附件 1：关于印发《物联网卡安全分类管理实施指引（试行）》的通知

详见下一页。

工业和信息化部司局简函

工网安函〔2020〕1173号

关于印发《物联网卡安全分类管理实施指引（试行）》的通知

中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司：

按照《工业和信息化部办公厅关于加强物联网卡安全管理工作的通知》（工信厅网安〔2020〕9号）要求以及工业和信息化部2020年重点工作部署，进一步加强物联网卡安全管理，防范被电信网络诈骗、暴力恐怖等违法犯罪活动利用，我局组织三家基础电信企业、中国信息通信研究院编写了《物联网卡安全分类管理实施指引（试行）》（以下称《实施指引》），指导各电信企业规范开展物联网卡分类登记和安全管理工作。经征求各单位意见，目前已就《实施指引》主要内容达成一致意见。

现将《实施指引》印发给你们，请对照制定本企业物联网卡安全管理规范，明确安全管理制度、责任体系和技术措施，抓好贯彻落实，切实保障物联网健康有序发展。请各集团公司于9月15日前将本企业制定的物联网卡安全管理规范报我局，并于2021年1月底前总结报送试行情况。

工业和信息化部网络安全管理局

2020年8月17日

（联系方式：010-68206196）

抄送：各省、自治区、直辖市通信管理局；中国信息通信研究院。

物联网卡安全分类管理实施指引

为进一步加强物联网卡安全管理，促进物联网业务健康发展，根据《工业和信息化部办公厅关于加强物联网卡安全管理工作的通知》（工信厅网安〔2020〕9号）要求，制定本指引。

本指引规定了物联网卡安全分类管理的基本要求，主要包括：物联网卡功能定义、安全管理技术措施、分类安全管理和用户入网管理（含开户、过户）等要求，指导电信企业开展物联网卡安全管理工作。

1 物联网卡功能定义

物联网卡是指基于蜂窝移动通信网络，实现人、机、物之间通信连接的用户识别卡，要求采用物联网专用号码作为通信号码，承载于物联网核心网专用网元。

1.1 语音功能

（1）定向语音

定向语音是指使用物联网卡只能与特定号码进行语音通话，包括呼入和呼出方向。各电信企业应按照最小必要原则，严格限制语音通话的白名单号码数量，原则上语音呼入和呼出的白名单号码数量合计不超过5个。

电信企业应严格限制定向语音白名单的变更次数，对于确需变更的，电信企业应加强审核，明确电信企业审核责任人，并留存签字审核表。

（2）非定向语音

非定向语音是指使用物联网卡可进行语音通话对象不受限制，包括呼入和呼出。

1.2 短信功能

（1）定向短信

定向短信是指使用物联网卡仅能与短信管理平台的号码进行收发短信，不允许物联网卡与物联网卡之间、物联网卡与公众移动网电话号码之间收发短信。各物联网卡对应的短信管理

平台号码由电信企业自行分配，原则上每张物联网卡绑定的平台号码数量（含发送和接收）合计不超过5个。

电信企业应严格限制定向短信白名单的变更次数，对于确需变更的，电信企业应加强审核，明确电信企业审核责任人，并留存签字审核表。

（2）非定向短信

非定向短信是指使用物联网卡发送或接收短信的对象不受限制。

1.3 流量功能

根据物联网卡流量功能是否受限，可分为定向流量和非定向流量。按照物联网卡使用流量额度，可以分为大流量和小流量。结合安全风险，物联网卡流量功能总体可分为定向流量、非定向大流量和非定向小流量。

（1）定向流量

定向流量是指可通过技术措施限定物联网卡仅能访问特定的IP或URL地址，原则上定向流量访问的IP和URL地址白名单数量合计不超过10个。

电信企业应严格限制定向流量白名单变更次数，对于确需变更的，电信企业应加强审核，明确电信企业审核责任人，并留存签字审核表。

（2）非定向小流量

非定向小流量指使用物联网卡可访问公网IP或URL地址不受限制，且月均使用流量不超过100MB。

（3）非定向大流量

非定向大流量是指使用物联网卡可访问公网IP或URL地址不受限制，且月均使用流量大于100MB。

2 物联网卡安全管理措施

2.1 前置规范管理

2.1.1 专用号段

专用号段是指工业和信息化部颁发给电信企业的用于物联网、机器通信等专用码号资源。电信企业在发展物联网用户时，

应严格使用物联网卡专用号段，并定期对专用号段使用合规性进行抽查。

2.1.2 卡片限定

卡片限定是指通过嵌入、焊接、非标等方式，实现物联网卡与终端进行物理绑定的技术手段，有效防止物联网卡被挪用。主要表现为贴片卡、eSIM卡和异形卡等，其中异形卡是通过改变SIM卡的形状和大小，仅在特定物联网终端中可以使用。

2.1.3 机卡绑定

机卡绑定主要是针对可插拔的普通SIM卡，通过在相应的系统平台配置机卡绑定参数实现物联网卡与终端的软绑定。具体实现方式可分为两类：一类是电信企业在网络侧或连接管理平台上配置终端IMEI与物联网号码、终端IMEI池与物联网号码池的绑定关系；另一类是在终端侧采用机卡互锁方式。物联网机卡绑定仅能由电信企业进行操作，不得由购卡用户自行操作。

（1）网络侧机卡绑定

一是通过HSS签约功能实现绑定。物联网号码在HSS签约机卡绑定功能；用户提前告知电信企业物联网终端的IMEI信息，由电信企业在网络侧进行配置，将IMEI与相应的物联网号码进行绑定；或终端首次发生通信行为时，通过省内无线网络接入后，上报实际设备的IMEI值到MME，MME设备将用户硬件信息上报到HSS，HSS将设备IMEI与IMSI进行绑定；之后，终端再次发生通信行为时，HSS核对用户的硬件信息和绑定的IMEI是否一致，如不一致，则直接拒绝用户接入。

