

# 《电力行业信息系统安全等级保护基本要求》释义

(管理类信息系统分册)

国家能源局 编著



电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>

# 《电力行业信息系统安全 等级保护基本要求》释义

(管理类信息系统分册)

国家能源局 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

## 内 容 简 介

《电力行业信息系统安全等级保护基本要求》是电力行业开展信息安全等级保护工作的基础性依据文件之一，本书是对它的权威解读，主要介绍了国家信息安全等级保护政策和标准、行业信息安全规范性文件、行业信息安全等级保护主要工作和各级信息系统等级保护基本要求释义。

本书为电力行业信息安全相关部门和电力信息系统管理、运维、开发、建设和外包服务等各类人员从事相关工作提供了重要参考，有助于相关人员理解和使用，是从事信息安全工作的不可多得的学习资料。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有，侵权必究。

## 图书在版编目 (CIP) 数据

《电力行业信息系统安全等级保护基本要求》释义.管理类信息系统分册 /国家能源局编著. —北京: 电子工业出版社, 2014.4

ISBN 978-7-121-22788-2

I. ①电… II. ①国… III. ①电力系统—信息安全—安全法规—法律解释—中国—职业培训—教材 IV.①D922.292.5

中国版本图书馆 CIP 数据核字 (2014) 第 062699 号

策划编辑: 杨 波

责任编辑: 杨 波

印 刷: 北京京师印务有限公司

装 订: 北京京师印务有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本: 787×1 092 1/16 印张: 12.5 字数: 320 千字

印 次: 2014 年 4 月第 1 次印刷

定 价: 38.00 元

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 zllts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线: (010) 88258888。



## 序

电力是关系国计民生的重要基础产业，也是关系千家万户的公用事业。电力安全可靠供应事关经济发展、人民生活和社会稳定，保障电力系统安全是国家安全的重要组成部分。现代电力工业具有高度网络化、系统化、自动化的特征，以网络、数据库及计算机自动控制技术为代表的信息处理技术已成为支撑电力生产控制和经营管理不可或缺的基础要素，保障电力网络与信息系统安全已成为电力系统安全稳定运行的重要前提。

同时，各国尤其是大国之间，在网络空间的控制与反控制、渗透与反渗透的斗争更加激烈，维护网络空间安全、保障国家重要基础设施安全已经成为国家战略的制高点。近年来发生的“震网”和“棱镜门”事件表明，某些西方大国为维持其全球霸权，一直在利用信息的原发优势，不断加强对其他国家网络空间的渗透、控制和破坏，对这些国家的政治、经济、军事安全构成了严重威胁。我国在网络空间方面，由于核心技术尚未完全掌握、关键设备大多从国外进口、国产水平较低、信息安全基础薄弱，维护网络空间安全，保障电力等国家关键基础设施和信息系统的的核心安全，实现信息安全“能控、在控、可控”的任务非常艰巨。

信息安全等级保护制度是我国在信息安全领域的一项基本制度。2003年，中央办公厅、国务院办公厅印发了《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号），明确要求重点保护国家基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统安全，抓紧建立信息安全等级保护制度。我国先后制定出台了《信息安全等级保护管理办法》及《信息系统安全等级保护基本要求》等一系列等级保护规范性文件 and 标准，有力促进了等级保护工作。公安部于2009年印发了《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安〔2009〕1429号），明确指出国家重点行业信息系统主管部门可以按照《信息系统安全等级保护

基本要求》等国家标准，在不低于等级保护基本要求的情况下，结合系统安全保护的特殊需求，制定行业标准、规范性文件或细则，指导本行业信息系统安全等级保护建设整改工作。

电力行业素有安全重于泰山的优良传统，经过多年的努力，逐步形成了具有行业特点比较完善的信息安全防护体系。在信息安全等级保护工作方面，率先在行业内全面贯彻落实国家信息安全等级保护制度并取得了良好成效。为结合行业实际，更好地贯彻落实国家基本要求，原电监会印发了《电力行业信息系统安全等级保护基本要求》（电监信息〔2012〕62号），经过几年的施行，有力促进了电力行业等级保护工作，保障了电力重要信息系统安全。

为做好《电力行业信息系统安全等级保护基本要求》的贯彻落实工作，国家能源局组织参与行业基本要求编制工作的有关专家，编写了这本释义。本书对《电力行业信息系统安全等级保护基本要求》的主要内容做了全面、详细、准确的诠释，是行业信息安全等级保护测评人员、信息系统建设和运行管理等人员准确把握行业基本要求的重要参考资料。我相信，这本释义的出版发行，将对落实电力行业信息安全等级保护制度、保障电力重要信息系统安全、维护国家安全，起到积极的促进作用。

