

计划函号：鄂采计[2018]-34168 号

---

# 湖北省省级政府采购项目 信息系统安全等级测评服务 竞争性谈判文件

---

项目编号：HBT-16180396-183989

采购人：湖北省审计厅

采购代理机构：湖北省招标股份有限公司

办公地址：武汉市武昌区中北路 108 号兴业银行大厦 5 层

## 目录

第一章谈判公告（代谈判邀请函）	1
一、项目概况	1
二、供应商资格要求	1
三、谈判文件的获取	2
四、谈判响应文件送达地点及截止时间	2
五、谈判地点及时间	2
六、公告期限	3
七、联系事项	3
第二章供应商须知	5
《供应商须知前附表》	5
供应商须知	7
一、总则	8
1、适用范围	8
2、定义	8
3、工程、货物及服务	8
4、费用	8
二、竞争性谈判文件	9
5、竞争性谈判文件的构成	9
6、谈判文件的澄清或修改	9
7、现场踏勘	9
三、竞争性谈判响应文件	10
8、语言和计量单位	10
9、竞争性谈判响应文件的构成	10
10、竞争性谈判响应文件的编制	10
11、谈判报价	10
12、备选方案	11
13、联合体	11
14、供应商资格证明文件	11
15、证明报价内容、服务合格性和符合竞争性谈判文件规定的文件	11
16、响应文件有效期	11
17、竞争性谈判响应文件的装订、签署和数量	11
四、竞争性谈判响应文件的递交	12
18、竞争性谈判响应文件的密封和标记	12

19、竞争性谈判响应文件的送达地点及截止时间	12
20、迟交的竞争性谈判响应文件	12
21、竞争性谈判响应文件的补充、修改或者撤回	12
五、谈判程序	13
22、谈判小组	13
23、谈判代表	13
24、资格审查和符合性审查	13
25、谈判	13
26、保密	14
六、成交与签订合同	14
27、合同授予标准	14
28、签订合同	14
七、质疑和投诉	15
29、质疑	15
30、质疑回复	15
31、投诉	15
八、政府采购政策	16
九、其他要求	17
十、适用法律	17
第三章项目采购需求	18
一、项目概况	18
二、项目需求	18
三、技术服务要求	18
3.1 定级备案服务	18
3.2 信息系统安全等级保护测评服务	18
3.3 第三级系统测评内容	19
3.3.1 物理安全	19
3.3.2 网络安全	21
3.3.3 主机安全	23
3.3.4 应用安全	25
3.3.5 数据安全及备份恢复	27
3.3.6 安全管理机构	27
3.3.7 安全管理制度	29
3.3.8 人员安全管理	29

3.3.9	系统建设管理	30
3.3.10	系统运维管理	33
3.4	第四级系统测评内容	38
3.4.1	物理安全	38
3.4.2	网络安全	40
3.4.3	主机安全	42
3.4.4	应用安全	44
3.4.5	数据安全及备份恢复	46
3.4.6	安全管理机构	47
3.4.7	安全管理制度	49
3.4.8	人员安全管理	50
3.4.9	系统建设管理	51
3.4.10	系统运维管理	54
3.5	等级保护合规咨询服务	59
3.6	标准和规范	59
3.7	测评实施原则	60
3.8	整体要求	61
3.9	专用工具要求	61
3.10	安全管理要求	61
3.11	测评风险规避要求	62
四、其他需求		63
第四章合同草案		64
第五章评审标准		65
一、资格性和符合性审查标准		65
二、推荐成交候选供应商标准		65
三、政府采购政策支持		66
第六章响应文件的格式		67
一、谈判书		69
二、法定代表人授权书		70
三、法定代表人身份证明书		71
四、报价一览表		72
五、分项报价表		73
六、偏离情况表		74
七、类似业绩一览表		75

八、拟投入项目组人员一览表	76
九、供应商的资格声明	77
十、资格证明文件	78
十一、供应商关联企业情况表	79
十二、无重大违法记录声明	80
十三、技术文件	81
十四、谈判供应商认为应该提交的其它文件（格式自拟）	82
十五、中小企业声明函	83
十六、节能环保产品证明材料	84

## 第一章谈判公告（代谈判邀请函）

依据湖北省财政厅政府采购预算执行计划“鄂采计[2018]-34168 号”要求，湖北省招标股份有限公司受湖北省审计厅的委托，对其“信息系统安全等级测评服务”以分散采购组织形式进行竞争性谈判采购，欢迎符合资格条件的供应商参与谈判。

### 一、项目概况

（一）项目编号：HBT-16180396-183989

（二）项目名称：信息系统安全等级测评服务

（三）采购预算：29 万元

（四）项目内容及需求：

1. 本次竞争性谈判共分 1 个项目包，具体需求如下。详细技术规格、参数及要求见本项目谈判文件第三章内容。

第  包：

（1）项目包编号：HBT-16180396-183989

（2）项目包名称：信息系统安全等级测评服务

（3）类别：服务

（4）用途：安全等级测评

（5）数量：1 项

（6）简要技术要求：详见谈判文件第三章“项目采购需求”

（7）采购预算：29 万元

（8）期限（交货期）：合同签订后 30 个工作日内完成等级测评和安全建设方案设计

（9）质保期：1 年

（10）其他：无

2. 供应商参加谈判的报价超过该包采购预算金额的，其该包谈判报价无效。

3. 参加多包投标的相关规定：无。

4. 供应商如需查询技术要求可将您的联系方式发送至        联系索取，也可直接到我处查阅谈判文件。

5. 采购项目需要落实的政府采购政策：本项目需落实的节能环保、中小微型企业扶持（含支持监狱企业发展、促进残疾人就业）等相关政府采购政策详见谈判文件。

### 二、供应商资格要求

（一）供应商必须符合《政府采购法》第二十二条规定的条件：

1. 具有独立承担民事责任的能力；
2. 具有良好的商业信誉和健全的财务会计制度；

3. 具有履行合同所必需的设备和专业技术能力；
4. 有依法缴纳税收和社会保障资金的良好记录；
5. 参加政府采购活动前三年内，在经营活动中没有重大违法记录；
6. 法律、行政法规规定的其他条件。

（二）各包特定资格要求：

1. 供应商参加政府采购活动前三年内未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人、重大税收违法案件当事人、政府采购严重违法失信行为记录名单和“中国政府采购”网站(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单（以递交响应文件截止当日查询结果为准）。

2. 供应商必须持有国家网络安全等级保护工作协调小组办公室颁发的“网络安全等级保护测评机构推荐证书”（需在投标文件中附复印件）。省外等保测评机构必须提供网络安全等级保护测评项目登记管理系统中审核通过记录的截图（加盖供应商公章）。

3. 供应商须提供 2017 参加 CNAS T0832 能力验证计划结果证书，最终评价结果为满意。

4. 本项目不接受联合体参与谈判。

（三）如国家法律法规对市场准入有要求的还应符合相关规定。

以上资格要求为本次供应商应具备的基本条件，参加各包谈判的供应商必须满足资格要求中的对应各包的所有条款，并按照相关规定递交资格证明文件。

### 三、谈判文件的获取

（一）获取时间：2018 年 12 月 27 日至 2018 年 12 月 29 日（北京时间每天上午 8:30~12:00、下午 14:00~16:30，法定节假日以及休息日（周六周日）除外）。

（二）获取地点：武汉市武昌区中北路 108 号兴业银行大厦 5 层 5011 室。

（三）获取方式：符合资格条件的供应商应当在获取时间内，携带以下材料领取谈判文件，谈判文件每套售价 200 元，售后不退。

1. 法定代表人自己领取的，凭法定代表人身份证明书及法定代表人身份证原件领取。
2. 法定代表人委托他人领取的，凭法定代表人授权书及受托人身份证原件领取。
3. 报名表原件。

### 四、谈判响应文件送达地点及截止时间

（一）送达地点：武汉市武昌区中北路 108 号兴业银行大厦 5 层湖北省招标股份有限公司 5 号会议室

（二）截止时间：2019 年 1 月 3 日 14:30（北京时间）

### 五、谈判地点及时间

（一）地点：武汉市武昌区中北路 108 号兴业银行大厦 5 层湖北省招标股份有限公司 5 号会议室

（二）时间：2019 年 1 月 3 日 14:30（北京时间）

届时敬请参加谈判的代表出席谈判仪式。

## 六、公告期限

本公告的公告期限为 2018 年 12 月 27 日至 2018 年 12 月 29 日共 3 个工作日。

## 七、联系事项

采购人联系方式：

采购人：湖北省审计厅

地址：武汉市武昌区天鹅路 3 号

联系人：刘驰

联系电话：13477099227

政府采购代理机构联系方式：

名称：湖北省招标股份有限公司

地址：武汉市武昌区中北路 108 号兴业银行大厦五层 5033 室

联系人：宋浠、李海燕

电话：027-87819169

传真：027-87360813

户名：湖北省招标股份有限公司

开户行：招商银行水果湖支行

行号：881098

账号：12790 54338 10603

湖北省招标股份有限公司

2018 年 12 月 26 日



## 附件：报名表

项目报名表			
项目名称			
项目编号			
供应商名称（公章）	（填写完整的单位全称，必须与投标文件上的供应商一致）		
报名包号	（填写报名包号，变更或放弃包号请来函告知，放弃投标请来函告知）		
授权代表	（填写联系人姓名）请填写一个固定联系人，变更请来函告知。		
授权代表手机	（填写联系人手机） 有关信息我们会短信发送至手机，请关注并收到后回复。	授权代表电子邮箱 /QQ	（填写联系人邮箱） 有关文件我们会邮件发至您邮箱，请收到后注意回执。
报名资料清单			
序号	资料内容	现场核实情况（√或×）	
1	法人或其他组织的营业执照或自然人身份证明		
2	法定代表人身份证明书（法人报名时提供）、法定代表人授权委托书及被授权人身份证明文件（授权代表报名时提供）		

## 第二章 供应商须知

### 《供应商须知前附表》

谈判供应商应仔细阅读本谈判文件的第二章“供应商须知”，下面所列资料是对“供应商须知”的具体补充和说明。如有矛盾，应以本表为准。

序号	条款名称	编列内容
1	采购人	湖北省审计厅
2	监管部门	湖北省政府采购管理处
3	采购代理机构	湖北省招标股份有限公司
4	谈判供应商	详见第一章第二条相关要求
5	采购代理服务费用	<p>根据采购人和采购代理机构签署的委托代理协议书约定：</p> <p>1) 采购代理服务费：<input checked="" type="checkbox"/>由成交供应商支付 <input type="checkbox"/>由采购人支付</p> <p>2) 代理服务费金额：人民币 4000 元整。</p> <p>3) 支付时间：采购代理服务费由成交供应商在领取成交通知书时，向代理机构支付。成交供应商按照成交结果公告公布的服务费金额及支付方式向采购代理机构交纳采购代理服务费，并凭采购代理服务费发票领取成交通知书。</p> <p>4) 支付方式：银行转账、现金支付。</p> <p>5) 银行账户信息</p> <p style="padding-left: 20px;">户名：湖北省招标股份有限公司</p> <p style="padding-left: 20px;">开户行：招商银行水果湖支行</p> <p style="padding-left: 20px;">行号：881098</p> <p style="padding-left: 20px;">账号：12790 54338 10603</p> <p>6) 其他事项：成交供应商交纳采购代理服务费时需携带以下开票资料：①开票单位名称、②纳税人识别号（或统一社会信用代码）、③营业执照或税务登记证地址、④单位联系电话及联系人、⑤开户行及账号。</p>
6	供应商确认收到询价文件澄清或者修改的时间	在收到相应澄清或者修改文件后 <u>24</u> 小时内
7	踏勘现场	<p><input checked="" type="checkbox"/>不组织，供应商自行踏勘</p> <p><input type="checkbox"/>组织，踏勘时间：</p> <p style="padding-left: 20px;">踏勘地点：</p> <p style="padding-left: 20px;">联系人：电话：</p>