二是通过连接管理平台实现绑定。终端首次发生通信行为时，通过网络侧抓取终端设备的IMEI值，并在电信企业物联网连接管理平台上存储该IMEI值与物联网号码的对应关系；后续物联网卡请求连接到网络时，物联网连接管理平台自动检查设备的IMEI值与物联网号码的对应关系，如不一致，则对物联网卡拒绝接入或采取停机措施。

三是通过IMEI池绑定。用户提前告知电信企业物联网终端的IMEI池信息，由电信企业在物联网连接管理平台或其他业务平台上进行配置，对应到相应的账户。终端发生通信行为时，

通过网络侧抓取终端设备的IMEI信息，并将抓取到的IMEI值抄送给相应的平台，由平台将该IMEI值与IMEI池进行比较。如果不在IMEI池内，则拒绝为用户提供服务。

（2）终端侧机卡互锁方式

在物联网卡内单独设置一个区域，用于存储要绑定的终端IMEI值；用户提前告知电信企业物联网终端的IMEI信息，由电信企业写入物联网卡内；终端开机后读取出物联网卡内存储的IMEI值，并与终端自身IMEI值进行比较，判断是否一致。如判定为否，则停止通信功能服务。采用此种方式的物联网终端需要具备判断IMEI值的功能。

2.2 业务功能限定

2.2.1 区域限制

对于终端设备位置固定的物联网场景，如水表、电表、市政监控设备、环境监测设备等，应严格限定物联网卡使用位置地点，如绑定基站标识或限制接入基站数量等。

对于终端设备限定在一定地理范围内使用的物联网场景，电信企业应通过技术手段严格限定其使用区域，限定区域不得超过省级范围。

2.2.2 限额管控

限额管控是指结合使用场景和使用需求，限制物联网卡的业务使用量。电信企业应结合物联网卡的网络制式、使用需求，对物联网卡业务使用量进行分档限额管理。对于达到限定使用量的物联网卡，电信企业应及时暂停服务。

2.2.3 定向访问

（1）定向语音

定向语音的实现方式主要包括：网络侧通过智能网进行语音控制，以及其他可以实现与固定的号码进行语音通话的技术手段。

通过智能网进行语音控制主要是通过智能网的SCP网元实现。通过智能网SCP的控制，可以限制语音呼出和呼入的白名单，从而实现物联网卡的定向语音功能。具体流程为，当主叫发起呼叫后，经过交换设备SSP（MSC/VLR），SSP查询信息并发送至

SCP，SCP根据SSP上报来的呼叫事件启动不同的业务逻辑，然后向SSP发出呼叫控制指令，指示SSP进行下一步的动作，例如收号、接续、放音等等，从而实现各种智能业务。

（2）定向短信

定向短信的实现方式可通过专用短信中心和专用网关控制短信收发号码，实现物联网卡仅可以与特定平台号码收发短信。

点对平台定向短信的实现流程为：当行业用户申请开通短信功能时，电信企业为其分配一个短信接入号码，即短信管理平台号码。电信企业在相关平台上配置短信接入号码后，配置后的短信接入码自动同步至业务网关。完成配置后，告知用户短信接入信息并配合用户进行接入联调。当物联网终端发送短信时，会经过省 MSC 设备转发至专用短信中心，经过物联网业务网关后发送至业务平台。

（3）定向流量

定向流量的实现方式包括：专线 VPDN、专用 APN、网络侧设置访问白名单、接入侧控制，以及其他可以实现仅访问固定的 IP 或 URL 地址的方式。

方式一：专线 VPDN

专线 VPDN 是通过 IP 承载网及传输专线的方式实现的。采用此种方式，需要客户平台通过传输专线连接至省公司的 AR 设备，通过 IP 专网 MPLS VPN+GRE（L2TP、IPsec）隧道的方式与 PGW 互通。

方式二：专用 APN

专用 APN 是通过各类 VPN 技术在公网疏通的逻辑隧道进行接入的。通过 GRE 方式实现企业 VPN 方案，终端通过 IP 方式的 PDP/承载激活接入到移动数据网络，移动数据网络提供到客户数据中心企业的接入，即 GGSN 提供到企业网的接入，移动数据网络为企业所在网络分配 APN。电信企业通过 APN 标识用户业务种类，同时对用户的业务访问权限进行控制。采用专用 APN 后，物联网终端的访问流程为：BTS/eNodeB->BSC->SGSN/MME+SGW->专网 GGSN/PGW，通过公网隧道连接集团客户数据中心。

方式三：网络侧设置访问白名单

网络侧设置访问白名单的具体实现流程如下：在物联网专网 PCRF 上或直接在专网 PGW 上设置物联网用户开户及策略控制；用户访问网络时，PGW 将首先到 PCRF 上查询用户签约时的业务策略，并且使对应的业务策略规则生效；如果用户访问的 IP 或 URL 地址在白名单内，则继续访问特定的业务平台或应用系统；如果不在白名单内，则停止访问。

方式四：接入侧控制

接入侧控制主要是通过在接入侧终端或网关中配备相应的安全能力，使得终端或网关具备接收、执行安全策略以及上报访问行为数据等能力。其中，安全策略包括设置黑白名单列表、限制访问能力等。

接入侧控制的技术思路如下：对于加载安全能力的终端，安全管理平台将安全策略直接下发至终端。终端访问应用平台时，自身安全能力将执行安全策略，判断目的 IP 地址、URL 等是否在黑白名单中。如在白名单中，则正常访问；如在黑名单中或不在白名单中，则拒绝访问。对于已部署安全管控功能的网关，可实现流量定向访问。具体实现为：根据不同业务配置的安全策略，当终端向网关发起流量访问请求时，网关通过自身安全能力执行安全策略，判断目的 IP 地址、URL 等是否在黑白名单中。如在白名单中，则正常接续访问；如在黑名单中或不在白名单中，则拒绝接续访问。

2.2.4 黑名单限制

黑名单限制是指通过在网络侧设置业务访问黑名单，或者在接入侧进行安全策略控制，技术原理及实现方式同5.2.3节。为有效防范物联网卡被违规挪用于手机上网业务，黑名单至少应包括以下4种类型的互联网应用：

