**四川省政府政务服务和公共资源交易服务中心 系统安全等级保护测评项目**

**招**

**标**

**文**

**件**

**四川省政务服务和公共资源交易服务中心**

**2020年08月**

# **第一章** **采购邀请函**

本项目为四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评项目，采购单位为四川省政府政务服务和公共资源交易服务中心。本项目采购内容在规定的集中采购目录之外，且在省直部门分散采购限额标准以下，因此我中心拟用参照政府采购竞争性磋商综合评分法方式进行自行采购。

**1、项目概况：**

1.1采购项目：四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评项目。

1.2项目资金：自筹资金。

1.3项目实施方式：在合同约定时间范围内为四川省政府政务服务和公共资源交易服务中心提供系统安全等级保护测评。

1.4质量效果要求：符合国家相关要求。

1.5采购内容：四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评项目。

1.6项目总预算：人民币 24 万元整（贰拾肆万元整）

1.7中选原则：**根据综合评分法按排名由高到低推荐第一名为中标候选人。**

**2、资格审查方式及投标人资格要求**

本项目采用资格预审，采购评审小组根据采购文件的规定对投标人进行资格审查，若资格审查不合格其投标文件将被否决，采购申请人资格要求如下：

2.1具有独立承担民事责任的能力。（注：①供应商若为企业法人：提供“统一社会信用代码营业执照”；未换证的提供“营业执照、税务登记证、组织机构代码证或三证合一的营业执照”；②若为事业法人：提供“统一社会信用代码法人登记证书”；未换证的提交“事业法人登记证书、组织机构代码证”；③若为其他组织：提供“对应主管部门颁发的准许执业证明文件或营业执照”；④若为自然人：提供身份证或其它有效“身份证明材料”。以上材料均提供复印件）。

2.2具备良好商业信誉的证明材料（提供承诺函原件，格式详见第3.5声明、承诺函）；

2.3具备健全的财务会计制度的证明材料。｛注：①可提供2018或2019年度经审计的财务报告复印件；②也可提供2018或2019年度供应商内部的财务报表复印件（至少包含资产负债表和利润表）；③也可提供投标文件递交截止日前一年内银行出具的有效资信证明；④供应商注册时间距投标文件递交截止日不足一年的，提供成立后任意时段的资产负债表复印件。⑤也可提供承诺函原件，格式详见第3.5声明、承诺函｝

2.4具有依法缴纳税收和社会保障资金良好记录的证明材料。｛注：①（2018年1月至今任意三个月缴纳社保和税收的证明材料（税收提供税务部门开具的收据或网银转帐回执单等有效证明材料；社保资金提供社保部门开具的收据、网银转帐回执单或社保部门出具的已缴费证明等有效证明材料。依法免税或不需要缴纳社会保障资金的供应商，应提供相应文件证明其依法免税或不需要缴纳社会保障资金）；②也可提供承诺函原件，格式详见第3.5声明、承诺函｝

2.5具备履行合同所必需的人员能力的证明材料（可提供承诺函原件，格式详见第3.5声明、承诺函）；

2.6参加采购活动前三年内在经营活动中没有重大违法记录的承诺函（可提供承诺函原件，格式详见第3.5声明、承诺函）；

2.7具有网络安全等级保护测评机构推荐证书；

2.8本次采购不接受联合体投标

**3、报名及采购邀请函的获取**

投标人通过电话报名预留电子邮箱地址，收取电子邮件的方式获取采购邀请函。获取文件时间为：2020年9月1日至9月7日17:00（北京时间）。

**4、投标文件的递交**

投标文件提交的截止时间为2020年9月11日上午10：00（北京时间），提交地点：四川省成都市青羊区人民中路三段35号四川省政府政务服务和公共资源交易服务中心603室。逾期送达的投标文件将被拒绝。

本次采购项目将于2020年9月11日在四川省成都市青羊区人民中路三段35号四川省政府政务服务和公共资源交易服务中心进行评审。无需采购申请人的法定代表人或其委托的授权代表参加。

**5、联系方式**

四川省政府政务服务和公共资源交易服务中心

联 系 人：郭韩斌

联系电话：15884132232

地址：四川省成都市青羊区人民中路三段35号

2020年8月31日

# **技术规范要求**

# 一、项目主要工作内容及要求

**1、项目概况**

本项目为四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评项目。

1. **项目主要内容**

本次安全等级测评项目的服务范围包括以下信息系统：

|  |  |  |
| --- | --- | --- |
| **序号** | **信息系统名称** | **定级** |
| **1** | 省中心**门户网站** | **3级** |
| **2** | 省中心**交易系统** | **3级** |

2.1安全咨询。

对信息系统进行梳理，按照网络安全相关政策、标准要求对系统进行定级梳理，为系统安全建设方面提供建议和参考。

2.2等级测评

按照等级保护相关标准对系统从技术、管理等方面进行安全等级测评工作；根据测试结果，拟定网络安全整改建议；编制测评报告。制定并提交网络安全等级测评报告。具体如下：

2.2.1测评准备

主要任务是掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

2.2.2方案编制

主要任务是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评实施手册，形成测评方案。

2.2.3现场测评

本活动的主要任务是按照测评方案的总体要求，严格执行测评实施手册，分步实施所有测评项目，包括单元测评和整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题并形成整改报告，指导并协助省中心相关部门完成整改，完成整改后确保省中心该项工作达到省公安厅要求的良好及以上水平。

