ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA 1277.1—2020
代替 GA 1277—2015

互联网交互式服务安全管理要求 第1部分:基本要求

Security management requirements for internet interactive service — Part 1: Basic requirements

2020-01-16 发布　　2020-03-01 实施

中华人民共和国公安部　　发布

目　　次

前　言

GA 1277《互联网交互式服务安全管理要求》拟分成多个部分，包括基本要求和具体服务类型中的要求。目前计划发布如下部分：

——第1部分：基本要求；

——第2部分：微博客服务；

——第3部分：音视频聊天室服务；

——第4部分：即时通信服务；

——第5部分：论坛服务；

——第6部分：移动应用软件发布平台；

——第7部分：云服务；

——第8部分：电子商务平台；

——第9部分：搜索服务；

——第10部分：互联网约车服务；

——第11部分：互联网短租房服务；

……

本部分为GA 1277的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GA 1277—2015《信息安全技术　互联网交互式服务安全保护要求》，与GA 1277—2015相比主要技术变化如下：

——修改了标准名称，由《信息安全技术　互联网交互式服务安全保护要求》修改为《互联网交互式服务安全管理要求》，并分成多个部分，本部分为《第1部分：基本要求》（见封面，2015年版的封面）；

——修改了“3 术语和定义”中的“互联网交互式服务”的定义，增加了“个人信息”“关键岗位人员”“个人信息安全事件”的定义（见3.1、3.4、3.5、3.6，2015年版的3.1）；

——修改了“4.1 制度与规程”，增加了安全责任制度，信息巡查制度，安全事件监测、预警、通报及应急响应制度等，同时将“8.1 操作规程”内容完善后置于4.1.1（见4.1、4.1.3，2015年版的4.1.1、4.1.3、8.1）；

——修改了“5 机构要求”为“5 组织机构”，“5.1 法律责任”修改为“5.1 机构要求”（见第5章、5.1，2015年版的第5章、5.1）；

——增加了“5.2 备案”的内容（见5.2）；

——修改了“8 网络与操作安全”为“8 安全技术措施”，原“8.2 网络与主机系统的安全”修改为“8.1 网络与系统运行安全”，并对其内容进行了增加（见第8章、8.1，2015年版的第8章、8.2）；

——修改了“8.3 备份”为“8.2 数据安全与备份”，并对其内容进行了增加（见8.2，2015年版的8.3）；

——修改了“8.4 安全审计”为“8.3 日志与用户数据记录”，并对其内容进行了修改，如将日志与注册信息等进行分离（见8.3，2015年版的8.4）；

——修改了“9 应用安全”为“9 业务安全”（见第9章，2015年版的第9章）；

——增加了基于生物特征的用户真实身份信息有效核验方法[见9.2.2 a)]；

——增加了违法有害信息过滤的技术措施[见9.3.4)]；

——修改了“10.2 技术措施”的相关内容（见10.2，2015年版的10.2）；

——修改了“10.3 个人信息泄露事件的处理”为“10.3 个人信息安全事件的处置”，并修改了具体的内容(见 10.3，2015 年版的 10.3)。

本部分由公安部网络安全保卫局提出。

本部分由公安部信息系统安全标准化技术委员会归口。

本部分起草单位：公安部网络安全保卫局、公安部第三研究所。

本部分主要起草人：金波、陈妍、陈飞燕、高爽、邓琦、贺滢睿、王庆华、顾玮、陈长松。

GA 1277.1 的历次版本发布情况为：

——GA 1277—2015。

互联网交互式服务安全管理要求
第1部分:基本要求

1 范围

GA 1277的本部分规定了互联网交互式服务安全管理的要求。

本部分适用于互联网交互式服务提供者落实互联网安全管理制度和安全技术措施。

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/T 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分:事件管理原理

GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GA 1278—2015 信息安全技术 互联网服务安全评估基本程序及要求

3 术语和定义

GB/T 22239、GB/T 20985.1—2017、GB/Z 20986—2007、GB/T 35273—2020 和 GA 1278—2015 界定的以及下列术语和定义适用于本文件。为了便于使用,以下重复列出了GB/T 35273—2020中的一些术语和定义。

