环境信息安全测试与评估技术规定

（征求意见稿）

编制说明

《环境信息安全测试与评估技术规定》编制组

二〇一〇年九月

目　　录

《环境信息安全测试与评估技术规定》编制说明

1 项目背景

1.1 任务来源

依据环信发[2009]11 号《关于确定“国家环境信息与统计能力项目”技术标准规范协作单位的通知》，根据国家发展改革委员会对“国家环境信息与统计能力项目”的批复要求，技术标准规范是其中五项建设之一。环境保护部项目办标准组组织方案比选和专家评议，最终确定各项技术标准规范的协作单位。其中，《环境信息安全测试与评估技术规定》的协作单位确定为北京神州绿盟科技有限公司（以下简称绿盟科技）。

1.2 工作过程

本次“国家环境信息与统计能力建设项目”信息化标准与技术规范/规定-《环境信息安全测试与评估技术规定》编制项目的具体工作内容如下：

1. 资料收集及业务调研工作，形成开题报告，并于 2010 年 3 月通过专家评审。
2. 标准的起草及修订工作
3. 标准的征求意见及改进修订
4. 标准的专家评审及改进修订
5. 标准（报批稿）的发布及培训
6. 标准（报批稿）发布或公布之日起， 6 个月的维护期

2 必要性分析

2.1 环境形势的变化对标准提出新的要求

随着环境保护工作的发展，在国家、省、城市三级正在逐步建立各类环保业务应用系统，环境监理信息系统覆盖了国家、省、城市三级相关的环境监理部门；环境保护建设项目管理系统正在建设国家级的系统，逐步扩展到省、城市、县三级环保管理部门；全国联网的排污费征收管理系统已建成并逐步应用在全国各级环境监察机构的排污申报登记、排污量核定、排污费征收等日常管理业务中；生物安全信息系统业已初步建成。部分省、城市的环境保护部门根据自身工作的需要，亦建设了一些覆盖本地区的环境保护业务应用系统。

各类业务信息化能力建设对信息标准化建设，特别是环境信息安全测试与评估技术规定建设提出了新的要求，本次工作正是在新形式的要求下开展进行的。

2.2 相关环保标准和环保工作的需要

环境保护信息安全标准的需求分为外部需求和内部需求。

从外部需求来看，环境保护信息系统作为国家经济可持续发展的重要系统，所运营使用的信息系统属于国家重要信息基础设施。环保信息系统所制定的信息安全制度，必须满足国家发布的一系列关于信息系统安全等级保护方面的制度、标准和规范的要求，必须参考国际相关信息安全标准规范的要求，内容应该涵盖信息安全所涉及的各个方面，包括人员、资产、

组织、信息系统等。

从内部需求来看，环保系统信息安全制度应满足以下三个要求：

●便于执行

由于环境保护信息系统从国家到省、地市等各级地方都有相应的机关，涉及的范围广，业务人员众多。因此，所设计的信息安全规范应充分考虑到各级业务人员的实际情况，便于在环境信息系统安全标准制定完善之后，相关业务人员参照执行。

●便于推广

由于环保系统的信息安全工作所涉及的信息系统数量较多，信息系统存在一定的差异性，因此所制定的信息安全规范应充分考虑到这一点，抽取和提炼信息系统的共性，兼顾信息系统的差异性，使制定出的信息安全标准能够便于推广使用，广泛适用于各级环境保护信息系统。

●便于更新和维护

制定环境保护系统信息安全标准是一个十分艰巨，而且工作量十分庞大的工程，所产生的制度相关文档的数量也很多，为了使信息安全制度能够跟上信息化发展的步伐，所制定的信息安全制度，必须经过优化，以便于后期的更新和维护。

2.3 标准的最新研究进展

环境信息安全标准应当与国家等级保护相关要求相结合，一方面适应国家等级保护工作的分级保护要求，另一方面评估环境保护系统自身的风险状况，加强安全制度与安全管理，形成有环保特色的安全体系。