1. 社交类网站：如微信、QQ、微博等；
2. 视频类网站：如抖音、快手、优酷、爱奇艺、腾讯视频等；
3. 购物类网站：如淘宝、京东、唯品会等；
4. 游戏类网站：如 QQ 游戏等。

电信企业可在此基础上，针对不同的物联网业务场景，在黑名单中增加互联网应用限制。

2.3 后向使用监测

2.3.1 业务合规监测

（1）机卡分离监测

机卡分离是指物联网卡被从一个物联网终端中拔出，在另一个终端设备中使用的行为。电信企业应按照前置规范管理要求对物联网卡与物联网终端进行机卡绑定，当物联网卡与终端的绑定关系发生变化或用在非IMEI池中的终端上时，电信企业应能及时发现，并输出相关的机卡分离记录。

（2）跨区域使用监测

跨区域使用是指某些可以固定在某个位置或区域使用、通常不会发生位置移动的物联网设备发生通信位置变化的行为。电信企业应针对此类物联网卡进行跨区域使用监测，通过分析物联网话单数据中使用所在地的小区标识，对物联网卡使用区域进行精细化监测。如超出物联网卡使用区域，电信企业应输出相关的跨区域使用记录。

可固定在某个位置使用的物联网卡使用场景包括但不限于以下场景：

1 公共服务：电梯报警、视频监控、市政设施、智能抄表、环境监测、智慧停车等；

2 零售服务：智能广告等；

3 智慧农业：环境监测等；

4 智慧工业：采集类设备、视频监控等；

5 智慧物流：智能快递柜、仓储视频监控等。

（3）超阈值使用监测

超阈值使用是指物联网卡每个月的短信、流量实际使用量超过开户时选择的使用量阈值的行为。电信企业应对物联网卡超阈值使用的行为进行监测，且在发现物联网卡超阈值使用后，输出相关的超阈值使用记录。

（4）超白名单使用监测

超白名单使用是指物联网卡的语音主被叫号码超出开户时设定的语音白名单号码、短信收发号码超出开户时设定的短信白名单号码、访问的IP或URL地址超出定向访问白名单号码的通信行为。电信企业应对物联网卡超白名单使用的情况进行监测，且在发现物联网卡超白名单使用后，输出相关的超白名单使用记录。

2.3.2 异常使用监测

（5）手机终端使用监测

手机终端使用是指物联网卡被放置在手机终端上使用的行为。电信企业应基于各企业内部的手机终端IMEI库，对物联网卡所使用的终端IMEI值进行监测。当发现物联网卡被使用在手机终端上时，应输出相关的手机终端使用记录。

（6）异常使用行为监测

异常使用行为是指物联网卡产生了与合同规定场景不符的业务使用行为，如典型的人联网应用访问行为。电信企业应通过分析物联网卡实际访问的URL地址，查看其是否访问了典型人联网应用。当发现物联网卡发生异常访问行为时，应输出相关的异常使用记录，并及时更新黑名单限制列表。

典型人联网应用包括但不限于以下：

① 社交类网站：如微信、QQ、微博等；

② 视频类网站：如抖音、快手、优酷、爱奇艺、腾讯视频等；

③ 购物类网站：如淘宝、京东、唯品会等；

④ 游戏类网站：如QQ游戏等。

电信企业可在此基础上，进一步增加其他人联网应用监测。

（7）异常流量使用监测

异常流量使用是指物联网卡当月流量使用量大于前三个月月均流量使用量2倍以上的行为。电信企业应对物联网卡异常流量使用的行为进行监测，且在发现物联网卡流量使用异常后，输出相关的异常流量使用记录。

（8）异常短信使用监测

异常短信使用是指物联网卡当月短信使用量大于前三个月月均短信发送量2倍以上的行为。电信企业应对物联网卡短信异常使用的行为进行监测，且在发现物联网卡短信使用异常后，输出相关的异常短信使用记录。

2.3.3 重点场景监测

（9）漫游至诈骗高发区使用监测

漫游至诈骗高发区使用是指物联网卡漫游至诈骗高发区使用的行为。电信企业应针对物联网卡的使用地点进行监测，当发现物联网卡漫游至诈骗高发区使用时，应输出相关的漫游至诈骗高发区使用记录。

（10）其他监测模型

对于超出以上9类监测模型的，企业可自行定义。

3 物联网卡安全管理基本要求

3.1 基本原则

3.1.1 责任对等原则

按照“谁销售、谁负责”的原则，电信企业为物联网卡安全管理的第一责任人，应采取有效技术和管理措施加强物联网卡安全管理，防止物联网卡被挪用或违规使用。

3.1.2 最小必要原则

物联网卡所开通功能、业务范围（包括可访问的IP地址、端口、通话及短信号码等）须与合同所约定的业务场景保持严格一致。

3.1.3 分类登记原则

结合物联网卡开通功能、业务属性等因素，通过综合评定物联网卡安全风险，分类实施登记管理。可参考附录《物联网卡行业分类及安全风险分析》。

3.2 总体要求

物联网卡安全管理总体要求，应至少包括以下：

（1）物联网卡默认应关闭语音、短信功能。对于确需开通的，须严格实施定向限制。

（2）对于开通流量功能的物联网卡，应设置最小必要数据流量限额。

（3）对于开通定向大流量的物联网卡，须采用机卡绑定和黑名单限制手段；

（4）对于开通非定向大流量的物联网卡，须严格采用卡片限定技术措施；

（5）对于位置范围固定的物联网卡，须实施区域限制。

3.3 物联网卡分类安全管理要求

3.3.1 开通全业务功能物联网卡

对于开通全业务功能的物联网卡，按照业务属性可分为5类场景，电信企业应采取管控措施，并做好用户登记。

（1）针对场景1和2，在可实现流量定向访问限制的情况下，电信企业应实施定向语音、定向短信和定向流量管控限制，并采取机卡绑定、限额管控、黑名单限制、使用监测等措施降低安全风险。在此基础上，电信企业可登记责任单位和责任人信息。

