附件三：

《环境信息系统安全技术规范》（征求意见稿）编制说明

《环境信息系统安全技术规范》编制组

二〇一二年三月

项目名称：环境信息系统安全技术规范

项目统一编号：1530.4

项目承担单位：环境保护部信息中心、北京神州绿盟科技有限公司

编制组主要成员：徐富春、付峥、刘定、白雷、陈煜欣、祝国鑫、韩季奇、程文静、孙宇、曹嘉、秦宇、谢斌、孙铁、王宝忱、王友强

标准所技术管理负责人：李晓倩、卢延娜

标准处项目负责人： 李晓弢

目　　录

《环境信息系统安全技术规范》编制说明

1项目背景

1.1 任务来源

本标准任务来源于国家环境保护标准制修订“十一五”计划，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。 于 2009 年 11 月启动，由环境保护部信息中心和北京神州绿盟科技有限公司共同承担。项目统一编号：1530.4。

1.2 工作过程

（1）国内外情况调研

标准任务下达后，标准承担单位成立了标准编制组，对国外标准化组织的安全标准及研究情况、国内安全标准的情况进行了调研。

在国际标准化组织 ISO/IEC 中安全管理标准已经形成一个完整的体系，并形成一个 27000 系列标准族，其中以建立信息安全管理体系为核心形成一套安全标准，其中几个主要的安全标准已经被采用为我国的国家标准。美、俄、日各国均以法律的形式规定和规范信息安全工作，形成完整的安全标准体系。

除了现有标准之外，国际上还开始研究业务连续性、计算机安全（Cyber security）、外包等领域内潜在的安全服务应用标准及指南的需求。

当前国家十分重视信息安全工作，由公安部负责制订了一系列的等级保护相关的安全标准，并逐步推进等级保护的相关工作，各部委、各行业均在结合国家标准的基础上制订行业信息安全规范与标准。

（2）标准开题论证会情况

编制组在前期调研的基础上形成了标准初稿及开题论证报告，2010 年 3 月 30 日，环保部科技标准司在环保部 209 会议室主持召开了标准开题论证会。会议听取了专家的意见，确定了标准的适用范围、制定技术路线，标准原名称为《环境信息安全技术规范》，建议名称修改为《环境信息系统安全技术规范》。

（3）标准征求意见稿编写工作

编制组根据标准开题论证会的专家意见，对《环境信息系统安全技术规范》标准初稿进行了修改，于 2010 年 9 月形成了标准征求意见稿及编制说明。

2标准制订的必要性分析

环境信息系统安全标准的制订是一项重要的工作，从以下几个方面对必要性进行分析：

（1）当前，国际上的信息安全技术与安全管理方面的标准已经非常成熟，国家的等级保护相关的信息安全标准已建成体系，各行业的安全标准也已经不断推出并在各行业信息安全工作中发挥着重要的作用，环境保护系统信息安全标准的制订工作应当是非常必要的。

（2）随着信息网络的开放，导致来自网络外部的威胁的不断增加，安全问题已经成为信息工作的一个重要方面，规范化的标准可以为环境信息安全工作提供有力的引导，且有利于各级环境部门确立信息安全目标，进而有效地开展各项信息安全工作。

（3）环境信息网络的覆盖范围广、结构复杂、安全需求多样，需要制订统一的规范性

的安全技术标准，以指导各级的环境信息部门建立安全系统、制订安全计划、防范安全事件。

（4）环境信息系统与网络的建设正在进行之中，环境网络、系统、应用都在不断发展，因此也面临着安全保护方面的课题。同时，环境信息系统更面临着需要保护的各类重要的环境信息。这些课题都需要环境保护系统尽快出台相关安全标准进行规范。

（5）信息系统安全建设所使用的安全技术与安全产品已经日趋多样化，在安全产品与安全防护措施的选择上，环境系统应当具有规范性安全防护要求以指导安全建设的具体执行。

环境保护信息安全标准方面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：

（1）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。

（2）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。

（3）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。

3标准编制的依据与原则

3.1 标准编制的依据

环境信息安全标准应当参照国标信息安全标准并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，另一方面参考国际上的最佳实践的做法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。

