陕西省交通运输厅
陕西省通信管理局
陕西省公安厅
中国人民银行西安分行
陕西省国家税务局
陕西省地方税务局
陕西省互联网信息办公室

文件

陕交发〔2018〕22号

关于进一步规范网络预约出租汽车经营者申请线上服务能力认定工作流程的通知

各设区市、杨凌示范区、韩城市交通运输局、公安局、人民银行、国税局、地税局、网信办：

根据《交通运输部办公厅 工业和信息化部办公厅 公安部办公厅 中国人民银行办公厅 税务总局办公厅 国家网信办秘书局

关于网络预约出租汽车经营者申请线上服务能力认定工作流程的通知》（交办运〔2016〕143号，以下简称《通知》）、《交通运输部办公厅关于印发〈网络预约出租汽车监管信息交互平台总体技术要求（暂行）〉的通知》（交办运〔2016〕180号，以下简称《总体技术要求》）要求，为进一步规范网络预约出租汽车经营者申请线上服务能力认定工作流程，现将有关事宜通知如下。

一、规范认定流程

（一）根据《网络预约出租汽车经营服务管理暂行办法》（交通运输部 工业和信息化部 公安部 商务部 工商总局 质检总局 国家网信办令2016年第60号）和《通知》的规定，在本省注册具有独立法人资格并从事网约车经营者，向所在地交通运输局提交线上服务能力认定相关材料（有关要求详见附件1）。

（二）网约车经营者所在地交通运输局初步查验《网络预约出租汽车经营申请表》和申请材料（共13项）后，将资料齐全、内容完整的材料及时转送省交通运输厅。省交通运输厅在收到申请表和申请材料2个工作日内分送联合发文各成员单位（以下简称各单位）进行审核。

（三）各单位要按照上级部门有关规定认真做好审核工作，并在10个工作日内向省交通运输厅反馈正式书面审核意见。因申请人材料不符合要求而重新补充材料造成的时间延误不计算在相应各单位审核材料的时间要求内。

（四）省交通运输厅在收到反馈意见后的3个工作日内审核

出具具备线上服务能力认定结果；同时，将审核结果上报交通运输部。对未通过审核的，出具不具备线上服务能力意见告知书。对于未通过认定的，企业整改合格后可再次申报。

（五）网约车经营者应当在取得相应《网络预约出租汽车经营许可证》并向企业注册地省级通信主管部门申请增值电信业务经营许可（有网站的需办理互联网信息服务备案）后，方可开展相关业务。网约车经营者应当自网络正式联通之日起30日内，到所在地省级人民政府公安机关指定的受理机关办理备案手续。

二、加强事后监管

各地交通运输局、公安局、人民银行、国税局、地税局和网信办要加强对网约车线上服务的监管，对在经营过程中网约车经营者达不到线上服务能力条件或者发生重大变化的，应及时上报各相应主管部门并抄送省交通运输厅。网约车经营者需按照《总体技术要求》的规定，将数据接入交通运输部监管平台。各市交通运输局通过监管平台对网约车平台、网约车车辆、网约车驾驶员及运营服务行为进行监督管理。

三、其他

网约车监管是一项全新的工作，随着出租汽车行业改革工作的深化，网约车经营者线上服务能力认定工作的相关政策和条件可能会有变化或调整，从而导致办理流程和检测机构发生细小变化。若有变化时，请各成员单位根据工作职责及时向社会公布，

不再另外联合行文通知。

附件：1. 陕西省网络预约出租汽车经营者线上服务能力认定相关材料及具体要求

2. 通信主管部门网络预约出租汽车经营者线上服务能力认定申请材料模板

3. 信息系统安全等级保护备案表

4. 信息系统安全等级保护定级报告模版

陕西省交通运输厅　　陕西省通信管理局

陕西省公安厅　　中国人民银行西安分行

陕西省国家税务局　　陕西省地方税务局

陕西省互联网信息办公室

2018年3月2日

附件1

陕西省网络预约出租汽车经营者申请线上服务能力认定相关材料及具体要求

一、技术研发和维护部门架构及人员证明材料，包括身份证明、技术能力证明及工作合同等材料；拟从事网约车业务的服务器及网络设备的采购或者租赁协议，服务器托管协议或互联网接入协议；平台软硬件及最大处理能力、数据库最大存储能力等情况说明。（审核部门：通信）

按照《通信主管部门网络预约出租汽车经营者线上服务能力认定申请材料模板》要求填写。

二、面向乘客和驾驶员移动互联网应用程序（APP）的信息内容和服务功能。（审核部门：交通运输、通信）

（一）交通运输部门要求：

APP使用说明书、功能情况等材料，通过下载进行核查比对。

（二）通信部门要求：

已包含在《通信主管部门网络预约出租汽车经营者线上服务能力认定申请材料模板》材料4中。

三、配合依法查询、调取相关数据信息的功能设计、工作制

度和责任机构、责任人以及联系方式等。（审核部门：交通运输、通信、公安、税务）

（一）交通运输部门要求：

符合交通运输部实现监管平台数据对接的要求，工作制度健全、责任机构、责任人落实明确。

（二）通信部门要求：

已包含在《通信主管部门网络预约出租汽车经营者线上服务能力认定申请材料模板》材料4中。

（三）公安部门要求：

提交的材料需包括的主要内容：1. 网络服务平台后台数据调取、查询功能可查询的字段项、可查询期限、支持的查询方式及相应反馈结果等。2. 案事件协查工作制度，包括协查流程、台帐登记、责任机构、责任人及联系方式等。

重点审核的内容：1. 数据查询方案内容是否完善、查询说明文档是否清晰；2. 协查工作制度建立是否符合规范，责任机构、责任人及联系方式是否明确。

审核方式：材料审核。

审核通过的标准：提交的材料是否准确、完备。

（四）税务部门要求：

税务部门依法就经营者线上服务能力进行审核，包括但不限于以下内容：1. 配合税务部门就其自身经营、税费申报缴纳等相关数据调查取证的能力。2. 协助税务部门就其关联企业经营、

