**标准草案意见汇总处理表**

**标准项目名称**：《信息安全技术 信息系统安全等级保护 测评要求》

**又名：**《信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求》

承办人：陈广勇 共 26 页

**标准项目负责起草单位**：公安部信息安全等级保护评估中心 电 话：18601190322

| **序号** | **标 准**  **条文号** | **意　见　内　容** | **提出专家**  **/提出单位** | **处理意见** | **备　　注** |
| --- | --- | --- | --- | --- | --- |
| **一、标准草案第三稿，2016年5月23日，评估中心大会议室，2016年5月24日填写** | | | | | |
|  | 标准范围 | 标准范围应该包括内容范围和适用范围，标准适用的范围要描述清楚。 | 全国信息安全标准化技术委员会崔书昆 | 采纳：  在标准范围部分明确了本标准的适应范围。 |  |
|  | 全文 | 严格按照基本要求国家标准编制测评要求标准，确保测评指标与基本要求指标一致。 | 海关总署科技司安全运行处李宏图 | 采纳：  已根据最新版的基本要求国家标准进行了调整。 |  |
|  | 全文 | 将标准全文的“机密性”和“保密性”统一为一个。 | 国家能源局信息中心安全处陈雪鸿 | 采纳：  已统一为保密性。 |  |
|  | 全文 | 格式要符合GB/T 1.1-2009。 | 国家新闻出版广电总局监管中心张瑞芝 | 采纳：  已根据GB/T 1.1-2009进行了修改。 |  |
|  | 术语定义 | 术语定义要准确。 | 全国信息安全标准化技术委员会崔书昆 | 采纳：  已对术语定义进行了修改。 |  |
|  | 全文 | 调整结构，去除不符合标准编写要求的悬置段。 | 国家新闻出版广电总局监管中心张瑞芝 | 采纳：  已调整了全文中的悬置段。 |  |
|  | 标准范围 | 建议将“本标准适用于为……”改为“本标准适用于”。 | 信息产业信息安全测评中心刘 健 | 采纳：  已改为“本标准适用于”。 |  |
|  | 规范性引用文件 | 规范性引用文件要写上国标号。 | 信息产业信息安全测评中心刘 健 | 采纳：  已在规范性引用文件前加上国标号。 |  |
|  | 全文 | 标题号数字过于细分，目录太深，标号需要调整。 | 海关总署科技司安全运行处李宏图 | 采纳：  已对标准全文进行了调整。 |  |
|  | 全文 | 文章中出现的一些词：如关键、重要等一些词没有具体的定义。 | 通信研究院安全研究部副主任卜 哲 | 不采纳：  关键、重要等不适用放在术语定义中。 |  |
|  | 全文 | 建议添加英文缩略语章节，解释（如VPN）等专业缩略词。 | 中国农业银行范原辉 | 不采纳：  安全相关专有名词，不需要在本标准中再次说明。 |  |
|  | 4.1 | 4.1章节的测评框架说明，描述不通顺，需要修改。 | 全国信息安全标准化技术委员会崔书昆 | 采纳：  已对测评框架说明进行了调整。 |  |
|  | 全文 | 建议给出测评指标测评指标编码规则说明，便于阅读标准。 | 中国农业银行范原辉 | 采纳：  已在附录中给出编码规则说明。 |  |
|  | 全文 | 岗位名称（如安全主管）尽量符合一般单位通常的称谓。 | 通信研究院安全研究部副主任卜 哲 | 采纳：  已在标准中调整。 |  |
| **二、标准草案第四稿，2016年8月12日，北京瑞安宾馆第5会议室，2016年8月15日填写** | | | | | |
|  | 范围 | 第一页1.范围，“本标准规定了…..本标准适用于…...”，建议为“本部分…...” | 国家信息中心刘蓓 | 采纳：  原为：“本标准规定了…..本标准适用于…...”  改为：  “本部分规定了…..本部分适用于…...” |  |
|  | 术语和定义 | 安全等级保护测评的定义和方法放进术语里。 | 国家信息中心刘蓓 | 部分采纳：  改为：  定义放术语里，方法不适合放术语里。 |  |
|  | 全文 | “测评实施”中，如果测评实施项只有一项，不建议用1）。 | 国家信息技术安全研究中心李建 | 采纳：  改为：  全文修改。 |  |
|  | 全文 | 是否可以在标准中增加测评方法论，对测评范围、测评对象分析、测评对象覆盖的程度、整体安全评价和结果分析等。 | 中国信息安全认证中心李嵩 | 部分采纳：  已经增加测评方法，其他在过程指南中解决。 |  |
|  |  | 未对标准内容进行提出意见，建议测评报告模板后续跟着新标准变动。 | 李蒙 | 采纳：  测评报告模板后续跟着新标准变动。 |  |
|  | 规范性引用 | 规范性引用注明最新版适用于本标准，已经注明了最新版只需要引用到22239.1就够了。 | 樊华 | 采纳：  已经调整。 |  |
|  | 全文 | 身份鉴别测试实施方面，身份鉴别的保护机制是否要加入测试，例如是否在RSA的密码强度是否有要求，如256位和512位是否都满足。 | 樊华 | 不采纳：  密码强度各单位要求不一，不宜在标准中明确。 |  |
|  | 8.2.4.5 | 8.2.4.5章节，漏洞和风险管理中，漏洞和风险管理不止在运维方面，而是在信息系统全生命周期存在。在前面的内容中也应该考虑。 | 林值 | 采纳：  随基本要求修订 |  |
|  | 8.1.4 | 8.1.2.6和8.1.3.5中提到了恶意代码防范内容，8.1.4应用安全里也应该增加恶意代码防范内容。恶意代码只是一部分，建议增加其他的漏洞问题。 | 林值 | 采纳：  随基本要求修订 |  |
