收费公路联网收费系统网络安全管理暂行办法

取消高速公路省界收费站总指挥部网络安全组

交通运输部路网监测与应急处置中心

2019年10月

目录

1 编制背景

1 编制背景

按照取消高速公路省界收费站总指挥部工作部署，为加强收费公路联网收费系统网络安全管理，构建全国性系统网络安全的管理体系和技术体系，实现**管理和技术“两手抓”**的双重保障，网络安全组在前期制定印发《联网收费系统省域系统并网接入网络安全基本技术要求》基础上，组织编制了《收费公路联网收费系统网络安全管理暂行办法》（简称“管理办法”）。

1 编制背景

管理办法主要基于以下背景编制：

构建全网整体安全管理体系的迫切需要

取消高速公路省界收费站实施之后，全国联网收费系统架构发生重大变化，形成“一张网”运行格局，原有的部省边界明确、防护体系分立的状态转变为全网安全一体化、局部风险全局化，必须通过建立整体的、协同的安全管理制度，有效界定各相关单位安全管理责任，明确各责任主体在建设运行等各环节的安全管理要求，构建“**全网一体、分工明确、部省协同、责任共担**”的安全管理体系，提升联网收费系统整体安全管理水平。

1 编制背景

贯彻落实国家网络安全管理制度标准的需要

《网络安全法》、网络安全等级保护制度等相关法规政策都对安全管理提出了一系列要求，特别是5月中旬国家新发布的网络安全等级保护2.0标准，对安全管理工作在制度、机构、人员、建设管理、运维管理等各方面作出了明确规定。

长期以来，全国联网收费系统不仅技术防护能力较低，安全管理也十分薄弱，存在管理制度不完善、责任界定不清晰、法律规定不落实、等保要求不达标等突出问题，导致系统建设和运行安全管理风险普遍存在，安全事件多发频发，加快实现“强监管、强约束、强保障”的安全管理已经势在必行。通过本办法的制定实施，将全面贯彻落实国家网络安全法规、制度、标准，有效填补目前联网收费系统在安全管理制度建设上的空白。

1 编制背景

规范撤站工程安全建设和系统长期安全稳定运行的迫切需要

当前，部和全国各省都在积极推动撤站工程实施，开展联网收费系统的大规模新改建工程建设，按照网络安全“三同步”的要求，必须对建设阶段的安全工作提出明确管理要求，保证安全建设依法合规，实现对新建系统安全的源头管控。同时，系统年底投入运行后，也亟需在日常安全运行管理、数据安全管理、外包及第三方服务、监测预警和应急处置、监督检查等方面提出明确的管理要求，确保统一的安全管理策略的有效落实。制定本办法，不仅是保障当前撤站任务圆满完成的需要，也是管全面、管长远，保障全国联网收费系统长期安全稳定运行的制度基础。

2 编制思路

2 编制思路

结合联网收费系统管理实际

牢固树立正确网络安全观

全面落实国家法规、制度和等级保护标准要求

强化风险管控，明确责任分工

全生命周期、全要素覆盖、全过程管控

注重管理体系一体化、管理要求基线化

管理内容可考核、防护体系可实现

3 主要内容

3 主要内容

《管理办法》共十章七十六条

收费公路联网收费系统网络安全管理暂行办法

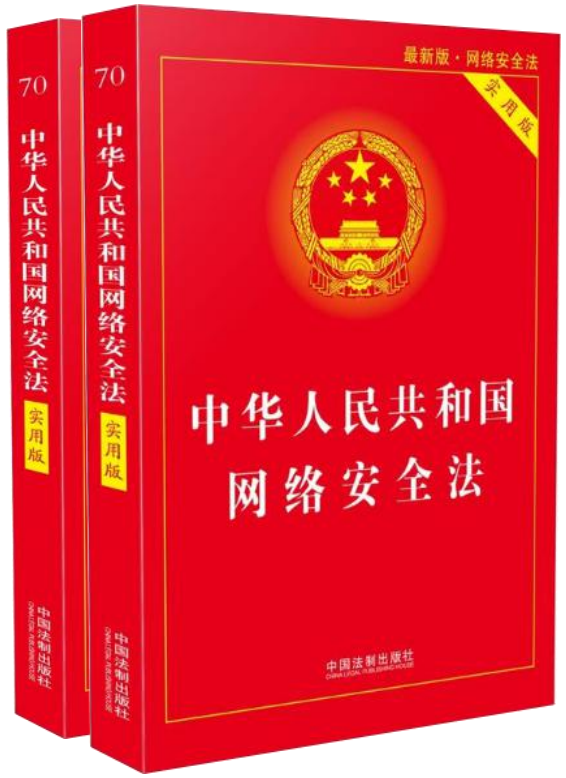
- 第一章总　则
- 第二章职责和分工
- 第三章建设网络安全管理
- 第四章运行维护网络安全管理
- 第五章数据安全和个人信息保护
- 第六章外包及第三方服务安全管理
- 第七章风险管控和预警应急
- 第八章监督检查与责任追究
- 第九章保障措施
- 第十章附　则

第一章 总则

本章明确了编制目的、依据、适用范围，联网收费系统定义及网络安全管理的方针和目标。

第一章 总则

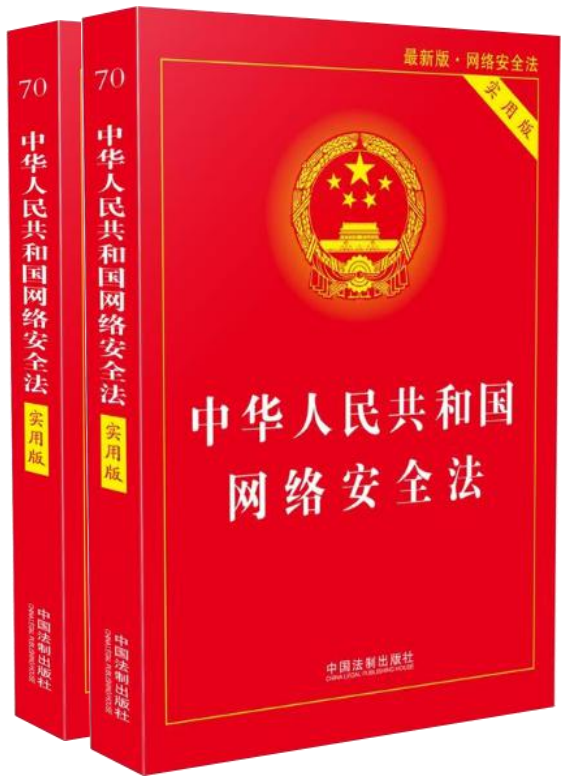
《网络安全法》提高了网络安全地位



- 加速推动信息领域核心技术突破
- 加强关键信息基础设施网络安全防护
- 加强网络安全预警监测
- 依法加强网络空间治理
- 切实维护国家网络空间主权安全，共同构建网络空间命运共同体

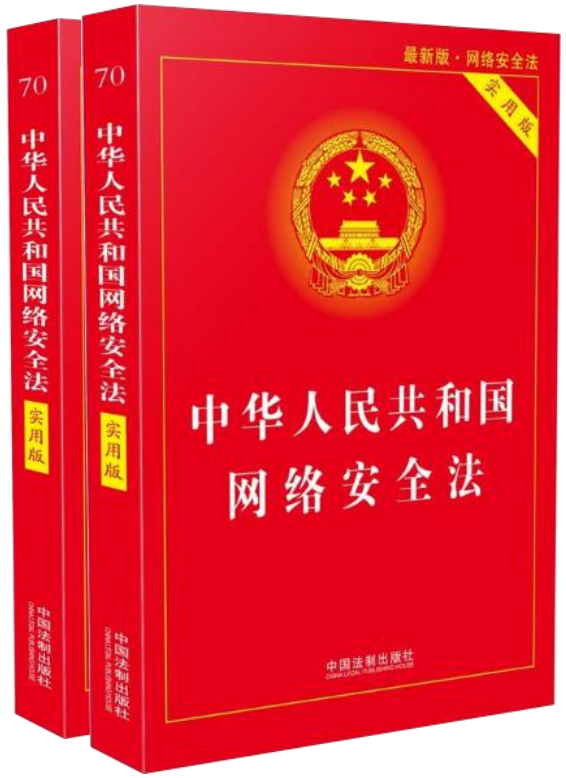
3 主要内容

第一章 总则



第一章 总则

重点一：推动网络安全等级保护制度



第二十一条 **国家实行网络安全等级保护制度。**网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全**管理制度和操作规程**，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的**技术措施**；

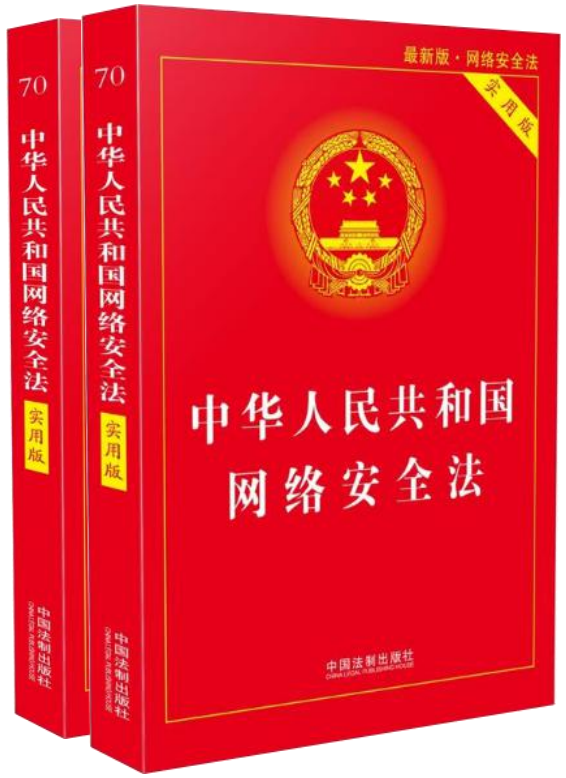
（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的**网络日志**不少于六个月；