序号	条款名称	编列内容
8	对多包采购的规定	详见第一章第一项第3条相关要求
9	备选方案	<input type="checkbox"/> 接受备选方案 <input checked="" type="checkbox"/> 不接受备选方案
10	联合体谈判	<input type="checkbox"/> 接受联合体 <input checked="" type="checkbox"/> 不接受联合体
11	资格证明文件	详见第一章“供应商资格要求”
12	其它资格证明文件	<input checked="" type="checkbox"/> 无 <input type="checkbox"/> 有；具体为： 1、 2、 3、
13	证明响应内容符合谈判文件要求的文件和谈判文件规定的其他资料	证明满足谈判文件第三章中技术要求及商务要求的所有相关规定的内容
14	投标保证金	本项目不设置投标保证金
15	响应文件有效期	<u>90</u> 日历天
16	竞争性谈判响应文件正、副本数量	本次采购项目响应文件正本一份，副本 <u>二</u> 份，电子文档一份，所有响应文件概不退还。响应文件的编制应按每包要求分别装订和封装。
17	样品	提交及退还样品的相关规定：无
18	竞争性谈判响应文件送达地点及递交截止时间	详见第一章《谈判公告》
19	谈判小组人数	谈判小组由采购人代表和评审专家共 <u>3</u> 人组成
20	评审专家的产生	<input checked="" type="checkbox"/> 政府采购专家库中随机抽取 <input type="checkbox"/> 其他：
21	提交最后报价供应商的确定方式	<input checked="" type="checkbox"/> 本项目按照第25.4（1）条规定确定提交最后报价供应商 <input type="checkbox"/> 本项目适用第25.4（2）条规定确定提交最后报价供应商
22	履约保证金	本项目不设履约保证金
23	成交通知书的领取时间	成交通知书与成交结果公告同时发出，成交供应商在成交结果公告发布以后即可领取。

序号	条款名称	编列内容
24	质疑期	供应商认为谈判文件、谈判过程和成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起 7 个工作日内，以书面形式向采购人或采购代理机构提出质疑。
25	质疑回复	采购人或采购代理机构应当在收到供应商的书面质疑后 7 个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复的内容不得涉及商业秘密。
26	是否接受进口产品	<input type="checkbox"/> 接受 <input checked="" type="checkbox"/> 不接受
	支持中小企业政策	<p>供应商如符合工信部联企业〔2011〕300 号文中对中小企业划型标准的，需提供本单位的《中小企业声明函》（详见附件）及企业相关证明材料。根据财库〔2011〕181 号文的相关规定在评定时对小型和微型企业产品的价格给予 6%的扣除，用扣除后的价格参与评审。</p> <p>大中型企业与小型、微型企业组成联合体共同参加非专门面向中小企业的政府采购活动，且联合体协议中约定小型、微型企业的协议合同金额占到联合体协议合同总金额 30%以上的，给予联合体 2%的价格扣除。</p>
	采购节能产品政策	<p>供应商提供的产品如属于政府强制采购节能产品范围，则该产品应在最新一期“节能产品政府采购清单”中。</p> <p>供应商所投产品如属于政府优先采购节能产品范围的，给予该项产品价格 1%的扣除，用扣除后的价格参与评审。</p>
	采购环保产品政策	供应商提供的产品列入最新一期“环境标志产品政府采购清单”的，给予该项产品价格 1%的扣除，用扣除后的价格参与评审。
27	其他要求	无
其他补充事项		
<p>1、除本谈判文件另有规定外，谈判文件中出现的类似于“近三年”或“前三年”、“近五年”或“前五年”均指递交响应文件时间以前3年或前5年，以此类推。如：递交响应文件时间为2017年3月1日，则“近三年”是指2014年3月1日至2017年3月1日。</p> <p>2、关于提交财务审计报告的年份要求：递交响应文件时间如在当年6月30日以前，则近三年指上上个年度往前推算的三年，如递交响应文件时间为2017年3月1日，则“近三年”是指2013年度、2014年度、2015年度。</p> <p>递交响应文件时间如在当年6月30日以后，则近三年是指上个年度往前推算的3年，如递交响应文件时间为2017年7月1日，则“近三年”是指2014年度、2015年度、2016年度。</p>		

### 供应商须知

## 一、 总则

### 1、适用范围

1.1 本竞争性谈判文件仅适用于本次竞争性谈判中所述项目的采购活动。

### 2、定义

2.1 “采购人”：本次谈判的采购人见《供应商须知前附表》。

2.2 “监管部门”：本次谈判的监管部门见《供应商须知前附表》。

2.3 “采购代理机构”：本次谈判的采购代理机构见《供应商须知前附表》。

2.4 “供应商”是指获取本竞争性谈判文件的法人、其他组织或者自然人。

2.5 “谈判供应商”是指

(1) 符合具备《中华人民共和国政府采购法》第二十二条规定的条件；

(2) 符合《供应商须知前附表》的相应条件；

(3) 通过竞争性谈判采购评审标准中资格性和符合性审查的供应商。

2.6 “成交供应商”是指经谈判小组评审推荐，采购人授予合同的供应商。

### 3、工程、货物及服务

3.1 “工程”是指建设工程，包括建筑物和构筑物的新建、改建、扩建及其相关的装修、拆除、修缮等。

3.2 “货物”是指各种形态和种类的物品，包括原材料、燃料、设备、产品等。

3.3 “服务”是指除货物（指各种形态和种类的物品，包括原材料、燃料、设备、产品等）和工程（指建设工程，包括建筑物和构筑物的新建、改建、扩建及其相关的装修、拆除、修缮等）以外的其他政府采购对象。

### 4、费用

4.1 供应商应承担所有与准备和参加谈判有关的费用，不论谈判的结果如何，采购人和采购代理机构均无义务和责任承担这些费用。

4.2 成交服务费：成交供应商须在收到成交通知书时向采购代理机构支付成交服务费。服务费支付标准和方法详见《供应商须知前附表》。

4.3 国家计委计价格[2002]1980 号规定标准收费：

中标金额（万元）	货物招标	服务招标	工程招标
100 以下	1.5%	1.5%	1.0%
100-500	1.1%	0.8%	0.7%
500-1000	0.8%	0.45%	0.55%
1000—5000	0.5%	0.25%	0.35%
5000-10000	0.25%	0.1%	0.2%
10000-100000	0.05%	0.05%	0.05%
100000 以上	0.01%	0.01%	0.01%

注：1、按本表费率计算的收费为招标代理服务全过程的收费基准价格，单独提供编制招标文件(有

标底的(含标底)服务的,可按规定标准的 30%计收。

2、招标代理服务收费按差额定率累进法计算。例如:某工程招标代理业务中标金额为 6000 万元,计算招标代理服务收费额如下:

100 万元 $\times$ 1.0%=1 万元

(500-100)万元 $\times$ 0.7%=2.8 万元

(1000-500)万元 $\times$ 0.55%=2.75 万元

(5000-1000)万元 $\times$ 0.35%=14 万元

(6000-5000)万元 $\times$ 0.2%=2 万元

合计收费=1+2.8+2.75+14+2=22.55(万元)

## 二、竞争性谈判文件

### 5、竞争性谈判文件的构成

5.1 本竞争性谈判文件包括:

- (1) 谈判公告(代谈判邀请函)
- (2) 供应商须知
- (3) 项目采购需求
- (4) 合同草案
- (5) 评审标准
- (6) 响应文件格式
- (7) 采购过程中由采购代理机构发出的澄清和修正文件
- (8) 谈判小组在谈判过程中发出的对本谈判文件的实质性变动

### 6、谈判文件的澄清或修改

6.1 提交响应文件截止之日前,采购人、采购代理机构或者谈判小组可以对已发出的谈判文件进行必要的澄清或者修改,澄清或者修改的内容作为谈判文件的组成部分。

6.2 对谈判文件澄清或者修改的内容可能影响响应文件编制的,采购人、采购代理机构或者谈判小组应当在提交响应文件截止之日3个工作日前,以书面形式通知所有接收谈判文件的供应商,不足3个工作日的,应当顺延提交首次响应文件截止时间。

6.3 供应商在收到澄清或者修改通知后,应在供应商须知前附表规定的时间内以书面形式通知采购人或采购代理机构,确认已收到该澄清或者修改通知。

### 7、现场踏勘

7.1 供应商须知前附表规定组织踏勘现场的,采购代理机构按供应商须知前附表规定的时间、地点组织供应商踏勘项目现场。

7.2 供应商踏勘现场发生的费用自理。

7.3 除采购人和采购代理机构的原因外,供应商自行负责在踏勘现场中所发生的人员伤亡和财产损失。

7.4 采购人在踏勘现场中介绍的项目场地和相关的周边环境情况,供应商在编制响应文件时参考,采购人和采购代理机构不对供应商据此作出的判断和决策负责。

### 三、竞争性谈判响应文件

#### 8、语言和计量单位

8.1 供应商提交的竞争性谈判响应文件以及供应商与采购代理机构或采购人就有关谈判的所有来往函电均应使用中文。供应商提交的支持文件或印刷的文献可以用另一种语言，但相应内容应附有中文翻译本，在解释竞争性谈判响应文件时以中文翻译本为准。

8.2 除非竞争性谈判文件中另有规定，计量单位均采用中华人民共和国法定的计量单位。

#### 9、竞争性谈判响应文件的构成

9.1 供应商编制的竞争性谈判响应文件应包括的内容详见本文件第六章要求。

注：响应文件目录及内容每页须顺序编写页码。

#### 10、竞争性谈判响应文件的编制

10.1 供应商应当按照本谈判文件的要求编制响应文件，并对其提交的响应文件及全部资料的真实性、合法性承担法律责任，并接受采购代理机构对其中任何资料进一步核实的要求。

10.2 供应商应认真阅读本谈判文件中的所有内容，并对本谈判文件提出的要求和条件作出实质性响应。如供应商没有按照本谈判文件的要求提交全部资料，或者没有对本谈判文件在各方面都做出实质性响应的，其响应文件将被视为无效文件。

10.3 供应商应完整地按本谈判文件的要求提交所有资料并按要求的格式填写规定的所有内容，无相应内容可填项的，应填写“无”、“未测试”、“没有相应指标”等明确的回答文字。如未规定格式的，相关格式由供应商自定。

10.4 供应商在编制响应文件时应注意本次采购对多包采购的规定，多包采购的规定见《供应商须知前附表》。

#### 11、谈判报价

11.1 谈判报价包括谈判供应商在首次提交的响应文件中的报价、谈判过程中的报价和最后报价。谈判供应商的报价均应以人民币报价。

11.2 供应商应按照本谈判文件规定的采购需求及合同条款进行报价，并按竞争性谈判文件确定的格式报出。报价中不得包含竞争性谈判文件要求以外的内容，否则，在评审时不予核减。报价中也不得缺漏竞争性谈判文件所要求的内容，否则，其响应文件将被视为无效文件。

11.3 供应商应根据本谈判文件的规定和要求、市场价格水平及其走势、谈判供应商的管理水平、谈判供应商的方案和由这些因素决定的谈判供应商之于本项目的成本水平等提出自己的报价。报价应包含完成本谈判文件采购需求全部内容的所有费用，所有根据本谈判文件或其它原因应由谈判供应商支付的税款和其他应交纳的费用都应包括在报价中。但谈判供应商不得以低于其成本的价格进行报价。