现场测评一般包括访谈、文档审查、配置检查、验证测试和实地察看等方面。

访谈是指测评人员与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。

文档审查是指检查《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）中规定的必须具有的制度、策略、操作规程等文档是否齐备，是否有完整的制度执行情况记录以及文件的完整性和这些文件之间的内部一致性。

配置检查是根据测评结果记录表格内容，利用上机验证的方式检查应用系统、主机系统、数据库系统以及网络设备的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计、数据审计等）。

验证测试是按照等级保护测评要求，配备必要的工具、仪器/设备对信息系统进行测试，采用的测评工具的生产商为正规厂商，具有一定的研发和服务能力，能够对产品进行持续更新并提供质量和安全保障。

2.2.4分析与报告编制

主要任务是根据省中心信息系统安全整改情况，结合差距分析报告，给出等级测评结论，形成测评报告文本。

2.3 成果递交

整理测评结果，提交被测网络安全等级保护测评报告以及相应文档，并在省公安厅备案。

## 2.4、项目组织与实施

本次等级测评项目，供应商应提供完善的项目组织，项目组织应由拥有国家要求的测评师证书的专业、高素质的技术人员组成，对项目进行全过程、全方位的计划、组织、管理、协调与控制。

## 2.5、测评工具

本次等级保护测评项目，供应商应提供完整齐全的信息安全服务测评工具。

## 2.6、安全措施

本次等级保护测评项目，供应商应提供项目质量的安全措施，项目进度的安全措施，为保证测评项目的实施过程中的安全性，保证实施安全。

2.7、设计依据

2.7.1《中华人民共和国网络安全法》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。

2.7.2《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） “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”。

2.7.3《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〔2003〕27号）文件规定：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。

2.7.4《信息安全等级保护管理办法》第十四条：信息系统建设完成后，运营、使用单位或其主管部门应当选择符合本办法规定条件的测评单位，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。”。

2.7.5《公安部关于印发信息安全等级保护工作的实施意见的通知》（公通字〔2004〕66号）

2.7.6《计算机信息系统安全保护等级划分准则》（ GB 17859-1999）

2.7.7《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）

2.7.8《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

2.7.9《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

2.7.10《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

2.7.11《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

2.7.12《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627-2018）

2.7.13《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

2.7.14《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

## 2.8、详细服务内容

本次等级保护测评项目，供应商应提供完整的实施方案，实施方案应包括但不限于测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动、测评内容、测评步骤、测评实施流程、测评方式等。

## 2.8.1测评准备活动

在测评准备活动，供应商应提供项目计划书、调查表格、现场测评授权书、文档交接单、会议记录表单等相关文档。等级测评项目确定后，双方成立测评项目组，双方协同梳理信息系统基本要素，供应商应该完成省中心信息系统基本要素和定级情况。

## 2.8.2方案编制活动

在方案编制活动阶段，供应商应提供测评方案，测评方案应包括但不限于测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定等。

供应商在获取省中心信息系统基本要素和定级情况后，供应商应明确项目内容、实施安排、人员配备、配合内容、注意事项、材料准备、测评指导书等内容完成测评方案编制，并与省中心确认测评方案和测评时间安排，确认正式现场测评步骤。

## 2.8.3现场测评活动

在现场测评活动阶段，为顺利完成测评任务，供应商应提供现场测评授权书、测评指导书、测评结果记录表格，并详细、准确、规范的记录测评证据，并保留电子证据，以便为后期的结果分析和报告编制准备充足的资料。

通过项目启动会议，供应商严格按照省中心工作要求，使用省中心提供的测评电脑等工具进入信息系统进行现场信息系统调查；根据各信息系统现场调查的结果，分别对各信息系统的物理、主机、网络、应用、数据、管理等方面进行安全测评，并且通过技术手段对信息系统测评对象实施安全测试和扫描，获取信息系统最真实的数据。此外供应商应该利用风险评估的方法对信息系统进行合理的信息系统风险分析。

## 2.8.4分析与报告编制活动

分析与报告编制活动中，供应商应通过单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论等几项内容来编制测评报告。

供应商应该根据现场测评实施获取的材料、信息、记录等进行统一汇总，分析得到单项测评结果，根据得到的单项测评结果计算得到单元测评结果。在单元测评的基础上，进一步分析信息系统已有安全措施的整体相关性，对信息系统实施整体测评，主要包括安全控制点间、层面间和区域间相互作用的安全测评，并且结合标准和行业特殊需求合理分析相关数据形成最终的等级测评结论，出具符合信息系统安全等级保护要求的信息安全等级保护测评符合性报告《测评报告》及对不符合信息安全等级保护有关管理规范和技术标准出具可行的、有效的信息系统《整改建议》。