史 2. 波

2014年3月18日

## 前 言

为贯彻落实国家信息安全等级保护制度，按照公安部《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安〔2009〕1429号）要求，结合行业信息系统特点和工作实践，依据《信息系统安全等级保护基本要求》、《电力行业网络与信息安全监督管理暂行规定》、《电力二次系统安全防护规定》等，原电监会信息中心（现国家能源局信息中心）组织编制了《电力行业信息系统安全等级保护基本要求》（电监信息〔2012〕62号），并于2012年11月正式印发施行，得到了行业内外广泛好评，有力促进了行业信息安全等级保护工作。

为进一步促进信息安全从业人员对规范性文件的理解，在国家能源局电力安全监管司的指导下，国家能源局信息中心组织电力行业信息安全等级保护测评中心各测评实验室（北京华电卓识信息安全测评技术中心有限公司——第一测评实验室，中国电力科学研究院——第二测评实验室，南京南瑞集团公司/国网电力科学研究院——第三测评实验室）编写了《〈电力行业信息系统安全等级保护基本要求〉释义（管理类信息系统分册）》和《〈电力行业信息系统安全等级保护基本要求〉释义（生产控制类信息系统分册）》，旨在促进电力行业信息安全相关部门和电力信息系统管理、运维、开发、建设和外包服务等各类人员更好地理解行业基本要求中的内容，同时规范测评机构对于电力信息系统的等级测评行为，规避因不熟悉电力信息系统测评工作而引发的测评次生风险。管理类信息系统分册主要介绍了国内信息安全相关政策标准、电力行业信息安全政策、电力行业信息安全等级保护工作和管理类信息系统不同级别安全保护基本要求释义。生产控制类信息系统分册将后续出版。

本书在编著过程中，得到了公安部网络安全保卫局、公安部信息安全等级保护评估中心、国家信息技术安全研究中心、中国信息安全测评中心、中国金融电子化公司测评中心、教育信息安全等级保护测评中心、中国人民解放军信息安全测评认证中心和行业内相关领导及专家的指导和帮助，在此一并表示衷心感谢。

编委会

2014年3月

# 《电力行业信息系统安全等级保护基本要求》释义

## (管理类信息系统分册)

### 编 委 会

- 主 编** 杨 昆 国家能源局总工程师
- 副 主 编** 韩 水 国家能源局电力安全监管司司长  
孙耀唯 国家能源局信息中心主任
- 执行副主编** 苑 舜 国家能源局电力安全监管司副司长  
胡红升 国家能源局信息中心副主任  
王继业 中国电力科学研究院副院长  
张 强 南瑞集团公司副总工程师  
王英彬 北京华电卓识信息安全技术测评中心  
有限公司董事长

#### 编写人员(排名不分先后)

温红子 许海铭 高昆仑 王泽宁 陈雪鸿 张 翎  
朱世顺 刘 韧 李 凌 毛 澍 刘 行 高艳坤  
郑晓崑 董 珏 赖宝亮 詹 雄 陈 刚 韩 震  
周 亮 朱晓欢 马庆余 杨维永 唐汗青 林为民  
毕 超 李 鹏 蒋 铮 房 磊 陈 杰 刘文彬  
焦安春 王恩库 曹宇飞 张志伟 赵丽国 刘 寅



# 目 录

<b>第一章 信息安全等级保护制度介绍</b> .....	1
1.1 等级保护基本概念.....	1
1.2 等级保护政策体系.....	2
1.3 等级保护标准体系.....	4
<b>第二章 电力行业信息安全等级保护工作介绍</b> .....	7
2.1 电力行业网络与信息安全监管政策体系.....	7
2.2 电力信息系统安全等级保护定级备案.....	8
2.3 电力行业信息安全等级保护测评机构建设.....	11
2.4 电力信息系统安全等级保护测评试点.....	11
2.4.1 管理类信息系统安全等级保护测评试点.....	12
2.4.2 生产控制类信息系统安全等级保护测评试点.....	12
2.5 电力行业信息安全等级保护监督检查.....	12
<b>第三章 《电力行业信息系统安全等级保护基本要求》简介</b> .....	13
3.1 编制背景.....	13
3.2 主要内容与框架.....	14
3.3 与国标基本要求差异说明.....	14
3.4 基本要求安全层面简介.....	15
3.4.1 总体要求.....	15
3.4.2 物理安全.....	15
3.4.3 网络安全.....	16
3.4.4 主机安全.....	17
3.4.5 应用安全.....	17
3.4.6 数据安全及备份恢复.....	18