11.4 供应商在响应文件中注明免费的项目将视为包含在报价中。

11.5 每一种采购内容只允许有一个报价，否则其响应文件将被视为无效文件。

11.6 成交供应商的报价在合同执行过程中是固定不变的，不得以任何理由予以变更。

## 12、备选方案

12.1是否允许备选方案见《供应商须知前附表》。不允许有备选方案的，若在响应文件中提交了备选方案，其响应文件将被视为无效文件。

## 13、联合体

13.1本次采购是否允许联合体参加详见《供应商须知前附表》。

13.2本次采购允许联合体参与谈判的，联合体各方不得再单独或者与其他供应商另外组成联合体参加本项目的谈判，否则相关响应文件均告无效。

## 14、供应商资格证明文件

14.1供应商应在响应文件提交证明其有资格参加谈判的证明文件，证明文件应包括：详见第六章“资格证明文件”。

14.2谈判文件要求供应商应提交的其它资格证明文件，应提交的其它资格证明文件见《供应商须知前附表》。

14.3除本须知14.1要求的资格证明文件外，如国家法律法规对市场准入有要求的还应提交相关资格证明文件。

14.4所有证书、证明文件包括按要求提供的官网截图必须是真实可查证的，须注明资料来源。资格证明文件应为原件的扫描件，响应文件中须编入清晰的扫描件或复印件。所有证明材料须清晰可辨认，如因证明材料模糊无法辨认，缺页、漏页导致无法进行评审认定的责任由供应商自负。如发现弄虚作假将按照有关规定严肃处理。证明材料仅限于供应商本身，参股或控股单位及独立法人子公司的材料不能作为证明材料，但供应商兼并的企业的材料可作为证明材料。

## 15、证明报价内容、服务合格性和符合竞争性谈判文件规定的文件

15.1证明报价内容符合竞争性谈判文件要求的文件和竞争性谈判文件规定的其他资料，具体要求见《供应商须知前附表》。

## 16、响应文件有效期

16.1响应文件有效期从谈判结束之日起计算，本次采购响应文件有效期见《供应商须知前附表》，谈判供应商承诺的响应文件有效期不足的，其响应文件将被视为无效文件。

16.2特殊情况下，在原响应文件有效期截止之前，采购代理机构或采购人可要求供应商延长响应文件有效期。需要延长响应文件有效期时，采购代理机构或采购人将以书面形式通知所有谈判供应商，供应商应以书面形式答复是否同意延长响应文件有效期。

16.3供应商同意延长的，其保证金有效期相应延长，但不得要求或被允许修改或撤销其响应文件；供应商拒绝延长的，其响应文件在原响应文件有效期满后将不再有效，供应商有权收回其保证金。

## 17、竞争性谈判响应文件的装订、签署和数量

17.1供应商提交的响应文件应包括正本、副本、完整的电子文档及单独提供的法定代表人授权委托书（或法定代表人身份证明书）、报价一览表、优惠声明（如有）。本次谈判供应商提交



响应文件正、副本和电子文档的数量见《供应商须知前附表》。

每套响应文件须清楚地标明“正本”、“副本”，响应文件的副本可采用正本的复印件，若副本与正本不符，以正本为准；如单独提供的法定代表人授权委托书（或法定代表人身份证明书）、报价一览表、优惠声明（如有）与响应文件正本不符，以正本为准。电子文档与纸质文件不符，以纸质文件为准。

17.2 正本需打印或用不褪色墨水书写，并由法定代表人或授权代表签字并加盖公章。由授权代表签字的，响应文件中应提交《法定代表人授权书》。供应商为自然人的，由供应商本人签字并附身份证明。

17.3 竞争性谈判响应文件中的任何行间插字、涂改和增删，必须由法定代表人或授权代表在旁边签字才有效。

17.4 响应文件应当采用不可拆卸的方法装订，对未经装订的竞争性谈判响应文件可能发生的文件散落或缺损及由此产生的后果由谈判供应商承担。

#### **四、 竞争性谈判响应文件的递交**

##### **18、竞争性谈判响应文件的密封和标记**

18.1 响应文件的正本、所有副本和电子文档必须密封和加盖供应商公章后递交，包装上应注明项目编号：项目名称、包号、供应商名称及“（谈判时间）前不得启封”的字样。

18.2 为方便谈判记录，供应商还应将一份《报价一览表》（原件）与一份《法定代表人授权书》（原件）、保证金缴纳证明（复印件）及报价优惠声明（如果有的话）单独密封提交，除需按上款要求注明外还应在信封上标明“报价一览表”字样。

18.3 未按要求密封和加写标记的响应文件为无效文件，采购人、采购代理机构将拒收。

18.4 要求在谈判时提交样品的，应在样品上标明谈判供应商名称。有关提交及退还样品的相关规定见《供应商须知前附表》。

##### **19、竞争性谈判响应文件的送达地点及截止时间**

19.1 截止时间是竞争性谈判文件中规定的首次送达、提交响应文件的最后时间。本次谈判响应文件的送达地点及截止时间见《供应商须知前附表》。

##### **20、迟交的竞争性谈判响应文件**

20.1 在本次谈判递交响应文件的截止时间以后送达的响应文件，不论何种原因，采购代理机构将拒收。

##### **21、竞争性谈判响应文件的补充、修改或者撤回**

21.1 在提交响应文件截止时间前，供应商可以对已提交的响应文件进行补充、修改或者撤回。供应商需要补充、修改或者撤回响应文件时，应以书面形式通知采购人、采购代理机构。补充、修改的内容是响应文件的组成部分，补充、修改的内容与响应文件不一致的，以补充、修改的内容为准。

21.2 从提交响应文件截止时间至谈判有效期期满这段时间，供应商不得修改或撤销其响应文

件，否则其保证金将不予以退还。

21.3 供应商所提交的响应文件在谈判结束后，无论成交与否都不退还。

## 五、谈判程序

### 22、谈判小组

22.1 采购人依照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》及现行法律规定组建谈判小组，谈判小组由采购人代表和评审专家共3人以上单数组成。谈判小组人数详见《供应商须知前附表》。

22.2 谈判小组中的评审专家人数不少于谈判小组成员总数的2/3，评审专家的产生详见《供应商须知前附表》。

22.3 谈判小组所有成员按事先抽取的谈判顺序，集中与单一供应商分别进行谈判，并给予所有参加谈判的供应商平等的谈判机会。

### 23、谈判代表

23.1 谈判供应商法定代表人或授权代表应携带本人身份证明参加谈判，授权代表参加谈判的，还应携带法定代表人授权书原件。谈判代表经谈判小组核对身份后，方可参加谈判。

### 24、资格审查和符合性审查

24.1 在正式谈判前，谈判小组按照本谈判文件第五章规定的标准，对供应商进行资格性审查和符合性审查，通过资格性审查和符合性审查的供应商方可进入谈判程序。资格性审查和符合性审查内容详见第五章“评审标准”。

### 25、谈判

25.1 谈判小组将根据本谈判文件第五章规定的程序、方法和标准与供应商进行谈判。在谈判过程中，谈判的任何一方不得透露与谈判有关的其他供应商的技术资料、价格和其他信息。

25.2 谈判小组可以根据谈判文件和谈判情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动谈判文件中的其他内容。实质性变动的内容，须经采购人代表确认。对谈判文件作出的实质性变动是谈判文件的有效组成部分，谈判小组将以书面形式同时通知所有谈判供应商。

25.3 供应商应当按照谈判文件的变动情况和谈判小组的要求重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

#### 25.4 最后报价

(1) 谈判文件能够详细列明采购标的的技术、服务要求的，谈判结束后，谈判小组应当要求所有继续参加谈判的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于3家。

已提交响应文件的供应商，在提交最后报价之前，可以根据谈判情况退出谈判。采购人、采购代理机构应当退还退出谈判的供应商的保证金。

(2) 谈判文件不能详细列明采购标的的技术、服务要求，需经谈判由供应商提供最终设计方案或解决方案的，谈判结束后，谈判小组应当按照少数服从多数的原则投票推荐3家以上供应商的设计方案或者解决方案，并要求其在规定时间内提交最后报价。本采购项目提交最后报价供应商的确定方式详见《供应商须知前附表》。

25.5如有需要，谈判小组可进行多轮谈判，直至最终确定谈判文件中的技术、服务要求以及合同草案条款。

25.6 谈判小组审核完最终报价后，根据谈判文件规定的评审程序、方法和标准推荐成交候选供应商或根据采购人的书面授权直接确定成交供应商。

25.7采购代理机构对谈判过程和重要谈判内容进行记录，谈判双方在记录上签字确认。

## 26、保密

26.1凡是属于审查、澄清、评价和比较的有关资料以及授标意向等，采购人、采购代理机构、监管人员、谈判小组及有关工作人员均不得向供应商或其它无关的人员透露。

## 六、 成交与签订合同

### 27、合同授予标准

27.1 采购人将把合同授予排名第一的供应商，特殊情况按本须知28.3的规定执行。

### 28、签订合同

28.1 竞争性谈判文件对履约保证金有规定的，成交供应商应按规定在签订合同前缴纳履约保证金。有关履约保证金的规定见《供应商须知前附表》。

28.2 采购人与成交供应商应当在成交通知书发出之日起30日内，按照谈判文件确定的合同文本以及采购标的、规格型号、采购金额、采购数量、技术和服务要求等事项签订政府采购合同。成交通知书发出时间详见《供应商须知前附表》。

采购人不得向成交供应商提出超出谈判文件以外的任何要求作为签订合同的条件，不得与成交供应商订立背离谈判文件确定的合同文本以及采购标的、规格型号、采购金额、采购数量、技术和服务要求等实质性内容的协议。

采购人应当自政府采购合同签订之日起2个工作日内，将政府采购合同在省级以上人民政府指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

28.3成交供应商拒绝签订政府采购合同的，采购人可以按照《政府采购非招标采购方式管理办法》（财政部第74号令）第三十六条第二款、第四十九条第二款规定的原则确定其他供应商作为成交供应商并签订政府采购合同，也可以重新开展采购活动。拒绝签订政府采购合同的成交供应商不得参加对该项目重新开展的采购活动。

28.4 签订政府采购合同后2个工作日内，采购人应将政府采购合同副本报同级政府采购监管部门备案。

28.5 采购代理机构将配合采购人与成交供应商签订政府采购合同。采购人与成交供应商应按竞争性谈判文件要求和成交供应商的竞争性谈判响应文件承诺订立书面合同，不得超出竞争性

谈判文件和成交供应商竞争性谈判响应文件的范围，也不得再行订立背离合同实质性内容的其他协议。

28.6 除不可抗力等因素外，成交通知书发出后，采购人改变成交结果，或者成交供应商拒绝签订政府采购合同的，应当承担相应的法律责任。

## 七、质疑和投诉

### 29、质疑

29.1 供应商认为谈判文件、谈判过程和成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人或采购代理机构提出质疑。

29.2 质疑书应当包括下列主要内容：

- (1) 质疑人的名称、地址、联系人及联系电话等；
- (2) 被质疑人的名称、地址、联系人及联系电话等；
- (3) 质疑项目名称及编号、质疑事项和明确的请求；
- (4) 质疑事项的事实根据、法律依据及其他必要的证明材料；质疑人提供的证明材料属于其他供应商投标（响应）文件未公开内容的，应当提供书面材料证明其合法来源；
- (5) 提出质疑的日期；
- (6) 质疑人的署名及签章（质疑人为自然人的，应当由本人签字；质疑人为法人或者其他组织的，应当由法定代表人或者主要负责人签字盖章并加盖公章）；
- (7) 法人授权委托书（质疑人或法人委托代理人办理质疑事务的，应当提供授权委托书，授权委托书应当载明委托代理的具体权限和事项）。

质疑书不符合上述要求的，采购人或代理机构应书面告知具体事项，质疑人应当按要求进行修改或补充，并在质疑有效期限内提交。

### 30、质疑回复

30.1 采购人或采购代理机构应当在收到供应商的书面质疑后7个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复的内容不得涉及商业秘密。

30.2 质疑答复应当包括下列内容：

- (1) 质疑人的名称、地址、联系人及联系电话；
- (2) 采购人或采购代理机构（委托项目一并列出）的名称、地址、联系人及联系电话；
- (3) 受理质疑的日期、质疑项目名称及编号、质疑事项；
- (4) 质疑事项答复的具体情况、事实根据、法律依据；
- (5) 告知质疑人依法投诉的权利和投诉方式；
- (6) 质疑答复日期。

