ICS 13.310
CCS A 90

DB5117

四 川 省 （ 达 州 市 ） 地 方 标 准

DB5117/T 56—2022

反恐怖防范管理基本规范

Basic specification for anti-terrorism precaution management

2022－05－19 发布　　2022－05－25 实施

达州市市场监督管理局　　发 布

目　　次

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。

本文件与《党政机关反恐怖防范规范》、《教育机构反恐怖防范规范》等系列标准共同构成达州市反恐怖防范标准体系。本文件是对反恐怖防范重点目标的管理通用要求，可以独立使用。《党政机关反恐怖防范规范》等系列标准是对特定反恐怖防范重点单位的反恐怖特殊要求，与本文件配套使用。

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

本文件由达州市公安局提出。

本文件由达州市反恐怖工作领导小组办公室归口。

本文件起草单位：达州市反恐怖工作领导小组办公室、四川省标准化研究院、中国电子科技集团公司电子科学研究院、中电科电科院科技有限公司、北京航空航天大学杭州创新研究院、中国电信股份有限公司达州分公司、中国移动通信集团四川有限公司达州分公司、中国联合网络通信有限公司达州分公司、北京至简墨奇科技有限公司、重庆紫光华山智安科技有限公司、太极计算机股份有限公司、成都易简云数科技有限公司、杭州海康威视数字技术股份有限公司、浙江宇视科技有限公司、浙江大华技术股份有限公司、四川易利数字城市科技有限公司。

本文件主要起草人：李森、叶春林、郭家彬、邓刚、况琳、彭维、毕严先、张瑞、吉祥、高启龙、任忠刚、陶建、赵胜、杨萌、郭庆浪、刘文辛、赵洲、何清、刘洋、黄军勇、杨保国、曹晔。

本文件为首次发布。

反恐怖防范管理基本规范

1 范围

本文件规定了反恐怖防范管理的术语和定义、反恐怖防范原则、重点目标分类和防范等级划分、重点目标重要部位、常态反恐怖防范、非常态反恐怖防范、应急准备要求、监督和检查。

本文件适用于达州市反恐怖防范重点目标的基本防范和管理，反恐怖防范一般目标可参照执行。

2 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 2887 计算机场地通用规范

GB/T 7027-2002 信息分类和编码的基本原则与方法

GB 10409 防盗保险柜（箱）

GB 12663 入侵和紧急报警系统 控制指示设备

GB 12664 便携式x射线安全检查设备通用规范

GB 12899 手持式金属探测器通用技术规范

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 15210 通过式金属探测门通用技术规范

GB/T 15408 安全防范系统供电技术要求

GB 17565 防盗安全门通用技术条件

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 22240 信息安全技术 网络安全等级保护定级指南

GB 24539 防护服装 化学防护服通用技术要求

GB/T 25724 公共安全视频监控数字视音频编解码技术要求

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 31167-2014 信息安全技术 云计算服务安全指南

GB/T 31488 安全防范视频监控人脸识别系统技术要求

GB/T 32581 入侵和紧急报警系统技术要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB 50348 安全防范工程技术标准

GB 50394 入侵报警系统工程设计规范

GB 50395 视频安防监控系统工程设计规范

GB 50396 出入口控制系统工程设计规范

GB 50526 公共广播系统工程技术规范
GA 68 警用防刺服
GA 69 防爆毯
GA/T 143 金库门通用技术条件
GA 294 警用防暴头盔
GA 308 安全防范系统验收规则
GA/T 367 视频安防监控系统技术要求
GA/T 394 出入口控制系统技术要求
GA 422 警用防暴盾牌
GA/T 594 保安服务操作规程与质量控制
GA 614 警用防割手套
GA/T 644 电子巡查系统技术要求
GA 667 防爆炸透明材料
GA/T 761 停车库（场）安全管理系统技术要求
GA 844 防砸透明材料
GA 883 公安单警装备 强光手电
GA 926 微剂量透射式X射线人体安全检查设备通用技术要求
GA/T 1126 近红外人脸识别设备技术要求
GA/T 1127 安全防范视频监控摄像机通用技术要求
GA/T 1132 车辆出入口电动栏杆机技术要求
GA/T 1145 警用约束叉
GA/T 1260 人行出入口电控通道闸通用技术要求
GA/T 1343 防暴升降式阻车路障
MH/T 2008 无人机围栏

3 术语和定义

下列术语和定义适用于本文件。

3.1

恐怖袭击 terrorist attack

极端人员人为制造的针对但不限于平民及民用设施的不符合道义的攻击方式，常见形式包括但不限于砍杀、投毒、纵火、撞击、爆炸、枪击等内容。

3.2

反恐怖防范 anti-terrorism precaution

为避免恐怖袭击伤害，运用科技手段、防护硬件、软件和实施相关管理制度和措施等，以避免、探测、延迟和应对恐怖威胁的行为。

3.3

反恐怖防范系统 anti-terrorism precaution system

以维护公共安全为目的，针对常态和非常态形势下反恐怖防范需求，综合运用人防、物防、技防、数据防和制度防手段而构成的反恐怖防范体系。

3.4

常态反恐怖防范 normal anti-terrorism precaution

在日常的安全管理工作中，采用一般性、常规性措施的反恐怖防范。

3.5

非常态反恐怖防范 non-normal anti-terrorism precaution

在特殊时期（如重大活动期间、重要时段）或应对恐怖袭击时，采取特别措施的反恐怖防范。

3.6

反恐怖主义工作领导机构及其办事机构 anti-terrorism work leading institution and agency

市、区（县）级反恐怖工作领导小组及其办公室。除特殊声明，本文件所指的反恐怖主义工作领导机构及其办事机构指达州市及各区（县）反恐怖工作领导小组及其办公室。

3.7

反恐怖防范重点目标 key target of anti-terrorism precaution

由公安机关会同有关部门确定，并经本级反恐怖主义工作领导机构备案的，存在遭受恐怖袭击的可能性较大以及遭受恐怖袭击可能造成重大的人身伤亡、财产损失或者社会影响的单位、场所、活动、设施等，也称防范恐怖袭击的重点目标或反恐重点目标，简称为重点目标。

3.8

反恐怖防范一般目标 general target of anti-terrorism precaution

除反恐怖防范重点目标以外，为避免恐怖袭击或伤害，需要予以防范的单位、场所、活动、设施等目标，简称为一般目标。

3.9

反恐怖防范重点目标重要部位 major sections of key target for anti-terrorism

反恐怖防范重点目标的各个组成部分中对国家安全、公共安全和人民生命财产安全等有显著影响的部位，简称为重点目标重要部位。

3.10

反恐怖防范重点目标重要岗位人员 important post staff of anti-terrorism key target major sections

对可能危及重点目标的安全负有直接责任和管理责任的人员，简称为重要岗位人员。

3.11

反恐怖防范重点目标责任主体 responsibility subject of anti-terrorism key target

反恐怖防范重点目标的经营、管理单位，包括机关、企事业单位等，简称为重点目标责任主体。

3.12

人力防范 personnel protection

执行反恐怖防范任务的具有相应素质人员或人员群体的一种有组织的防范行为，包括人、组织和管理等，简称为人防。

3.13

实体防范 physical protection

能威慑、阻止、延迟恐怖袭击事件发生的各种实体防护手段，包括利用现有建（构）筑物、加固建（构）筑物，增设屏障、器具、设备、改进防护系统等，简称为物防。

3.14

技术防范 technical protection

利用各种电子信息设备组成系统或网络以提高探测、延迟、反应等能力及防护功能的反恐怖防范手段，简称为技防。

3.15

数据防范 data protection

为避免因数据泄露而造成的恐怖袭击或伤害而采取的安全技术手段，如数据加密、数据防火墙、数据脱敏等，简称为数据防。

3.16

制度防范 system protection

为确保人防、物防、技防、数据防的有效实施并达到预期目的而制定的各项规章制度，如管理标准、工作标准和技术标准等，简称为制度防。

3.17

管理标准 administrative standard

对反恐怖防范工作中需要协调统一的管理事项所制定的标准化文件。

注：管理事项主要指在反恐怖防范工作中，所涉及人防管理、物防管理、技防管理相关联的管理制度， 如人防中安保人员管理、物防中安防设备设施管理、技防中视频监控信息管理等。