税费申报缴纳等相关数据调查取证的能力。3. 发票开具方式及相关技术方案。

提交材料需包含的内容：

1. 网络服务平台后台数据调取、查询功能可查询的字段项、可查询属期、支持的查询方式及查询结果反馈形式。2. 线上服务软件在线支付方式、付款渠道，与银行的结算方式。3. 开具电子发票的，提供技术方案、数据接口规范以及开票流程说明；开具其他发票的，提供相应的开票流程说明。4. 与第三方企业数据交互内容、方式以及查询方式。5. 以上内容相关的工作制度、责任机构、责任人以及联系方式。

重点审核的内容：

1. 能否完整、准确反映全部、指定期间或每一笔交易的数据。2. 能否顺畅、准确开具发票。3. 工作制度是否完整、合理，责任机构、责任人及联系方式是否准确、可用。

审核方式：材料审核、现场查看

审核通过的标准：提交的材料是否准确、完备，现场查看情况与提交的材料是否一致。

四、提供由国务院交通运输主管部门出具的数据库具备接入交通运输部网约车监管信息交互平台条件的情况说明。只为本地提供服务的平台公司，可提供由服务所在地出租汽车行政主管部门出具的具备数据库接入当地监管平台条件的情况说明。（审核部门：交通运输）

按照《交通运输部办公厅关于印发〈网络预约出租汽车监管信息交互平台总体技术要求（暂行）〉的通知》（交办运〔2016〕180号）文件要求实现监管平台的数据对接，并由所在地交通运输主管部门/交通运输部出具接入证明。

五、网络应用、数据等所有服务器机房地址、接入地址、IP地址、用途分工等情况说明。（审核部门：通信、公安）

（一）通信部门要求：

已包含在《通信主管部门网络预约出租汽车线上服务能力认定申请材料模板》材料4中。

（二）公安部门要求：

提交的材料需包括的主要内容：1. 详细说明服务器机房地址仅限境内（精确到门牌号），所属运营商（包含联系方式）、所有对应IP地址等信息。2. 列明网络拓扑结构图，说明服务网络架构及相关用途。3. 对CDN（内容分发）、云服务等方式部署的，要详细说明所购买服务单位及部署方式。

重点审核的内容：基础设施、硬件设备及网络资源等自建、租用证明的原始材料（机房、线路、机架、服务器租用协议、合同等）。

审核方式：材料审核。

审核通过的标准：提交的材料是否准确、完备、必要时可第三方核实。

六、网络与信息系统安全等级保护定级报告、专家评审意

见、备案证明及测评报告。(审核部门：公安)

提交的材料需包括的主要内容：

1.《信息系统安全等级保护定级报告》(信息系统安全保护等级共分为五个等级，网约车经营者依据《信息安全等级保护管理办法》和《网络安全等级保护定级指南》(GA/T1389—2017)确定安全保护等级并报网安主管部门审查)；

2. 专家评审意见(网约车经营者组织外部专家依照《信息安全等级保护管理办法》和《网络安全等级保护定级指南》进行评审并出具意见)；

3.《信息系统安全等级保护备案表》、《信息系统安全等级保护备案证明》(网约车经营者根据已经确定的信息系统安全等级，在规定日期内向其所有地设区的市级以上公安机关提交《信息系统安全等级保护备案表》备案，公安机关网络安全保卫部门审查通过后，办理《信息系统安全等级保护备案证明》)；

4.《信息系统安全等级保护测评报告》(国家等级保护测评机构推荐目录推荐的专业测评机构开展测评并出具测评报告)。

重点审核的内容：备案证明、等保测评报告。

审核方式：材料、现场审核、技术测试、可视情采取现场检查方式。

审查通过的标准：材料明确、完备，按规定和标准落实国家网络安全等级保护制度，信息系统具备相应等级的安全保护能力。

七、网络安全防护水平、网络数据安全和个人信息保护措施满足通信行业网络安全管理相关要求的证明材料。（审核部门：通信）

按照《通信主管部门网络预约出租汽车经营者线上服务能力认定申请材料模板》要求填写。

八、具有完备的用户真实身份认证管理制度、措施，个人隐私数据保护措施和数据跨境流动情况说明。（审核部门：公安）

提交的材料需包括的主要内容：1. 用户真实身份认证管理制度、措施的文本。2. 个人隐私数据保护措施和数据跨境流动情况说明。

重点审核的内容：1. 用户注册需提交的具体信息内容及所采取的认证方式和流程。2. 个人隐私数据保护措施包括：数据存储是否加密存储，是否具有相关的数据安全保护措施。数据留存服务器及数据传输链路、路由方式等内容。

审核方式：材料、现场审核。

审查通过的标准：

1. 用户真实身份认定管理制度、措施：用户在注册时需同时提供以下真实信息：（1）认证手机号；（2）上传本人身份证清晰照；（3）上传手持本人身份证的照片，并保持身份证正面与头像清晰（采用线下面审方式的应提供说明材料）；（4）绑定支付帐号（如：银行借记卡、微信、支付宝等）；（5）上传本人的驾驶证；（6）上传车辆行驶证、车牌号照片以及对应的车辆照片。

上述信息必须提供完整（其中，普通用户只需提供第1项，网约车司机需提供所有信息；企业采用B2C模式统一提供车辆并聘用司机、人车无固定对应关系的，由网约车经营者统一提供车辆信息，并建立出车登记制度）。

2. 个人隐私数据保护措施和数据跨境流动情况说明：落实个人隐私数据保护措施，并达到相应等级保护要求；平台出现数据跨境流动的情况时，需对数据跨境流动的原因进行说明，并提供跨境数据流动内容和流向描述，跨境流动数据内容和流向目的地IP地址和端口、时间等相关的日志信息平台应长期保存。