（2）针对场景3和4，在流量无法实施定向限制，且开通大流量的情况下，针对位置固定的物联网卡，电信企业应实施定向语音、定向短信限制，采取卡片限定、区域限制、黑名单限制、使用监测等措施，防止作为流量卡使用。在此基础上，可登记到责任单位和责任人。针对位置不固定的物联网卡，电信企业应实施定向语音、定向短信限制，采取卡片限定、使用监测等措施，并登记到实际使用人。

（3）针对场景5和6，在流量无法实施定向限制，且开通小流量的情况下，针对位置固定的物联网卡，电信企业应实施定向语音、定向短信限制，采取区域限制、限额管控、黑名单限制，机卡绑定、使用监测等措施，降低挪用风险。在此基础上，可登记到责任单位和责任人。针对位置不固定的物联网卡，电信企业应实施定向语音、定向短信限制，采取限额管控、黑名单限制、机卡绑定、使用监测等措施，并登记到责任单位和责任人。

表1 开通全功能的物联网卡场景及管控要求

分类	售前评估						原始安全风险	技术管控										登记要求		典型行业应用
	业务功能			业务属性				特定措施							通用措施					
								定向限制			卡片限定	区域限制	限额管控	黑名单限制	机卡绑定	使用监测			
	语音	短信	流量	流量定向	大流量	位置固定		定向语音	定向短信	定向流量							实名个人	登记单位	
1	√	√	√	√	√	–	中风险	√	√	√		√		√	√	√		√	公共安全（电梯报警）
2	√	√	√	√	×	–	中风险	√	√	√			√		√	√		√	个人医疗设备等
3	√	√	√	×	√	√	中风险	√	√		√	√		√		√		√	智能快递柜等
4	√	√	√	×	√	×	高风险	√	√		√					√	√		车联网、个人可穿戴设备、移动办公等
5	√	√	√	×	×	√	中风险	√	√			√	√	√	√	√		√	–
6	√	√	√	×	×	×	中风险	√	√				√	√	√	√		√	–

注：“√”代表满足此条件；“×”代表不满足此条件；“–”代表无需考虑此属性；

3.3.2 开通短信和流量功能物联网卡

对于开通短信和流量功能的物联网卡，按照业务属性可分为5类场景，电信企业应对应采取管控措施，并做好用户登记。

（1）针对场景1和2，在可实现流量定向访问限制的情况下，电信企业应实施定向短信和定向流量管控限制，并采取机卡绑定、黑名单限制、限额管控、使用监测等措施降低安全风险。在此基础上，电信企业可登记责任单位和责任人信息。

（2）针对场景3和4，在流量无法实施定向限制，且开通大流量的情况下，针对位置固定的物联网卡，电信企业应实施定向短信限制，采取卡片限定、区域限制、黑名单限制、使用监测等措施，防止作为流量卡使用。在此基础上，可登记到责任单位和责任人。针对位置不固定的物联网卡，电信企业应实施定向短信限制，采取卡片限定、使用监测等措施，并登记到实际使用人。

（3）针对场景5和6，在流量无法实施定向限制，且开通小流量的情况下，针对位置固定的物联网卡，电信企业应实施定向短信限制，采取区域限制、限额管控、黑名单限制，机卡绑定、使用监测等措施，降低挪用风险。在此基础上，可登记到责任单位和责任人。针对位置不固定的物联网卡，电信企业应实施定向短信限制，采取限额管控、黑名单限制、机卡绑定、使用监测等措施，并登记到责任单位和责任人。

表2 开通短信和流量功能的物联网卡场景及管控要求

分类	售前评估						原始安全风险	技术管控										登记要求		典型行业应用
	业务功能			业务属性				特定措施							通用措施					
								定向限制			卡片限定	区域限制	限额管控	黑名单限制	机卡绑定	使用监测			
	语音	短信	流量	流量定向	大流量	位置固定		定向语音	定向短信	定向流量							实名个人	登记单位	
1	×	√	√	√	√	-	中风险		√	√		√		√	√	√		√	视频监控类、工业采集等
2	×	√	√	√	×	-	中风险		√	√			√		√	√		√	环境监测等
3	×	√	√	×	√	√	中风险		√		√	√		√		√		√	智能广告等
4	×	√	√	×	√	×	高风险		√		√					√	√		手持终端等
5	×	√	√	×	×	√	中风险		√			√	√	√	√	√		√	市政设施、智能抄表等
6	×	√	√	×	×	×	中风险		√				√	√	√	√		√	货物跟踪等

注：“√”代表满足此条件；“×”代表不满足此条件；“-”代表无需考虑此属性；

3.3.3 仅开通流量功能物联网卡

对于仅开通流量功能的物联网卡，按照业务属性可分为5类场景，电信企业应对应采取管控措施，并做好用户登记。

（1）针对场景1和2，在可实现流量定向访问限制的情况下，电信企业应实施定向流量管控限制，并采取机卡绑定、黑名单限制、限额管控、使用监测等措施降低安全风险。在此基础上，电信企业可登记责任单位和责任人信息。

（2）针对场景3和4，在流量无法实施定向限制，且开通大流量的情况下，针对位置固定的物联网卡，电信企业应采取卡片限定、区域限制、黑名单限制、使用监测等措施，防止作为流量卡使用。在此基础上，可登记到责任单位和责任人。针对位置不固定的物联网卡，电信企业应采取卡片限定、使用监测等措施，并登记到实际使用人。

（3）针对场景5和6，在流量无法实施定向限制，且开通小流量的情况下，针对位置固定的物联网卡，电信企业应采取区域限制、限额管控、黑名单限制，机卡绑定、使用监测等措施，降低挪用风险。在此基础上，可登记到责任单位和责任人。针对位置不固定的物联网卡，电信企业应采取限额管控、黑名单限制、机卡绑定、使用监测等措施，并登记到责任单位和责任人。

