**公路水路关键信息基础设施安全保护管理办法**

**（征求意见稿）**

### 第一章 总 则

**第一条** 为规范公路水路关键信息基础设施安全保护管理，落实关键信息基础设施安全保护工作责任，根据《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》等法律、行政法规，制定本办法。

**第二条** 在公路水路关键信息基础设施规划建设、识别认定、安全防护、检测评估、监测预警、事件处置及监管等过程中，为保障关键信息基础设施安全稳定运行和维护数据的完整性、保密性、可用性所执行的各项工作，适用于本办法。

**第三条** 公路水路关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，加强和规范交通运输主管部门监督管理，强化和夯实公路水路关键信息基础设施运营者（以下简称运营者）主体责任，引导和发挥网络安全服务机构等社会各方面的作用，共同保护公路水路关键信息基础设施安全。

**第四条** 交通运输部在职责范围内负责公路水路关键信息基础设施安全保护和监督管理工作，是负责全国公路水路关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。交通运输部网络安全管理部门按照有关规定，主要承担以下具体工作：

（一）制定公路水路关键信息基础设施安全规划；

（二）组织认定公路水路关键信息基础设施；

（三）制定公路水路关键信息基础设施相关标准规范；

（四）建立公路水路关键信息基础设施网络安全监测预警通报制度和应急工作体系；

（五）组织公路水路关键信息基础设施检查检测、风险评估和应急演练。

**第五条** 地方交通运输主管部门在地方党委和政府的领导下，按照谁主管谁负责、属地管理的原则，对本地区公路水路关键信息基础设施实施安全保护和监督管理，配合上级交通运输主管部门和同级网信、公安等部门开展相关工作。

**第六条** 运营者应当在国家网络安全等级保护制度的基础上，履行安全保护管理的主体责任，突出保护重点，落实防护措施，加强全生命周期管理，保护公路水路关键信息基础设施业务连续运行和重要数据不泄露、不受破坏。

**第七条** 任何个人和组织不得实施非法侵入、干扰、破坏公路水路关键信息基础设施的活动，不得危害公路水路关键信息基础设施安全。

未经国家网信部门、国务院公安部门批准或者交通运输部、运营者授权，任何个人和组织不得对公路水路关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。

**第八条** 对在公路水路关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照有关规定给予表彰，激励担当作为。

### 第二章 公路水路关键信息基础设施认定

**第九条** 交通运输部制定和完善公路水路关键信息基础设施认定规则，并报国务院公安部门备案。

制定修订认定规则应当主要考虑下列因素：

（一）网络设施、信息系统等对于公路水路关键核心业务的重要程度；

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

（三）对其他行业和领域的关联性影响。

公路水路关键信息基础设施中包含的网络设施、信息系统，其网络安全保护等级应不低于第三级。

**第十条** 交通运输部根据认定规则负责组织认定公路水路关键信息基础设施，及时将认定结果通知运营者，形成公路水路关键信息基础设施清单，并通报国务院公安部门。

地方交通运输主管部门管辖范围内的公路水路关键信息基础设施，其认定需经地方交通运输主管部门审核后报交通运输部评审认定。

**第十一条** 公路水路关键信息基础设施发生改建、扩建、运营者变更等较大变化时，应重新开展识别工作，可能影响认定结果的，运营者应当及时将相关情况报告交通运输部。交通运输部自收到报告之日起3个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门，更新公路水路关键信息基础设施清单。

地方交通运输主管部门管辖范围内的公路水路关键信息基础设施，发生可能影响认定结果的较大变化时，相关情况需经地方交通运输主管部门报告交通运输部。

### 第三章 运营者责任和义务

**第十二条** 在公路水路关键信息基础设施新建、扩建、升级改造等建设阶段，运营者应当实现安全防护措施与关键信息基础设施主体工程同步规划、同步建设、同步使用，并采取检测评估、攻防演练等方式验证。

**第十三条** 运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对所辖的公路水路关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护、安全防护策略制定和重大网络安全事件处置等工作，组织研究解决重大网络安全问题。