（四）采取**数据分类**、**重要数据备份和加密**等措施；

（五）法律、行政法规规定的其他义务。

第一章 总则

重点二：加强关键信息基础设施运行安全

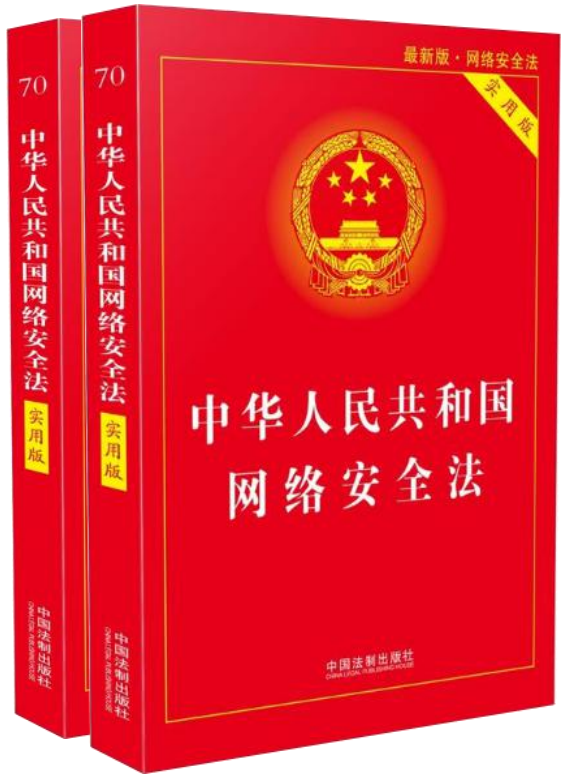


第三十一条 国家对公共通信和信息服务、能源、**交通**、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，**在网络安全等级保护制度的基础上，实行重点保护。**关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第一章 总则

重点三：加强个人信息保护，保障数据安全



第二十二条 ..... 网络产品、服务具有收集用户信息功能的，其提供者应当**向用户明示并取得同意**；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第四章 网络信息安全

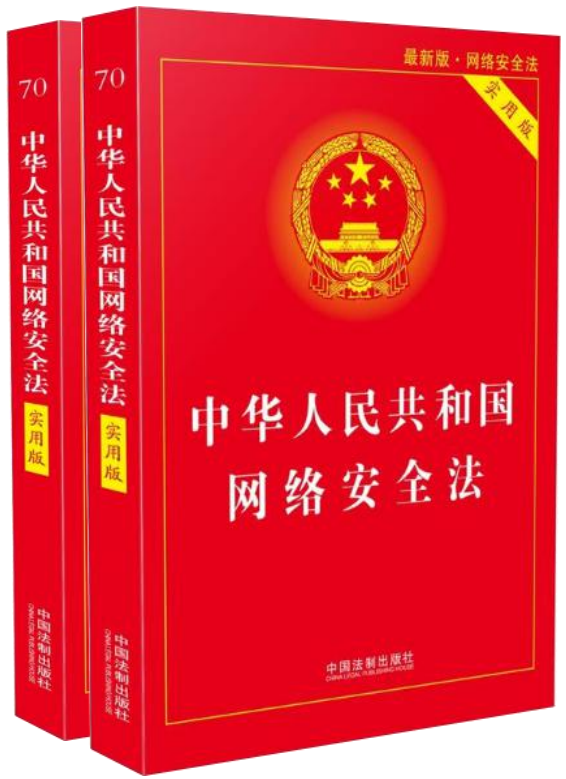
第四十条 网络运营者应对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循**合法**、**正当**、**必要**的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第一章 总则

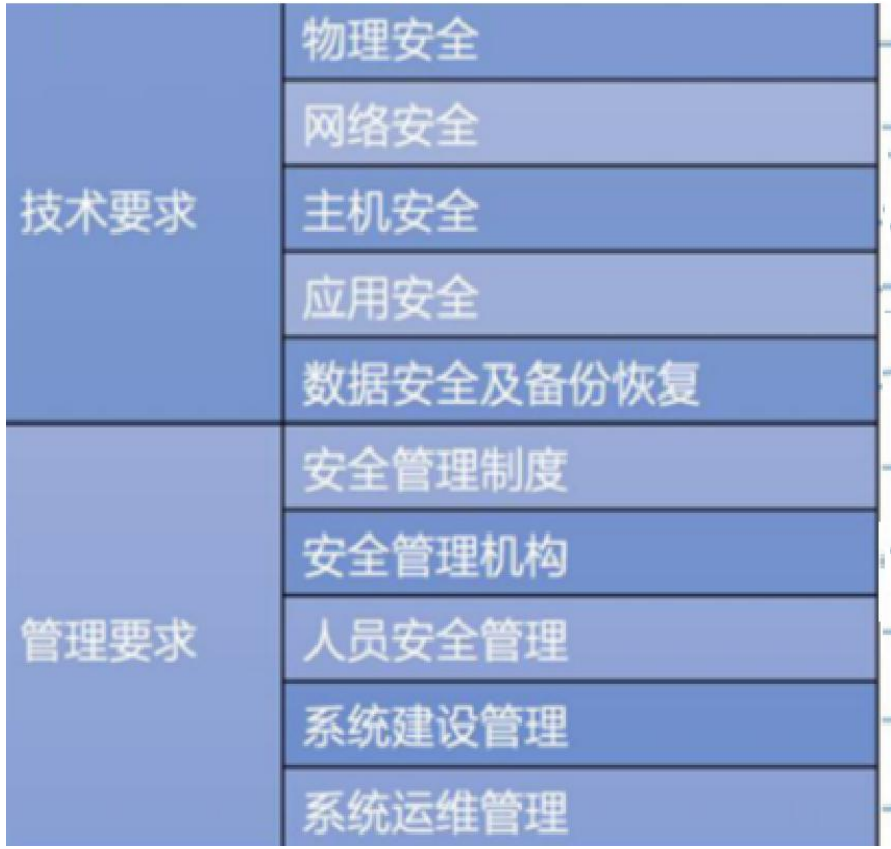
重点四：快速响应，实施网络安全风险应急预案



第二十五条 网络运营者应当**制定网络安全事件应急预案**，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第一章 总则

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求



等保1.0

安全物理环境	技术要求
安全通信网络	
安全区域边界	
安全计算环境	
安全管理中心	
安全管理制度	管理要求
安全管理机构	
安全管理人员	
安全建设管理	
安全运维管理	

等保2.0

第一章 总则

增加了应用场景说明

增加了描述等级保护安全框架和关键技术、云计算应用场景、移动互联应用场景、物联网应用场景、工业控制系统应用场景。如图为附录中新增的等级保护安全框架。

第一章 总则

- 《中华人民共和国网络安全法》
- 《计算机信息系统安全保护条例》
- 《收费公路管理条例》
- 《收费公路联网收费技术要求》
- 《GB/T 22239—2019信息安全技术 网络安全等级保护基本要求》

第一章 总则

。

方针
- 依法管理、安全可控、全网一体、共同保护

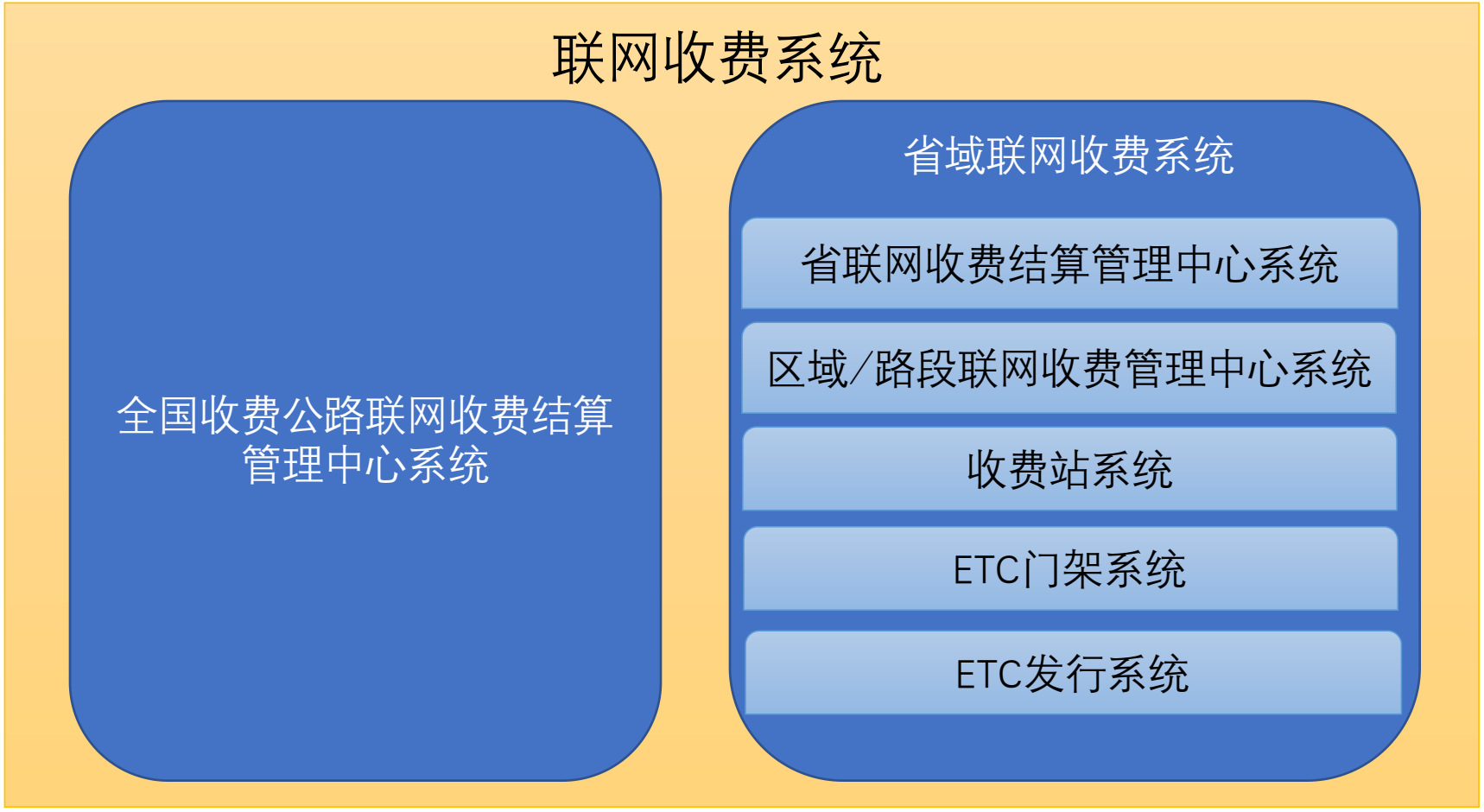
要求
- 同步规划、同步建设、同步使用

围绕
- 全生命周期、全要素覆盖、全过程监测

注重
- **风险管控**和应急预防

第一章 总则

本办法所称联网收费系统，是指用于开展收费公路联网收费的计算机信息系统。



第一章 总则

省联网中心系统包含省级清分结算系统等业务处理类系统，省级稽查与信用管理系统、密钥管理系统、客服系统等业务辅助系统，以及网络基础运行环境。具有清分结算功能的区域及路段中心以省联网中心安全要求为标准。