## 2.8.5 测评内容

网络安全等级保护测评内容依据国家等保2.0相关标准实施，主要内容具体如下：

### 2.8.5.1 通用安全要求

#### 2.8.5.1.1 安全物理环境测评

1）测评指标

表 8‑1安全物理环境（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** | **备注** |
| 1 | 物理位置选择 | a）机房场地应选择在具有防震、防风和防雨等能力的建筑内； |  |
| 2 | b）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。 |  |
| 3 | 物理访问控制 | a）机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。 |  |
| 4 | 防盗窃和防破坏 | a）应将设备或主要部件进行固定，并设置明显的不易除去的标识； |  |
| 5 | b）应将通信线缆铺设在隐蔽安全处。 |  |
| 6 | c）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。 | 三级 |
| 7 | 防雷击 | a）应将各类机柜、设施和设备等通过接地系统安全接地。 |  |
| 8 | b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。 | 三级 |
| 9 | 防火 | a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； |  |
| 10 | b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。 |  |
| 11 | c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。 |  |
| 12 | 防水和防潮 | a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； |  |
| 13 | b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。 |  |
| 14 | c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。 | 三级 |
| 15 | 防静电 | a）应采用防静电地板或地面并采用必要的接地防静电措施。 |  |
| 16 | b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。 | 三级 |
| 17 | 温湿度控制 | a）应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 |  |
| 18 | 电力供应 | a）应在机房供电线路上配置稳压器和过电压防护设备； |  |
| 19 | b）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。 |  |
| 20 | c）应设置冗余或并行的电力电缆线路为计算机系统供电。 | 三级 |
| 21 | 电磁防护 | a）电源线和通信线缆应隔离铺设，避免互相干扰； |  |
| 22 | b）应对关键设备实施电磁屏蔽。 | 三级 |

2）测评实施

安全物理环境测评中，测评人员将以文档查阅与分析和现场观测等检查方法为主，访谈为辅来获取测评证据（如机房的温湿度情况），用于评测机房的安全保护能力。

安全物理环境测评涉及的测评对象主要为机房和相关的安全文档。

#### 7.5.1.2 安全通信网络测评

1）测评指标

表 8‑2安全通信网络（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** | **备注** |
| 1 | 网络架构 | a）应保证网络设备的业务处理能力满足业务高峰期需要； |  |
| 2 | b）应保证网络各个部分的带宽满足业务高峰期需要； |  |
| 3 | c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； | 三级 |
| 4 | d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； | 三级 |
| 5 | e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。 | 三级 |
| 6 | 通信传输 | a）应采用校验技术或密码技术保证通信过程中数据的完整性； |  |
| 7 | b）应采用密码技术保证通信过程中数据的保密性。 | 三级 |
| 8 | 可信验证 | a）可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |  |

2） 测评实施

安全通信网络测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统的安全保护能力。

#### 8.5.1.3 安全区域边界测评

1）测评指标

表 8‑3安全区域边界（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** | **备注** |
| 1 | 边界  防护 | a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； |  |
| 2 | b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； | 三级 |
| 3 | c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； | 三级 |
| 4 | d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 | 三级 |
| 5 | 访问  控制 | a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； |  |
| 6 | b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； |  |
| 7 | c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； |  |
| 8 | d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； |  |
| 9 | e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 | 三级 |
| 10 | 入侵  防范 | a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； |  |
| 11 | b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； | 三级 |
| 12 | c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； | 三级 |
| 13 | d）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 | 三级 |
| 14 | 恶意代码和垃圾邮件防范 | a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； |  |
| 15 | b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 | 三级 |
| 16 | 安全  审计 | a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |  |
| 17 | b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |  |
| 18 | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； |  |
| 19 | d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 | 三级 |
| 20 | 可信  验证 | a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |  |

2） 测评实施

安全区域边界测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统的网络安全保护能力。

#### 8.5.1.4 安全计算环境测评

1） 测评指标

表 8‑4安全计算环境（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** | **备注** |
| 1 | 身份  鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |  |
| 2 | b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； |  |
| 3 | c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； |  |
| 4 | d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 三级 |
| 5 | 访问  控制 | a）应对登录的用户分配账户和权限； |  |
| 6 | b）应重命名或删除默认账户，修改默认账户的默认口令； |  |
| 7 | c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； |  |
| 8 | d）应授予管理用户所需的最小权限，实现管理用户的权限分离； |  |
| 9 | e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； | 三级 |
| 10 | f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； | 三级 |
| 11 | g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 | 三级 |
| 12 | 安全  审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |  |
| 13 | b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |  |
| 14 | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； |  |
| 15 | d）应对审计进程进行保护，防止未经授权的中断。 | 三级 |
| 16 | 入侵  防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； |  |
| 17 | b）应关闭不需要的系统服务、默认共享和高危端口； |  |
| 18 | c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |  |
| 19 | d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； |  |
| 20 | e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； |  |
| 21 | f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 | 三级 |
| 22 | 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |  |
| 23 | 数据  完整性 | a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； |  |
| 24 | b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 | 三级 |
| 25 | 数据  保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； | 三级 |
| 26 | b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 | 三级 |
| 27 | 数据  备份  恢复 | a）应提供重要数据的本地数据备份与恢复功能； |  |
| 28 | b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； |  |
| 29 | c）应提供重要数据处理系统的热冗余，保证系统的高可用性。 | 三级 |

2） 测评实施

安全计算环境测评中，技术检测人员主要关注服务器操作系统、数据库管理系统、网络设备、安全设备以及应用系统在身份鉴别、访问控制、安全审计等方面的安全保护能力，将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况），用于评测系统的安全保护能力。

#### 8.5.1.5 安全管理中心测评

1） 测评指标

表8‑5安全管理中心（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全**  **子类** | **测评指标描述** | **备注** |
| 1 | 系统  管理 | a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； |  |
| 2 | b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 |  |
| 3 | 审计  管理 | a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； |  |
| 4 | b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |  |
| 5 | 安全  管理 | a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； | 三级 |
| 6 | b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 | 三级 |
| 7 | 集中  管控 | a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； | 三级 |
| 8 | b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； | 三级 |
| 9 | c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； | 三级 |
| 10 | d）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，并保证审计记录的留存时间符合法律法规要求； | 三级 |
| 11 | e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； | 三级 |
| 12 | f）应能对网络中发生的各类安全事件进行识别、报警和分析。 | 三级 |