环境信息安全的测试与评估工作需要遵循国家相关信息系统安全测评标准的要求，并结合环境信息能力建设项目的安全需求。

3 国内外相关标准情况的研究

3.1 主要国家、地区及国际组织相关标准情况的研究

信息化发展比较好的发达国家，特别是美国，非常重视国家信息安全的管理工作。美、俄、日等国家都已经或正在制订自己的信息安全发展战略和发展计划，确保信息安全沿着正确的方向发展。美国信息安全管理的最高权力是美国国土安全局，分担信息安全管理和执行的机构有美国国家安全局、美国联邦调查局、美国国防部等，主要是根据相应的方针和政策结合自己部门的情况实施信息安全保障工作。美国已经出台了电脑空间安全计划，旨在加强关键基础设施、计算机系统网络免受威胁的防御能力。日本信息技术战略本部及信息安全会议拟定了信息安全指导方针。俄罗斯批准了《国家信息安全构想》，明确了保护信息安全的措施。

美、俄、日均以法律的形式规定和规范信息安全工作，对有效实施安全措施提供了有力保证。美国通过了电子签名法案已经正式生效。美参议院通过了《互联网网络完备性及关键设备保护法案》。日本公布了旨在对付黑客的《信息网络安全可靠性基准》的补充修改方案。俄罗斯实施了关于网络信息安全的法律。

当前国际国内重要的信息安全测评的标准包括：DOD 准则、CC 通则、党政机关信息安全测评规范、密码设备评估准则等。

3.2 国内标准情况的研究

2003 年 9 月，中共中央办公厅、国务院办公厅转发《国家信息化领导小组关于加强国家信息安全保障工作的意见》（简称 27 号文）。27 号文对国家信息安全保障工作提出了具体的意见。

为进一步贯彻落实《国家信息化领导小组关于加强信息安全保障工作的意见》和公安部、国家保密局、国家密码管理局、国务院信息化工作办公室《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》精神，提高环保信息系统的信息安全保护能力和水平，维护国家安全、社会稳定和公共利益，保障和促进税收信息化建设工作的开展，环保系统安全信息化建设主要依据以下政策性文件。

- 《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》（公信安[2007]861 号）
- 《信息安全等级保护管理办法》（公通字[2007]43 号）
- 《信息安全技术 信息系统安全等级保护实施指南》（报批稿）
- 《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）
- 《信息安全技术 信息系统安全等级保护定级指南》（报批稿）
- 《信息安全技术 信息系统安全等级保护基本要求》（报批稿）
- 《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）
- 《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）

其中的相关信息安全测评的标准包括：

- 《信息系统安全保障等级评估准则-1-简介和一般模型》
- 《信息系统安全保障通用评估准则-2-技术准则》
- 《信息系统安全保障等级评估准则-3-管理准则》
- 《信息系统安全保障等级评估准则-4-工程准则》