3.1

互联网交互式服务 internet interactive service

通过互联网为用户提供向社会公众发布信息以及基于信息交互提供的相关服务。

注1:交互形式包括文字、图片、音视频等。

注2:包括但不限于论坛、社区、贴吧、文字或音视频聊天室、微博客、博客、即时通信、电子商务平台、搜索、互联网约车、互联网短租房、移动下载、分享存储、第三方支付、云服务等互联网信息服务。

3.2

违法有害信息 illegal and harmful information

违反国家法律、法规,危害国家安全、荣誉和利益、公共安全、社会公德、公序良俗、公民人身财产安全及合法权益等的信息。

3.3

破坏性程序 destructive program

具有对计算机信息系统的功能或存储、处理及传输的数据进行非授权获取、删除、增加、修改、干扰、破坏等功能的程序。

3.4

关键岗位人员　personnel in key position

在互联网交互式服务提供者处从事与网络与系统运行安全、数据安全、业务安全、个人信息安全等相关的人员。

注1：关键岗位人员包括但不限于系统管理员、安全管理员、审计管理员、数据管理员、内容编辑与审核员。

注2：关键岗位人员可以是互联网交互式服务的主要负责人、网络安全责任人、安全管理负责人及其他责任人员等。

3.5

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

[GB/T 35273—2020，定义3.1]

3.6

个人信息安全事件　personal information security incident

发生个人信息的泄露、损毁、丢失，并对个人造成一定或相当影响的安全事件。

4　安全管理制度

4.1　制度与规程

4.1.1　互联网交互式服务提供者应建立文件化的安全管理制度，安全管理制度文件应包括：

a）　安全责任制度；

b）　安全岗位管理制度；

c）　安全培训制度；

d）　人员管理制度；

e）　安全运维管理制度；

f）　安全评估报备制度；

g）　用户注册制度；

h）　信息发布审核制度；

i）　信息巡查制度；

j）　个人信息保护制度；

k）　用户投诉举报接收处理制度；

l）　安全事件监测、预警、通报及应急响应制度；

m）　适用的现行法律、法规、规章、标准和行政审批文件。

4.1.2　安全管理制度应经过管理层批准并发布执行。

4.1.3　互联网交互式服务提供者应建立与安全管理制度相配套的操作规程，包括但不限于：网络与系统运行安全、数据安全和备份、日志与用户数据记录、信息发布审核、违法有害信息防范和处置、个人信息保护、破坏性程序防范、分包等。

4.2　文件控制

安全管理制度文件应予以保护和控制，包括但不限于：

a）　按计划的时间间隔或在发生重大的变化时评审安全管理制度文件，以确保文件是适当的；

b) 确保在使用处获得适用文件的最新授权版本；
c) 确保文件的清晰、可识别；
d) 确保对外来文件进行识别，并进行分发控制；
e) 确保文件是现行有效的。

4.3 记录控制

互联网交互式服务提供者应保留安全管理制度的制定、变更、执行等过程中相关的记录并加以保护与控制，防止未经授权的访问或修改。

5 组织机构

5.1 机构要求

5.1.1 互联网交互式服务提供者应是能够承担法律责任的组织或个人。
5.1.2 互联网交互式服务提供者从事的服务需要行政许可的应取得相关许可。

5.2 备案

5.2.1 互联网交互式服务提供者应在服务上线前填写用户备案表，并到当地公安机关备案。
5.2.2 互联网交互式服务提供者如需使用国际互联网，应在服务上线开通起 30 日内向地市及以上公安机关指定的受理机关办理国际联网备案手续。

5.3 网络与信息安全组织

5.3.1 互联网交互式服务提供者应建立与业务和规模相适应的安全组织机构，包括但不限于：
a) 组建专职安全管理队伍，定义管理人员的工作岗位职责；
b) 安全管理人员经过安全培训并取得相关资质；
c) 安全管理人员数量与业务规模相适应，并符合 9.3 要求的对违法有害信息防范和处置能力。
5.3.2 互联网交互式服务提供者应配备安全管理人员，履行以下职责：
a) 负责安全管理制度的建立、实施与保持；
b) 负责新服务、新功能的风险评估与安全方案审核；
c) 向最高管理者报告安全状况与改进建议。
5.3.3 互联网交互式服务提供者应配备专门人员负责配合公安机关的工作。