ETC**发行系统**主要包含发行中心系统、网点发行系统、互联网发行系统、便携式发行系统等。ETC发行系统不承担联网收费业务生产控制核心功能，但其与联网收费系统存在网络连接和数据交互，且存有大量公民个人信息。

ETC发行系统应按照等级保护第三级要求进行定级、备案、测评、保护，同时应通过严格的网络访问控制策略管控其与省联网中心系统的网络连接和数据交互，同时，针对互联网访问边界进行严格管控，并应按照**《GB/T 35273-2017信息安全技术 个人信息安全规范》**等有关国家标准重点加强个人信息保护。

第一章 总则

区域/路段中心系统包含：ETC门架系统的运行监测与预警系统、收费稽查管理系统等业务辅助类系统及有关网络基础运行环境，同时包含省联网中心与收费站的通信网络传输系统。区域/路段中心系统一般不承担联网收费业务生产控制、业务数据处理等核心业务，但其存在与省联网收费系统和收费站间的网络连接和数据交换。

收费站系统主要包括：ETC车道系统、ETC/MTC混合车道系统、站级管理系统及有关网络基础运行环境。

ETC门架系统主要包含ETC门架收费软件，车道控制器、RSU、车牌图像识别等设施设备及有关网络基础运行环境。

第二章 职责与分工

主要是依据《网络安全法》和网络安全工作责任制的相关规定，对联网收费系统安全管理涉及各方的职责分工进行了界定，明确了部省两级交通运输主管部门、全国中心和省中心管理单位、收费公路经营管理单位以及ETC发行机构等各相关主体在建设、运行维护安全、数据安全、监测应急和监管检查工作责任，解决了长期以来各相关单位存在管理权责不清、责任真空的问题。

第二章 职责与分工

各单位主要负责人是网络安全工作的第一责任人

主管网络安全的领导班子成员是直接负责人

第二章 职责与分工

- 国务院国家交通运输主管部门
- 省级交通运输主管部门
- 交通运输部路网监测与应急处置中心
- 承担全国联网收费结算管理业务的机构
- 承担省级联网收费结算管理业务的机构
- 收费公路经营管理单位
- ETC发行服务机构

第二章 职责与分工

省级交通运输主管部门是本地区联网收费系统网络安全工作主管部门，承担综合协调和指导监督职责，主要包括：

（一） 组织贯彻落实国家、行业、地方网络安全相关法律法规、标准规范，指导和监督联网收费系统网络安全制度和标准在本地区的贯彻执行；

（二） 指导建立完善本地区联网收费系统网络安全监测预警、应急处置和监督检查工作机制，协调组织本地区的重大及以上网络安全风险预警、网络安全事件应急处置工作；

（三） 组织开展本地区联网收费系统网络安全检查工作，指导和监督省级联网收费结算管理中心、收费公路经营管理单位、ETC发行服务机构等相关单位履行网络安全责任；

（四）协调处理本地区跨部门的网络安全重要事项，配合上级交通运输主管部门和同级网信、公安有关部门开展工作。。

第二章 职责与分工

交通运输部路网监测与应急处置中心（以下简称“部路网中心”）承担全国联网收费系统网络安全工作协调组织和日常管理职责，主要包括：

（一） 指导全国中心系统运行单位建立健全网络安全管理制度体系和综合防范体系，**协调省联网中心系统运行单位建立健全网络安全管理制度体系和综合防范体系**；

（二） **承担省域系统并网接入的安全管理**；

（三） 指导全国中心系统数据安全管理工作，**协调省级联网中心数据安全管理工作**；

（四） 组织建立联网收费系统**监测预警**和**应急处置**工作机制，参与重大及以上网络安全风险预警、网络安全事件应急处置工作；

（五） 组织建立联网收费系统网络安全**信息通报**机制，承担联网收费系统网络安全信息通报工作组日常工作；

（六） 建立联网收费系统网络安全**教育培训**机制，负责加强有关工作人员网络安全教育培训；

（七） 配合上级有关部门组织开展联网收费系统网络安全检查和整改督促等工作；

（八） 承担上级部门交办的其他工作。

第二章 职责与分工

承担全国联网收费结算管理业务的机构是全国中心系统网络安全建设和运行主体责任单位，承担全国中心系统网络安全工作协调组织和日常管理职责，主要包括主要包括：

（一） 负责建立完善全国中心系统网络安全管理制度体系和综合防范体系；

（二） **负责ETC门架系统计费软件安全开发和安全升级管理工作；**

（三） 负责全国中心系统、ETC发行系统等数据安全管理，建立数据安全管理制度；

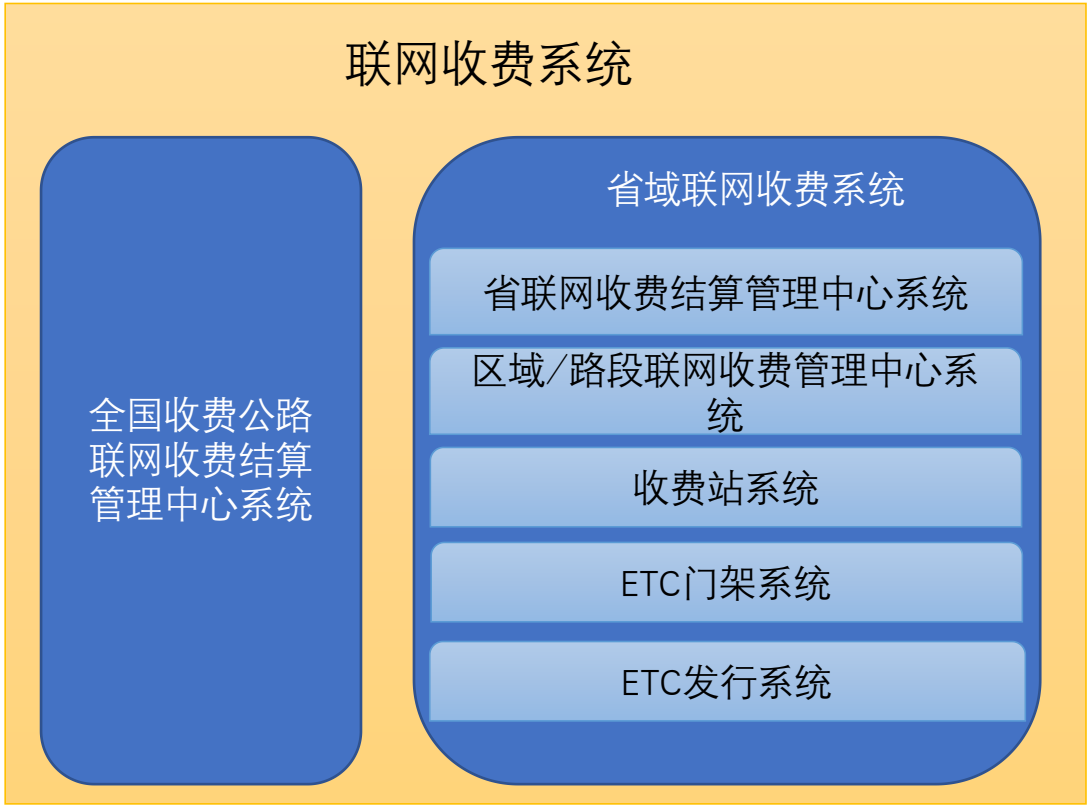
（四） 建立全国中心系统的监测预警和应急工作机制，组织网络安全风险预警响应和网络安全事件应急处置；

（五） 负责全国中心系统网络安全信息通报工作；

（六） 配合上级部门开展全国中心系统网络安全检查和整改督促工作，配合网信、公安等部门开展工作；

（七） 负责全国中心系统有关工作人员网络安全教育培训；

（八） 承担上级部门交办的其他工作。



第二章 职责与分工

承担省级联网收费结算管理业务的机构（以下简称“省联网中心”）是省联网中心系统网络安全建设和运行主体责任单位，承担**省域系统**网络安全工作协调组织和日常管理职责，主要包括：

（一） 负责建立完善省联网中心系统网络安全管理制度体系和综合防范体系；

（二） 履行省联网中心系统并网接入责任，**负责本地区省域系统联网安全管理**；

（三） 负责省联网中心系**统数据安全管理**，建立数据安全管理制度，指导本地区收费公路经营管理单位、ETC发行服务机构等数据安全管理工作；

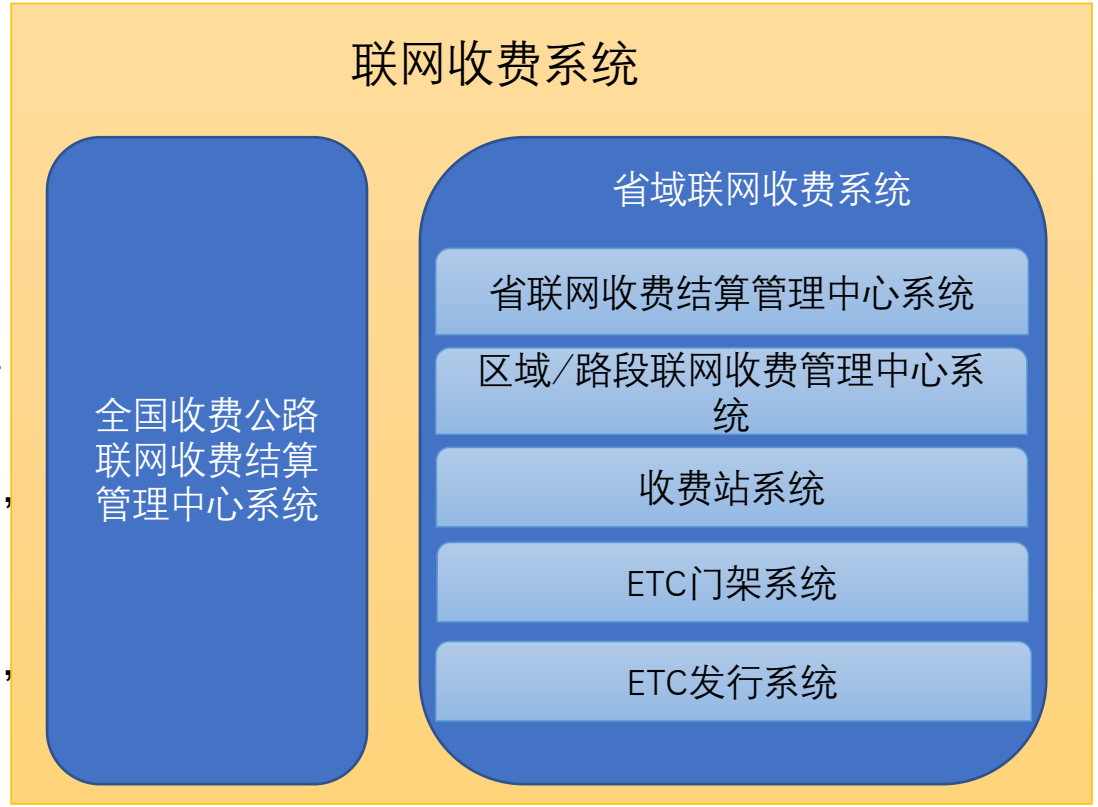
（四） 建立本地区省域联网收费系统的**监测预**警和**应急**工作机制，组织、协调本地区省域联网收费系统网络安全风险预警响应和事件**应急处**置工作；

