ICS 35.040
R07

JT

中华人民共和国交通运输行业标准

JT/T XXX—XXXX

交通运输行业信息系统安全等级保护实施策略

Implementation guide for security classified protection of transportation information system

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国交通运输部　发布

目　次

前　言

本标准按照GB/T1.1-2009给出的规则起草。

本标准由交通运输部科技司提出。

本标准由交通运输部信息通信及导航标准化技术委员会归口。

本标准起草单位：中国交通通信信息中心。

本标准主要起草人：李璐瑶、戴明、武俊峰、成瑾、肖榕、刘佳、王梓博、杜渐。

交通运输行业重要信息系统等级保护实施策略

1 范围

本标准规定了交通运输行业重要信息系统等级保护工作涉及的角色及各角色在等级保护工作中不同阶段的工作职责。

本标准适用于指导交通运输行业信息系统等级保护工作中各角色的工作内容。

2 规范性引用文件

本实施策略的编制主要依据或引用以下政策及标准，下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本标准。

中华人民共和国计算机信息系统安全保护条例　国务院 147 号令

关于信息安全等级保护工作的实施意见　公通字[2004]66 号

信息安全等级保护管理办法　公通字[2007]43 号

关于开展信息系统等级保护安全建设整改工作的指导意见　公信安[2009]1429 号

信息安全等级保护备案实施细则　公信安[2007]1360 号

交通运输行业信息安全等级保护定级指南

交通运输行业信息安全等级保护基本要求

GB17859　　计算机信息系统安全保护等级划分准则

GB/T25058-2010　　信息安全技术 信息系统安全等级保护实施指南

GB/T22239-2008　　信息安全技术 信息系统安全等级保护基本要求

3 等级保护概述

3.1 等级保护对象

交通运输行业等级保护的主要对象是交通运输行业重要信息系统，具体指二级（含）以上信息系统。

3.2 等级保护目标

通过对交通运输行业重要信息系统进行安全等级划分，按照国家及交通运输行业标准的安全等级保护要求进行规划、建设、运维、管理和监督，从而加强交通运输行业重要信息系统的安全防护能力，确保其安全性和可靠性。

3.3 等级保护实施基本原则

交通运输行业重要信息系统安全等级保护的核心是对信息系统分等级、按标准进行建设、管理和监督。交通运输行业重要信息系统安全等级保护实施过程中应遵循以下基本原则：

a)　自主保护原则

信息系统运营、使用单位及其主管部门按照国家相关法规和标准，自主确定信息系统的安全保护等级，自行组织实施安全保护。

b） **重点保护原则**

根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及交通运输行业核心业务或关键信息资产的信息系统。

c） **同步建设原则**

信息系统在新建、改建、扩建时应当同步规划和设计安全方案，投入一定比例的资金建设信息安全设施，保障信息安全与信息化建设相适应。

d） **动态调整原则**

要跟踪信息系统的变化情况，调整安全保护措施。由于信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据相关法规、标准和要求，重新确定信息系统的安全保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。

3.4 等级保护角色和职责

交通运输行业重要信息系统安全等级保护实施过程中，涉及的等级保护角色和职责如下：

负责依照国家相关法规、标准和要求，实施信息安全等级保护工作。信息系统运营、使用单位分为部级层面和行业层面两部分。

部级层面：包括部机关、部直属单位及为部服务的单位。

行业层面：包括省厅、市局、县局及部直属单位省级、市级、县级业务管理部门。

a） **信息系统主管部门**

负责依照国家相关法规、标准和要求，督促、检查和指导信息系统运营、使用单位的信息安全等级保护工作。

- 部科技司：部机关、部直属单位及为部服务单位所运营、使用的信息系统的主管部门，指导、监督、检查部、省两级信息系统运营、使用单位的信息安全等级保护工作。中国交通通信信息中心作为日常执行机构，受部科技司委托承担具体执行工作。
- 部直属单位：部直属单位在省级、市级、县级的业务管理部门所运营、使用的信息系统的主管部门。
- 交通运输厅（局）：省级、市级、县级交通运输厅（局）各机关所运营、使用的信息系统的主管部门，指导、监督、检查省、市、县三级信息系统运营、使用单位的信息安全等级保护工作。

