

# 招 标 文 件

(服务类)

采购项目名称：陕西省巨灾防范工程一等级保护测评及密码应用安全性评估项目采购计划

采购项目编号：KY2024-1-218

(地震局)地方编制

陕西开源招标有限公司共同编制

2024年09月06日

# 第一章 投标邀请

陕西开源招标有限公司（以下简称“代理机构”）受（地震局）地方编制委托，拟对陕西省巨灾防范工程—等级保护测评及密码应用安全性评估项目采购计划进行国内公开招标，兹邀请符合本次招标要求的供应商参加投标。

## 一、采购项目编号：KY2024-1-218

## 二、采购项目名称：陕西省巨灾防范工程—等级保护测评及密码应用安全性评估项目采购计划

## 三、招标项目简介

采购包1：陕西省地震局等保测评，预算金额：140000元，具体内容详见招标文件第三部分，简要技术要求、用途：等保测评。采购包2：灾备中心等保测评，预算金额：160000元，具体内容详见招标文件第三部分，简要技术要求、用途：等保测评。采购包3：灾备中心密码测评，预算金额：120000元，具体内容详见招标文件第三部分，简要技术要求、用途：密码测评。

## 四、供应商参加本次政府采购活动应具备的条件

（一）满足《中华人民共和国政府采购法》第二十二条规定；

（二）落实政府采购政策需满足的资格要求：

落实政府采购促进中小企业发展的相关政策：

无

（三）本项目的特定资格要求：

采购包1：

1、有效的主体资格证明：具有独立承担民事责任能力的法人、其他组织或自然人，并出具合法有效的营业执照或事业单位法人证书等国家规定的相关证明，自然人参与的提供其身份证明。

2、财务状况报告：提供2022年度或2023年度经审计的财务报告（包括“四表一注”，即资产负债表、利润表、现金流量表、所有者权益变动表及其附注，成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前六个月内银行出具的资信证明。（以上两种形式的资料提供任何一种即可）

3、税收缴纳证明：提供2023年7月至今已缴纳至少一个月的依法缴纳税款的相关凭据（时间以税款所属日期为准、税种须包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税款的投标人，应提供相关证明文件。

4、社会保障资金缴存证明：提供2023年7月至今已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。

5、书面声明：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纪，以及未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单的书面声明。本项目拒绝被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为的投标人参与。

6、承诺函：提供具有履行合同所必需的设备和专业技术能力的承诺函。

7、法定代表人授权书：法定代表人授权书及被授权人身份证明。（法定代表人直接投标只须提供其身份证明）

8、特定资质：具备《网络安全等级测评与检测评估机构服务认证证书》。

采购包2：

1、有效的主体资格证明：具有独立承担民事责任能力的法人、其他组织或自然人，并出具合法有效的营业执照或事业单位法人证书等国家规定的相关证明，自然人参与的提供其身份证明。

2、财务状况报告：提供2022年度或2023年度经审计的财务报告（包括“四表一注”，即资产负债表、利润表、现金流量

表、所有者权益变动表及其附注，成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前六个月内银行出具的资信证明。（以上两种形式的资料提供任何一种即可）

3、税收缴纳证明：提供**2023年7月**至今已缴纳至少一个月的依法缴纳税款的相关凭据（时间以税款所属日期为准、税种须包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税款的投标人，应提供相关证明文件。

4、社会保障资金缴存证明：提供**2023年7月**至今已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保障参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。

5、书面声明：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纪，以及未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单的书面声明。本项目拒绝被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为的投标人参与。

6、承诺函：提供具有履行合同所必需的设备和专业技术能力的承诺函。

7、法定代表人授权书：法定代表人授权书及被授权人身份证明。（法定代表人直接投标只须提供其身份证明）

8、特定资质：具备《网络安全等级测评与检测评估机构服务认证证书》。

采购包3：

1、有效的主体资格证明：具有独立承担民事责任能力的法人、其他组织或自然人，并出具合法有效的营业执照或事业单位法人证书等国家规定的相关证明，自然人参与的提供其身份证明。

2、财务状况报告：提供**2022年度或2023年度**经审计的财务报告（包括“四表一注”，即资产负债表、利润表、现金流量表、所有者权益变动表及其附注，成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前六个月内银行出具的资信证明。（以上两种形式的资料提供任何一种即可）

3、税收缴纳证明：提供**2023年7月**至今已缴纳至少一个月的依法缴纳税款的相关凭据（时间以税款所属日期为准、税种须包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税款的投标人，应提供相关证明文件。

4、社会保障资金缴存证明：提供**2023年7月**至今已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保障参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。

5、书面声明：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纪，以及未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单的书面声明。本项目拒绝被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为的投标人参与。

6、承诺函：提供具有履行合同所必需的设备和专业技术能力的承诺函。

7、法定代表人授权书：法定代表人授权书及被授权人身份证明。（法定代表人直接投标只须提供其身份证明）

8、特定资质：投标人须是国家密码管理局第**42**号文中《商用密码应用安全性评估试点机构目录》的测评机构，提供证明材料。

## 五、电子化采购相关事项

本项目实行电子化采购，使用的电子化交易系统为：陕西省政府采购综合管理平台的项目电子化交易系统（以下简称“项目电子化交易系统”），登录方式及地址：通过陕西省政府采购网（<http://www.ccgp-shaanxi.gov.cn/>）首页供应商用户登录陕西省政府采购综合管理平台（以下简称“政府采购平台”），进入项目电子化交易系统。供应商应当按照以下要求，参与本次电子化采购活动。

（一）供应商应当自行在陕西省政府采购网-办事指南查看相应的系统操作指南，并严格按照操作指南要求进行系统操作。在登录、使用政府采购平台前，应当按照要求完成供应商注册和信息完善，加入政府采购平台供应商库。

（二）供应商应当使用纳入陕西省政府采购综合管理平台数字证书互认范围的数字证书及签章（以下简称“互认的证书及签章”）进行系统操作。供应商使用互认的证书及签章登录政府采购平台进行的一切操作和资料传递，以及加盖电子签章确认采

购过程中制作、交换的电子数据，均属于供应商真实意思表示，由供应商对其系统操作行为和电子签章确认的事项承担法律责任。

已办理互认的证书及签章的供应商，校验互认的证书及签章有效性后，即可按照系统操作要求进行身份信息绑定、权限设置和系统操作；未办理互认的证书及签章的供应商，按要求办理互认的证书及签章并校验有效性后，按照系统操作要求进行身份信息绑定、权限设置和系统操作。互认的证书及签章的办理与校验，可查看陕西省政府采购网-办事指南-CA及签章服务。

供应商应当加强互认的证书及签章日常校验和妥善保管，确保在参加采购活动期间互认的证书及签章能够正常使用；供应商应当严格互认的证书及签章的内部授权管理，防止非授权操作。

（三）供应商应当自行准备电子化采购所需的计算机终端、软硬件及网络环境，承担因准备不足产生的不利后果。

（四）政府采购平台技术支持：

在线客服：通过陕西省政府采购网-在线客服进行咨询

技术服务电话：029-96702

CA及签章服务：通过陕西省政府采购网-办事指南-CA及签章服务进行查询

## 六、招标文件获取时间、方式及地址

（一）招标文件获取时间：详见采购公告

（二）在招标文件获取开始时间前，采购人或代理机构将本项目招标文件上传至项目电子化交易系统，向供应商提供。供应商通过项目电子化交易系统获取招标文件。成功获取招标文件的，供应商将收到已获取招标文件的回执函。未成功获取招标文件的供应商，不得参与本次采购活动，不得对招标文件提起质疑。

成功获取招标文件后，采购人或代理机构进行澄清或者修改的，澄清或者修改的内容可能影响投标文件编制的，采购人或代理机构将通过项目电子化交易系统发布澄清或者修改后的招标文件，供应商应当重新获取招标文件；澄清或者修改后的招标文件发布日期距提交投标文件截止日期不足15日的，采购人或代理机构顺延提交投标文件的截止时间。供应商未重新获取招标文件或者未按照澄清或者修改后的招标文件编制投标文件进行投标的，自行承担不利后果。

## 七、投标文件提交截止时间及开标时间、地点、方式

（一）投标文件提交截止时间及开标时间：详见采购公告

（二）投标文件提交方式、地点：供应商应当在投标文件提交截止时间前，通过项目电子化交易系统提交投标文件。成功提交的，供应商将收到已提交投标文件的回执函。

（三）本项目采取网上开标，即采购人或代理机构通过项目电子化交易系统“开标/开启大厅”组织在线开标。

## 八、本投标邀请在陕西省政府采购网以公告形式发布

## 九、供应商信用融资

根据《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》（陕财办采〔2020〕15号）和《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23号）文件要求，为助力解决政府采购成交供应商资金不足、融资难、融资贵的困难，促进供应商依法诚信参加政府采购活动，有融资需求的供应商可登录陕西省政府采购网—陕西省政府采购金融服务平台（<http://www.ccgp-shaanxi.gov.cn/zcdservice/zcd/shanxi/>），选择符合自身情况的“政采贷”银行及其产品，凭项目中标（成交）结果、中标（成交）通知书等信息在线向银行提出贷款意向申请、查看贷款审批情况等。

## 十、联系方式

采购人：（地震局）地方编制

地址：陕西省西安市边家村水文巷4号

邮编：710068

联系人：柳老师

联系电话： 029-88465436

**代理机构：陕西开源招标有限公司**

地址： 西安市雁展路1111号莱安中心T6-15层

邮编： 716000

联系人： 尚娇、牛佩文、刘金柯、卢韶华

联系电话： 029-81206622-821

**采购监督机构：财政厅政府采购管理处**

联系人： 柴老师、杨老师

联系电话： 029-68936409、029-68936410

## 第二章 投标人须知

### 2.1 投标人须知前附表

序号	应知事项	说明和要求
1	采购预算（实质性要求）	<p>本项目各包采购预算金额如下：</p> <p>采购包1：140,000.00元</p> <p>采购包2：160,000.00元</p> <p>采购包3：120,000.00元</p> <p>投标人的采购包投标报价高于采购包采购预算的，其投标文件将按无效处理。</p>
2	最高限价（实质性要求）	<p>详见第三章。</p> <p>投标人的采购包投标报价高于最高限价的，其投标文件将按无效处理。</p>
3	评标方法	<p>采购包1：综合评分法</p> <p>采购包2：综合评分法</p> <p>采购包3：综合评分法</p> <p>（详见第五章）</p>
4	是否接受联合体	<p>采购包1：不接受</p> <p>采购包2：不接受</p> <p>采购包3：不接受</p> <p>如以联合体响应的，联合体各方均应当具备本招标文件要求的资格条件和能力。</p> <p>（1）联合体各方均应具有承担本项目必备的条件，如相应的人力、物力、资金等。</p> <p>（2）招标文件对投标人资格条件有特殊要求的，联合体各个成员都应当具备规定的相应资格条件。</p> <p>（3）同一专业的单位组成的联合体，应当按照资质等级较低的单位确定联合体的资质等级。如：某联合体由三个单位组成，其中两个单位资质等级为甲级，另一单位资质等级为乙级，则该联合体资质等级等级为乙级。</p>
5	落实节能、环保产品政策	<p>1.根据《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）相关要求，政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门确定实施政府优先采购和强制采购的产品类别，以品目清单的形式发布并适时调整。</p> <p>2.本项目采购如有产品属于节能产品政府采购品目清单中应强制采购的产品范围，供应商应当提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则作无效投标处理。</p> <p>3.本项目采购如有产品属于节能产品政府采购品目清单中应优先采购的产品范围，本项目采购如有产品属于环境标志产品政府采购品目清单中应优先采购的产品范围，评审得分/响应报价相同的，按供应商提供的优先采购产品认证证书数量由多到少顺序排列。</p>

6	小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除（仅非预留份额采购项目或预留份额采购项目中的非预留部分采购包适用）	关于本项目采购包中执行小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除情况、具体扣除比例和规则详见第五章。
7	充分、公平竞争保障措施（实质性要求）	<p>核心产品允许有多个，不同供应商提供了任意一个相同品牌的核心产品，即视为提供相同品牌的供应商。</p> <p>使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会采取随机抽取方式确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。</p> <p>采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照随机抽取方式确定一个参加评标的投标人，其他投标无效。</p> <p>核心产品清单详见第三章。</p> <p>在符合性审查环节提供核心产品品牌不足3个的，视为有效投标人不足3家。</p>
8	不正当竞争预防措施（实质性要求）	在评标过程中，评标委员会认为投标人投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内通过项目电子化交易系统进行书面说明，必要时提交相关证明材料。投标人提交的书面说明，应当加盖投标人公章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则视为不能证明其投标报价合理性。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效投标处理。
9	投标保证金	<p>采购包1保证金金额：2,500.00元</p> <p>采购包2保证金金额：3,000.00元</p> <p>采购包3保证金金额：2,000.00元</p> <p>缴交渠道：电子保函,转账、支票、汇票等（需通过实体账户、户名及开户行信息）</p> <p>开户名称：陕西开源招标有限公司</p> <p>开户银行：交通银行西安甜水井街支行</p> <p>银行账号：86113010750181501003429</p>
10	标书费信息	免费获取