3.4.7	安全管理制度	18
3.4.8	安全管理机构	19
3.4.9	人员安全管理	19
3.4.10	系统建设管理	20
3.4.11	系统运维管理	21
<b>第四章 《电力行业信息系统安全等级保护基本要求》释义</b>		<b>22</b>
4.1	总体要求释义	22
4.1.1	总体技术要求	22
4.1.2	总体管理要求	23
4.2	第一级基本要求释义	24
4.2.1	物理安全	24
4.2.2	网络安全	26
4.2.3	主机安全	28
4.2.4	应用安全	30
4.2.5	数据安全及备份恢复	31
4.2.6	安全管理制度	32
4.2.7	安全管理机构	32
4.2.8	人员安全管理	33
4.2.9	系统建设管理	35
4.2.10	系统运维管理	39
4.3	第二级基本要求释义	42
4.3.1	物理安全	42
4.3.2	网络安全	46
4.3.3	主机安全	52
4.3.4	应用安全	58
4.3.5	数据安全及备份恢复	62
4.3.6	安全管理制度	62
4.3.7	安全管理机构	64
4.3.8	人员安全管理	66
4.3.9	系统建设管理	68
4.3.10	系统运维管理	73
4.4	第三级基本要求释义	81

4.4.1 物理安全	81
4.4.2 网络安全	88
4.4.3 主机安全	97
4.4.4 应用安全	105
4.4.5 数据安全及备份恢复	111
4.4.6 安全管理制度	112
4.4.7 安全管理机构	114
4.4.8 人员安全管理	118
4.4.9 系统建设管理	121
4.4.10 系统运维管理	129
<b>附录一 《电力行业信息系统安全等级保护基本要求》(管理类信息系统)</b>	<b>141</b>
第一部分 通用要求	142
1 适用范围	142
2 规范性引用文件	142
3 术语和定义	142
4 信息系统安全等级保护概述	143
第二部分 管理类信息系统要求	144
5 总体要求	144
6 第一级基本要求	145
7 第二级基本要求	152
8 第三级基本要求	167
<b>附录二 图、表索引</b>	<b>190</b>

# 第一章 信息安全等级保护制度介绍

## 1.1 等级保护基本概念

信息安全等级保护制度是我国信息安全的基本制度，也是当今发达国家保护关键信息基础设施和保障信息安全的通行做法。随着信息技术的广泛应用和信息化的快速发展，社会对信息化的依赖程度越来越高，网络和信息系统的安全问题愈加重要。为保障基础网络和重要信息系统安全，维护国家利益和社会秩序，2003年7月，国家信息化领导小组审议通过了《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号），提出了我国信息安全保障工作的总体纲领，并明确指出建立信息安全等级保护制度是我国信息安全工作的一项基本要求。2007年，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合印发了《信息安全等级保护管理办法》（公通字〔2007〕43号），具体规范了信息安全等级保护管理的各个方面。2009年，公安部印发了《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安〔2009〕1429号），提出了信息系统安全等级保护建设工作的时间进度安排。2010年，公安部印发《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安〔2010〕303号），推动了信息安全等级保护测评工作的有序开展。2012年，国务院发布了《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号），提出以信息安全等级保护为基础性工作的国家信息安全保障体系，对维护国家安全具有重大意义。

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应和处置。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。信息系统的安全保护等级分为以下五级：第一级为用户自主保护级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。第二级为系统审计保护级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩

序和公共利益造成损害，但不损害国家安全。第三级为安全标记保护级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。第四级为结构化保护级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。第五级为访问验证保护级，信息系统受到破坏后，会对国家安全造成特别严重的损害。

信息系统等级保护工作主要分为定级、备案、建设整改、等级测评和监督检查五个环节。

**定级工作：**对信息系统进行定级是等级保护工作的基础，定级工作的流程是确定定级对象、确定信息系统安全保护等级、组织专家评审、主管部门审批、公安机关审核。

**备案工作：**信息系统定级以后，应到所在地区的市级以上公安机关办理备案手续，备案工作的流程是信息系统备案、受理、审核和备案信息管理等。

**建设整改工作：**信息系统安全等级定级以后，应根据相应等级的安全要求，开展信息系统安全建设整改工作：对于新建系统，在规划设计时应确定信息系统安全保护等级要求，按照等级要求，同步规划、同步设计、同步实施安全保护技术措施；对于在用系统，可以采取“分区、分域”的方法，按照“整体保护”原则进行整改方案设计，对信息系统进行加固改造。