2） 测评实施

安全管理中心测评中，技术检测人员将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况），用于评测系统的安全保护能力。

#### 8.5.1.6 安全管理制度测评

1） 测评指标

表 8‑6安全管理制度（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** | **备注** |
| 1 | 安全策略 | a）应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。 |  |
| 2 | 管理制度 | a）应对安全管理活动中的各类管理内容建立安全管理制度； |  |
| 3 | b）应对管理人员或操作人员执行的日常管理操作建立操作规程； |  |
| 4 | c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。 | 三级 |
| 5 | 制定和发布 | a）应指定或授权专门的部门或人员负责安全管理制度的制定； |  |
| 6 | b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。 |  |
| 7 | 评审  和修订 | a）应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。 |  |

2） 测评实施

安全管理类测评中，技术检测人员将以文档查看和分析为主，访谈为辅获取证据，来评测项目委托单位安全管理类措施的落实情况。安全管理类测评主要涉及安全主管、安全管理人员、管理制度文档、各类操作规程文件和操作记录等。

#### 8.5.1.7 安全管理机构测评

1） 测评指标

表 8‑7安全管理机构（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** | **备注** |
| 1 | 岗位设置 | a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权； |  |
| 2 | b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； |  |
| 3 | c）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。 | 三级 |
| 4 | 人员配备 | a）应配备一定数量的系统管理员、审计管理员和安全管理员等； |  |
| 5 | b）应配备专职安全管理员，不可兼任。 | 三级 |
| 6 | 授权  和审批 | a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； |  |
| 7 | b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； |  |
| 8 | c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。 | 三级 |
| 9 | 沟通  和合作 | a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； |  |
| 10 | b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； |  |
| 11 | c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 | 三级 |
| 12 | 审核  和检查 | a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； |  |
| 13 | b）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； | 三级 |
| 14 | c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。 | 三级 |

2）测评实施

安全管理机构测评主要涉及安全主管、相关管理制度以及相关工作/会议记录等技术检测对象。

#### 8.5.1.8 安全管理人员测评

1） 测评指标

表 8‑8安全管理人员（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** | **备注** |
| 1 | 人员录用 | a）应指定或授权专门的部门或人员负责人员录用； |  |
| 2 | b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核； |  |
| 3 | c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。 | 三级 |
| 4 | 人员离岗 | a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； |  |
| 5 | b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。 | 三级 |
| 6 | 安全意识  教育和培训 | a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施； |  |
| 7 | b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训； | 三级 |
| 8 | c）应定期对不同岗位的人员进行技能考核。 | 三级 |
| 9 | 外部人员  访问管理 | a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； |  |
| 10 | b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案； |  |
| 11 | c）外部人员离场后应及时清除其所有的访问权限； |  |
| 12 | d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。 | 三级 |

2） 测评实施

安全管理人员测评主要涉及安全主管、相关管理制度以及相关工作/会议记录等检测对象。

#### 8.5.1.9 安全建设管理测评

1） 测评指标

表 8‑9安全建设管理（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** | **备注** |
| 1 | 定级和备案 | a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； |  |
| 2 | b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； |  |
| 3 | c）应保证定级结果经过相关部门的批准； |  |
| 4 | d）应将备案材料报主管部门和相应公安机关备案。 |  |
| 5 | 安全  方案  设计 | a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； |  |
| 6 | b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件； |  |
| 7 | c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。 |  |
| 8 | 产品采购  和使用 | a）应确保网络安全产品采购和使用符合国家的有关规定； |  |
| 9 | b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求； |  |
| 10 | c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。 | 三级 |
| 11 | 自行  软件  开发 | a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； |  |
| 12 | b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； |  |
| 13 | c）应制定代码编写安全规范，要求开发人员参照规范编写代码； | 三级 |
| 14 | d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制； | 三级 |
| 15 | e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； | 三级 |
| 16 | f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制； | 三级 |
| 17 | g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。 | 三级 |
| 18 | 外包  软件  开发 | a）应在软件交付前检测其中可能存在的恶意代码； |  |
| 19 | b）应保证开发单位提供软件设计文档和使用指南； |  |
| 20 | c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。 | 三级 |
| 21 | 工程实施 | a）应指定或授权专门的部门或人员负责工程实施过程的管理； |  |
| 22 | b）应制定安全工程实施方案控制工程实施过程； |  |
| 23 | c）应通过第三方工程监理控制项目的实施过程。 | 三级 |
| 24 | 测试验收 | a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； |  |
| 25 | b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。 |  |
| 26 | 系统交付 | a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； |  |
| 27 | b）应对负责运行维护的技术人员进行相应的技能培训； |  |
| 28 | c）应提供建设过程文档和运行维护文档。 |  |
| 29 | 等级测评 | a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； |  |
| 30 | b）应在发生重大变更或级别发生变化时进行等级测评； |  |
| 31 | c）应确保测评机构的选择符合国家有关规定。 |  |
| 32 | 服务  供应商选择 | a）应确保服务供应商的选择符合国家的有关规定； |  |
| 33 | b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务； |  |
| 34 | c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。 | 三级 |