11	履约保证金（实质性要求）	<p>采购包1：缴纳</p> <p>本采购包履约保证金为合同金额的5.0%</p> <p>说明：本项目履约保证金为合同总价款的5%，合同签订后7个工作日内必须缴纳，履约保证金缴纳形式：中标人应当以银行转账、支票、汇票、本票、保函等非现金形式缴纳。</p> <p>采购包2：缴纳</p> <p>本采购包履约保证金为合同金额的5.0%</p> <p>说明：本项目履约保证金为合同总价款的5%，合同签订后7个工作日内必须缴纳，履约保证金缴纳形式：中标人应当以银行转账、支票、汇票、本票、保函等非现金形式缴纳。</p> <p>采购包3：缴纳</p> <p>本采购包履约保证金为合同金额的5.0%</p> <p>说明：本项目履约保证金为合同总价款的5%，合同签订后7个工作日内必须缴纳，履约保证金缴纳形式：中标人应当以银行转账、支票、汇票、本票、保函等非现金形式缴纳。</p>
12	投标有效期（实质性要求）	提交投标文件的截止之日起不少于90天。
13	招标代理服务费（实质性要求）	<p>本项目收取代理服务费</p> <p>代理服务费用收取对象：中标/成交供应商</p> <p>代理服务费收费标准：1、依据计价格【2002】1980号、发改价格【2011】534号文件规定的收费标准下浮40%计取(不足3000元按3000元计取)。2、本项目代理服务费按服务计取。</p>
14	采购结果公告	采购结果将在陕西省政府采购网予以公告。
15	中标通知书	采购结果公告发布的同时，采购人或代理机构通过项目电子化交易系统向中标供应商发出中标通知书；中标供应商通过项目电子化交易系统获取中标通知书。
16	政府采购合同公告、备案	<p>政府采购合同签订之日起2个工作日内，采购人将政府采购合同在陕西省政府采购网予以公告；</p> <p>政府采购合同签订之日起7个工作日内，采购人将政府采购合同报本级财政部门备案。</p>
17	进口产品	不允许
18	是否组织潜在投标人现场考察	<p>采购包1：组织现场踏勘：否</p> <p>采购包2：组织现场踏勘：否</p> <p>采购包3：组织现场踏勘：否</p>
19	特殊情况	<p>出现下列情形之一的，采购人或者代理机构应当中止电子化采购活动，并保留相关证明材料备查：</p> <p>（一）交易系统发生故障（包括感染病毒、应用或数据库出错）而无法正常使用的；</p> <p>（二）因组织场所停电、断网等原因，导致采购活动无法继续通过交易系统实施的；</p> <p>（三）其他无法保证电子化交易的公平、公正和安全的情况。</p> <p>出现上述的情形，不影响采购公平、公正的，采购人或者代理机构可以待上述情形消除后继续组织采购活动；影响或者可能影响采购公平、公正的，采购人或者代理机构应当依法废标。</p> <p>（一）交易系统发生故障（包括感染病毒、应用或数据库出错）而无法正常使用的；</p> <p>（二）因组织场所停电、断网等原因，导致采购活动无法继续通过交易系统实施的；</p> <p>（三）其他无法保证电子化交易的公平、公正和安全的情况。出现上述的情形，不影响采购公平、公正的，采购人或者采购代理机构可以待上述情形消除后继续组织采购活动；影响或者可能影响采购公平、公正的，采购人或者采购代理机构应当依法废标。</p>

## 2.2 总则



### 2.2.1适用范围

一、本招标文件仅适用于本次公开招标采购项目。

二、本招标文件的最终解释权由（地震局）地方编制和陕西开源招标有限公司享有。对招标文件中供应商参加本次政府采购活动应当具备的条件，招标项目技术、服务、商务及其他要求，评标细则及标准由（地震局）地方编制负责解释。除上述招标文件内容，其他内容由陕西开源招标有限公司负责解释。

### 2.2.2有关定义

一、“采购人”是指依法进行政府采购的各级国家机关、事业单位、团体组织。本次招标的采购人是（地震局）地方编制。

二、“投标人”是指按照采购公告规定获取了招标文件，拟参加投标和向采购人提供货物、工程或服务的法人、其他组织或者自然人。

三、“代理机构”是指政府采购集中采购机构和从事政府采购代理业务的社会中介机构。本项目的代理机构是陕西开源招标有限公司。

四、“网上开标”是指代理机构通过项目电子化交易系统在线完成签到、开标、唱标和记录等活动，供应商通过项目电子化交易系统在线完成投标文件解密、参与开标活动。

五、“电子评标”是指通过项目电子化交易系统在线完成资格审查小组和评审小组组建，开展资格和符合性审查、比较与评价、出具评标报告、推荐中标候选人等活动。

## 2.3招标文件

### 2.3.1招标文件的构成

一、招标文件是投标人准备投标文件和参加投标的依据，同时也是资格审查、评标的重要依据。招标文件用以阐明招标项目所需的资质、技术、服务及报价等要求、招标投标程序、有关规定和注意事项以及合同主要条款等。本招标文件包括以下内容：

- （一）投标邀请；
- （二）投标人须知；
- （三）招标项目技术、服务、商务及其他要求；
- （四）资格审查；
- （五）评标办法；
- （六）投标文件格式；
- （七）拟签订采购合同文本。

二、投标人应认真阅读和充分理解招标文件中所有的事项、格式条款和规范要求。投标人没有对招标文件全面作出实质性响应所产生的风险由投标人承担。

### 2.3.2招标文件的澄清和修改

一、在投标文件提交截止时间前，采购人或者代理机构可以对已发出的招标文件进行必要的澄清或者修改。

二、澄清或者修改的内容为招标文件的组成部分，采购人或者代理机构将在陕西省政府采购网发布更正公告，投标人应及时关注本项目更正公告信息，按更正后公告要求进行响应。更正内容可能影响投标文件编制的，采购人或者代理机构将通过项目电子化交易系统发布更正后的招标文件，投标人应依据更正后的招标文件编制投标文件。若投标人未按前述要求进行投标响应的，自行承担不利后果。

## 2.4投标文件

### 2.4.1投标文件的语言

一、投标人提交的投标文件以及投标人与采购人或代理机构就有关投标的所有来往书面文件均须使用中文。投标文件中如附有外文资料，主要部分要对应翻译成中文并附在相关外文资料后面。未翻译的外文资料，评标委员会将其视为无效材料。

二、翻译的中文资料与外文资料如果出现差异和矛盾时，以中文为准。涉嫌提供虚假材料的按照相关法律法规处理。

三、如因未翻译而造成对投标人的不利后果，由投标人承担。

#### **2.4.2 计量单位**

除招标文件中另有规定外，本项目均采用国家法定的计量单位。

#### **2.4.3 投标货币**

本次项目均以人民币报价。

#### **2.4.4 知识产权**

一、投标人应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权。

二、投标人将在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，投标人需提供开发接口和开发手册等技术资料，并承诺提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）。

三、如采用投标人所不拥有的知识产权，则在投标报价中必须包括合法使用该知识产权的相关费用。

#### **2.4.5 投标文件的组成**

投标人应当按照招标文件的要求编制投标文件。投标文件应当对招标文件提出的要求和条件作出明确响应。

投标文件具体内容详见第六章。

#### **2.4.6 投标文件格式**

一、投标人应按照招标文件第六章中提供的“投标文件格式”填写相关内容。

二、对于没有格式要求的投标文件由投标人自行编写。

#### **2.4.7 投标报价（实质性要求）**

一、投标人的报价是投标人响应招标项目要求的全部工作内容的价格体现，包括投标人完成本项目所需的一切费用。

二、投标人每种货物及服务内容只允许有一个报价，并且在合同履行过程中是固定不变的，任何有选择或可调整的报价将不予接受，并按无效投标处理。

三、投标文件报价出现前后不一致的，按照招标文件第五章评标办法规定予以修正，修正后的报价经投标人通过项目电子化交易系统进行确认，并加盖投标人（法定名称）电子印章，投标人未在规定时间内确认的，其投标无效。

#### **2.4.8 投标有效期（实质性要求）**

投标有效期详见第二章“投标人须知前附表”，投标文件未明确投标有效期或者投标有效期小于“投标人须知前附表”中投标有效期要求的，其投标文件按无效处理。

#### **2.4.9 投标文件的制作、签章和加密（实质性要求）**

一、投标文件应当根据招标文件进行编制，投标人应通过陕西省政府采购网-办事指南-CA及签章服务下载投标（响应）客户端，使用客户端编制投标文件。

二、投标人应按照客户端操作要求，对应招标文件的每项实质性要求，逐一如实响应；未如实响应或者响应内容不符合招标文件对应项的要求的，其投标文件作无效处理。

三、投标人完成投标文件编制后，应按照招标文件第一章明确的签章要求，使用互认的证书及签章对投标文件进行电子签章和加密。

四、招标文件澄清或者修改的内容可能影响投标文件编制的，代理机构将重新发布澄清或者修改后的招标文件，投标人应重新获取澄清或者修改后的招标文件，按照澄清或者修改后的招标文件进行投标文件编制、签章和加密。

#### **2.4.10 投标文件的提交**

一、（实质性要求）投标人应当在投标文件提交截止时间前，通过项目电子化交易系统完成投标文件提交。

二、在投标文件提交截止时间后，采购人或者代理机构不再接受投标人提交投标文件。投标人应充分考虑影响投标文件提交的各种因素，确保在投标文件提交截止时间前完成提交。

#### **2.4.11 投标文件的补充、修改、撤回（实质性要求）**

投标文件提交截止时间前，投标人可以补充、修改或者撤回已成功提交的投标文件；对投标文件进行补充、修改的，应当先行撤回已提交的投标文件，补充、修改后重新提交。

供应商投标文件撤回后，视为未提交过投标文件。

## **2.5 开标、资格审查、评标和中标**

### **2.5.1 开标及开标程序**

一、本项目为网上开标项目。网上开标的开始时间为投标文件提交截止时间。成功提交或解密电子投标文件的投标人不足3家的，不予开标，采购人或代理机构将作废标处理。

#### 二、开标准备工作

开标/开启前30分钟内，供应商需登录项目电子化交易系统-“供应商开标大厅”-进入开标选择对应项目包组操作签到，签到完成后等待代理机构开标/开启。

投标文件提交截止时间前30分钟，投标人登录项目电子化交易系统-“开标/开启大厅”参与开标。

#### 三、解密投标文件（实质性要求）

投标文件提交截止时间后，成功提交投标文件的投标人符合招标文件规定数量的，代理机构将启动投标文件解密程序，解密时间为30分钟；投标人应在规定的解密时间内，使用互认的证书及签章通过项目电子化交易系统进行投标文件解密。投标人未在规定的解密时间内完成解密的，按无效投标处理。

#### 四、开标

解密时间截止或者所有投标人投标文件均完成解密后（以发生在先的时间为准），由代理机构通过项目电子化交易系统对投标人名称、投标文件解密情况、投标报价进行展示。

开标过程中，各方主体均应遵守互联网有关规定，不得发表与采购活动无关的言论。投标人对开标过程和开标记录有疑义，以及认为采购人或代理机构相关工作人员有需要回避的情形的，及时向工作人员提出询问或者回避申请。采购人或代理机构对投标人提出的询问或者回避申请应当及时处理。

投标人完成投标文件解密后，自主决定是否参加网上在线开标，未参加的，视同认可开标结果。

### **2.5.2 查询及使用信用记录**

开标结束后，采购人或代理机构根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的要求，通过“信用中国”网站（[www.creditchina.gov.cn](http://www.creditchina.gov.cn)）、“中国政府采购网”网站（[www.ccgp.gov.cn](http://www.ccgp.gov.cn)）等渠道，查询投标人在投标文件提交截止时间前的信用记录并保存信用记录结果网页截图，拒绝列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单中的供应商参加本项目的采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个投标人的身份共同参加政府采购活动的，将对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

### **2.5.3 资格审查**

详见招标文件第四章。

### **2.5.4 评标**

详见招标文件第五章。

### **2.5.5 中标通知书**

一、采购人或者评标委员会确认中标供应商后，代理机构在陕西省政府采购网发布中标结果公告、通过项目电子化交易系统发出中标通知书，中标供应商通过项目电子化交易系统获取中标通知书。

