ICS 35.030
L70

团　　体　　标　　准

T/CCSA XXXX—XXXX

车联网网络安全防护定级实施指南

Internet of Vehicles Cyber security protection classification implementation guideline

（征求意见稿）

（本草案完成时间：8 月 4 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国通信标准化协会　　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。

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。

本文件由中国通信标准化协会提出。

本文件由中国通信标准化协会归口。

本文件起草单位： 中国信息通信研究院、中国一汽集团有限公司、重庆长安汽车股份有限公司、上海蔚来汽车有限公司、北京交通大学、北京航空航天大学、北京天融信网络安全技术有限公司、杭州安恒信息技术股份有限公司、北京云驰未来科技有限公司

本文件主要起草人：

车联网网络安全防护定级实施指南

1 范围

本文件规定了车联网网络安全防护定级备案实施要求，包括定级备案实施总体流程、定级备案要求、定级原则、等级确定、定级实施方法及等级变更等内容。

本文件适用于基础电信运营企业、有关车联网运营企业及智能网联汽车生产企业等车联网相关运营单位。

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 22240-2020 信息安全技术 网络安全等级保护定级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

车联网 Internet of Vehicles

以车内网、车际网和车载移动互联网为基础，按照约定的通信协议和数据交互标准，在车-X（X：车、路、行人及互联网等）之间，进行有线、无线通信和信息交换的大系统网络，是能够实现智能化交通管理、智能动态信息服务和车辆智能化控制的一体化信息物理系统。

3.2

网络安全 Cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[GB/T 22240-2020，定义3.1]

3.3

车联网网络设施 Internet of Vehicles network infrastructure

为车联网系统提供信息流通、网络运行等基础支撑作用的网络设备设施，主要包括车内网、车际网和车载移动互联网等专用通信网及相关设备等。

3.4

备案对象 Target of Record-keeping

落实车联网安全等级防护工作的企业。

3.5

定级对象 Target of Classification

车联网安全等级防护工作直接作用的对象，包括不限于车联网服务系统及平台等。

3.6

备案管理系统 Record-keeping Management System

车联网定级备案管理系统，由企业备案信息填报、定级对象等级确认、安全防护落实、检查评估、整改、定级对象终止等子业务模块构成，用于车联网网络设施及系统定级备案流程管理。