|  | 8.1.4 | 是否应该增加源代码检测和二进制代码检测。 | 林值 | 不采纳：  标准中已有源代码检测要求。 |  |
| **三、标准草案第四稿，截止2016年8月22日，WG5工作组成员单位征求意见，2016年8月23日填写** | | | | | |
|  | 前言和引言 | 前言和引言，内容有些交差，系列标准结构适合放在前言当中。引言重点写三要性和背景。 | 浙江蚂蚁小微金融服务集团有限公司 | 不采纳：  标准编制有规定格式要求，本标准满足相关要求。 |  |
|  | 术语和定义 | 3术语和定义应当按照GB1.1格式编写 | 浙江蚂蚁小微金融服务集团有限公司 | 采纳：  已经调整。 |  |
|  | 8.1.1.4.2 8.1.1.5.2 | 8.1.1.4.2 8.1.1.5.2等建议根据信息系统不同等级要求明确对应的防雷、耐火材料等方面的等级要求，使之符合分等级保护的思想。 | 浙江蚂蚁小微金融服务集团有限公司 | 不采纳：  防雷、耐火材料等属于基础设施建设相关范畴。 |  |
|  | 8.1.3.3、8.1.3.4 | 8.1.3.3、8.1.3.4等上述几个条款的测评对象应包含网络设备和安全设备 | 浙江蚂蚁小微金融服务集团有限公司 | 采纳：  已经调整。 |  |
|  | 附录B | 附录B应为规范性附录，严格规范 | 浙江蚂蚁小微金融服务集团有限公司 | 采纳：  修改为规范性附录 |  |
|  | 5.1.1.3.1 | 5.1.1.3.1防雷击，设备接地测评判定，建议检测接地电阻。比如：直接搭接的直流电阻不大于10mΩ。可参考电磁兼容性EMC标准。 | 南京中新赛克科技有限责任公司 | 不采纳：  机房或大楼建设有相关标准要求，建设完成后应有验收文档 ，这里采信验收文档即可。 |  |
|  | 6.1.1.7 | 6.1.1.7防静电，设备接地测评判定，同上。 | 南京中新赛克科技有限责任公司 | 不采纳：  机房建设有相关标准要求，建设完成后应有验收文档 ，这里采信验收文档即可。 |  |
|  | 6.2.3.3.2 | 6.2.3.3.2 （7.2.3.3.2、8.2.3.3.2）测评单元 c) 测评实施 1) 应访谈建设负责人，询问是否采用了密码产品，密码产品的采购和使用是否符合国家密码主管部门的要求。 建议修改为： 1）检查是否使用了密码产品；如使用，检查该密码产品是否获得有效的国家密码管理规定的密码产品型号证书。 | IBM | 采纳：  随基本要求变动进行修订。 |  |
|  | 6.2.4.9 | 6.2.4.9 （7.2.4.9、8.2.4.9）密码管理 a) 测评指标 应使用符合国家密码管理规定的密码技术和产品； c) 测评实施 1) 应访谈安全管理员，询问是否使用了密码产品，密码技术和产品的使用是否遵照国家密码管理规定。 建议修改为： 修改基本要求的相应部分并引用。  1）检查是否使用了密码产品；如使用，检查该密码产品是否获得有效的国家密码管理规定的密码产品型号证书。 2）检查网络安全产品中是否使用了密码模块；如使用，检查该密码模块是否具有国家密码管理规定的密码模块检测报告。 | IBM | 采纳：  随基本要求变动进行修订。 |  |
|  | 7.2.4.7 | 7.2.4.7 恶意代码防范管理，缺少相对应的对可信计算技术的管理要求。 | IBM | 采纳：  随基本要求变动进行修订。 |  |
|  | 8.2.4.7 | 8.2.4.7 恶意代码防范管理，在“基本要求”标准中，要求只能采用可信计算技术，而此处却只有查杀病毒方面的要求。 | IBM | 采纳：  随基本要求变动进行修订。 |  |
| **四、标准草案第四稿，截止2016年8月22日，等级测评机构反馈意见，2016年8月23日填写** | | | | | |
|  | 第4章 | 第4章中出现 “等级保护测评”、“安全等级保护测评”、“等级测评”名词，建议在第3章中明确其定义，并在全文使用中进行统一。 | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  全文调整。 |  |
|  | 4.2 | 第4.2节中第1段第1句话可理解为对“等级保护测评实施”的介绍或者解释，因此建议将“等级保护测评实施的基本方法是针对特定的测评对象……”修改为“等级保护测评实施是针对特定的测评对象……”，并将“……给出达到特定级别安全保护能力的评判”修改为“……给出是否达到特定级别安全保护能力的评判”。而且这段内容与4.1节内容有重叠，可以考虑合并。 | 电力行业信息安全等级保护测评中心第四实验室 | 部分采纳：  已做调整。 |  |
|  | 4.2  4.3 | 建议将4.2节和4.3节交换顺序，并将原4.2节中关于“单项测评”的相关内容合并到原4.3节中。 | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  已做调整，将4.2节和4.3节进行了合并。 |  |
|  | 7.1.2.4.2 | 第7.1.2.4.2节测评实施第1）条，建议修改为“应检查设备访问控制策略，访谈安全管理员每一条策略的用途，查看是否不存在多余或无效的访问控制策略”。 | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  已做调整。 |  |
|  | 7.1.3.2.4 | 第7.1.3.2.4节测评实施的第2）条，与测评指标无关，建议修改为“应检查管理用户权限是否为其工作任务所需的最小权限”。 | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  已做调整。 |  |