### 31、投诉

31.1 质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后15个工作日内向同级政府采购监督管理部门投诉。供应

商投诉应当有明确的请求和必要的证明材料，且投诉的事项不得超出已质疑事项的范围。

31.2 政府采购监督管理部门应当在收到投诉后30个工作日内，对投诉事项作出处理决定，并以书面形式通知投诉人和与投诉事项有关的当事人。财政部门处理投诉事项，需要检验、检测、鉴定、专家评审以及需要投诉人补正材料的，所需时间不计算在投诉处理期限内。

## 八、政府采购政策

32.1 除非“**供应商须知前附表**”中有特殊规定，本项目所采购的货物应当为中华人民共和国境内提供。

32.2 为促进中小企业发展，本项目供应商如符合工信部联企业〔2011〕300号文中对中小企业划型标准的，可按照“**供应商须知前附表**”中相关规定，对产品的价格给予一定比例的扣除，用扣除后的价格参与评审。具体扣除比例详见“**供应商须知前附表**”。

32.3 根据《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51号）规定，供应商所投产品如属于政府强制采购节能产品范围，则该产品必须在最新一期“节能产品政府采购清单”中。供应商所投产品如属于政府优先采购节能产品范围，可按照“**供应商须知前附表**”中相关规定，对该项产品的价格给予一定比例的扣除，用扣除后的价格参与评审。具体扣除比例详见“**供应商须知前附表**”。

（1）“节能产品政府采购清单”以中华人民共和国财政部网站（<http://www.mof.gov.cn>）、中国政府采购网（<http://www.ccgp.gov.cn>）、国家发展改革委网站（<http://hzs.ndrc.gov.cn>）和中国质量认证中心网站（<http://www.cqc.com.cn>）公示为准。

（2）投标产品如属于政府优先采购节能产品范围的，须提供如下相关证明资料：

a 投标产品所在当期节能清单页面截图（包含制造商、品牌、产品型号、节字标志认证证书号、认证证书有效截止日期），复印件加盖供应商公章；

b 投标产品节能清单产品查询系统查询结果截图；

（<http://www.ccgp.gov.cn/search/jnqdcxaxun.htm>）（复印件加盖供应商公章）

c 政府优先采购节能产品范围的投标产品的单独分项报价。

32.4 根据财政部、国家环保总局《关于环境标志产品政府采购实施的意见》（财库〔2006〕90号）文件规定。为积极推进环境友好型社会建设，发挥政府采购的环境保护政策功能，应当优先采购环境标志产品政府采购清单（以下简称“环保清单”）中的产品，对符合该文件规定的供应商享受如下政府政策评审优惠：

（1）投标产品列入最新一期环保清单的，对该项产品的价格给予一定比例的扣除，用扣除后的价格参与评审。具体扣除比例详见“**供应商须知前附表**”。

（2）如供应商所提供的工程项目中投标产品符合以上文件政策的，须提供如下证明资料

a 投标产品所在当期环保清单页面截图（包含企业名称、品牌、产品名称型号规格、中国环境标志认证证书编、认证证书有效截止日期）；（复印件加盖供应商公章）

b 投标产品环保清单查询系统查询结果截图；

(<http://www.ccgp.gov.cn/search/hbqdchaxun.htm>) (复印件加盖供应商公章)

c 投标产品属于环保清单内产品须单独分项报价。

32.5 上述政府采购政策优惠须经谈判小组评审后执行，未提供单独分项报价或证明资料不全的不给予价格扣除。

## 九、其他要求

见《供应商须知前附表》。

## 十、适用法律

采购人、采购代理机构及供应商的一切招标投标活动均适用于《政府采购法》及相关规定。

## 第三章项目采购需求

### 一、项目概况

- 1、项目名称：湖北省审计厅网络安全等级测评项目
- 2、项目工期：合同签订后 30 个工作日内完成等级测评和安全建设方案设计

### 二、项目需求

名称	数量
审计大数据平台系统（第四级）	1 项
审计专网系统（第三级）	1 项
安全等级保护合规咨询服务	1 项

根据相关文件及标准要求，对湖北省审计厅需要进行测评的信息系统的信息系统实施安全等级保护定级、备案、测评、协助整改等工作，根据“关于传发《信息安全等级保护测评报告模版（2015 年版）》的通知（公信安[2014]2866 号）”文件的精神，出具符合格式要求的等级测评报告。

### 三、技术服务要求

#### 3.1定级备案服务

协助湖北省审计厅对需要进行测评的信息系统进行定级、备案材料的编写，协助湖北省审计厅到公安监管等部门办理备案手续，确保信息系统安全保护等级定级准确、备案完整。

#### 3.2信息安全等级保护测评服务

依据《GB/T 22239-2008 信息安全技术信息系统安全等级保护基本要求》、《GB/T 28448-2012 信息安全技术信息系统安全等级保护测评要求》、《GB/T 20984-2007 信息安全技术信息安全风险评估规范》、《GB/T 22080-2008 信息技术安全技术信息安全管理体系要求》、《GB/T 22081-2008 信息技术安全技术信息安全管理实用规则》等标准的要求，对湖北省审计厅需要进行测评的信息系统进行等级测评，出具符合国家等级保护格式要求的等级测评报告。测评范围为项目目标所涉及的机房基础设施、网络环境、主机层面、应用层、数据库层及相关安全辅助设备与管理制度。服务目标为项目目标最终通过公安部门及相关部门的等级保护检查要求。

测评内容应包括但不限于以下内容：

(1) 安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据安全等五个方面的安全测评；

(2) 安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评；

(3) 系统整体测评：控制间测评、层面间测评、区域间测评、系统结构安全测评。

### 3.3 第三级系统测评内容

#### 3.3.1 物理安全

测评对象主要为主机房，涉及工作单元 10 个，具体如下表：

序号	工作单元名称	测评指标
1	物理位置的选择	a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。
		b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。
2	物理访问控制	a) 机房出入口应安排专人值守，控制、鉴别和记录进入的人员；
		b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。
		c) 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；
		d) 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。
3	防盗窃和防破坏	a) 应将主要设备放置在机房内；
		b) 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记；
		c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
		d) 应对介质分类标识，存储在介质库或档案室中；
		e) 应利用光、电等技术设置机房防盗报警系统；
		f) 应对机房设置监控报警系统。
4	防雷击	a) 机房建筑应设置避雷装置；



序号	工作单元名称	测评指标
		b) 应设置防雷保安器，防止感应雷；
		c) 机房应设置交流电源地线。
5	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；
		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；
		c) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。
6	防水和防潮	a) 水管安装，不得穿过机房屋顶和活动地板下；
		b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		c) 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；
		d) 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。
7	防静电	a) 关键设备应采用必要的接地防静电措施；
		b) 机房应采用防静电地板。
8	温湿度控制	a) 机房应设置温、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。
9	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；
		b) 应提供短期的备用电力供应，至少满足关键设备在断电情况下的正常运行要求；
		c) 应设置冗余或并行的电力电缆线路为计算机系统供电；
		d) 应建立备用供电系统。
10	电磁防护	a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；
		b) 电源线和通信线缆应隔离铺设，避免互相干扰；
		c) 应对关键设备和磁介质实施电磁屏蔽。

### 3.3.2 网络安全

测评对象主要为网络互联设备、网络安全设备以及网络拓扑结构等三大类，具体为：核心交换机、接入交换机等网络互连设备；防火墙等网络安全设备；信息系统的整体网络拓扑结构，涉及工作单元 6 个，具体如下表：

序号	工作单元名称	测评指标
1	结构安全	a) 应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
		b) 应保证网络各个部分的带宽满足业务高峰期需要；
		c) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；
		d) 应绘制与当前运行情况相符的网络拓扑结构图；
		e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；
		f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。
2	访问控制	a) 应在网络边界部署访问控制设备，启用访问控制功能；
		b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；
		c) 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；
		d) 应在会话处于非活跃一定时间或会话结束后终止网络连接；
		e) 应限制网络最大流量数及网络连接数；
		f) 重要网段应采取技术手段防止地址欺骗；
		g) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统资源访问，控制粒度为单个用户；

序号	工作单元名称	测评指标
		h)应限制具有拨号访问权限的用户数量。
3	安全审计	a)应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；
		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；
		c)应能够根据记录数据进行分析，并生成审计报表；
		d)应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。
4	边界完整性检查	a)应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；
		b)应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。
5	入侵防范	a)应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
		b)当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
6	恶意代码防范	a)应在网络边界处对恶意代码进行检测和清除。
		b)应维护恶意代码库的升级和检测系统的更新。
7	网络设备防护	a)应对登录网络设备的用户进行身份鉴别；
		b)应对网络设备的管理员登录地址进行限制；
		c)网络设备用户的标识应唯一；
		d)主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；
		e)身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
		f)应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
		g)当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
		h)应实现设备特权用户的权限分离。

### 3.3.3 主机安全

测评对象主要为主要服务器和重要终端设备的操作系统、数据库，如 AIX、Linux、Windows、MS-SQL Server、Oracle 等，涉及工作单元 7 个，具体如下表：

序号	工作单元名称	测评指标
1	身份鉴别	a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
		b) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
		c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
		d) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；
		e) 为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；
		f) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。
2	访问控制	a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；
		b) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
		c) 应实现操作系统和数据库系统特权用户的权限分离；
		d) 应严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令；
		e) 应及时删除多余的、过期的账户，避免共享账户的存在；
		f) 应对重要信息资源设置敏感标记；
		g) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。
3	安全审计	a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；
		b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

序号	工作单元名称	测评指标
		c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
		d) 应能够根据记录数据进行分析，并生成审计报表；
		e) 应保护审计进程，避免受到未预期的中断；
		f) 应保护审计记录，避免受到未预期的删除、修改或覆盖等。
4	剩余信息保护	a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
		b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。
5	入侵防范	a) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
		b) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；
		c) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。
6	恶意代码防范	a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；
		b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；
		c) 应支持防恶意代码的统一管理。
7	资源控制	a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；
		b) 应根据安全策略设置登录终端的操作超时锁定；
		c) 应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；
		d) 应限制单个用户对系统资源的最大或最小使用限度；

序号	工作单元名称	测评指标
		e) 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

### 3.3.4 应用安全

序号	工作单元名称	测评指标
1	身份鉴别	a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
		b) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；
		c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
		d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
2	访问控制	a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
		b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
		c) 应由授权主体配置访问控制策略，并严格限制默认账户的访问权限；
		d) 应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
		e) 应具有对重要信息资源设置敏感标记的功能；
		f) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。
3	安全审计	a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；
		b) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
		c) 审计记录的内容至少应包括事件的日期、事件、发起者信息、类型、描述和结果等；

		d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。
4	剩余信息保护	a) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
		b) 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。
5	通信完整性	a) 应采用密码技术保证通信过程中数据的完整性。
6	通信保密性	a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；
		b) 应对通信过程中的整个报文或会话过程进行加密。
7	抗抵赖	a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
		b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。
8	软件容错	a) 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数据格式或长度符合系统设定要求。
		b) 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。
9	资源控制	a) 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
		b) 应能够对系统的最大并发会话连接数进行限制；
		c) 应能够对单个账户的多重并发会话进行；
		d) 应能够对一个时间段内可能的并发会话连接数进行限制；
		e) 应能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；
		f) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警；
		g) 应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源；

## 3.3.5 数据安全及备份恢复

序号	工作单元名称	测评指标
1	数据完整性	a)应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
		b)应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。
2	数据保密性	a)应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；
		b)应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。
3	数据备份和恢复	a)应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；
		b)应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；
		c)应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；

## 3.3.6 安全管理机构

序号	工作单元名称	测评指标
1	岗位设置	a) 应设立信息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；
		b) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；
		c) 应成立指导和管理信息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委任或授权；
		d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。
2	人员配置	a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；
		b) 应配备专职安全管理员，不可兼任；