5.4 网安警务室工作支持

互联网交互式服务提供者应为已建的公安机关网安警务室开展工作提供相应的环境和支持配合，并接受网安警务室的安全管理和指导。

6 人员安全管理

6.1 安全责任与岗位职责

6.1.1 互联网交互式服务提供者应在安全责任制度中明确主要负责人、网络安全责任人、安全管理负责人及其他责任人员的责任。
6.1.2 互联网交互式服务提供者应在安全岗位管理制度中明确关键岗位人员及其职责，其中职责应包

括保密管理职责。

6.2 关键岗位人员核查

6.2.1 任用关键岗位人员之前，互联网交互式服务提供者应按照相关法律法规、道德规范和对应的业务要求执行安全背景核查：

a） 个人身份核查；

b） 个人履历核查；

c） 从事关键岗位所必需的能力考核；

d） 其他核查。

6.2.2 互联网交互式服务提供者应与关键岗位人员签订保密协议。

6.3 安全培训

互联网交互式服务提供者应在安全培训制度中明确需定期对所有工作人员进行网络安全培训，对安全岗位人员进行安全技能培训，提高全员的网络安全意识和安全岗位人员能力，包括但不限于：

a） 上岗前的培训；

b） 安全制度的培训；

c） 新服务、新功能上线前后的培训；

d） 与法律法规发展保持同步的继续教育培训；

e） 安全知识和技能的持续教育。

6.4 人员离岗

互联网交互式服务提供者应在人员管理制度中严格规范人员离岗过程，包括但不限于：

a） 及时终止离岗员工的所有访问权限；

b） 关键岗位人员须书面承诺调离后的保密义务后方可离开；

c） 配合公安机关工作的人员变动及时通报公安机关。

7 访问控制管理

7.1 访问管理

互联网交互式服务提供者应在安全运维管理制度中建立包括物理的和逻辑的系统访问权限管理要求。

7.2 权限分配

互联网交互式服务提供者应根据人员职责按以下原则分配不同的访问权限：

a） 角色分离，如访问请求、访问授权、访问管理；

b） 满足工作需要的最小权限；

c） 未经明确允许，则一律禁止。

7.3 特殊权限

互联网交互式服务提供者应限制和控制特殊访问权限的分配和使用，包括但不限于：

a） 标识出每个系统或程序的特殊权限；

b） 按照“按需使用”“一事一议”的原则分配特殊权限；

c） 记录特殊权限的授权与使用过程；

d） 特殊访问权限的分配需经过管理层的批准。

注：特殊权限是系统超级用户、数据库管理等系统的管理权限及运维权限。

7.4 权限的检查

互联网交互式服务提供者应定期对访问权限进行检查，对特殊访问权限授权情况的检查需更频繁，如发现不恰当的权限设置，应及时予以调整。

8 安全技术措施

8.1 网络与系统运行安全

互联网交互式服务提供者应综合考虑系统的安全需求，制定整体的安全防护方案，落实安全防护措施，建立应急响应体系，包括但不限于：

a） 重要系统和数据库具备容灾能力；

b） 根据业务需求，及时进行补丁更新；

c） 实施计算机病毒等恶意代码的预防、检测和系统被破坏后的恢复措施；

d） 实施不间断地网络攻击和网络入侵行为的预防、检测与响应措施；

e） 适用时，对重要文件的完整性进行检测，并具备文件完整性受到破坏后的恢复措施；

f） 采取技术措施监测、记录网络运行状态、信息安全事件和用户活动行为等；

g） 对系统的脆弱性进行评估，并采取适当的措施处理相关的风险。

注：系统脆弱性评估包括采用安全扫描、渗透测试等多种方式。

8.2 数据安全与备份

互联网交互式服务提供者应对数据采取备份和保护等措施，保证数据的安全，包括但不限于：

a） 对数据进行分级分类；

b） 对重要数据的传输和存储采取加密等安全保护措施；