|  | 7.1.3.3.4 | 第7.1.3.3.4节测评实施中，建议不要列出测评对象“服务器操作系统和数据库管理系统”，与“b) 测评对象无法对应”，在理解上容易混淆。 | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  已做调整。 |  |
|  | 7.1.3.4.2 | 第7.1.3.4.2节测评实施中第2）条，建议修改为“应确认是否已关闭非必要的高危端口”。 | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  已做调整。 |  |
|  | 7.1.3.4.4 | 第7.1.3.4.4节测评实施中第1）条，建议修改为“应进行漏洞扫描，检查是否不存在高风险漏洞”。 | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  已做调整。 |  |
|  | 7.1.4.1.1 | 第7.1.4.1.1 节测评实施第5）条，建议修改为“应检查用户配置信息或访谈应用系统管理员，查看是否不存在空密码用户” | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  已做调整。 |  |
|  | 7.1.4.2.5 | 第7.1.4.2.5节测评实施第3）条，建议修改为“应测试用户是否不存在可越权访问情形”。 | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  已做调整。 |  |
|  | 10.1 | 第10.1节中“安全控制点测评是指对其所有要求项的符合程度进行分析和判定。”中“其”理解上容易有歧义，建议修改为“单个控制点中”。 | 电力行业信息安全等级保护测评中心第四实验室 | 采纳：  已做调整。 |  |
|  | 10.3  10.4 | 第10.3和10.4节中第2段内容均只给出了“如果经过综合分析单项测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失，该安全控制点的测评结论应调整为符合”的情况，那如果在安全控制点间和层面间分析时发现不能完全形成弥补效果，即相应控制点测评结论无法调整为符合时应该怎么处理？是否也应该在此说明？ | 电力行业信息安全等级保护测评中心第四实验室 | 不采纳：  “安全控制点、安全控制点间、层面间”测评是并列关系，有一个不符合则该控制点为不符合。 |  |
|  | 5.1.1 | 建议机房安全的测评对象可细化到机房内的对应设施。 | 江苏金盾杨超 | 不采纳：  标准粒度不宜过于细化 |  |
|  | 6.1.1.2.1 | 6.1.1.2.1 测评单元（L2-PES1-03）C）测评实施中1）和2）感觉内容上有重复，建议删掉一条，再增加一条对专人值守记录或机房人员进出记录验证的条款。 | 江苏金盾杨超 | 采纳：  已做调整。 |  |
|  | 6.1.1.2.2 | 6.1.1.2.2 测评单元（L2-PES1-04）c) 测评实施中 建议对监控记录进行细化，明确监控记录需包含哪些内容，如人员进出记录、视频监控记录等，如果这里包含了人员进出记录那么上面6.1.1.2.1一条建议就可不必修改。 | 江苏金盾杨超 | 不采纳：  具体监控内容由各单位自行定义，需针对不同对象分别设置，如厂商人员和检查人员的监控内容就不一样。 |  |
|  | 7.1.1.3.3 | 建议7.1.1.3.3 测评单元（L3-PES1-06）C）测评实施中增加监控视频可回放时间要求，如至少90天。 | 江苏金盾杨超 | 不采纳：  监控视频保存时间由各单位自行要求。 |  |
|  | 11.3 | 建议11.3中也注明测评结论是对整体测评之后单项测评结果的风险分析给出的。 | 江苏金盾杨超 | 不采纳：  测评流程中已明确，先进行整体测评，然后才能给出测评结论。 |  |
|  | 第9章 | 测评实施及单项判断中未明确一票否决项，即哪一分项不符合则该指标项直接判定为不符合。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  单项判定已明确哪些是必须要做到。 |  |
|  | 全文 | 网络设备“安全审计”部分归入“网络和通信安全”层面，但“身份鉴别”等层面确归入“设备与计算安全层面”，现场测评与结果记录如何明确？ | 江西神舟信息安全评估中心有限公司 | 不采纳：  本标准根据基本要求条款编制。 |  |
|  | 7.1.1.1.2 a) | 7.1.1.1.2 a)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。建议增加一个指标项：UPS电池间应采取承重加固。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  机房承重加固等属于基础设施建设相关范畴。 |  |
|  | 7.1.1.2.1 c) | 7.1.1.2.1 c）-2）应检查电子门禁系统是否可以鉴别、记录进入的人员信息。建议增加应检查门禁系统最长保存的记录时间，门禁系统记录数据是否保存3个月。 | 江西神舟信息安全评估中心有限公司 | 部分采纳：  增加应检查门禁系统记录数据的保存时间。具体保存时间各单位要求不一样，不做规定，或建议至少保存3个月。 |  |
|  | 7.1.1.3.1 c) | 7.1.1.3.1 c)-1）应检查机房内设备或主要部件是否固定；2）应检查机房内设备或主要部件上是否设置了明显且不易除去的标记。建议机房内设备或主要部件应明确包含通信线缆。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  标准中主要部件不宜一一列举。 |  |