3.18

工作标准 duty standard

对反恐怖防范工作中需要协调统一的工作事项所制定的标准化文件。

注：工作事项主要指在执行相应管理标准和技术标准时与工作岗位的职责、岗位人员基本技能、工作内容、要求与方法、检查与考核等有关的重复性事物和概念。

3.19

技术标准 technical standard

对反恐怖防范工作中需要协调统一的技术事项所制定的标准化文件。

注：本文件所指的技术标准主要指物防中所使用安防设备设施的产品标准、技防中所涉及的工程标准、验收规范等。

3.20

安保力量 security forces

实施安全防范系统的操作、管理、维护和反恐怖事件响应的专（兼）职人员和队伍。

3.21

保安员 security guard

专职承担门卫、巡逻、守护、安全检查、秩序维护、安全技术防范和安全风险评估等职能，并经专业培训取得资格证的安全保卫人员。

3.22

危险物品 dangerous goods

可能危及人身安全和财产安全的物品，如民用爆炸物品、易燃性物品、危险化学品、核与放射性物品、毒害性物品、腐蚀性物品、传染病病原体等。

3.23

恐怖威胁预警 early-warning of terrorism threats

反恐怖主义工作领导机构以及公安机关等部门对有关情报信息进行筛查、研判、核查、监控，认为有发生恐怖事件危险所发出的预警。

3.24

恐怖威胁预警响应 early-warning response of terrorism threats

反恐怖防范重点目标根据恐怖威胁预警等级信息而采取的相应级别的应对措施。

3.25

周界 perimeter

建筑体或建筑群外部界面，包括独立院落的指独立院落周边外墙，单体建筑物的指建筑物外立面及天顶，合用建筑体（即与其他单位合用）的指建筑体周界及与其它单位交界处。

4 反恐怖防范原则

4.1 反恐怖防范工作应遵循“属地负责，逐级监管”，“谁主管，谁负责”，“谁经营，谁负责”的原则。

4.2 反恐怖防范工作应在反恐怖主义工作领导机构统一领导和指挥下开展，公安机关、有关行业主管部门履行安全管理、指导、监督和检查责任。

5 重点目标分类和防范等级划分

5.1 重点目标分类

重点目标的分类按目标的规模、性质及其遭受恐怖袭击后可能造成的人员伤亡、财产损失和社会影响等要素划分为以下几类：

a） 政治敏感类：包括党政机关、广电传媒和涉外机构等政治影响大的敏感机构；

b) 人员密集类：包括教育机构、科研机构、医疗卫生机构、商场超市、酒店宾馆、游乐场所、园林公园、旅游景区、城市广场、步行街市、大型专业市场、体育场馆、影视剧院、会展场馆、宗教活动场所等公众聚集密度大的场所；
c) 交通枢纽类：包括民用机场、船舶港口码头、公交客运站场、隧道桥梁、铁路轨道交通等；
d) 基础设施类：包括水、电、粮、油、气、通信、信息、金融、邮政物流等关系国计民生的重要基础设施（包括物资储备仓库）；
e) 涉危涉爆类：包括危险化学品、民用爆炸物品、核与放射性物品等生产、经营、运输、使用、检测、储存、废弃处置的单位、场所及设施；
f) 大型活动类：重大活动、群体性活动；
g) 商住建筑类：包括住宅小区、高层建筑；
h) 特殊类：其他需要反恐怖防范的重点单位、场所、活动、设施等。

5.2 防范等级划分

5.2.1 防范分类

反恐怖防范等级按防范管理性质分为常态反恐怖防范和非常态反恐怖防范两类。

5.2.2 非常态反恐怖防范等级

非常态反恐怖防范等级按恐怖威胁预警响应的要求分为四级：
a) 四级非常态反恐，Ⅳ级（一般），用蓝色表示；
b) 三级非常态反恐，Ⅲ级（较大），用黄色表示；
c) 二级非常态反恐，Ⅱ级（重大），用橙色表示；
d) 一级非常态反恐，Ⅰ级（特别重大），用红色表示。

6 重点目标重要部位

6.1 确定原则

重点目标责任主体应根据自身实际情况，将对国家安全、公共安全和人民生命财产安全等有显著影响的部位确定为重点目标重要部位；重点目标责任主体可根据实际情况对重要部位划分等级，报行业主管部门、属地公安机关和反恐怖主义工作领导机构的协事机构备案，并接受监督、检查、指导。

6.2 重要部位

重点目标重要部位主要包括：
a) 人员密集区域：在一定时间段内聚集人数较多、密度较大的场所；
b) 系统的关键部位：如供电、供水、供气、供油以及网络通信、监控、调度、通风、空调、出入口等；
c) 涉危险物品区域：生产、使用、运输、保管危险化学品、民用爆炸物品，核与放射性物品等的部位；
d) 涉密部位：如机密档案室、信息中心等；
e) 其他重要部位：如停车场（库）、停机坪等。

7 常态反恐怖防范

7.1 人防

7.1.1 设置原则

重点目标责任主体应根据有关规定，结合目标的规模、人员数量、重要部位分布等安全防范工作实际需要，配备足够的安保力量，明确常态安保力量人数。

7.1.2 人防组织

重点目标责任主体应指定专门的工作机构，并明确责任领导、责任部门、联络员及相关岗位。

7.1.3 人防配置

重点目标的人防配置应符合表1要求。

表1 人防配置表

序号	项目		配设要求	设置要求
1	工作机构		组织健全、分工明确、责任落实	应设
2	责任领导		主要负责人为第一责任人	应设
3	责任部门		安保部门兼任或独立	应设
4	联络员		指定联络员1名	应设
5	安保力量	技防岗位	重要技防设施	应设
6		固定岗位	监控中心、出入口等重要部位	应设
7		重要部位	重要部位	应设
8		网络与信息安全管理岗位	网络安全维护	应设
9		机动岗位	备勤、周界	应设

7.1.4 人防管理

7.1.4.1 重点目标责任主体应建立与反恐怖主义工作领导机构、公安机关及行业主管部门的工作联系，定期报告反恐怖防范措施落实情况。发现可疑人员、物品应及时向公安机关报告。

7.1.4.2 重点目标责任主体应：

a) 加强反恐怖防范教育宣传、开展应急技能训练和应急处突演练，提升人防技能；
b) 对重要岗位人员开展背景审查、建立人员档案并备案，确保用人安全；
c) 加强门卫与寄递物品管理、开展巡查与安检、视频监控系统的值班监看和运维，确保人防职责落实；
d) 加强检查督导，开展制度体系实施与改进，提高人防效率。

7.1.4.3 重点目标应指定专职联络员，联络员应确保 24 h 通信畅通。联络员的配置和变更，应及时向行业主管部门、属地公安机关和反恐怖主义工作领导机构的办事机构备案。

7.1.5 安保力量要求

重点目标安保力量应符合以下要求：

a) 反恐怖防范工作机构设置、责任领导、责任部门、联络员及相关岗位人员的设定及变更应向反恐怖主义工作领导机构、公安机关及行业主管部门备案；
b) 保安员应符合 GA/T 594 的相关要求，承担保安职责；
c) 保安员应持证上岗，并掌握必备的专业知识和技能；
d) 反恐怖防范专（兼）职工作人员应熟悉重点目标内部和周边环境、消防通道和各类疏散途径；
e) 反恐怖防范专（兼）职工作人员应熟悉本重点目标反恐怖防范工作情况及相关规章制度、应急预案等；
f) 应对涉恐突发事件，配合反恐怖主义工作领导机构、公安机关、有关行业主管部门开展工作；
g) 网络与信息安全管理人员应具有计算机相关专业技术能力，熟悉网站和信息系统的安全机制，按网络安全管理制度开展网络安全防范工作；
h) 其他需承担的反恐怖防范工作。