二、中标通知书是采购人和中标供应商签订政府采购合同的依据，是合同的有效组成部分。如果出现政府采购法律法规、规章制度规定的中标无效情形的，将以公告形式宣布发出的中标通知书无效，中标通知书将自动失效，并依法重新确定中标供应商或者重新开展采购活动。

三、中标通知书对采购人和中标供应商均具有法律效力。

## **2.6 签订及履行合同和验收**

### **2.6.1 签订合同**

- 一、采购人应在中标通知书发出之日起三十日内与中标人签订采购合同。
- 二、采购人和中标人签订的采购合同不得对招标文件确定的事项以及中标人的投标文件作实质性修改。

### **2.6.2 合同分包和转包（实质性要求）**

#### **2.6.2.1 合同分包**

- 一、投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。
  - 二、分包履行合同的部分应当为采购项目的非主体、非关键性工作，不属于中标人的主要合同义务。
  - 三、采购合同实行分包履行的，中标人就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。
  - 四、中小企业依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的政策获取政府采购合同后，小型、微型企业不得将合同分包或转包给大型、中型企业，中型企业不得将合同分包或转包给大型企业。
- 采购包1：不允许合同分包。
- 采购包2：不允许合同分包。
- 采购包3：不允许合同分包。

#### **2.6.2.2 合同转包**

- 一、严禁中标供应商将本项目转包。本项目所称转包，是指将本项目转给他人或者将本项目全部肢解以后以分包的名义分别转给他人的行为。
- 二、中标供应商转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

### **2.6.3 采购人增加合同标的的权利**

采购合同履行过程中，采购人需要追加与合同标的相同的货物或者服务的，在不改变合同其他条款的前提下，可以与中标人协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

### **2.6.4 履行合同**

- 一、合同一经签订，双方应严格履行合同规定的义务。
- 二、在合同履行过程中，如发生合同纠纷，合同双方应按照《中华人民共和国民法典》规定及合同条款约定进行处理。

### **2.6.5 履约验收方案**

- 采购包1：
- 1、招标文件、投标文件、澄清表（函）； 2、合同及附件文本； 3、国家相应的标准、规范。
- 采购包2：
- 1、招标文件、投标文件、澄清表（函）； 2、合同及附件文本； 3、国家相应的标准、规范。
- 采购包3：
- 1、招标文件、投标文件、澄清表（函）； 2、合同及附件文本； 3、国家相应的标准、规范。

### **2.6.6 资金支付**

采购人按财政部门的相关规定及采购合同的约定进行支付。

## **2.7 纪律要求**

### **2.7.1 评标活动纪律要求**

采购人、代理机构应保证评标活动在严格保密的情况下进行，采购人、代理机构、投标人和评标委员会成员应当严格遵守政府采购法律法规规章制度和本项目招标文件以及代理机构现场管理规定，接受采购人委派的监督人员的监督，任何单位和个人不得非法干预和影响评标过程和结果。

对各投标人的商业秘密，评标委员会成员应予以保密，不得泄露给其他投标人。

## 2.7.2 投标人不得具有的情形（实质性要求）

投标人参加投标不得有下列情形：

一、有下列情形之一的，视为投标人串通投标：

- （一）不同投标人的投标文件由同一单位或者个人编制；
- （二）不同投标人委托同一单位或者个人办理投标事宜；
- （三）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；
- （四）不同投标人的投标文件异常一致或者投标报价呈规律性差异；
- （五）不同投标人的投标文件相互混装；

二、提供虚假材料谋取中标；

三、采取不正当手段诋毁、排挤其他投标人；

四、与采购人或代理机构、其他投标人恶意串通；

五、向采购人或代理机构、评标委员会成员行贿或者提供其他不正当利益；

六、在招标过程中与采购人或代理机构进行协商谈判；

七、中标后无正当理由拒不与采购人签订政府采购合同；

八、未按照招标文件确定的事项签订政府采购合同；

九、将政府采购合同转包或者违规分包；

十、提供假冒伪劣产品；

十一、擅自变更、中止或者终止政府采购合同；

十二、拒绝有关部门的监督检查或者向监督检查部门提供虚假情况；

十三、法律法规规定的其他禁止情形。

投标人有上述情形的，按照规定追究法律责任，具有前述一至十三条情形之一的，其投标文件无效，或取消被确认为中标供应商的资格或认定中标无效。

## 2.7.3 采购人员及相关人员回避要求

政府采购活动中，采购人员及相关人员与投标人有下列利害关系之一的，应当回避：

- （1）参加采购活动前3年内与投标人存在劳动关系；
- （2）参加采购活动前3年内担任投标人的董事、监事；
- （3）参加采购活动前3年内是投标人的控股股东或者实际控制人；
- （4）与投标人的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；
- （5）与投标人有其他可能影响政府采购活动公平、公正进行的关系。

投标人认为采购人员及相关人员与其他投标人有利害关系的，可以向代理机构书面提出回避申请，并说明理由。代理机构将及时询问被申请回避人员，有利害关系的被申请回避人员应当回避。

## 2.8 询问、质疑和投诉

一、询问、质疑、投诉的接收和处理严格按照《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》《政府采购质疑和投诉办法》等规定办理。

二、供应商询问、质疑的答复主体：

根据委托代理协议约定，供应商对招标文件中采购需求的询问、质疑由 陕西开源招标有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由陕西开源招标有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 陕西开源招标有限公司 负责答复。

三、供应商提出的询问，应当明确询问事项，如以书面形式提出的，应由供应商签字并加盖公章。

为提高采购效率，降低社会成本，鼓励询问主体对于不损害国家及社会利益或自身合法权益的问题或情形采用询问方式处

理解决（包含但不限于文字错误、标点符号、不影响投标文件的编制的情形）。

四、供应商认为采购文件、采购过程、中标或者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、代理机构提出质疑。供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。供应商应知其权益受到损害之日，是指：（一）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日；（二）对采购过程提出质疑的，为各采购程序环节结束之日；（三）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

五、本项目不接受在线提交质疑，供应商通过书面形式线下向采购人或代理机构提交质疑资料。

六、供应商提出质疑时应当准备的资料

- （一）质疑函正本1份；（政府采购供应商质疑函范本详见附件一）
- （二）法定代表人或主要负责人授权委托书1份（委托代理人办理质疑事宜的需提供）；
- （三）法定代表人或主要负责人身份证复印件1份；
- （四）委托代理人身份证复印件1份（委托代理人办理质疑事宜的需提供）；
- （五）针对质疑事项必要的证明材料（针对招标文件提出的质疑，需提交从项目电子化交易系统获取的招标文件回执单）。

答复主体：代理机构

联系人：尚娇、牛佩文、刘金柯、卢韶华

联系电话：029-81206622-821

地址：西安市雁展路1111号莱安中心T6-15层

邮编：716000

注：根据《中华人民共和国政府采购法》的规定，供应商质疑不得超出招标文件、采购过程、采购结果的范围。

七、供应商对采购人或代理机构的质疑答复不满意，或者采购人或代理机构未在规定期限内作出答复的，供应商可以在答复期满后15个工作日内向同级财政部门提起投诉。

投诉受理单位：本采购项目同级财政部门。（政府采购供应商投诉书范本详见附件二）

### 第三章 招标项目技术、服务、商务及其他要求

（注：带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

#### 3.1 采购项目概况

采购包1：陕西省地震局等保测评，预算金额：140000元，具体内容详见服务要求，简要技术要求、用途：等保测评。  
采购包2：灾备中心等保测评，预算金额：160000元，具体内容详见服务要求，简要技术要求、用途：等保测评。 采购包3：灾备中心密码测评，预算金额：120000元，具体内容详见服务要求，简要技术要求、用途：密码测评。

#### 3.2 服务内容及服务要求

##### 3.2.1 服务内容

采购包1：  
采购包预算金额（元）：140,000.00  
采购包最高限价（元）：140,000.00  
供应商报价不允许超过标的金额  
（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额 （元）	计量 单位	所属行业	是否核 心产品	是否允许 进口产品	是否属于 节能产品	是否属于环境 标志产品
1	等级保护测评	1. 0 0	140,000. 00	项	软件和信息技术服务业	否	否	否	否

采购包2：  
采购包预算金额（元）：160,000.00  
采购包最高限价（元）：160,000.00  
供应商报价不允许超过标的金额  
（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额 （元）	计量 单位	所属行业	是否核 心产品	是否允许 进口产品	是否属于 节能产品	是否属于环境 标志产品
1	等级保护测评	1. 0 0	160,000. 00	项	软件和信息技术服务业	否	否	否	否

采购包3：  
采购包预算金额（元）：120,000.00  
采购包最高限价（元）：120,000.00  
供应商报价不允许超过标的金额  
（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额 (元)	计量 单位	所属行业	是否核 心产品	是否允许 进口产品	是否属于 节能产品	是否属于环境 标志产品
1	密评	1. 0 0	120,000. 00	项	软件和信息技术服务业	否	否	否	否

3.2.2服务要求

采购包1：  
 供应商报价不允许超过标的金额  
 （招单价的）供应商报价不允许超过标的单价  
 标的名称：等级保护测评

参数性质	序号	技术参数与性能指标									
		<div>一、工作内容</div> <div> <p>此次项目拟对以下信息系统开展等级保护测评与整改，并提供测评报告等相关报告。信息系统名称及安全保护等级如下表：</p> <table> <tr> <th>序号</th><th>系统名称</th><th>系统等级</th></tr> <tr> <td>1</td><td>防震减灾一体化系统</td><td>二级</td></tr> <tr> <td>2</td><td>陕西省地震数据资源平台</td><td>二级</td></tr> </table> </div> <div> <div>二、项目服务内容</div> <div> <p>系统调研：在系统相关人员的协助下，对信息系统进行调研和梳理，了解系统当前信息系统资产现状。</p> <p>现场测评：根据国家等级测评的相关标准及已编制的相关等级保护测评指导书对信息系统中的相关资产进行测评项的检查、记录检查结果，出具相关系统测评报告。</p> <p>分析整改：根据前述工作内容，分析信息系统安全情况与等级保护基本要求的差距，提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，配合采购单位开展安全整改工作。</p> <p>系统复测：根据整改情况重新进行系统测评，记录复测结果，根据复测结果出具相关系统复测报告。</p> <p>配合验收：整理项目过程中所有相关的过程文档，提交系统相关人员，做好验收汇报和整改工作。</p> <p>安全演练：组织并开展一次针对陕西省地震局信息系统的安全应急模拟演练，编制演练方案，制定应急预案，进行模拟处置，记录演练过程与结果，形成演练总结。</p> <p>重保驻场：按照采购方需求，年度服务期内提供不少于<b>15</b>天的重保期安全驻场服务，每天驻场时长及驻场具体时间由采购方根据重保要求确定。</p> </div> </div>	序号	系统名称	系统等级	1	防震减灾一体化系统	二级	2	陕西省地震数据资源平台	二级
序号	系统名称	系统等级									
1	防震减灾一体化系统	二级									
2	陕西省地震数据资源平台	二级									



### 三、其他要求

1. 测评人员要求：本项目的全部测评人员需具有1年或1年以上测评工作经验，项目经理和质量负责人必须具备丰富的安全服务经验及相关资质认证，并提供人员管理及配备方案，并确保人员稳定。如需更换测评人员，须由采购单位同意。

2. 人员配备：投标方参与此项目组人员不少于5人（其中高级测评师不少于1人，中级测评师不少于2人），提供现场服务的测评师不少于2人（至少1名中级）。投标人必须为本项目成立本地化等级保护测评小组，由测评小组组长统一负责，测评小组组长具有一定的技术及管理知识和经验，能容易地与客户沟通，能很好的执行与完成测评工作，并根据适当情况增加测评人员。

3. 攻防演练应做好应急预案，攻击过程开展实时监控，确保不因演练导致的信息系统业务异常。

4. 投标人应按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

### 四、服务交付内容

在本次等级保护测评项目中，服务商须提交主要成果文档包含如下：

1. 《信息系统安全等级保护项目计划书》；
2. 《信息系统安全等级保护测评方案》（两个系统各一份）；
3. 《信息系统安全等级保护测评报告》（两个系统各一份）；
4. 《信息系统整改建议报告》（两个系统各一份）；
5. 《信息系统安全等级保护复测报告》（两个系统各一份）；
6. 《网络安全应急演练实施方案》；
7. 《网络安全应急演练应急预案》；
8. 《网络安全应急演练总结报告》；
9. 对服务期内出现的网络安全事件或问题提供溯源和解决；
10. 服务期内依据采购方需求提供不少于15天的安全驻场服务；
11. 提供不少于2次全局范围关于网络安全的培训内容。

### 五、等保测评技术标准及要求

#### （一）总体要求

根据《中华人民共和国网络安全法》《信息安全等级保护管理办法》(公通字[2007]43号)与《信息安全技术 网络安全等级保护基本要求》GB/T22239-2019要求，等级测评工作须覆盖安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面的内容，并根据现场实际情况完成风险分析工作，最终为完善等级保护安全防护体系提供指导依据。