4 定级备案管理流程

车联网网络设施及系统的定级备案管理流程，包括企业备案、对象定级、安全防护落实、检查评估、整改、定级对象终止等阶段。如图1：

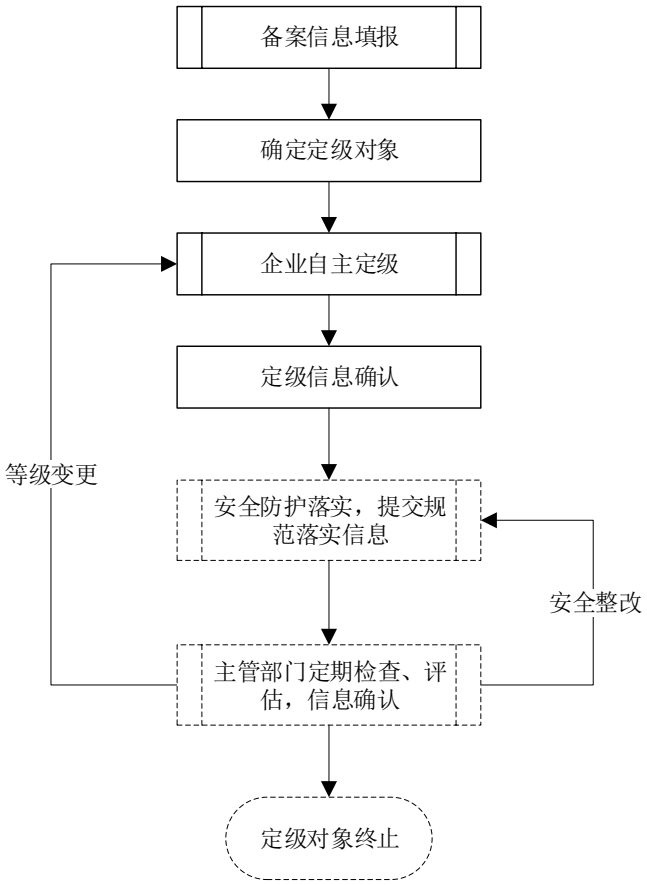

图1 车联网网络设施及系统的定级备案管理流程

本文件主要涉及企业备案、对象定级等阶段工作，其他阶段不在本文件规定的范围内。

定级对象停止维护表明定级对象终止。

5 备案要求

5.1 备案对象

备案对象以企业为主体，包含基础电信运营企业、车联网运营企业及智能网联汽车生产企业等车联网相关运营单位，对其持有或运营的车联网网络设施及系统分别备案。各个类别涉及到的企业类型如下：

a) 基础电信运营企业：提供互联网网络基础设施和服务的企业等；
b) 车联网运营企业：至少包括车联网信息服务提供商、车联网数字化运营企业及车路协同建设运营企业等。
c) 汽车生产制造企业：包括从事汽车整车制造企业以及装配或车用发动机、零部件和配套件生产的企业。

5.2 备案信息

企业向备案管理系统提交备案信息应包括但不限于：

a) 企业基本信息：包含企业法人信息、营业执照、车联网安全责任人信息、联系人信息、企业类别、企业性质、企业规模等；
b) 车联网网络设施及系统基本信息：包含名称、相关生产厂家、软硬件版本型号、产品规格、物理位置、接入 IP 地址、服务器建设情况、车辆及设备接入情况、网络安全服务采用情况等；
c) 安全管理信息：包括网络安全制度、规范、测试报告、安全建设及运营方案等；
d) 定级对象信息：用于系统或平台进行定级确认的信息，参见 6.2 定级信息。

5.3 备案流程

企业备案工作的一般流程如图2所示。

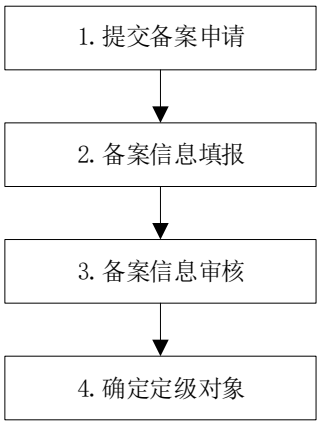

图2 企业备案工作的一般流程

备案工作的具体步骤如下：
a) 企业提交备案申请，通过注册的方式获取用户账号、密码，通过该账号向备案管理系统提交备案信息；
b) 备案信息填报应满足定级对象确定的最小集合，包含但不限于 5.2 备案信息所列举的内容；
c) 各省级电信主管部门会同工业和信息化主管部门对备案信息进行审核，应确保备案填报信息的完整度，审核结果通过备案管理系统进行反馈，主管部门的账号由备案管理系统统一分配；
d) 审核通过后，通过企业自主填报、各省级电信主管部门会同工业和信息化主管部门核准方式来确定定级对象。

6 定级要求

6.1 定级对象

定级对象包括车联网运营单位所持有或运营的所有车联网相关的业务系统和服务平台，贯穿车联网产品和服务的全生命周期。企业提供的定级信息应覆盖定级对象相关联的必要资产，包括但不限于车端联网设备、路侧基础设施、通信单元、网络单元、接口设备、云端设备等，填报信息范围应满足定级需要的最小集合。企业应对其备案的服务系统及平台进行自主定级，确定后的等级应通过行业主管部门认定的第三方机构的评估，并向备案管理系统提交相关证明材料。

按照车联网相关业务系统和服务平台所提供的服务类别，定级对象应包括但不限于：
a) 信息服务类：包括导航地图、定位服务、GIS 等；
b) 车辆服务类：包括车辆监控、远程控制、OTA 服务、信息安全等；
c) 金融服务类：包括移动支付、UBI 车险等；
d) 应用生态服务类：包括车机 APP、新闻、天气、娱乐、游戏等；
e) 出行服务类：包括共享出行、分时租赁等；
f) 后市场服务类：包括维修保养、紧急救援、违章查询等；

g） 企业服务类：包括车辆分析、用户画像、数字营销等；
h） 行业运营服务类：包括车队管理、两客一危、物流调动、公交出租等；
i） 自动驾驶服务类：包括编队行驶、远程驾驶、自主泊车等；
j） 智能交通应用类：包括智能信控、绿波车道、高精度地图、路侧边缘计算等。

