DBXX/XXX—2022

湖南省市场监督管理局 发布

2022-XX--XX实施

2022--XX--XX发布

党政机关治安反恐防范要求

Anti-terrorist precaution requirements for public security of Party and government organs

（征求意见稿）

DB

湖南省地方标准

ICS XXXXXXX

X XX

备案号：XXXX-XXXX

目   次

[前言 Ⅱ](#_Toc92661005)

[引言 Ⅳ](#_Toc92661006)

[1　范围 1](#_Toc92661007)

[2　规范性引用文件 1](#_Toc92661008)

[3　术语和定义 2](#_Toc92661009)

[4　重点目标等级和重点部位 3](#_Toc92661022)

[5　总体防范要求 4](#_Toc92661025)

[6　常态三级防范要求](#_Toc92661026) 10

[7　常态二级防范要求 1](#_Toc92661026)3

[8　常态一级防范要求 1](#_Toc92661026)3

[9　非常态防范要求](#_Toc92661037) 14

[10 安全防范系统技术要求 1](#_Toc92661026)4

[附录A（规范性）　党政机关常态人力防范措施](#_Toc92661040) 17

[附录B（规范性）　党政机关常态防范设施配置](#_Toc92661041) 19

[参考文献](#_Toc92661045) 26

1. 前   言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由湖南省公安厅提出并归口。

本文件起草单位：湖南省公安厅治安管理总队、湖南省公安厅反恐总队、中共湖南省委机关保卫处、湖南省人民政府机关保卫处、湖南省人大常委会机关保卫处、湖南省政协机关保卫处、湖南省高级人民法院机关保卫处、长沙市人民政府机关保卫处、长沙市公安局内保支队、海康威视数字技术股份有限公司、湖南声迅保安服务有限公司、湖南三迈信息科技有限公司、邵阳市金盾保安服务有限公司、湖南元一保安科技有限公司、世邦通信股份有限公司、湖南戍融智能科技有限公司、浙江大华技术股份有限公司、湖南省保安协会、湖南敏求电子科技有限公司。

本文件主要起草人：张小兵、温昊、刘绘锦、尹年春 、谢永、刘禹、罗则范、罗再良、唐兴众、朱云军、李克伟、胡毅、朱和平、胡超超、田建云、余求理、杨慧、唐爱华、陈治国、汤烈、申文娟、胡令权、王诗侃、罗劭轩、王韬才、吴旭辉。

1. 引   言

本文件依据《中华人民共和国反恐怖主义法》、《中华人民共和国突发事件应对法》、《企业事业单位内部治安保卫条例》和《湖南省实施<中华人民共和国反恐怖主义法>办法》等有关法律、法规，针对可能威胁公共安全和公众生命、财产安全的风险因素，区分治安反恐防范重点目标和重点部位，对重点目标进行分级，提出了相应的常态防范要求和非常态防范要求，并且基于同地方标准《湖南省反恐防范管理系统要求》（DB43/T 1026.1）相一致，非常态防范要求分成了三个级别，各级别又包括人力防范、实体防范和电子防范要求，是规范和加强湖南省党政机关治安防范和反恐防范工作与管理的重要依据。

党政机关治安反恐防范要求

* 1. 范围

本文件规定了党政机关治安反恐防范的重点目标、重点部位、总体防范要求、常态三级防范要求、常态二级防范要求、常态一级防范要求、非常态防范要求和安全防范系统技术要求。

本文件适用于党政机关治安反恐防范工作与管理。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T 3836.1 爆炸性环境 第1部分：设备通用要求

GB 10409 防盗保险柜(箱)

GB 12899 手持式金属探测器通用技术规范

GB 14287.1　电气火灾监控系统　第1部分　电气火灾监控设备

GB 14287.2　电气火灾监控系统　第2部分：剩余电流式电气火灾监控探测器

GB 15208.1 微剂量X射线安全检查设备 第1部分：通用技术要求

GB 15208.2 微剂量X射线安全检查设备 第2部分：透射式行包安全检查设备

GB 15210 通过式金属探测门通用技术规范

GB/T 16917.1　家用和类似用途的带过电流保护的剩余电流动作断路器（RCBO）　第1部分：一般规则

GB 17565—2007 防盗安全门通用技术条件

GB/T 22239 信息安全技术网络安全等级保护基本要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 30147 安防监控视频实时智能分析设备技术要求

GB/T 32581 入侵和紧急报警系统技术要求

GB 35114 公共安全视频监控联网信息安全技术要求

GB/T 37078 出入口控制系统技术要求

GB 50348 安全防范工程技术标准

GB 50526 公共广播系统工程技术标准

GB 55029 安全防范工程通用规范

GA 69 防爆毯

GA/T 594 保安服务操作规程与质量控制

GA/T 644 电子巡查系统技术要求

GA/T 761 停车库（场）安全管理系统技术要求

GA 871 防爆罐

GA 1016 枪支（弹药）库室风险等级划分与安全防范要求

GA/T 1093 出入口控制人脸识别系统技术要求

GA/T 1302 停车服务与管理信息系统通用技术条件

* 1. 术语和定义

GB 50348、DB43/T 1026.1界定的以及下列术语和定义适用于本文件。



党政机关 party and government organs

中国共产党机关、人大常委会机关、行政机关、政协机关、监察机关、审判机关、检察机关以及各级党政机关派出、派驻机构。



常态防范 regular protection

运用人力防范、实体防范、电子防范等多种手段和措施，常规性预防、延迟、阻止发生治安和恐怖案事件的管理行为。



非常态防范 unusual protection

在重要会议、重大活动等重要时段以及获得重大治安、恐怖袭击等预警信息或发生上述案事件时，相关单位临时性加强防范手段和措施，提升治安反恐防范能力的管理行为。



人力防范 personnel prevention

具有相应素质的人员有组织的防范、处置等安全管理行为。

[来源：GB 50348—2018，2.0.2]



实体防范 physical prevention

利用建（构）筑物、屏障、器具、设备或其组合，延迟或阻止风险事件发生的实体防护手段。

[来源：GB 50348—2018，2.0.3]



电子防范 electronic prevention

利用传感、通信、计算机、信息处理及其控制、生物特征识别等技术，提高探测、延迟、反应能力的防护手段。

[来源：GB 50348—2018，2.0.4]