c） 根据数据分类结果建立不同数据的备份策略，提供足够的备份设施，确保必要的信息和软件在灾难或介质故障时可以恢复；

d） 建立数据安全备份和恢复流程，必要时对备份和恢复过程进行演练，并对备份数据进行定期校验。

8.3 日志与用户数据记录

8.3.1 互联网交互式服务提供者应记录用户注册的相关信息，包括用户唯一标识、用户名称及修改记录、实名信息、注册时间、IP 地址及源端口、用户备注信息等，其中实名信息可为姓名、证件类型、证件号码、电子邮箱地址、手机号码等。

8.3.2 对于记录的用户活动日志，其内容应包括但不限于：

a） 用户的登录日志，包括：

1） 用户唯一标识；

2） 登录时间；

3） 退出时间；

4） IP 地址及端口号。

b） 用户的信息发布日志，包括：

1） 用户唯一标识；

2） 信息标识；

3） 信息发布时间；

4） IP 地址及端口号；

5） 信息标题或摘要，包括图片摘要。

c） 用户的行为日志，包括：

1） 发布、修改、删除所发信息的行为；

2） 上传、下载文件的行为；

3） 用户自身属性变更的行为。

d） 匿名用户行为，包括：

1） 访问时间；

2） 来源 IP 地址。

适用时，应记录使用客户端终端设备的标识、位置。

8.3.3 互联网交互式服务提供者应确保日志内容的可溯源性，即可追溯到用户 ID、网络地址和协议。涉及消息服务的，应能防范伪造、隐匿发送者真实标记的消息的措施；涉及地址转换技术的服务，如移动上网、网络代理、内容分发等，应记录转换前后的地址与端口信息；涉及短网址服务的，应记录原始 URL 与短 URL 之间的映射关系。

8.3.4 互联网交互式服务提供者应确保日志与用户数据记录的时间由系统范围内唯一确定的时钟产生。

8.3.5 互联网交互式服务提供者应保护日志，确保无法单独中断审计进程，防止未授权的删除、修改和覆盖。

8.3.6 互联网交互式服务提供者应根据公安机关要求留存用户访问指定信息的日志。

8.3.7 互联网交互式服务提供者应留存相关的日志和用户数据，具体保存周期要求如下：

a） 永久保留用户注册信息及历史变更记录；

b） 留存网络运行日志和系统维护日志不少于 6 个月；

c） 留存网络安全事件日志不少于 6 个月；

d） 留存用户活动日志不少于 6 个月；

e） 留存用户发布的信息内容不少于 6 个月。

9 业务安全

9.1 安全评估及报备

互联网交互式服务者应在互联网服务安全评估制度中明确互联网新服务、新功能应在上线前进行安全评估，应制定信息网络安全技术方案，并将安全风险评估结果向管辖地公安机关报备。

9.2 用户管理

9.2.1 互联网交互式服务提供者应在用户注册时，与用户签订服务协议，告知相关权利义务及需承担的法律责任。

9.2.2 互联网交互式服务提供者应建立用户管理机制，包括但不限于：

a) 对用户真实身份信息进行有效核验，有校核验方法应能追溯到用户登记的真实身份，如：
   1) 身份证与姓名的实名验证服务；
   2) 有效的银行卡；
   3) 合法、有效的数字证书；
   4) 已确认真实身份的网络服务的注册用户；
   5) 经电信运营商接入实名认证的用户；
   6) 生物特征。
b) 禁止匿名用户的信息发布权限，仅提供基本的浏览、查看等功能。
c) 对用户的账号、昵称、头像和备注等信息进行审核，禁止使用以下内容：
   1) 违反国家现行法律法规规定的；
   2) 违背社会公序良俗的；
   3) 容易引起公众不良反应或误解的。
d) 建立用户黑名单制度，对互联网交互式服务提供者自行发现以及公安机关通报的多次、大量发送传播违法有害信息的用户应纳入黑名单管理。