7.2 物防

7.2.1 配置原则

7.2.1.1 应纳入重点目标工程建设总体规划，并应同步设计、同步建设、同步运行。
7.2.1.2 使用的设备和设施应经法定机构检验或认证合格。

7.2.2 物防组成

重点目标物防包括实体防护设施、个人应急防护装备、公共应急防护装备及设施、行包寄存设施、巡逻船舶等。

7.2.3 物防配置

重点目标的物防配置应符合表2要求。

表2 物防配置表

序号	项目		安放区域或位置	设置要求
1	实体防护设施	机动车阻挡装置	主要出入口（无实体防护屏障）	应设
2		防机动车冲撞或隔离设施	主要出入口、受机动车冲击后容易受到重大伤害的重要部位	应设
3		防盗安全门、金属防护门或防尾随联动互锁安全门、金库门	监控中心等重要部位出入口	应设
4		防盗保险柜、防盗保险箱	财务室、收银处	应设
5		围墙或栅栏	周界	应设
6		人车分离通道	出入口	应设
7		刀片刺网	周界围墙	宜设
8		人行出入口通道闸	出入口	宜设
9		对讲机、强光手电、防护棍棒	保安员、门卫室、值班室、监控中心、消控中心	应设
10	个人应急防护装备	毛巾、口罩	各工作区域	宜设
11		防护面罩	各工作区域	宜设

表 2 （续）

序号	项目		安放区域或位置	设置要求
12	个人应急防护装备	防暴盾牌、钢叉	监控中心或保安装备存放处、门卫室、值班室	应设
13		防暴头盔、防割（防刺）手套、防刺服	监控中心或保安装备存放处	应设
14		化学防护服、铅衣及相关药品	监控中心或保安装备存放处	宜设
15	公共应急防护装备及设施	防爆毯（含防爆围栏）	监控中心或保安装备存放处	应设
16		应急警报器	监控中心、传达登记处、门卫处、重要部位、人员密集区域	应设
17		灭火器	各工作区域	应设
18	行包寄存设施		出入口附近，距离重要部位>30 m	应设
19	巡逻船舶		水域	应设

7.2.4 物防要求

7.2.4.1 防护设备设施要求

重点目标物防配置的设备设施应符合以下要求：

a) 车辆出入口的电动栏杆应符合 GA/T 1132 的要求；
b) 机动车阻挡装置宜采用立柱式阻挡方式；若采用防暴升降式的阻挡装置时应符合 GA/T 1343 的要求；
c) 实体防护中使用的防爆炸玻璃应符合 GA 667 的要求，防砸玻璃应符合 GA 844 的要求；
d) 防盗安全门应符合 GB 17565 的要求；
e) 金库门应符合 GA/T 143 的要求；
f) 防盗保险柜（箱）应符合 GB 10409 的要求；
g) 人行出入口通道闸应符合 GA/T 1260 的要求；
h) 强光手电应符合 GA 883 的要求；
i) 防暴盾牌应符合 GA 422 的要求；
j) 防暴钢叉应符合 GA/T 1145 的要求；
k) 防暴头盔应符合 GA 294 的要求；
l) 防割（防刺）手套应符合 GA 614 的要求；
m) 防刺服应符合 GA 68 的要求；
n) 化学防护服应符合 GB 24539 的要求；
o) 防爆毯应符合 GA 69 的要求
p) 实体围墙或栅栏应符合以下要求：
    1) 实体围墙的结构应坚固，一般采用钢板网、钢筋网、钢筋混凝土预制板等结构形式；
    2) 钢栅栏的设置应符合消防的有关规定。

7.2.4.2 防护设备设施采购与维护

7.2.4.2.1 物防设备设施的采购应按采购管理制度开展，制定采购计划、选择合格供方和实施采购质量验收。

7.2.4.2.2 责任部门应有人负责物防设备设施维护工作，按设备设施档案制度建立台账和档案，并确

保台账和档案信息完善、准确， 设备设施有效。

7.2.4.2.3 制定设备设施的工作状态检查表，定期检查应按照设备设施的维护保养要求进行，定期检查的间隔不应超过三个月，发生以下情况应马上组织相关检查：

a) 进入或可能会进入非常态反恐怖防范时；
b) 应急演练前；
c) 物防管理人员交接；
d) 恶劣天气；
e) 重大活动；
f) 其他对物防设备有重大影响的情况。

7.2.4.2.4 发现失效的物防设备设施应及时维修或更换，对有效使用期内失效的设备设施应进行原因分析，制定纠正和预防措施。

7.2.4.2.5 各物防设备设施应制定操作规程，使用、维护时应遵循操作规程的要求，操作规程应包括：

a) 规程适用的设备或设施；
b) 责任部门和定置管理要求；
c) 使用步骤；
d) 维护要求；
e) 注意事项（必要时）。

7.3 技防

7.3.1 建设原则

7.3.1.1 应纳入重点目标工程建设总体规划，并应同步设计、同步建设、同步运行。

7.3.1.2 使用的设备和设施应经法定机构检验或认证合格。

7.3.2 技防组成

技防系统应包括监控中心、视频监控系统、入侵报警系统、出入口控制系统、停车库（场）管理系统、电子巡查系统、公共广播系统、无线通信对讲指挥调度系统、防爆安检系统、通讯显示记录系统、无人机监控系统等。

7.3.3 技防配置

重点目标的技防配置应符合表3要求。

表3 技防配置表

序号	项目		安装区域或覆盖范围	设置要求
1	监控中心		根据实际情况确定	应设
2	视频监控系统	摄像机	与外界相通的出入口	应设
3			周界及内部主要通道	应设
4			办公楼大厅、电梯等候区	应设
5			电梯轿厢、自动扶梯口	应设
6			各楼梯口、通道	应设
7			人员密集区域	应设

表 3 （续）

序号	项目		安装区域或覆盖范围	设置要求
8	视频监控系统	摄像机	区域内供参观、开放区域	应设
9			食堂（餐厅）及其出入口	应设
10			100人（座）以上的会议厅（室、礼堂）	应设
11			水、气、电、油、网络通讯、空调控制区域、新风口	应设
12			危险物品存放处	应设
13			枪支、弹药存放场所及其出入口	应设
14			寄递物品收发处、传达登记处、门卫处	应设
15			停车库（场）、停机坪及其主要通道和出入口	应设
16			防范目标高空瞭望处	应设
17			监控中心	应设
18			电脑中心机房、财务室、档案馆（库）、贵重物品存放场所	应设
19		声音复核装置	周界、主要出入口	宜设
20			危险物品存放处	应设
21			枪支、弹药存放场所	应设
22			寄递物品收发处、传达登记处、门卫处	宜设
23		视频智能分析系统	监控中心、图像采集前端	宜设
24		人脸识别系统	监控中心、图像采集前端	宜设
25		机动车牌照识别系统	停车库（场）	宜设
26		控制、数据存储、显示装置	监控中心	应设
27	入侵报警系统	入侵探测（报警）器	周界	应设
28			水、气、电、油、网络通讯控制区域	应设
29			枪支、弹药存放处	应设
30			危险物品存放处	应设
31			电脑中心机房、财务室、档案馆（库）、贵重物品存放场所	应设
32		紧急报警装置（一键报警）	传达登记处、门卫处、重要部位、人员密集区域、监控中心	应设
33		报警控制器	监控中心及相关的独立设防区域	应设
34		终端图形显示装置	监控中心	宜设
35	出入口控制系统		水、气、电、油、网络通讯、空调主要控制区域	应设
36			枪支、弹药存放处	应设
37			危险物品存放处	应设
38			监控中心	应设
39	出入口控制系统	虹膜识别系统	监控中心、图像采集前端	宜设
40		身份证验证系统	出入口	宜设
41	停车库（场）管理系统		停车库（场）	应设