6.2 定级信息

定级应提交以下信息及对应证明材料：
a） 对象系统规模：定级对象服务的用户和车辆的数量；
b） 业务重要程度：该对象所涉及的子系统的数量，子系统业务类型及业务描述，如是否包含OTA升级、远程控制等重要功能等；
c） 数据安全防护程度：该对象存储的数据类型、数据收集范围、数据收集频率、数据收集量、数据使用范围等；
d） 安全风险程度：对象面临的安全风险等级、受影响范围等；
以上内容，应同步提交证明材料至备案管理系统用于定级确认。

6.3 定级流程

定级工作的一般流程如图3所示。

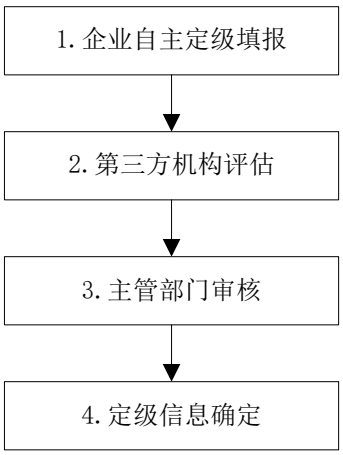

图3 定级工作的一般流程

定级工作的具体步骤如下：
a） 定级对象确定之后，企业进行自主定级，并提交行业主管部门认定的第三方机构进行评估；
b） 企业通过行业主管部门认定的第三方机构进行评估，并将评估结果提交至备案管理系统；
c） 各省级电信主管部门会同工业和信息化主管部门对企业自主定级及第三方机构评估结果进行审核；
d） 审核通过后，确定定级信息，如审核未通过，企业应配合提交相关信息，进行重新定级。

6.4 命名规则

定级对象应按照统一的命名规则命名。命名按照车联网定级对象的颗粒度，具体规则如下：
[车联网安全运营单位（备案企业）]（[集团公司/X分公司]）[车联网安全服务或平台名称（定级对象）]
例如：
中国XX集团 XX集团XX分公司 车联网OTA升级系统（包括车端设备、网络通信及云端服务平台）
中国XX集团 某省分公司 车联网某服务平台

7 定级原则

7.1 安全等级

根据车联网网络安全定级备案对象遭到破坏后可能对国家安全、经济运行、社会秩序、公众利益的危害程度，将企业的定级对象级别由高到低划分为三级、二级、一级。

三级：严重影响企业自身运行、造成重大人员伤亡，会对社会秩序、经济运行和公众利益造成严重损害，或对国家安全造成严重损害。

二级：影响企业自身运行、造成人员伤亡，或对社会秩序、经济运行和公众利益造成较大损害，或对国家安全造成轻微损害；

一级：影响企业自身运行，造成轻微人员伤害，或对社会秩序、经济运行和公众利益造成轻微损害，不损害国家安全。

7.2 等级评定

根据对象系统规模、业务重要性、数据安全防护程度、安全风险程度等因素，得出具体的分值K。

$$K= \mathrm{Round1}\{\mathrm{Log}_2[\sum_{i=1}^{4}\alpha_i \cdot 2^{K_i}]\}$$

其中， K代表安全等级值， K_i代表7.3节所述对象系统规模、业务重要程度、数据安全防护程度和安全风险程度的指标赋值， Round1{} 表示四舍五入处理，保留1位小数， Log2[]表示取以2为底的对数，α_i分别表示指标赋值所占的权重。

安全等级值和安全等级的关系：

安全等级值K	安全等级
$1 \leq K < 1.5$	一级
$1.5 \leq K < 2.5$	二级
$2.5 \leq K < 3$	三级

7.3 定级要素

7.3.1 概述

定级对象定级要素包括：

a) 对象系统规模；（i=1；α_1 = 1/5）

b) 业务重要程度；（i=2；α_2 = 1/5）

c) 数据安全防护程度；（i=3；α_3 = 1/5）

d) 安全风险程度；（i=4；α_4 = 2/5）

7.3.2 对象系统规模

定级要素及分值 K_1	要素说明	
对象系统规模	根据对象系统接入的注册车辆和用户数量，系统持有数据量的级别将对象的规模分为大、中、小。 用户数 u（单位万），车辆数 v（单位万），数据量 d（Tbit） K_1=u/20+v/70+d/100	
评分规则	规模大：用户数大于等于 20 万且车辆数大于等于 70 万且数据量大于等于 100Tbit	3
	规模中：用户数小于 20 万或车辆数小于 70 万或数据量小于 100Tbit	2