（五） 组织建立本地区省域联网收费系统网络安全**信息通报**机制，负责有关上传下达工作；

（六） 配合交通运输主管部门组织开展本地区省域联网收费系统网络**安全检查和整改督促**工作，配合网信、公安等部门开展工作；

（七） 建立网络安全**教育培训**机制，负责加强本地区省域联网收费系统有关工作人员网络安全教育培训；

（八） 承担上级部门交办的其他工作。



第二章 职责与分工

收费公路经营管理单位承担本单位区域/路段中心系统、收费站系统、ETC门架系统的网络安全建设和运行主体责任，主要包括：

（一）负责建立所辖路段的区域/路段中心系统、收费站系统、ETC门架系统的网络安全管理制度体系和综合防范体系；

（二）履行本单位建设的区域/路段中心系统、收费站系统、ETC门架系统的**并网接入安全责任**；

（三）负责本单位建设、运行的区域/路段中心系统、收费站系统、ETC门架系统的**数据安全管理**，建立数据安全管理制度，组织下属各单位落实数据安全管理措施；

（四）建立本单位的网络安全**监测预警和应急处置工作机制**，组织网络安全风险预警响应和网络安全事件应急处置；

（五）负责本单位联网收费系统的网络安全**信息通报工作**；

（六）配合交通运输主管部门、省联网中心组织开展网络**安全检查**，负责开展问题整改工作，配合网信、公安等部门开展工作；

（七）负责加强本单位联网收费系统有关工作人员网络安全**教育培训**工作；

（八）承担上级部门交办的其他工作。

第二章 职责与分工

ETC发行服务机构是各省区市开展ETC发行和服务的行业机构，承担本单位ETC发行系统的网络安全建设和运行主体责任，主要包括：

（一）负责建立ETC发行系统的网络安全管理制度体系和综合防范体系，协调银行业金融机构、 、非银行支付机构和互联网企业等ETC发行合作发行单位机构建立ETC发行系统网络安全管理机制；

（二）负责ETC发行系统的数据安全管理，建立数据及**个人信息安全管理制度**，落实数据及个人信息安全管理措施；

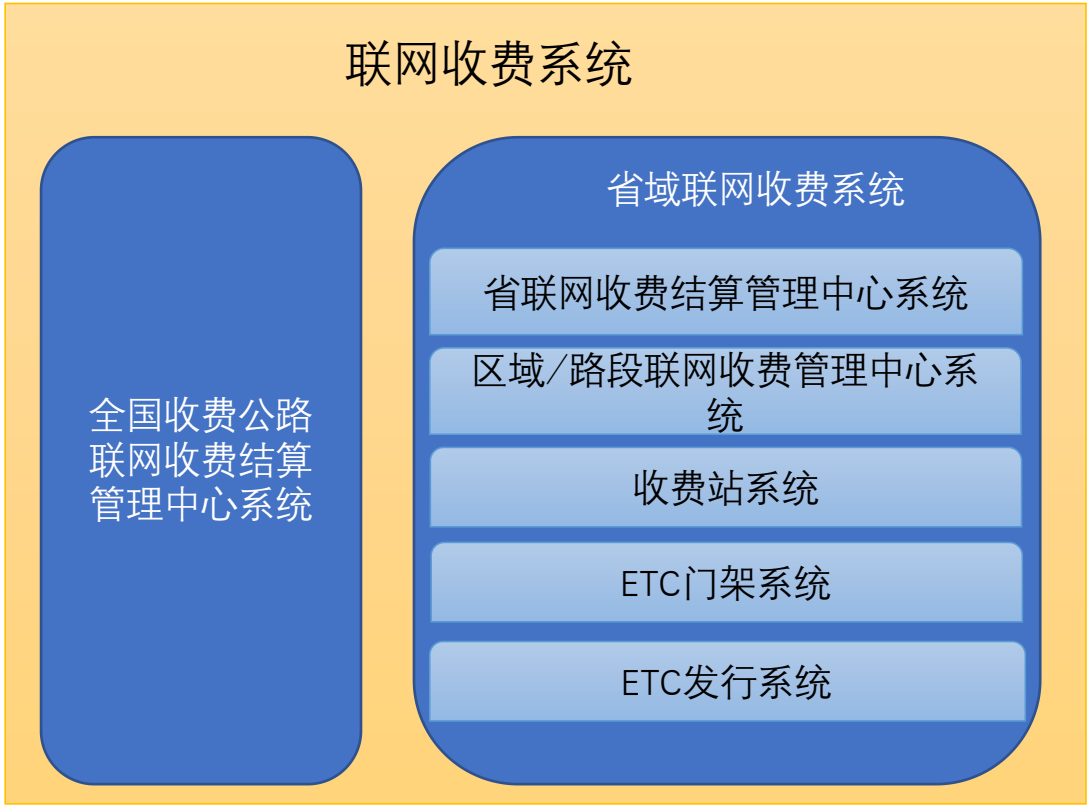
（三）建立ETC发行系统的网络安全监测预警和应急工作机制，组织本单位的网络安全风险预警响应和网络安全事件应急处置；

（四）负责ETC发行系统的网络安全信息通报工作；

（五）配合交通运输主管部门、省联网中心组织开展网络安全检查，负责开展问题整改工作，配合网信、公安等部门开展工作；

（六）负责加强本单位有关工作人员网络安全教育培训工作；

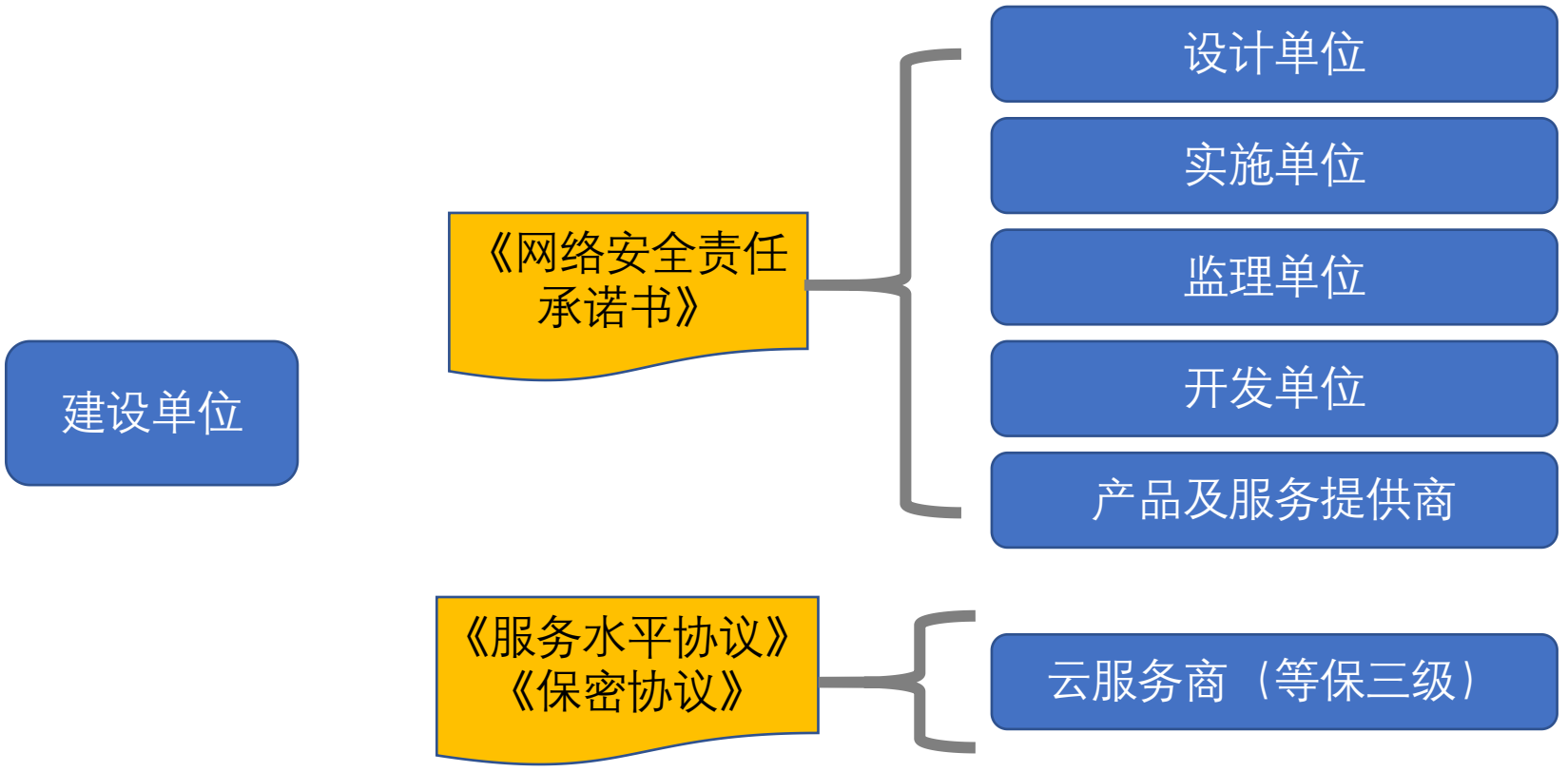
（七） 承担上级部门交办的其他工作。



第三章 建设网络安全管理

从建设内容出发，为避免“先天性风险隐患”，对系统建设过程中规划设计、建设开发、部署上线等环节的网络安全工作进行了规定，包括参建单位的责任界定、安全设计、设备采购、云服务商选择、数据备份、软件开发、安全检测、密码应用、质量管理等相关内容，并重点就交付验收和并网运行前严格管控提出要求。