具体内容：

- 1 . 防震减灾一体化系统、陕西省地震数据资源平台系统开展二级等保测评，需公司依据等保二级要求进行信息系统测评，形成测评方案、测评报告、整改报告、复测报告等。
- 2.根据等保要求以及陕西省地震局需求，提供制度完善、网络安全预案修正以及网络安全相关方案的编制等服务。包含但不限于陕西省地震局现有安全相关各项规章制度进行细化、完善、整改等编制，网络安全预案的修订，网络安全相关方案或报告如安全自查报告、安全保障方案等资料的编制。
- 3.提供日常及重要安保时期的网络安全事件处置和溯源服务。
- 4 . 提供全局范围内针对终端用户、以及针对管理部门有关法律法规等的公开培训，不少于两次。

从甲方通知开始测评日期起，30个工作日完成等保测评和报告提交的所有工作；同时从合同签订时间起一年内提供一次安全攻防模拟演练、不限次数的制度完善与方案编制、应急响应与安全事件处置、配合检查、电话支持、安全咨询等服务在内的安全维保服务。

（二）第一阶段：等级保护

信息安全等级保护工作共分为五步，分别是：“定级、备案、建设整改、等级测评、监督检查”。该项目主要完成系统的安全测评工作，依据安全技术和安全管理两个方面的测评要求，分别从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个安全类别进行安全测评。

1. 等级保护测评要求

服务商在测评过程中要求按照《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实施指南》（GB/T25058-2010）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）等相关的标准规范开展等级测评工作，对系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理共10个层面进行安全等级保护测评。

2. 等级保护测评流程及内容

等级保护测评过程中要求服务商严格按照下列流程开展工作，具体工作流程如下：

- （1） 测评准备阶段：是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的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） 方案编制阶段：是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本活动的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指导书，形成测评方案。
- （3） 现场测评阶段：是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格按照测评指导书执行，分步实施所有测评项目，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。
- （4） 分析与报告编制阶段：是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和《等级测评过程指南》的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成《信息系统安全等级测评报告》文本。

### （三）第二阶段：渗透检测

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机信息系统是否安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，通常该分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机信息系统是否安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，通常该分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

### （四）第三阶段：代码审计

对系统进行代码审计。内容包括但不限于：

1. 审核应用流程中是否存在可被绕过的隐患；
2. 审核应用代码中是否有一般性的漏洞类型；
3. 审核应用代码中因需要开放给管理员或用户而可能导致的隐蔽漏洞；
4. 审核应用系统中三方组件及产品的漏洞隐患；
5. 结合黑盒渗透测试方法，对应用代码审计结果验证；
6. 发现安全隐患，确定后给出加固解决方案；
7. 对应用代码中不符合安全规范的部分进行规范；
8. 对今后应用代码编写的安全措施给出指导意见。

### （五）第四阶段：漏洞扫描与分析

针对系统进行漏洞扫描，涉及漏洞包括OWASP TOP 10等主流安全漏洞,包括：SQL注入、XSS跨站脚本、伪造跨站请求（CSRF）、隐藏字段、表单绕过、AJAX注入、弱配置、敏感信息泄露、HI-JACK攻击、弱口令、Xpath注入、LDAP注入、框架注入、链接注入、操作系统命令注入、Flash源代码泄露、Flash跨域攻击、Cookie注入、敏感文件、其他各类CGI漏洞。

### （六）第五阶段：安全检测

安全检测采用专业工具扫描（漏洞扫描采用产品必须为商业化产品）、人工评估、渗透测试三种相结合的方式，对目标系统进行评估，包括：帐户与口令安全、网络服务安全、内核参数安全、文件系统安全、日志安全等；从应用系统相关硬件、软件和数据等方面。其他评估内容应至少包括网络设备与防火墙、Web服务、文件服务、Mail服务、数据库问题、跨站脚本攻击、其他服务、其他问题等。

### （七）第六阶段：建设整改咨询及安全加固（不涉及硬件）

建设整改咨询工作以等级测评和渗透检测发现的安全问题为工作重点，编写《信息系统安全建设整改建议》；将信息系统的安全建设整改需求落实到可操作的安全技术和管理上，提出能够实现的技术参数或制度及其具体规范。

### （八）第七阶段：安全培训服务

#### 1. 政策、安全意识培训

对网络安全知识进行宣传培训。内容包括：网络安全法律法规知识普及、典型信息安全事件知识案例讲解、安全保密意识建立以及前沿信息安全技术知识培训等。

#### 2. 安全技术能力培训

针对主机安全、应用安全、网络安全、数据库安全相关的检查方法进行培训，确保项目建设完成后技术人员可以独立完成检测项目的工作内容并完成报告的输出。

### （九）第八阶段：服务与售后

为期一年的服务与售后工作中，服务方将向陕西省地震局提供包括制度完善与方案编制、应急响

	<p>应与安全事件处置、配合检查、电话支持、安全咨询等服务在内的安全维保服务。具体服务时效如下：</p> <p>（1）制度完善与方案编制服务</p> <p>服务方提供制度完善与方案编制等服务。服务时效5X8小时，同时按需提供现场服务，得到通知后4小时内到现场。</p> <p>（2）应急响应与安全事件处置服务</p> <p>针对本次项目，服务方提供7X24的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话10分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。对于网络安全事件处置按需提供现场服务，得到通知后1小时到现场。</p> <p>（3）配合检查服务</p> <p>服务方协助陕西省地震局响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助陕西省地震局准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。</p> <p>（4）电话支持服务</p> <p>每周7天/每天24小时不间断的电话支持服务，解答陕西省地震局在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不小于10分钟，根据不同响应需求到达现场，解决问题不超过24小时。</p> <p>（5）安全咨询服务</p> <p>服务方为陕西省地震局免费提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到用户的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全面配合陕西省地震局做好业务系统全保障工作。</p>
--	---

采购包2：

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

标的名称：等级保护测评

参数性质	序号	技术参数与性能指标
		<p>根据国家《信息安全等级保护管理办法》(公通字[2007]43号)、《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）、《陕西省信息安全等级保护安全建设整改工作指导意见》（陕等保办2011 2号）等相关文件要求，对中国地震局第二监测中心的质检平台软件（三级）和中试平台软件（二级）实施网络安全等级保护测评工作，并提供两年安全维保服务。</p> <p>一、项目服务内容</p> <p>（一）投标人对一个三级系统（质检平台软件）和一个二级系统（中试平台软件）进行网络安全等级保护测评与整改工作，并提交测评报告：</p> <p>1.系统调研：在系统相关人员的协助下，对信息系统进行调研和梳理，了解系统当前信息系统资产现状。</p> <p>2.现场测评：根据国家等级测评的相关标准及已编制的相关等级保护测评指导书对信息系统中的</p>

相关资产进行测评项的检查、记录检查结果。

3.分析整改：根据前述工作内容，分析信息系统安全情况与等级保护基本要求的差距,提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，配合采购单位安全整改工作。

4.结论报告：根据前述工作内容，分析当前信息系统安全保护能力是否符合相应等级的安全要求，针对整改项进行再次测评,提供安全等级符合性测评服务，出具相关系统测评报告。

5.配合验收：整理项目过程中所有相关的过程文档，提交系统相关人员。

6.安全维保服务：提供为期两年的安全维保服务。

7.从合同签订时间起60个工作日完成信息系统的备案、等保测评和报告提交的工作，同时从合同签订时间起两年内提供安全维保服务。

## 二、其他要求

1.测评人员要求：本项目的测评人员需具有1年或1年以上测评工作经验，项目经理和质量负责人必须具备丰富的安全服务经验及相关资质认证，并提供人员管理及配备方案，并确保人员稳定。如需更换测评人员，须由采购单位同意。

2.人员配备：投标方参与此项目不少于6人，现场测评人员不得少于4人，其中至少包含1名高级测评师，3名中级测评师。投标人必须为本项目成立本地化等级保护测评小组，由测评小组组长统一负责，测评小组组长具有一定的技术及管理知识和经验，能容易地与客户沟通，能很好的执行与完成测评工作，并根据适当情况增加测评人员。

3.投标人应按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

## 三、项目技术标准及要求

### (一)总体要求

根据国家《信息安全等级保护管理办法》(公通字[2007]43号)与《信息安全技术 网络安全等级保护基本要求》GB/T22239-2019要求，等级测评工作须覆盖安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面的内容，并根据现场实际情况完成风险分析工作,最终为完善等级保护安全防护体系提供指导依据。

提供为期两年的安全维保服务，确保能够及时应对各项网络安全风险，确保信息系统安全。

### (二)第一阶段：等级保护

信息安全等级保护工作共分为五步，分别是：“定级、备案、建设整改、等级测评、监督检查”。该项目主要完成一个三级和一个二级信息系统的安全测评工作，依据安全技术和安全管理两个方面的测评要求，分别从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个安全类别进行安全测评。

#### 1.定级要求

该项工作开展的主要依据是《网络安全等级保护定级指南》（GB/T 22240-2020），确定两个信息系统的等级。

#### 2.备案

信息系统的安全保护等级确定后，二级以上（含二级）信息系统的运营使用单位或主管部门应到属地公安机关办理备案手续。按照国家政策要求，跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，向当地设区的市级以上公安机关备案。该项目系统应向归属地网络安全监察支队申请重要信息系统备案。

完成备案的信息系统，将获得公安机关颁发的《信息系统安全等级保护备案证明》。

### 3.等级保护测评要求

服务商在测评过程中要求按照《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 网络安全等级保护实施指南》（GB/T25058-2019）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）等相关的标准规范开展不同等级的信息系统等级测评工作，分别对应的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理共10个层面进行安全等级保护测评。测评指标如下：

#### 等级保护技术要求（二级）

安全层面	安全控制点	测评指标
安全物理环境	物理位置	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；
	选择	b) 机房场地应避免设在建筑物的高层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应有专人值守，控制、鉴别和记录进入的人员。
	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记；
		b) 应将通信线缆铺设在隐蔽安全处；
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	防火	a) 机房应设置火灾自动消防系统，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；
	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；
		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。
	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
	温湿度控制	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。
	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，至少满足主要设备在断电情况下的正常运行要求。
	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
安全通信网络	网络架构	a) 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；
		b) 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。
	通信传输	应采用校验技术保证通信过程中数据的完整性。
	可信验证	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。

安全区域 边界	边界防护	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。
	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；
		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；
		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；
		d) 应能根据会话状态信息对进出数据流提供明确的允许/拒绝访问的能力；
	入侵防范	应在关键网络节点处监视网络攻击行为。
	恶意代码防范	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。
	安全审计	a)应在网络边界、重要网络节点处进行安全审计，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；
		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。
	可信验证	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。
安全计算 环境	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；
		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；
		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。
	访问控制	a) 应对登录的用户分配账户和权限；
		b) 应重命名或删除默认账户，修改默认账户的默认口令；
		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；
		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。
	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；
		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。
	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；
		b)应关闭不需要的系统服务、默认共享和高危端口；
		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；
		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；

			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；
		恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。
		可信验证	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。
		数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。
		数据和备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；
			b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
		剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
		个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；
			b) 应禁止未授权访问和非法使用用户个人信息。
	安全管理中心	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；
			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。
		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；
			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。
	安全管理制度	安全策略	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。
		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；
			b) 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。
		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。
			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。
		评审和修订	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。
	安全管理机构	岗位设置	a) 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；
			b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各工作岗位的职责。
		人员配备	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。
		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执行审批过程。
		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；
			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；



				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。
			审核和检查	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。
安全管理 人员	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。
	人员离岗			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。
	安全意识教育和培训			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。
	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。
				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；
				c)外部人员离场后应及时清除其所有的访问权限。
	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；
				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；
				c)应保证定级结果经过相关部门的批准；
				d)应将备案材料报主管部门和相应公安机关备案。
安全建设 管理	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；
				b)应根据保护对象的安全保护等级进行安全方案设计；
				c)应组织相关部门和有关安全专家对安全方案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。
	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；
				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。
	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；
				b)应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。
	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；
				b) 应保证开发单位提供软件设计文档和使用指南。
	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) 应制定安全工程实施方案控制工程实施过程。
	测试验收			a) 应制定测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
				b)应进行上线前的安全性测试，并出具安全测试报告。
	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；
				b)应对负责运行维护的技术人员进行相应的技能培训；
				c)应提供建设过程文档和运行维护文档。
	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；
				b)应在发生重大变更或级别发生变化时进行等级测评；

			c)应确保测评机构的选择符合国家有关规定。
			a)应确保服务供应商的选择符合国家的有关规定；
		服务供应商选择	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。
			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；
			b)应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；
			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。
		安全运维管理	资产管理
			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。
			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；
			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。
			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；
			b)应对配套设施、软硬件维护管理做出规定，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。
			漏洞和风险管理
			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。
			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；
			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；
			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；
			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；
			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。
			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；
			b)应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；
			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。
			配置管理
			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。
			a)应遵循密码相关国家标准和行业标准；
			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。