**等级测评工作：**信息系统安全等级保护测评工作是指测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对未涉及国家秘密的信息系统安全等级保护状况进行检测评估的活动。等级测评过程可以分为四个活动：测评准备、方案编制、现场测评与分析、报告编制，常用的测评方法是访谈、检查和测试。

**监督检查工作：**公安机关依据有关规定，会同行业主管部门对非涉密重要信息系统运营使用单位等级保护工作开展和落实情况进行检查，监督、检查其建设安全设施、落实安全措施、建立并落实安全管理制度、落实安全责任、落实责任部门和人员。

## 1.2 等级保护政策体系

近年来，为组织开展信息安全等级保护工作，国家相关部委相继出台了一系列文件，对具体工作提供了指导意见和规范，这些文件构成了信息安全等级保护政策体系，如图 1-1 所示。

《中华人民共和国计算机信息系统安全保护条例》和《国家信息化领导小组关于加强信息安全保障工作的意见》是开展信息安全保护工作的源头文件。前者是国务院于 1994 年发布的第 147 号令，明确规定了“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。后者明确指出：“实

行信息安全等级保护。要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

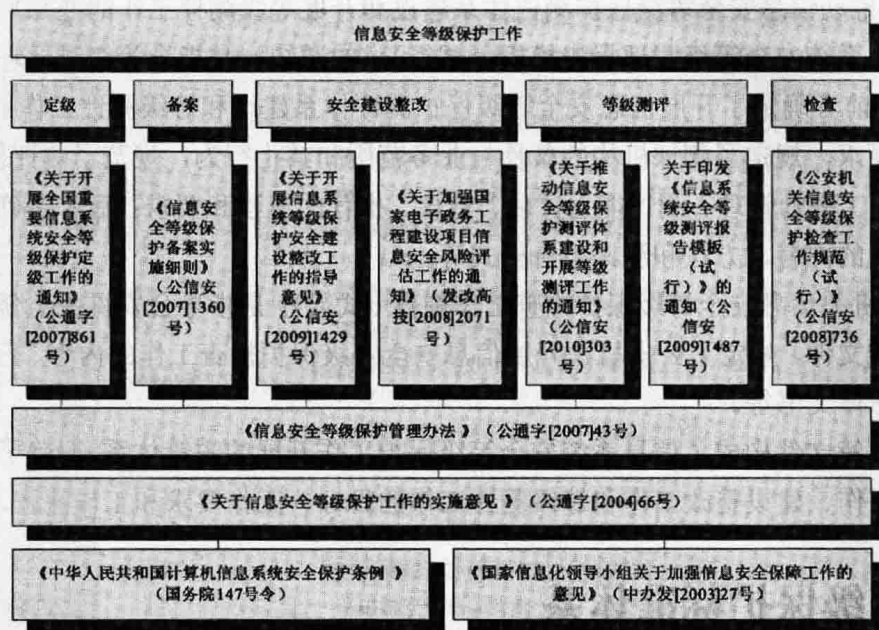


图 1-1 信息安全等级保护政策体系

《关于信息安全等级保护工作的实施意见》是开展等级保护工作的政策指导性文件，明确了开展等级保护工作的重要意义，规范了等级保护工作的基本内容、工作要求和实施计划以及各部门职责分工等。

《信息安全等级保护管理办法》是开展等级保护工作的政策性文件，明确了信息安全等级保护制度的基本内容、流程及工作要求，规范了信息系统定级、备案、安全建设整改和等级测评的实施与管理、信息安全产品和测评机构选择等。

《关于开展全国重要信息系统安全等级保护定级工作的通知》是组织开展全国重要信息系统安全等级保护定级工作的政策文件，标志着全国信息安全等级保护工作的正式启动。通过定级工作摸清了信息系统的底数，找到了系统等级保护的重点，奠定了等级保护后续工作的基础。

《信息安全等级保护备案实施细则》是规范备案环节工作的政策文件，该文件规定了公安机关受理信息系统运营使用单位信息系统备案工作的内容、流程、审核等，可用于指导各级公安机关受理信息系统备案工作。

《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》是指导安全建设整改环节工作的政策文件，提出了已定级信息系统开展安全建设整改工作的目标、内容、流程和要求等。