序号	工作单元名称	测评指标
		c) 关键事务岗位应配备多人共同管理。
3	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； 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； 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； d) 应记录审批过程并保存审批文档。
4	沟通与合作	a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题； b) 应加强与兄弟单位、公安机关、电信公司的合作与沟通； c) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通； d) 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； e) 应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。
5	审核与检查	a) 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； b) 应由内部人员或上级单位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； 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； d) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

## 3.3.7 安全管理制度

序号	工作单元名称	测评指标
1	管理制度	a) 应制定信息安全工作的总体方针和安全策略,说明机构安全工作的总体目标、范围、原则和安全框架等;
		b) 应对安全管理活动中的各类管理内容建立安全管理制度;
		c) 应对要求管理人员或操作人员执行的日常管理操作建立操作规程;
		d) 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。
2	制定与发布	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;
		b) 安全管理制度应具有统一的格式,并进行版本控制;
		c) 应组织相关人员对制定的安全管理制度进行论证和审定
		d) 安全管理制度应通过正式、有效的方式发布;
		e) 安全管理制度应注明发布范围,并对收发文进行登记。
3	评审和修订	a) 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定;
		b) 应定期或不定期对安全管理制度进行检查和审定,对存在不足或需要改进的安全管理制度进行修订。

## 3.3.8 人员安全管理

序号	工作单元名称	测评指标
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;
		b) 应严格规范人员录用过程,对被录用人的身份、背景、专业资格和资质等进行审查,对其所具有的技术技能进行考核;
		c) 应签署保密协议;
		d) 应从内部人员中选拔从事关键岗位的人员,并签署岗位安全协议。

序号	工作单元名称	测评指标
2	人员离岗	a) 应严格规范人员离岗过程, 及时终止离岗员工的所有访问权限;
		b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备;
		c) 应办理严格的调离手续, 关键岗位人员离岗须承诺调离后的保密义务后方可离开。
3	人员考核	a) 应定期对各个岗位的人员进行安全技能及安全认知的考核;
		b) 应对关键岗位的人员进行全面、严格的安全审查和技能考核;
		c) 应对考核结果进行记录并保存。
4	安全意识教育和培训	a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训;
		b) 应对安全责任和惩戒措施进行书面规定并告知相关人员, 对违反违背安全策略和规定的人员进行惩戒;
		c) 应对定期安全教育和培训进行书面规定, 针对不同岗位制定不同的培训计划, 对信息安全基础知识、岗位操作规程等进行培训;
		d) 应对安全教育和培训的情况和结果进行记录并归档保存。
5	外部人员访问管理	a) 应确保在外部人员访问受控区域前先提出书面申请, 批准后由专人全程陪同或监督, 并登记备案;
		b) 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定, 并按照规定执行。

### 3.3.9 系统建设管理

序号	工作单元名称	测评指标
1	系统定级	a) 应明确信息系统的边界和安全保护等级;
		b) 应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由;
		c) 应组织相关部门和有关安全技术专家对信息系统定

序号	工作单元名称	测评指标
		级结果的合理性和正确性进行论证和审定；
		d) 应确保信息系统的定级结果经过相关部门的批准。
2	安全方案设计	a) 应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；
		b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；
		c) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；
		d) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；
		e) 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。
3	产品采购	a) 应确保安全产品采购和使用符合国家的有关规定；
		b) 应确保密码产品采购和使用符合国家密码主管部门的要求；
		c) 应指定或授权专门的部门负责产品的采购；
		d) 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。
4	自行软件开发	a) 应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；
		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；
		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；
		d) 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；
		e) 应确保对程序资源库的修改、更新、发布进行授权和批准。
5	外包软件开发	a) 应根据开发需求检测软件质量；
		b) 应在软件安装之前检测软件包中可能存在的恶意代

序号	工作单元名称	测评指标
		码；
		c) 应要求开发单位提供软件设计的相关文档和使用指南；
		d) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门。
6	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；
		b) 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；
		c) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。
7	测试验收	a) 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；
		b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
		c) 应对系统测试验收的控制方法和人员行为准则进行书面规定；
		d) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
		e) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。
8	系统交付	a) 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
		b) 应对负责系统运行维护的技术人员进行相应的技能培训；
		c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；
		d) 应对系统交付的控制方法和人员行为准则进行书面规定；
		e) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。
9	系统备案	a) 应指定专门的部门或人员负责管理系统定级的相关

序号	工作单元名称	测评指标
		材料，并控制这些材料的使用；
		b) 应将系统等级及相关材料报系统主管部门备案；
		c) 应将系统等级及其他要求的备案材料报相应公安机关备案。
10	等级测评	a) 在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；
		b) 应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
		c) 应选择具有国家相关技术资质和安全资质的测评单位进行等级测评；
		d) 应指定或授权专门的部门或人员负责等级测评的管理。
11	安全服务商选择	a) 应确保安全服务商的选择符合国家的有关规定；
		b) 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；
		c) 应确保选定的安全服务商提供技术培训和承诺，必要的与其签订服务合同。

### 3.3.10 系统运维管理

序号	工作单元名称	测评指标
1	环境管理	a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
		b) 应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
		c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
		d) 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应

序号	工作单元名称	测评指标
		确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。
2	资产管理	<p>a) 应编制并保存与信息系统相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容;</p> <p>b) 应建立资产安全管理制度, 规定信息系统资产管理的责任人员或责任部门, 并规范资产管理和使用的行为;</p> <p>c) 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;</p> <p>d) 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。</p>
3	介质管理	<p>a) 应建立介质安全管理制度, 对介质的存放环境、使用、维护和销毁等方面作出规定;</p> <p>b) 应确保介质存放在安全的环境中, 对各类介质进行控制和保护, 并实行存储环境专人管理;</p> <p>c) 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, 对介质归档和查询等进行登记记录, 并根据存档介质的目录清单定期盘点;</p> <p>d) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理, 对带出工作环境的存储介质进行内容加密和监控管理, 对送出维修或销毁的介质应首先清除介质中的敏感数据, 对保密性较高的存储介质未经批准不得自行销毁;</p> <p>e) 应根据数据备份的需要对某些介质实行异地存储, 存储地的环境要求和管理方法应与本地相同;</p> <p>f) 应对重要介质中的数据和软件采取加密存储, 并根据所承载数据和软件的重要程度对介质进行分类和标识管理。</p>
4	设备管理	<p>a) 应对信息系统相关的各种设备 (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;</p> <p>b) 应建立基于申报、审批和专人负责的设备安全管理制度, 对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理;</p> <p>c) 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、涉</p>

序号	工作单元名称	测评指标
		外维修和服务的审批、维修过程的监督控制等；
		d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理,按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
		e) 应确保信息处理设备必须经过审批才能带离机房或办公地点。
5	监控管理和安全管理中心	a) 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警,形成记录并妥善保存；
		b) 应组织相关人员定期对监测和报警记录进行分析、评审,发现可疑行为,形成分析报告,并采取必要的应对措施；
		c) 应建立安全管理中心,对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。
6	网络安全管理	a) 应指定专人对网络进行管理,负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
		b) 应建立网络安全管理制度,对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；
		c) 应根据厂家提供的软件升级版本对网络设备进行更新,并在更新前对现有的重要文件进行备份；
		d) 应定期对网络系统进行漏洞扫描,对发现的网络安全漏洞进行及时的修补；
		e) 应实现设备的最小服务配置,并对配置文件进行定期离线备份；
		f) 应保证所有与外部系统的连接均得到授权和批准；
		g) 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；
		h) 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。
7	系统安全管理	a) 应根据业务需求和系统安全分析确定系统的访问控制策略；
		b) 应定期进行漏洞扫描,对发现的系统安全漏洞及时



序号	工作单元名称	测评指标
		进行修补；
		c) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；
		d) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；
		e) 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；
		f) 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
		g) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。
8	恶意代码防范管理	a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
		b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
		c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；
		d) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。
9	密码管理	a) 应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。
10	变更管理	a) 应确认系统中要发生的变更，并制定变更方案；
		b) 应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告；
		c) 应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；
		d) 应建立中止变更并从失败变更中恢复的文件化程

序号	工作单元名称	测评指标
		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。
11	备份和恢复管理	<p>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；</p> <p>b) 应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；</p> <p>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，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；</p> <p>d) 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；</p> <p>e) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。</p>
12	安全事件处理	<p>a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；</p> <p>b) 应制定安全事件报告和处置管理制度，明确安全事件的类型，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；</p> <p>c) 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；</p> <p>d) 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；</p> <p>e) 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，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；</p> <p>f) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。</p>
13	应急预案管理	<p>a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；</p> <p>b) 应从人力、设备、技术和财务等方面确保应急预案</p>

序号	工作单元名称	测评指标
		的执行有足够的资源保障；
		c) 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；
		d) 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
		e) 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

### 3.4第四级系统测评内容

#### 3.4.1 物理安全

序号	工作单元名称	测评指标
1	物理位置的选择	a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。
		b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。
2	物理访问控制	a) 机房出入口应安排专人值守并配置电子门禁系统，控制、鉴别和记录进入的人员；
		b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。
		c) 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；
		d) 重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。
3	防盗窃和防破坏	a) 应将主要设备放置在机房内；
		b) 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记；
		c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
		d) 应对介质分类标识，存储在介质库或档案室中；
		e) 应利用光、电等技术设置机房防盗报警系统；

序号	工作单元名称	测评指标
		f) 应对机房设置监控报警系统。
4	防雷击	a) 机房建筑应设置避雷装置；
		b) 应设置防雷保安器，防止感应雷；
		c) 机房应设置交流电源地线。
5	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；
		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；
		c) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。
6	防水和防潮	a) 水管安装，不得穿过机房屋顶和活动地板下；
		b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		c) 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；
		d) 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。
7	防静电	a) 关键设备应采用必要的接地防静电措施；
		b) 机房应采用防静电地板。
		c) 应采用静电消除器等装置，减少静电的产生。
8	温湿度控制	a) 机房应设置温、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。
9	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；
		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；
		c) 应设置冗余或并行的电力电缆线路为计算机系统供电；
		d) 应建立备用供电系统。
10	电磁防护	a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

序号	工作单元名称	测评指标
		b) 电源线和通信线缆应隔离铺设，避免互相干扰；
		c) 应对关键区域实施电磁屏蔽。

### 3.4.2 网络安全

序号	工作单元名称	测评指标
1	结构安全	a) 应保证网络设备的业务处理能力具备冗余空间，满足业务高峰期需要； b) 应保证网络各个部分的带宽满足业务高峰期需要； c) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径； d) 应绘制与当前运行情况相符的网络拓扑结构图； e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段； f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。
2	访问控制	a) 应在网络边界部署访问控制设备，启用访问控制功能； b) 应不允许数据带通用协议通过； c) 应根据数据的敏感标记允许或拒绝数据通过； d) 应不开放远程拨号访问功能。
3	安全审计	a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录； 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； c) 应能够根据记录数据进行分析，并生成审计报告； d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

序号	工作单元名称	测评指标
		e) 应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生；
		f) 应根据信息系统的统一安全策略，实现集中审计，时钟保持与时钟服务器同步。
4	边界完整性检查	a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确确定出位置，并对其进行有效阻断；
		b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确确定出位置，并对其进行有效阻断。
5	入侵防范	a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
		b) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警及自动采取相应动作。
6	恶意代码防范	a) 应在网络边界处对恶意代码进行检测和清除。
		b) 应维护恶意代码库的升级和检测系统的更新。
7	网络设备防护	a) 应对登录网络设备的用户进行身份鉴别；
		b) 应对网络设备的管理员登录地址进行限制；
		c) 网络设备用户的标识应唯一；
		d) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；
		e) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
		f) 网络设备用户的身份鉴别信息至少应有一种是不可伪造的；
		g) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
		h) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
		i) 应实现设备特权用户的权限分离。