表 3 （续）

序号	项目		安装区域或覆盖范围	设置要求
42	电子巡查系统		出入口	应设
43			周界	应设
44			重要部位和人员密集区域	应设
45	公共广播系统		区域全覆盖	应设
46	无线通信对讲指挥调度系统		区域全覆盖、监控中心	应设
47	通讯显示记录系统		服务、咨询电话、总机	宜设
48	防爆安检系统	X 射线物品安检机（或/和便携式）	出入口或重要部位	宜设
49		通过式金属探测门	出入口或重要部位	宜设
50		手持式金属探测器	出入口或重要部位	应设
51		X 射线人体安检门	出入口或重要部位	宜设
52		爆炸物探测仪	出入口或重要部位	宜设
53	无人机监控系统		区域全覆盖	宜设

7.3.4 技防要求

7.3.4.1 技防系统的总体要求应满足：

a) 技防建设应符合 GB 50348 的相关要求；
b) 技防系统的供电应符合 GB/T 15408 的相关要求；
c) 监控中心应符合 GB/T 2887 的相关要求。

7.3.4.2 技防各子系统的建设和使用应符合以下要求：

a) 视频监控系统应符合 GB 50395、GB/T 25724、GB/T 28181、GA/T 367 和 GA/T 1127 的要求；
b) 人脸识别系统应符合 GB/T 31488 和 GA/T 1126 的要求；
c) 入侵报警系统应符合 GB 12663、GB/T 32581 和 GB 50394 的要求；
d) 出入口控制系统应符合 GB 50396 和GA/T 394 的要求；
e) 停车库（场）管理系统应符合 GB 50396 和GA/T 761 的要求；
f) 电子巡查系统应符合 GA/T 644 的要求；
g) 公共广播系统应符合 GB 50526 的要求；
h) 防爆安检系统应符合 GB 12664、GB 12899、GB 15208.1、GB 15210 和 GA 926 的要求。

7.3.4.3 与外界相通的出入口等重点部位配置的摄像机应满足GA/T 1127 中规定的 C 类高清晰度及以上要求，具有宽动态、低照度、强光抑制等功能的机型，视频信息应与公安机关联网。

7.3.4.4 报警系统信息本地保存时间应不少于 180 d，并具备与公安机关联动的接口。

7.3.4.5 视频录像保存时间应不少于 90 d。

7.3.4.6 视频监控范围内的报警系统发生报警时，应与该视频系统联动。辅助照明灯光应满足视频系统正常摄取图像的照度要求。

7.3.4.7 视频监控系统的备用电源应满足至少 4 h 正常工作的需要；入侵报警系统备用电源应满足至少 24 h 正常工作的需要。

7.3.4.8 存在来自无人机威胁风险的重点目标应根据防范需要配备边界雷达、音频探测器、复合视频监控、射频干扰设备等无人防御手段，以达到侦测、识别、反制（或击落）进入电子围栏的非法无人机，

电子围栏的设定符合 MH/T 2008 的要求。发现无人机入侵需报属地公安机关，击落的无人机送交属地公安机关。

7.3.5 系统检验与验收

7.3.5.1 技防系统竣工后应进行检验，系统检验应符合 GB 50348 和本文件的要求。

7.3.5.2 技防系统验收应符合 GB 50348、GA 308 和本文件的要求。

7.3.6 运行维护及保养

7.3.6.1 重点目标责任主体应制定技防系统管理制度，建立运行维护保障的长效机制，设置专人负责系统日常管理工作。

7.3.6.2 技防系统应确保有人员值班，值班人员应培训上岗，掌握系统运行维护的基本技能。

7.4 数据防

7.4.1 设置原则

7.4.1.1 应纳入重点目标工程建设总体规划，并应同步设计、同步建设、同步运行。

7.4.1.2 使用的设备和设施应经法定机构检验或认证合格。

7.4.2 数据分类分级

7.4.2.1 数据分类方法

应按照GB/T 7027进行数据分类，可按数据主体、主题、业务等不同的属性进行分类。

7.4.2.2 数据分级方法

7.4.2.2.1 应对已有数据或新采集的数据进行分级，数据分级需要重点目标责任主体、业务专家、安全专家等共同确定。政府数据分级应按照 GB/T 31167-2014 中 6.3 的规定，将非涉密数据分为公开、敏感数据。个人信息和个人敏感信息应参照GB/T 35273-2020 执行。

7.4.2.2.2 涉密信息的处理保存、传输、利用，按国家保密法律法规执行。

7.4.2.2.3 可根据法律法规、行业部门需要等，对敏感数据进步分级，以提供相适应的安全管理和技术措施。

7.4.2.2.4 针对不同级别的数据应按照 GB/T 35274-2017 第 4 章～第6 章的规定，选择恰当的管理和技术措施对数据实施有效的安全保护。

7.4.3 数据安全管理

7.4.3.1 数据安全管理目标

实现数据价值的同时，确保数据安全。应：

a) 满足数据相关方的数据保护要求；

b) 通过技术和管理手段，保证自身控制和管理的数据安全风险可控。

7.4.3.2 数据安全管理内容

主要包括以下内容：

a） 数据安全需求。应分析大数据环境下数据的保密性、完整性和可用性所面临的新问题，分析大数据活动可能对国家安全、社会影响、公共利益、个人的生命财产安全等造成的影响，并明确解决这些问题和影响的数据安全需求；
b） 数据分类分级。应先对数据进行分类分级，根据不同的数据分级选择适当的安全措施；
c） 大数据活动安全要求。应理解主要大数据活动的特点，可能涉及的数据操作，并明确各大数据活动的安全要求；
d） 评估大数据安全风险。除开展信息系统安全风险评估外，还应从大数据环境潜在的系统的脆弱性恶意利用后果等不利因素，以及应对措施等评估大数据安全风险。

7.4.4 数据防内容

重点目标数据防包括物理安全、主机安全、网络安全、应用安全和数据安全等。

7.4.5 数据防要求

数据防的相关信息系统应符合GB/T 22239、GB/T 22240、GB/T 39786的要求。

7.5 制度防

7.5.1 建设原则

7.5.1.1 为确保人防、物防、技防、数据防的有效实施达到预期目的，应实现反恐怖防范工作制度化、标准化，构成由上而下、紧密互联的制度体系。
7.5.1.2 各行业主管部门应根据本文件要求，结合重点目标的实际情况制定所属行业相应的反恐怖防范管理要求。
7.5.1.3 重点目标责任主体应根据本文件要求，结合自身的特点，形成一套完整、协调配合的反恐怖防范管理体系和自我完善的运行机制，确保反恐怖防范工作持续有效运作。

7.5.2 制度防组成

制度防组成包括管理标准、工作标准、技术标准等标准化文件。

7.5.3 制度防配置

7.5.3.1 基础要求

7.5.3.1.1 方针和目标

7.5.3.1.1.1 反恐怖防范的指导方针是全面部署、突出重点，全民参与、综合施策，利用标准化、教育等手段全面提升反恐怖防范能力。
7.5.3.1.1.2 反恐怖防范的总体目标是防范恐怖活动，维护国家安全、公共安全和人民生命财产安全。
7.5.3.1.1.3 重点目标责任主体应结合全市反恐怖防范管理的指导方针和总体目标，根据自身实际情况，制定可量化考核和可实现的防范工作目标。

7.5.3.1.2 工作机构

重点目标责任主体应制定人防组织和配置的架构图，并明确责任领导的管理职责和责任部门的工作职责。配置专人负责反恐怖防范制度管理工作，所有制度文件应受控，确保制度的宣贯、实施与持续改进。