九、网络服务平台后台的用户信息、日志记录、留存技术措施，有害信息屏蔽、过滤等安全防范技术措施的说明材料。（审核部门：通信、公安）

（一）通信部门要求：按照《通信主管部门网络预约出租汽车线上服务能力认定申请材料模板》要求填写。

（二）公安部门要求：

提交的材料需包括的主要内容：1. 有论坛或跟帖的应取消该功能。2. 数据留存内容及说明文件。3. 有害信息屏蔽、过滤等安全防范技术措施的文本。

重点审核的内容：1. 用户注册信息、登陆日志信息、上网行为轨迹信息的留存数据项及留存时限。2. 有害信息发现、屏蔽、过滤的处置流程和处置响应时间。

审核方式：材料、现场审核。

审查通过的标准：

1. 用户信息、日志记录、留存技术措施方面：平台应留存（1）用户注册信息应包含用户名、用户 ID、手机号等数据项；（2）司机注册信息应包括用户名、用户 ID、手机号、身份证号、车牌号、车架号、车身颜色、车辆品牌、车辆型号、绑定支付帐号（银行卡、第三方支付平台帐号等）等数据项；（3）登录日志应包含用户 ID、用户名、登录时间等数据项；（4）订单信息应包括用户 ID、订单内容（语音、文字）、下单时间、接单时间、预约上车地址、预约上车经纬度、预约下车地址、预约下车经纬度等数据项；（5）行驶轨迹日志信息应包括订单 ID、时间、经纬度等数据项；（6）寄递类数据信息应包括快递单号、收件者姓名、收件者联系电话、收件地址等数据项。其中，用户（司机）注册信息企业需永久留存、其他相关信息留存六个月以上。

2. 有害信息屏蔽、过滤等安全防范技术措施方面：建立信息安全审核团队，配备足够的信息安全审核人员；建立 人工和技术相结合的审核、巡查机制，实现 7X24 小时的监控巡查；落实违法有害信息屏蔽过滤技术措施，达到违法信息屏蔽过滤 10 分钟内生效，屏蔽过滤有效率达 100%；建立快速处置制度措施，违法有害信息 5 分钟内处置。

十、为依法防范、调查恐怖活动提供技术接口的说明材料。（审核部门：公安）

提交的材料需包括的主要内容：

已配合网安部门开展技术接口建设的网约车平台，由网约车平台运营管理主体所在地网安部门出具相应的证明材料；未开展技术接口建设的网约车平台，出具与网约车平台运营管理主体所在地网安部门配合开展技术接口建设的承诺书和保密协议。

重点审核的内容：警用技术接口建设方案符合技术接口相关规定。

审核方式：材料、现场审核。

审核通过的标准：已建技术接口，相关功能符合公安部门下发技术接口建设要求；未开展技术接口建设的，建设方案符合公安部门下发技术接口建设相关要求。

十一、网络与信息安全保障制度文本、互联网新技术新业务安全评估制度文本、应急处置预案文本，企业保证服务质量、信息和数据安全的承诺书。（审核部门：通信、公安）

（一）通信部门要求：按照《通信主管部门网络预约出租汽车线上服务能力认定申请材料模板》要求填写。

（二）公安部门要求：

提交的材料需包括的主要内容：1. 网络与信息安全保障制度，包括用户管理、日志留存、信息安全管理、网络安全管理等制度内容。2. 互联网新技术新业务安全评估制度包括，新技术新业务上线报备、安全评审等内容。3. 应急处置预案包括，应急处置工作流程、应急处置团队等，企业保证服务质量、信息和数据安全的承诺书等。

重点审核的内容：1. 用户信息留存的具体内容和时间、信息发布审核的流程、违法有害信息发现、处置及上报流程。2. 新服务、新功能安全评估流程、应急响应处置流程，承诺书中的网络安全组织、网络信息安全保护管理制度及安全保护技术措施、网络信息安全事件上报机制等工作是否详实。

审核方式：材料审核。

审核通过的标准：提交的材料是否准确、完备，必要时可现场进行检查。

十二、网上内容处置能力证明材料，网约车平台是否具备信息发布、评论跟帖、动员能力的群组等功能的情况说明。企业保证不应用网约车平台发布有害信息，不为企业、个人及其他团体组织发布有害信息提供便利的承诺书。（审核部门：公安、网信）

提交的材料需包括的主要内容：1. 网上内容处置能力证明材料。2. 网约车企业出具的有关网约车平台信息发布、评论跟帖、有动员能力的群组等功能的情况说明。3. 拒绝发布有害信息的承诺书。

重点审查的内容：网约车平台的功能介绍、重点是否具有用户互动功能的情况介绍以及已采取的网络信息安全保障功能的情况说明。

审核方式：材料审核。

审核通过的标准：提交的材料是否准确、完备。

十三、企业与银行或非银行支付机构合作业务模式的详细描

述，包括企业与银行或非银行支付机构签订的协议文本、企业是否设立资金池、是否为用户开立支付账户等情况的说明。（审核部门：人行）

需提交的材料：

1. 与商业银行或支付机构签订的支付服务协议原件或复印件，为复印件的应注明“与原件相符”并加盖单位行政公章。

2. 业务模式详细说明，包括：

（1）网约车业务模式说明：明确本次线上服务能力认定范围；

（2）账户开立情况说明。至少包括户名、账号、开户银行名称或开户支付机构名称、账户种类、账户功能、适用范围、出入金方式等信息。

（3）支付业务流程说明：申请人与支付机构或商业银行之间、与乘客之间、驾驶人员之间、其他相关参与方之间资金流转过程和业务合作模式。

附件 2

通信主管部门网络预约出租汽车经营者线上服务能力认定申请材料模板

整体要求：填写完整，不留空白栏；字迹工整，清晰可辨，提交申请时留下申请负责人的联系方式

法人代表签字：_____

申报单位：全称，与营业执照保持一致（盖章）

申报日期：_____年_____月_____日

材料 1：公司基本信息

公司名称			
企业法人营业执照 注 册 号		注册地址	
法定代表人姓名		身份证号	
法人代表联系方式			
通信地址			
技术负责人姓名		技术负责人手机	
技术负责人固话（区号-电话号码）		技术负责人电子邮箱	
联系人姓名		联系人手机	
联系人固话（区号-电话号码）		联系人电子邮箱	
公司业务介绍			

填表说明

1. 法人代表、技术负责人、联系人的联系方式应真实有效。

附件：公司企业法人营业执照副本、法定代表人身份证原件正反面复印件；

材料 2：技术部门及人员信息

技术部门名称及职责 （可填多个）	

公司技术及安全负责人名单

（至少应包括专人专岗的技术负责人、网络及信息安全负责人）

序号	姓名	身份证号码	职务	学历	联系电话	职称/资质证明

公司主要技术人员名单

序号	姓名	身份证号码	职务	专业	学历	联系电话	职称/资质证明

填表说明

1. 技术部门应包括技术研发部门和维护部门。 2. 技术及安全负责人应不少于2人，至少应包括专人专岗的技术负责人、网络及信息安全负责人。 3. 人员姓名、身份证号应与有效期内的身份证信息完全一致，且其职务和联系电话真实有效。 4. 职称/资质证明包括行业认证、职业技能鉴定等技术能力证明材料。

附件：技术负责人、网络与信息安全负责人、主要技术人员身份证正反面复印件或社保部门出具的境外人士工作证明，技术能力证明材料复印件(职称、资质证明等)，正式劳动合同复印件，公司近期为员工所上的社保证明（至少三个月，应加盖社保机构红章）.