保安员 security staff

依照《保安服务管理条例》取得保安员证，从事保安服务工作的人员。



安全保卫人员 security guard

由党政机关直接聘用和管理，并与其有劳动合同关系的从事安全保卫工作的管理人员及工作人员。通常包括负责安全工作的保卫干部、保安员等。

一键报警　one key alarm

人员使用物理按钮或移动终端等，通过一次触发，用有线或无线通信方式向公安机关传输音频/视频、位置等紧急报警信号的报警方式。

电气火灾监控系统 electricalfiremonitoringsystem

当被保护电气线路中的被探测参数超过报警设定值时，能发出报警信号、控制信号并能指示报警部

位的系统，由电气火灾监控设备和电气火灾监控探测器组成。

电气火灾监控探测器 electricalfiremonitoringdetector

探测被保护线路中的剩余电流、温度、故障电弧等电气火灾危险参数变化和由于电器故障引起的烟

雾变化及可能引起电气火灾的静电、绝缘参数变化的探测器。

断路器 circuit-breaker

能接通、承载和分断正常电路条件下电流以及也能在规定的非正常条件下（例如短路）接通、承载

一定的时间和（自动地）分断电流的机械开关电器。

剩余电流动作断路器 residualcurrentoperatedcircuit-breaker

在正常运行条件下接通、承载和分断电流，以及在规定条件下当剩余电流达到规定值时能使触头断开的机械开关电器。

治安反恐防范综合管理平台 comprehensive management platform for security and anti-terrorism security

以治安防范和反恐防范为目的，对安全防范系统的各子系统及相关信息系统进行集成，实现实体防护系统、电子防护系统和人力防范资源的有机联动、信息的集中处理与共享应用、风险事件的综合研判、事件处置的指挥调度、系统和设备的统一管理与运行维护等功能的硬件和软件组合。

[来源：GB 50348-2018，2.0.16，有修改]

* 1. 重点目标等级和重点部位
     1. 重点目标等级

4.1.1 根据党政机关所处的地理位置，党政机关的规模、遭受恐怖袭击后可能造成的人员伤亡、财产损失、社会影响等要素，结合湖南省范围内党政机关的数量、人流量、开放性程度、周边环境、管理状况，对党政机关进行反恐防范重点目标等级划分。

4.1.2 党政机关治安反恐防范重点目标的等级由低到高分为三级重点目标、二级重点目标、一级重点目标，由公安机关会同有关部门、相关机关单位依据国家有关规定共同确定。具体为：

a) 省级治安保卫重点单位的党政机关为一级重点目标。

b) 市（地、州）级治安保卫重点单位的党政机关为二级重点目标。

c) 县（市、区）级治安保卫重点单位的党政机关为三级重点目标。

4.1.3 重点目标的防范级别分为常态防范和非常态防范。常态防范级别按防范能力由低到高分别是三级防范、二级防范、一级防范，防范级别应与目标等级相适应。三级重点目标对应常态三级防范、二级重点目标对应常态二级防范、一级重点目标对应常态一级防范。

4.1.4 常态二级防范要求应在常态三级防范要求基础上执行，常态一级防范要求应在常态二级防范要求基础上执行，非常态防范要求应在常态防范要求基础上执行。

* + 1. 重点部位

下列部位确定为党政机关治安反恐防范的重点部位：

1. 党政机关大院（大楼）周边；
2. 党政机关大门外：党政机关大院（大楼）大门外人员、车辆密集集中的区域，包含专用停车场、临时停车区等；
3. 具有独立院落的党政机关大院周界、出入口；
4. 党政机关大院内办公楼出入口、楼顶；
5. 无院落的党政机关大楼周界、出入口、楼顶；
6. 门卫室（传达室），警务室，值班岗亭等；
7. 党政机关大院内主要道路、广场；
8. 办事大厅、接访场所；
9. 公文交换中心；
10. 财务室、档案室、资料室；
11. 机关工作人员宿舍楼（区）出入口、主要通道、楼顶；
12. 食堂（餐厅）操作间、配餐间、留样间、储藏室、就餐区；
13. 机要室、保密室；
14. 数据中心、案件管理中心
15. 枪支弹药存放场所；
16. 水、电、气、热、通信等设备间；
17. 安防监控中心（室）；
18. 机动车停车场、非机动车停车区；
19. 其他经评估需要防范的重点部位。
    1. 总体防范要求

5.1 党政机关治安反恐防范应遵循“预防为主、单位负责、突出重点、保障安全、专群结合”的方针，“属地负责、逐级监管”和“谁主管、谁负责”的原则。

5.2 新建、改建、扩建党政机关的安全防范系统应与主体工程同步规划，同步设计、同步建设、同步验收、同步运行。已建、在建的党政机关应按本文件要求补充完善安全防范系统。

5.3 党政机关是内部安全保卫工作和反恐怖防范的责任主体，应建立安全保卫和反恐怖工作领导机构，法定代表人为第一责任人，并确定相关机构或者责任人员负责反恐怖主义工作，落实反恐怖主义工作责任制，明确岗位职责。

5.4 党政机关应建立重点目标的“一岗双责”制度，领导干部既要对所在岗位具体业务工作负责，又要对所在岗位治安反恐防范工作负责。

5.5 党政机关应落实反恐怖主义工作专项经费保障，配备、更新防范和处置设备、设施。常态防范条件下，治安反恐防范涉及费用应纳入机关预算，予以专项保障；并根据实际情况，考虑非常态防范条件下的费用保障措施。

5.6 党政机关应建立健全治安反恐防范管理档案和台账，包括重点目标的名称、地址或位置、目标等级、防范级别、单位负责人、保卫部门负责人，现有人力防范、实体防范、电子防范措施，平面图、结构图、应急预案、疏散图等。

5.7 党政机关应根据公安机关及有关部门的要求，依法提供重点目标的相关信息和重要动态。

5.8 党政机关应对重要岗位人员进行安全背景审查。对有不适合情形的人员，应当调整工作岗位，并将有关情况通报公安机关。

5.9 党政机关应建立安防设施隐患排查、安全管理制度风险监测和安保措施防控治理的机制，并加强用水、用电、消防、防盗和人身防护等方面的安全教育与安防专题培训，内部工作人员应掌握避险、逃生、自救等方法。

5.10 党政机关应根据可能发生的爆炸、燃烧、劫持人质等恐怖袭击活动，制定突发事件应急处置预案，并组织开展相关培训和定期演练。应急处置预案应至少包括针对的事件、人员及分工、处置的流程及措施、设备（设施或装备）的使用和人员疏散方案等内容。

5.11 党政机关应与属地公安机关建立信息共享和联动联防工作机制，构建内部、周边与社会相结合的治安反恐防控体系。

5.12 党政机关应建立安全防范系统运行与维护的保障体系和长效机制，并设专人负责系统日常管理工作，保持系统处于良好的运行状态。

5.13 安全技术防范系统建设单位及服务单位应接受公安机关的监督管理，监督管理包括技术系统的运行情况、服务质量及服务管理规范检查等。

5.14 党政机关安全技术防范系统建设完工后应进行验收，验收应符合GB 50348的相关要求。

5.15 党政机关的网络与信息系统应明确安全保护等级，采取GB/T 22239中相应的安全保护等级的防护措施。

5.16 应对党政机关信息网络及安防信息网络进行定级备案，根据信息安全等级保护备案要求进行定期评估测评，通过评估测评对网络系统进行必要的加固完善，以应对网络攻击、信息安全渗透新技术手段的恐怖袭击。