|  | 7.1.1.3.2 c) | 7.1.1.3.2 c)-1) 应检查机房内通信线缆是否铺设在隐蔽处。建议调整，因为通信线缆除了可铺设在隐蔽处（地下或管道中），还应允许铺设在桥架中。 | 江西神舟信息安全评估中心有限公司 | 采纳：  调整为 应检查机房内通信线缆是否铺设在隐蔽处或桥架中。 |  |
|  | 7.1.1.3.3 a) | 7.1.1.3.3 a) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。建议改为“机房应设置视频监控系统，并设置防盗报警系统或安排专人值守”。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  修改建议变成了必须要求有视频监控系统，违背了标准原要求。 |  |
|  | 7.1.1.3.3 c) | 7.1.1.3.3 c)-2）应检查防盗报警系统或视频监控系统是否启用。建议明确监控记录保存时间。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  由其他标准规定。 |  |
|  | 7.1.1.5.3 c) | 7.1.1.5.3 c)-1）应访谈机房管理员是否进行了区域划分；建议增加细则要求，例如UPS电池应与重要设备一定要设置防火隔离措施。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  标准的7.1.1.5.3已做要求。 |  |
|  | 7.1.1.9.2 a) | 7.1.1.9.2 a) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；建议明确备用供电时间，例如2小时。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  备用供电时间与设备规模密切相关，各单位对断电事故的容忍度不一。 |  |
|  | 7.1.2.1.4 c) | 7.1.2.1.4 c)-1）应访谈网络管理员并查看网络拓扑图，检查重要网路区域不能部署在网络边界处且直接连接外部等级保护对象；建议将网路改为“网络”。 | 江西神舟信息安全评估中心有限公司 | 采纳：  已做调整。 |  |
|  | 7.1.2.3.2 a) | 7.1.2.3.2 a) 应能够对非授权设备私自联到内部网络的行为进行限制或检查；建议改为“应能够对非授权设备私自联到内部网络的行为进行检查和限制；” | 江西神舟信息安全评估中心有限公司 | 不采纳:  这是基本要求原条款要求。 |  |
|  | 7.1.2.3.3 a) | 7.1.2.3.3 a) 应能够对内部用户私自联到外部网络的行为进行限制或检查；建议改为“应能够对内部用户私自联到外部网络的行为进行检查和限制；” | 江西神舟信息安全评估中心有限公司 | 不采纳：  这是基本要求原条款要求。 |  |
|  | 7.1.2.8.1 b) | 7.1.2.8.1 b) 安全管理员和网络拓扑图。建议增加“安全管理系统” | 江西神舟信息安全评估中心有限公司 | 不采纳：  无法定义安全管理系统。 |  |
|  | 7.1.2.8.4 a) | 7.1.2.8.4 a) 应对分散在各个设备上的审计数据进行收集汇总和集中分析；建议明确审计数据保存时间。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  标准要求的是进行收集汇总和集中分析。 |  |
|  | 7.1.3.1.1 c) | 7.1.3.1.1 c)-4）应检查用户鉴别信息是否具有复杂度要求并定期更换。建议明确复杂度具体要求，如口令长度，数字、字母、字符组合；明确定期更换时间。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  口令复杂度不宜在标准中固定，需根据技术的发展而调整。 |  |
|  | 7.1.3.4.1a) | 7.1.3.4.1a) 应遵循最小安装的原则，仅安装需要的组件和应用程序。建议增加安装安全补丁。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  安全补丁在7.1.3.4.4部分已做要求。 |  |
|  | 7.1.3.5.1 c) | 7.1.3.5.1 c)-1）应查看防恶意代码工具的安装和使用情况，或查看是否采用可信计算技术建立从系统到应用的信任链；建议列举可信计算技术具体实现的方式。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  可信计算技术具体实现的方式不是本标准范围。 |  |
|  | 7.1.3.6 | 7.1.3.6 资源控制。建议增加一个测评指标：应根据安全策略设置登录终端的操作超时锁定。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  标准中已有相关要求。 |  |
|  | 7.1.4.1.1 c) | 7.1.4.1.1 c)-4）应检查鉴别信息是否具有复杂度要求并定期更换；建议明确口令复杂度要求和更换时间。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  口令复杂度不宜在标准中固定，需根据技术的发展而调整。 |  |
|  | 7.1.4.1.4 d) | 7.1.4.1.4 d) 如果 1）-2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。建议改为1）或2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。 | 江西神舟信息安全评估中心有限公司 | 采纳：  改为1）或2）为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。 |  |