b） **信息安全服务机构**

负责根据信息系统运营、使用单位的委托，依照国家相关法规、标准和要求，协助信息系统运营、使用单位完成等级保护的相关工作，包括确定信息系统的安全保护等级、进行安全需求分析、安全总体规划、实施安全建设和安全改造、安全运维等。

c） **信息安全等级测评机构**

负责根据信息系统运营、使用单位的委托或根据国家管理部门的授权，协助信息系统运营、使用单位，按照国家信息安全等级保护的管理规范和技术标准，对已经完成等级保护建设的信息系统进行等级测评。

d） **信息安全产品供应商**

按照等级保护相关要求销售信息安全产品，并为信息系统运营、使用单位提供相关服务。

3.5 等级保护实施的基本流程

交通运输行业重要信息系统按照等级保护全生命周期，可以划分为系统定级和备案、总体安全规划、安全设计与实施、安全运行与维护、等级测评、安全检查等阶段。

交通运输行业重要信息系统等级保护实施基本流程见图 1。

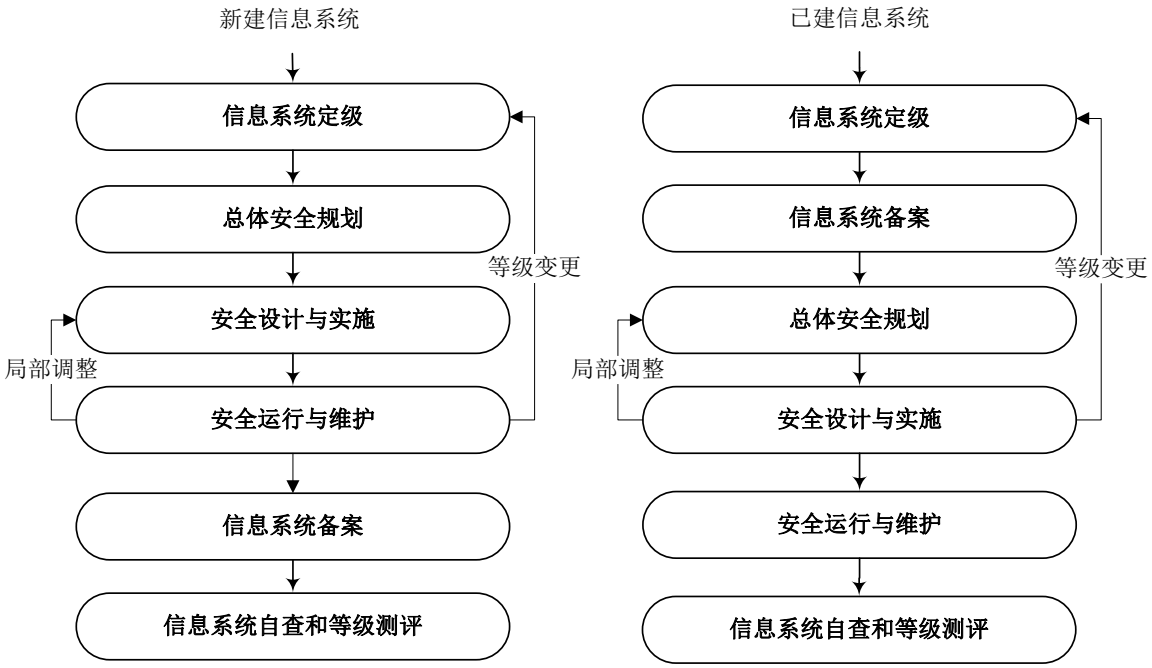

图 1 交通运输行业重要信息系统等级保护实施基本流程

在安全运行与维护阶段，交通运输行业重要信息系统因需求变化等原因导致局部调整，而系统的安全保护等级并未改变，应从安全运行与维护阶段进入安全设计与实施阶段，重新设计、调整和实施安全措施，确保满足等级保护的要求；但交通运输行业重要信息系统发生重大变更导致系统安全保护等级变化时，应从安全运行与维护阶段进入信息系统定级阶段，重新开始一轮信息安全等级保护的实施过程。

