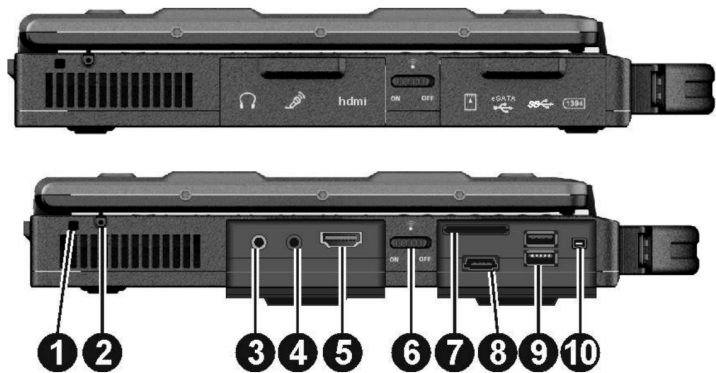
| 编号 | 组件             | 说明                   |
|----|----------------|----------------------|
| ❶  | 电源端口           | 连接交流适配器              |
| ❷  | USB3.0 端口      | 连接 USB 设备，如打印机、数码相机等 |
| ❸  | 串行端口           | 连接 RS232 串行鼠标或串行通信设备 |
| ❹  | RJ-45 端口       | 连接 LAN 线             |
| ❺  | VGA 端口         | 连接外部显示器              |
| ❻  | Kensington 安全锁 | 将电脑锁在固定物体上的安全锁       |

H.1.10.3 左侧面板

左侧面板应有如下端口：

- a) 2个USB3.0的端口；
- b) 1个SD存储卡端口；
- c) 1个HDMI端口；
- d) 1个音频输出端口；
- e) 1个麦克风端口；
- f) 1个eSATA端口。

左侧面板布局如图H. 3所示，各个组件的说明见表H. 3。



图H. 3 专用工具左侧面板布局示意图

表H. 3 专用工具左侧面板组件说明

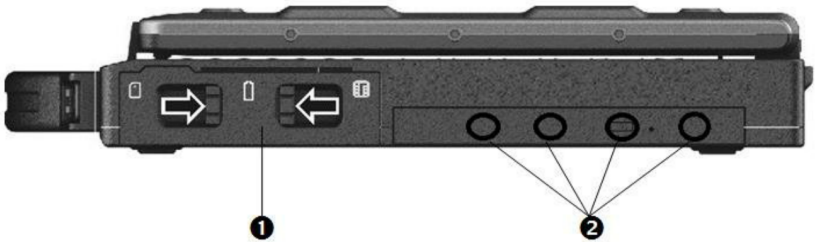
| 编号 | 组件         | 说明                                     |
|----|------------|----------------------------------------|
| ❶  | 笔绳孔        | 笔绳系于此处                                 |
| ❷  | 触控笔（可选）    | 用来在屏幕上点击，用于操控                          |
| ❸  | 音频输出端口     | 连接一组耳机或者带功放的外部扬声器                      |
| ❹  | 麦克风端口      | 连接外部麦克风                                |
| ❺  | HDMI 端口    | 连接 HDMI 显示器或电视                         |
| ❻  | RF（射频）开关   | 用作主控制，可一次打开和关闭所有无线射频                   |
| ❼  | 存储卡读卡器     | 接受 MMC、MMC Plus 或 SD 存储卡               |
| ❽  | eSATA 端口   | 连接 eSATA 设备，如外部硬盘或光驱。也可以作为 USB2.0 端口使用 |
| ❾  | USB 3.0 端口 | 连接 USB 设备，如打印机、数码相机等                   |
| ❿  | 固定锁        | 固定锁                                    |

H.1.10.4 右侧面板

右侧面板应有4个专用端口，并且在专用端口的边上有专用U口检查工具名称缩写的标识：

- a) “Windows主机配置检查工具” 名称缩写为“WIN检查”；
- b) “病毒检查工具” 名称缩写为“病毒检查”；
- c) “木马检查工具” 名称缩写为“木马检查”；
- d) “网站恶意代码检查工具” 名称缩写为“挂马检查”。