|  | 7.1.4.3.4 a) | 7.1.4.3.4 a) 应对审计进程进行保护，防止未经授权的中断；应用系统通常无审计进程，建议改指标项删除。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  应用系统审计进程可以和系统进程在一起。 |  |
|  | 7.2.2.2.1c) | 7.2.2.2.1c）-1）应访谈信息安全主管，确认各岗位人员配备情况；建议明确人员配备最低的要求。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  人员配备最低要求由单位根据实际设置，标准要求有专职人员。 |  |
|  | 7.2.4.1 | 7.2.4.1环境管理。建议对环境管理的机房管理员应明确机房管理员的专业技能，特别是部分基础设施和设备的使用操作。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  标准中7.2.2.6和7.2.2.8对人员能力有要求。 |  |
|  | 7.2.4.1.1c) | 7.2.4.1.1c)-1）应访谈物理安全负责人，询问是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理、对基础设施（如空调、供配电设备、灭火设备等）进行定期维护，由何部门/何人负责；建议增加“查看机房基础设施的巡检记录”要求。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  测评实施最后一条已做要求。 |  |
|  | 7.2.4.2.2 a) | 7.2.4.2.2 a) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；资产的范围太广泛，此处应重点强调信息系统相关的资产（含实体设备、信息资产及数据资产）。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  标准指的就是信息系统相关资产。 |  |
|  | 7.2.4.12 | 7.2.4.12 安全事件处置。建议应保留原测评指标“应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响， 对本系统计算机安全事件进行等级划分;”；等级保护定义中就明确了安全事件分级管理，这是国家信息安全保障体系中的重要环节，也是各单位在事件响应时如何界定和资源投入的关键指导。 | 江西神舟信息安全评估中心有限公司 | 不采纳：  根据基本要求进行调整。 |  |
|  | 5.1.1.4 | 5.1.1.4 建议增加对灭火设备放置位置的检查内容。 | 信息产业信息安全测评中心 | 不采纳：  放置位置是否有机房场地建设相关标准来规范。 |  |
|  | 5.1.2.2 | 5.1.2.2 建议增加测试内容，可以分析传输数据。 | 信息产业信息安全测评中心 | 部分采纳：  二级、三级、四级增加传输数据测试相关内容。 |  |
|  | 5.1.2.3 | 5.1.2.3 第3），应为“是否没有其他未受控端口进行跨越边界的网络通信”。 | 信息产业信息安全测评中心 | 采纳：  调整为3) 应访谈安全管理员或检查设备配置信息，是否不存在其他未受控端口进行跨越边界的网络通信。 |  |
|  | 5.1.3.1.2 | 5.1.3.1.2 第1）项应该是包含2）、3）吧？是否重复了？限制非法登录次数后的处理机制不仅仅是锁定账户，还可以锁定IP、锁定账户一段时间等，建议写成开放性说法：“配置了非法登录次数阈值及启用了锁定账户等处置措施。” | 信息产业信息安全测评中心 | 采纳：  判定应该为或的关系，不是且关系，调整为：去掉1），调整2）为配置了非法登录次数阈值及启用了锁定账户等处置措施。保留3）。判定改为1）或2）为肯定。 |  |
|  | 5.1.3.2.1 | 5.1.3.2.1 在这里的测试是否应该考虑权限的合理性？明确权限分配原则？“如果1）-2）均为肯定”，应改为“如果2）为肯定”。 | 信息产业信息安全测评中心 | 不采纳：  权限分配在第三级有专门条款，1）为访谈，2）为测试，判定没有问题。 |  |
|  | 5.1.3.2.2 | 5.1.3.2.2 判定与要求不符，要求是“或”的关系，在判定里面是“且”的关系。 | 信息产业信息安全测评中心 | 采纳：  调整为1）或2）为肯定。 |  |
|  | 5.1.3.3.1 | 5.1.3.3.1 建议将“确认”改为“检查”，测试方法中没有“确认”。是否能分清楚“网络服务”与“系统服务”？归类和定义是什么？比如如果启用了IIS，这个是定义为网络服务还是系统服务？建议不如直接就用要求中的词语“组件和应用程序”。 | 信息产业信息安全测评中心 | 采纳：  调整为2) 应确认是否已经关闭非必要的组件和应用程序。 |  |
|  | 5.1.3.3.2 | 5.1.3.3.2 如何确认“高危端口”，个人感觉仅仅是为了突出？“不需要的系统服务”其实已包括了“高危端口”，一般端口会对应服务。 | 信息产业信息安全测评中心 | 不采纳：  高危端口是基本要求中的提法。 |  |
|  | 5.1.3.4.1 | 5.1.3.4.1 判定与测评实施对应不上。 | 信息产业信息安全测评中心 | 采纳：  测评实施调整为1) 应查看防恶意代码工具的安装和使用情况，检查是否定期进行升级和更新防恶意代码库。 |  |