安全运维管理	变更管理	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。
	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；
		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；
		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。
	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；
		b)应制定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；
		c)应在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。
	应急预案管理	a)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；
		b)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。
	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；
		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。

### 等级保护技术要求（三级）

安全层面	安全控制点	测评指标
安全物理环境	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；
		b)机房场地应避免设在建筑物的高层或地下室，否则应加强防水和防潮措施。
	物理访问控制	a)机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a)应将设备或主要部件进行固定，并设置明显的不易去除的标识；
		b)应将通信线缆铺设在隐蔽安全处；
		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。
	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；
		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。
	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)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。
	防水防潮	a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		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；
		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。
	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；
		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。
	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。
	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。

	电磁防护	a)电源线和通信线缆应隔离铺设，避免互相干扰；
		b)应对关键设备实施电磁屏蔽。
安全通信网络	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；
		b)应保证网络各个部分的带宽满足业务高峰期需要；
		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；
		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；
		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。
	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；
		b)应采用密码技术保证通信过程中数据的保密性。
	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，在监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。
安全区域边界	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；
		b)应能够对非授权设备私自联到内部网络的行为进行检测或限制；
		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；
		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。
	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；
		b)应删除多余或无效的控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
		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；
		d)应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；
		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。
	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；
		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；
		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；
		d)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。
	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；
		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。

安全计算环境	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；
		b)审计记录应包括事件的日期、用户、事件类型、事件是否成功及其他与审计相关的信息；
	可信验证	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；
		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。
	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。
	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；
		b)应启用登陆失败处理功能，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时自动退出等相关措施；
		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；
		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实现。
	访问控制	a)应对登录的用户分配账户和权限；
		b)应重命名或删除默认账户，修改默认账户的默认口令；
		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；
		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；
		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；
		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；
		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。
	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；
		b)审计记录应包括事件的日期、时间、事件类型、事件是否成功及其他与审计相关的工作；
		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；
		d)应对审计进程进行保护，防止未经授权的中断。
	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；
		b)应关闭不需要的系统服务、默认共享和高危端口；
		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；
		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。
		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；

				f)应能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。
	恶意代码 防范			a)应采用免受恶意代码攻击的技术措施，或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
	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。
	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，包括但不限于数据鉴别、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；
				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，包括但不限于数据鉴别、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。
	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，包括但不限于数据鉴别、重要业务数据和重要个人信息等；
				b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于数据鉴别、重要业务数据和重要个人信息等。
	数据备份和恢复			a)应提供重要数据的本地数据备份与恢复功能；
				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用场地；
				c)应提供重要数据处理系统的冗余，保证系统的高可用性。
	剩余信息 保护			a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
				b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
	个人信息 保护			a)应仅采集和保存业务必需的用户个人信息；
				b)应禁止未授权访问和非法使用用户个人信息。
	安全管理中心	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；
				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。
		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；
				b)应通过审计管理员对审计记录进行分析，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。
		安全管理		a)应对安全管理员进行身份鉴别，只允许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；
				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识，对主体进行授权，配置安全可信验证策略等。
				a)应划分特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

			集中管控	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；	
				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；	
				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；	
				e) 应对安全策略、安全代码、补丁升级等安全事项进行集中管理；	
				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。	
			安全管理制度	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。
					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；
				管理制度	b) 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；
					c) 应形成由安全策略，管理制度，操作规程，记录表单等构成安全管理制度体系。
				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；
					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。
				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。
			安全管理机构	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；
					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；
					c) 应设立系统管理员、审计管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。
				人员配备	a) 应配备一定数量的系统管理员、审计管理员、安全管理员等；
					b) 应配备专职的安全管理员，不可兼任。
				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，及时更新授权和审批的项目、审批部门和审批人等信息。
				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。；
					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；
					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。
				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；
					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、安全配置和安全策略的一致性，安全管理制度的执行情况等；

	安全管理人 员		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。	
		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) 应对被录用人的身份、安全背景、专业资格或资质等进行审查，对其所有的技术技能进行考核；	
			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。	
		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；	
			b) 应办理严格的调离手续，并承诺调离后的保密义务方可离开。	
		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；	
			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；	
			c) 应定期对不同岗位的人员进行技能考核。	
		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；	
			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；	
			c) 外部人员离场后应及时清除其所有的访问权限；	
			d) 获得系统访问授权的外部人员签署保密协议，不得进行非授权操作，不得复制和泄露敏感信息。	
		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安全保护等级的方法和理由；	
			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；	
			c) 应保证定级结果经过相关部门的批准；	
			d)应将备案材料报主管部门和相应公安机关备案	
			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；
				b) 应根据保护对象的安全保护等级及与其他级别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；
				c) 应组织相关部门和有关安全技术专家对整体安全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。
			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；
				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；
				c)应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新产品候选名单。
				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；
				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；				



安全建设管理	自行软件开发	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；
		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；
		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；
		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。
	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；
		b) 应保证开发单位提供软件设计文档和使用指南；
		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面和隐蔽信道。
	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) 应制定安全工程实施方案控制实施过程；
		c) 应通过第三方工程监理控制项目的实施过程。
	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；
		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安全测试内容。
	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；
		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) 应提供建设过程文档和运行维护文档。
	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；
		b) 在发生重大变化或级别发生时进行等级测评；
		c) 应确保测评机构的选择符合国家相关规定。
	服务供应商管理	a) 应确保服务供应商的选择符合国家的有关规定；
		b) 应与选定的服务商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
		c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务进行控制。
	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；
		b) 应建立机房安全管理制度，对有关物理访问，物品带进带出和环境安全等方面的管理作出规定；
		c) 应不在重要区域接待来访人员，不随意放置包含敏感信息的纸质文件和移动介质。
	资产管理	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；
		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；

					c) 应对信息分类与标识方法做出规定，并对信息的使用，传输和存储等进行规范化管理。
				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； 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，并对介质归档和查询等进行登记记录。
				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； 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； c) 信息处理设备应经过审批才能带离机房或办公地点，含有储存介质的设备带出工作环境时其重要数据应加密； d) 含有存储介质的设备在报废或重用前，应进行完全清除或完全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
				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； 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。
				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； 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； 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； 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； 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、参数的设置和修改的内容； 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； 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，操作结束后应同步配置更新配置信息库； 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； 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； 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行为。
			安全运维管理		

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；
	b) 应定期验证防范恶意代码攻击的技术措施的有效性。
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、各类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；
	b) 应将基本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。
密码管理	a) 应遵循密码相关国家标准和行业标准；
	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。
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；
	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；
	c) 应建立终止变更并从失败的变更中恢复的程序，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。
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；
	b) 应规定备份信息的备份方式、备份频度、存储介质和保存期等；
	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。
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；
	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；
	c) 应在安全事件和响应处理过程中，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；
	d) 对造成系统中断和造成信息泄露的重大安全事件应采用不同的处理程序和报告程序。
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；
	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；
	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；
	d) 应定期对原有的应急预案重新评估，修订完善。
外包运维管理	a) 应确保外包运维服务商的选择符合国家有关规定；
	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；
	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，并将能力在签订的协议中明确；
	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、储存要求，对IT基础设施中断服务的应急保障要求等。

(三) 第三阶段：建设整改咨询及安全加固（不涉及硬件）

建设整改咨询工作以等级测评发现的安全问题为工作重点，编写《信息系统安全建设整改建议》；将信息系统的安全建设整改需求落实到可操作的安全技术和管理上，提出能够实现的技术参数或制度及其具体规范。

之后在中国地震局第二监测中心依据相关《信息系统安全建设整改建议》开展建设整改工作时，服务方将提供建设整改过程中的与建设整改相关的咨询服务。

对信息系统安全整改建议进行确认，并依照建议，协助我方进行漏洞修复，补丁升级等非硬件层面的安全加固，制定可执行的安全整改方案和计划，然后协助我方分步实施安全整改工作。

#### **(四)第四阶段：售后服务**

为期两年的售后服务工作中，服务方将向中国地震局第二监测中心提供包括应急响应、安全监测、配合检查、电话支持、安全咨询、网络安全培训等服务在内的安全维保服务。具体服务内容如下：

##### **(1) 应急响应服务**

针对本次项目，服务方提供**7X24**的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话**10**分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。

##### **(2) 配合检查服务**

服务方免费协助中国地震局第二监测中心响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助中国地震局第二监测中心准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

##### **(3) 电话支持服务**

每周**7**天/每天**24**小时不间断的电话支持服务，解答中国地震局第二监测中心在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不超过**10**分钟，到达现场时间不超过**2**小时，解决问题不超过**24**小时。

##### **(4) 安全咨询服务**

服务方为中国地震局第二监测中心免费提供二年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到用户的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全面配合中国地震局第二监测中心做好业务系统安全保障工作。

##### **(5) 重保时间段驻场服务**

提供不少于**15**天的重大时期安全保障服务，包括网络安全事件处置和溯源分析，每次重保完成提供分析报告。

##### **(6) 网络安全培训服务**

提供不少于两次的网络安全培训服务，针对网络安全知识及安全法规培训，培训内容包括不限于：网络安全法律法规知识普及、典型信息安全事件知识案例讲解、网络安全风险防范、安全保密意识建立以及前沿信息安全技术知识培训等。

##### **(7) 应急演练服务**

提供网络安全应急演练，模拟网络安全攻击，进行应急演练，增强系统应对安全突发事件的应急处置能力。

#### **四、交付内容**

在本次等级保护测评项目中，服务商须提交主要成果文档包含如下：

- 1.《信息系统安全等级保护定级备案证明》（两个系统各一份）；

		<div>2.《信息系统安全等级保护测评方案》（两个系统各一份）；</div> <div>3.《信息系统安全等级保护测评报告》（两个系统各一份）；</div> <div>4.《信息系统整改建议书》（两个系统各一份）；</div> <div>5.《信息系统渗透测试报告》（三级系统一份）；</div> <div>6.《网络安全应急演练实施方案及总结报告》；</div> <div>7.提供不少于2次网络安全的培训内容。</div>
--	--	--

采购包3：

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

标的名称：密评

参数性质	序号	技术参数与性能指标						
		<div>一、项目概况</div> <div>依据陕西省政务信息化相关要求和新建信息系统验收标准，需要对陕西省巨灾防范工程-数据质检平台项目进行测评服务，该项目主要包含数据质检平台，服务内容包括商用密码应用安全性评估。</div> <div>信息系统商用密码应用安全性评估是根据《中华人民共和国网络安全法》、《商用密码管理条例》《商用密码应用安全性评估管理办法》以及国家关于网络安全等级保护和重要领域密码应用的有关要求，通过对陕西省巨灾防范工程-数据质检平台项目在商用密码技术应用及安全管理方面的测评，对系统密码应用的合规性、正确性、有效性做出判断，给出系统在物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置等方面与其相应安全等级信息系统密码应用基本要求之间的差距，完成商用密码应用安全性评估，出具密码应用安全性评估报告。</div> <div>二、工作内容</div> <div>需按要求完成对陕西省巨灾防范工程-数据质检平台项目的商用密码应用安全性评估服务，并出具经权威机构认可的《商用密码应用安全性评估报告》，协助用户单位进行问题整改，整改后进行复测评工作。</div> <table><tr><td>服务内容</td><td>系统数量</td><td>系统名称</td></tr><tr><td>商用密码应用安全性评估服务</td><td>1</td><td>数据质检平台</td></tr></table>	服务内容	系统数量	系统名称	商用密码应用安全性评估服务	1	数据质检平台
服务内容	系统数量	系统名称						
商用密码应用安全性评估服务	1	数据质检平台						