材料 3：服务器、网络设备清单

设备类型	设备型号	数量	制造商	主要性能指标	采购或租赁协议

附件：服务器、网络设备等设施的采购或租赁协议复印件.

材料 4：线上服务功能说明（可另附页）

平台线上服务简介	业务内容描述、服务范围、目标用户、收费模式等
平台服务功能介绍	面向乘客和驾驶员功能介绍
平台信息内容	1. 信息种类、内容。 2. 数据的采集、存储、传输、使用、加密方式说明。 3. 信息保护制度设计说明。
监管数据接口功能说明	配合监管部门依法查询、调取数据信息的接口功能说明
接入服务商及接入地	
服务器放置地	
IP地址及功能（连续IP地址用“-”链接；多个IP地址用“;”隔开）	

填表说明

1. 服务器放置、接入地址精确到机房。 2. 公网 IP 地址段要写全，对应系统功能要说明。 3. 平台含互联网平台和移动应用程序（APP）。

附件：服务器托管协议或互联网接入协议复印件。
附件：托管方或接入商经营资质证明材料复印件。
附件：配合依法查询、调取相关数据信息的功能设计、工作制度和责任机构、责任人以及联系方式等材料说明。

材料 5：平台软硬件及数据库说明（可另附页）

平台软硬件说明	1. 服务平台的软件构成，含软件类型、数量、研发单位或生产商等。 2. 平台架构及网络拓扑（含文字说明），对外服务链路带宽。 3. 平台响应速度、最大并发数等性能指标。
数据库情况说明	数据库结构（含数据结构、I/O等）以及数据库容量、存储参数等性能指标。

填表说明

1. 平台含互联网平台和移动应用程序（APP）。

材料 6：网约车网络安全定级备案信息表

6.1-企业基本信息表

<table>
<tr><td>企业名称</td><td colspan="4"></td></tr>
<tr><td rowspan="3">网络安全
负责人</td><td>姓　　名</td><td></td><td>职务/职称</td><td></td></tr>
<tr><td>办公电话</td><td></td><td rowspan="2">电子邮件</td><td rowspan="2"></td></tr>
<tr><td>移动电话</td><td></td></tr>
<tr><td rowspan="6">网络安全应急
联系人</td><td>姓　　名</td><td></td><td>职务/职称</td><td></td></tr>
<tr><td>办公电话</td><td></td><td rowspan="2">电子邮件</td><td rowspan="2"></td></tr>
<tr><td>移动电话</td><td></td></tr>
<tr><td>姓　　名</td><td></td><td>职务/职称</td><td></td></tr>
<tr><td>办公电话</td><td></td><td rowspan="2">电子邮件</td><td rowspan="2"></td></tr>
<tr><td>移动电话</td><td></td></tr>
<tr><td colspan="5">网络安全防护定级备案总体情况</td></tr>
<tr><td rowspan="4">网络与系统单元列表
（注：每个网络与系统单元需单独填写“2-网络与系统单元定级备案信息表”）</td><td>网络与系统单元 1</td><td colspan="3"></td></tr>
<tr><td>网络与系统单元 2</td><td colspan="3"></td></tr>
<tr><td>网络与系统单元 3</td><td colspan="3"></td></tr>
<tr><td>……</td><td colspan="3"></td></tr>
</table>

6.2-网络与系统单元定级备案信息表

<table>
<tr><td>系统名称</td><td colspan="6"></td></tr>
<tr><td>主要功能及服务</td><td colspan="6"></td></tr>
<tr><td>服务范围</td><td colspan="6">□全国 □省（自治区、直辖市）内 □跨省（自治区、直辖市） 跨____个，分别为: _____</td></tr>
<tr><td>自定安全等级</td><td colspan="6">□第2级 □第3级 □第4级</td></tr>
<tr><td>所在机房 1</td><td colspan="6"></td></tr>
<tr><td>接入地 1</td><td colspan="6"></td></tr>
<tr><td>所在机房 2</td><td colspan="6"></td></tr>
<tr><td>接入地 2</td><td colspan="6"></td></tr>
<tr><td>……</td><td colspan="6"></td></tr>
<tr><td rowspan="3">主要应用软件情况
（注: 主要包括为对外提供服务开发的应用软件，包括 APP 等; 不含 office 等通用应用软件）</td><td>序号</td><td>名称</td><td>研发方</td><td>当前版本</td><td>维护方式</td><td>已运行时间</td></tr>
<tr><td>1</td><td></td><td>□自行研发
□第三方研发_____</td><td></td><td>□远程
□本地</td><td></td></tr>
<tr><td>2</td><td>……</td><td></td><td></td><td></td><td></td></tr>
<tr><td>网络用户信息存储处理情况</td><td colspan="6">□未处理或存储信息 □处理或存储信息，（请提供存储或处理的网络用户信息的类型名称）</td></tr>
<tr><td>公网 IP 地址段</td><td colspan="6"></td></tr>
<tr><td>主要协议和端口</td><td colspan="6"></td></tr>
<tr><td>接入总带宽（MB）</td><td colspan="6"></td></tr>
<tr><td>所用域名</td><td colspan="6"></td></tr>
<tr><td>.cn 域名相关记录</td><td>NS 记录</td><td colspan="2"></td><td>A 记录</td><td colspan="2"></td></tr>
<tr><td>域名注册服务机构信息</td><td>机构名称</td><td colspan="2"></td><td>联系人及办公电话</td><td colspan="2"></td></tr>
<tr><td>填表人</td><td colspan="2"></td><td>填表日期</td><td colspan="3"></td></tr>
</table>