4 编制的基本原则和技术路线

4.1 标准制修订的基本原则

标准性原则：规范的编制将依据国内或国际的相关标准进行；

规范性原则：制定标准规范工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制；

整体性原则：标准规范的制定需要考虑安全涉及的各个层面，不能够存在疏漏，也不能过于强调某一方面；

保密原则：环保信息系统的调研数据、标准规范文档等相关材料将被严格保密，未经授权不会泄漏给任何第三方单位或个人。

PDCA 方法：标准规范的制定将遵循调研、制定、评审、试用、再改进的方法循序渐进、逐步完善的方式进行。

4.2 制修订技术路线

绿盟科技针对标准制订工作绘制了详细的技术路线图，并且明确制定过程中的技术难

点及解决途径，具体内容如下表：

时间段	工作阶段	工作内容	技术难点	解决途径
2009.12 初	项目启动	由主管领导主持召开项目启动会，为项目实施顺利进行奠定基础。	已经完成	
2009.12-- 2010.3	调研	调研技术系统现状及管理体系现状，梳理技术需求及业务管理需求。 输出：《环境信息安全测试与评估技术规定开题报告》	取得完整、全面的系统安全现状。	充分与环境保护主管领导协作与沟通，与承担安全相关标准的其他各方共同进行调研工作。
2010.3— 2010.5	编制及修订	在需求确定之后，将进入编制和修订阶段。这一阶段将输出“征求意见稿”和“送审稿”。征求意见稿根据各方意见反复修订后，形成的送审稿将进入下一阶段。 输入：《环境信息安全测试与评估技术规定需求调研报告》 输出：《环境信息安全测试与评估技术规定（征求意见稿）》、《环境信息安全测试与评估技术规定（送审稿）》3	把握安全规范的核心思想，建设完备的安全规范内容。	与各方沟通规范内容，充分征求内部与外部专家的意见。
2010.5— 2010.9	评审及修订	在这一阶段，专家将就评审稿展开评审。评审后再根据专家意见进行修订，最终形成报批稿。 如有必要，评审可进行多次。 输入：《环境信息安全测试与评估技术规定（送审稿）》 输出：《环境信息安全测试与评估技术规定（报批稿）》	及时的修订规范的内容。	对专家意见深入理解并及时交流补充
2010.9-- 2010.11	试用及改进	安排标准规范的试运行。在一段时间的试运行后，再根据情况进行改进，最终完成审批过程。 输入：《环境信息安全测试与评估技术规定（报批稿）》 输出：《环境信息安全测试与评估技术规定》正式稿	依据实际情况进行改进	深入调研规范的试用情况，及时改进。
2010.11— 2010.12	发布及培训	发文件、召开会议予以正式发布，并安排全局的培训活		

		动，促进标准规范的落地。 输入：《环境信息安全测试与评估技术规定》正式稿		

5 主要内容

5.1 适用范围

本技术规定适用于“国家环境信息与统计能力项目”中对于环境信息安全进行安全测试与评估的活动。

5.2 结构框架

本规定共有 6 章和 2 个附录组成，主要内容如下：

第一章为适用范围：概述了本标准的适用范围。

第二章为术语和定义：列出了在本标准中出现的相关术语及其定义。

第三章为总则：对环境信息安全测试与评估的总体要求。

第四章为安全评估机构：为对环境信息系统进行安全测试与评估的安全评估机构的要求。

第五章安全评估的内容：提出了环境信息安全测试与评估应采取的方式和评估的内容规范，包括评估流程、技术与管理评估实施内容、技术测试、整改实施。

第六章为安全测试与评估实施：提出评估的主要环节和程序以及对安全评估活动的管理。

资料性附录 A 为环境信息安全检查表样例：提供了一个环境信息安全检查的检查表的样例。

资料性附录B以Windows安全审计和防火墙访问控制为例提供了相关的测试用例样本。

6 拟开展的主要工作

- 调研

  针对标准规范的技术需求、管理需求展开针对性的调研工作，这一阶段至关重要，将决定最终标准规范的方向和质量。

  调研阶段将输出调研及需求报告，为下一步标准规范的编制提供依据。

- 编制及修订

  在需求确定之后，将进入编制和修订阶段。这一阶段将输出“征求意见稿”和“送审稿”。征求意见稿根据各方意见反复修订后，形成的送审稿将进入下一阶段。

- 评审及修订

  在这一阶段，专家将就评审稿展开评审。评审后再根据专家意见进行修订，最终形成报批稿。

  如有必要，评审可进行多次。

- 试用及改进

报批稿完成后，可安排标准规范的试运行，运行期间，将安排一定范围的培训工作。在一段时间的试运行后，再根据情况进行改进，最终完成审批过程，将规范发布。

●发布及培训

标准规范正式发布时，应下发文件、召开会议予以正式发布。发布执行过程中，可安排全面的培训活动，促进标准规范的落地。

7 拟提交的工作成果

1. 《环境信息安全测试与评估技术规定》征求意见稿及编制说明
2. 《环境信息安全测试与评估技术规定》送审稿及编制说明
3. 《环境信息安全测试与评估技术规定》报批稿及编制说明
4. 《环境信息安全测试与评估技术规定》应用指南