第三章 建设网络安全管理



3 主要内容

第三章 建设网络安全管理

信息安全技术 关键信息基础设施网络安全保护基本要求（征求意见稿）

附□录□A
（资料性附录）
安全保密协议模版

甲方单位名称：_____·····地址：_____

乙方单位名称：_____·····地址：_____

本协议于_____年_____月_____日起生效。

根据我国有关网络安全及信息保密相关法律法规，本着平等、自愿、公平、诚信的原则，双方就采购网络产品和服务事宜及后续合作过程中有关网络安全保密事项达成以下协议，并由双方共同遵守。采购网络产品和服务的一方应为“甲方”，提供网络产品和服务的一方应为“乙方”。

A. 1□保密内容和范围

甲乙双方确认，乙方承担保密义务的甲方信息包括但不限于以下内容：

(1) 技术信息：同甲方业务相关的程序、代码、流程、方法、文档、数据等内容；
(2) 业务信息：同甲方业务相关的人员、财务、策略、计划、资源消耗数量、通信流量大小等业务信息；
(3) 安全信息：包括账号、口令、密钥、授权等用于对网络、系统、进程等进行访问的身份与权限数据，还包括对正当履行自身工作职责所需要的重要、适当和必要的信息。

A. 2□保密义务

A. 2. 1□乙方明确所接收的保密信息及其载体均为甲方所有。乙方承认甲方在本协议规定的保密信息上

第三章 建设网络安全管理

系统设计、建设

- 全国联网收费结算管理中心系统
- 省联网收费结算管理中心系统
- ETC发行系统
- 区域/路段联网收费管理中心系统
- 收费站系统
- ETC门架系统

等保三级定级、设计

通信网络、区域边界、计算环境参照等保三级设计

国家关键信息基础设施

联网收费系统省域系统并网接入网络安全基本技术要求

第三章 建设网络安全管理

采购产品及服务
符合国家法律、行政法规的规定和强制性国家标准要求

冗余备份
数据分级分类
备份恢复策略
设备、线路冗余设计

软件开发及升级
规范 版本控制
文档 源代码
仿真测试环境

交付验收
建设过程文档
运行维护文档
技能培训

四部联合发布《网络关键设备和网络安全专用产品目录（第一批）》的公告

国家互联网信息办公室
中华人民共和国工业和信息化部
中华人民共和国公安部
中国国家认证认可监督管理委员会

公　　告

2017 年　第 1 号

关于发布《网络关键设备和网络安全专用产品目录(第一批)》的公告

为加强网络关键设备和网络安全专用产品安全管理，依据《中华人民共和国网络安全法》，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目

录(第一批)》，现予以公布，自印发之日起施行。

一、列入《网络关键设备和网络安全专用产品目录》的设备和产品，应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

具备资格的机构指国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室按照国家有关规定共同认定的机构。

二、网络关键设备和网络安全专用产品认证或者检测委托人，选择具备资格的机构进行安全认证或者安全检测。

三、网络关键设备、网络安全专用产品选择安全检测方式的，经安全检测符合要求后，由检测机构将网络关键设备、网络安全专用产品检测结果(含本公告发布之前已经本机构安全检测符合要求、且在有效期内的设备与产品)依照相关规定分别报工业和信息化部、公安部。

选择安全认证方式的，经安全认证合格后，由认证机构将认证结果(含本公告发布之前已经本机构安全认证合格、且在有效期内的设备与产品)依照相关规定报国家认证认可监督管理委员会。

国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一发布。

特此公告。

四部联合发布《网络关键设备和网络安全专用产品目录（第一批）》的公告

附件

网络关键设备和网络安全专用产品目录(第一批)

	设备或产品类别	范围
网络关键设备	1. 路由器	整系统吞吐量(双向)≥12Tbps 整系统路由表容量≥55 万条
	2. 交换机	整系统吞吐量(双向)≥30Tbps 整系统包转发率≥10Gpps
	3. 服务器(机架式)	CPU 数量≥8 个 单 CPU 内核数≥14 个 内存容量≥256GB
	4. 可编程逻辑控制器(PLC 设备)	控制器指令执行时间≤0.08 微秒
网络安全专用产品	5. 数据备份一体机	备份容量≥20T 备份速度≥60MB/s 备份时间间隔≤1 小时
	6. 防火墙(硬件)	整机吞吐量≥80Gbps 最大并发连接数≥300 万 每秒新建连接数≥25 万
	7. WEB 应用防火墙(WAF)	整机应用吞吐量≥6Gbps 最大 HTTP 并发连接数≥200 万
	8. 入侵检测系统(IDS)	满检速率≥15Gbps 最大并发连接数≥500 万
	9. 入侵防御系统(IPS)	满检速率≥20Gbps 最大并发连接数≥500 万
	10. 安全隔离与信息交换产品(网闸)	吞吐量≥1Gbps 系统延时≤5ms
	11. 反垃圾邮件产品	连接处理速率(连接/秒)＞100 平均延迟时间＜100ms
	12. 网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5 万条/秒
	13. 网络脆弱性扫描产品	最大并行扫描 IP 数量≥60 个
	14. 安全数据库系统	TPC－E tpsE(每秒可交易数量)≥4500 个
	15. 网站恢复产品(硬件)	恢复时间≤2ms 站点的最长路径≥10 级

抄送：中央国家机关有关部门。

国家互联网信息办公室秘书局　　2017 年 6 月 1 日印发

共印 200 份

第三章 建设网络安全管理

系统验收

全国联网收费结算管理中心系统

省联网收费结算管理中心系统

ETC发行系统

区域/路段联网收费管理中心系统

收费站系统

ETC门架系统

等级保护定级备案证明和测评报告

密码应用安全评估报告

信息安全风险评估报告

并网接入技术要求符合性检测报告

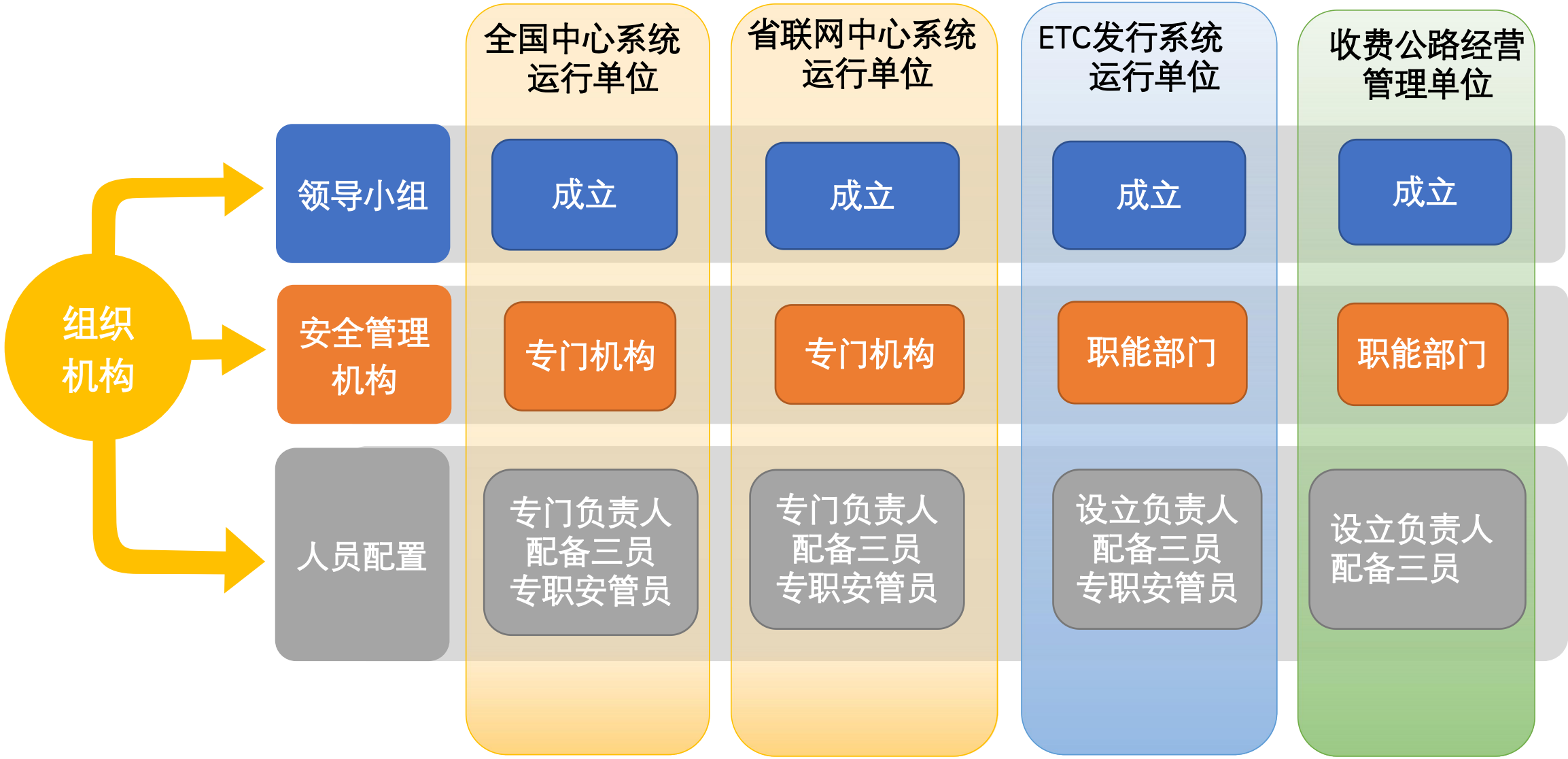
第四章 运行维护网络安全管理

从运行安全角度出发，按照等级保护标准要求，对运维管理制度体系和组织机构建设、人员配备、机房管理、网络边界管理、软硬件设备运行维护等方面的安全管理提出了工作要求。同时，对计算机终端、介质、远程维护访问、漏洞管理、恶意代码防范、运维操作、配置管理等重点环节的安全防护工作提出了明确要求。