7.5.3.2 管理标准配置

重点目标的管理标准配置应符合表4要求。

表4 管理标准配置

序号	项目		配设要求	设置要求
1	人防	教育培训制度	见附录A.2.1	应设
2		人员背景审查制度	见附录A.2.2	应设
3		人员档案及备案制度	见附录A.2.3	应设
4		门卫与寄递物品管理制度	见附录A.2.4	应设
5		巡查与安检制度	见附录A.2.5	应设
6		值班监看和运维制度	见附录A.2.6	应设
7		训练演练制度	见附录A.2.7	应设
8		检查督导制度	见附录A.2.8	应设
9		人防增援配置制度	见附录A.2.9	应设
10	物防、技防	采购管理制度	见附录A.2.10	应设
11		设备设施档案制度	见附录A.2.11	应设
12		技防系统管理制度	见附录A.2.12	应设
13	数据防	网络安全管理制度	见附录A.2.13	应设
14	综合	工作报告制度	见附录A.2.14	应设
15		专项经费保障制度	见附录A.2.15	应设
16		情报信息管理制度	见附录A.2.16	应设
17		恐怖威胁预警响应制度	见附录A.2.17	应设
18		恐怖威胁风险评估制度	见附录A.2.18	应设
19		联动配合机制	见附录A.2.19	应设
20		应急管理制度	见附录A.2.20	应设

7.5.3.3 工作标准配置

7.5.3.3.1 制定重点目标责任主体责任领导、责任部门的正（副）职、联络员的职责和权限。

7.5.3.3.2 制定技防、固定、巡查、网络与信息安全管理、机动等岗位工作通用标准，每个岗位按作业顺序列出工作细节，明确与其他工作接口相互协调要求。

7.5.3.3.3 规定定额的岗位应制定定额，有数量和时间方面要求的，宜量化。

7.5.3.3.4 制定详细的考核条件和奖惩办法，明确检查、考核部门、时间要求，明确考核程序和考核办法，应有考核记录。

7.5.3.4 技术标准配置

7.5.3.4.1 配备本文件及相关系列标准中引用文件中所列的相关标准及文件。

7.5.3.4.2 配备反恐怖防范工作中所涉及到物防、技防等相关的国家、行业和地方标准。

7.5.3.4.3 对于尚未有现行的国家、行业和地方标准的技术事项，应制定相应的内控管理标准化文件。

8 非常态反恐怖防范

8.1 非常态反恐怖防范启动

8.1.1 根据反恐怖主义工作领导机构或有关职能部门发布的恐怖威胁预警，进入非常态反恐怖防范。

8.1.2 重点目标责任主体可以根据实际工作需要进入非常态反恐怖防范。

8.2 非常态反恐怖防范实施

8.2.1 重点目标责任主体应积极响应恐怖威胁预警要求，采取的非常态反恐怖防范等级应不低于有关部门或机构发布的恐怖威胁预警等级。

8.2.2 非常态反恐怖防范等级和恐怖威胁预警等级对应关系见表 5。

表5 非常态反恐怖防范等级和恐怖威胁预警等级对应关系表

非常态反恐怖防范等级	恐怖威胁预警等级	威胁预警颜色	防范等级颜色
四级（IV）	四级（IV）	蓝色	蓝色
三级（III）	三级（III）	黄色	黄色
二级（II）	二级（II）	橙色	橙色
一级（I）	一级（I）	红色	红色

8.3 四级非常态反恐怖防范

应在符合常态反恐怖防范的基础上，同时采取以下工作措施：

a) 启动反恐怖应急指挥部，各类防范、处置装备设施处于待命状态；
b) 责任主体安保部门负责人带班组织防范工作；
c) 在常态安保力量的基础上增派 50%以上；
d) 严格执行各项管理制度，检查物防、技防设施；
e) 对出入口进行控制，对重要部位进行巡视、值守，保持通信联络畅通，专人收集、通报情况信息；
f) 联系属地公安机关和行业主管部门指导防范工作；
g) 每天主动向属地公安机关和行业主管部门报告防范工作落实情况，重要情况应随时报告；
h) 配合反恐怖主义工作领导机构及其办事机构、公安机关、行业主管部门开展工作；
i) 根据反恐怖主义工作领导机构及其办事机构、公安机关、行业主管部门要求采取的其他防范措施。

8.4 三级非常态反恐怖防范

应在符合四级非常态反恐怖防范的基础上，同时采取以下工作措施：

a) 责任主体分管领导带班组织防范工作；
b) 在常态安保力量的基础上增派 70%以上；
c) 对区域内人员、车辆、物品进行安全检查；
d) 每半天主动向属地公安机关和行业主管部门报告防范工作落实情况，重要情况应及时报告；
e) 联系属地公安机关和行业主管部门派员指导防范工作。

8.5 二级非常态反恐怖防范

应在符合三级非常态反恐怖防范的基础上，同时采取以下工作措施：

a) 责任主体主要领导及分管领导共同带班组织防范工作；
b) 在常态安保力量的基础上增派 100%以上；
c) 重要部位巡视频率较常态提高 1 倍；出入口派员加强值守；
d) 主要出入口设置障碍，严禁外部车辆进入；
e) 联系属地公安机关和行业主管部门派员参与反恐怖防范工作。

8.6 一级非常态反恐怖防范

应在符合二级非常态反恐怖防范的基础上，同时采取以下工作措施：
a) 责任主体主要领导、分管领导及领导班子其他成员共同带班组织防范工作；
b) 装备、力量、保障进入临战状态；
c) 重要部位应有 2 名以上安保人员守护，实行 24 h 不间断巡查；
d) 对无关工作人员进行疏散，必要时转移重要信息、物资；
e) 封闭出入口，严密监视内外动态；
f) 对目标区域进行全面、细致检查；
g) 危急情况下对相关要害部位、设施、场所实施关闭，暂停相关活动。

8.7 非常态反恐怖防范的人防、物防、技防和数据防配置

重点目标责任主体应有机制确保启动非常态反恐怖防范时人防、物防、技防和数据防配置的要求，确保增派的安保力量、物防设备设施和技防系统能及时到位。

9 应急准备要求

9.1 重点目标责任主体应针对恐怖事件的规律、特点和可能造成的社会危害，分级分类制定并实施应急预案，应对可能遭受的恐怖袭击或危害的紧急情况，并对本单位的应急准备和应急能力进行评估。

9.2 应急预案应规定恐怖事件应对处置的组织指挥体系、恐怖事件安全防范、应对处置程序以及事后社会秩序恢复等内容：

a) 应包括目标概况、风险分析、应急基本原则、组织机构、应急联动、信息报告、应急指挥、应急（等级）响应、应急措施、保障、应急解除等内容；
b) 根据情况应提供基本情况说明、工作人员信息详表（背景审查记录）、应急联络通讯表、实景照片、地理位置标示图、周边环境图、单位平面图、应急疏散通道（路线）图、应急装备（设备）分布图、消防设施分布图、防范设施标示图；
c) 宜提供电路设施网分布图、自来水管网分布图、地下管网分布图、信息系统网络分布图及相应的视频资料或三维建模（配合 3D 地图采集建模）等。

9.3 宜建立相应的数据库和应急指挥系统。

9.4 组建具有组织人员疏散、保护重要部位、控制损失和准确反馈现场情况等能力的应急作战队伍。

9.5 重点目标责任主体应定期按照应急预案开展演练，动态修订和完善应急预案。

10 监督和检查

10.1 监督职责

10.1.1 反恐怖主义工作领导机构的办事机构

反恐怖主义工作领导机构的办事机构应设置与公安机关、行业主管部门、重点目标责任主体对接的岗位人员，负责全市各重点目标的备案、日常指导和监督检查工作。

10.1.2 公安机关

公安机关应掌握重点目标的基本信息和重要动态，指导、监督重点目标责任主体履行防范恐怖袭击的各项职责，应当依照有关规定对重点目标进行警戒、巡逻、检查。

10.1.3 行业主管部门

10.1.3.1 行业主管部门应掌握主管领域内重点目标的基本信息和重要动态，指导、监督重点目标责任主体履行防范恐怖袭击的各项职责。

10.1.3.2 重点目标涉及一个行业主管部门管理的，应由该行业主管部门领导班子成员分管反恐怖防范工作，并应设置专职工作人员管理重点目标。

10.1.3.3 重点目标涉及多个行业主管部门管理的，应由反恐怖主义工作领导机构指定一个牵头部门负责，其他行业主管部门配合，共同管理重点目标。牵头部门应设置专职工作人员。