2） 测评实施

安全建设管理测评主要涉及系统建设负责人、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

#### 8.5.1.10 安全运维管理测评

1） 测评指标

表 8‑10 安全运维管理（通用要求）测评指标

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **安全子类** | **测评指标描述** | **备注** |
| 1 | 环境管理 | a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； |  |
| 2 | b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定； |  |
| 3 | c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 |  |
| 4 | 资产管理 | a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； |  |
| 5 | b）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； | 三级 |
| 6 | c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。 | 三级 |
| 7 | 介质管理 | a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； |  |
| 8 | b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 |  |
| 9 | 设备  维护  管理 | a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； |  |
| 10 | b）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等； |  |
| 11 | c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密； | 三级 |
| 12 | d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。 | 三级 |
| 13 | 漏洞和风险管理 | a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补； |  |
| 14 | b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。 | 三级 |
| 15 | 网络和系统安全管理 | a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； |  |
| 16 | b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； |  |
| 17 | c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； |  |
| 18 | d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； |  |
| 19 | e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； |  |
| 20 | f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为； | 三级 |
| 21 | g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库； | 三级 |
| 22 | h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据； | 三级 |
| 23 | i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道； | 三级 |
| 24 | j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。 | 三级 |
| 25 | 恶意代码  防范管理 | a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； |  |
| 26 | b）应定期验证防范恶意代码攻击的技术措施的有效性。 |  |
| 27 | c）应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。 | 三级 |
| 28 | 配置管理 | a）应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等； |  |
| 29 | b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。 | 三级 |
| 30 | 密码管理 | a）应遵循密码相关国家标准和行业标准； |  |
| 31 | b）应使用国家密码管理主管部门认证核准的密码技术和产品。 |  |
| 32 | 变更管理 | a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施； |  |
| 33 | b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程； | 三级 |
| 34 | c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。 | 三级 |
| 35 | 备份与恢复管理 | a）应识别需要定期备份的重要业务信息、系统数据及软件系统等； |  |
| 36 | b）应规定备份信息的备份方式、备份频度、存储介质、保存期等； |  |
| 37 | c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。 |  |
| 38 | 安全事件  处置 | a）应及时向安全管理部门报告所发现的安全弱点和可疑事件； |  |
| 39 | b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； |  |
| 40 | c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训； |  |
| 41 | d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。 | 三级 |
| 42 | 应急预案  管理 | a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容； |  |
| 43 | b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； |  |
| 44 | c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； | 三级 |
| 45 | d）应定期对原有的应急预案重新评估，修订完善。 | 三级 |
| 46 | 外包运维  管理 | a）应确保外包运维服务商的选择符合国家的有关规定； |  |
| 47 | b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容； |  |
| 48 | c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确； | 三级 |
| 49 | d）应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT 基础设施中断服务的应急保障要求等。 | 三级 |

2） 测评实施

安全运维管理测评主要涉及安全主管、各类运维人员、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

### 8.5.2 扩展安全要求

### 8.5.2.1 安全物理环境测评

表8‑11安全物理环境（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全  扩展要求 | 基础设施位置 | a）应保证云计算基础设施位于中国境内。 |
| 2 | 移动互联网  安全扩展要求 | 无线接入点的物理位置 | a）应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。 |
| 3 | 物联网  安全扩展要求 | 感知节点设备物理防护 | a）感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动； |
| 4 | b）感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）； |
| 5 | c）感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等； |
| 6 | d）关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力）。 |
| 7 | 工业控制系统  安全扩展要求 | 室外控制设备物理防护 | a）室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等； |
| 8 | b）室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。 |
| 9 | 大数据系统  安全扩展要求 | 大数据平台 | a）应保证承载大数据存储、处理和分析的设备机房位于中国境内。 |

#### 8.5.2.2 安全通信网络测评

表 8‑12安全通信网络（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全  扩展要求 | 网络架构 | a）应保证云计算平台不承载高于其安全保护等级的业务应用系统； |
| 2 | b）应实现不同云服务客户虚拟网络之间的隔离； |
| 3 | c）应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力； |
| 4 | d）应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略； |
| 5 | e）应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。 |
| 6 | 工业控制系统  安全扩展要求 | a）工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段； |
| 7 | b）工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段； |
| 8 | c）涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离。 |
| 9 | 通信传输 | a）在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。 |
| 10 | 大数据系统  安全扩展要求 | 大数据平台 | a）应保证大数据平台不承载高于其安全保护等级的大数据应用； |
| 11 | b）应保证大数据平台的管理流量与系统业务流量分离。 |

#### 8.5.2.3 安全区域边界测评

表 8‑13安全区域边界（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全  扩展要求 | 访问控制 | a）应在虚拟化网络边界部署访问控制机制，并设置访问控制规则； |
| 2 | b）应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。 |
| 3 | 入侵防范 | a）应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； |
| 4 | b）应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等； |
| 5 | c）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量； |
| 6 | d）应在检测到网络攻击行为、异常流量情况时进行告警。 |
| 7 | 安全审计 | a）应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； |
| 8 | b）应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 |
| 9 | 移动互联网  安全扩展要求 | 边界防护 | a）应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。 |
| 10 | 访问控制 | a）无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。 |
| 11 | 入侵防范 | a）应能够检测到非授权无线接入设备和非授权移动终端的接入行为； |
| 12 | b）应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为； |
| 13 | c）应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态； |
| 14 | d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等； |
| 15 | e）应禁止多个AP使用同一个认证密钥； |
| 16 | f）应能够阻断非授权无线接入设备或非授权移动终端。 |
| 17 | 物联网安全  扩展要求 | 接入控制 | a）应保证只有授权的感知节点可以接入。 |
| 18 | 入侵防范 | a）应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为； |
| 19 | b）应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。 |
| 20 | 工业控制系统  安全扩展要求 | 访问控制 | a）应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-Mail、Web、Telnet、Rlogin、FTP等通用网络服务； |
| 21 | b）应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警。 |
| 22 | 拨号使用控制 | a）工业控制系统确需使用拨号访问服务的，应限制具有拨号访问权限的用户数量，并采取用户身份鉴别和访问控制等措施； |
| 23 | b）拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施。 |
| 24 | 无线使用控制 | a）应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别； |
| 25 | b）应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制； |
| 26 | c）应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护； |
| 27 | d）对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为。 |