材料 7：企业网络安全管理制度建立情况相关材料

按照《网络安全法》、《通信网络安全防护管理办法》（工信部令 11 号）等法律法规要求，网络安全管理制度建立情况应包括企业设置网络安全专门管理机构、企业网络安全主管领导的情况、配备网络安全专门工作人员情况，以及企业建立的网络安全防护管理、安全事件应急、重大事件报告、网络安全应急预案等规章制度情况。其中，网络安全应急预案文本内容应包括：事件应急负责人及联系方式、针对不同等级的网络安全事件制定的应急预案程序与处置流程、说明应急预案启动的条件、发生安全事件后要采取的信息报送工作流程、后期恢复措施等。

材料 8：网约车互联网平台网络安全防护相关报告

网约车互联网平台应按照《通信网络安全防护管理办法》（工信部令 11 号）、《电信网和互联网安全等级保护实施指南》等通信行业网络安全防护相关法规和标准要求，开展网络安全防护工作，落实防护措施，及时消除安全隐患，保障网络与系统安全，主要包括网络与系统定级备案、网络安全符合性评测和风险评估。并向通信主管部门提交定级备案报告、符合性评测报告、风险评估及整改报告。

网约车互联网平台网络安全定级备案可在省级通信主管部门指导下采取自主定级方式，网络安全符合性评测报告、风险及整改评估报告可由具备网络安全评估等相应安全服务能力的第三方安全检测机构提供或者企业自行开展。报告的具体内容有：

8.1 网络安全定级报告内容

1. 根据《电信网和互联网安全等级保护实施指南（YD/T 1729-2008）》关于通信行业网络安全防护相关标准要求，对网约车互联网平台进行安全等级划分等活动的概述。总体原则是：按照定级对象受到破坏后对国家安全、社会秩序、经济运行、公共利益以及网络和企业合法权益的损害程度，进行安全等级划分。

2. 对网络与系统（定级对象）信息的详细描述，包括：

（1）企业特征、业务范围、安全管理基本情况以及其他基本情况；

（2）安全技术情况，包括网络与系统所在的物理环境、网络拓扑结构、网络关键设备（包括服务器、安全设备、应用系统等）情况、服务范围、网络处理和传送的信息资产、服务范围和用户类型等信息，网络边界。

3. 说明网络安全等级定级理由、要素以及安全等级确定结果等。

8.2 网络安全符合性评测报告

1. 评估任务及标准概述，其中评估标准包括：

（1）《电信网和互联网安全防护管理指南（YD/T1728-2008）》

（2）《电信网和互联网信息服务业务系统安全防护要求（YD/T2243-2016）》

（3）《电信网和互联网信息服务业务系统安全防护检测要求（YD/T2244-2011）》

（4）《电信网和互联网管理安全等级保护要求

（YD/T1756-2008）》

（5）《电信网和互联网管理安全等级保护检测要求（YD/T1757-2008）》

（6）《电信网和互联网安全防护基线配置要求网络设备（YD/T2698-2014）》

（7）《电信网和互联网安全防护基线配置要求安全设备（YD/T2699-2014）》

（8）《电信网和互联网安全防护基线配置要求数据库（YD/T2700-2014）》

（9）《电信网和互联网安全防护基线配置要求操作系统（YD/T2701-2014）》

（10）《电信网和互联网安全防护基线配置要求中间件（YD/T2702-2014）》等电信网和互联网安全防护系列标准。

（11）《电信网和互联网安全防护基线配置要求 WEB 应用系统（YD/T 2703-2014）》

（12）《第三方安全服务能力评定准则（YD/T2669-2013）》

2.符合性评测活动采取的技术措施，如采用访谈、检查、仪表测试、人工测试等方式，对受测网络单元的安全状况以及相关设备、系统潜在的安全隐患进行技术检测。

3.技术检测应包括系统安全加固、网络拓扑、冗余与灾难备份、网络及设备安全策略、设备漏洞、口令安全、介质管理、日志与安全审计等方面。技术检测对象应包括:

（1）生产主机：检查生产运行主机的操作系统、数据库、中间件以及第三方软件，包括账号安全、口令安全、授权安全、Web 安全、补丁安全、客户信息安全、开放端口安全、安全配置、日志与审计等；

（2）网络设备：检查交换机、防火墙等网络设备，包括账号安全、口令安全、授权安全、Web 安全、补丁安全、IP 协议安全等；

（3）安全防护设备：检查 IPS、IDS、web 应用防火墙、防 dos 设备等安全防护设备，包括账号安全、口令安全、授权安全、补丁安全、开放端口安全、Web 安全、防护策略配置、告警配置、攻击防护、IP 协议、日志与审计等；

（4）其他：检查与约车主要平台相连的辅助系统的安全性，包括账号安全、口令安全、授权安全、补丁安全、客户信息安全、Web 安全、开放端口安全、安全配置、日志与审计等。

4.符合性评测结果，包括符合性评测得分、达标率、不达标项说明，系统的整体安全性是否达到标准要求。

8.3 风险评估及整改报告

1.风险评估过程的描述，包括：采用的技术评估手段，如工具扫描、远程仪表测试、人工测试等方式；技术评估内容，如漏洞扫描、网络安全性检测、主机安全性检测、应用安全性检测、管理安全性检测和渗透性测试等。

2.风险评估分析结果说明，例如被检测网络与系统的安全隐患类型、漏洞数量和级别、可导致的后果，并附截图证据。

3. 总结被检网络与系统存在的主要问题，以及针对检测发现的具体问题进行整改的情况。

材料 9：网约车移动应用程序（APP）安全保障能力报告

报告需由具备网络安全评估等相应安全服务能力的第三方安全检测机构出具。根据《电信和互联网用户个人信息保护规定》（工信部令 24 号）及移动应用程序（APP）网络安全相关标准要求，重点证明网约车移动应用程序（APP）中不含恶意代码、在收集用户信息或调用系统权限时已告知并取得用户同意等。对于网约车移动应用程序（APP）后台系统，与网约车互联网平台的要求相同，应提供相应的网络与系统定级备案、网络安全符合性评测、风险评估及整改报告。

网约车相关移动应用程序（APP）安全保障能力报告内容应包括：

1. 被测网约车相关移动应用程序（APP）列表，并提供应用软件运营者、主要功能、后台服务器及所在机房等信息。

2. 安全检测的主要方法、测试人员组成、测试案例和测试结论等。经检测，应证明移动应用程序（APP）不含有《移动互联网恶意程序描述格式》等标准中所称恶意程序、符合“未经明示且经用户同意，不得实施收集使用用户个人信息等侵害用户合法权益或危害网络安全的行为。”等的规定。