运营者应当设立首席网络安全官，为每个公路水路关键信息基础设施明确一名安全管理责任人。

**第十四条** 运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查和安全技能培训，符合要求的人员方能上岗。鼓励网络安全专门人才从事公路水路关键信息基础设施安全保护工作。

开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

当专门安全管理机构的负责人和关键岗位人员的身份、安全背景等发生变化或必要时，运营者应当根据情况重新进行安全背景审查。

**第十五条** 专门安全管理机构具体负责本单位的公路水路关键信息基础设施安全保护工作，履行下列职责：

（一）建立健全网络安全管理、评价考核制度，拟订公路水路关键信息基础设施安全保护计划；

（二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

（三）按照国家及公路水路行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；

（四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

（五）组织网络安全教育、培训；

（六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；

（七）对公路水路关键信息基础设施设计、建设、运行、维护等服务实施安全管理；

（八）按照规定报告网络安全事件和重要事项。

**第十六条** 运营者应合理安排专门安全管理机构的运行经费，并严格规范经费使用和管理，防止资金闲置或挤占挪用。当重要网络设施和安全设备达到使用期限，应优先保障设施设备更新经费。

**第十七条** 运营者应当加强供应链安全保护，优先采购安全可信的网络产品和服务；采购网络产品和服务影响或者可能影响国家安全的，运营者应当预判网络产品和服务投入使用后可能带来的国家安全风险，按照国家有关规定申报网络安全审查。

运营者应当采购通过检测认证的网络关键设备和网络安全专用产品，采购的云计算服务应当从已通过云计算服务安全评估的云平台中选择。

**第十八条** 运营者应当加强数据安全保护，明确重要数据和个人信息的保护措施，将在我国境内运营中收集和产生的个人信息和重要数据存储在境内，因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估，法律、行政法规另有规定的，依照其规定执行。

**第十九条** 法律、行政法规和国家有关规定要求使用商用密码进行保护的公路水路关键信息基础设施，运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估。商用密码应用安全性评估应当与公路水路关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

**第二十条** 运营者应当加强全过程保密管理，分别与从业人员、维护人员、网络产品和服务提供者等签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。安全保密协议内容应包括安全职责、保密内容、违约责任及行政、刑事违法责任提醒、有效期等。

**第二十一条** 运营者应制定网络安全教育培训制度，定期开展网络安全教育培训和技能考核，首席网络安全官、专门安全管理机构负责人和关键岗位人员等公路水路关键信息基础设施从业人员每人每年教育培训时长不得少于30个学时。

**第二十二条** 运营者应当自行或者委托网络安全服务机构对公路水路关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并及时向交通运输部报送整改情况。

地方交通运输主管部门管辖范围内的公路水路关键信息基础设施，其整改情况需经地方交通运输主管部门审核后报交通运输部。

**第二十三条** 运营者对交通运输部、地方交通运输主管部门以及网信、公安等其他有关部门依法开展的网络安全检查检测工作应当予以配合，提供网络安全管理制度、网络拓扑图、重要资产清单、网络日志等必要的资料。

**第二十四条** 运营者应当制定本单位的监测预警和信息通报制度，对公路水路关键信息基础设施开展7×24小时监测，研判整体安全态势。

**第二十五条** 运营者应当建立网络安全事件管理制度，组织建立专门网络安全应急支撑队伍、专家队伍，制定应急预案等网络安全事件管理文档，每年定期开展本单位的应急演练。

**第二十六条** 公路水路关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者按照有关规定向交通运输部、地方交通运输主管部门、公安机关报告，并立即启动本单位网络安全事件应急预案，固定证据，留存线索。涉及网络攻击的，运营者应当及时向公安机关报案。