|  | 5.1.4.1.1 | 5.1.4.1.1 建议全文中提到“标识与鉴别”时，应增加检查如何实现用户标识，然后再检查鉴别措施。“应测试应用系统对用户身份标识有效性是否进行鉴别”不太通顺，意思是否是“应测试应用系统的用户身份标识与鉴别措施是否有效”。 | 信息产业信息安全测评中心 | 不采纳：  标准原文不存在问题。 |  |
|  | 全文 | 全文，个人认为将“空密码用户”改为“不需要鉴别的用户”更严谨。 | 信息产业信息安全测评中心 | 不采纳：  空密码用户更便于理解。 |  |
|  | 5.1.4.1.2 | 5.1.4.1.2 1）应该包含3）了吧？ | 信息产业信息安全测评中心 | 不采纳：  1）测评的是有安全措施，3）测评的是具体的安全措施。 |  |
|  | 5.1.4.3.1 | 5.1.4.3.1 建议将1）2）3）顺序调整下，应为2）3）1）。 | 信息产业信息安全测评中心 | 采纳  已调整顺序。 |  |
|  | 5.1.4.4.1 | 5.1.4.4.1 建议删除“或加解密技术”，要求拔高了，应该是三级要求。 | 信息产业信息安全测评中心 | 不采纳：  标准内容是或的关系，不是必要条件。 |  |
|  | 5.2.4.1.1  5.2.4.5.1 | 5.2.4.1.1和5.2.4.5.1 应该是句号结尾。 | 信息产业信息安全测评中心 | 采纳：  已调整为句号结尾。 |  |
|  | 5.2.4.5.2 | 5.2.4.5.2 判定与实施不符。 | 信息产业信息安全测评中心 | 采纳：  调整为2) 应检查相关审批记录或流程，查看是否对申请账户、建立账户、删除账户等进行控制。 |  |
|  | 6.1.2.1.2 | 6.1.2.1.2 判定与实施不符。 | 信息产业信息安全测评中心 | 采纳：  判定调整为如果2）为肯定， |  |
|  | 6.1.2.1.3 | 6.1.2.1.3 判定与实施不符。应该有对划分合理性的判断。 | 信息产业信息安全测评中心 | 不采纳：  网络划分原则各单位不一，标准无法给出统一原则。 |  |
|  | 6.1.2.1.4 | 6.1.2.1.4 “，检查重要网路区域不能部署在网络边界处且没有边界防护措施”应改为“，检查重要网路区域是否未部署在网络边界处且没有边界防护措施”。 | 信息产业信息安全测评中心 | 不采纳：  标准原文表述更清晰。 |  |
|  | 6.1.2.2.1 | 6.1.2.2.1 测评对象应该不是“加解密设备或组件”，采用校验码技术即可。 | 信息产业信息安全测评中心 | 部分采纳：  修改测评测评实施，采用校验码技术。 |  |
|  | 7.1.2.5.1 | 7.1.2.5.1 判定与实施不符。 | 信息产业信息安全测评中心 | 采纳：  调整测评实施中的测评对象。 |  |
| **五、标准草案第四稿， 2016年8月25日，WG5工作组在研标准推进会，2016年8月26日填写** | | | | | |
|  | 6.2.4.9.1 | 中国对于密码产品有专门的证书或报告，但是对于非密码产品中的密码模块并没有相关认定证书或报告，建议在标准中对密码模块检查进行明确，另外密码产品只通过访谈检查力度较弱。 | IBM | 部分采纳：  密码管理需要遵照国家密码管理规定，已调整密码管理检查力度，增加检查相关证书或报告环节。 |  |
|  | 全文 | 如果标准中只有一条测评实施，那么单项判定时不应该有部分符合的提法。 | 阿里巴巴 | 采纳：  已做调整。  不采纳： |  |
| **六、标准草案第五稿，测评机构反馈意见，2016年9月6日填写** | | | | | |
|  | 前言、引言 | 应该按照GB/T 1.1-2009要求编制 | 成都市锐信安信息安全技术有限公司 | 采纳：  已经调整。 |  |
| **七、标准草案第五稿，2016年9月8日，评估中心大会议室，2016年9月9日填写** | | | | | |
|  | 全文 | 单元测评有标号，没有名称。 | 中国信息安全认证中心/李嵩 | 不采纳：  测评单元使用基本要求的要求项，无法命名。 |  |
|  | 全文 | 在术语定义中测评、测试、评估区分开 | 中国信息安全认证中心/李嵩 | 部分采纳：   1. 有些评估源自基本要求。 2. 部分已经调整，增加评估定义。 |  |
|  | 全文 | 很多单位安全策略不完善，或者没有贯彻下去，相关策略不一致，因此要对安全策略进行整体分析，并做策略一致性检查。 | 中国信息安全认证中心/李嵩 | 采纳：  在测评实施中完善相关内容。 |  |
|  | 全文 | 访谈的力度较弱，有些地方只有访谈，可考虑增加技术核查手段。 | 中国信息安全认证中心/李嵩 | 部分采纳：  已经调整。 |  |
|  | 7.2.2.4 | 7.1.2.1.4中测评对象是网络拓扑图，实际中很多单位的网络拓扑图与真实环境不一致，应核查网络拓扑图与真实环境是否一致。 | 中国信息安全认证中心/李嵩 | 采纳：  已经调整。 |  |
|  | 全文 | 附录里再做个附录，形成面向对象的测评单元汇总。 | 中国信息安全认证中心/李嵩 | 部分采纳。  与第132条建议合并，增加相关汇总表。 |  |
|  | 全文 | 标准中的测评单元与单元测评，都是指的单元，该如何区分，容易引起误解，最好进行定义，另外单项判定是否应为单元判定。 | 国家信息中心/禄凯 | 采纳。  单项判定改为单元判定。 |  |
|  | 全文 | 标准中要求对所有用户身份标识进行检查，实际是否能够做到，建议慎用所有这种词。 | 国家信息中心/禄凯 | 采纳：  已经调整。 |  |