5.17 党政机关安全防范系统和设备登录密码不应是弱口令，不应存在网络安全漏洞和隐患。当基于不同传输网络的系统和设备联网时，应采取相应的网络边界安全管理措施。

5.18 党政机关安全防范系统中涉及公民个人信息的，应依法依规进行处理，包括收集、存储、使用、加工、传输、提供、公开、删除等。

5.19 所有寄递到党政机关的邮件、快件、包裹均应经过寄递企业安检并盖有安检戳记，未盖安检戳记的邮件，不得进入党政机关院内。

5.20　党政机关常态防范设施配置应符合附录B的规定。

* 1. 常态三级防范要求
     1. 人力防范要求

6.1.1 党政机关反恐怖防范工作领导机构应由机关内部各单位责任领导成员组成，下设办公室并指定工作联络人员，落实主体责任，做好反恐怖防范工作。

6.1.2 党政机关应每季度至少开展一次全面的安全工作检查，每半年至少开展一次风险评估工作并作出评估结论，每年度至少开展一次安全专项督查工作。

6.1.3 党政机关反恐怖主义工作领导机构及办事机构应与行业主管（监管）职能部门加强防范与应急联系，实现涉恐信息的实时报送、更新、交互和对接。

6.1.4 党政机关反恐怖防范工作领导机构办公室设在保卫部门，由专职保卫干部、在编工作人员和机关内部各单位指定的安全保卫负责人组成，承担反恐怖防范日常工作。

6.1.5 党政机关应建立并实施人力防范管理制度，并做好相应的记录。人力防范管理制度应符合以下内容：

1. 背景审查与行为评估制度：应对公安机关出具的无违法犯罪记录的证明材料及直系亲属背景进行审查确认，并对其行为安全风险进行评估；
2. 值守与巡查制度：根据实际情况在党政机关门口、供水、供电、控制中心等重要部位开展值守、巡查；
3. 人员与物品检查制度：依照规定对进入党政机关的人员及携带物品进行安全检查；
4. 防范、应急联动制度：党政机关应与当地公安部门建立防范、应急联动机制；
5. 教育与培训制度：对安保力量及相关员工进行反恐怖防范知识、技能的教育、培训；
6. 安全防范与应急演练制度：每年组织不少于一次的反恐怖防范或应急演练；
7. 检查与督察制度：每半年不少于一次反恐怖防范检查、督察，掌握反恐怖防范措施的落实和电子防范、实体防范设备（设施）装备的配置使用情况；
8. 考核与奖惩制度：定期对安保力量及相关员工的反恐怖防范工作进行考核、奖惩。

6.1.6 党政机关反恐怖安保力量和人力防范装备应符合相关规定。

6.1.7 党政机关宜直接与保安公司签订保安服务合同。党政机关应聘用专职保安员和专职门卫，年龄原则上不得超过45周岁，退伍军人和警校毕业生比例不低于20%。

6.1.8 门卫、保安员应取得《保安员证》或职业资格证书。专职安全保卫人员应取得保卫管理员职业资格证书。

6.1.9 所配党政机关专（兼）职保安员和专职门卫应按照属地管理原则到辖区公安派出所备案。

6.1.10 门卫和保安员应配备取得安防产品合格证的对讲机、防暴头盔、棍棒、钢叉、防护盾牌、防刺背心、防割手套、强光手电等必要的护卫器械，并建立使用保管制度。

6.1.11 安全保卫人员应培训上岗，掌握党政机关安全管理、治安保卫的基本技能。

6.1.12 党政机关的门卫室（传达室）、值班岗亭应24h 有人值守。

6.1.13 党政机关应对开启的出入口有人值守，并对进入党政机关的人员、车辆进行核查验证和信息登记，禁止无关人员和院外机动车入内，禁止将易燃易爆物品、有毒物品、动物和管制器具等危险物品带入党政机关。

6.1.14 安全保卫人员应对党政机关重点部位进行每日不少于 8 次的巡逻，其中夜间开展不少于4次的夜间巡逻。

6.1.15 党政机关应安排安全保卫人员在岗值勤，在重要节日或敏感时段要增强在岗值勤人员。

6.1.16 落实安防监控中心（室）等重要部位值守力量，重要部位落实巡逻力量，落实日常机动备勤力量，建立机关干部、安全保卫人员等组成的群众性第一应急处置力量队伍。

6.1.17 属地公安机关应当加强与党政机关合作，按照规定在党政机关及周边建设警务室按照规定在党政机关及周边建设警务室，公安机关派不少于一名正式干警和不少于两名协警值班，并配齐警用设施设备；建立健全党政机关周边日常巡逻防控制度。

6.1.18 党政机关应根据有关规定，结合单位工作性质及地理位置、单位面积、工作人员数量、重要部位分布等反恐怖防范工作实际需要，设置保卫机构，配备专职的保卫干部和足够的安全保卫人员。

6.1.19 党政机关反恐怖人力防范措施配置应符合附录A的规定。

* + 1. 实体防范要求

6.2.1 党政机关办公大院周边公共停车场、广场、道路等室外公共区域应当根据需要设置规范的安全警示牌、交通标志标牌标线、交通信号灯、人行设施、分隔设施、停车设施和减速带等。

6.2.2 具有独立院落的党政机关大院出入口、无院落的党政机关大楼出入口和人员行进主要道路、办公楼出入口和宿舍楼通道等部位、地段应当安装路灯，亮化率达100%。

6.2.3 党政机关大院周边应规范设置安全警示牌和人行、分隔、停车等设施，宜设置警务室、治安岗亭等设施。

6.2.4 党政机关大门外应设置限速和警示标志、减速带、人行横道和交通信号灯。

6.2.5 具有独立院落的党政机关大院，其周界应设置实体围墙或栅栏等实体屏障，实体屏障外侧整体高度（含防攀爬设施）应大于或等于2.5米。

6.2.6 具有独立院落的党政机关大院出入口应设置隔离栏、隔离墩或升降柱等硬质防冲撞设施。

6.2.7 无院落的党政机关大楼出入口应设置隔离栏、隔离墩或升降柱等硬质防冲撞设施。

6.2.8 党政机关大院内主要道路应设置限速和警示标志。

6.2.9 财务室、档案室、资料室、机要室、保密室、数据中心、案件管理中心、安防监控中心（室）、水电气热等设备间的出入口应安装符合GB 17565—2007要求的乙级及以上防盗安全门，其与外界相通的窗户应安装钢制栅栏，钢筋直径应大于或等于12 mm，单个栅栏空间最大面积应小于或等于250 mm×100 mm。