《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》规范了涉密和非涉密国家电子政务项目按照不同的政策标准规范开展信息安全风险评估工作的各个方面。

《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》和《关于印发〈信息系统安全等级测评报告模板（试行）〉的通知》是指导等级测评环节工作的政策文件。前者确定了开展信息安全等级保护测评体系建设和等级测评工作的目标、内容和工作要求，规定了测评机构的条件、业务范围和禁止行为，规范了测评机构申请、受理、测评工程师管理、测评能力评估、审核、推荐的流程和要求；后者明确了等级保护测评活动的内容、方法和测评报告格式等。

《公安机关信息安全等级保护检查工作规范（试行）》是指导公安机关监督检查环节工作的政策文件，规定了公安机关开展信息安全等级保护检查工作的内容、程序、方式以及相关法律文书等。

以上政策文件构成了信息系统安全等级保护工作开展的政策体系，明确了组织开展等级保护工作、建设整改工作和等级测评工作的目标、工作要求和工作流程。

### 1.3 等级保护标准体系

为推动我国信息安全等级保护工作，全国信息安全标准化技术委员会和公安部信息安全标准化技术委员会组织制定了信息安全等级保护工作需要的一系列标准，为开展等级保护工作提供了标准保障。这些标准可以分为基础类、应用类、产品类和其他类，这些标准与等级保护工作之间的关系如图 1-2 所示。

标准类型	子类型	标准名称
基础类	//	计算机信息系统安全保护等级划分准则 (GB 17859—1999)
应用类	信息系统定级	信息系统安全保护等级定级指南 (GB/T 22240—2008)
	等级保护实施	信息系统安全等级保护实施指南 (GB/T 25058—2010)
		信息系统安全等级保护基本要求 (GB/T 22239—2008)
	信息系统安全建设	信息系统通用安全技术要求 (GB/T 20271—2006)
		信息系统等级保护安全设计技术要求 (GB/T 24856—2009)
		信息系统安全管理要求 (GB/T 20269—2006)
		信息系统安全工程管理要求 (GB/T 20282—2006)
		信息系统物理安全技术要求 (GB/T 21052—2007)
		网络基础安全技术要求 (GB/T 20270—2006)
		信息系统安全等级保护体系框架 (GA/T 708—2007)
		信息系统安全等级保护基本模型 (GA/T 709—2007)
		信息系统安全等级保护基本配置 (GA/T 710—2007)
		信息系统安全等级保护测评要求 (GB/T 28448—2012)
	等级测评	信息系统安全等级保护测评过程指南 (GB/T 28449—2012)
	信息系统安全管理测评 (GA/T 713—2007)	

图 1-2 等级保护标准体系与等级保护工作关系图

标准类型	子类型	标准名称
产品类	操作系统	操作系统安全技术要求 (GB/T 20272—2006)
		操作系统安全评估准则 (GB/T 20008—2005)
	数据库	数据库管理系统安全技术要求 (GB/T 20273—2006)
		数据库管理系统安全评估准则 (GB/T 20009—2005)
	网络	网络端设备隔离部件技术要求 (GB/T 20279—2006)
		网络端设备隔离部件测试评价方法 (GB/T 20277—2006)
		网络脆弱性扫描产品技术要求 (GB/T 20278—2006)
		网络脆弱性扫描产品测试评价方法 (GB/T 20280—2006)
		网络交换机安全技术要求 (GA/T 684—2007)
		虚拟专用网安全技术要求 (GA/T 686—2007)
	PKI	公钥基础设施安全技术要求 (GA/T 687—2007)
		PKI 系统安全等级保护技术要求 (GB/T 21053—2007)
	网关	网关安全技术要求 (GA/T 681—2007)
	服务器	服务器安全技术要求 (GB/T 21028—2007)
	入侵检测	入侵检测系统技术要求和检测方法 (GB/T 20275—2006)
		计算机网络入侵分级要求 (GA/T 700—2007)
	防火墙	防火墙安全技术要求 (GA/T 683—2007)
		防火墙技术要求和测评方法 (GB/T 20281—2006)
		包过滤防火墙评估准则 (GB/T 20010—2005)
	路由器	路由器安全技术要求 (GB/T 18018—2007)
		路由器安全评估准则 (GB/T 20011—2005)
		路由器安全测评要求 (GA/T 682—2007)
	交换机	网络交换机安全技术要求 (GB/T 21050—2007)
		交换机安全测评要求 (GA/T 685—2007)
	其他产品	终端计算机系统安全等级技术要求 (GA/T 671—2006)
		终端计算机系统测评方法 (GA/T 671—2006)
		审计产品技术要求和测评方法 (GB/T 20945—2006)
虹膜特征识别技术要求 (GB/T 20979—2007)		
虚拟专网安全技术要求 (GA/T 686—2007)		
应用软件系统安全等级保护通用技术指南 (GA/T 711—2007)		
应用软件系统安全等级保护通用测试指南 (GA/T 712—2007)		
其他类	风险评估	信息安全风险评估规范 (GB/T 20984—2007)
		信息安全事件管理指南 (GB/Z20985—2007)
	事件管理	信息安全事件分类分级指南 (GB/Z20986—2007)
		信息系统灾难恢复规范 (GB/T 20988—2007)