	规模小：除以上规模的其他情况	1

7.3.3 业务重要程度

定级要素及分值 K_2	要素说明	
业务重要程度	根据对象服务覆盖子系统数量，以及对象业务高、中、低不同重要程度，将各个子系统的安全等级进行分别取值，确定对象业务系统的重要程度取值。	
评分规则	程度高：安全等级 g 取值为 3 程度中：安全等级 g 取值为 2 程度低：安全等级 g 取值为 1 系统数量 s $K_2=\begin{cases}3, & if\ 2<\frac{1}{s}\sum s_i g_i \le 3\\ 2, & if\ 1<\frac{1}{s}\sum s_i g_i \le 2\\ 1, & if\ \frac{1}{s}\sum s_i g_i \le 1\end{cases}$ 业务重要程度的取值，按照子业务系统安全等级就高不就低原则。	取值为 1，2，3

7.3.4 数据安全防护程度

定级要素及分值 K_3	要素说明	
数据安全防护程度	根据对象数据安全防护及合规情况，将对象数据安全分为高、中、低三个防护水平，需要考虑到数据的保密性、完整性和可用性防护措施	
评分规则	高：造成大量关键数据和重要敏感信息丢失或被窃取、篡改、假冒，侵害到多个利益相关方的隐私，造成严重的后果。	3
	中：造成较多关键数据和重要敏感信息丢失或被窃取、篡改、假冒，侵害到特定利益相关方的隐私，造成较大的后果；	2
	低：造成少量关键数据和重要敏感信息丢失或被窃取、篡改、假冒，违反法规，对特定利益相关方造成一定的、轻微的后果。	1

7.3.5 安全风险程度

定级要素及分值 K_4	要素说明	
安全风险程度	判定定级备案对象一旦发生安全事件，将产生的人身安全、经济或社会影响，如人员伤亡、组织信誉破坏、组织的正常经营，经济损失、社会影响等程度，分为重大影响、较大影响、一般影响	
评分规则	重大影响：一旦发生将产生非常严重的人身安全、经济或社会影响，如人员严重伤亡、组织信誉严重破坏、严重影响组织的正常经营，人员伤亡严重、经济损失重大、社会影响恶劣。	3
	较大影响：一旦发生将产生较大的人身安全、经济或社会影响，在一定范围内给相关人员、组织的经营和信誉、社会造成损害；	2
	一般影响：一旦发生会造成一定的人身安全、经济、社会或生产经营影响，但影响面和影响程度不大。	1

8 等级确定

根据车联网网络安全定级对象系统规模、业务重要程度、数据安全防护程度和安全风险程度四个定级要素的分值的总和，确定车联网定级对象的等级值。

车联网定级对象等级与安全防护要求的关系如下：

a) 车联网定级对象的等级为三级，则其相关联的车联网网络设施及系统资产应落实相应的网络安全措施，以达到全部增强级防护要求；
b) 车联网定级对象的等级为二级，则其相关联的车联网网络设施及系统资产应落实相应的网络安全措施，以达到基础级防护要求及增强级要求特定项；
c) 车联网定级对象的等级为一级，则其相关联的车联网网络设施及系统资产应落实相应的网络安全措施，以达到基础级防护要求；

9 实施要求

车联网相关运营单位应在车联网网络设施及系统已投入运营（含试运营）后九十日内，通过备案管理系统提交办理备案申请。

车联网运营单位报备的信息应真实、完整、合理。

10 等级变更

车联网相关运营单位已备案的车联网网络设施及系统由于其用途、类型、资产以及社会影响力、规模和服务范围、所提供服务的重要性等涉及车联网网络设施及系统的定级要素发生变化或者由于改建、扩建、拆分、合并等原因导致备案信息更新或安全等级调整时，应在三十日内通过备案管理系统提出备案信息更新申请。