（1）国外相关标准情况

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。

国际信息安全管理已步入标准化与系统化管理时代。国际上负责信息安全相关标准研究和制定的是 ISO/IEC JTC1/SC27。SC27 设有 5 个工作组，其中 WG1 信息安全管理体系标准；WG2 安全技术和机制；WG3 安全评估；WG4 安全控制与服务；WG5 身份管理和隐私。

2005 年 SC27 正式启动了信息安全管理体系(ISMS)标准族的研制计划，即 ISO/IEC27000 系列标准。该系统标准对当时已有的几个内容重叠的信息安全管理标准进行了整合和改进。吸纳了与 ISMS 主题相关的其它信息安全管理标准项目。目前 ISO/IEC27001 和 ISO/IEC27002 这两个核心、基础标准已于 2005 年 10 月正式发布。用于指导 ISMS 审核认证机构工作的 ISO/IEC27006 也于 2007 年 3 月正式发布，其他诸如 ISO/IEC27000/27003/27004/27005 等支撑 ISO/IEC27001 实施的标准正在制定过程中，关于 ISMS 审核的标准，即 ISO/IEC27007 也开始了标准制定流程。

除了上述现有标准之外，国际上还开始研究业务连续性、计算机安全(Cyber security)、外包等领域内潜在的安全服务应用标准及指南的需求。

（2）国内安全标准相关资料

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，保障和促进环保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》

《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》

《信息安全技术 信息系统安全等级保护基本要求》

《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）

3.2 标准编制的原则

《环境信息系统安全技术规范》的制定遵循了以下原则：

（1）合规性原则：标准的编制将依据国内或国际的相关标准进行；

（2）规范性原则：标准制定项目中的过程和文档，具有很好的规范性，以便于项目的跟踪和控制；

（3）整体性原则：标准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；

（4）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。

（5）PDCA 方法：标准的制定将遵循调研、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标准主要技术内容

4.1 标准适用范围

本标准规定了环境信息系统安全的技术要求，提出环境信息系统安全架构、等级防护机制。

本标准适用于国家环境保护相关的各级、各类信息系统。

4.2 标准结构框架

本标准共有 12 章组成，主要内容如下：

（1）适用范围：概述了本标准的适用范围。

（2）规范性引用文件：列出本标准引用的相关标准文件。

（3）术语和定义：列出了在本标准中出现的相关术语及其定义。

（4）基本原则：给出了环境信息安全风险应对的基本原则。

（5）安全总体架构：包括环境信息系统安全目标、环境信息网络结构及环境信息系统安全保障体系的要求。

（6）环境系统等级防护机制：包括环境信息系统分类、环境信息和应用分类及信息分类防护措施。

（7）物理安全：为物理环境的技术安全要求。包括安全区域、设备安全、存储媒介的安全及通用控制措施、

（8）通信与运营安全：为通信与运营方面的技术安全要求。

（9）系统及网络的访问控制：为系统及网络的访问控制的技术安全要求。

（10）数据备份与恢复：为数据备份与恢复的技术安全要求。

（11）应用开发与维护的安全：为应用开发与维护方面的技术安全要求。

（12）应急响应与事件管理：为应急响应与事件管理的技术安全要求。

4.3 术语和定义

本规范中的术语和定义部分依据《GB/T 5271.8-2001 信息技术 词汇 第八部分 安全》由编制组给出的术语包括：1、可用性；2、机密性；3、信息保障；4、信息系统、5、信息系统安全；6、完整性；7、风险；8、安全域；9、威胁；10、脆弱性。

4.4 安全总体架构

环境信息系统安全的目标是通过建立统一的安全规范，从而建立信息安全保障的体系，以等级保护为指导划分安全等级，依据标准对信息系统的安全进行设计、建设、运行与维护。在总体架构中环境信息网络包括了国家、省、地市、县四级环境信息专网。

4.5 等级防护机制

依据等级保护的思想对环境信息系统进行划分，提出了环境信息系统的具体分类。规定环境保护核心业务应用系统分为环境监测管理信息系统、污染监控管理信息系统、生态保护管理信息系统、核安全与辐射管理信息系统、环境应急管理信息系统。