图 1-2 等级保护标准体系与等级保护工作关系图 (续)

《计算机信息系统安全保护等级划分准则》是强制性国家标准，是等级保护标准系列的基础。

《信息系统安全等级保护基本要求》是在《计算机信息系统安全保护等级划分准则》以及各技术类标准、管理类标准和产品类标准基础上制定的，给出了各级信息系统应当具备的安全防护能力，并从技术和管理两个方面提出了相应的措施，是信息系统进行建设整改的安全需求。

《信息系统安全等级保护定级指南》规定了定级的依据、对象、流程和方法以及等

级变更等内容，同各行业发布的定级实施细则共同用于指导开展信息系统定级工作。

《信息系统安全等级保护实施指南》和《信息系统等级保护安全设计技术要求》构成了指导信息系统安全建设整改的方法指导类标准。前者阐述了在系统建设、运维和废止等各个生命周期阶段中如何按照信息安全等级保护政策、标准要求实施等级保护工作；后者提出了信息系统等级保护安全设计的技术要求，包括安全计算环境、安全区域边界、安全通信网络、安全管理中心等各方面的要求。

《信息系统安全等级保护测评要求》和《信息系统安全等级保护测评过程指南》构成了指导开展等级测评的标准规范。前者阐述了等级测评的原则、测评内容、测评强度、单元测评、整体测评、测评结论的产生方法等内容；后者阐述了信息系统等级测评的过程，包括测评准备、方案编制、现场测评、分析与报告编制等各个活动的工作任务、分析方法和工作结果等。

以上各标准构成了信息系统安全等级保护标准体系，为推动和开展等级保护五个环节的工作提供了强有力的支撑。

## 第二章 电力行业信息安全等级保护 工作介绍

现代电力生产具有高度信息化、网络化的特征，信息技术应用广泛，信息安全问题也得到及时密切的关注。2005年，原电监会印发《电力二次系统安全防护规定》（5号令），规范了电力二次系统安全防护工作。2007年至2012年，原电监会先后印发了《电力行业网络与信息安全监督管理暂行规定》（电监信息〔2007〕50号）、《电力行业信息系统安全等级保护定级工作指导意见》（电监信息〔2007〕44号）、《关于开展电力行业信息系统安全等级保护定级工作的通知》（电监信息〔2007〕34号）、《电力行业信息系统安全等级保护基本要求》（电监信息〔2012〕62号）等文件，全面推进信息安全等级保护建设工作，规范了电力行业信息安全等级保护定级、备案、建设整改、等级测评、督导检查、人才队伍建设等。

### 2.1 电力行业网络与信息安全监管政策体系

2006年，原国家网络与信息安全协调领导小组授权原国家电力监管委员会负责电力行业网络与信息安全监督管理工作。原国家电力监管委员会按照要求，整合力量，成立了电力行业网络与信息安全领导小组，领导小组下设办公室，设在电监会信息中心（现国家能源局信息中心）。2007年，原电监会信息中心对于行业网络与信息安全监管工作进行了深入研究，并根据“统一领导、分级负责，统筹规划、突出重点，整合资源、形成合力，以我为主、兼收并蓄”的原则，对电力行业网络与信息安全监督管理规章制度体系进行规划和设计，陆续印发了《电力行业网络与信息安全监督管理暂行规定》、《电力行业信息系统安全等级保护定级工作指导意见》、《电力行业网络与信息安全信息通报暂行办法》、《电力行业网络与信息安全应急预案》、《电力行业信息系统安全等级保护基本要求》等一系列文件，使等级保护、风险评估、信息通报、应急处置等工作走上了规范化、法制化的道路，实现了依法监管，如图2-1所示。

在电力行业网络与信息安全监管体系文件中，规范电力行业信息安全等级保护工作的文件有：