6.2.10 党政机关大院内建筑工地、陡坡、水池、楼梯等易发生危险的地方应设置警示标志或防护设施。办公楼顶、宿舍楼顶、水塘边等危险区域，应有明显的警示标识。

6.2.11 党政机关设置有停车场的，宜设置对行车路线、停车场位置、车位有指引或标识。宜根据情况设置限速标识。

6.2.12 防毒面罩、毛巾、口罩等应急用品的配置根据各单位具体情况进行配置。

* + 1. 电子防范要求

6.3.1 党政机关大门外应设置视频图像采集装置，视频监视和回放图像应能容易识别25米监视范围内人员体貌特征与车辆号牌；视频监视和回放图像应清楚辨别50米范围内进出人员体貌特征和进出车辆颜色及车型等。

6.3.2 具有独立院落的党政机关大院周界应设置视频图像采集装置，视频监视和回放图像应能清晰显示周界区域人员活动情况，宜设置入侵探测装置或具有入侵探测功能的视频图像采集装置，探测范围应对周界实现有效覆盖，不得有盲区。

6.3.3 具有独立院落的党政机关大院主出入口应设置视频图像采集装置，视频监视和回放图像应能清晰显示进出人员的体貌特征和进出车辆的号牌，并符合以下要求：

1. 宜设置人脸识别视频图像采集装置，智能视频分析装置应对进入党政机关人员的人脸图像进行动态采集和图像比对，对党政机关出入口及周边人员徘徊、滞留可视频分析报警提示给门卫保安。宜将人脸图像发送到公安人脸识别系统做监视名单的人脸比对，对重点人员可视频分析报警；
2. 宜设置对党政机关工作人员进行身份识别的出入口控制通道装置；
3. 宜设置访客人脸识别装置，配置读取身份证存储照片与持证人员人脸进行比对。

6.3.4 无独立院落的党政机关大楼周界应设置视频图像采集装置，视频监视和回放图像应能清晰显示周界情况；其出入口应设置视频图像采集装置，视频监视和回放图像应能清晰显示进出人员的体貌特征，并符合以下要求：

a) 宜设置人脸识别视频图像采集装置，智能视频分析装置应对进入党政机关人员的人脸图像进行动态采集和图像比对，对党政机关出入口及周边人员徘徊、滞留可视频分析报警提示给门卫保安。宜将人脸图像发送到公安人脸识别系统做监视名单的人脸比对，对重点人员可视频分析报警；

b) 宜设置对党政机关工作人员进行身份识别的出入口控制通道装置；

c) 宜设置访客人脸识别装置，配置读取身份证存储照片与持证人员人脸进行比对。

6.3.5 具有独立院落的党政机关大院主出入口或周边和无独立院落的党政机关大楼周界、出入口应设置体温检测、个人健康信息码识别等通用设备设施。

6.3.6 门卫室（传达室、值班岗亭）内部应设置紧急（一键）报警、视频图像采集装置和公共广播装置，视频监视和回放图像应能清晰显示人员活动情况，紧急报警信号应传动到安防监控中心（室）。

6.3.7 办事大厅接待席位、信访接待席位、对外接待处应设置视频图像采集装置、音频采集装置，视频监视和回放图像应能清晰显示办事大厅内人员活动情况，并并设置紧急（一键）报警装置，报警信号应传送至安防监控中心（室）。

6.3.8 党政机关大院内主要道路、广场等室外人员集中活动区域应设置视频图像采集装置，视频监视和回放图像应能清晰显示监视区域内人员活动情况。

6.3.9 党政机关大院主出入口，大院内主要道路、广场等室外人员集中活动区域，党政机关大楼出入口宜配置人员密度监测或检测设备设施，对拥挤情况告警提醒，避免踩踏事件发生。

6.3.10 党政机关宿舍楼（区）的主要出入口应设置视频图像采集装置，视频监视和回放图像应清楚辨别进出人员体貌特征；宜设置人脸识别装置，对异常对象出入实现提示预警；宜设置出入口控制装置；应配置视频实时智能分析，对夜晚翻越宿舍围墙行为预警。

6.3.11 党政机关宿舍楼（区）的值班室应设置紧急（一键）报警，发出的报警信号应传送至24小时有人值守的门卫室（传达室）和安防监控中心（室）。

6.3.12 党政机关建筑物应配备电气火灾监控探测器和断路器，应在发生电气漏电、过流过载、过压欠压、短路、打火等情况时根据预先设定的参数主动告警和断路保护。

6.3.13 党政机关大院内建筑工地、陡坡、水池、楼梯等易发生危险的地方应设置视频图像采集装置，视频监视和回放图像应能清晰显示监视区域内人员活动情况；宜对一些危险动作如翻越护栏、涉水等行为进行识别与告警。

6.3.14 公文交换中心、数据中心、案件管理中心出入口应设置出入口控制装置和视频图像采集装置，视频监视和回放图像应能清晰显示进出人员的面部特征，其内部应设置视频图像采集装置、入侵探测装置，视频监视和回放图像应能清晰显示室内人员活动情况，入侵探测装置能对入侵行为探测报警。

6.3.15 枪支弹药存放场所等应设置视频图像采集装置，视频监视和回放图像应能辨别进出人员体貌特征，清晰显示人员活动情况。枪支（弹药）库其他要求应符合GA 1016的相关规定。

6.3.16 食堂操作间、配餐间、留样间和储藏室的出入口应设置视频图像采集装置，视频监视和回放图像应能辨别进出人员体貌特征。

6.3.17 食堂操作间、配餐间、留样间、储藏室、就餐区宜设置视频图像采集装置，视频监视和回放图像应能清晰显示人员活动情况。

6.3.18 食堂操作间、配餐间、留样间、储藏室、就餐区宜设置操作人员规范着装、规范操作的智能识别监控系统，对未戴帽子、未戴口罩、未穿工作服、未佩戴工牌、未熄火离岗等行为进行监测告警。

6.3.19 财务室、档案室、资料室、机要室、保密室应设置入侵探测装置或具有入侵探测功能的视频图像采集装置。财务室、档案室应设置紧急（一键）报警装置，报警信号应传送至安防监控中心（室）。

6.3.20 配电室、锅炉房、水泵房等水电气热等设备间应设置入侵探测装置或具有入侵探测功能的视频图像采集装置，并设置紧急（一键）报警装置，报警信号应传送至安防监控中心（室）。