#### 8.5.2.4 安全计算环境测评

表 8‑14安全计算环境（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全  扩展要求 | 身份鉴别 | a）当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。 |
| 2 | 访问控制 | a）应保证当虚拟机迁移时，访问控制策略随其迁移； |
| 3 | b）应允许云服务客户设置不同虚拟机之间的访问控制策略。 |
| 4 | 入侵防范 | a）应能检测虚拟机之间的资源隔离失效，并进行告警； |
| 5 | b）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警； |
| 6 | c）应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。 |
| 7 | 镜像和快照保护 | a）应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务； |
| 8 | b）应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改； |
| 9 | c）应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 |
| 10 | 数据完整性  和保密性 | a）应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定； |
| 11 | b）应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限； |
| 12 | c）应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； |
| 13 | d）应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 |
| 14 | 数据备份恢复 | a）云服务客户应在本地保存其业务数据的备份； |
| 15 | b）应提供查询云服务客户数据及备份存储位置的能力； |
| 16 | c）云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致； |
| 17 | d）应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。 |
| 18 | 剩余信息保护 | a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除； |
| 19 | b）云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。 |
| 20 | 移动互联网  安全扩展要求 | 移动终端管控 | a）应保证移动终端安装、注册并运行终端管理客户端软件； |
| 21 | b）移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。 |
| 22 | 移动应用管控 | a）应具有选择应用软件安装、运行的功能； |
| 23 | b）应只允许指定证书签名的应用软件安装和运行； |
| 24 | c）应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。 |
| 25 | 物联网安全  扩展要求 | 感知节点  设备安全 | a）应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更； |
| 26 | b）应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力； |
| 27 | c）应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。 |
| 28 | 网关节点  设备安全 | a）应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力； |
| 29 | b）应具备过滤非法节点和伪造节点所发送的数据的能力； |
| 30 | c）授权用户应能够在设备使用过程中对关键密钥进行在线更新； |
| 31 | d）授权用户应能够在设备使用过程中对关键配置参数进行在线更新。 |
| 32 | 抗数据重放 | a）应能够鉴别数据的新鲜性，避免历史数据的重放攻击； |
| 33 | b）应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。 |
| 34 | 数据融合处理 | a）应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用。 |
| 35 | 工业控制系统  安全扩展要求 | 控制设备安全 | a）控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制； |
| 36 | b）应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作； |
| 37 | c）应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理； |
| 38 | d）应使用专用设备和专用软件对控制设备进行更新； |
| 39 | e）应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。 |
| 40 | 大数据系统  安全扩展要求 | 大数据平台 | a）大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别； |
| 41 | b）大数据平台应能对不同客户的大数据应用实施标识和鉴别； |
| 42 | c）大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力； |
| 43 | d）大数据平台应对其提供的辅助工具或服务组件，实施有效管理； |
| 44 | e）大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行； |
| 45 | f）大数据平台应提供静态脱敏和去标识化的工具或服务组件技术； |
| 46 | g）对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理； |
| 47 | h）大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施； |
| 48 | i）大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求； |
| 49 | j）大数据平台应在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致； |
| 50 | k）涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作； |
| 51 | l）应在数据清洗和转换过程中对重要数据进行保护,以保证重要数据清洗和转换后的一致性，避免数据失真,并在产生问题时能有效还原和恢复； |
| 52 | m）应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求； |
| 53 | n）大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。 |

#### 8.5.2.5 安全建设管理测评

表 8‑15安全建设管理（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全  扩展要求 | 云服务商选择 | a）应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力； |
| 2 | b）应在服务水平协议中规定云服务的各项服务内容和具体技术指标； |
| 3 | c）应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等； |
| 4 | d）应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除； |
| 5 | e）应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。 |
| 6 | 供应链管理 | a）应确保供应商的选择符合国家有关规定； |
| 7 | b）应将供应链安全事件信息或安全威胁信息及时传达到云服务客户； |
| 8 | c）应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。 |
| 9 | 移动互联网  安全扩展要求 | 移动应用软件  采购 | a）应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名； |
| 10 | b）应保证移动终端安装、运行的应用软件由指定的开发者开发。 |
| 11 | 移动应用软件  开发 | a）应对移动业务应用软件开发者进行资格审查； |
| 12 | b）应保证开发移动业务应用软件的签名证书合法性。 |
| 13 | 工业控制系统  安全扩展要求 | 产品采购和使用 | a）工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。 |
| 14 | 外包软件开发 | a）应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容。 |
| 15 | 大数据系统  安全扩展要求 | 大数据平台 | a）应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力； |
| 16 | b）应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容； |
| 17 | c）应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力。 |