|  | 全文 | 整体测评的控制点间、层面间关联分析很难把握，标准中能否给出一个已知关联度表，用于指导开展整体测评工作。 | 国家信息中心/禄凯 | 部分采纳。  调整部分文字描述。 |  |
|  | 全文 | 对描述结构“类——层面——控制点——要求项”进行定义。汇报PPT中的类实际应该是安全层面。 | 国家能源局信息中心/陈雪鸿 | 不采纳。  基本要求描述结构“层面（类）-控制点-要求项”定义。 |  |
|  | 全文 | 有些测评对象写得太笼统，比如物理环境测评中测评对象都是机房，应进一步明确。 | 国家能源局信息中心/陈雪鸿 | 采纳。  已经调整。 |  |
|  | 全文 | 新版等级测评报告已采用打分制，标准中单项判定是否也应该进行量化。 | 国家能源局信息中心/陈雪鸿 | 部分采纳。  相关内容在测评过程指南中描述。 |  |
|  | 全文 | 在术语中的检查与国家的安全检查容易混淆。 | 国家能源局信息中心/陈雪鸿 | 采纳。  改为核查（verification），增加核查定义。 |  |
|  | 全文 | 要求项一样，但不同级别中测评方法却不同，不太合理。 | 国家能源局信息中心/陈雪鸿 | 部分采纳。   1. 部分调整描述。 2. 级别不同测评实施有可能不同。 |  |
|  | 全文 | 测评对象的叫法不统一，网络通信类设备、网络安全类设备？ | 中国电子科技集团公司第十五研究所/刘健 | 采纳：  已经调整。 |  |
|  | 全文 | 默认口令应该放在访问控制还是身份鉴别？ | 中国电子科技集团公司第十五研究所/刘健 | 部分采纳：  随基本要求修订。 |  |
|  | 参考资料 | 18336评估准则已经发布最新版本了，应参考最新标准。 | 中国电子科技集团公司第十五研究所/刘健 | 采纳。  已改为 18336.1-2015、18336.2-2015、18336.3-2015 |  |
|  | 全文 | 新标准将数据安全与应用安全合并了，但很多单位关注数据安全，是否将数据安全独立出来。 | 国家信息技术安全研究中心/李蒙 | 部分采纳。  根据基本要求描述结构而来。 |  |
|  | 全文 | 标准中只有主体对客体的访问控制要求，客体对主体的访问控制是否也应说明。 | 国家信息技术安全研究中心/李蒙 | 部分采纳。  根据基本要求描述结构而来。 |  |
|  | 全文 | 对于Linux类系统，不安装防病毒软件这种特殊情况是否要指出来。 | 国家信息技术安全研究中心/李蒙 | 部分采纳。  此类情况在测评中作为不适用提出。 |  |
|  | 全文 | 边界的概念很模糊，是网络边界还是区域边界，还是系统边界、应用边界。 | 北京工业大学/赵勇 | 部分采纳。  根据基本要求描述结构而来。 |  |
|  | 全文 | 如何定义访问控制类设备，哪些属于访问控制类设备。 | 北京工业大学/赵勇 | 采纳：  已经调整。 |  |
|  | 全文 | 标准结构—集中管控的范围：是指管网络还是都管。 | 北京工业大学/赵勇 | 部分采纳。  根据基本要求描述结构而来。 |  |
|  | 全文 | 网络设备自身安全去掉了，要求加到了主机层面里了，建议单独说。 | 北京工业大学/赵勇 | 部分采纳。  根据基本要求描述结构而来。 |  |
|  | 全文 | 网络架构部分中关于架构安全的只有一条，像无线管理、集中管理等都是架构安全。 | 北京工业大学/赵勇 | 部分采纳。  根据基本要求描述结构而来。 |  |
|  | 全文 | 三级与四级之间的级差较少，在范围上能不能体现。 | 北京工业大学/赵勇 | 采纳：  通过测评实施的不同测评强度和广度来实现。 |  |
|  | 全文 | 对于非法外联，测评对象不应为准入设备，防垃圾邮件网关是否不用单独提出。 | 北京工业大学/赵勇 | 部分采纳。  对于非法外联，测评对象修改为终端管理系统。防垃圾邮件网关是基本要求中要求的。 |  |
|  | 全文 | 增加各级别汇总类大表索引，这样更清晰些。 | 中国电子技术标准化研究院/刘贤刚 | 采纳。  增加对应表。 |  |
|  | 全文 | 标准中有力度，还有广度、深度，相互之间的关系，如何与基本要求对应。 | 中国电子技术标准化研究院/刘贤刚 | 采纳：  基本要求维度为级差。测评通过测评广度和深度来体现测评要求级差。 |  |
|  | 全文 | 标准写法不统一，有的地方是访谈，有的是询问。 | 中国电子技术标准化研究院/刘贤刚 | 采纳。  统一调整为访谈。 |  |
|  | 全文 | 单项测评结论中没有不适用，是否以后取消了不适用。 | 阿里云信息技术有限公司/廖智杰 | 不采纳。  在等级测评实施工程中，才有可能出现不适用情况。 |  |
|  | 全文 | 将具体的测评对象放在测评实施里，这样是否更清晰。 | 阿里云信息技术有限公司/廖智杰 | 部分采纳。  调整测评对象的描述，使之更为明确；测评实施中部分做调整，明确测评对象。 |  |
|  | 全文 | 测评实施有多个项，单项判定中为符合、不符合或部分符合，而访谈与检查的力度是不一样的，应该是检查结果比访谈结果更可信。 | 阿里云信息技术有限公司/廖智杰阿里云信息技术有限公司/廖智杰 | 部分采纳。  在技术测评中，若访谈以了解为目的，则单项判定结果以检查结果为主（合并了解性）；管理测评中，访谈结果与检查结果同时采纳。 |  |
|  | 全文 | 单项测评中有没有必要引入穿行测试？ | 阿里云信息技术有限公司/廖智杰 | 不采纳。  根据基本要求的描述结构，等级测评由单项测评和整体测评组成，是由点到面到整体，穿行测试不适用于等级测评。 |  |
|  | 全文 | 测评单元与基本要求的文本号之间没有对应关系。 | 阿里云信息技术有限公司/廖智杰 | 采纳。  以汇总表方式体现测评单元与基本要求条款的对应。 |  |