### 三、技术依据

《中华人民共和国密码法》

《中华人民共和国网络安全法》

《信息安全技术 信息系统密码应用基本要求》GB/T 39786-2021

《信息系统密码应用测评要求》GM/T0115-2021

《信息系统密码应用测评过程指南》GM/T0116-2021

信息系统密码应用高风险判定指引（2021）

商用密码应用安全性评估量化评估规则（2023版）

《商用密码应用安全性评估管理办法》

《政务信息系统密码应用与安全性评估工作指南（2020 版）》

GB/T 15843.3-2016《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》

GM/T 0001.1-2012《祖冲之序列密码算法 第1部分：算法描述》

GM/T 0001.2-2012《祖冲之序列密码算法 第2部分：基于祖冲之算法的机密性算法》

GM/T 0001.3-2012《祖冲之序列密码算法 第3部分：基于祖冲之算法的完整性算法》

GM/T 0002-2012《SM4分组密码算法》

GM/T 0003.1-2012《SM2椭圆曲线公钥密码算法 第1部分：总则》

GM/T 0003.2-2012《SM2椭圆曲线公钥密码算法 第2部分：数字签名算法》

GM/T 0003.3-2012《SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议》

GM/T 0003.4-2012《SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法》

GM/T 0003.5-2012《SM2椭圆曲线公钥密码算法 第5部分：参数定义》

GM/T 0004-2012《SM3密码杂凑算法》

GM/T 0005-2012《随机性检测规范》

GM/T 0006-2012《密码应用标识规范》

GM/T 0008-2012《安全芯片密码检测准则》

GM/T 0009-2012《SM2密码算法使用规范》

GM/T 0010-2012《SM2密码算法加密签名消息语法规范》

GM/T 0011-2012《可信计算 可信密码支撑平台功能与接口规范》

GM/T 0012-2012《可信计算 可信密码模块接口规范》

GM/T 0013-2012《可信计算 可信密码模块接口符合性测试规范》

GM/T 0014-2012《数字证书认证系统密码协议规范》

GM/T 0015-2012《基于SM2密码算法的数字证书格式规范》

GM/T 0016-2012《智能密码钥匙密码应用接口规范》

GM/T 0017-2012《智能密码钥匙密码应用接口数据格式规范》

GM/T 0018-2012《密码设备应用接口规范》

GM/T 0019-2012《通用密码服务接口规范》

GM/T 0020-2012《证书应用综合服务接口规范》

GM/T 0021-2012《动态口令密码应用技术规范》

GM/T 0022-2014《IPSec VPN 技术规范》

GM/T 0023-2014《IPSec VPN 网关产品规范》

- GM/T 0024-2014 《SSL VPN 技术规范》
- GM/T 0025-2014 《SSL VPN 网关产品规范》
- GM/T 0026-2014 《安全认证网关产品规范》
- GM/T 0027-2014 《智能密码钥匙技术规范》
- GM/T 0028-2014 《密码模块安全技术要求》
- GM/T 0029-2014 《签名验签服务器技术规范》
- GM/T 0030-2014 《服务器密码机技术规范》
- GM/T 0031-2014 《安全电子签章密码技术规范》
- GM/T 0032-2014 《基于角色的授权管理与访问控制技术规范》
- GM/T 0033-2014 《时间戳接口规范》
- GM/T 0034-2014 《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》
- GM/T 0035.1-2014 《射频识别系统密码应用技术要求 第1部分：密码安全保护框架及安全级别》
- GM/T 0035.2-2014 《射频识别系统密码应用技术要求 第2部分：电子标签芯片密码应用技术要求》
- GM/T 0035.3-2014 《射频识别系统密码应用技术要求 第3部分：读写器密码应用技术要求》
- GM/T 0035.4-2014 《射频识别系统密码应用技术要求 第4部分：电子标签与读写器通信密码应用技术要求》
- GM/T 0035.5-2014 《射频识别系统密码应用技术要求 第5部分：密钥管理技术要求》
- GM/T 0036-2014 《采用非接触卡的门禁系统密码应用技术指南》
- GM/T 0037-2014 《证书认证系统检测规范》
- GM/T 0038-2014 《证书认证密钥管理系统检测规范》
- GM/T 0039-2015 《密码模块安全检测要求》
- GM/T 0040-2015 《射频识别标签模块密码检测准则》
- GM/T 0041-2015 《智能IC卡密码检测规范》
- GM/T 0042-2015 《三元对等密码安全协议测试规范》
- GM/T 0043-2015 《数字证书互操作检测规范》
- GM/T 0044-2016 《SM9标识密码算法》
- GM/T 0045-2016 《金融数据密码机技术规范》

#### 四、技术要求

##### 1、商用密码应用安全性评估技术要求；

商用密码应用安全性评估工作依据《信息安全技术 信息系统密码应用基本要求》、《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》标准，工作过程分为四项基本测评活动：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。测评双方之间的沟通与洽谈贯穿整个测评过程。

测评准备活动：本活动是开展测评工作的前提和基础，本活动的主要任务是掌握被测系统的详细情况，准备测评工具，为编制测评方案做好准备。

方案编制活动：本活动是开展测评工作的关键活动，本活动的主要任务是确定与被测系统相适应的测评对象、测评指标及测评内容等，形成测评方案，为实施现场测评提供依据。

	<p><b>现场测评活动：</b>本活动是开展测评工作的核心活动。主要任务是按照测评方案的总体要求，分步实施所有测评项目，包括单项测评、测评单元和整体测评等方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的密码应用安全性问题。</p> <p><b>分析与报告编制活动：</b>本活动是给出测评工作结果的活动，是总结被测系统商用密码整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和《信息系统密码应用基本要求》等文件的有关要求，通过单项测评结果判定、测评单元结果判定、整体测评和风险分析等方法，找出整个系统商用密码的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出测评结论，形成测评报告文本。</p> <p><b>整改咨询阶段：</b>建设整改咨询工作以测评发现的问题为重点，编写信息系统密码测评整改建议；开展建设整改工作时，投标人提供建设整改相关的咨询服务。</p> <p><b>2、其他要求：</b></p> <p><b>（1）服务质量保证：</b>测评机构应根据质量体系要求建立科学的质量保证体系，从人员配备、工具保障以及科学的测评方法论、工作过程等多方面保证项目实施过程的质量。并在重要环节进行文档评审，保证报告结论准确性；测评机构需要位于国家密码管理局公告（第42号）商用密码应用安全性评估试点机构目录（共48家）中。</p> <p><b>（2）测评工具配备：</b>要求在测评工作过程中配备专用测评工具，投标人应提供工具采购证明材料。</p> <p><b>（3）测评人员要求：</b>本项目的测评人员需具有 1年以上测评工作经验，项目负责人和质量负责人必须具备丰富的安全服务经验及相关资质认证，并提供人员配备方案，并确保人员稳定。如需更换测评人员，须由招标单位同意。</p> <p><b>（4）测评人员配备：</b>本项目要求测评人员不少于5人，项目经理与项目组成员要求具备“商用密码应用安全性评估人员测评能力考核合格证书”。</p> <p><b>（5）项目保密要求：</b>a.采购人应严格遵守采购单位有关保密规定，不得泄漏相关系统的一切信息。</p> <p>b.采购人要对项目进行深入细致调研，并结合实际对测评方案进行完善。在测评过程中，采购人需保证工具测试过程中不影响系统正常运行，并保证网络拓扑、IP地址等信息不被泄露。</p> <p>c.在技术服务期间，采购人对接触到的有关采购单位商业活动、技术情报和技术资料等文件进行保密。</p> <p><b>五、成果验收及资料提交</b></p> <p>由采购人统一组织，采购人与相关人员组成验收小组完成验收。双方根据最终验收情况，编写验收报告。</p> <p>中标人应完成项目验收资料的准备，出具经权威机构认可的《商用密码应用安全性评估报告》，协助用户单位进行问题整改，整改后进行复测评工作。</p>
--	--

### 3.2.3人员配置要求

采购包1:

详见服务内容及服务要求

采购包2:

详见服务内容及服务要求



采购包3:

详见服务内容及服务要求

### **3.2.4设施设备配置要求**

采购包1:

详见服务内容及服务要求

采购包2:

详见服务内容及服务要求

采购包3:

详见服务内容及服务要求

### **3.2.5其他要求**

采购包1:

详见服务内容及服务要求

采购包2:

详见服务内容及服务要求

采购包3:

详见服务内容及服务要求

## **3.3商务要求**

### **3.3.1服务期限**

采购包1:

服务期：从甲方通知开始测评日期起，30个工作日完成等保测评和报告提交的所有工作；同时从合同签订时间起一年内提供一次安全应急模拟演练、不限次数的制度完善与方案编制、应急响应与安全事件处置、配合检查、电话支持、安全咨询等服务在内的安全维保服务。

采购包2:

服务期：从合同签订时间起60个工作日完成信息系统的备案、等保测评和报告提交的工作，同时从合同签订时间起两年内提供安全维保服务。

采购包3:

服务期：自项目实施起45日历天内完成。

### **3.3.2服务地点**

采购包1:

陕西省地震局指定地点。

采购包2:

陕西省地震局指定地点。

采购包3:

陕西省地震局指定地点。

### **3.3.3考核（验收）标准和方法**

采购包1:

1、招标文件、投标文件、澄清表（函）； 2、合同及附件文本； 3、国家相应的标准、规范。

采购包2:

1、招标文件、投标文件、澄清表（函）； 2、合同及附件文本； 3、国家相应的标准、规范。

采购包3:

1、招标文件、投标文件、澄清表（函）； 2、合同及附件文本； 3、国家相应的标准、规范。

#### **3.3.4支付方式**

采购包1:

一次付清

采购包2:

一次付清

采购包3:

一次付清

#### **3.3.5.支付约定**

采购包1: 付款条件说明: 合同签订后7个工作日内, 由乙方向甲方支付5%的履约保证金, 甲方收到后, 达到付款条件起 15 日内, 支付合同总金额的 100.00%。

采购包2: 付款条件说明: 合同签订后7个工作日内, 由乙方向甲方支付5%的履约保证金, 甲方收到后, 达到付款条件起 15 日内, 支付合同总金额的 100.00%。

采购包3: 付款条件说明: 合同签订后7个工作日内, 由乙方向甲方支付5%的履约保证金, 甲方收到后, 达到付款条件起 15 日内, 支付合同总金额的 100.00%。

#### **3.3.6违约责任与争议解决的方法**

采购包1:

根据招标文件、投标文件及合同约定执行。

采购包2:

根据招标文件、投标文件及合同约定执行。

采购包3:

根据招标文件、投标文件及合同约定执行。

#### **3.5其他要求**

1、本项目兼投不兼中, 评审时按标段顺序进行评审, 投标人如为上一标段的第一中标候选人, 则下一标段将不进入中标候选人推荐。 2、供应商需要在线提交所有通过电子化交易平台实施的政府采购项目的响应文件, 同时, 线下提交响应文件正本 壹 份、副本 贰 份 (双面打印, 自行编辑页码及目录)、电子版 壹 份 (U盘一套标明供应商名称, 单独密封)。 3、线下纸质文件递交截止时间: 同在线递交电子响应文件截止时间一致; 线下纸质文件递交地点: 西安市雁展路1111号莱安中心 T6-15层。(如需邮寄, 建议顺丰速运, 并将单位名称、联系人、电话及运单号发至809502949@qq.com邮箱)

## 第四章 资格审查

资格审查由采购人或代理机构组建的资格审查小组依据法律法规和招标文件的规定，对投标文件中的资格证明等进行审查，以确定投标人是否具备投标资格，并出具资格审查报告。

资格审查标准及要求如下：

### 4.1 一般资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标人资格条件证明文件-采购包1 投标函
2	供应商应提供健全的财务会计制度的证明材料；	供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人资格条件证明文件-采购包1
3	单位负责人为同一人或者存在直接控股、管理关系的不同供应商不得参加同一合同项下的政府采购活动； 为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标人资格条件证明文件-采购包1 投标函

采购包2：

序号	资格审查要求概况	评审点具体描述	关联格式
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标人资格条件证明文件-采购包2 投标函
2	供应商应提供健全的财务会计制度的证明材料；	供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人资格条件证明文件-采购包2
3	单位负责人为同一人或者存在直接控股、管理关系的不同供应商不得参加同一合同项下的政府采购活动； 为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标人资格条件证明文件-采购包2 投标函

采购包3：

序号	资格审查要求概况	评审点具体描述	关联格式
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函 投标人资格条件证明文件-采购包3

2	供应商应提供健全的财务会计制度的证明材料；	供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人资格条件证明文件-采购包3
3	单位负责人为同一人或者存在直接控股、管理关系的不同供应商不得参加同一合同项下的政府采购活动；为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函 投标人资格条件证明文件-采购包3

4.2特殊资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	有效的主体资格证明	具有独立承担民事责任能力的法人、其他组织或自然人，并出具合法有效的营业执照或事业单位法人证书等国家规定的相关证明，自然人参与的提供其身份证明。	投标人资格条件证明文件-采购包1
2	财务状况报告	提供2022年度或2023年度经审计的财务报告（包括“四表一注”，即资产负债表、利润表、现金流量表、所有者权益变动表及其附注，成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前六个月内银行出具的资信证明。（以上两种形式的资料提供任何一种即可）	投标人资格条件证明文件-采购包1
3	税收缴纳证明	提供2023年7月至今已缴纳至少一个月的依法缴纳税款的相关凭据（时间以税款所属日期为准、税种须包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税款的投标人，应提供相关证明文件。	投标人资格条件证明文件-采购包1
4	社会保障资金缴存证明	提供2023年7月至今已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。	投标人资格条件证明文件-采购包1
5	书面声明	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纪，以及未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单的书面声明。本项目拒绝被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为的投标人参与。	投标人资格条件证明文件-采购包1