#### 8.5.2.6 安全运维管理测评

表 8‑16安全运维管理（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 1 | 云计算安全  扩展要求 | 云计算环境管理 | a）云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。 |
| 2 | 移动互联网  安全扩展要求 | 配置管理 | a）应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。 |
| 3 | 物联网安全  扩展要求 | 感知节点管理 | a）应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护； |
| 4 | b）应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理； |
| 5 | c）应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。 |
| 6 | 大数据系统  安全扩展要求 | 大数据平台 | a）应建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程； |
| 7 | b）应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施； |
| 8 | c）应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程； |
| 9 | d）应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更。 |

## 2.8.6测评方法

本次等级保护测评项目，供应商应提供科学、合理的测评方法开展等级保护测评工作。

## 2.8.7测评步骤

本次等级保护测评项目，供应商应从差距测评和整体测评的测评步骤进行开展等级保护测评工作。

2.8.8 保密承诺

中标供应商应签订保密承诺书和保密协议。

# **第三章 评审办法（综合评分法）**

## **3.1评审的量化因素及权重比值**

**本项目采用综合评分方式确定中标候选人排名**。综合评分包括： 价格评分（20分）+项目实施方案（10分）+投标人综合实力（31分）+实施人员能力（31分）+项目实施能力（6分）+响应文件规范性（2分）。

谈判人最终得分=价格评审得分+项目实施方案+投标人综合实力实力+实施人员能力+项目实施能力+响应文件规范性

## **3.3** **评审方法**

**3.3.1谈判申请文件的初步评审**

3.3.1.1在初步评审中，评审小组将首先审定每份谈判申请文件是否响应了谈判文件的下述要求。

3.3.1.2如发现下列情况之一的，其谈判将被评审小组否决：

（1）投标文件未按招标文件要求进行签署、盖章的；

（2）资格证明文件不全的；

（3）同一投标人提交两个以上不同的投标文件或者报价，以及投标文件没有提交谈判报价的；

（4）投标文件载明的招标项目完成期限超过谈判文件规定的期限；

（5）经评审小组认定投标人的报价低于成本价形成恶性竞争的；

（6）明显不符合招标文件服务标准的要求；

（7）投标文件附有采购人不能接受的条件；

（8）报价超过招标文件规定的限价；

（9）其他不符合招标文件实质性要求及法律、法规规定的其他情形。

**3.3.2 报价计算错误的修正原则**

3.3.2.1 评审小组将对确定为实质上响应招标文件要求的投标文件进行校核，看其是否有计算上或汇总上的算术错误，修正错误的原则如下：

（1）投标文件中的大写金额与小写金额不一致的，以大写金额为准；

**3.3.3 谈判申请文件的详细评审**

综合评审包括：价格评审得分+项目实施方案+投标人综合实力实力+实施人员能力+项目实施能力+响应文件规范性。

评委将根据评分标准，依据综合评分结果排名。

评分标准

| **序号** | **评分因素**  **及权重** | **分值** | **评分标准** | **说明** |
| --- | --- | --- | --- | --- |
| 1 | 报价20% | 20分 | 以本次经评审的有效的最低最后报价为基准价，报价得分=（基准价/报价）×20。 | 报价为n个系统的等级保护测评费用 |
| 2 | 项目实施方案10% | 10分 | 1.项目实施方案完备性评分：  投标人项目实施方案组成应包括：项目实施标准、测评准备、方案编制、现场测评、报告编制、项目人员安排、项目实施周期等内容每有一个得1分，最多5分，没有的不得分。  2.项目实施方案理解程度评分：  能准确理解项目的意义和背景，对项目的需求、目标、意义、以及本项目开展思路和框架有全面、准确的理解，能够明确项目的输出成果，得2分；对项目的需求及输出成果理解不明确的，不得分。  3.项目实施方案合理性与可执行性评分：  方案系统整体性很强，设计方案统一明晰，项目计划明晰，时间把控非常合理，服务内容的安排十分明确、合理，制定了详细、规范的项目计划，每符合一个得0.5分，最多得3分；没有不得分。 |  |
| 3 | 投标人  综合实力31% | 31分 | 1.供应商具有中国合格评定国家认可委员会颁发的CNAS证书得7分；  2.供应商具有中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质证书得6分；  3.供应商具有ISO9001质量体系认证证书、ISO14001环境管理体系认证证书、ISO45001职业健康安全管理体系认证证书，认证范围包括“网络安全等级保护测评”，每有1个得2分，最多得6分，没有不得分。  4.供应商具有ISO27001信息安全管理体系认证证书，认证范围包括“网络安全等级保护测评”得6分。  5.供应商具有ISO20000-1服务管理体系认证证书，认证范围包括“信息系统测试服务”得6分。 | 须提供有效证书复印件并加盖投标人公章。 |
| 4 | 实施人员能力  31% | 31分 | 1.拟派本项目的项目负责人同时具有信息安全等级测评师（高级）证书、信息系统项目管理师证书（高级）、咨询师证书，得6分，每少提供一个证书扣2分，扣完为止。  2.拟派本项目的项目经理同时具有信息安全等级测评师（中级）证书、CISP证书、CISAW证书、ISO27001证书、COBIT证书、CIIP-A证书，每具有一个证书得2分，最多10分。  3.拟派本项目的测评人员同时具有信息安全等级测评师（中级）证书、CISAW证书、ITIL证书得6分，每少提供一个证书扣2分，扣完为止。  4.拟派本项目的其他测评人员具有CISP-PTE证书、ISO27001证书、ITIL证书，每具有一个证书得3分（每个证书不能重复得分），最多9分。 | 提供相关人员有效的证书复印件并加盖投标人公章。提供相关人员的社保证明。 |
| 5 | 项目实施能力6% | 6分 | 具有测评服务的能力，提供一个项目案例证明材料得1分，最多得6分。 | 提供相关证明材料加盖投标人公章。 |
| 6 | 响应文件规范性2% | 2分 | 响应文件制作规范，没有细微偏差情形的得2分；有一项细微偏差扣0.5分，扣完为止。 |  |