|  | 全文 | 进一步对照基本要求和设计要求修改，不要有矛盾。 | 解放军信息安全测评中心/崔书昆 | 采纳。  已进行对照修改。 |  |
|  | 全文 | 文字进一步梳理，不要有歧义，不要词不达意。 | 解放军信息安全测评中心/崔书昆 | 采纳。  已进行文字校对。 |  |
| **八、标准草案第五稿，2016年9月18日，测评机构和用户反馈，2016年9月18日填写** | | | | | |
|  | 全文 | 应用和数据安全部分：特别是3,4级系统，建议加入“抗抵赖”、“重放检测”、“时间戳”等安全要求； | 中国邮政储蓄银行 | 采纳：  随基本要求修订。 |  |
|  | 全文 | 应用和数据安全部分：建议加入“系统参数及代码完整性”的安全要求，特别是这些对于app客户端有实际测评意义。 | 中国邮政储蓄银行 | 采纳：  随基本要求（移动互联）修订。 |  |
|  | 全文 | 另外“密码管理”部分，除管理要求外，建议对技术上提些要求。比如加密算法的选择，特别是国密算法的选择。 | 中国邮政储蓄银行 | 不采纳：  由国家密码局规定，本标准只能规定符合国家规定。 |  |
|  | 全文 | 在技术类测试确定测评对象上，有些条款写了相关人员，有些则没有写，比如7.1.2 网络和通信安全部分，7.1.2.8 集中管控等等，因为在测评实施中提到了要访谈相关人员，所以在确定测评对象时，都将相关人员列为测评对象，如7.1.2.1.2测评对象是“网络管理员或综合网管系统”。7.1.2.1.4测评对象是“网络管理员和网络拓扑图”等，而在7.1.2.2 通信传输部分，测评实施中都访谈了安全管理员，在测评对象中则没有安全管理员。文中有多处这样不一致的地方，我认为不应该把人员作为测评对象，因为测评面对的是技术系统安全和部门的安全管理，而不是某一个人员，所以要统一的话，建议在测评对象中去掉相关人员的描述。 | 国家广播电影电视总局广播电视信息安全测评中心/张瑞芝 | 部分采纳：  已经调整。 |  |
|  | 全文 | 在管理类测试中，有些测评对象是人员，建议都改为相关的文档资料，如“7.2.1.3 制定和发布”，测评对象是“信息安全主管”，我认为应该改为“授权文件”，因为人员不应该是测评对象，应该是制度、文件、记录等等是测评对象。因为信息安全基础是对人的防范，所有人都是受技术和管理的安全策略防范的，人是被约束的对象，被访谈的对象，而不是被测试的对象。 | 国家广播电影电视总局广播电视信息安全测评中心/张瑞芝 | 部分采纳：  已经调整。 |  |
|  | 全文 | 有些测试实施文字中，多处提到“验证策略有效性”，很难实现啊，如“7.1.2.5 入侵防范”中，对“IPS 、IDS 、抗APT 攻击、防DDoS 和网络回溯等系统或设备等测试对象”，“3) 应测试网络入侵防范设备，验证其策略有效性”；改为查看其策略，如何？ | 国家广播电影电视总局广播电视信息安全测评中心/张瑞芝 | 部分采纳：  调整相关描述，体现不同级别测评强度不同和保障策略有效性及一致性。 |  |
|  | 全文 | “7.1.2.5.3 测评单元（L3-NCS1-19）”在结果判定中，“如果1 ）- 2）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合本单项测评指标要求。”，没有不符合或部分符合的描述，与其他测评项的描述不一致，比如“7.1.2.5.4 测评单元（L3-NCS1-20）”等多个地方都与7.1.2.5.3一样，也是先查看有没有相关的设备，然后查验设备的有效性，但在结果判定中，符合、不符合或部分符合的描述都有。 | 国家广播电影电视总局广播电视信息安全测评中心/张瑞芝 | 采纳：  已经调整。 |  |
|  | 全文 | 测评实施只有一条的，是不是结果判定就不应该再有“否则，等级保护对象不符合或部分符合本单项测评指标要求”的描述了，就一条要么符合，要么不符合，好像应该没有部分符合吧。如果要有部分符合，是不是就应该把一条拆分成两条以上啊。 | 国家广播电影电视总局广播电视信息安全测评中心/张瑞芝 | 采纳：  已经调整。 |  |
|  | 7.1.3.2.2 | 7.1.3.2.2 测评单元（L3-ECS1-06）  a) 测评指标  应重命名默认账号或修改这些账号的默认口令。  c) 测评实施  1) 应检查是否不存在默认账号或默认账号已重命名；  2) 应检查是否已修改默认账号的默认口令。  修改意见：对于linux中root，oracle中system等账户不易或不能重命名如何判定？ | 国家广播电影电视总局广播电视信息安全测评中心/张瑞芝 | 采纳：  可以选择不适用。 |  |
|  | 全文 | 文件中多处出现的一些测评实施描述中，有阈值、使用率、复杂度等，是否应该给一个大概的标准，便于在测评中掌握呢，如机房温湿度范围、UPS后备时间、CPU使用率和内存使用率、密码复杂度、定期更换的频率等等。 | 国家广播电影电视总局广播电视信息安全测评中心/张瑞芝 | 不采纳：  由于具体需求不太一致，难以在标准中体现具体参数。 |  |
|  | 全文 | 为什么要有“附录C测评要求与设计要求对应表”？我觉得测评要求和设计要求是属于不同的专业范围，如果是基本要去与设计要求对应表是可以理解的，测评要求是基于基本要求的，测评要求与设计要求的对应完全取决于基本要求，把这个对应表放在这里好奇怪。如果一定要有对比，也应该放在基本要求里，是基本要求与设计要求的对应。 | 国家广播电影电视总局广播电视信息安全测评中心/张瑞芝 | 部分采纳：  调整附录C。 |  |

信息安全技术 网络安全等级保护测评要求 第1部分：安全通用要求标准编制修订组

2016年9 月 18日