在信息系统备案阶段，新建系统是在系统投入运行后 30 日内进行备案；已建信息系统是在系统定级后进行备案。

4 系统定级和备案

新建、升级改造、扩建的交通运输行业重要信息系统在可研、初设阶段就需由信息系统运营、使用单位确定系统等级；已建系统应根据交通运输行业总体工作部署，有序确认系统等级。

4.1 定级

交通运输行业重要信息系统定级遵循以下原则：

- 各单位自建（与上级单位无关）的信息系统：由信息系统运营、使用单位自主确定安全保护等级；对拟确定为第四级（含）以上信息系统的，由信息系统主管部门联合部科技司组织信息安全等级保护专家进行评审。
- 跨省或全国统一联网运行的信息系统：
  - 集中部署的信息系统：由信息系统主管部门统一确定安全保护等级；由信息系统主管部门联合部科技司组织信息安全等级保护专家进行评审。
  - 分布部署的信息系统：由信息系统运营、使用单位自主确定安全保护等级；对拟确定为第四级（含）以上信息系统的，由信息系统主管部门联合部科技司组织信息安全等级保护专家进行评审。

4.2 定级结果审批

- 第二级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：初步确定了安全保护等级后，采取两级审核机制，由信息系统主管部门审核批准后，形成信息系统定级评审意见并上报部科技司审核批准，并形成信息系统定级评审意见。
  - 其它系统：初步确定了安全保护等级后，由信息系统主管部门审核批准，形成信息系统定级审批意见。
- 第三级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：初步确定了安全保护等级后，采取两级审核机制，由信息系统主管部门审核批准后，形成信息系统定级评审意见并上报部科技司审核批准，并形成信息系统定级评审意见。
  - 其它系统：初步确定了安全保护等级后，由信息系统主管部门审核批准，形成信息系统定级审批意见。
- 第四级（含）以上系统：初步确定了安全保护等级后，采取两级审核机制，由信息系统主管部门审核批准后，形成信息系统定级评审意见并上报部科技司审核批准，并形成信息系统定级评审意见。

4.3 定级报备

信息系统运营、使用单位在信息系统安全保护等级确定后，向公安机关备案，备案通过后，应将信息系统定级结果上报省级信息系统主管部门，并由省级信息系统主管部门于每年12 月初统一上报部科技司备案，由部科技司形成《交通运输行业信息系统等级保护年报》。

4.4 等级变更

信息系统安全保护等级发生等级变更后，需重新定级。重新定级后，应按要求向公安机关重新备案，并重新进行定级报备工作。

4.5 系统备案

信息系统运营、使用单位根据国家管理部门对备案的要求，整理相关备案材料，并向受理备案的单位提交备案材料。

- 新建信息系统

在系统投入运行后 30 日内，由信息系统运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

- 已建信息系统

在系统定级后 30 日内，由信息系统运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

- 跨省或全国统一联网运行的信息系统：
  - 集中部署的信息系统，由信息系统主管部门向公安部办理备案手续。
  - 分布部署的信息系统：由信息系统运营、使用单位向当地设区的市级以上公安机关备案。

5 总体安全规划

交通运输行业重要信息系统总体安全规划工作涉及三方面的内容：安全需求分析、总体安全设计、安全项目建设规划。总体安全规划阶段的工作由信息系统运营、使用单位依靠自身的技术力量或在信息安全服务机构的协助下来完成。