6	承诺函	提供具有履行合同所必需的设备和专业技术能力的承诺函。	投标人资格条件证明文件-采购包1
7	法定代表人授权书	法定代表人授权书及被授权人身份证明。（法定代表人直接投标只须提供其身份证明）	投标人资格条件证明文件-采购包1
8	特定资质	具备《网络安全等级测评与检测评估机构服务认证证书》。	投标人资格条件证明文件-采购包1

采购包2:

序号	资格审查要求概况	评审点具体描述	关联格式
1	有效的主体资格证明	具有独立承担民事责任能力的法人、其他组织或自然人，并出具合法有效的营业执照或事业单位法人证书等国家规定的相关证明，自然人参与的提供其身份证明。	投标人资格条件证明文件-采购包2
2	财务状况报告	提供2022年度或2023年度经审计的财务报告（包括“四表一注”，即资产负债表、利润表、现金流量表、所有者权益变动表及其附注，成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前六个月内银行出具的资信证明。（以上两种形式的资料提供任何一种即可）	投标人资格条件证明文件-采购包2
3	税收缴纳证明	提供2023年7月至今已缴纳至少一个月的依法缴纳税款的相关凭据（时间以税款所属日期为准、税种须包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税款的投标人，应提供相关证明文件。	投标人资格条件证明文件-采购包2
4	社会保障资金缴存证明	提供2023年7月至今已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。	投标人资格条件证明文件-采购包2
5	书面声明	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纪，以及未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单的书面声明。本项目拒绝被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为的投标人参与。	投标人资格条件证明文件-采购包2
6	承诺函	提供具有履行合同所必需的设备和专业技术能力的承诺函。	投标人资格条件证明文件-采购包2
7	法定代表人授权书	法定代表人授权书及被授权人身份证明。（法定代表人直接投标只须提供其身份证明）	投标人资格条件证明文件-采购包2

8	特定资质	具备《网络安全等级测评与检测评估机构服务认证证书》。	投标人资格条件证明文件-采购包2
---	------	----------------------------	------------------

采购包3:

序号	资格审查要求概况	评审点具体描述	关联格式
1	有效的主体资格证明	具有独立承担民事责任能力的法人、其他组织或自然人，并出具合法有效的营业执照或事业单位法人证书等国家规定的相关证明，自然人参与的提供其身份证明。	投标人资格条件证明文件-采购包3
2	财务状况报告	提供2022年度或2023年度经审计的财务报告（包括“四表一注”，即资产负债表、利润表、现金流量表、所有者权益变动表及其附注，成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前六个月内银行出具的资信证明。（以上两种形式的资料提供任何一种即可）	投标人资格条件证明文件-采购包3
3	税收缴纳证明	提供2023年7月至今已缴纳至少一个月的依法缴纳税款的相关凭据（时间以税款所属日期为准、税种须包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税款的投标人，应提供相关证明文件。	投标人资格条件证明文件-采购包3
4	社会保障资金缴存证明	提供2023年7月至今已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。	投标人资格条件证明文件-采购包3
5	书面声明	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纪，以及未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单的书面声明。本项目拒绝被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为的投标人参与。	投标人资格条件证明文件-采购包3
6	承诺函	提供具有履行合同所必需的设备和专业技术能力的承诺函。	投标人资格条件证明文件-采购包3
7	法定代表人授权书	法定代表人授权书及被授权人身份证明。（法定代表人直接投标只须提供其身份证明）	投标人资格条件证明文件-采购包3
8	特定资质	投标人须是国家密码管理局第42号文中《商用密码应用安全性评估试点机构目录》的测评机构，提供证明材料。	投标人资格条件证明文件-采购包3

#### 4.3落实政府采购政策资格审查

采购包1:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包2:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包3:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

## 第五章 评标办法

### 5.1 总则

一、根据《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》《政府采购货物和服务招标投标管理办法》等法律法规，结合采购项目特点制定本评标办法。

二、评标工作由代理机构负责组织，具体评标事务由采购人或代理机构依法组建的评标委员会负责。评标委员会由采购人代表和评审专家组成。

三、评标工作应遵循公平、公正、科学及择优的原则，并以相同的评标程序 and 标准对待所有的投标人。

四、本项目采取电子评审，通过项目电子化交易系统完成评审工作。评标委员会成员、采购人、代理机构和投标人应当按照本招标文件规定和项目电子化交易系统操作要求开展或者参加评标活动。

五、评标过程中的书面材料往来均通过项目电子化交易系统传递，投标人通过互认的证书及签章加盖其电子印章后生效。出现无法在线签章的特殊情况，评标委员会成员可以线下签署评标报告，由代理机构对原件扫描后以附件形式上传。

六、评标过程应当独立、保密，任何单位和个人不得非法干预评标活动。投标人非法干预评标活动的，其投标文件将作无效处理；代理机构、采购人及其工作人员、采购人监督人员非法干预评标活动的，将依法追究其责任。

### 5.2 评标委员会

评审专家是采取随机方式在政府采购平台的专家库系统（以下简称专家库系统）抽取/由采购人根据《陕西省政府采购评审专家管理实施办法》（陕财办采〔2018〕20号）的规定，报主管部门同意后自行选定。

二、评标委员会成员应当满足并适应电子化采购评审的工作需要，使用已身份认证并具备签章功能的证书，登录项目电子化交易系统进入项目评审功能模块确认身份、签到、推荐评标委员会组长。采购人代表可以使用采购人代表专用签章确认评审意见。

三、评标委员会成员获取解密后的投标文件，开展评标活动。出现应当回避的情形时，评标委员会成员应当主动回避；代理机构按规定申请补充抽取评审专家；无法及时补充抽取的，采购人或者代理机构应当封存供应商投标文件，按规定重新组建评标委员会，解封投标文件后，开展评标活动。

四、评标委员会按照招标文件规定的评标程序、评标方法和标准进行评标，并独立履行下列职责：

- （一）熟悉和理解招标文件；
- （二）审查供应商投标文件等是否满足招标文件要求，并作出评价；
- （三）根据需要要求采购组织单位对招标文件作出解释；根据需要要求供应商对投标文件有关事项作出澄清、说明或者更正；
- （四）推荐中标候选供应商，或者受采购人委托确定中标供应商；
- （五）起草评标报告并进行签署；
- （六）向采购组织单位、财政部门或者其他监督部门报告非法干预评审工作的行为；
- （七）法律、法规和规章规定的其他职责。

### 5.3 评标方法

采购包1：综合评分法

采购包2：综合评分法

采购包3：综合评分法

### 5.4 评标程序

#### 5.4.1 熟悉和理解招标文件和停止评标



一、评标委员会正式评审前，应当对招标文件进行熟悉和理解，内容主要包括招标文件中供应商资格资质性要求、采购项目技术、服务和商务要求、评审方法和标准以及可能涉及签订政府采购合同的内容等。

二、本招标文件有下列情形之一的，评标委员会应当停止评标：

- （一）招标文件的规定存在歧义、重大缺陷的；
- （二）招标文件明显以不合理条件对供应商实行差别待遇或者歧视待遇的；
- （三）采购项目属于国家规定的优先、强制采购范围，但是招标文件未依法体现优先、强制采购相关规定的；
- （四）采购项目属于政府采购促进中小企业发展的范围，但是招标文件未依法体现促进中小企业发展相关规定的；
- （五）招标文件规定的评标方法是综合评分法、最低评标价法之外的评标方法，或者虽然名称为综合评分法、最低评标价法，但实际上不符合国家规定；
- （六）招标文件将投标人的资格条件列为评分因素的；
- （七）招标文件有违反国家其他有关强制性规定的情形。

出现上述应当停止评标情形的，评标委员会应当通过项目电子化交易系统向采购组织单位提交相关说明材料，说明停止评审的情形和具体理由。除上述情形外，评标委员会不得以任何方式和理由停止评标。

出现上述应当停止评标情形的，采购组织单位应当通过项目电子化交易系统书面告知参加采购活动的供应商，并说明具体原因，同时在陕西省政府采购网公告。采购组织单位认为评标委员会不应当停止评标的，可以书面报告采购项目同级财政部门依法处理，并提供相关证明材料。

5.4.2 符合性审查

评标委员会依据本招标文件的实质性要求，对符合资格的投标文件进行审查，以确定其是否满足本招标文件的实质性要求。本项目符合性审查事项，必须以本招标文件的明确规定的实质性要求作为依据。

在符合性审查过程中，如果出现评标委员会成员意见不一致的情况，按照少数服从多数的原则确定，但不得违背政府采购基本原则和招标文件规定。

符合性审查标准见下表（按以下顺序审查）：

采购包1：

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	1.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。 2.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。	开标一览表 标的清单 报价表、分项报价表

2	投标人名称	投标人名称与营业执照、资质证书一致	商务条款响应说明 投标人资格条件证明文件-采购包1 投标函 中小企业声明函 残疾人福利性单位声明函 保证金交纳凭证 标的清单 服务内容及服务要求应答表 投标人承诺书 投标文件封面 报价表、分项报价表 监狱企业的证明文件
3	投标文件的签署、盖章	投标文件按招标文件要求的数量、计量单位、报价货币及签字盖章	商务条款响应说明 投标人资格条件证明文件-采购包1 投标函 中小企业声明函 残疾人福利性单位声明函 保证金交纳凭证 标的清单 服务内容及服务要求应答表 投标人承诺书 投标文件封面 报价表、分项报价表 监狱企业的证明文件
4	投标有效期	投标有效期达到招标文件要求	投标函
5	投标保证金	保证金交纳符合招标文件要求	保证金交纳凭证
6	其他实质性要求	符合法律、法规和招标文件中规定的其他实质性要求	商务条款响应说明 服务内容及服务要求应答表

采购包2:

序号	符合审查要求概况	评审点具体描述	关联格式
----	----------	---------	------

1	不正当竞争预防措施（实质性要求）	<p>1.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。</p> <p>2.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	<p>开标一览表 标的清单 报价表、分项报价表</p>
2	投标人名称	投标人名称与营业执照、资质证书一致	<p>商务条款响应说明 投标人资格条件证明文件-采购包2 投标函 中小企业声明函 残疾人福利性单位声明函 保证金交纳凭证 标的清单 服务内容及服务要求应答表 投标人承诺书 投标文件封面 报价表、分项报价表 监狱企业的证明文件</p>
3	投标文件的签署、盖章	投标文件按招标文件要求的数量、计量单位、报价货币及签字盖章	<p>商务条款响应说明 投标人资格条件证明文件-采购包2 投标函 中小企业声明函 残疾人福利性单位声明函 保证金交纳凭证 标的清单 服务内容及服务要求应答表 投标人承诺书 投标文件封面 报价表、分项报价表 监狱企业的证明文件</p>
4	投标有效期	投标有效期达到招标文件要求	投标函
5	投标保证金	保证金交纳符合招标文件要求	保证金交纳凭证

6	其他实质性要求	符合法律、法规和招标文件中规定的其他实质性要求	商务条款响应说明 服务内容及服务要求应答表
---	---------	-------------------------	-----------------------

采购包3:

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	<p>1.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。</p> <p>2.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	<p>开标一览表 标的清单 报价表、分项报价表</p>
2	投标人名称	投标人名称与营业执照、资质证书一致	<p>商务条款响应说明 投标函 中小企业声明函 残疾人福利性单位声明函 保证金交纳凭证 标的清单 服务内容及服务要求应答表 投标人承诺书 投标文件封面 报价表、分项报价表 监狱企业的证明文件 投标人资格条件证明文件-采购包3</p>

3	投标文件的签署、盖章	投标文件按招标文件要求的数量、计量单位、 报价货币及签字盖章	商务条款响应说明 投 标函 中小企业声明函 残疾人福利性单位声 明函 保证金交纳凭证 标的清单 服务内容及 服务要求应答表 投标 人承诺书 投标文件封 面 报价表、分项报价 表 监狱企业的证明文 件 投标人资格条件证 明文件-采购包3
4	投标有效期	投标有效期达到招标文件要求	投标函
5	投标保证金	保证金交纳符合招标文件要求	保证金交纳凭证
6	其他实质性要求	符合法律、法规和招标文件中规定的其他实质 性要求	商务条款响应说明 服 务内容及服务要求应 答表

以上实质性要求全部响应并满足采购需求的，则通过符合性审查；如有任意一项未响应或不满足采购需求的，则按无效投标文件处理。如果评标委员会认为投标人有任意一项不通过的，应在符合性审查表中载明不通过的具体原因。