## 3.4.3 主机安全

序号	工作单元名称	测评指标
1	身份鉴别	a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
		b) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
		c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
		d) 应设置鉴别警示信息，描述未授权访问可能导致的后果；
		e) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；
		f) 为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；
		g) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，并且身份鉴别信息至少有一种是不可伪造的。
2	安全标记	应对所有主体和客体设置敏感标记；
3	访问控制	a) 应依据安全策略和所有主体和客体设置的敏感标记控制主体对客体的访问；
		b) 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、记录和字段级。
		c) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
		d) 应实现操作系统和数据库系统特权用户的权限分离；
		e) 应严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令；
		f) 应及时删除多余的、过期的账户，避免共享账户的存在；
4	可信路径	a) 在系统对用户进行身份鉴别时，系统与用户之间应能够建立一条安全的信息传输路径。
		b) 在用户对系统进行访问时，系统与用户之间应能够建立一条安全的信息传输路径。

序号	工作单元名称	测评指标
5	安全审计	a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；
		b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；
		c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
		d) 应能够根据记录数据进行分析，并生成审计报表；
		e) 应保护审计进程，避免受到未预期的中断；
		f) 应保护审计记录，避免受到未预期的删除、修改或覆盖等。
		g) 应能够根据信息系统的统一安全策略，实现集中审计。
6	剩余信息保护	a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
		b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。
7	入侵防范	a) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
		b) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；
		c) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。
8	恶意代码防范	a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；
		b) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；
		c) 应支持防恶意代码的统一管理。
9	资源控制	a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；



序号	工作单元名称	测评指标
		b)应根据安全策略设置登录终端的操作超时锁定；
		c)应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；
		d)应限制单个用户对系统资源的最大或最小使用限度；
		e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

### 3.4.4 应用安全

序号	工作单元名称	测评指标
1	身份鉴别	<p>a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；</p> <p>b) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的；</p> <p>c) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；</p> <p>d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；</p> <p>e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。</p>
2	安全标记	应提供为主体和客体设置安全标记的功能并在安装后启用；
3	访问控制	<p>a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；</p> <p>b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；</p> <p>c) 应由授权主体配置访问控制策略，并禁止默认帐户的访问；</p> <p>d) 应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；</p>

		e) 应通过比较安全标记来确定是授予还是拒绝主体对客体的访问。
4	可信路径	<p>a) 在应用系统对用户进行身份鉴别时，应能够建立一条安全的信息传输路径。</p> <p>b) 在用户通过应用系统对资源进行访问时，应用系统应保证在被访问的资源与用户之间应能够建立一条安全的信息传输路径。</p>
5	安全审计	<p>a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；</p> <p>b) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；</p> <p>c) 审计记录的内容至少应包括事件的日期、事件、发起者信息、类型、描述和结果等；</p> <p>d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。</p> <p>e) 应根据系统统一安全策略，提供集中审计接口。</p>
6	剩余信息保护	<p>a) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；</p> <p>b) 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。</p>
7	通信完整性	a) 应采用密码技术保证通信过程中数据的完整性。
8	通信保密性	<p>a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始验证；</p> <p>b) 应对通信过程中的整个报文或会话过程进行加密。</p> <p>c) 应基于硬件化的设备对重要通信过程进行加解密运算和密钥管理。</p>
9	抗抵赖	<p>a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；</p> <p>b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。</p>

10	软件容错	a) 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数据格式或长度符合系统设定要求。
		b) 应提供自动保护功能，当故障发生时自动保护当前所有状态；
		c) 应提供自动恢复功能，当故障发生时立即自动启动新的进程，恢复原来的工作状态。
9	资源控制	a) 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
		b) 应能够对系统的最大并发会话连接数进行限制；
		c) 应能够对单个帐户的多重并发会话进行限制；
		d) 应能够对一个时间段内可能的并发会话连接数进行限制；
		e) 应能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；
		f) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警；
		g) 应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源；

### 3.4.5 数据安全及备份恢复

序号	工作单元名称	测评指标
1	数据完整性	a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
		b) 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。
		c) 应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据完整性。
2	数据保密性	a) 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；

		b)应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。
		c) 应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用协议的攻击破坏数据保密性。
3	数据备份和恢复	a)应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；
		b) 应建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，提供业务应用的实时无缝切换；
		c) 应提供异地实时备份功能，利用通信网络将数据实时备份至灾难备份中心；
		d) 应采用冗余技术设计网络拓扑结构，避免存在网络单点故障；
		e) 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

### 3.4.6 安全管理机构

序号	工作单元名称	测评指标
1	岗位设置	a) 应设立信息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；
		b) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；
		c) 应成立指导和管理信息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委任或授权；
		d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。
2	人员配置	a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；
		b) 应配备专职安全管理员，不可兼任；
		c) 关键事务岗位应配备多人共同管理。
3	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；

序号	工作单元名称	测评指标
		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；
		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；
		d) 应记录审批过程并保存审批文档。
4	沟通与合作	a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；
		b) 应加强与兄弟单位、公安机关、电信公司的合作与沟通；
		c) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通；
		d) 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；
		e) 应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。
5	审核与检查	a) 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
		b) 应由内部人员或上级单位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；
		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；
		d) 应制定安全审核和安全检查制度规范安全审核和安

序号	工作单元名称	测评指标
		全检查工作，定期按照程序进行安全审核和安全检查活动。

### 3.4.7 安全管理制度

序号	工作单元名称	测评指标
1	管理制度	a) 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
		b) 应对安全管理活动中的各类管理内容建立安全管理制度；
		c) 应对要求管理人员或操作人员执行的日常管理操作建立操作规程；
		d) 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。
2	制定与发布	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；
		b) 安全管理制度应具有统一的格式，并进行版本控制；
		c) 应组织相关人员对制定的安全管理制度进行论证和审定
		d) 安全管理制度应通过正式、有效的方式发布；
		e) 安全管理制度应注明发布范围，并对收发文进行登记。
		f) 有密级的安全管理制度，应注明安全管理制度密级，并进行密级管理。
3	评审和修订	a) 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；
		b) 应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。
		c) 应明确需要定期修订的安全管理制度，并指定负责人或负责部门负责制度的日常维护；
		d) 应根据安全管理制度的相应密级确定评审和修订的操作范围。

## 3.4.8 人员安全管理

序号	工作单元名称	测评指标
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；
		b) 应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
		c) 应签署保密协议；
		d) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。
2	人员离岗	a) 应制定有关管理规范，严格规范人员离岗过程，及时终止离岗员工的所有访问权限；
		b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
		c) 应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。
3	人员考核	a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；
		b) 应对关键岗位的人员进行全面、严格的安全审查和技能考核；
		c) 应建立保密制度，并定期或不定期对保密制度执行情况进行检查或考核；
		d) 应对考核结果进行记录并保存。
4	安全意识教育和培训	a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
		b) 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
		c) 应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；
		d) 应对安全教育和培训的情况和结果进行记录并归档保存。
5	外部人员访问管理	a) 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案；

序号	工作单元名称	测评指标
		b) 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。
		c) 对关键区域不允许外部人员访问。

### 3.4.9 系统建设管理

序号	工作单元名称	测评指标
1	系统定级	a) 应明确信息系统的边界和安全保护等级； b) 应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由； c) 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定； d) 应确保信息系统的定级结果经过相关部门的批准。
2	安全方案设计	a) 应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施； b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划； c) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件； d) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施； e) 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。
3	产品采购	a) 应确保安全产品采购和使用符合国家的有关规定； b) 应确保密码产品采购和使用符合国家密码主管部门的要求； c) 应指定或授权专门的部门负责产品的采购； d) 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。



序号	工作单元名称	测评指标
		e) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。
4	自行软件开发	a) 应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；
		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；
		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；
		d) 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；
		e) 应确保对程序资源库的修改、更新、发布进行授权和批准。
		f) 应确保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。
5	外包软件开发	a) 应根据开发需求检测软件质量；
		b) 应在软件安装之前检测软件包中可能存在的恶意代码；
		c) 应要求开发单位提供软件设计的相关文档和使用指南；
		d) 应要求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。
6	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；
		b) 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；
		c) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。
		d) 应通过第三方工程监理控制项目的实施过程。
7	测试验收	a) 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；
		b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；

序号	工作单元名称	测评指标
		c) 应对系统测试验收的控制方法和人员行为准则进行书面规定；
		d) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
		e) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。
8	系统交付	a) 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
		b) 应对负责系统运行维护的技术人员进行相应的技能培训；
		c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；
		d) 应对系统交付的控制方法和人员行为准则进行书面规定；
		e) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。
9	系统备案	a) 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；
		b) 应将系统等级及相关材料报系统主管部门备案；
		c) 应将系统等级及其他要求的备案材料报相应公安机关备案。
10	等级测评	a) 在系统运行过程中，应至少每半年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；
		b) 应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
		c) 应选择具有国家相关技术资质和安全资质的测评单位进行等级测评；
		d) 应指定或授权专门的部门或人员负责等级测评的管理。
11	安全服务商选择	a) 应确保安全服务商的选择符合国家的有关规定；
		b) 应与选定的安全服务商签订与安全相关的协议，明

序号	工作单元名称	测评指标
		确约定相关责任；
		c) 应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

## 3.4.10 系统运维管理

序号	工作单元名称	测评指标
1	环境管理	<p>a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；</p> <p>b) 应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；</p> <p>c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；</p> <p>d) 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。</p> <p>e) 应对机房和办公环境实行统一策略的安全管理，对出入人员进行相应级别的授权，对进入重要安全区域的活动行为实时监视和记录。</p>
2	资产管理	<p>a) 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；</p> <p>b) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；</p> <p>c) 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；</p> <p>d) 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。</p>
3	介质管理	<p>a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；</p> <p>b) 应确保介质存放在安全的环境中，对各类介质进行</p>

序号	工作单元名称	测评指标
		控制和保护，并实行存储环境专人管理；
		c) 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，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；
		d) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，重要数据的存储介质带出工作环境必须进行内容加密并进行监控管理，对于需要送出维修或销毁的介质应采用多次读写覆盖、清除敏感或秘密数据、对无法执行删除操作的受损介质必须销毁，保密性较高的信息存储介质应获得批准并在双人监控下才能销毁，销毁记录应妥善保存；
		e) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；
		f) 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。
4	设备管理	a) 应对信息系统相关的各种设备（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；
		b) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
		c) 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、涉外维修和服务的审批、维修过程的监督控制等；
		d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
		e) 应确保信息处理设备必须经过审批才能带离机房或办公地点。
5	监控管理和安全管理中心	a) 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；
		b) 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；

序号	工作单元名称	测评指标
		c) 应建立安全管理中心,对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。
6	网络安全管理	a) 应指定专人对网络进行管理,负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作;
		b) 应建立网络安全管理制度,对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定;
		c) 应根据厂家提供的软件升级版本对网络设备进行更新,并在更新前对现有的重要文件进行备份;
		d) 应定期对网络系统进行漏洞扫描,对发现的网络系统安全漏洞进行及时的修补;
		e) 应实现设备的最小服务配置,并对配置文件进行定期离线备份;
		f) 应保证所有与外部系统的连接均得到授权和批准;
		g) 应禁止便携式和移动式设备接入网络;
		h) 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。
		i) 应严格控制网络管理用户的授权,授权程序中要求必须有两人在场,并经双重认可后方可操作,操作过程应保留不可更改的审计日志。
7	系统安全管理	a) 应根据业务需求和系统安全分析确定系统的访问控制策略;
		b) 应定期进行漏洞扫描,对发现的系统安全漏洞及时进行修补;
		c) 应安装系统的最新补丁程序,在安装系统补丁前,首先在测试环境中测试通过,并对重要文件进行备份后,方可实施系统补丁程序的安装;
		d) 应建立系统安全管理制度,对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定;
		e) 应指定专人对系统进行管理,划分系统管理员角色,明确各个角色的权限、责任和风险,权限设定应当遵循最小授权原则;
		f) 应依据操作手册对系统进行维护,详细记录操作日志,包括重要的日常操作、运行维护记录、参数的设置