右侧面板布局如图H. 4所示，各个组件的说明见表H. 4。



图H. 4 专用工具右侧面板布局示意图

表H. 4 专用工具右侧面板组件说明

| 编号 | 组件   | 说明                 |
|----|------|--------------------|
| ❶  | 电池组  | 当未连接外部电源时可为电脑供应电源  |
| ❷  | 专用端口 | 信息安全检查专用 U 口检查工具端口 |

H.1.10.5 上侧面板

上侧面板应有如下内容：

- a) 警徽；

- b) 产品名称“网络安全等级保护检查专用工具”；
- c) 产品编码。

**H.1.10.6 下侧面板**

下侧面板上面应有如下内容：技术支持电话（应为800或400技术支持电话）。

**H.1.10.7 挡板**

所有接口的区域应该有挡板防护。

**H.1.11 其他**

**H.1.11.1 操作系统**

安全可靠操作系统。

**H.1.11.2 专用 USB 转换线**

专用USB转换线放置于防护箱内。

**H.1.11.3 环境适应性**

等级保护检查专用工具应具有很好的环境适应性，要求如下：

- a) 防撞；
- b) 耐摔；
- c) 支持低温启动并能正常工作。

**H.1.11.4 产品编码**

各个检查工具研发厂商都应有各自的检查工具产品编码范围，有如下要求：

- a) 所有检查工具产品的编码唯一，便于核对检查工具的生产厂商和使用单位；
- b) 检查工具产品编码共为十位，前两位编码为厂商缩写的大写字母，中间六位编码为采购检查工具的公安机关代码前六位（可参见GA 380-2002），后两位编码为检查工具的编号；
- c) 防护箱和等级保护检查专用工具的箱体表面上印制检查工具产品编码，以统一编码形式出现，不允许在箱体表面出现检查工具研发厂商的标志或徽标等任何相关标识；
- d) 防护箱和等级保护检查专用工具都要有警徽和编号；
- e) 等级保护检查专用工具的背面有800或400的技术支持电话。

**H.2 辅助检查设备规格要求**

**H.2.1 便携式打印机**

便携式打印机规格要求见表H. 5。

**表H. 5 便携式打印机规格要求**

| 序号 | 参数名称   | 规格要求                      |
|----|--------|---------------------------|
| 1  | 最高分辨率  | 不低于 4800dpi×1200dpi       |
| 2  | 黑白打印速度 | 不低于 22 页/min              |
| 3  | 彩色打印速度 | 不低于 18 页/min              |
| 4  | 系统平台   | 支持 Windows 7              |
| 5  | 介质类型   | 普通 A4 打印纸                 |
| 6  | 接口类型   | 支持 USB2.0（含）以上            |
| 7  | 产品尺寸   | 体积不大于 5500cm <sup>3</sup> |
| 8  | 产品重量   | 不大于 2.5kg                 |
| 9  | 墨盒     | 墨盒与喷头为一体                  |

H.2.2 扫描仪

扫描仪规格要求见表H. 6。

表H. 6 扫描仪规格要求

| 序号 | 参数名称   | 规格要求            |
|----|--------|-----------------|
| 1  | 分辨率    | 不低于 300dpi      |
| 2  | 色彩     | 支持彩色/黑白         |
| 3  | 接口     | 支持 USB2. 0      |
| 4  | 操作系统   | 支持 Windows 7    |
| 5  | 扫描最大幅面 | 支持 A4           |
| 6  | 扫描介质   | 文件、图片           |
| 7  | 输出格式   | 支持 JPG、BMP      |
| 8  | 接口类型   | 支持 USB2. 0（含）以上 |
| 9  | 存储容量   | 不低于 4GB         |

H.2.3 数码相机

数码相机规格要求见表H. 7。

表H. 7 数码相机规格要求

| 序号 | 参数名称  | 规格要求              |
|----|-------|-------------------|
| 1  | 总像素   | 不低于 1600 万        |
| 2  | 操作模式  | 全自动               |
| 3  | 变焦方式  | 光学变焦              |
| 4  | 变焦倍数  | 不低于 20 倍          |
| 5  | 对焦方式  | 自动对焦              |
| 6  | 机身闪光灯 | 内置闪光灯             |
| 7  | 数据接口  | 支持 USB2. 0（含）以上接口 |
| 8  | 存储容量  | 不低于 4GB           |