10.2 检查

10.2.1 自我检查及自我评价

10.2.1.1 重点目标责任主体应定期和不定期地开展自我检查，定期检查每半年应不少于一次，不定期检查根据实际工作需要开展。

10.2.1.2 重点目标责任主体每年应对其反恐怖防范系统开展至少一次的自我评价，对反恐怖防范工作中存在的问题实施持续改进，不断完善人防、物防、技防、数据防和制度防，提高其反恐怖防范能力。自我评价及其改进参见附录 B。

10.2.1.3 自我评价可结合定期的自我检查一起开展。

10.2.1.4 应及时向行业主管部门递交自我评价报告。

10.2.2 部门检查

公安机关、行业主管部门应定期、不定期地开展反恐怖防范的工作检查，每年对管辖范围内重点目标的检查覆盖率达100%。公安机关、行业主管部门每半年应向反恐怖主义工作领导机构提交检查报告，报告内容包括：

a) 本行业反恐怖防范概况及重点目标增减情况；
b) 本阶段部门检查情况及整改情况；
c) 存在的问题及原因分析；
d) 下一阶段的部门检查计划。

10.2.3 督导检查

反恐怖主义工作领导机构的办事机构应按反恐怖主义法等法律法规要求开展反恐怖防范工作的督导检查，应确保督导检查覆盖重点目标的各个分类。反恐怖主义工作领导机构的办事机构应每年向反恐怖主义工作领导机构提交年度督导检查报告。

10.2.4 检查的实施

自我检查、部门检查和督导检查的实施参见附录C。

附 录 A
（规范性）
管理标准要求

A.1 制度的基本框架

制度的基本框架至少应包括以下内容：

a) 制度的管理目的（或适用范围）；
b) 制度的引用文件；
c) 制度的管理职责，如制定、维护、落实责任部门或岗位；
d) 管理内容与实施方法；
e) 制度实施报告和记录；
f) 制度的编号、版本号、实施时效、制定人、审核人和批准实施人。

A.2 管理制度

A.2.1 教育培训制度

重点目标责任主体应制定教育培训制度，持续提升人防技能，至少应包括：

a) 保安员培训：保安员应经专业装备使用技能培训并取得相应专业资格证书，保安员除应熟悉服务单位地理环境、消防通道和各类出入口外，还应熟悉应急处突装备的放置区域，并管理好个人所配备的防护和应急装备，严防被不法分子所用；
b) 全员培训：每年至少应组织一次反恐怖防范与应急知识的全员教育培训；
c) 责任部门培训：每个季度至少应组织一次重要岗位反恐怖防范与应急知识的部门教育培训；
d) 宣传教育：协助各有关部门开展反恐怖主义宣传教育。

A.2.2 人员背景审查制度

A.2.2.1 重点目标责任主体应当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。

A.2.2.2 重要岗位人员至少应包括：

a) 责任领导；
b) 责任部门负责人；
c) 联络员；
d) 保安员；
e) 技防岗位人员。

A.2.2.3 人员背景审查的内容至少应包括：

a) 个人资料，身份信息和户口信息；
b) 个人经历，教育、就业履历和出入境记录；
c) 个人无犯罪记录；
d) 本人及亲属是否有涉及极端主义，恐怖主义活动或关联的有关信息。

A.2.3 人员档案及备案制度

重点目标责任主体应建立人员档案并及时向有关部门备案，人员档案至少应包括以下内容：

a) 基本信息；
b) 背景审查情况；
c) 反恐怖防范继续教育情况；
d) 证件（身份证、保安员证书等复印件）；
e) 岗位聘用情况；
f) 备案信息。备案信息至少包括：备案日期、备案人相关信息、备案部门。

A.2.4 门卫与寄递物品管理制度

重点目标责任主体应：

a) 对出入口人员、车辆进行登记检查；
b) 加强寄递物品验视、签收和登记管理；
c) 安全检查中发现违禁品和管制物品，应当予以扣留并立即向公安机关报告；
d) 发现涉嫌违法犯罪人员，应当立即向公安机关报告。

A.2.5 巡查与安检制度

重点目标责任主体应确定出入口、周界、重要部位的巡查路径和方式，明确值守、巡查的要求和措施；确定安检设备的使用位置和使用规范。

A.2.6 值班监看和运维制度

重点目标责任主体应做好视频监控系统的值班监看、信息保存使用，定期开展技防各系统的运行维护检查，保障各系统的正常运行。

A.2.7 训练演练制度

重点目标责任主体应结合工作实际，制定训练演练大纲，有计划地定期组织开展应急技能训练和应急处突演练，应急技能训练每周至少一次，应急演练每月至少一次。

训练演练制度应明确：

a) 安保力量的训练演练要求；
b) 训练演练计划的要求；
c) 训练大纲，包括训练的目的、类型及对应的内容、训练效果评价方法；
d) 演练大纲，包括演练的目的、类型及对应的内容、演练效果评价方法。

A.2.8 检查督导制度

重点目标责任主体应定期开展反恐怖防范督导、检查、考核工作，落实反恐怖防范措施。

A.2.9 人防增援配置制度

重点目标责任主体应具备当启动非常态反恐怖防范时增派安保力量的保障能力，包括：

a) 建立后备的安保力量；
b) 与安保企事业单位签定临派安保力量的服务合同；
c) 通过联动配合机制获得安保力量；

d) 其他途径获取的可靠安保力量。

A.2.10 采购管理制度

A.2.10.1 重点目标责任主体应对采购活动进行控制，制定采购管理标准。采购过程中，应要求：

a) 供方应提供其具备合格供方能力的证据，包括：
   1) 供方的产品、程序、过程、设备、人员的概况；
   2) 供方的产品安全认证（必要时）；
   3) 供方的质量管理等体系的认证。
b) 根据供方提供产品的能力，进行评价和选择；
c) 制定选择评价和重新评价合格供方的准则；
d) 保存评价结果及评价记录。

A.2.10.2 重点目标责任主体应建立并实施验收标准，包括提供合格证明文件、现场验证等方式，以确保采购的产品满足规定的物防、技防要求。

A.2.11 设备设施档案制度

重点目标的设备设施应有台账管理，并建立档案，档案内容至少应包括：

a) 物品名称、型号、编号；
b) 物品管理编号，领用人或保管人；
c) 物品使用说明书，合格证、保修证、检验报告、验收报告及相关发票（原件或复印件）；
d) 物品的使用状态，包括在用、停用和报废；
e) 操作手册（使用、维护和保养）；
f) 维护保养记录。

A.2.12 技防系统管理制度

A.2.12.1 重点目标应有技防系统的总台账、各系统的设备设施台账、系统操作手册（包括使用、维护和保养），并建立系统管理档案。

A.2.12.2 技防系统的总台账至少应包括以下内容：

a) 系统名称、型号；
b) 工程提供和建设方名称；
c) 系统责任人；
d) 维护保养周期。

A.2.12.3 系统管理档案至少包括以下内容：

a) 采购有关资料；
b) 建设工程有关的资料，包括设计、验收报告等；
c) 所有设备设施的使用说明书，合格证、保修证、检验报告和验收资料；
d) 操作手册（使用、维护和保养）；
e) 维护保养记录。

A.2.13 网络安全管理制度

对重点目标的网站等信息系统，应依法履行网络安全等级保护责任，按照GB 17859中规定计算机信息系统安全保护能力第三级（安全标记保护级）或以上的要求开展备案、等级测评，落实等级相应的保护责任、技术措施及安全管理制度。强化主体责任意识，加强网络安全监测和隐患排查、整改。在发生安全案件时，应及时上报属地公安机关。