6.3.21 机动车停车场、非机动车停车区应设置视频图像采集装置，视频监视和回放图像应能辨别监视区域内人员和车辆活动情况。

6.3.22 党政机关设置有停车场的，宜根据情况设置对超速行为进行警示的电子信息提示装置。

6.3.23 安防监控中心（室）出入口应设置出入口控制装置和视频图像采集装置，视频监视和回放图像应能清晰显示进出人员的面部特征，其内部应设置紧急（一键）报警和视频图像、音频采集装置，视频监视和回放图像应能清晰显示值守人员活动情况，紧急报警信号应传动到属地公安接处警平台。

6.3.24 党政机关安全防范的重点部位宜设置电子巡查装置。宜建立安防场地、设施、设备自动巡检系统，自动发现安防隐患，如消防通道占用、感应设备视效等，弥补人工巡检不足。

6.3.25 党政机关安防监控中心（室）应设置治安反恐防范综合管理平台。

6.3.26 党政机关的安全防范系统应不低于GB/T 22239中规定第二级安全要求。

* 1. 常态二级防范要求
     1. 人力防范要求

7.1.1　党政机关每半年组织不少于一次的反恐怖防范或应急演练。

7.1.2　党政机关应每季度不少于一次反恐怖防范检查、督察。

7.1.3　党政机关上下班高峰时间，应至少保证党政机关出入口有2位安保人员值班待守。

7.1.4　安全保卫人员应对党政机关重点部位进行每日不少于10次的巡逻，并对宿舍开展每天不少于5次的夜间巡查。

* + 1. 实体防范要求

7.2.1　党政机关宜配备防爆罐、防爆毯、防毒面罩、毛巾、口罩等应急用品。

7.2.2　党政机关周界车辆出入口应配置减速带和限速标志。

7.2.3　党政机关设置有停车场的，应设置对行车路线、停车场位置、车位有指引或标识。应根据情况设置限速标识。

* + 1. 电子防范要求

7.3.1 具有独立院落的党政机关大院、 无院落的党政机关大楼的主出入口或门卫室（传达室）应设置安全检查区域，配备微剂量X射线安全检查设备、通过式金属探测门、手持式金属探测器，宜配备禁限带物品智能识别设备、爆炸物探测仪、液态物品检查仪等安全检查设备。

7.3.2 具有独立院落的党政机关大院周界应设置入侵探测装置或具有入侵探测功能的视频图像采集装置，探测范围应对周界实现有效覆盖，不得有盲区。

7.3.3 具有独立院落的党政机关大院出入口、无院落的党政机关大楼出入口应设置人脸识别视频图像采集装置，智能视频分析装置应对进入党政机关人员的人脸图像进行动态采集和图像比对，对党政机关出入口及周边人员徘徊、滞留可视频分析报警提示给门卫保安。宜将人脸图像发送到公安人脸识别系统做监视名单的人脸比对，对重点人员可视频分析报警；应设置访客人脸识别装置，配置读取身份证存储照片与持证人员人脸进行比对。

7.3.4 党政机关宿舍楼（区）的主要出入口应设置人脸识别装置，对异常对象出入实现提示预警；应设置出入口控制装置；应配置视频实时智能分析，对夜晚翻越宿舍围墙行为预警。

7.3.5 食堂操作间、配餐间、留样间、储藏室、就餐区应设置视频图像采集装置，视频监视和回放图像应能清晰显示人员活动情况。

7.3.6 党政机关设置有停车场的，应设置对超速行为进行警示的电子信息提示装置。

7.3.7 党政机关安全防范的重点部位应设置电子巡查装置。

7.3.8 党委、人大、政府、政协等党政机关应配备符合国家有关规定的固定式反无人机主动防御系统设备。

* 1. 常态一级防范要求
     1. 人力防范要求

8.1.1 安全保卫人员应对党政机关重点部位进行每日不少于12次的巡逻，其中夜间开展不少于6次的夜间巡逻。

8.1.2　党政机关应每两个月不少于一次反恐怖防范检查、督察。

* + 1. 实体防范要求

8.2.1 党政机关应配备防毒面罩、毛巾、口罩等应急用品。

8.2.2 办事大厅、接访场所出入口应设置软质导流围栏等隔离疏导设施。

* + 1. 电子防范要求

8.3.1 具有独立院落的党政机关大院出入口及周边和无院落的党政机关大楼出入口应符合以下要求：

* 1. 应设置人脸识别视频图像采集装置，智能视频分析装置应对进入党政机关人员的人脸图像进行动态采集和图像比对，对党政机关出入口及周边人员徘徊、滞留可视频分析报警提示给门卫保安。宜将人脸图像发送到公安人脸识别系统做监视名单的人脸比对，对重点人员可视频分析报警；
  2. 应设置对党政机关工作人员进行身份识别的出入口控制通道装置；
  3. 应设置访客人脸识别装置，配置读取身份证存储照片与持证人员人脸进行比对。

8.3.2 党政机关人员集中出入的主要通道和出入口应配置人员密度监测或检测设备设施，对拥挤情况告警提醒，避免踩踏事件发生。

8.3.3 食堂操作间、配餐间、留样间、储藏室、就餐区应设置操作人员规范着装、规范操作的智能识别监控系统，对未戴帽子、未戴口罩、未穿工作服、未佩戴工牌、不按要求操作、未熄火离岗等行为进行监测告警。

* 1. 非常态防范要求
     1. 非常态防范等级

9.1.1 非常态治安反恐防范按照采取措施的不同要求分为三个等级,从低到高依次为：三级非常态防范、二级非常态防范和一级非常态防范。

9.1.2 在重要会议、重大活动等重要时段应采取三级非常态防范措施，在获得重大治安案事件、恐怖袭击案事件等预警信息时应采取二级非常态防范措施，在发生重大治安案事件、恐怖袭击案事件时应采取一级非常态防范措施。

9.1.3 二级非常态防范要求应在三级非常态防范要求基础上加强，一级非常态防范要求应在二级非常态防范要求基础上加强。

* + 1. 非常态防范要求

一级、二级、三级非常态情况下的人力防范、实体防范、电子防范具体措施应根据本地区反恐怖工作领导小组具体要求落实。

* 1. 安全防范系统技术要求
     1. 一般要求

10.1.1 安全防范系统所用的设施设备、材料和装备器械等应符合国家、行业现行相关标准的要求，并经检验或认证合格。

10.1.2 安全防范管理平台应对系统内具有计时功能的设备进行校时，设备的时钟与北京时间误差应不大于5s。

10.1.3 安全防范系统应配置备用电源，保证入侵和紧急报警系统的应急供电时间应不小于8小时，视频监控系统关键设备的应急供电时间应不小于1小时，出入口控制系统执行装置正常运行的应急供电时间应不小于48小时。