注：如某网站采用已经实名认证的第三方帐户登录，可认为该网站的用户已进行有效核验。

9.2.3 当用户利用互联网从事的服务需要行政许可时，互联网交互式服务提供者应查验其合法资质，查验可以通过以下方法进行：

a) 通过核对行政许可文件查验；
b) 通过行政许可主管部门的公开信息查验；
c) 通过行政许可主管部门的验证电话、验证平台查验。

9.3 违法有害信息防范和处置

9.3.1 互联网交互式服务提供者应建立与交互式服务特点相符的信息巡查制度，及时发现并处置违法有害信息。

9.3.2 互联网交互式服务提供者应采取管理与技术措施，及时发现并停止违法有害信息的发布。

9.3.3 互联网交互式服务提供者应采用人工或自动化方式，对发布的信息进行审核或过滤。

9.3.4 互联网交互式服务提供者应采取技术措施过滤违法有害信息，包括但不限于：

a) 基于关键词的违法有害文字信息(支持文字的变种、混淆等)的屏蔽过滤；
b) 基于样本数据特征值的违法有害音视频、图片的屏蔽过滤；
c) 基于违法有害外域链接的屏蔽过滤。

9.3.5 互联网交互式服务提供者应采取技术措施对违法有害信息的来源实施控制，防止继续传播。违法有害信息来源控制技术措施包括但不限于：封禁特定账号、禁止新建账号、禁止分享、禁止留言及回复、控制特定发布来源、控制特定地区或指定 IP 账号登陆、禁止客户端推送、切断与第三方应用的互联互通等。

9.3.6 互联网交互式服务提供者应建立涉嫌违法犯罪线索、异常情况报告、安全提示和案件调查配合机制，包括：

a) 对发现的违法有害信息，立即停止发布传输，保留相关证据(包括用户注册信息、用户登录信息、用户发布信息等记录)，并向属地公安机关报告；
b) 对于煽动非法聚集、策划恐怖活动、扬言实施个人极端行为等重要情况或重大紧急事件立即向属地公安机关报告，同时配合公安机关做好调查取证工作；
c) 在不破坏数据完整性、有效性的前提下，将相关电子数据及时传给属地公安机关，通知相应的

公安机关进行现场处理。

9.3.7 互联网交互式服务提供者应与公安机关建立全天候的违法有害信息快速处置工作机制，应能及时删除有明确 URL 的单条违法有害信息，特定文本、图片、视频、链接等信息的源头以及分享中的任一环节，相关的屏蔽过滤措施应能及时生效。

9.4 破坏性程序防范

9.4.1 互联网交互式服务提供者应能发现破坏性程序并采取措施立即停止发布，同时保留发现的破坏性程序的相关证据。

9.4.2 对软件下载服务提供者（包括应用软件商店），其应检查用户发布的软件是否含有计算机病毒等恶意代码。

10 个人信息保护

10.1 处理规则

10.1.1 网络交互式服务提供者应在个人信息保护制度中明确个人信息收集、使用、处理规则，并在显著位置予以公示。在用户注册时，应在与用户签订服务协议中明示收集、使用、处理个人信息的目的、范围与方式。

10.1.2 网络交互式服务提供者仅收集为实现正当商业目的和提供网络服务所必需的个人信息；收集个人信息时，应取得用户明确授权同意；将个人信息交给第三方处理时，处理方应符合本部分要求，并取得用户明确授权同意；法律、行政法规另有规定的，从其规定。

10.1.3 修改个人信息处理规则时，网络交互式服务提供者应告知用户，并取得其同意。

10.2 技术措施

网络交互式服务提供者应建立覆盖个人信息处理的各个环节的安全保护制度和技术措施，防止个人信息泄露、损毁、丢失，包括：

a) 采用加密方式保存用户密码等重要信息；
b) 对内部员工涉及个人信息的所有操作进行审计，并对审计结果进行分析，预防内部员工故意泄露；
c) 对个人信息的采集、存储或传输行为进行审计，作为信息是否泄露、毁损、丢失的查询依据；
d) 建立程序来控制对涉及个人信息的系统和服务的访问权的分配，这些程序涵盖用户访问生存周期内的各个阶段。