序号	工作单元名称	测评指标
		和修改等内容，严禁进行未经授权的操作；
		g) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。
		h) 应对系统资源的使用进行预测，以确保充足的处理速度和存储容量，管理人员应随时注意系统资源的使用情况，包括处理器、存储设备和输出设备。
8	恶意代码防范管理	a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
		b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
		c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；
		d) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。
9	密码管理	a) 应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。
10	变更管理	a) 应确认系统中要发生的变更，并制定变更方案；
		b) 应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告；
		c) 应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；
		d) 应建立中止变更并从失败变更中恢复的文件化程序，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。
		e) 应定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性。
11	备份和恢复管理	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；
		b) 应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；

序号	工作单元名称	测评指标
		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, 备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法;
		d) 应建立控制数据备份和恢复过程的程序, 记录备份过程, 对需要采取加密或数据隐藏处理的备份数据, 进行备份和加密操作时要求两名工作人员在场, 所有文件和记录应妥善保存;
		e) 应定期执行恢复程序, 检查和测试备份介质的有效性, 确保可以在恢复程序规定的时间内完成备份的恢复。
		f) 应根据信息系统的备份技术要求, 制定相应的灾难恢复计划, 并对其进行测试以确保各个恢复规程的正确性和计划整体的有效性, 测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等, 根据测试结果, 对不适用的规定进行修改或更新。
12	安全事件处理	a) 应报告所发现的安全弱点和可疑事件, 但任何情况下用户均不应尝试验证弱点;
		b) 应制定安全事件报告和处置管理制度, 明确安全事件的类型, 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;
		c) 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;
		d) 应制定安全事件报告和响应处理程序, 确定事件的报告流程, 响应和处置的范围、程度, 以及处理方法等;
		e) 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, 制定防止再次发生的补救措施, 过程形成的所有文件和记录均应妥善保存;
		f) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。
		g) 发生可能涉及国家秘密的重大失、泄密事件, 应按照规定向公安、安全、保密等部门汇报
		h) 应严格控制参与涉及国家秘密事件处理和恢复的人员, 重要操作要求至少两名工作人员在场并登记备案。

序号	工作单元名称	测评指标
13	应急预案管理	a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
		b) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；
		c) 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；
		d) 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
		e) 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。
		f) 应随着信息系统的变更定期对原有的应急预案重新评估，修订完善。

### 3.5等级保护合规咨询服务

参照国家等级保护标准GB/T22239、GB/T22240及行业等级保护标准要求，提供重要信息系统信息安全等级保护合规建设过程的专业咨询服务，协助客户完成系统定级和备案、信息安全技术和管理体系设计和实施、以及等级保护测评等工作，确保客户方重要信息系统符合国家和行业关于信息安全等级保护的监管要求，具备足够的信息安全保障能力。

### 3.6标准和规范

《中华人民共和国计算机信息系统安全保护条例》国务院[1994]147号

《关于加强信息安全保障工作的意见》中办发[2003]27号

《关于信息等级保护工作的实施意见》（公通字66号）

《信息安全等级保护管理办法》公通字[2007]43号

《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》（发改高技[2008]2071号）

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）

《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240-2008）



《信息安全技术 信息系统安全等级保护测评要求》(GB/T 28448-2012)

《信息安全技术 信息安全等级保护 信息系统物理安全技术要求》(GB/T 21052-2007)

《信息安全技术 信息系统安全等级保护实施指南》

《信息安全技术 信息系统安全等级保护测评准则》

《信息安全技术 信息系统通用安全技术要求》(GB/T20271-2006)

《信息安全技术 网络基础安全技术要求》(GB/T20270-2006)

《信息安全技术 操作系统安全技术要求》(GB/T20272-2006)

《信息安全技术 数据库管理系统安全技术要求》(GB/T20273-2006)、

《信息安全技术 服务器技术要求》

《信息安全技术 终端计算机系统安全等级技术要求》(GA/T671-2006)

《信息安全技术 信息系统安全管理要求》(GB/T20269-2006)

《信息安全技术 信息系统安全工程管理要求》(GB/T20282-2006)

《信息技术信息安全管理实用规则》(GB/T 19716-2005 )

《信息技术 安全技术 信息技术安全性评估准则》(GB/T 18336)

《信息安全技术 信息安全风险评估规范》(GB/T 20984-2007)

### 3.7测评实施原则

在项目实施过程中必须满足以下原则：

**保密原则：**对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标方的行为。

**标准性原则：**测评方案的设计与实施应依据国家信息系统安全等级保护的相关标准进行。

**规范性原则：**投标方的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。

**可控性原则：**项目安排工作进度要跟上进度表的安排，保证工作的可控性。

**最小影响原则：**测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

**整体性原则：**测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

### 3.8整体要求

(1) 投标人应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

(2) 投标人应详细描述测评人员的组成、资质及各自职责的划分。投标人应配置有测评资质的专业人员进行本次信息安全等级保护测评工作。

(3) 供应商必须具备丰富的等级测评项目经验，参与项目的测评人员不少于4人；投标供应商必须提供本项目的高级测评师的资质证明或中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类一级）或质量管理体系认证证书（ISO9001）或软件企业证书。

(4) 本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件（包括测试工具和报告编写工具）应符合国家相关要求，报告编写工具必有取得中关村测评联盟授权，经招标人确认后由投标人提供并在信息系统等级保护测评中使用。

(5) 信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。

### 3.9专用工具要求

本项目涉及工程实施和验收测试所需的工具，由投标方负责提供。用于测评的工具主要包括服务器安全测评工具、网络设备安全测评工具、终端计算机安全测评工具、网站等应用系统安全测评工具等。在使用前，应对工具进行测评，如果需要则对工具进行软件或代码升级。

### 3.10安全管理要求

为做好全过程的安全保密工作，在等级保护测评前、中、后三个阶段都要做好安全保密工作。

#### (1)等级保护测评前

- 1) 对等级保护测评人员要进行安全保密教育，制定安全保密措施；
- 2) 签订安全保密协议。

#### (2)等级保护测评中

- 1) 对被测单位的性质、机房物理位置、网络与系统、应用与服务、资料与数

据、人员与管理等方面的信息进行严格的安全保密管理；

2) 等级保护测评工具应经过严格测试和检验，确保不对被测系统造成损失，工作结束后不驻留任何程序；

3) 对被测单位信息系统的信息资产、发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围；

4) 对测评设备、介质进行严格的保密管理；

5) 工作过程中对人员要实施封闭式集中管理；

6) 对进场人员遵守被测单位的相关管理规定。

### (3) 等级保护测评后

1) 认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏；

2) 现场工作结束后，按被测单位的要求及时还原系统，确保系统中不遗留任何代码或可执行程序；

3) 在其他风险测评任务或宣传材料中不涉及被测单位的秘密、敏感情况。

## 3.11 测评风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责信息安全测评过程中的安全保密管理工作，对测评活动、测评人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

安全测评工作中可能出现的安全风险点，按照检测对象周密制定测评方法，根据被测对象的不同采取相应的风险控制手段。不限于以下方法：

### 1) 操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

### 2) 操作时间控制

对测评直接影响系统工作时，尽可能避开敏感时期。

### 3) 人员与数据管理

必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测单位之间应签署长期保密协议，测评人员与被测单位之间也要有相应

的约束和控制措施，按国家有关要求做好保密工作。

#### 4) 制定应急预案

根据测评范围界定的系统情况，在实施前制定应急预案。

#### 5) 关键业务系统风险控制

对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、测评和简单测试的方式进行。

#### 6) 优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

#### 7) 数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止测评过程中对设备与主机的损伤影响业务系统的正常运行。

#### 8) 厂商协作

厂商需要提供各应用系统的名称、版本、协议、开发语言、进程名和相应的端口号等信息，在测评之前，由三方共同分析测评对业务可能造成的风险，分析可能存在的问题。在测评过程中尽量规避这些风险。

### 四、其他需求

1、如成交供应商发生兼并、重组，由新组建的公司按投标文件承担相应售后服务；

2、供应商使用的技术装备、设施应当符合《信息安全等级保护管理办法》中对信息安全产品的要求；

3、供应商的技术方案中应有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

4、供应商需提供等级保护测评案例成交通知书和合同复印件备查；

## 第四章合同草案

甲方（采购人）：

地址：

乙方（中标人）：

地址：

本合同依据《中华人民共和国合同法》，由（以下简称“甲方”）和(中标人名称)（以下简称“乙方”）根据项目招标文件要求和投标文件承诺，签订本合同。

合同文本包括但不限于以下内容：

一、合同标的及价款

二、服务期、服务地点：

三、质量标准及质保期：

四、服务要求：

五、验收标准：

六、付款方式：

七、违约责任：

八、争议解决方式：

九、其他约定事项：

甲方（单位全称、公章）：

乙方（单位全称、公章）：

法定代表人或授权代表（签字）：

法定代表人或授权代表（签字）：

电话（手机）：

电话（手机）：

传真：

传真：

开户银行：

开户银行：

行号：

行号：

帐号：

帐号：

年月日

年月日

签约地点：

## 第五章评审标准

### 一、资格性和符合性审查标准

序号	审核内容	供应商名称
1.	响应文件未按照谈判文件规定要求密封、签署、盖章的；	
2.	不符合第一章谈判公告“二、供应商资格要求”的；	
3.	供应商的响应文件或资格证明文件未提供或不符合谈判文件要求的： 1) 营业执照或事业单位法人证书或个体工商户营业执照等证明文件。 2) 上一年度经审计的财务报告或基本开户银行出具的资信证明文件。 3) 具备履行合同所必须的设备和专业技术能力的证明材料。 4) 供应商依法缴纳税收的证明材料和依法缴纳社会保障资金的证明材料。 5) 参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明。 6) 具备法律、行政法规规定的其他条件的证明材料。 7) 符合本文件第一章第二条要求的证明资料。	
4.	供应商未按谈判文件要求进行报价。	
5.	响应文件有效期不足的。	
6.	响应文件中附有采购人不能接受条件的。	
7.	响应文件中的内容出现重大偏离的、明显不符合谈判文件的技术规格、技术标准的；或不符合谈判文件规定的其他实质性要求的。	
8.	供应商在谈判过程中使用不真实材料的。	
9.	供应商提供产品或服务实质性不满足谈判文件要求的。	
10.	符合谈判文件中规定响应无效的其它条款。	
审核结论		

说明：

- 谈判小组分别对每一响应文件依据上表进行检查。
- 谈判小组评审只根据响应文件本身的真实无误的内容，而不依据外部的证据，但响应文件有不真实不正确的内容时除外。
- 满足要求的条款打“√”，否则为“×”。
- 对于响应文件中有任意一条不满足要求将导致其响应无效，不进入下一项评审。
- 资格性审查：按照谈判文件第一章所要求的供应商资质要求进行评审。
- 通过资格性和符合性审查的供应商才能提交最后报价。

### 二、推荐成交候选供应商标准

谈判小组从质量和服务均能满足谈判文件实质性响应要求的供应商中，按照最后报价由低到高的顺序提出3名以上成交候选人，并编写评审报告。

当最后报价相同时，由谈判小组按照技术指标优劣情况确定成交候选人排序。

### 三、政府采购政策支持

谈判小组在计算供应商最后报价时，应执行以下政府采购政策：

#### 1、支持中小企业政策

供应商如符合工信部联企业〔2011〕300 号文中对中小企业划型标准的，需提供本单位的《中小企业声明函》（详见附件）及企业相关证明材料。

证明材料需为政府相关职能部门出具的企业划型证明材料，需同时提供制造商及代理商双方的证明材料（制造商直接投标的仅提供制造商材料），并填写《中小企业声明函》，材料不全的不予折扣。

经评委会审核确认供应商符合工信部联企业〔2011〕300 号文中对中小企业划型标准的，将根据财库〔2011〕181 号文的相关规定在评定时对小型和微型企业产品的价格给予 6%的扣除，用扣除后的价格参与评审。