3. 报告应证明企业是否采取措施留存其所提供的应用软件、有关版本、上线时间、功能简介、用途、MD5 等校验值、服务器接入等

信息以备追溯检测，相关信息的留存时间应不短于60日。

材料10：网络数据安全和用户信息保护自证报告

根据《网络安全法》、《电信和互联网用户个人信息保护规定》（工信部令24号）、《电信和互联网用户个人电子信息保护通用技术要求和管理要求（YD/T 2692-2014）》等相关法律法规和标准要求，企业应采取适当措施，确保网络数据和用户个人信息安全。报告内容应至少包括以下内容：

1.数据分级分类管理措施情况。重点包括数据分级分类管理制度建设和落实情况，重要数据和用户个人信息的分级分类方法。

2.数据收集环节安全情况。重点包括收集用户个人信息是否符合相关法律法规和相关标准规定；采集用户数据前履行告知义务的情况，采集前获得用户同意的情况；

3.数据传输存储环节安全情况。重点包括重要网络数据和敏感用户个人信息加密传输、存储情况；数据访问控制权限管理和审计情况；数据容灾备份情况。证明在我国境内运营中产生的用户个人信息和重要数据存储在境内，同时具备数据防篡改、防泄露、防窃取等能力。

4.数据使用共享环节安全管理情况。重点包括使用、共享用户个人信息是否符合相关法律法规和相关标准规定；数据处理外包服务安全管理情况；与企业内部涉及重要数据、用户个人信息处理的工作人员签订保密协议或责任书的情况等。

5. 数据跨境传输安全管理情况。企业跨境传输数据是否符合《网络安全法》规定。

材料11：承诺书

****通信管理局：**

我公司承诺：

1. 保证提交的全部资料真实有效，复印件与原件相符。如线上服务能力出现重大变更，将及时书面告知通信主管部门并更新相关材料。

2. 保证资金、技术人员、各项软硬件设施、公司制度能够满足线上服务能力需求。保证服务质量满足监管要求及客户需求。

3. 严格遵守《电信和互联网用户个人信息保护规定》（工业和信息化部第24号令）、《互联网信息服务管理办法》（国务院第292号令）及其他通信行业监管法律、法规和政策，合法从事经营活动。

4. 接受各级通信主管部门的行业管理和监督检查，及时按要求报送相关材料。

5. 根据电信业务市场监测需要，按照要求向通信主管部门报送相应的监测信息。

6. 保证网络安全与信息、数据安全。保证线上服务业务符合国家信息安全的要求；严格执行国家安全管理部门和通信主管部门的安全保密管理规定；严格履行国家要求的网络与信息安全责任。具体包括：

（1）按照通信行业管理部门要求，配备相应数量的专职网络与信息安全管理人员，成立相应的网络与信息安全管理机构，建立健全网络与信

息安全保障制度，制定应急处置预案，并定期将相关业务开展情况和网络与信息安全责任落实情况向业务开展地通信行业管理部门报备。

（2）按照相关法律法规及通信行业管理部门要求建立违法违规信息发现和过滤技术手段，能对违法违规信息进行隔离、过滤处置。严格落实违法违规信息发现处置机制，阻断违法违规信息发布，对于已发布的违法违规信息应当立即停止传输，保存有关记录，并向有关主管部门报告。

（3）严格落实重大信息安全事件应急处置和报告制度，对于涉及业务相关数据安全、涉及国家网络信息安全的重大事件进行紧急处置，并上报主管部门。

（4）定期开展信息安全相关法律法规及安全政策文件、配合政府监管机制、信息安全保障制度等方面培训，培养员工信息安全意识，提高员工信息安全工作能力。

（5）网约车平台日志记录、留存技术措施满足《网络安全法》、《互联网信息服务管理办法》等法律法规有关要求。

（6）按照《互联网新技术新业务安全评估指南》（YD/T3169-2016）等通信行业标准，建立互联网新技术新业务安全评估制度，在新技术、业务或应用上线（含合作推广、试点、商用等）时，在基础资源配置、技术实现方式、业务功能或用户规模等方面发生较大变化时，开展网络信息安全评估，积极防范网络信息安全风险，并在安全评估完成30日内向通信主管部门提交书面评估报告。

（7）按照《通信网络安全防护管理办法》（工信部令第11号）等有关要求，制定网络安全防护管理制度，落实网络安全“三同步”、定级备案、

符合性评测和风险评估等要求。

（8）按照国家用户信息保护有关法律法规和《电信和互联网用户个人信息保护规定》（工信部令第24号）等要求，开展网络数据和用户信息保护工作，防范重要数据和敏感用户信息泄露。

（9）制定并落实网络安全事件应急预案和网络安全事件应急处置报告制度，明确网络安全事件应急处置机制、网络安全事件上报和网络安全应急演练等要求。发生重大网络安全事件时，于第一时间向通信主管部门报告，并根据通信主管部门要求采取应急处置措施。

（10）当网络安全应急联系人发生变动时，在两个工作日内主动向通信主管部门报备。

本企业网络与信息安全应急联系人及联系方式：

_____

以上承诺如有违反，愿接受通信行业管理部门的依法处罚。

法定代表人签字：

公　章：

二〇　年　月　日

其他材料：通信主管部门要求提交的其他材料

附件 3

备案表编号：

信息系统安全等级保护备案表

备 案 单 位：_____（盖章）_____

备 案 日 期：_____

受理备案单位：_____（盖章）_____

受 理 日 期：_____

中华人民共和国公安部监制

填 表 说 明

一、 制表依据。根据《信息安全等级保护管理办法》（公通字[2007]43号）之规定，制作本表；

二、 填表范围。本表由第二级以上信息系统运营使用单位或主管部门（以下简称“备案单位”）填写；本表由四张表单构成，表一为单位信息，每个填表单位填写一张；表二为信息系统基本信息，表三为信息系统定级信息，表二、表三每个信息系统填写一张；表四为第三级以上信息系统需要同时提交的内容，由每个第三级以上信息系统填写一张，并在完成系统建设、整改、测评等工作，投入运行后三十日内向受理备案公安机关提交；表二、表三、表四可以复印使用；