第四章 运行维护网络安全管理

安全管理制度体系

第四章 运行维护网络安全管理



第四章 运行维护网络安全管理

授权审批制度	人员管理制度	机房管理制度	资产管理制度
◆ 审批程序 ◆ 审批部门 ◆ 审批人	◆ 录用人员审查、保密协议 ◆ 关键岗位签署岗位责任协议 ◆ 调离手续	◆ 指定部门、人员 ◆ 出入登记 ◆ 定期检查	◆ 明确责任部门 ◆ 使用、维护、报废 ◆ 软硬件资产清单、网络拓扑

第四章 运行维护网络安全管理

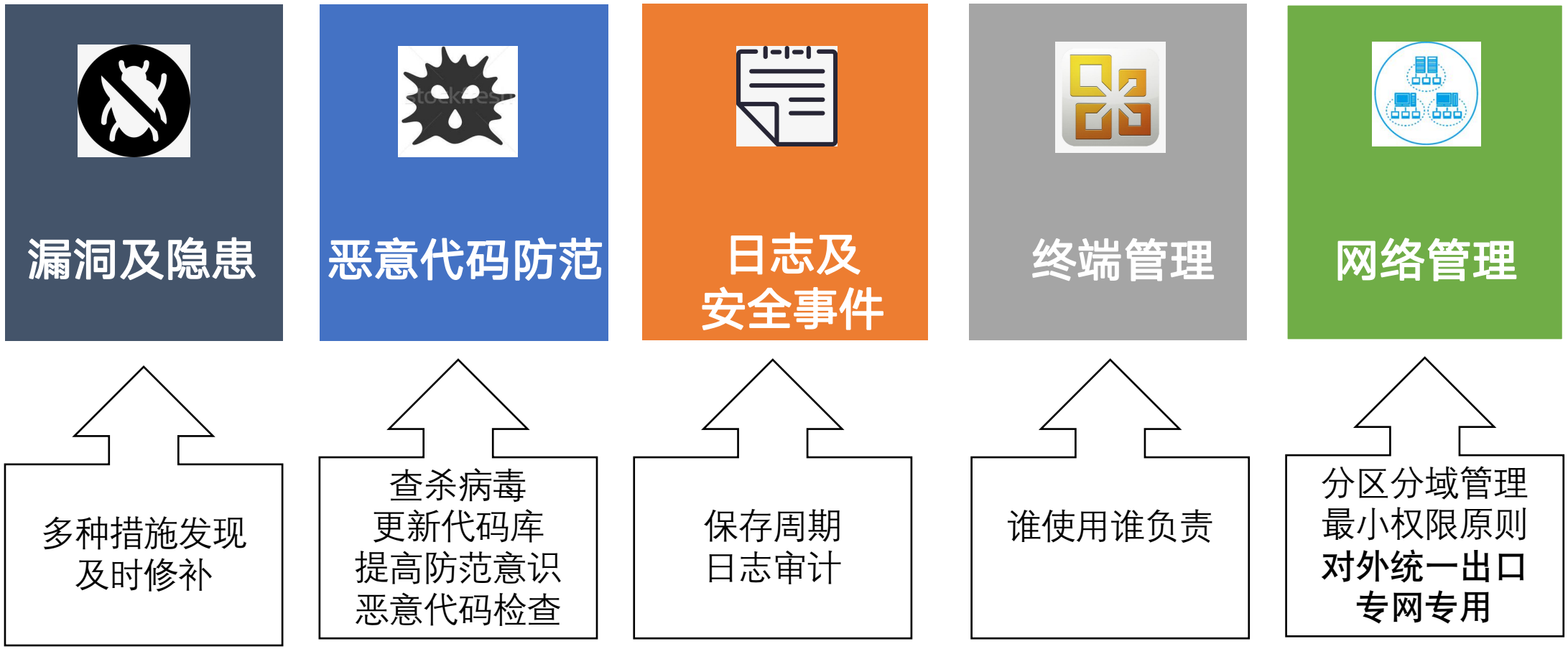
介质管理
- 介质清单
- 介质使用登记记录
- 报废/重用
- 使用管理要求

权限管理
- 账户管理
- 用户密码强度、更换频率
- 离职离岗权限回收

设备维护
- 指定部门或人员
- 设备带离要求
- 实时监测、定期巡检

运维规程
- 变更性运维管理
- 运维工具使用管理
- 远程运维管理

第四章 运行维护网络安全管理



第四章 运行维护网络安全管理

第五章 数据安全和个人信息保护

从保护重要数据和个人信息安全的角度，提出了信息采集、信息处理、信息保护和信息共享等方面的相关要求，主要涉及数据分类分级、数据备份与恢复、数据共享及个人信息保护等方面。

鉴别数据

公民个人信息

关键业务数据

交易和清分数据、拆分数据等

服务支撑数据

基础数据、费率数据、黑名单数据、稽查数据、车辆图像数据等

第五章 数据安全和个人信息保护

《GB/T 35273-2017 信息安全技术个人信息安全规范》

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

判定某项信息是否属于个人信息，应考虑以下两条路径：

一是**识别**，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。

二是**关联**，即从个人到信息，如已知特定自然人，则由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。

符合上述两种情形之一的信息，均应判定为个人信息。

表A.1 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮箱等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等
网络身份标识信息	系统账号、IP 地址、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息，及体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账号、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的用户操作记录，包括网站浏览记录、软件使用记录、点击记录等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/android ID/IDFA/OPENUDID/GUID、SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

第五章 数据安全和个人信息保护

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。

第五章 数据安全和个人信息保护

表B.1个人敏感信息举例

个人财产信息	**银行账号**、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、**交易和消费记录**、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	**身份证**、**军官证**、**护照**、**驾驶证**、工作证、社保卡、居住证等
网络身份标识信息	**系统账号**、邮箱地址及与前述有关的**密码**、**口令**、口令保护答案、用户个人数字证书等
其他信息	**个人电话号码**、性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、**行踪轨迹**、网页浏览记录、住宿信息**精准定位信息**等

第五章 数据安全和个人信息保护

制定数据分级分类策略

明确收集、处理流程

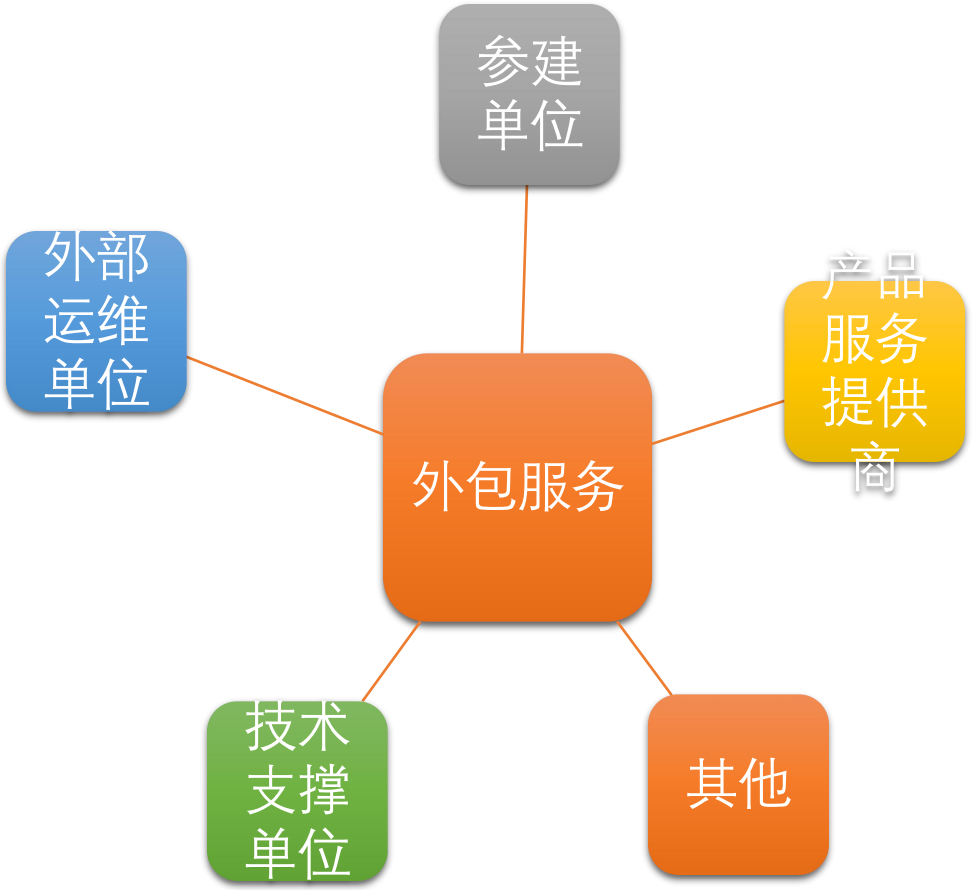
制定数据备份、恢复策略

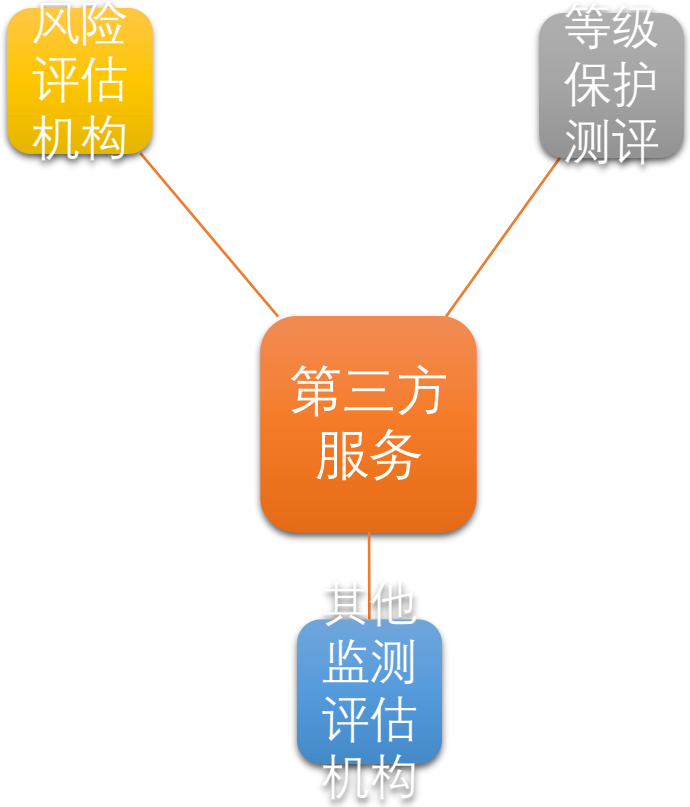
定期开展恢复演练

第六章 外包及第三方服务安全管理

主要根据联网收费系统外包及第三方服务单位较多的实际情况，为保障供应链安全，对系统建设运维过程中的外包及第三方服务范围及要求进行规定，包括外包服务过程监测、设备出入、账号管理、外包人员管理及项目结束管理等内容。