10.1.4 防爆环境使用的安全防范设施，防爆等级应符合GB 3836.1的相关规定。

10.1.5 安全防范系统的各子系统应符合GB 55029的相关规定。

* + 1. 入侵和紧急报警系统

10.2.1 入侵和紧急报警系统应能探测入侵和紧急事件。系统报警后，安防监控中心或门卫值班室应能声、光指示，并能准确指示报警的位置。

10.2.2 入侵和紧急报警系统应符合以下要求：

1. 紧急（一键）报警宜具备视频/音频采集和对讲功能。
2. 入侵和紧急报警系统应采用两种以上对外报警信息传输方式。用于报警信息传输的电话线路上不应挂接其他设备。
3. 紧急（一键）报警触发后，系统应能发出声、光指示，并准确指示报警的位置，声报警装置报警声压室内不低于80dB（A），室外应不不低于100dB（A）。报警持续时间应不小于5分钟。
4. 紧急（一键）报警装置应具备防误报措施和自锁装置，在出现警情触发紧急按钮后不得自动复位，必须人工手动复位。
5. 紧急报警系统应设置2 个（含）以上独立防区紧急按钮，能识别测试报警和紧急报警，每季度进行定期测试。

10.2.3 系统应具备自检、防拆、防破坏、开路、短路、故障、断电报警等功能。应24h设防。

10.2.4 系统应与视频监控系统联动。

10.2.5 系统布防、撤防、故障和报警信息存储时间应大于或等于 90 天。

10.2.6 系统的安全等级应符合GB/T 32581—2016中规定的2级要求。。

* + 1. 视频监控系统

10.3.1 系统监视和回放图像的水平像素数应不小于1920，垂直像素数应不小于1080，图像帧率应不小于25 帧/秒

10.3.2 音视频数据应实时记录，保存时间应大于或等于 30天。反恐防范重点部位的音视频数据保存时间应大于或等于90天。

10.3.3 涉及公共安全重点区域的视频图像信息采集应符合 GB 37300 的相关规定。

10.3.4 具有探测报警功能的视频分析系统，应符合 GB/T 30147 的相关规定。

10.3.5 系统应与入侵和紧急报警系统联动。

10.3.6 在人员密集场所，宜使用具有密度监测功能的视频监控设备，监测人员密度，并根据密度阈值进行预警。

* + 1. 出入口控制系统

10.4.1 出入口控制系统应能对强行破坏、非法进入的行为发出报警信号，报警信号应与相关出入口的视频图像联动。

10.4.2 系统应满足人员逃生时的相关要求，当需要紧急疏散时，各闭锁通道应开启，保障人员迅速安全通过。

10.4.3 系统信息存储时间应大于或等于 180 天。

10.4.4 系统的安全等级应不低于GB/T 37078—2018中规定的2级要求。

* + 1. 电子巡查系统

10.5.1 电子巡查系统的巡查路线、巡查时间应能根据安全管理需要进行设定和修改。

10.5.2 系统巡查记录保存时间应大于或等于90天。

10.5.3 系统的其他要求应符合 GA/T 644 的相关规定。

* + 1. 安全检查系统

10.6.1 系统应能对爆炸物、武器、管制器具或其他违禁品进行探测、显示、报警和记录。

10.6.2 微剂量X射线安全检查设备应符合GB 15208.1、GB 15208.2的相关规定。

10.6.3 禁限带物品智能分析设备应能自动识别禁止和限制带入党政机关的物品，并能发出报警信息。

10.6.4 通过式金属探测门应符合GB15210的相关规定，宜集成人体测温装置，实现非接触体温监测，当温度超过预先设定的报警阈值时，应有声光及语音报警提示。

10.6.5 手持式金属探测器应符合GB 12899的相关规定。

10.6.6 爆炸物探测仪应符合GA/T 841的相关规定。

10.6.7 液态物品安全检查设备应满足下列要求：

1. 使用非侵入式检测技术，不需打开包装即可对玻璃、塑料、陶瓷、纸质材质容器以及简易金属包装内的液体进行检测；
2. 至少能够检测出汽油、煤油、油漆、稀料、香蕉水、松香水等易燃物品。

10.6.8 防爆毯、防爆罐应分别符合GA 69、GA 871的相关规定。

* + 1. 公共广播系统

10.7.1 公共广播系统应能够根据不同的事件，进行相应的应急语音告警。

10.7.2 公共广播系统应能够在发生事件时，通过语音进行应急指挥与人员疏散。

10.7.3 公共广播系统应符合GB 50526的相关规定。

* + 1. 反无人机主动防御系统

10.8.1 系统发射功率和使用频段应符合国家有关规定。

10.8.2 系统应具备不间断探测预警和触发无线电阻断功能，系统探测范围应能覆盖党政机关防控区域。

10.8.3 系统应能自动24小时持续工作，无需人员值守；

10.8.4 系统不应对党政机关运行的系统及重要设施产生干扰，也不应对周边环境的通讯、网络、导航等信号产生干扰。

10.8.5 系统应与安防监控中心（室）联网，系统探测报警信息和故障信息应能传送到安全防范综合管理平台。

10.8.6 系统应取得国家安全防范报警系统产品质量监督检验中心或国家级无线电设备检测机构出具的检测报告。

* + 1. 电气火灾监控系统

10.9.1 电气火灾监控系统应满足下列要求：

1. 电气火灾监控系统探测器宜采用剩余电流式电气火灾监控探测器，其性能符合GB 14287.2的相关规定；
2. 电气火灾监控系统设备应符合GB 14287.1的相关规定。

10.9.2 电气火灾监控系统用短路器宜采用剩余电流动作断路器，其性能应满足下列要求：

* + - * 1. 瞬间电流分断能力大于或等于6kA
        2. 过流过载保护；超过额定电流5%状态下，10s内断路；超过额定电流35%的状态下，5s内断路；超过额定电流100%的状态下，1s内断路；
        3. 过压欠压保护：加载电压低于190V或大于250V时预警，持续10s大于263V短路器断路；
        4. 剩余电流动作断路器的其他技术要求应符合GB/T 16917.1的相关规定。
    1. 集成联网

10.10.1 党政机关安防监控中心（室）应配置治安反恐防范综合管理平台，实现对入侵和紧急报警、视频监控、出入口控制、电子巡查、安全检查、公共广播、电气火灾监控、反无人机主动防御等各安全防范子系统的集成与管理。