环境信息的分类分为公开信息和部门信息两类；环保系统的业务应用主要分为环保办公、公共服务等。

各级环境信息系统应当依据等级保护要求进行定级，各类环境信息应当依据规范要求进行保护。

4.6 物理安全

环境信息系统中的关键或敏感的网络与信息处理设施应被放置在安全区域内，由指定的安全边界予以保护。根据不同的安全需求等级，应划分不同的安全区域，例如：机房、办公区和第三方接入区。针对不同的安全区域，应采取不同等级的安全防护和访问控制措施，阻止非法访问、破坏和干扰。工程施工期间也应遵守相关规定，加强安全区域的保护。

应制订清理办公环境及合理使用计算机设备的规定。网络与信息处理设施的处置与转移

应遵守相应的安全要求。

本部分需要说明的是：

在 7.2 小节中保护网络与信息处理设备的安全是降低数据遭受非授权访问的风险和保护数据不受破坏及丢失的必要措施。

在 7.2.4 小节中工作区域外的设备可分为两类：一类是带离工作区域的信息处理设备，如笔记本电脑、测试仪表、移动硬盘等；另一类是固定在公共区域的设备，如监测基站、天线等。

安全区域是需要被保护的生产和办公场所，和放置网络与信息处理设施的物理区域。例如：办公室、机房等。

安全边界可以建立这种关卡的实物，例如：墙壁、门禁、接待处等。

在 7.4.1 小节中在不使用信息资产时，做好屏幕和桌面的清理工作，可以有效防止信息的未授权访问，是保护信息资产，防止其泄露、丢失、破坏的一种重要措施。例如：清理信息处理设施屏幕；清洁桌面的纸张文件和可移动存储媒介。

4.7 通信与运营安全

本部分规定了环境信息系统应建立网络与信息处理设施的管理和操作的职责及流程，并尽可能地实现职责分离。开发、调测和运营环境应保持相对隔离。应做好系统容量的监视和规划。配套安全系统应与业务系统“同步规划、同步建设、同步运行”。新建或扩容系统的审批应包含安全内容，并在交付使用前做好测试和验收工作。涉及安全方面的审批工作应由安全机构人员负责。应加强防范意识，采取有效措施，预防和控制恶意软件。应采取相应技术手段，确保时钟和时间同步。应建立严格的软件管理制度，及时加载安全补丁，定期进行系统安全漏洞评估，并执行系统加固解决方案。

本部分需要说明的是：

（1） 在 8.1.5 小节中开发、测试活动有可能造成严重的问题，例如：在运行系统中引入未经授权和测试的代码，软件与信息的修改，信息泄密等。

（2）在 8.2.4 小节中设备入网包含两层含义：一是某种型号的设备进入环境信息网络使用，二是新建或扩容的设备进入现网运行。应制定相应的管理办法并严格执行，严把入网关。

（3）在 8.6.6 小节中应制定系统安全测评制度，从系统功能、安全状况、业务表现等方面进行测评。测评的目的是检查网络与信息系统的安全运行情况与服务质量情况，主动发现网络与信息系统的安全隐患，做到早发现、早处理。

（4）在 8.7 节中网络面临的典型威胁包括：未经授权的访问，信息在传送过程中被截获、篡改，黑客攻击，滥用和误用等。这些威胁可能导致敏感信息泄露、信息不完整、信息不可用等后果。因此，必须制定一系列控制措施，确保网络中的数据安全，并保护连接服务，避免非法接入。

4.8 系统及网络的访问控制

本部分规定了环境信息系统应基于业务和安全需求，制定访问控制策略，并明确用户职责，加强用户访问控制管理。应加强对移动办公和远程办公的管理。应加强对网络系统、操作系统、应用系统的访问控制，如在网络边界设置合适的接口，采取有效的用户和设备验证机制，控制用户访问，隔离敏感信息。同时应监控对系统的访问和使用，记录并审查事件日志。