表3 仅开通流量功能的物联网卡场景及管控要求

分类	售前评估						原始安全风险	技术管控									登记要求		典型行业应用
	业务功能			业务属性				特定措施							通用措施				
								定向限制			卡片限定	区域限制	限额管控	黑名单限制	机卡绑定	使用监测	实名个人	登记单位	
	语音	短信	流量	流量定向	大流量	位置固定		定向语音	定向短信	定向流量									
1	×	×	√	√	√	-	中风险			√		√		√	√	√		√	视频监控类、工业采集等
2	×	×	√	√	×	-	中风险			√			√		√	√		√	环境监测等
3	×	×	√	×	√	√	中风险				√	√		√		√		√	智能广告等
4	×	×	√	×	√	×	高风险				√					√	√		手持终端等
5	×	×	√	×	×	√	中风险					√	√	√	√	√		√	市政设施、智能抄表等
6	×	×	√	×	×	×	中风险						√	√	√	√		√	货物跟踪等

注：“√”代表满足此条件；“×”代表不满足此条件；“-”代表无需考虑此属性；

4　物联网卡入网管理规范

4.1　办理渠道要求

电信企业在向行业用户销售物联网卡时，应通过自有实体渠道或自有人员上门服务的方式办理。

4.2　出示证件要求

电信企业应要求行业用户提供单位有效证件、责任人和经办人有效证件、责任人和经办人的单位委托授权书。

（1）单位证件

单位有效证件应包括下列有效证件之一：

1）组织机构代码证；

2）营业执照；

3）加载统一社会信用代码的营业执照；

4）事业单位法人证书或社会团体法人登记证书；

5)法律、行政法规和国家规定的其他有效证件或证明文件。

（二）个人证件

经办人、责任人以及实际使用人应按照下列要求出示个人有效证件：

1）居住在中国境内的中国公民，应出具居民身份证、临时居民身份证或者户口簿；

2）中国人民解放军军人，中国人民武装警察办理用于个人或社会活动的电话号码，应出具居民身份证；办理用于执行公务、办理公务的电话号码，应出具军官证、士兵证、警官证等军队、武装警察部队制发的身份证件，并同时出具单位相关证明文件；

3）中国香港、中国澳门居民，应出具港澳居民往来内地通行证、港澳居民居住证或者其他有效旅行证件；中国台湾居民，应出具台湾居民来往大陆通行证、台湾居民居住证或者其他有效旅行证件；

4）外国公民，应出具护照或外国人永久居留身份证；外国人永久居留身份证的查验要求、使用场所等同居民身份证；

5）如无法提供第（1）至（4）项规定的身份证件的，可以使用法律、行政法规和国家规定的其他有效身份证件。

4.3 单位资质审核要求

电信企业应对物联网购卡行业用户单位资质做严格审核，审核要点包括但不限于：

（1）单位类型：购卡用户应为真实的物联网终端生产企业、物联网产品销售企业、物联网产品集成商、物联网平台运营企业、具有市政性质的央企和国企单位、具备真实合理使用场景的其他企业；

（2）注册时间：电信企业应对注册时间少于3个月的购卡用户，严格限制售卡数量，并确定为高风险用户；

（3）单位查验：电信企业应通过国家企业信用信息公示系统等途径认真查验购卡用户单位证件真实性、企业经营情况和信用情况。对于公安通报、媒体曝光、用户投诉举报的且经核实确属从事违法活动或违规销售物联网卡，以及被纳入物联网行业用户黑名单的购卡用户，电信企业不得向其销售物联网卡。

（4）现场考察：电信企业应对行业用户的使用场景进行现场考察，并留存现场考察材料，包括审核人员与行业用户单位的照片、设备照片、生产工厂或办公场所照片等。

（5）资料归档：电信企业在完成对行业用户的资质审核后，应由电信企业审核人员与行业用户经办人或负责人现场签字确认，并将签字单据和考察资料作为合同资料一并归档。

4.4 合同管理要求

电信企业与用户签订的物联网卡销售合同中，应明确物联网卡的使用场景、开通功能、用户身份信息登记、安全管理要求、禁止二次转售、防范垃圾短信和骚扰诈骗电话、违约责任等条款，并对违约使用和涉嫌违法犯罪活动的物联网卡约定处罚措施。当物联网卡停止使用后，电信企业应将物联网卡所开通的功能全部关闭，避免物联网卡被用作它途。

对于采用定向访问限制的物联网卡，电信企业应明确要求用户不得通过非法跳转的方式访问公网，如发现存在违规行为，电信企业应立即将该用户名下的同一批次物联网卡全部关停，由此产生的风险由用户自行承担。

4.5 证件真实性查验要求

对于单位有效证件，电信企业应根据有关部门已公布的单位有效证件判定规则，查验用户出示的单位有效证件真实性。对于具备技术查验条件的，电信企业应通过技术手段查验单位有效证件及所载信息的真实性。

对于个人有效证件，电信企业应使用居民身份证识别设备查验居民身份证、外国人永久居留身份证、港澳台居民居住证真实性，并通过居民身份识别设备自动读取和录入用户身份信息，严禁人工录入。鼓励与“全国公民身份信息库”联网查验用户身份信息。对于无法通过技术手段查验证件真实性查验的，电信企业受理人员应根据相关部门已公布的证件判定规则，核实个人有效证件的真实性。

4.6 人证一致性查验要求

对于登记至责任单位的场景，电信企业应查验经办人出示的身份证件的真实性和有效性，判断证件所载性别、照片等信息与经办人是否一致，并采用人像比对技术手段，做好用户人证一致性查验。

对于最终登记至实际使用人的场景，用户可持本人有效证件在电信企业自有营业厅办理实名登记。其中，对于持居民身份证、外国人永久居留身份证、港澳台居民居住证的用户，电信企业可通过网络渠道为其办理实名登记，要求用户上传个人有效证件正反面照片和用户正面免冠照片，并采用在线视频实人认证方式查验用户身份信息，确保用户人证一致。