10.3 个人信息安全事件应急处置

对于个人信息安全事件安全事件，互联网交互式服务提供者应具备以下能力：

a) 发现并识别个人信息安全事件，同时保留原始记录；
b) 立即采取补救措施，防止信息安全事件继续发生；
c) 及时告知用户，并立即报告属地公安机关。

11 投诉

11.1 投诉制度

网络交互式服务提供者应在用户投诉举报接收处理制度中明确用户投诉举报渠道、处理流程、方式、时限，鼓励用户举报违法有害信息。

11.2 受理与处理

网络交互式服务提供者应遵循合法、合理、公平、公正、及时准确的基本原则，积极维护国家利益、公共利益和行业利益，尊重用户的合法权益。

网络交互式服务提供者应验证与处理用户投诉，并将处理结果反馈投诉人。

11.3 投诉渠道

网络交互式服务提供者应根据业务类型、投诉数量和投诉内容等建立适当的投诉渠道，如线上投诉、上门投诉、电话投诉、传真投诉、邮件投诉、快递投诉等。

网络交互式服务提供者应以明显可见的方式向社会公开投诉渠道。

11.4 记录留存

网络交互式服务提供者应保存投诉处理的全部记录，保证可追溯。

12 分包服务

12.1 基本要求

12.1.1 互联网交互式服务提供者可将本部分的安全保护要求分包。

12.1.2 分包安全保护工作时，网络交互式服务提供者应：

a) 查验分包方的相关资质，明确分包方的安全服务交付水准；

b) 与分包方签订与安全有关的协议，明确约定相关责任。

12.2 分包商要求

分包商也应达到本部分的安全要求。

12.3 不可分包的项目

依据法律法规、标准规定不可分包的项目，互联网交互式服务提供者不得分包。

13 安全事件管理

13.1 安全事件分类

13.1.1 网络交互式服务提供者应在安全事件管理制度中明确安全事件的监测、报告和应急处置流程，确保快速、有效和有序地响应安全事件。

13.1.2 安全事件应包括违法有害信息、危害计算机信息系统安全的异常情况(如系统漏洞、计算机病毒、网络攻击、网络入侵等)及突发公共事件。

13.2 应急预案

网络交互式服务提供者应制定安全事件应急处置预案，向属地公安机关报备，并定期开展应急演练。

13.3 突发公共事件处理

网络交互式服务提供者应参照 GB/Z 20986—2007 将突发公共事件分为四级：Ⅰ级（特别重大事件）、Ⅱ级（重大事件）、Ⅲ级（较大事件）、Ⅳ级（一般事件），互联网交互式服务提供者应建立相应处置机制，当突发公共事件发生后，投入相应的人力与技术措施开展处置工作：

a) Ⅰ级：应投入安全管理等部门 80％甚至全部人力开展处置工作；

b) Ⅱ级：应投入安全管理等部门 50％～80％的人力开展处置工作；

c) Ⅲ级：应投入安全管理等部门 30％～50％的人力开展处置工作；

d) Ⅳ级：应投入安全管理等部门 30％的人力开展处置工作。

13.4 技术接口

网络交互式服务提供者应为公安机关提供符合国家标准或公共安全行业标准的技术接口，确保实时、有效地提供相关证据。

参 考 文 献

[1] 计算机信息网络国际联网安全保护管理办法,1997 年 12 月 11 日国务院批准,1997 年 12 月 16 日公安部令第 33 号发布,1997 年 12 月 30 日实施,2011 年 1 月 8 日修订.

[2] 互联网安全保护技术措施规定,2005 年 12 月 13 日公安部令第 82 号发布,2006 年 3 月 1 日起施行.

[3] 国家突发公共事件总体应急预案,2005 年 1 月 26 日国务院第 79 次常务会议通过,2006 年 1 月 8 日发布并实施).

[4] 信息安全等级保护管理办法,2007 年 6 月 22 日公通字[2007]43 号印发.

[5] 中华人民共和国网络安全法,2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过,2017 年 6 月 1 日实施.

中华人民共和国公共安全
行业标准
互联网交互式服务安全管理要求
第1部分:基本要求
GA 1277.1—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2020年10月第一版
*
书号:155066·2-35598

GA 1277.1-2020