# 中华人民共和国交通运输部令

2023 年第 4 号

《公路水路关键信息基础设施安全保护管理办法》已于 2023 年 4 月 14 日经第 8 次部务会议通过,现予公布,自 2023 年 6 月 1 日起施行。

部长 李小鹏

2023 年 4 月 24 日

# 公路水路关键信息基础设施
# 安全保护管理办法

## 第一章　总　　则

**第一条** 为了保障公路水路关键信息基础设施安全，维护网络安全，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** 公路水路关键信息基础设施的安全保护和监督管理工作，适用本办法。

前款所称公路水路关键信息基础设施是指在公路水路领域，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、国计民生和公共利益的重要网络设施、信息系统等。

**第三条** 交通运输部负责全国公路水路关键信息基础设施安全保护和监督管理。对在全国范围运营以及其他经交通运输部评估明确由部管理的公路水路关键信息基础设施（以下统称部级设施），由交通运输部具体实施安全保护和监督管理工作。

省级人民政府交通运输主管部门按照职责对本行政区域内运营的公路水路关键信息基础设施（以下统称省级设施）具体实施安全保护和监督管理。

交通运输部和省级人民政府交通运输主管部门以下统称交通运输主管部门。

**第四条** 公路水路关键信息基础设施安全保护坚持强化和落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，加强和规范交通运输主管部门监督管理，充分发挥社会各方面的作用，共同保护公路水路关键信息基础设施安全。

**第五条** 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。

## 第二章　公路水路关键信息基础设施认定

**第六条** 交通运输部负责制定和修改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。

制定和修改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、信息系统等是否存储处理国家核心数据，以及网络设施、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。

**第七条** 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，形成公路水路关键信息基础设施清单，及时将认定结果通知运营者，并通报国务院公安部门。

**第八条** 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，可能影响其认定结果的，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，更新公路水路关键信息基础设施清单，并通报国务院公安部门。

**第九条** 省级人民政府交通运输主管部门应当按照交通运输部的相关要求，负责组织筛选识别省级行政区域内运营的公路水路关键信息基础设施待认定对象，并研究提出初步认定意见报交通运输部。

交通运输部应当将认定结果通知省级人民政府交通运输主管部门。

## 第三章　运营者责任义务

**第十条** 新建、改建、扩建或者升级改造公路水路关键信息基础设施的，安全保护措施应当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。

运营者应当按照国家有关规定对安全保护措施予以验证。

**第十一条** 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和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

运营者应当明确管理本单位公路水路关键信息基础设施安全保护工作的具体负责人。

**第十二条** 运营者应当设置专门安全管理机构，明确负责人和关键岗位人员并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。

运营者应当保障专门安全管理机构的人员配备，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。

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者必要时，运营者应当重新进行安全背景审查。

**第十三条** 运营者应当保障专门安全管理机构的运行经费，并依法依规严格规范经费使用和管理，防止资金挤占挪用。

重要网络设施和安全设备达到使用期限的，运营者应当优先保障设施设备更新经费。

**第十四条** 运营者应当加强公路水路关键信息基础设施供应链安全管理，应当采购依法通过检测认证的网络关键设备和网络安全专用产品，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可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

鼓励运营者从已通过云计算服务安全评估的云计算服务平台中采购云计算服务。

**第十五条** 运营者应当加强公路水路关键信息基础设施个人信息和数据安全保护，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。

**第十六条** 公路水路关键信息基础设施的网络安全保护等级应当不低于第三级。

运营者应当在网络安全等级保护的基础上，对公路水路关键信息基础设施实行重点保护，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障公路水路关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

**第十七条** 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。部级设施的运营者应当直接向交通运输部报送相关情况；省级设施的运

营者应当将相关情况报经省级人民政府交通运输主管部门审核后报送交通运输部。

**第十八条** 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，其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。

**第十九条** 运营者应当加强保密管理，按照国家有关规定与网络产品和服务提供者等必要人员签订安全保密协议，明确提供者等必要人员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。

**第二十条** 运营者应当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。教育培训的具体内容和学时应当遵守国家有关规定。

**第二十一条** 运营者应当建设本单位网络安全监测系统，对公路水路关键信息基础设施开展全天候监测和值班值守。

运营者应当加强本单位网络安全信息通报预警力量建设，依托国家网络与信息安全信息通报机制，及时收集、汇总、分析各方网络安全信息，组织开展网络安全威胁分析和态势研判，及时通报预警和处置。

**第二十二条** 运营者应当按照国家有关要求制定网络安全事件应急预案，建立网络安全事件应急处置机制，加强应急力量建设和应急资源储备，每年至少开展一次应急演练，并针对应急演练发现的突出问题和漏洞隐患，及时整改加固，完善保护措施。

**第二十三条** 部级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，运营者应当直接向交通运输部、公安机关报告，并立即启动本单位网络安全事件应急预案。

省级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，运营者应当立即向省级人民政府交通运输主管部门、公安机关报告，并启动本单位网络安全事件应急预案。省级人民政府交通运输主管部门应当将相关情况及时报告交通运输部。

公路水路关键信息基础设施发生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，交通运输部应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

## 第四章　保障和监督

**第二十四条** 交通运输部应当制定公路水路关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。

交通运输主管部门、运营者应当严格落实公路水路关键信息基础设施安全规划。

**第二十五条** 交通运输部应当建立公路水路关键信息基础设施网络安全监测预警制度，充分利用网络安全信息共享机制，及时掌握公路水路关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

省级人民政府交通运输主管部门应当及时掌握省级设施的运行状况、安全态势，并组织做好预警通报和安全防范工作。

**第二十六条** 交通运输部应当按照国家网络安全事件应急预案的要求，建立健全公路水路网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

省级人民政府交通运输主管部门应当依据前款规定组织做好本行政区域内公路水路网络安全事件应急预案、应急演练相关工作，并将应急预案、应急演练情况及时报告交通运输部。省级人民政府交通运输主管部门应当指导省级设施运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

**第二十七条** 交通运输主管部门应当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，指导监督运营者建立问题台账，制定整改方案，及时整改安全隐患、完善安全措施。省级人民政府交通运输主管部门应当将检查检测情况及时报告交通运输部。

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。

**第二十八条** 运营者对交通运输主管部门开展的网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的公路水路关键信息基础设施网络安全检查工作应当予以配合，并如实提供网络安全管理制度、重要资产清单、网络日志等必要的资料。

**第二十九条** 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，或者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，并加大网络安全监督检查力度。

**第三十条** 交通运输主管部门、网络安全服务机构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。

## 第五章　法律责任

**第三十一条** 运营者违反本办法规定的，由交通运输主管部门按照《关键信息基础设施安全保护条例》等法律、行政法规的规定予以处罚。

**第三十二条** 交通运输主管部门及其工作人员存在以下情形之一的，按照《关键信息基础设施安全保护条例》等法律、行政法规的规定予以处分:

（一）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;

（二）在开展公路水路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;

（三）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。

## 第六章 附 则

**第三十三条** 本办法自 2023 年 6 月 1 日起施行。