4.7 现场拍照留存要求

对于登记至责任单位的场景，电信企业应现场拍摄留存一张经办人的正面免冠照片。

对于最终登记至实际使用人的场景，通过线下办理的，电信企业应现场拍摄留存一张实际使用人的正面免冠照；通过线上办理的，电信企业应在用户认证视频中随机截取和留存两张用户正面清晰照片。

电信企业应通过后台系统自动实时调用拍照设备，现场拍摄留存用户照片并上传后台系统。严禁未经现场拍摄通过本地上传用户照片和在本地保存用户照片。用户照片应使用 JPG、

BMP、PNG 等通用格式。照片像素不低于 48 万、照片文件大小不低于50KB、照片长宽比为 16:9 或 4:3。用户头像部分占比不小于照片的三分之一，且清晰可辨。留存照片应加盖水印，水印应注明照片用途和拍摄日期，并包含渠道编号信息或上门服务人员工号信息，拍摄日期应精确到秒。加盖水印应不影响照片关键信息的识别。

4.8 日志留存要求

电信企业应记录行业用户办理入网手续时的联网查验日志，并至少留存两年以上。联网查验日志应记录用户姓名、号码、联网查验时间和查验结果等。

4.9 用户登记要求

电信企业应如实登记证件类别、证件上所记载的姓名（名称）、号码、住址等信息。

（1）电信企业应参考6.3节分功能安全管理措施，对行业用户进行登记。

（2）对于最终流转到实际使用人使用的场景，在测试期内电信企业可登记责任单位和责任人信息，并参照登记到责任单位和责任人的场景进行安全功能限制。测试期结束后，电信企业应关闭物联网卡全部功能，直至流转到最终实际使用人时，应通过自有实体渠道或网络渠道为实际使用人办理用户登记，并开通相应功能。

（3）对于同一合同分批次开卡的，电信企业应在每批次开卡时均要求出示单位有效证件，经办人和责任人的有效证件及单位委托授权书，对行业用户及经办人、责任人的身份信息进行核查和登记，并拍摄留存经办人正面免冠照片。

（4）电信企业应严格限制登记到个人名下的物联网卡数量，同一用户在同一电信企业全国范围内名下所登记的物联网卡数量不超过10张。个人用户名下的物联网卡数量和公众移动电话卡数量分别单独统计。

（5）针对用户证件核验和录入要求，电信企业应参照《电话用户真实身份信息登记实施规范》（工信部网安[2018]105号）文件中有关要求进行办理。

附录　物联网卡行业分类和安全风险分析

1. 车联网

（1）车辆前装

车辆前装设备主要包括车载前装T-BOX、定位终端、一键救援等。车辆前装产品属于汽车原厂配置，多数是由车企从电信企业购卡，产品形态为贴片卡，采用焊接工艺，固定在前置车载设备中。前装产品类型较多，所需开通的功能各不相同，如一键救援需要语音，定位终端需要流量，部分设备激活或重启时需要短信。

安全风险分析：从卡片形态来看，车辆前装产品基本为贴片卡，无法拔出，挪用风险较低。从个人属性来看，车辆前装产品类型较多，对于仅向车企传送特定车辆数据的物联网卡，通常车主感知不到物联网卡的存在，无个人属性。但对于为车主提供服务的物联网卡，通常可关联到实际使用人，个人属性较强。从开通功能来看，车辆前装产品以用户购买服务为主，需要开通通用流量，存在一定的安全风险。

（2）车辆后装

车辆后装设备主要包括车载导航、行车记录仪、智能后视镜、一键救援、车载T-BOX、车载wifi等。物联网卡通常集成在后装设备中，用来为车主提供通讯、娱乐等服务。后装物联网卡多数使用可插拔式SIM卡。后装产品类型也较多，所需开通的功能各不相同，如车载导航需要访问网站，一键救援需开通语音功能，智能后视镜通常集成多种娱乐应用。

安全风险分析：从卡片形态来看，因多数为可插拔式SIM卡，存在被挪用的风险。从个人属性来看，车辆后装设备通常可关联到实际使用人。从开通功能来看，多数设备需要访问多种应用，且流量较大，因此，整体安全风险较高。

2. 公共服务

公共服务通过让市政设施智能互联，实现智能化管理的目标。当前公共服务中物联网卡的使用场景可分为以下7类：

（1）公共安全

主要用于公共区域中安全基础设施，包括安防视频监控设备、小区门禁系统、电梯报警、电梯维修检测以及智慧消防设备，如烟感设备、报警设备等。对于视频监控类设备，需要的流量较大；对于门禁系统、电梯报警等，需要开通语音功能，向物业管理人员拨打电话；对于智慧消防设备，仅需要小流量传输设备感知数据即可。对于公共安全类设备，通常位置较为固定。

安全风险分析：从个人属性来看，公共安全类设备通常部署在公共区域，难以对应到实际使用人。从开通功能来看，开通语音、短信的场景均可开通定向语音和定向短信，开通流量的场景，如视频监控，应实施定向限制，仅向特定的平台传输数据。对于无法实现定向流量的，存在违规滥用的风险。从使用位置来看，对于公共安全应用场景，电信企业可以通过监测使用位置的变化来发现安全风险。

（2）移动办公

移动办公类设备主要包括移动执法仪、PAD类办公设备等。此类设备主要是工作人员可以随身携带的设备，随时随地进行办公，目前行政执法、金融服务等领域应用较多。对于移动执法仪来说，主要用来拍摄并传送现场执法监控录像，以及联系相关人员，因此需要开通语音、流量业务。对于PAD类办公设备，主要用于访问专用的办公系统或特定的应用展示，如金融贷款服务平台、办公平台等。

安全风险分析：从购卡单位来看，多数为党政军客户、大型企事业单位，安全性较高。从个人属性来看，移动办公设备均为工作人员直接使用，可关联到实际使用人。从开通功能来看，需要语音和大流量业务，存在较高安全风险。