信息系统运营、使用单位应将总体安全规划阶段形成的信息系统安全总体方案、信息系统安全项目建设规划报备。

- 第二级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：上报信息系统主管部门和部科技司备案。
  - 其它系统：上报信息系统主管部门备案。
  - 第三级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：上报信息系统主管部门和部科技司备案。
  - 其它系统：上报信息系统主管部门备案。
- 第四级（含）以上系统：上报信息系统主管部门和部科技司备案。

6 安全设计与实施

交通运输行业重要信息系统安全设计与实施是按照信息系统安全总体方案的要求，结合交通运输行业重要信息系统安全建设项目计划，分期分步落实安全措施，包括管理措施和技术措施。安全设计与实施阶段的工作由信息系统运营、使用单位依靠自身的技术力量或在信息安全服务机构的协助下来完成。

6.1 安全设计方案

信息系统运营、使用单位形成的安全设计方案经审批后进行信息系统安全实施工作。

- 第二级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：上报部科技司审批，形成审批意见。
  - 其它系统：不需审批。
- 第三级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：上报部科技司审批，形成审批意见。
  - 其它系统：不需审批。
- 第四级（含）以上系统：上报部科技司审批，行成审批意见。

6.2 信息安全产品认证

信息系统主管部门推荐信息安全产品，上报部科技司审核，由部科技司进行审核，审核通过后发布《交通运输行业信息安全产品名录》。信息安全产品应满足如下条件：

- 产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，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；
- 产品研制、生产单位及其主要业务、技术人员无犯罪记录；
- 产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；
- 对国家安全、社会秩序、公共利益不构成危害；
- 对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

对于不同级别的信息系统，分别采取强制使用和推荐使用《交通运输行业信息安全产品名录》两种方式。

- 第二级信息系统

- 跨省或全国统一联网、集中部署的信息系统：强制使用《交通运输行业信息安全产品名录》中的产品。
- 其它系统：推荐使用。

- 第三级（含）以上信息系统：强制使用《交通运输行业信息安全产品名录》中的产品。

6.3 系统验收

系统验收是检验系统是否严格按照安全详细设计方案进行建设，是否实现了设计的功能和性能。信息系统运营、使用单位或协助其进行信息系统安全建设的信息安全服务机构应提交系统验收所需下列材料供验收单位审查：信息系统运营、使用单位与信息安全服务机构签订的合同书、系统需求分析报告、系统定级报告、信息系统安全总体方案、信息系统安全项目建设规划、信息系统安全详细设计方案。

- 第二级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：由信息系统运营、使用单位联合部科技司共同进行验收，对验收文档进行审查；
  - 其它系统：由信息系统运营、使用单位进行验收，对验收文档进行审查。
- 第三级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：由信息系统运营、使用单位联合部科技司共同进行验收，对验收文档进行审查；
  - 其它系统：由信息系统运营、使用单位进行验收，对验收文档进行审查。
- 第四级（含）以上系统：由信息系统运营、使用单位联合信息系统主管部门、部科技司共同进行验收，对验收文档进行审查。

验收文档审查通过后，由信息系统运营、使用单位或协助其进行信息安全建设的信息安全服务机构形成系统验收报告。

7 等级测评

信息系统等级测评是根据已经确定的安全管理等级，检验信息系统安全管理体系和管理水平是否满足确定等级的管理要求。信息系统运营、使用单位在信息系统备案（拟建、新建系统）或整改建设（已建信息系统）完成后应委托符合国家等级保护规定的信息安全等级测评机构进行等级测评。

信息系统运营、使用单位为委托主体，信息安全等级测评机构为测评执行主体。

7.1 等级测评机构选择

信息系统运营、使用单位应选择经交通运输部认可的测评机构。

中国交通通信信息中心推荐国家级别的信息安全测评机构名单，各省厅信息系统主管部门分别推荐各省级信息安全等级测评机构名单，上报部科技司审核，审核通过后发布《交通运输行业全国等级保护测评机构推荐目录》。等级测评机构应满足如下条件：