### 第四章 保障和监督管理

**第二十七条** 公路水路关键信息基础设施安全规划由交通运输部制定并组织实施，应当符合国家及交通运输行业总体规划，明确保护目标、基本要求、工作任务、具体措施。

**第二十八条** 交通运输部按照国家数据分类分级保护制度要求，组织运营者识别认定重要数据，纳入交通运输重要数据目录，实施重点保护。

地方交通运输主管部门管辖范围内的公路水路关键信息基础设施，其重要数据识别需经地方交通运输主管部门审核后报交通运输部认定。

**第二十九条** 交通运输部、地方交通运输主管部门及其工作人员对于在公路水路关键信息基础设施安全保护过程中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。

**第三十条** 交通运输部、地方交通运输主管部门定期组织开展公路水路关键信息基础设施网络安全检查检测，督促运营者建立问题台账，制定整改方案，及时完成整改加固和复测。

公路水路关键信息基础设施网络安全检查检测应当在国家网信部门的统筹协调下开展，避免不必要的检查和交叉重复检查。检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

**第三十一条** 交通运输部、地方交通运输主管部门按照国家有关规定，对网络安全工作不力、重大安全问题隐患久拖不改，或存在重大网络安全风险、发生重大网络安全事件的运营者，约谈单位负责人，并加大网络安全检查检测力度。

**第三十二条** 交通运输部建立公路水路关键信息基础设施网络安全监测预警制度，依托国家网络与信息安全信息通报机制，完善信息共享和联防联控机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息。

**第三十三条** 交通运输部、地方交通运输主管部门按照国家网络安全事件应急预案的要求，建立健全公路水路行业网络安全事件应急预案，定期组织应急演练。

**第三十四条** 公路水路关键信息基础设施发生整体中断运行或者主要功能故障、重要数据泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，交通运输部在收到报告后，及时向国家网信部门、国务院公安部门报告，立即启动网络安全事件应急预案，指导运营者做好应急处置，并根据需要组织提供技术支持与协助。

### 第五章 法律责任

**第三十五条** 运营者有下列情形之一的，由交通运输部、地方交通运输主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款：

（一）在公路水路关键信息基础设施发生改建、扩建、运营者变更等较大变化时，未及时报告交通运输部，或者未按照交通运输部的要求对公路水路关键信息基础设施进行处置的；

（二）安全保护措施未与公路水路关键信息基础设施同步规划、同步建设、同步使用的；

（三）未建立健全网络安全保护制度和责任制的；

（四）未设置专门安全管理机构的；

（五）未对专门安全管理机构负责人和关键岗位人员进行安全背景审查的；

（六）开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的；

（七）专门安全管理机构未履行本办法第十五条规定的职责的；

（八）采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的；

（九）公路水路关键信息基础设施从业人员每人每年教育培训时长少于30个学时的；

（十）未对公路水路关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照交通运输部要求报送情况的。

**第三十六条** 运营者在公路水路关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向交通运输部、地方交通运输主管部门报告的，由交通运输部、地方交通运输主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

**第三十七条** 运营者违反网络安全审查规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，按照《网络安全法》《网络安全审查办法》有关规定进行处罚。

**第三十八条** 运营者对交通运输部、地方交通运输主管部门开展的网络安全检查检测工作不予配合的，由交通运输部、地方交通运输主管部门责令改正；拒不改正的，处5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款；情节严重的，依法追究相应法律责任。

**第三十九条** 交通运输部、地方交通运输主管部门及其工作人员未履行公路水路关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。

**第四十条** 交通运输主管部门在开展关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的，由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。

**第四十一条** 交通运输部、地方交通运输主管部门、网络安全服务机构及其工作人员将在公路水路关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的，依法对直接负责的主管人员和其他直接责任人员给予处分。

**第四十二条** 公路水路关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

**第四十三条** 电子政务类公路水路关键信息基础设施的运营者不履行本办法规定的网络安全保护义务的，依照《中华人民共和国网络安全法》有关规定予以处理。

**第四十四条** 违反本办法规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

**第四十五条** 网信、公安等部门履行职责，对公路水路关键信息基础设施运营者违法违规行为实施行政处罚的，按照有关法律法规执行。

### 第六章 附则

**第四十六条** 本办法下列用语的含义：

（一）公路水路关键信息基础设施，是指一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的公路水路重要网络设施、信息系统等。

（二）网络产品和服务，是指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。

**第四十七条** 存储、处理涉及国家秘密信息的公路水路关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

**第四十八条** 本办法自202X年X月X日起施行。