（3）市政设施

市政设施管理类设备主要包括智能化的路灯、智能井盖、为新能源汽车提供充电服务的充电桩、铁塔监控等。通常情况下仅需要传输小流量数据（不超过100MB），因此仅需要开通流量即可。特殊情况下，部分设备上带有广告应用，如公用充电

桩，需要通过特定平台推送广告，因此所需流量较大，但多数为下行流量。对于市政设施管理类设备，通常情况下位置固定。

安全风险分析：从个人属性来看，市政设施通常部署在公共区域，难以对应到实际使用人。从开通功能来看，无需语音功能，部分设备需要使用短信对设备进行激活或上报故障，个别场景需要卡通大流量。从使用位置来看，市政设施通常不会发生位置移动，电信企业可以通过监测使用位置的变化来发现安全风险。

（4）智能抄表

智能抄表类包括电表、水表、热表、气表等。此类设备多数为贴片卡，且网络制式多采用NB-IoT窄带物联网，速率较低且月均流量较小（不超过100MB），通常情况下仅需要小流量，且位置不会发生移动。

安全风险分析：此类设备主要为贴片卡，仅开通点对平台短信、小流量或定向流量，且使用位置不会发生变化，安全风险相对较小。

（5）环境监测

环境监测类设备主要包括空气质量监测、水质监测等设备。一般情况下仅需向特定平台传输监测数据，所需流量较小，且一般位置不会发生变化。

安全风险分析：与智能抄表类似，安全风险相对较小。

（6）智慧停车

智慧停车设备一般部署在停车场，实时掌握停车位的占用情况，通常情况下仅需要小流量，且位置较为固定，不会发生变化。

安全风险分析：从个人属性来看，通常部署在公共区域，难以对应到实际使用人。仅开通小流量或定向流量，且使用位置不会发生变化，安全风险相对较小。

（7）共享服务

共享服务包括共享自行车、共享电动车、共享充电宝、共享wifi设备等应用场景。共享自行车、共享电动车等设备仅需

要流量业务传输设备定位数据和使用情况数据。对于共享wifi设备，需开通通用流量功能，且流量较大，安全风险较高。

安全风险分析：对于开通小流量功能的共享自行车、共享电动车等设备，安全风险整体可控。对于共享wifi设备，安全风险较高，必须严格按照电话实名制相关要求进行实名登记。

3. 零售服务

（1）金融支付

金融支付包括无线POS机、自助终端、税控设备等。金融支付场景需要访问微信、支付宝、银联等多种支付场景，同时部分设备上还有广告业务，所需流量较大。

安全风险分析：从个人属性来看，无线POS机设备为商家所有，可关联到实际使用人。从开通功能来看，无需语音，需要开通较大流量，存在一定的安全风险。

（2）智能广告

智能广告主要是通过特定平台推送广告，所需流量较大，主要为下行流量。

安全风险分析：从个人属性来看，智能广告通常是部署在路边广告牌位置，难以对应到实际使用人，但使用位置相对固定。从开通功能来看，无需语音，需要较大流量。

4. 智慧家居

（1）个人可穿戴设备

个人可穿戴设备主要包括腕表、鞋类、智能眼镜、智能头盔、智能服装等产品形态，具有移动性强、交互性高、使用数据量大、产品形态丰富等特点。个人可穿戴设备中使用的物联网卡有贴片卡，也有可插拔卡，多数由设备厂家从电信企业购卡。各类可穿戴设备所需开通的功能各不相同，如腕表类产品需要开通全业务功能，部分产品激活需要短信功能，鞋类、智能头盔等各类应用需要使用流量传输数据。

安全风险分析：对于个人可穿戴设备场景，从个人属性来看，与人关联性较强。从开通功能来看，需要开通通用语音、通用短信、通用流量功能，且移动性较强，因此安全风险较高。

（2）智能家电

智能家电中的物联网卡多数属于家电设备原厂配置，采用贴片卡的形式居多，主要包括智能空调、智能冰箱、智能洗衣机等。对于智能家电设备来说，通常是将使用数据传送至特定的平台，以支撑对家电设备的管理和服务收费等，多数通过窄带物联网连接，且使用流量不大。

安全风险分析：从个人属性来看，智能家电多数为家庭使用，与人关联性较强。从开通功能来看，无需语音，部分设备需要使用短信对设备进行激活或上报故障，多数设备对于流量的使用要求较小，并可通过定向进行限制，安全风险较小。

（3）家庭安防

家庭安防主要包括视频监控、智能门锁等设备。对于视频监控来说，流量较大，但通常是向特定平台传输视频数据。对于智能门锁设备，使用流量通常不大，而且是向特定平台传输门锁相关信息。

安全风险分析：从个人属性来看，家庭安防基本为家庭使用，与人关联性较强。从开通功能来看，无需语音，仅需开通点对平台定向短信和定向流量功能，但流量使用量较大，因此存在一定的功能滥用风险。

（4）家庭网关

主要是实现路由转换和公网访问。所需流量通常较大，且需要访问各类网站。家庭网关中的物联网卡通常是由设备厂家从电信企业直接购买，放置在网关设备中。

安全风险分析：从个人属性来看，家庭网关是为家庭中的人员提供公网访问服务的，与人关联性较强。从开通功能来看，无需语音，但需要开通通用流量，且流量使用量较大，因此安全风险较高。

5. 智慧农业

（1）环境监测

环境监测设备包括温湿度监测设备、土壤监测设备、水利监测设备等，主要用于传输感知设备监测到的室内外环境各项参数。此类设备一般不需要语音，需要使用短信用于设备激活

或重启，需要开通流量向特定平台传输感知数据。同时，环境监测类设备一般部署后，位置不会发生变化。

安全风险分析：从个人属性来看，环境监测设备通常是部署在室外环境中的，与人关联性较弱。从开通功能来看，无需语音，部分设备需要开通点对平台定向短信，多数设备对于流量的使用要求较小，且可以做定向限制。从使用位置来看，设备部署后通常不会发生位置变化，电信企业可以后期通过监测使用位置的变化来发现安全风险，因此安全风险较小。