- 在中华人民共和国境内注册成立（港澳台地区除外）；
- 由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；
- 从事相关检测评估工作两年以上，无违法记录；
- 工作人员仅限于中国公民；
- 法人及主要业务、技术人员无犯罪记录；
- 使用的技术装备、设施应当符合本实施策略对信息安全产品的要求；
- 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全

管理制度；

- 对国家安全、社会秩序、公共利益不构成威胁。

对于不同级别信息系统，分别采用强制使用和推荐使用《交通运输行业等级保护测评机构推荐名录》两种方式。

- 第二级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：信息系统运营、使用单位需选择《交通运输行业等级保护测评机构推荐名录》中的等级测评机构进行等级测评。
  - 其它系统：推荐使用。
- 第三级（含）以上系统：信息系统运营、使用单位应选择《交通运输行业等级保护测评机构推荐名录》中的等级测评机构进行等级测评。

7.2 等级测评

- 第二级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：每年进行一次等级测评，等级测评报告需上报信息系统主管部门和部科技司备案。
  - 其它系统：建议每年进行一次等级测评，等级测评报告需上报信息系统主管部门备案。
- 第三级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：每半年进行一次等级测评，等级测评报告需上报信息系统主管部门和部科技司备案。
  - 其它系统：每年进行一次等级测评，等级测评报告需上报信息系统主管部门备案。
- 第四级信息系统：每半年进行一次等级测评，等级测评报告需上报信息系统主管部门和部科技司备案。
- 第五级信息系统：略。

8 安全运行与维护

交通运输行业重要信息系统的信息安全运行与维护模式包括自运维、外包运维和混合运维。本实施策略中的安全运行与维护包括以上三种运维模式，分别由交通运输行业重要信息系统运营、使用单位依靠自身的技术力量或者在信息安全服务机构协助下完成信息系统安全运行与维护。

9 安全检查

安全检查采取各信息系统运营、使用单位自查与信息系统主管部门、部科技司安全抽查相结合的方式进行。

9.1 自查

- 第二级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：每年自查一次。
  - 其它系统：建议每年自查一次。
- 第三级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：每半年自查一次。
  - 其它系统：每年自查一次。
- 第四级信息系统：每半年自查一次。

- 第五级信息系统：略。

9.2 安全抽查

各级管理部门应定期或不定期对信息系统等级保护工作进行安全抽查。

- 第二级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：每年不定期抽查至少一次，由信息系统主管部门联合部科技司进行安全抽查。
  - 其它系统：由信息系统主管部门不定期抽查。
- 第三级信息系统
  - 跨省或全国统一联网、集中部署的信息系统：每年不定期抽查至少两次，由信息系统主管部门联合部科技司进行安全抽查。
  - 其它系统：每年不定期抽查至少一次，由信息系统主管部门进行安全抽查。
- 第四级信息系统：每年不定期抽查至少两次，由信息系统主管部门联合部科技司进行安全抽查。
- 第五级信息系统：略。

上述安全检查结果由省级信息系统主管部门于每年 12 月初上报部科技司备案，由部科技司形成《交通运输行业信息系统等级保护年报》。

9.3 改进方案制定

信息系统运营、使用单位根据安全检查的结果，调整信息系统的安全状态，保证信息系统安全防护的有效性。确定安全改进的工作方法、工作内容、人员分工、时间计划等，制定安全改进方案。安全改进方案只适用于小范围内的安全改进，如安全加固、配置加强、系统补丁等。

9.4 安全改进实施

信息系统运营、使用单位应保证按照安全改进方案实现各项补充安全措施，并确保原有的技术措施和管理措施与各项补充的安全措施一致有效地工作。按照安全改进方案实施和落实各项补充的安全措施后，要调整和修订各类相关的技术文件和管理制度，保证原有体系完整性和一致性。