A.2.14 工作报告制度

A.2.14.1 重点目标责任主体应定期向反恐怖主义工作领导机构的办事机构、属地公安机关和相关行业主管部门提交工作报告，每半年至少一次，内容至少应包括：

a) 人防配置及实施情况；
b) 物防配置及实施情况；
c) 技防配置及实施情况；
d) 数据防配置及实施情况；
e) 制度防配置及实施情况；
f) 自我检查（评价）报告。

A.2.14.2 存在下列情况时应提交工作报告：

a) 非常态反恐怖防范的响应及实施总结；
b) 特殊活动安全防范总结；
c) 人防、物防、技防、数据防、制度防的重大变化；
d) 其他重要情况。

A.2.15 专项经费保障制度

重点目标责任主体应建立反恐怖主义工作专项经费保障制度，做好年度经费预算，确保：

a) 人防配置及奖励制度有效落实；
b) 物防配备、更新防范和处置设备设施；
c) 技防系统正常运维；
d) 数据防系统正常运维；
e) 各项制度实施经费保障，如教育培训经费、物防设施设备验收、技防委托验收、人防增援配置等。

A.2.16 情报信息管理制度

A.2.16.1 重点目标应建立快速高效的情报信息工作机制，主动收集重点目标范围内的情报信息，对收集到的有关线索、人员、活动等情报信息应及时分析整理，及时向责任领导、责任部门汇报。

A.2.16.2 发现恐怖活动嫌疑或者恐怖活动嫌疑人员的信息应及时向行业主管部门和属地公安机关报送，必要时经责任领导批准后提升内部的反恐怖防范等级。

A.2.16.3 联络员接到上级部门或属地公安机关情报信息，应立即向责任领导、责任部门报告并落实相应工作措施。

A.2.17 恐怖威胁预警响应制度

重点目标责任主体应建立恐怖威胁预警响应制度。根据获取的情报信息，重点目标责任主体同时或先于反恐怖有关部门发布的恐怖威胁预警，采用相同等级或高于恐怖威胁预警等级的应对措施，预警等级响应制度应包括：

a) 情报信息的响应；
b) 恐怖威胁预警等级的确定原则；
c) 启动相应的应急预案；
d) 确立本单位的指挥员；
e) 非常态恐怖威胁预警等级的下调或取消准则。

A.2.18 恐怖威胁风险评估制度

重点目标实行风险评估制度，实时监测安全威胁，编写恐怖威胁风险评估报告。每半年至少要开展一次恐怖威胁风险评估，评估内容包括：

a) 本领域内国内外恐怖活动及影响；
b) 本领域内的安全防范隐患或危险源；
c) 监测安全威胁信息的汇总与分析；
d) 自身成为恐怖活动实施对象的潜在可能性分析；
e) 防范体系的不足及改进措施。

A.2.19 联动配合机制

重点目标责任主体应与公安机关、应急管理、街道等有关政府职能部门建立联动机制，实现资源共享，信息互通。

A.2.20 应急管理制度

重点目标责任主体应制定应急管理制度，针对恐怖事件的规律、特点和可能造成的社会危害，分级分类制定并实施反恐怖应急预案。

附 录 B
（资料性）
反恐怖防范系统自我评价及改进

B.1 自我评价

B.1.1 评价目的

确定其建立和实施的人防、物防、技防、数据防及制度防与反恐怖防范目标的适宜性、充分性和有效性。

B.1.2 评价时间

B.1.2.1 重点目标责任主体建立了反恐怖防范系统所需的人防、物防、技防、数据防及制度防并有效实施三个月后方可开展首次自我评价。

B.1.2.2 后续评价时间间隔不宜大于半年，每年应至少一次。

B.1.3 评价组织

成立包括责任领导、责任部门负责人在内的自我评价小组，并确定一名组长，成员包括各岗位的负责人数名，必要时可外聘反恐专家协助。

B.1.4 评价方法

B.1.4.1 评价一般采用整体评价的方法，由重点目标责任主体所在单位组成评价小组，对建立、实施和开展反恐怖防范全过程进行评价。

B.1.4.2 具体方法主要通过评价人员的现场核查、观察、提问、对方陈述、检查、比对、验证等获取客观证据的方式进行。

B.1.4.3 根据评价结果，对不符合标准要求的项目制定纠正和预防措施，并跟踪实施和改进。

B.1.5 评价程序

评价活动应按以下程序进行：

a) 成立评价小组；
b) 制定评价计划；
c) 评价准备；
d) 评价实施；
e) 编写自我评价报告和不合格报告；
f) 评价结果处置；
g) 考核奖惩。

B.1.6 评价内容

覆盖人防、物防、技防、数据防和制度防等所有要素。

B.1.7 评价结果处置

评价后，应编写评价报告。对评价结果，特别是发现的问题、不合格项产生的根源要进行分析研究，制定纠正和预防措施。

B.2 改进

B.2.1 改进目的

持续改进是重点目标责任主体一项长期工作，是不断完善管理、实现最终反恐怖防范目标的有效办法，持续改进应按照PDCA（计划-实施-检查-改进）管理模式进行。

B.2.2 改进计划

根据自我评价报告，制定改进计划。

B.2.3 改进的实施及依据

B.2.3.1 收集有关不符合反恐怖防范要求的信息，明确信息来源，组织有关人员对信息进行分析，确定现有的和潜在的问题根源。

B.2.3.2 根据信息分析的结果，督导责任部门会同有关人员共同制定纠正和预防措施，对制度、程序、人员或管理部门进行调整，并报责任领导批准，避免不符合情况再次发生。

B.2.3.3 实施改进的依据包括：

a) 公众反馈安全防范漏洞的意见；
b) 物防中所涉及安防产品日常检查、技防工程的验收、周期检验的报告；
c) 各项制度落实的记录、报表中反映的数据；
d) 有关部门检查发现的问题；
e) 安保人员等有关人员的建议。

B.2.4 持续改进

重点目标责任主体通过实施纠正措施，对标准、制度文件或岗位人员进行调整，直至达到预期效果。

B.2.5 改进后评价

对改进的有效性进行跟踪评价。

附 录 C
（资料性）
反恐怖防范工作检查实施

C.1 检查基本信息

检查基本信息至少应包括：

a） 责任主体的名称、地址；

b） 检查执行机构名称，检查人员签名（不少于 2 人）；

c） 检查的时间。

C.2 检查的实施机构

C.2.1 自我检查由重点目标责任主体自行组织实施。

C.2.2 部门检查由公安机关、行业主管部门组织实施。

C.2.3 督导检查由反恐怖主义工作领导机构的办事机构组织实施。

C.3 检查内容

检查内容见表C.1

C.4 检查结果及处置

C.4.1 自我检查的结果及处置

自我检查中应做好书面记录，并应根据自我检查的结果进行整改，由责任领导检查整改情况，确保整改措施落实。

C.4.2 部门检查的结果及处置

部门检查中，进行检查的部门应做好书面记录，将检查情况汇总通报被检查单位并反馈检查意见书，督促和检查整改的完成。发现有重大涉恐隐患的，应及时向反恐怖主义工作领导机构的办事机构汇报。

C.4.3 督导检查的结果及处置

督导检查中，反恐怖主义工作领导机构的办事机构应做好书面记录，将检查情况现场通报被检查单位和相关行业管理部门并反馈督导检查意见书，视检查情况出具限期整改通知书并督导整改的完成。