第六章 外包及第三方服务安全管理





第六章 外包及第三方服务安全管理

单位管理

√具有相关专业资质

√外包单位签订保密协议

人员管理

√必要的背景审查

禁 关键岗位

√变更管理

√账户管理

服务要求

√登记备案制度

√监测操作行为

√设备、资料和介质离场管理

服务结束

√归还设备设施

√冻结、删除外包账户

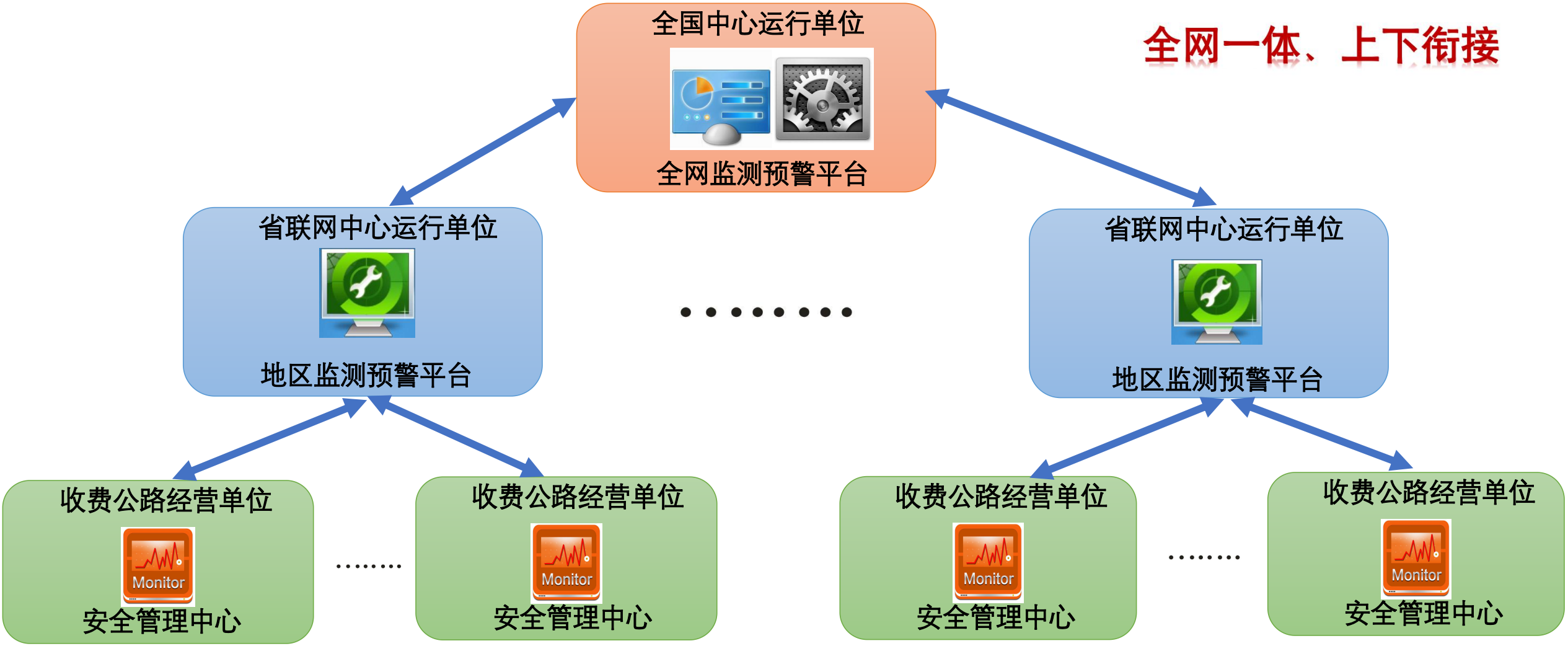
√关闭本地或远程访问通道

第七章　风险管控和预警应急

各单位应以**风险管控**理念为指引，建立健全机制，加强联网收费系统规划、建设、运行维护各环节以及制度、设备、网络、数据等各方面的风险识别、评价、预防和控制，强化监测预警和动态防护，积极应对技术和管理缺陷带来的内外部安全风险，有效处置网络安全事件。

第七章　风险管控和预警应急

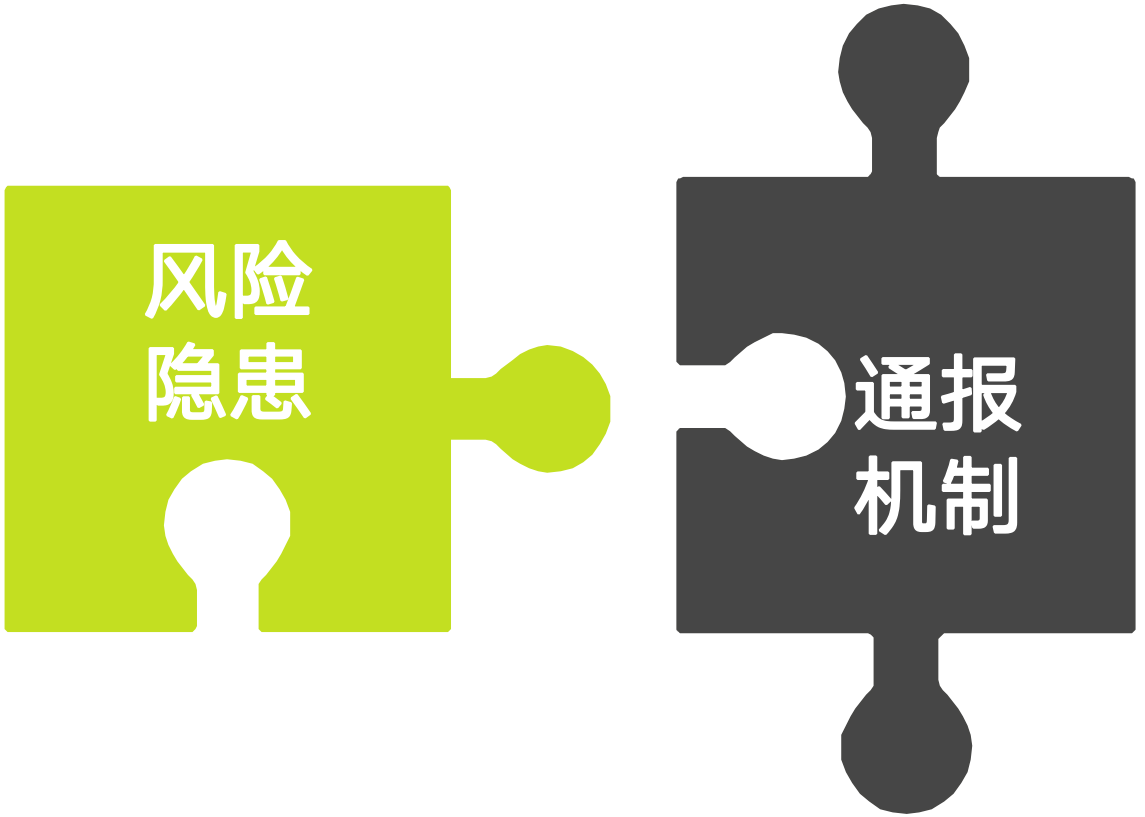
全网一体、上下衔接



第七章　风险管控和预警应急

管控

- 建立风险隐患台账
- 履行整改第一责任
- 及时完成整改



执行

- 加强信息收集、分析和共享，
- 确保通报信息传达到位
- 及时通报
- 逐级反馈

第七章　风险管控和预警应急

- 明确应急工作机构
- 制定应急预案
- **每年至少一次**应急演练
- 细化的应急处置流程
- 建立协调机制

- 立即启动应急预案
- 做好初步处置
- 及时开展信息通报

- 完成事件调查和评估工作
- 处理意见和改进措施

3 主要内容

第七章　风险管控和预警应急

《网络安全事件应急预案》

一．总则

二．事件分级分类

三．组织机构和职责

四．监测与预警

五．应急处置

六．预防工作与应急准备

七．保障措施

八．总则

3 主要内容

《收费公路联网收费系统网络安全信息通报工作规范（试行）》

附件4 收费公路联网收费系统网络安全事件分级分类

（一）有害程序事件

（二）网络攻击事件

（三）信息破坏事件

（四）信息内容安全事件

（五）设备设施故障

（六）灾害性事件

（七）内部潜在威胁事件

（八）其他事件

3 主要内容

特别重大网络安全事件（I级）

1. 联网收费系统所有个人信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

2. 其他对联网收费系统安全稳定运行构成特别严重威胁，对社会秩序和公众利益造成特别严重影响的网络安全事件，为特别严重网络安全事件。

3 主要内容

重大网络安全事件（II级）

4. 导致2日内3省（含）以上省域联网收费系统累计**10000台以上终端**（含ETC门架系统）、**500台以上服务器或其他关键网络设备**发生大规模有害程序事件，对正常办公、公众服务或重要业务运行造成严重影响的。

5. 因遭受网络攻击、设备故障、灾害等，导致**2日内3省（含）以上**联网收费系统业务**中断达24个小时（含）以上**对政府形象和公众服务造成严重损害的网络安全事件。

6. 联网收费系统泄露**5万人以上**行踪轨迹、家庭住址等**个人敏感信息**。

3 主要内容

较大网络安全事件（III级）

1.联网收费系统发生信息内容安全事件，造成交通运输行业秘密或重要内部敏感信息、反动信息、煽动性信息、谣言等大范围传播，对国家安全、社会稳定和政府形象造成较大损害的。

2.导致省联网中心系统、ETC发行系统核心设备已被渗透控制或大量关键敏感数据、个人重要信息发生严重毁损、丢失、篡改或泄露，对国家安全、社会稳定、行业运行造成较大损害的。

3.导致**2日内两省（含）以上**省域联网收费系统累计**3000台以上终端（含ETC门架系统）、300台以上服务器或其他关键网络设备**发生大规模有害程序事件，对正常办公、公众服务或重要业务运行造成较大影响的。

4.因遭受网络攻击、设备故障、灾害等，导致**两省（含）以上**联网收费系统业务中断达**72个小时**（含）以上对政府形象和公众服务造成严重损害的网络安全事件。

第八章 监督检查和责任追究

- 网络安全责任制落实情况
- 等级保护工作落实情况
- 并网接入技术要求落实情况
- 网络安全专项行动部署落实情况
- 信息通报工作开展
- 风险预警处置措施
- 教育培训工作开展