10.10.2 治安反恐防范综合管理平台应符合以下要求：

a) 联动控制功能：应能实现相关子系统的联动功能，入侵报警信号、紧急（一键）报警信号、出入口控制系统的报警信号等应能联动视频监控系统、平台的电子地图及应急预案等；

b) 人员管理功能：应能实现对安全保卫人员、安全检查人员、门卫值班室值班人员等人员的档案管理、排班管理、培训管理、考核管理、事件处置记录管理等；

c) 数据统计功能：应能对设备故障、入侵报警、紧急（一键）报警、电气火灾预警、安全检查出的禁限带物品、维护保养等数据进行统计、分析，能自动生成相关报表；

d) 电子地图功能：应能实现在二维地图或三维地图上的报警弹窗及定位功能；

e) 预案管理功能：应具有分等级报警预案功能，并自动显示配置的预案内容；

f) 系统校时功能：平台应设置独立的NTP授时服务器，能对系统及设备的时钟进行自动校时。

g) 系统运维功能：应能对系统及设备的日常运行状态实时监测，故障修复闭环管理，并形成相关记录。

h) 应急指挥管理功能：应急情况下，应能通过电子地图报警定位、视频联动和应急计划、预案内容，快速调度应急物资和安全保卫人员。

i) 非常态管理功能：平台应能提供紧急状态下的快捷操作，快速向公安等有关部门报告，并自动联络医疗急救部门。

10.10.3 安全防范管理平台的故障不应影响各子系统的正常运行，某一子系统的故障不应影响其他子系统的正常运行。

10.10.4 视频监控系统应留有与公共安全视频图像信息共享交换平台联网的接口，联网信息传输、交换、控制协议应符合GB/T 28181的相关规定，联网信息安全应符合GB 35114的相关规定。

1. （规范性）  
   党政机关常态人力防范措施
   1. 党政机关常态人力防范措施应符合表A.1的规定。

表A.1 党政机关常态人力防范措施

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 项目 | | 配设要求 | 设置标准 | | |
| 一级重点目标 | 二级重点目标 | 三级重点目标 |
| 1 | 反恐怖防范工作领导机构 | 责任领导 | 法定代表人为第一责任人 | ● | ● | ● |
| 2 | 责任部门 | 党政机关保卫部门 | ● | ● | ● |
| 3 | 专职联络员 | 指定联络员 1名 | ● | ● | ● |
| 4 | 办公室 | 设在保卫部门，由专职保卫干部、在编工作人员和机关内部各单位指定的安保负责人组成 | ● | ● | ● |
| 5 | 安全保卫负责人 | 内部各单位指定人员 | ● | ● | ● |
| 6 | 人力防范管理制度 | 背景审查与行为评估制度 | 公安机关出具的无违法犯罪记录的证明材料 | ● | ● | ● |
| 7 | 值守与巡查制度 | 在党政机关门口、供水、供电、控制中心等重要部位开展值守、巡查 | ● | ● | ● |
| 8 | 人员与物品检查制度 | 对进入党政机关的人员及携带物品进行安全检查 | ● | ● | ● |
| 9 | 防范、应急联动制度 | 与当地公安部门建立防范、应急联动机制 | ● | ● | ● |
| 10 | 教育与培训制度 | 对安保力量及相关员工进行反恐怖防范知识、技能的教育、培训 | ● | ● | ● |
| 11 | 安全防范与应急演练制度 | 每年组织不少于一次的反恐怖防范或应急演练 |  |  | ● |
| 12 | 每半年组织不少于一次的反恐怖防范或应急演练 | ● | ● |  |
| 13 | 检查与督察制度 | 每半年不少于一次反恐怖防范检查、督察，落实反恐怖防范措施和电子防范、实体防范设备（设施）装备 | ● | ● | ● |
| 14 | 每季度不少于一次反恐怖防范检查、督察 |  | ● |  |
| 15 | 两个月不少于一次反恐怖防范检查、督察 | ● |  |  |
| 16 | 考核与奖惩制度 | 定期对安保力量及相关员工的反恐怖防范工作进行考核、奖惩 | ● | ● | ● |
| 17 | 安保力量 | 专职保安员和专职门卫 | 年龄原则上不得超过45周岁，退伍军人和警校毕业生比例不低于20% | ● | ● | ● |
| 18 | 取得保卫管理员职业资格证书 | ● | ● | ● |
| 19 | 属地管理原则到辖区公安派出所备案 | ● | ● | ● |
| 20 | 取得《保安员证》或职业资格证书 | ● | ● | ● |
| 21 | 必要的护卫器械，并建立使用保管制度 | ● | ● | ● |
| 22 | 应培训上岗，掌握党政机关安全管理、治安保卫的基本技能 | ● | ● | ● |
| 23 | 每日不少于 8 次的巡逻，其中夜间开展不少于4次的夜间巡逻 |  |  | ● |
| 24 | 节假日在岗执勤 | ● | ● | ● |
| 25 | 上下班高峰时间，应至少保证党政机关出入口有2位安保人员值班待守 | ● | ● |  |
| 26 | 党政机关重点部位进行每日不少于10次的巡逻，并对宿舍开展每天不少于5次的夜间巡查 |  | ● |  |
| 27 | 每日不少于12次的巡逻，其中夜间开展不少于6次的夜间巡逻 | ● |  |  |
| 28 |  | 门卫室（传达室、值班岗亭） | 24h 有人值守 | ● | ● | ● |
| 注：表中“●”表示“应配置”，“○”表示“宜配置”。 | | | | | | |

1. （规范性）  
   党政机关常态防范设施配置
   1. 党政机关常态防范设施配置应符合表B.1的规定。

表B.1 党政机关常态防范设施配置

| 序号 | 重点部位 | | 防范设施 | | 配置要求 | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 一级重点目标 | 二级重点目标 | 三级重点目标 |
| 1 | 具有独立院落的党政机关大院 | 周边 | 实体防范设施 | 安全警示牌和人行、分隔、停车等设施、警务室、治安岗亭 | ● | ● | ● |
| 2 | 视频监控系统 | 视频图像采集装置 | ● | ● | ○ |
| 3 | 周界 | 实体防范设施 | 实体围墙或栅栏 | ● | ● | ● |
| 4 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 5 | 入侵和紧急报警系统 | 入侵探测装置 | ● | ● | ● |
| 6 | 出入口 | 实体防范设施 | 隔离栏、隔离墩或升降柱等硬质防冲撞设施、减速带和限速标志 | ● | ● | ● |
| 7 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 8 | 出入口控制系统 | 出入口控制装置 | ● | ● | ○ |
| 9 | 人体测温设备 | 人体测温设备 | ● | ● | ● |
| 10 |  | 健康信息码核验设备 | ● | ● | ● |
| 11 | 主要道路、广场 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 12 | 党政机关 | 周边公共停车场、广场、道路等室外公共区域 | 实体防范设施 | 安全警示牌、交通标志标牌标线、交通信号灯、人行设施、分隔设施、停车设施和减速带 | ● | ● | ● |
| 13 | 无院落的党政机关大楼 | 周界 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 14 | 出入口 | 实体防范设施 | 隔离栏、隔离墩或升降柱等硬质防冲撞设施、减速带和限速标志 | ● | ● | ● |
| 15 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 16 | 人体测温设备 | 人体测温设备 | ● | ● | ● |
| 17 | 健康信息码核验设备 | 健康信息码核验设备 | ● | ● | ● |