大中型企业与小型、微型企业组成联合体共同参加非专门面向中小企业的政府采购活动，且联合体协议中约定小型、微型企业的协议合同金额占到联合体协议合同总金额 30%以上的，给予联合体 2%的价格扣除。

#### 2、采购节能产品政策

供应商提供的产品如属于政府强制采购节能产品范围，则该产品应在最新一期“节能产品政府采购清单”中。

供应商所投产品如属于政府优先采购节能产品范围的，给予该项产品价格 1%的扣除，用扣除后的价格参与评审。

#### 3、采购环保产品政策

供应商提供的产品列入最新一期“环境标志产品政府采购清单”的，给予该项产品价格 1%的扣除，用扣除后的价格参与评审。

## 第六章响应文件的格式

封面：

政府采购

# 响应文件

（正本/副本）

项目编号：

项目名称：

报价内容：

谈判供应商名称：

日期：年月日



## 响应文件目录

1. 谈判书
  2. 法定代表人授权书
  3. 法定代表人身份证明书
  4. 报价一览表
  5. 分项报价表
  6. 偏离说明表
  7. 类似业绩一览表
  8. 拟投入项目组人员一览表
  9. 供应商的资格声明
  10. 资格证明文件
  11. 供应商关联企业情况表
  12. 无重大违法记录声明
  13. 技术文件
  14. 谈判供应商认为应该提交的其它文件（格式自拟）
  15. 中小企业声明函
- 注：竞争性谈判响应文件目录及内容每页须顺序编写页码。

## 一、谈判书

（政府采购代理机构）：

依据贵方（项目名称/项目编号：）项目采购货物及服务的谈判邀请，我方代表（姓名、职务）经正式授权并代表供应商（供应商的名称、地址）提交下述文件正本一份，副本份。

- 1、 竞争性谈判响应文件；
- 2、 资格证明文件；

**并进行如下承诺声明：**

1. 我公司在参加本次政府采购活动前三年内在经营活动中没有重大违法记录；

2. 我公司在本响应文件中所提供的全部资格证明文件均真实有效，我方承诺对其真实性负责并承担相应后果；

3. 我公司在本响应文件中所响应的内容均将成为签订合同的依据，并承诺按响应内容提供相应服务；

4. 我公司若有幸成为本项目的成交供应商，则我公司承诺按照采购文件及成交结果公告规定的方式、时间和金额向采购代理机构交纳成交服务费。逾期未交，采购人及采购代理机构有权将我公司上报至政府采购监管部门，并承担被列入政府采购失信行为名单之风险。

其它承诺：如有的话，可自行填写；

在次，我方宣布同意如下：

1. 所附《报价一览表》中规定的应提交和交付的货物报价总价为（注明币种，并用文字和数字表示的报价总价）。

2. 将按竞争性谈判文件的约定履行合同责任和义务。
3. 已详细审查全部竞争性谈判文件，包括（补充文件等），对此无异议。
4. 本竞争性谈判响应文件的有效期自开标之日起共个日历日。
5. 同意提供按照贵方可能要求的与其报价有关的一切数据或资料。
6. 与本报价有关的一切正式往来信函请寄：。

供应商：（公章）

通讯地址：

传 真：

电话：

电子函件：

授权代表签字：

日期：

## 二、法定代表人授权书

兹授权\_\_\_\_\_同志为我公司参加贵单位组织的（项目名称）采购活动的供应商代表人，全权代表我公司处理在该项目采购活动中的一切事宜。代理期限从年月\_\_\_\_\_日起至年月日止。

授权单位（签章）：

法定代表人（签字或盖章）：

签发日期：年月日

附：

代理人工作单位：

职务：性别：

身份证号码：

粘贴被授权人身份证（复印件）：

### 三、法定代表人身份证明书

兹证明（姓名）在我单位任职务，系（供应商）的法定代表人。

供应商（盖章）：

法定代表人（签章）：

性别：年龄：

身份证号码：

年月日

被授权人身份证（复印件）：

注：

- 1、本表适用于供应商不授权代理人，而由法定代表人直接参加谈判并签署响应文件的情况；
- 2、如供应商具有企业法人代表证书，则还应在本证明书后附上企业法人代表证书复印件。

## 四、报价一览表

项目名称：

项目编号：

供应商名称	
供应商地址	
总报价（含报价声明）	
交货期/服务期	
备注	

说明：（1）人民币报价。

（2）价格应按照“供应商须知”的要求报价。

（3）此表除保留在竞争性谈判响应文件中外，另复制一份与法定代表人授权书（原件）、保证金缴纳证明（复印件）及报价优惠声明一起另外密封装在一个小信封中，作为记录之用。

谈判供应商法定代表人或授权代表签字：

谈判供应商名称（签章）：

时间：年月日

## 五、分项报价表

项目名称：

项目编号：

序号	名称	数量	规格型号	品牌	制造商	单价	总价	备注
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
.....								
总计								

说明：

1. 所有价格按照“供应商须知”要求执行，精确到个位数。
2. 分项报价总计价格必须与《报价一览表》报价一致。

谈判供应商法定代表人或授权代表签字：

谈判供应商名称（签章）：

时间：年月日

## 六、偏离情况表

项目名称：

项目编号：

序号	采购需求	报价响应	偏离说明
技术要求			
1			
2			
3			
.....			
商务要求			
1			
2			
3			
.....			
响应审核（含资格要求）			
1			
2			
3			
.....			
评分要求（如有的话）			
1			
2			
3			
.....			

说明：

1. 供应商应对竞争性谈判文件的各项要求，逐条说明竞争性谈判响应文件做出的实质性响应，并申明竞争性谈判响应文件的偏离和例外。优于竞争性谈判文件要求的为正偏离，不满足的为负偏离。“技术要求”、“商务要求”对应本谈判文件第三章要求；
2. 对有具体参数要求的指标，谈判供应商必须提供所投产品的具体参数值。如果仅注明“符合”，“满足”或简单复制竞争性谈判文件要求，将可能导致报价被拒绝。

谈判供应商法定代表人或授权代表签字：

谈判供应商名称（签章）：

时间：年月日

七、类似业绩一览表

项目名称：

项目编号：

合同签订时间	采购人单位	项目概况	合同金额	项目经理	采购人单位联系人及电话	备注

- 说明：
1.

响应供应商应将过去三年中完成过的类似项目的情况填入本表中；
2.

必须按要求附提供合同复印件等资料。



八、拟投入项目组人员一览表

项目名称：

项目编号：

序号	姓名	在本项目中担 当职位	年龄	从业经历	其他
1		项目负责人			
2					
3					
4					
5					
6					
7					
8					
...					

说明：后附相关人员简介及证明材料等。

## 九、供应商的资格声明

### 1. 名称及基本情况：

(1) 供应商名称：

(2) 地址： 邮箱：

电话： 传真：

(3) 成立或注册日期：

(4) 公司性质：

(5) 法定代表人或主要负责人：

(6) 员工人数：

(7) 注册资本：

(8) 实收资本：

(9) 上年末资产负债率：

#### 1) 固定资产

原值： 净值：

#### 2) 流动资产：

#### 3) 长期负债：

#### 4) 短期负债：

### 2. 与报价服务内容有关的情况：

(1) 供应商提供此响应服务内容的经验（包括年限、项目采购人、额定能力、商业运营的起始日期等）；

(2) 服务网点分布（可另行附表）：

服务网点名称和地址	主要服务范围	服务人员数	内部等级

### 3. 供应商认为需要声明的其他情况：

兹证明上述声明是真实的、正确的，并提供了全部能提供的资料和数据，我们同意遵照采购代理机构要求出示的有关证明文件。

供应商名称：

供应商签字：

电话：

传真：

日期： 年 月 日

## 十、资格证明文件

（复印件）

供应商应提供国家有关主管部门颁发的资质证书的复印件，包括但不限于：

- 1) 营业执照或事业单位法人证书或个体工商户营业执照等证明文件。
- 2) 上一年度经审计的财务报告或基本开户银行出具的资信证明文件。
- 3) 具备履行合同所必须的设备和专业技术能力的证明材料。
- 4) 供应商依法缴纳税收的证明材料：本项目公告发布时间前3个月内交纳增值税（营业税）和企业所得税的凭据（完税证、缴款书、印花税票、银行代扣（代缴）转账凭证等均可）；  
供应商依法交纳社会保障资金的证明材料：社会保险登记证和本项目公告发布时间前3个月内交纳社会保险的凭据（专用收据或社会保险交纳清单）；

供应商为其他组织或自然人的，也需要按此项规定提供缴纳税收的凭据和交纳社会保险的凭据；

依法免税或不需要交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交纳社会保障资金。

- 5) 参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明（格式要求详见第六章《响应文件格式》）。
- 6) 具备法律、行政法规规定的其他条件的证明材料。
- 7) 符合本文件第一章第二条要求的证明资料。

所有证书、证明文件包括按要求提供的官网截图必须是真实可查证的，须注明资料来源。资格证明文件应为原件的扫描件，响应文件中须编入清晰的扫描件或复印件。所有证明材料须清晰可辨认，如因证明材料模糊无法辨认，缺页、漏页导致无法进行评审认定的责任由供应商自负。如发现弄虚作假将按照有关规定严肃处理。

证明材料仅限于参与谈判的供应商本身，参股或控股单位及独立法人子公司的材料不能作为证明材料，但参与谈判的供应商兼并的企业的材料可作为证明材料。

## 十一、供应商关联企业情况表

关联企业情况：

1、与我公司单位负责人为同一人的其他单位名称：

☐ 无；

☐ 有：。

2、与我公司存在控股、管理关系的其他单位的名称：

☐ 无；

☐ 有：。

供应商名称：

年月日

备注：

1、“单位负责人”是指单位法定代表人或者法律、行政法规规定代表单位行使职权的主要负责人。

2、本条所规定的控股、管理关系仅限于直接控股、直接管理关系，不包括间接的控股或管理关系。

## 十二、无重大违法记录声明

采购人和采购代理机构：

我方在此声明，我方在参加本次政府采购活动前三年内，在经营活动中没有以下重大违法记录：

- 1、我方因违法经营被追究过刑事责任；
- 2、我方因违法经营被责令停产停业、吊销许可证或者执照；
- 3、我方因违法经营被处以较大数额罚款等行政处罚。

随本声明附上我方参加本次政府采购活动前 3 年内发生的诉讼及仲裁情况表以及相关的法律证明文件供贵方核验。我方保证上述信息的完整、客观、真实、准确，并愿意承担我方因提供虚假材料骗取中标、成交所引起的一切法律后果。

特此声明！

投标人（供应商）：\_\_\_\_\_（盖单位章）

法定代表人或其委托代理人：\_\_\_\_\_（签字）

\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

## 十三、技术文件

项目实施方案须包含但不限于以下内容：

- 1) 项目重难点分析；
- 2) 服务内容；
- 3) 服务质量标准；
- 4) 服务验收方案及标准；
- 5) 服务承诺（含处罚措施）；
- 6) 人员安排计划；
- 7) 拟投入机械设备（如有）；
- 8) 应急措施；
- 9) 供应商认为需要提供的其他技术资料。

#### 十四、谈判供应商认为应该提交的其它文件（格式自拟）

## 十五、中小企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181号）的规定，本公司为\_\_\_\_\_（请填写：中型、小型、微型）企业。即，本公司同时满足以下条件：

1. 根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）规定的划分标准，本公司为\_\_\_\_\_（请填写：中型、小型、微型）企业。

2. 本公司参加\_\_\_\_\_单位的\_\_\_\_\_项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他\_\_\_\_\_（请填写：中型、小型、微型）企业\_\_\_\_（制造商名称）/\_\_\_\_（产地）（填写此次投标所供主要货物制造商名称或价值最高的货物制造商名称及生产产地）制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：



## 十六、节能环保产品证明材料

（供应商所提供产品若为节能环保产品，则应按本谈判文件第二章“供应商须知”第八条提供相关证明文件）