检查

自查

责令改正

通报批评

问责程序

第九章 保障措施

宣传教育

人才保障

经费保障

组织领导

绩效考核

第十章 附则

第七十四条 省级交通运输主管部门应根据本办法制定本地区联网收费系统网络安全管理制度。

第七十五条 本办法由交通运输部科技司负责解释。

第七十六条 本办法自 2019 年 7 月 10 日起施行。

4 小结

4 小结

◆风险隐患严重

1.网络边界管理混乱

- 收费专网终端配置双网卡、配备USB无线网卡，使收费专网与互联网混搭运行;
- 视频监控网与收费专网共用同一台核心交换机，且无边界防护措施，破坏专网属性。

2.防火墙等基础安全设备策略缺乏

- 安全设备只采购部署、从未配置
- 访问策略为any to any的“透明防火墙”
- 防火墙、入侵检测设备防病毒模块过期

3.大量主机终端缺乏病毒防护和终端管控

- 收费终端存在大量木马病毒
- 联网收费系统办公终端存在移动存储介质违规使用情况
- 未遵循最小化安装原则，在各类终端上安装无关软件

4.存在重大风险隐患

- 发现存在由互联网渗透入侵收费专网核心系统的重大风险隐患。
- 发现存在核心业务数据和个人信息泄露的重大安全隐患。
- 联网收费相关管理类系统普遍存在高风险安全隐患。

4 小结

◆网络安全管理粗放

1.网络安全底数不清

- 网络拓扑图与现状差别较大。
- 两清单报送不全，描述不清，责任主体不明。

2.日常安全管理不严。

- 大量终端及系统存在弱口令
- 联网收费系统终端U盘乱用
- 收费终端违规外联
- 不同业务混用网络设备
- 省部链路缺少备份冗余
- 核心交换机单机部署

3.安全要求落实不力

- 等级保护基本制度落实不到位，定级备案滞后、测评工作不到位、定级不准、不定级
- 设计和开发不合规，“先天性隐患”突出，后期整改难度极大
- 整体上“专网不专”“带病运行”问题十分突出

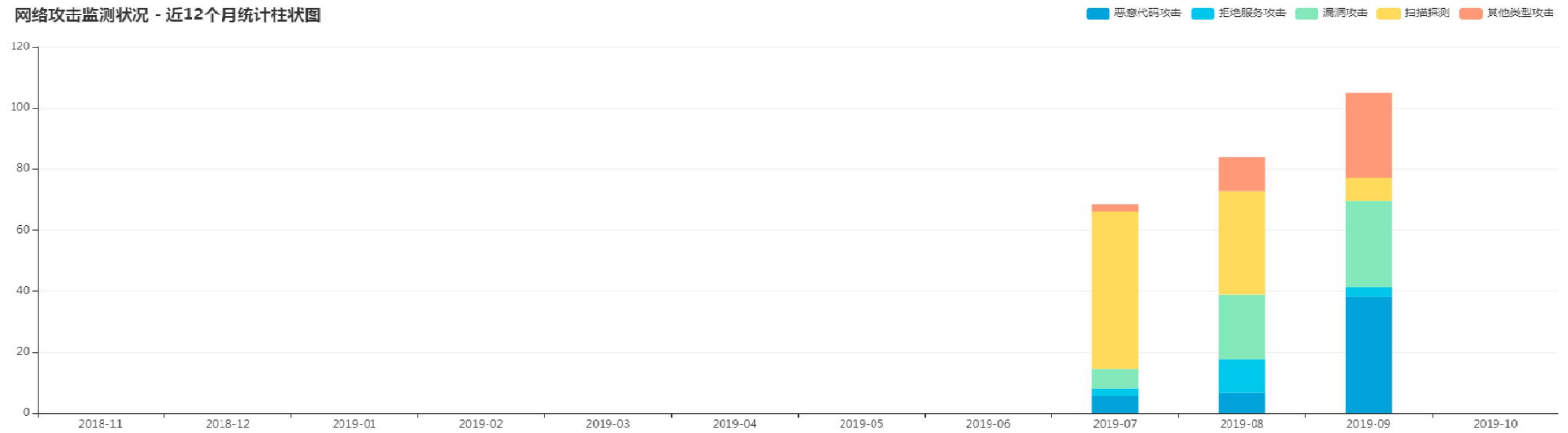
4 小结

◆工程安全设计存在差距

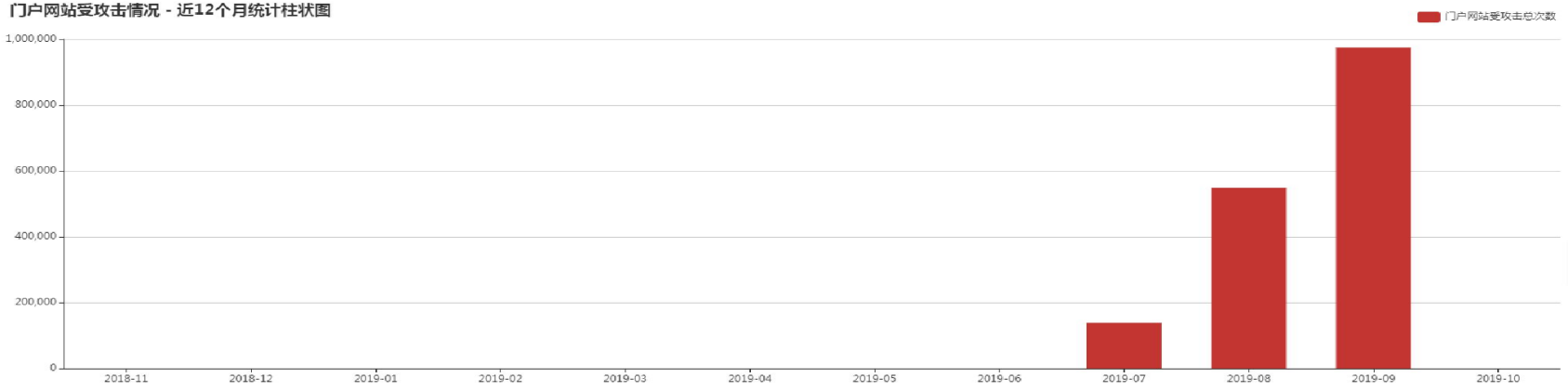
- 安全设计基础不扎实
- 边界防护设计缺失
- 数据保护措施亟待完善
- 密码应用系统建设方案缺失
- 关键设备未冗余部署
- 备份恢复措施缺失
- 配套工作支撑不足
- 标准引用不规范

4 小结

网络攻击监测状况 - 近12个月统计柱状图



门户网站受攻击情况 - 近12个月统计柱状图



4 小结

原因分析：

一是安全意识淡薄

不少单位领导不重视网络安全，对网络安全存在模糊认识和错误认识。对安全管理敷衍了事、对运维保障漠不关心，没有将设计、建设、运维安全整体考虑、融会贯通。

二是责任落实不到位

- 安全责任体系缺失，履行党委（党组）网络安全责任制不到位
- 省联网中心和收费公路经营单位的安全建设和运维主体责任落实不力
- 对外包及第三方服务单位普遍缺乏有效管控
- 全网1900多个系统不能确保有效落实各方责任

4 小结

三是管理制度不落地

- 对网络安全法规和制度标准不了解、不掌握
- 建设安全质量把关不严，未落实同步规划、同步建设、同步使用的要求
- 运维要求约束宽泛，缺乏细化、可操作的建设、运行管理制度和安全运维操作规程
- 有规定不执行，有要求不落实
- 风险漏洞管理松散，漏洞迟改、漏改、未改

四是安全运维水平较低

- 看摊不负责，甩手不管理。过度依赖外部第三方服务单位，缺乏对供应链单位的管控
- 只装大门不上锁：运维不规范，专网隔离不严，网络权限控制不严，进入专网后“内网漫游、为所欲为”
- 不统筹不协调，运维主体较为分散，难以形成全网安全保障的合力

4 小结

取消省界站后，全国 “一张网”运行，全网面临严峻安全挑战。

- 全网安全一体化、局部风险全局化
- 全网面临“由上至下、由下至上”的纵向风险和跨省跨区域跨路段的横向风险
- 任何一个系统或终端都是全网的风险点

4 小结

安全类	控制点	相关制度或规定	相关表单
安全管理制度	管理制度	《网络安全方针和策略》	
	制定和发布	《网络安全制度文件控制管理规定》	网络安全管理制度文件清单
	评审和修订		
安全管理机构	岗位设置	《网络安全组织机构及职责》 《信息系统安全检查管理规定》 《信息安全授权和审批管理办法》	相关专家和单位联系表
	人员配备		
	授权和审批		
	沟通和合作		
	审核和检查		
安全管理人员	人员录用	《安全管理人员》	保密协议 岗位安全协议 人员培训及考核记录 网络安全岗位职责说明书
	人员离岗		
	安全教育意识和培训		
	外部人员访问管理		
安全建设管理	定级和备案	《安全建设管理规定》	
	安全方案设计		
	产品采购和使用		
	自行软件开发		
	外包软件开发		
	工程实施		
	测试验收		
	系统交付		
	登记测评		
	服务供应商选择		

4 小结

安全类	控制点	相关制度或规定	相关表单
安全运维管理	环境管理	《机房安全管理规定》 《办公环境安全管理制度》	基础设施检测检修记录 机房设备进出登记表 机房出入登记表
	资产管理	《资产安全管理制度》	资产清单 设备清单 IP地址使用表
	介质管理	《介质安全管理制度》	介质使用记录
	设备维护管理	《设备维护管理制度》	设备维护记录单
	漏洞和风险管理	《漏洞和风险管理制度》	
	网络和系统安全管理	《网络和系统安全管理制度》	日常监控记录表
	恶意代码防范管理制度	《恶意代码防范管理制度》	
	配置管理	《配置管理规范》	配置清单
	密码管理	《账号管理制度》 《密码管理制度》	账户申请单
	变更管理	《系统变更管理制度》	应用系统上线/变更申请表 系统变更申请表 变更实施记录 变更验收记录
	备份与恢复管理	《信息备份与恢复管理制度》	信息备份识别清单 信息备份计划 数据恢复记录
	安全事件处置	《网络安全事件管理规范》	事件处理记录
	应急预案管理	《信息系统应急预案管理》	
	外包运维管理	《外包运维管理规范》	施工或运维工作人员名单

感谢聆听！