表B.1　 党政机关常态防范设施配置（续）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 重点部位 | | 防范设施 | | 配置要求 | | |
| 一级重点目标 | 二级重点目标 | 三级重点目标 |
| 18 | 门卫室（传达室），警务室，值班岗亭 | 内部 | 入侵和紧急报警系统 | 紧急（一键）报警 | ● | ● | ● |
| 19 | 安全检查区域 | 安全检查系统 | 微剂量X射线安全检查设备 | ● | ● | ● |
| 20 | 通过式金属探测门 | ● | ● | ● |
| 21 | 手持式金属探测器 | ● | ● | ● |
| 22 | 禁限带物品智能识别设备 | ● | ○ | ○ |
| 23 | 爆炸物探测仪 | ● | ○ | ○ |
| 24 | 液态物品检查仪 | ● | ○ | ○ |
| 25 | 办事大厅、接访场所 | 接待席位、接待席位、信访接待席位、对外接待处 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 26 | 声音采集装置 | 声音采集装置 | ● | ● | ● |
| 27 | 入侵和紧急报警系统 | 紧急（一键）报警 | — | ● | ● |
| 28 | 出入口 | 实体防护设施 | 软质导流围栏等隔离疏导设施 | ● | ○ | ○ |
| 29 | 公文交换中心、数据中心、案件管理中心 | 出入口 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 30 | 出入口控制装置 | 出入口控制装置 | ● | ● | ● |
| 31 | 内部 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 32 | 入侵和紧急报警系统 | 入侵探测装置 | ● | ● | ● |
| 33 | 财务室、机要室、保密室 机要室、保密室 | 出入口 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 34 | 内部 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 35 | 入侵和紧急报警系统 | 入侵探测装置 | ● | ● | ● |
| 36 | 紧急（一键）报警 | — | ● | ● |
| 37 | 档案室、资料室 | 出入口 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 38 | 内部 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 39 | 入侵和紧急报警系统 | 入侵探测装置 | ● | ● | ● |
| 40 | 机关工作人员宿舍楼（区） | 出入口 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 41 | 人脸识别装置 | ● | ● | ○ |
| 42 | 视频实时智能分析装置 | ● | ● | ● |
| 43 | 出入口控制装置 | 出入口控制装置 | ● | ● | ○ |
| 44 | 主要通道 | 视频监控系统 | 人员密度监测装置 | ● | ● | ● |
| 45 | 楼顶 | 实体防护设施 | 警示标志 | ● | ● | ● |
| 46 | 值班室 | 入侵和紧急报警系统 | 紧急（一键）报警 | ● | ● | ● |
| 47 | 党政机关建筑物 | | 电气火灾监控系统 | 电气火灾监控探测器和断路器 | ● | ● | ● |
| 48 | 食堂（餐厅）操作间、配餐间、留样间、储藏室、就餐区 | 出入口 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 49 | 内部 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 50 | 智能识别监控系统 | 监测告警装置 | ● | ● | ○ |

表B.1　 党政机关常态防范设施配置（续）

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 重点部位 | | | 防范设施 | | 配置要求 | | |
| 一级重点目标 | 二级重点目标 | 三级重点目标 |
| 51 | 财务室、档案室、资料室、机要室、保密室、数据中心、案件管理中心、安防监控中心（室）、水电气热等设备间 | | 与外界相通的窗户 | 实体防护设施 | 钢制栅栏 | ● | ● | ● |
| 52 | 出入口 | 实体防护设施 | 防盗安全门 | ● | ● | ● |
| 53 | 枪支弹药存放场所 | | | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 54 | 水、电、气、热、通信等设备间 | | 出入口 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 55 | 内部 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 56 | 入侵和紧急报警系统 | 入侵探测装置 | ● | ● | ● |
| 57 | 安防监控中心（室） | | 出入口 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 58 | 出入口控制装置 | 出入口控制装置 | ● | ● | ● |
| 59 | 内部 | 入侵和紧急报警系统 | 紧急（一键）报警 | ● | ● | ● |
| 60 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 61 | 音频采集装置 | 音频采集装置 | ● | ● | ● |
| 62 | 机动车停车场、非机动车停车区 | | 机动车停车场 | 实体防护设施 | 对行车路线、停车场位置、车位有指引或标识、限速标识。 | ● | ● | ○ |
| 63 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 64 | 行车管控系统 | 电子信息提示装置 | ● | ● | ○ |
| 65 | 非机动车停车区 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 66 | 党政机关安全防范重点区域 | | | 电子巡查系统 | 电子巡查装置 | ● | ● | ○ |
| 67 | 自动巡检系统 | ● | ● | ○ |
| 68 | 党政机关大门和人员行进主要道路、办公楼和宿舍楼通道 | | | 实体防范设施 | 路灯，亮化率达100% | ● | ● | ● |
| 69 | 危险区域 | 办公楼顶、宿舍楼顶、水塘边等 | | 告警系统 | 警示标志 | ● | ● | ● |
| 70 | 防护装置 | ● | ● | ● |
| 71 | 视频监控系统 | 视频图像采集装置 | ● | ● | ● |
| 72 | 视频智能分析系统 | ● | ● | ● |
| 73 | 保卫执勤岗位 | | | 防毒面罩、毛巾、口罩等应急用品 | | ● | ○ | — |
| 74 | 防爆罐、防爆毯 | | ● | ○ | — |
| 75 | 党委、人大、政府、政协办公建筑物 | | | 固定式反无人机主动防御系统 | | ● | ● | — |
| 注：表中“●”表示“应配置”，“○”表示“宜配置”，“—”表示不要求。 | | | | | | | | |

参 考 文 献

[1] 《中华人民共和国反恐怖主义法》 中华人民共和国主席令 第三十六号

[2] 《中华人民共和国突发事件应对法》 中华人民共和国主席令 第六十九号

[3] 《企业事业单位内部治安保卫条例》 中华人民共和国国务院令 第 421 号

[4] GB/T 38961 个人健康信息码　参考模型

[5] 《湖南省反恐怖防范管理规范》