**符合性审查**

|  |  |
| --- | --- |
| 符合性审查 | 评审内容 |
| 资格证明文件不全的或招标人资格条件不满足招标文件要求的； |
| 投标文件没有投标人授权代表签字和加盖单位章； |
| 投标标文件没有报价的或投标人投报两个或多个报价的； |
| 明显不符合技术规范书的要求； |
| 投标文件附有招标人不能接受的条件； |
| 存在恶意报价行为且损害招标人利益的； |
| 其他不符合招标文件实质性要求及法律、法规规定的其他情形； |

在详细评审之前，评审小组将首先根据谈判文件中载明的资格审查标准对谈判申请人递交的谈判文件进行审查，有任何一项因素不符合审查标准的，不能通过资格审查，同时审定每份投标文件是否在实质上响应了谈判文件的要求。

只有资格审查满足要求及符合性审查合格的投标人人，其投标文件才能参与评价与比较。

**附：资格审查标准**

|  |  |  |
| --- | --- | --- |
| **谈判申请人资格审查标准** | | |
| **序号** | **审查内容** | **审查标准** |
| 1 | 具有独立承担民事责任的能力 | ①供应商若为企业法人：提供“统一社会信用代码营业执照”；未换证的提供“营业执照、税务登记证、组织机构代码证或三证合一的营业执照”；②若为事业法人：提供“统一社会信用代码法人登记证书”；未换证的提交“事业法人登记证书、组织机构代码证”；③若为其他组织：提供“对应主管部门颁发的准许执业证明文件或营业执照”；④若为自然人：提供身份证或其它有效“身份证明材料”。以上材料均提供复印件 |
| 2 | 具备良好商业信誉的证明材料 | 提供承诺函原件，格式详见第**3.5声明**、承诺函 |
| 3 | 具备健全的财务会计制度的证明材料 | ①可提供2018或2019年度经审计的财务报告复印件；②也可提供2018或2019年度供应商内部的财务报表复印件（至少包含资产负债表和利润表）；③也可提供投标文件递交截止日前一年内银行出具的有效资信证明；④供应商注册时间距投标文件递交截止日不足一年的，提供成立后任意时段的资产负债表复印件。⑤也可提供承诺函原件，格式详见第**3.5声明**、承诺函 |
|  | 具有依法缴纳税收和社会保障资金良好记录的证明材料 | ①2018年1月至今任意三个月缴纳社保和税收的证明材料（税收提供税务部门开具的收据或网银转帐回执单等有效证明材料；社保资金提供社保部门开具的收据、网银转帐回执单或社保部门出具的已缴费证明等有效证明材料。依法免税或不需要缴纳社会保障资金的供应商，应提供相应文件证明其依法免税或不需要缴纳社会保障资金）；②也可提供承诺函原件，格式详见第**3.5声明**、承诺函 |
| 4 | 具备履行合同所必需的设备和专业技术能力的证明材料 | 可提供承诺函原件，格式详见第**3.5声明**、承诺函 |
| 5 | 参加采购活动前三年内在经营活动中没有重大违法记录的承诺函 | 可提供承诺函原件，格式详见第**3.5声明**、承诺函 |
| 6 | 具有网络安全等级保护测评机构推荐证书 | 提供具有网络安全等级保护测评机构推荐证书原件 |
| 7 | 本项目不接受联合体  报价 |  |

**3.4** **报价表（格式）**

**报价表**

**项目名称：四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评项目报价表**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务内容** | **报价（元）** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| .... |  |  |
| 合? | 小写： 大写： | |

报价（大写人民币）：

供应商名称：　　 　　　　　　(加盖公章)

法定代表人或代理人：　　 　　　　　　（签字）

日期：

**说明：报价应是包括邀请文件中规定的全部响应内容的报价（包含中标供应商应承担的物耗、人工、税费等）。**

**3.5声明（格式）**

**声 明**

**致：四川省政府政务服务和公共资源交易服务中心**

我单位作为四川省政府政务服务和公共资源交易服务中心系统安全等级保护测评项目的供应商，在此郑重声明：

一、我单位参加采购活动前三年内，在经营活动中**（说明：填写“无”或“有”**）重大违法记录。

二、我单位**（说明：填写“具有”或“不具有”**）良好的商业信誉。

三、与我单位存在直接控股、管理关系的相关供应商：**（说明：填写“无”或“（一）供应商名称１；（二）供应商名称２ ；（三）……”）。**

四、在行贿犯罪信息查询期限内，我公司及我公司现任法定代表人、主要负责人**（说明：填写“没有”或“有”）**行贿犯罪记录。

五、我公司**（说明：填写“未列入”或“被列入”**）失信被执行人、重大税收违法案件当事人名单。

我公司**（说明：填写“未列入”或“被列入”**）采购严重违法失信行为记录名单。

我公司**（说明：填写“没有”或“有”**）未依法缴纳税收和社会保障资金的不良记录。

特此声明。

供应商名称：　　 (加盖公章)

日 期：　　年　　月　　日