C.5 检查表

检查表应包括依据标准的条款，检查内容概要，检查过程记录和检查结论，见表C.1。

表C.1 检查表

序号	标准条款	内容概要	检查记录	检查结论
1	重要部位	重点目标重要部位分布图/列表是否清晰、完整， 是否及时报备		

表 C.1（续）

序号	标准条款	内容概要	检查记录	检查结论
2	人防	是否按要求建立了专责、健全的反恐怖防范工作机构并在主要负责人的领导下开展工作，做到分工明确，责任落实。		
3		是否按实际需要配备了技防岗位、固定岗位、巡查岗位、网络与信息安全管理岗位和机动岗位等安保力量。		
4		与反恐怖主义工作领导机构、公安机关及行业主管部门的工作联系途径是否有效		
5		是否对重要岗位人员开展背景审查，查看审查记录		
6		是否建立重要岗位人员档案并备案，查看档案资料及备案回执		
7		是否对出入口人员、车辆进行登记检查，检查记录		
8		是否对寄递物品进行验视、签收和登记管理，检查记录		
9		是否按有效的路径和方式开展巡查，检查记录		
10		是否在正确的位置正确使用安检设备开展安检工作		
11		视频监控系统的值班监看是否到位		
12		检查教育培训记录，是否按教育计划开展		
13		检查训练记录，是否按训练计划开展		
14		检查演练记录，是否按演练计划开展		
15		是否开展自我检查督导和反恐怖防范体系自我评价工作，查看相关记录		
16		是否指定了专职联络员，联络员的配置和变更，是否及时按要求报备，年内是否存在工作联系不到的情况		
17		反恐怖防范工作机构设置、责任领导、责任部门等是否按要求报备，查看备案回执		
18		保安员承担保安职责，是否满足《保安服务管理条例》和GA/T 594的相关要求并持证上岗		
19		反恐怖防范专（兼）职工作人员是否熟悉重点目标内部和周边环境、消防通道和各类疏散途径		
20		反恐怖防范专（兼）职工作人员是否熟悉本重点目标反恐怖防范工作情况及相关规章制度、应急预案等		
21		应对涉恐突发事件，年内是否存在不配合反恐怖主义工作领导机构、公安机关、有关行业主管部门开展工作的情况		
22		年内是否存在网络失控情况		

表 C.1（续）

序号	标准条款	内容概要	检查记录	检查结论
23	物防	机动车阻挡装置设置是否已覆盖无实体防护屏障的主要出入口		
24		防机动车冲撞或隔离设施是否已覆盖主要出入口和受机动车冲击后容易受到重大伤害的重要部位		
25		监控中心等重要部位出入口有否设立防盗安全门等实体防护设施		
26		财务室、收银处有否设立防盗保险柜或防盗保险箱		
27		周界是否设置围墙或栅栏		
28		出入口是否设置人车分离通道		
29		是否按实际需要配备了对讲机、强光手电、防护棍棒、防暴盾牌、钢叉、防暴头盔、防割（防刺）手套、防刺服等个人应急防护装备		
30		是否按实际需要配备了防爆毯和防爆围栏等公共应急防护装备		
31		监控中心、传达登记处、门卫处、重要部位、人员密集区域等是否已按要求设置了应急警报器		
32		各工作区域是否按要求设置了灭火器		
33		行包寄存设施是否设置在出入口附近，且距离重要部位＞30 m		
34		水域是否设置了巡逻船舶		
35		其它需要设置的物防设施		
36		采购物防设备设施标准是否符合要求		
37		查看物防设备设施是否按计划采购，所属供方是否是在合格供方名单中，是否有产品合格证明		
38		是否建立设备设施台账和档案，信息是否准确、完整，是否对设备设施制定操作规程		
39		是否存在失效设备设施，是否对正常使用周期内失效的设备设施进行失效原因分析并制定纠正和预防措施		
40	技防	是否已按要求设置了监控中心，监控中心是否设有控制、数据存储、显示等装置		
41		摄像机是否已覆盖与外界相通的出入口、周界及内部主要通道、办公楼大厅、电梯及等候区、各楼梯口、人员密集区域、食堂（餐厅）及其出入口、重要设备设备设施区域、网络通讯和空调控制区域、新风口、危险物品存放处及其出入口、寄递物品收发处、传达登记处、门卫处、停车库（场）、停机坪及其主要通道和出入口、防范目标高空瞭望处、监控中心、电脑中心机房、财务室、档案馆（库）、贵重物品存放场所等区域		

表 C.1（续）

序号	标准条款	内容概要	检查记录	检查结论
42	技防	枪支、弹药及危险物品存放场所是否已安装声音复核装置		
43		入侵探测（报警）器是否已覆盖周界，水、气、电、油、网络通讯控制区域，枪支、弹药及危险物品存放处， 电脑中心机房、财务室、档案馆（库）、贵重物品存放等重要场所		
44		紧急报警装置（一键报警）是否已设置在传达登记处、门卫处、重要部位、人员密集区域、监控中心		
45		报警控制器是否已设置在监控中心及相关的独立设防区域		
46		出入口控制系统是否已设置在水、气、电、油、网络通讯、空调主要控制区域、枪支、弹药及危险物品存放处、监控中心		
47		停车库（场）是否设置停车库（场）管理系统		
48		出入口、周界、重要部位和人员密集区域是否设置了电子巡查系统		
49		公共广播系统是否已区域全覆盖		
50		无线通信对讲指挥调度系统是否已安装在监控中心并做到区域全覆盖		
51		出入口或重要部位是否设置了手持式金属探测器		
52		其它需要设置的技防设施		
53		技防系统的设置是否满足GB 50348、GB/T 15408、GB/T 2887等的相关要求		
54		与外界相通的出入口等重点部位配置的摄像机是否满足GA/T 1127中规定的C类高清晰度及以上要求，视频信息是否与公安机关联网		
55		报警系统信息本地保存时间是否不少于180 d，并具备与公安机关联动的接口		
56		视频录像保存时间是否不少于90 d		
57		视频监控范围内的报警系统发生报警时，是否能与该视频系统联动。辅助照明灯光是否满足视频系统正常摄取图像的照度要求		
58		视频监控系统的备用电源是否满足至少4 h正常工作的需要；入侵报警系统备用电源是否满足至少24 h正常工作的需要		
59		是否存在发现无人机入侵未报属地公安机关的情况		
60		系统检验与验收是否符合要求		
61		运行维护及保养是否符合要求，是否有技防系统的总台账、各系统的设备设施台账、系统操作手册（使用、维护和保养），并建立系统管理档案		

表 C.1（续）

序号	标准条款	内容概要	检查记录	检查结论
62	数据防	是否建立了数据安全分类分级制度		
63		是否明确了数据安全管理目标和内容		
64		是否落实网络安全等级保护测评、备案		
65		是否落实商用密码应用安全性评估、备案		
66	制度防	是否制定了可量化考核和可实现的防范工作目标，是否与指导方针与总体目标一致		
67		是否制定了人防组织和配置的架构图，并明确责任领导的管理职责和责任部门的工作职责。是否指定专人负责反恐怖防范制度管理工作		
68		是否按要求配置了相关管理制度，包括教育培训制度、人员背景审查制度、人员档案及备案制度、门卫与寄递物品管理制度、巡查与安检制度、值班监看和运维制度、训练演练制度、检查督导制度、人防增援配置制度、采购管理制度、设备设施档案制度、技防系统管理制度、网络安全管理制度、工作报告制度、专项经费保障制度、情报信息管理制度、恐怖威胁预警响应制度、恐怖威胁风险评估制度、联动配合机制、应急管理制度等		
69		工作标准配置是否符合要求		
70		技术标准配置是否符合要求		
71	其他防范管理	是否按要求制定了各级非常态反恐怖防范应对措施		
72		是否制定了应急预案		
73		应急预案的内容是否全面		
74		是否有组建应急作战队伍并建立有效增援保障措施		
75		是否按规定开展应急预案的演练		
76		是否定期开展自我评价并向行业主管部门递交自我评价报告		
77		是否对反恐怖防范工作中存在的问题实施持续改进		
78		专项经费是否符合实际防范工作需要		
79		情报信息管理是否符合要求		
80		恐怖威胁预警是否得到快速有效响应		
81		是否开展恐怖威胁风险评估工作		
82		是否建立有效联动配合机制		

参 考 文 献

[1] 《中华人民共和国密码法》
[2] 《中华人民共和国反恐怖主义法》
[3] 《中华人民共和国网络安全法》
[4] 《中华人民共和国突发事件应对法》
[5] 《中华人民共和国数据安全法》
[6] 《中华人民共和国个人信息保护法》
[7] 《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
[8] 《保安服务管理条例》 中华人民共和国国务院令 第564号