三、 保存方式。本表一式二份，一份由备案单位保存，一份由受理备案公安机关存档；

四、 本表中有选择的地方请在选项左侧“□”划“√”，如选择“其他”，请在其后的横线中注明详细内容；

五、 封面中备案表编号（由受理备案的公安机关填写并校验）：分两部分共 11 位，第一部分 6 位，为受理备案公安机关代码前六位（可参照行标 GA380-2002）。第二部分 5 位，为受理备案的公安机关给出的备案单位的顺序编号；

六、 封面中备案单位：是指负责运营使用信息系统的法人单位全称；

七、 封面中受理备案单位：是指受理备案的公安机关公共信息网络安全监察部门名称。此项由受理备案的公安机关负责填写并盖章；

八、 表一 04 行政区划代码：是指备案单位所在的地(区、市、州、盟)行政区划代码；

九、 表一 05 单位负责人：是指主管本单位信息安全工作的领导；

十、 表一 06 责任部门：是指单位内负责信息系统安全工作的部门；

十一、表一 08 隶属关系：是指信息系统运营使用单位与上级行政机构的从属关系，须按照单位隶属关系代码（GB/T12404—1997）填写；

十二、表二 02 系统编号：是由运营使用单位给出的本单位备案信息系统的编号；

十三、表二 05 系统网络平台：是指系统所处的网络环境和网络构架情况；

十四、表二 07 关键产品使用情况：国产品是指系统中该类产品的研制、生产单位是由中国公民、法人投资或者国家投资或者控股，在中华人民共和国境内具有独立的法人资格，产品的核心技术、关键部件具有我国自主知识产权；

十五、表二 08 系统采用服务情况：国内服务商是指服务机构在中华人民共和国境内注册成立（港澳台地区除外），由中国公民、法人或国家投资的企事业单位；

十六、表三 01、02、03 项：填写上述三项内容，确定信息系统安全保护等级时可参考《信息系统安全等级保护定级指南》，信息系统安全保护等级由业务信息安全等级和系统服务安全等级较高者决定。01、02 项中每一个确定的级别所对应的损害客体及损害程度可多选；

十七、表三 06 主管部门：是指对备案单位信息系统负领导责任的行政或业务主管单位或部门。部级单位此项可不填；

十八、解释：本表由公安部公共信息网络安全监察局监制并负责解释，未经允许，任何单位和个人不得对本表进行改动。

表一　单位基本情况

01 单位名称				
02 单位地址	_____省(自治区、直辖市) _____地(区、市、州、盟) _____县(区、市、旗)			
03 邮政编码			04 行政区划代码	
05 单位负责人	姓　名		职务/职称	
	办公电话		电子邮件	
06 责任部门				
07 责任部门联系人	姓　名		职务/职称	
	办公电话		电子邮件	
	移动电话			
08 隶属关系	□1 中央　□2 省(自治区、直辖市)　□3 地(区、市、州、盟) □4 县（区、市、旗）　□9 其他_____			
09 单位类型	□1 党委机关　□2 政府机关　□3 事业单位　□4 企业　□9 其他_____			
10 行业类别	□11 电信　□12 广电　□13 经营性公众互联网 □21 铁路　□22 银行　□23 海关　□24 税务 □25 民航　□26 电力　□27 证券　□28 保险 □31 国防科技工业　□32 公安　□33 人事劳动和社会保障　□34 财政 □35 审计　□36 商业贸易　□37 国土资源　□38 能源 □39 交通　□40 统计　□41 工商行政管理　□42 邮政 □43 教育　□44 文化　□45 卫生　□46 农业 □47 水利　□48 外交　□49 发展改革　□50 科技 □51 宣传　□52 质量监督检验检疫 □99 其他_____			
11 信息系统总数	个	12 第二级信息系统数	个	13 第三级信息系统数　个
		14 第四级信息系统数	个	15 第五级信息系统数　个

表二（ / ）信息系统情况

<table>
<tr><td colspan="2">01 系统名称</td><td colspan="4"></td><td>02 系统编号</td><td></td></tr>
<tr><td rowspan="2">03 系统承载业务情况</td><td>业务类型</td><td colspan="6">□1 生产作业 □2 指挥调度 □3 管理控制 □4 内部办公
□5 公众服务 □9 其他_____</td></tr>
<tr><td>业务描述</td><td colspan="6"></td></tr>
<tr><td rowspan="2">04 系统服务情况</td><td>服务范围</td><td colspan="6">□10 全国 □11 跨省（区、市） 跨____个
□20 全省（区、市） □21 跨地（市、区） 跨____个
□30 地（市、区）内
□99 其它_____</td></tr>
<tr><td>服务对象</td><td colspan="6">□1 单位内部人员 □2 社会公众人员 □3 两者均包括 □9 其他_____</td></tr>
<tr><td rowspan="2">05 系统网络平台</td><td>覆盖范围</td><td colspan="6">□1 局域网 □2 城域网 □3 广域网 □9 其他_____</td></tr>
<tr><td>网络性质</td><td colspan="6">□1 业务专网 □2 互联网 □9 其它_____</td></tr>
<tr><td colspan="2">06 系统互联情况</td><td colspan="6">□1 与其他行业系统连接 □2 与本行业其他单位系统连接
□3 与本单位其他系统连接 □9 其它_____</td></tr>
<tr><td colspan="2" rowspan="7">07 关键产品使用情况</td><td>序号</td><td>产品类型</td><td>数量</td><td colspan="3">使用国产品率</td></tr>
<tr><td></td><td></td><td></td><td>全部使用</td><td>全部未使用</td><td>部分使用及使用率</td></tr>
<tr><td>1</td><td>安全专用产品</td><td></td><td>□</td><td>□</td><td>□ ____%</td></tr>
<tr><td>2</td><td>网络产品</td><td></td><td>□</td><td>□</td><td>□ ____%</td></tr>
<tr><td>3</td><td>操作系统</td><td></td><td>□</td><td>□</td><td>□ ____%</td></tr>
<tr><td>4</td><td>数据库</td><td></td><td>□</td><td>□</td><td>□ ____%</td></tr>
<tr><td>5</td><td>服务器</td><td></td><td>□</td><td>□</td><td>□ ____%</td></tr>
<tr><td>6</td><td>其他 ____</td><td></td><td>□</td><td>□</td><td>□ ____%</td></tr>
<tr><td colspan="2" rowspan="9">08 系统采用服务情况</td><td>序号</td><td colspan="2">服务类型</td><td colspan="3">服务责任方类型</td></tr>
<tr><td></td><td colspan="2"></td><td>本行业（单位）</td><td>国内其他服务商</td><td>国外服务商</td></tr>
<tr><td>1</td><td>等级测评</td><td>□有□无</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td>2</td><td>风险评估</td><td>□有□无</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td>3</td><td>灾难恢复</td><td>□有□无</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td>4</td><td>应急响应</td><td>□有□无</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td>5</td><td>系统集成</td><td>□有□无</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td>6</td><td>安全咨询</td><td>□有□无</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td>7</td><td>安全培训</td><td>□有□无</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td>8</td><td>其它_____</td><td></td><td>□</td><td>□</td><td>□</td></tr>
<tr><td colspan="2">09 等级测评单位名称</td><td colspan="6"></td></tr>
<tr><td colspan="2">10 何时投入运行使用</td><td colspan="6">年 月 日</td></tr>
<tr><td colspan="2">11 系统是否是分系统</td><td colspan="6">□是 □否（如选择是请填下两项）</td></tr>
<tr><td colspan="2">12 上级系统名称</td><td colspan="6"></td></tr>
<tr><td colspan="2">13 上级系统所属单位名称</td><td colspan="6"></td></tr>
</table>