本部分需要说明的是：

在 9.2 小节中用户包括使用环保网络与信息系统的人，包括操作管理设备的内部人员或第三方，也包括享用服务的客户。

在 9.2.2 小节中特殊权限账户是指由特殊人员或特殊系统应用（进程）执行操作，完成某种特殊功能的账户。

在 9.2.2 小节中超级权限是指超越系统或应用的控制措施，高于普通用户拥有的特殊权限。超级权限使用不当是导致系统故障的主要因素之一。

在 9.4.2 小节逻辑安全区域是指具有相同安全保护需求、并相互信任的网络与信息系统组成的区域。例如：内部核心区、第三方接入区、互联网接入区（DMZ 区）等。安全域内部又可以分为安全子域。

在 9.4.5 小节中网络互联分为两大类：内部网络互联和内部与外部网络互联。内部互联指内部各类不同业务功能的网络间的互联；内部与外部网络互联指管理范畴内的网络与第三方的网络互联，包括其他企事业单位、合作伙伴、其它环境监测组织网络等。

4.9 数据备份与恢复

本部分规定了环境信息系统应当制定备份制度，执行备份策略，并定期演练数据恢复过程。记录操作和故障日志。应采取多种控制措施，保护网络设备及其上信息的安全，尤其是网络边界和与公共网络交换的信息。可采取的控制措施如：访问控制技术、加密技术、网管技术、安全设备、安全协议等。应制定信息存储介质的管理制度和处置流程。应特别加强对可移动存储介质和系统文档的管理。在与其他组织交换信息和软件时，应遵从相应的法律或合同规定，采取必要的控制措施。应制定相应的程序和标准，以保护传送过程中的信息和媒介安全，尤其要考虑门户网站、电子邮件等应用的安全控制需求。

4.10 应用开发与维护安全

本部分规定了新系统的开发的安全，包括网络基础设施、支撑系统，必须遵循系统安全生命周期管理流程。在开发新系统之前，应确认安全需求。在设计中应采用合适的控制措施、审计跟踪记录和活动日志，包括输入数据、内部处理和输出数据的验证。应用系统不应在程序或进程中固化账户和口令，系统应具备对口令猜测的防范机制和监控手段。应通过风险评估来确定加密策略，基于统一的标准和程序建立加密管理规范。在系统开发及维护过程中，应严格执行系统开发流程管理，包括对开发、测试和生产环境的变更控制，以保证系统软硬件和数据的安全。

4.11 应急响应与事件管理

本部分规定了环境信息系统应当贯彻“积极预防、及时发现、快速反应与确保恢复”的方针，建立安全事件响应流程和奖惩机制。如有必要，应尽快收集相关证据。应实施业务连续性管理，通过分析安全事件对业务系统的影响，制定并实施应急方案，并定期更新、维护和测试。

本部分需要说明的是：

安全事件是有可能损害资产安全属性（机密性、完整性、可用性）的任何活动。安全事件响应是针对已经发生或可能发生的安全事件进行监控、分析、协调、处理，保护资产安全属性的活动。

事件管理是指通过预防和恢复控制措施，确保关键业务不会因安全事件或自然灾害造成中断，或以最短的时间恢复业务运作的过程。

5对实施本标准的建议

实施《环境信息系统安全技术规范》，应当在统一部署下分阶段，分区域、有计划地进行实施。

（1）适当定级

按照《环境信息系统安全技术规范》标准的规定，各级各类环保信息系统应当确定等级保护的相应等级，并依据不同的等级要求进行信息安全建设的规划。

（2）明确差距

各信息系统应当通过实施信息安全测试与评估工作，发现现有的系统漏洞与安全问题，全面分析信息系统的等级差距，明确安全建设目标，确定安全工作思路与规划。

（3）分期建设

建议在环保系统的统一部署下，对现有安全问题采用分期、分批的处理原则，对于风险处置采取先高后低的原则，对于实施工作采取先易后难的方式，通过技术手段与管理制度相结合的方法，逐步完成信息安全体系建设。

（4）持续运维

信息安全不但需要一次性的建设，还需要长期性的运行维护，建议通过系统变更的安全控制，新上线系统安全验收，系统开发安全管理以及周期性的安全检查与审计，保障系统持续的安全运行。