H.2.4 录音笔

录音笔规格要求见表H. 8。

表H. 8 录音笔规格要求

| 序号 | 参数名称 | 规格要求             |
|----|------|------------------|
| 1  | 录音格式 | 支持 mp3 和 wav 格式  |
| 2  | 录音时间 | mp3 录音格式不低于 200h |
| 3  | 麦克风  | 内置高灵敏度麦克风        |
| 4  | 扬声器  | 内置扬声器            |
| 5  | 显示屏  | 中文数码显示屏          |



表H.8 （续）

| 序号 | 参数名称 | 规格要求           |
|----|------|----------------|
| 6  | 机身重量 | 不大于 70g        |
| 7  | 录音距离 | 不低于 4m         |
| 8  | 接口类型 | 支持 USB2.0（含）以上 |
| 9  | 容量   | 不低于 8GB        |

### H.2.5 执法记录仪

执法记录仪规格要求见表H.9。

表H.9 执法记录仪规格要求

| 序号 | 参数名称   | 规格要求                                 |
|----|--------|--------------------------------------|
| 1  | 像素     | 不低于 1600 万                           |
| 2  | 摄像时间   | 连续摄像不小于 6h                           |
| 3  | 夜视距离   | 不低于 10 米                             |
| 4  | 待机时间   | 不低于 24h                              |
| 5  | 接口类型   | 支持 USB2.0（含）以上                       |
| 6  | 支持操作系统 | 支持 Windows 7                         |
| 7  | 存储容量   | 不低于 16GB                             |
| 8  | 技术要求   | 应符合《GA/T 947-2011 单警执法视音频记录仪》中的技术要求。 |

### H.2.6 防护箱

防护箱规格要求见表H.10。

表H.10 防护箱规格要求

| 序号 | 参数名称 | 规格要求                                       |
|----|------|--------------------------------------------|
| 1  | 耐温范围 | 箱体应在-40℃至+99℃之间保持正常形态                      |
| 2  | 耐用性  | 正常使用（负重在 15Kg 以内）的情况下，箱体可以正常使用             |
| 3  | 防水性  | 箱体应在完全浸入水面 5cm 以下，保持 1h 不发生渗漏              |
| 4  | 复用性  | 箱体浸入水下 1h 后取出，箱盖应能自由开关 5 次以上               |
| 5  | 防雨性  | 箱体应在雨量每小时 100mm 的环境下，6 个面分别至少经受 40min 以上雨淋 |
| 6  | 防尘性  | 箱体应具有 IP 6 级的防尘能力，防止灰尘进入                   |

表H. 10 （续）

| 序号 | 参数名称 | 规格要求                                                     |
|----|------|----------------------------------------------------------|
| 7  | 防冲击性 | 箱体应能防直径 3.2cm、顶端为半球形、重 6kg 的重物从 500mm 高自由落下冲击            |
| 8  | 承重性  | 箱体内装载 15kg 负重情况下，箱体把手应能支持悬挂 8h 以上。<br>箱体应能承受不超过 60kg 的重量 |
| 9  | 防摔性  | 箱体内装载 20kg 负重情况下，应能从 640mm 高处角棱面全方位自由跌落 8 次              |
| 10 | 防震性  | 箱体应能承受 5Hz 到 50Hz 3 个轴向，每轴向 40min，总计 120min 的震动          |
| 11 | 易用性  | 箱体应配备拉杆和滑轮，以方便使用                                         |
| 12 | 锁具   | 防护箱应配备锁具（锁具为密码锁）                                         |
| 13 | 箱体大小 | 长、宽、高三边之和不超过 130cm                                       |
| 14 | 总重量  | 防护箱及所有硬件（包括等级保护检查专用工具和辅助检查设备）的总重量不得超过 20kg               |

## 参 考 文 献

- [1] GA 380-2002 全国公安机关机构代码编制规则
  - [2] GA/T 947-2011 单警执法视音频记录仪
-