表三（ / ）信息系统定级情况

	损害客体及损害程度	级别
01 确定业务信息安全保护等级	□仅对公民、法人和其他组织的合法权益造成损害	□第一级
	□对公民、法人和其他组织的合法权益造成严重损害 □对社会秩序和公共利益造成损害	□第二级
	□对社会秩序和公共利益造成严重损害 □对国家安全造成损害	□第三级
	□对社会秩序和公共利益造成特别严重损害 □对国家安全造成严重损害	□第四级
	□对国家安全造成特别严重损害	□第五级
02 确定系统服务安全保护等级	□仅对公民、法人和其他组织的合法权益造成损害	□第一级
	□对公民、法人和其他组织的合法权益造成严重损害 □对社会秩序和公共利益造成损害	□第二级
	□对社会秩序和公共利益造成严重损害 □对国家安全造成损害	□第三级
	□对社会秩序和公共利益造成特别严重损害 □对国家安全造成严重损害	□第四级
	□对国家安全造成特别严重损害	□第五级

03 信息系统安全保护等级	□第一级 □第二级 □第三级 □第四级 □第五级
04 定级时间	年 月 日
05 专家评审情况	□已评审 □未评审
06 是否有主管部门	□有 □无（如选择有请填下两项）
07 主管部门名称	
08 主管部门审批定级情况	□已审批 □未审批
09 系统定级报告	□有 □无 附件名称_____
填表人：	填表日期： 年 月 日

备案审核民警： 审核日期： 年 月 日

表四（ / ）第三级以上信息系统提交材料情况

01 系统拓扑结构及说明	□有	□无	附件名称_____
02 系统安全组织机构及管理制度	□有	□无	附件名称_____
03 系统安全保护设施设计实施方案或改建实施方案	□有	□无	附件名称_____
04 系统使用的安全产品清单及认证、销售许可证明	□有	□无	附件名称_____
05 系统等级测评报告	□有	□无	附件名称_____
06 专家评审情况	□有	□无	附件名称_____
07 上级主管部门审批意见	□有	□无	附件名称_____

表五（ / ）涉及国家秘密的信息系统分级保护备案表

单位名称	
涉密信息系统名称	
系统密级（保护等级）	□ 秘密 □ 机密 □ 绝密
系统联接范围	□局域网 □城域网 □广域网（跨____个省或地）
系统安全域划分和安全域密级确定	□未划分安全域 □划分安全域（共有____个，其中绝密级____个，机密级____个，秘密级____个，内部级____个）
系统主要承建单位	
系统投入使用时间	
系统运行管理部门	
系统安全保密管理部门	
系统分级保护实施情况	□已经实施 □正在实施 □计划_____年实施

填报日期: 年 月 日 填报单位:（盖章）

填表说明:

1. “系统密级”依据《涉及国家秘密的信息系统分级保护管理办法》和国家保密标准 BMB17-2006 确定。

2. 涉密信息系统一般应划分安全域，同一系统内的不同安全域根据所处理信息的重要程度，可分别确定密级。

3. 表中“□”项，确认划“√”。

4. 填报多个涉密信息系统，可复印此表。

国家保密局制

附件 4

《信息系统安全等级保护定级报告》模版

一、XXX 信息系统描述

简述确定该系统为定级对象的理由。从三方面进行说明：一是描述承担信息系统安全责任的相关单位或部门，说明本单位或部门对信息系统具有信息安全保护责任，该信息系统为本单位或部门的定级对象；二是该定级对象是否具有信息系统的基本要素，描述基本要素、系统网络结构、系统边界和边界设备；三是该定级对象是否承载着单一或相对独立的业务，业务情况描述。

二、XXX 信息系统安全保护等级确定（定级方法参见国家标准《网络安全等级保护定级指南》）

（一）业务信息安全保护等级的确定

1. 业务信息描述

描述信息系统处理的主要业务信息等。

2. 业务信息受到破坏时所侵害客体的确定

说明信息受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。

3. 信息受到破坏后对侵害客体的侵害程度的确定

说明信息受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

4. 业务信息安全等级的确定

依据信息受到破坏时所侵害的客体以及侵害程度，确定业务信息安全等级。

（二）系统服务安全保护等级的确定

1. 系统服务描述

描述信息系统的服务范围、服务对象等。

2. 系统服务受到破坏时所侵害客体的确定

说明系统服务受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。

3. 系统服务受到破坏后对侵害客体的侵害程度的确定

说明系统服务受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

4. 系统服务安全等级的确定

依据系统服务受到破坏时所侵害的客体以及侵害程度确定系统服务安全等级。

（三）安全保护等级的确定

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定，最终确定 XXX 系统安全保护等级为第几级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
XXX 信息系统	X	X	X

陕西省交通运输厅　　2018年3月12日印发