（2）定位场景

定位类设备主要是牲畜定位跟踪等，用于实时或定期向特定平台上报位置数据，具有使用位置不固定的特点。定位类设备多采用NB-IoT窄带物联网连接，速率较低且月均流量较小。

安全风险分析：从个人属性来看，定位类设备主要用于物体上，与人关联性较弱。从开通功能来看，无需语音，部分设备需要开通点对平台定向短信，多数设备对于流量的使用要求较小，且可以做定向限制用于实现对特定平台上报数据，安全风险较小。

6. 智慧工业

（1）采集类设备

采集类设备主要包括生产环境监控、设备运行状态监测、能耗监测设备等，用于向网关或特定平台传送各类设备的生产数据和自身数据。此类设备一般不需要语音，需要开通短信用于设备激活或重启，需要流量对采集信息进行上报，一般所需流量较小。

安全风险分析：从个人属性来看，采集设备主要部署于工业生产线上，难以关联到实际使用人。从开通功能来看，无需语音，需要点对平台定向短信及小流量用于传输采集数据，且可以定向限制，安全风险较小。从使用位置来看，采集类设备使用场景一般情况下位置较为固定。

（2）视频监控类设备

视频监控类设备主要包括工业生产线、工业园区内的视频监控设备。此类设备一般不需要语音，需要较大流量上传视频数据。

安全风险分析：从个人属性来看，视频监控设备主要部署于工业生产线上或工业园区内，难以关联到实际使用人。从开通功能来看，无需语音，但需要较大流量向特定平台进行视频数据传输。

（3）高端装备

高端装备主要包括数控机床、机器人、无人机等，使用物联网卡主要用于传输生产数据或回传视频等。一般不需要语音，需要短信用于设备的激活和故障上报，需要流量传输相关数据。若传输的是生产线上的生产数据，一般流量不需要太大；但若为回传视频，尤其是无人机回传的高清视频，所需流量较大。

安全风险分析：从个人属性来看，当前高端装备的应用场景主要为工业生产线、酒店服务、无人机航拍等，难以关联到实际使用人。从开通功能来看，针对高清视频回传，流量使用量较大，存在安全风险。

（4）工业网关类设备

工业网关中使用物联网卡主要用于访问公网，提供互联网接入服务。对于目前市场上的5G CPE设备，使用流量较大。

安全风险分析：从个人属性来看，难以关联到实际使用人。从开通功能来看，需要流量较大，且需要访问公网，因此安全风险较高。

7. 智慧医疗

（1）医院医疗设备

医院医疗设备包括佩戴在病人身上的监测设备、医生手持医疗终端、大型远程诊断设备等，主要用于医院使用。对于此类设备，通常不需要语音，需要开通短信用于设备的激活和故障上报。部分设备所需流量较小，仅需向特定平台上传病人的病案信息，例如病人身上佩戴的监测设备。部分设备所需流量较大，需要实时上传病人的影像及视频等，例如医生手持的PDA诊疗仪器。

安全风险分析：从个人属性来看，医院医疗设备属于公用设备，与人关联性较弱。从开通功能来看，无需语音，需要开通点对平台定向短信，需要开通流量向医院特定平台上报数据或视频信息，所需流量较大。

（2）个人医疗设备

个人医疗设备主要是病人佩戴的医疗可穿戴设备，具有移动性强、使用数据量大、产品形态丰富等特点。鉴于个人医疗设备的使用场景，所需开通的功能有所不同，如部分设备具备紧急呼救功能，需要语音通话功能，部分设备激活需要短信功能，监测类设备需要流量功能向特定平台实时上传病患数据等，流量使用量不大。

安全风险分析：从个人属性来看，通常是个人使用，与人关联性较强。从开通功能来看，需要开通定向语音、定向短信、定向流量，且流量使用量较大。

8. 智慧物流

（1）物流手持终端设备

物流手持终端可以分为仓库人员手持终端和物流人员手持终端。仓库人员手持终端主要用于在仓库中对货物进行条码扫描、货物出入库、货物盘点等，一般仅需短信用于设备的激活和故障上报，需要流量向特定平台上传货物信息。物流人员手持终端功能较为复杂，通常具备货物条码扫描、接收实时订单、刷卡支付等功能。

安全风险分析：对于仓库人员手持终端，可开通点对平台定向短信和定向流量功能，且流量使用量不大，安全风险较低。对于物流人员手持终端，从个人属性来看，通常为快递员随身携带使用，可关联到实际使用人。从开通功能来看，需要开通通用流量功能，且人员变更频繁，安全风险较高。

（2）货物跟踪设备

货物跟踪设备主要包括货物定位跟踪设备、冷链温湿度监测设备等，用于向特定平台传输货物的定位信息或环境监测信息，流量使用量一般较小。

安全风险分析：从开通功能来看，无需语音，需要开通点对平台定向短信，需要开通小流量向特定平台传输数据，安全风险较小。

（3）智能快递柜

智能快递柜是一种集物品识别、快递收费、安防监控等于一体的智慧物流末端解决方案，部分智能快递柜还具备一键联系厂家的功能（如智能快递柜出现故障时）、智能广告等功能。另外，智能快递柜一旦投入使用，一般不会发生位置变化。

安全风险分析：从个人属性来看，通常是集成在快递柜中，难以关联到实际使用人。从开通功能来看，需要开通定向语音、定向短信以及流量功能，用于数据传送或特定平台的广告推送，且使用量较大。一般情况下使用位置较为固定。

（4）仓储视频监控设备

仓储视频监控中使用物联网卡主要是用于向特定平台传输采集到的视频信息，所需流量通常较大。

安全风险分析：从个人属性来看，通常是部署在仓库中，与人关联性较弱。从开通功能来看，无需语音，需要点对平台定向短信和定向流量，且流量使用量较大，存在安全风险。