#### 5.4.3解释、澄清有关问题

一、评标过程中，评标委员会认为招标文件有关事项表述不明确或需要说明的，可以提请代理机构书面解释。代理机构的解释不得改变招标文件的原义或者影响公平、公正，解释事项如果涉及投标人权益的以有利于投标人的原则进行解释。

二、对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当要求投标人作出必要的澄清、说明或更正，并给予投标人必要的反馈时间。投标人应当按评标委员会的要求进行澄清、说明或者更正。投标人的澄清、说明或者更正不得超出投标文件的范围或者改变投标文件的实质性内容。澄清、说明或者更正不影响投标文件的效力，有效的澄清、说明或者更正材料是投标文件的组成部分。

三、投标人的澄清、说明或者更正需进行电子签章，应当不超出投标文件的范围、不实质性改变投标文件的内容、不影响投标人的公平竞争、不导致投标文件从不响应招标文件变为响应招标文件的条件。下列内容不得澄清：

- （一）投标人投标文件中不响应招标文件规定的技术参数指标和商务应答；
- （二）投标人投标文件中未提供的证明其是否符合招标文件资格、符合性规定要求的相关材料。
- （三）投标人投标文件中的材料因印刷、影印等不清晰而难以辨认的。

四、投标文件报价出现下列情况的，按以下原则处理：

- （一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；
- （二）大写金额和小写金额不一致的，以大写金额为准，但大写金额出现文字错误，导致金额无法判断的除外；
- （三）单价金额小数点或者百分比有明显错位的，以开标一览表总价为准，并修改单价；
- （四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

五、对不同语言文本投标文件的解释发生异议的，以中文文本为准。

六、代理机构宣布评标结束前，投标人应通过项目电子化交易系统随时关注评标消息提示，及时响应评标委员会发出的澄清、说明或更正要求。投标人未能及时响应的，自行承担不利后果。

评标委员会应当积极履行澄清、说明或者更正的职责，不得滥使用权力。

#### **5.4.4比较与评价**

评标委员会应当按照招标文件规定的评标细则及标准，对符合性检查合格的投标文件进行商务和技术评估，综合比较和评价。

#### **5.4.5复核**

评分汇总结束后，评标委员会应当进行复核，对拟推荐为中标候选供应商、报价最低、投标文件被认定为无效等进行重点复核。

评标结果汇总完成后，评标委员会拟出具评标报告前，代理机构应当组织不少于2名工作人员，在采购监督人员的监督之下，依据有关的法律制度和招标文件对评标结果进行复核，出具复核报告。

评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

- （一）分值汇总计算错误的；
- （二）分项评分超出评分标准范围的；
- （三）评标委员会成员对客观评审因素评分不一致的；
- （四）经评标委员会认定评分畸高、畸低的。

评标报告签署前，经复核发现存在以上情形之一的，评标委员会应当当场修改评标结果，并在评标报告中记载；评标报告签署后，采购人或者代理机构发现存在以上情形之一的，应当组织原评标委员会进行重新评审，重新评审改变评标结果的，书面报告本级财政部门。

#### **5.4.6确定中标候选人名单**

采购包1：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包2：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包3：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

#### **5.4.7编写评标报告**

评标报告是评标委员会根据全体评标成员签字的评标记录和评标结果编写的报告，其主要内容包括：

- 一、招标公告刊登的媒体名称、开标日期和地点；
- 二、投标人名单和评标委员会成员名单；
- 三、评标方法和标准；
- 四、开标记录和评标情况及说明，包括投标无效投标人名单及原因；
- 五、评标结果，确定的中标候选人名单或者经采购人委托直接确定的中标人；
- 六、其他需要说明的情况，包括评标过程中投标人根据评标委员会要求进行的澄清、说明或者更正，评标委员会成员的更换等；

七、报价最高的投标人为中标候选人的，评标委员会应当对其报价的合理性予以特别说明。

评标委员会成员应当在评标报告中签字或加盖电子签章确认，对评标过程和结果有不同意见的，应当在评标报告中写明并

说明理由。签字但未写明不同意见或者未说明理由的，视同无意见。拒不签字或加盖电子签章又未另行说明其不同意见和理由的，视同同意评标结果。

5.5 评标争议处理规则

评标委员会在评标过程中，对于符合性审查、对投标人文件作无效投标处理及其他需要共同认定的事项存在争议的，应当以少数服从多数的原则作出结论，但不得违背法律法规和招标文件规定。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。持不同意见的评标委员会成员认为认定过程和结果不符合法律法规或者招标文件规定的，应当及时向采购人或代理机构书面反映。采购人或代理机构收到书面反映后，应当书面报告采购项目同级财政部门依法处理。

5.6 评标细则及标准

一、评标委员会只对通过资格审查的投标文件，根据招标文件的要求采用相同的评标程序、评分办法及标准进行评价和比较。

二、评标委员会成员应依据招标文件规定的评分标准和方法独立评审。

5.6.1 评分办法

（综合评分法适用）采用综合评分法的，由评标委员会各成员对通过资格检查和符合性审查的投标人的投标文件进行独立评审。

投标报价得分=（评标基准价 / 投标报价）×100

评标总得分=F1×A1+F2×A2+.....+Fn×An

F1、F2.....Fn分别为各项评审因素的得分；

A1、A2、.....An 分别为各项评审因素所占的权重（A1+A2+.....+An=1）。

评标过程中，不得去掉报价中的最高报价和最低报价。

因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

5.6.2 评分标准

采购包1：

评审因素		评审标准			
分值构成		详细评审90.0000分 报价得分10.0000分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式

	实施方案	<p>投标人结合本项目实际需求，提供完整的项目工作流程和实施方案，对被测单位信息系统现状掌握、熟悉，信息等级测评各个工作阶段的工作内容、工作方法及工作成果具有详细说明。1、方案内容全面、细致详细、合理可行，完全满足项目需求，计20分；2、方案内容较为全面、切合实际，基本满足项目需求，计15分；3、方案内容基本全面、可行性一般，计10分；4、方案内容欠缺，可行性差，计5分；5、理解有偏差，无法满足本项目需求，计1分；6、未提供的计0分。</p>	20.0000	主观	投标方案说明-采购包1
	风险防范和保密措施	<p>针对本项目的服务提供明确的过程风险防范措施和保密措施，并明确保密责任与赔偿承诺。1、措施内容详尽，切合实际，完全满足项目需求，计10分；2、措施内容较为全面、切合实际、基本满足项目需求，计7分；3、措施内容基本全面、可行性一般，计3分；4、措施内容简单，不切合实际，计1分；5、未提供的计0分。</p>	10.0000	主观	投标方案说明-采购包1
	质量管控	<p>方案需详细说明本项目的质量管控措施、过程控制及监控手段，能保证技术人员按照相应的操作指导规范实施测评。1、措施详细具体、合理可行，完全满足项目需求，计10分；2、措施较为全面详细，切合实际，基本满足项目需求，计7分；3、措施基本全面合理，可行性一般，计3分；4、措施内容欠缺，可行性差，计1分；5、未提供的计0分。</p>	10.0000	主观	投标方案说明-采购包1



详细评审	测评团队	<p>本项目派往现场的测评团队成员不少于5人，工作经验不少于1年，否则本项不计分。1、团队成员中至少5人为中级或以上测评师，其中高级测评师不少于2人，计5分；2、团队成员中4人为中级或以上测评师，其中高级测评师不少于2人，计3分；3、团队成员中3人为中级或以上测评师，其中高级测评师不少于2人，计2分；4、其余情况不计分。注：以相关证书、相关人员在本站的任职证明及全国网络安全等级保护网查询结果为准。</p>	5.0000	客观	投标方案说明-采购包1
	项目经理	<p>拟派本项目的项目经理在具备高级测评师证书基础上具备以下证书（无高级测评师证书本项不计分）： 1、注册信息安全开发人员（CISP-CISD）；2、渗透测试工程师（高级）证书；3、网络安全能力认证证书（CCSC）-网络安全管理II级及以上；4、注册密码技术专家证书（CISP-CTE）；5、信息系统安全专业认证证书（CISSP）；每具备一项计2分，此项满分10分。注：以证书复印件及相关人员在本站的任职证明为准。</p>	10.0000	客观	投标方案说明-采购包1

团队证书	拟派本项目团队（除项目经理）在具备中级或以上测评师证书基础上具备以下证书（无中级或以上测评师证书本项不计分）： 1）信息安全保障人员认证证书（CISAW）-风险管理（专业级）； 2）渗透测试工程师（高级）证书或注册渗透测试工程师（CISP-PTE）； 3）重要信息系统保护人员证书（CIIP-D）； 4）注册信息安全工程师证书（CISP-CISE）； 5）网络安全能力认证证书(CCSC)-网络安全技术； 每具备一项计1分，此项满分5分。 注：以证书复印件及相关人员在本单位的任职证明为准。	5.0000	客观	投标方案说明-采购包1
售后服务	为保障测评项目结束后的信息安全，要求投标人提供完善的售后服务，包括应急响应服务、电话支持服务、配合检查服务、安全咨询服务、安全培训服务等内容，能提供以上售后服务并做出相应服务说明。 1、方案内容全面、细致详细、合理可行，完全满足项目需求，计5分； 2、方案内容基本全面、可行性一般，计3分； 3、方案内容欠缺，可行性差，计1分； 4、未提供的计0分。	5.0000	主观	投标方案说明-采购包1
培训方案	投标人针对本项目提供详尽的培训方案及培训计划，包括培训需求分析、培训对象、培训方式、培训人数、培训时间等安排。 1、方案内容完善，合理可行，针对性强，计5分； 2、方案内容基本完整、合理性、可行性、针对性一般，计3分； 3、方案内容欠缺，可行性差，计1分； 4、未提供的计0分	5.0000	主观	投标方案说明-采购包1

	企业实力	1、投标人具有CCRC信息安全服务资质认证证书（风险评估），计2分。2、投标人具有CCRC信息安全服务资质认证证书（网络安全审计三级及以上），计2分。3、投标人具备信息技术服务管理体系认证ISO/IEC20000，计2分。4、投标人具有质量管理体系认证ISO9001，计2分。5、投标人具有信息安全管理体系统认证证书ISO/IEC27001，计2分。	10.0000	客观	投标方案说明-采购包1
	业绩	提供投标人2021年7月1日至今同类项目业绩合同，每份计2分，满分10分。	10.0000	客观	投标方案说明-采购包1
价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价 / 投标报价)×价格权值×100 计算分数时四舍五入取小数点后两位	10.0000	客观	开标一览表 标的清单 报价表、分项报价表

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.0000 %	<p>（1）根据《关于进一步加大政府采购支持中小企业力度的通知》财库〔2022〕19号的相关规定，对小型和微型企业的价格给予10%的扣除，用扣除后的价格参与评审。</p> <p>（2）根据《财政部民政部中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，对符合条件的残疾人福利性单位产品的价格给予10%的扣除，用扣除后的价格参与评审。小型、微型企业和监狱企业级符合财政部、民政部、中国残疾人联合会关于促进残疾人就业政府采购政策的通知，以上政策同时具备的仅对其进行一次10%的价格扣除，不重复扣除。</p>	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 报价表、分项报价表 监狱企业的证明文件
---	-----------------------	--------------------	-----------	---	--

采购包2:

评审因素		评审标准			
分值构成		详细评审90.0000分 报价得分10.0000分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式

	测评服务方案	投标人根据国家相关标准并结合本项目实际需求，提供完整的等级保护测评服务方案，内容包括定级备案、系统调研、初测评、差距测评、复测评等内容，并对测评各个工作阶段的工作内容、工作方法及工作成果具有详细说明。1、方案内容全面、细致详细、合理可行，完全满足项目需求，计20分；2、方案内容较为全面、切合实际，基本满足项目需求，计15分；3、方案内容基本全面、可行性一般，计10分；4、方案内容欠缺，可行性差，计5分；5、理解有偏差，无法满足本项目需求，计1分；6、未提供的计0分。	20.0000	主观	投标方案说明-采购包2
	风险防范和保密措施	针对本项目的服务提供明确的过程风险防范措施和保密措施，并明确保密责任与赔偿承诺。1、措施内容详尽，切合实际，完全满足项目需求，计10分；2、措施内容较为全面、切合实际、基本满足项目需求，计7分；3、措施内容基本全面、可行性一般，计3分；4、措施内容简单，不切合实际，计1分；5、未提供的计0分。	10.0000	主观	投标方案说明-采购包2
	质量管控	针对本项目具有严格的项目质量管控措施、过程控制及监控手段，能保证技术人员按照相应的操作指导规范实施测评。1、措施详细具体、合理可行，完全满足项目需求，计10分；2、措施较为全面详细，切合实际，基本满足项目需求，计7分；3、措施基本全面合理，可行性一般，计3分；4、措施内容欠缺，可行性差，计1分；5、未提供的计0分。	10.0000	主观	投标方案说明-采购包2

详细评审	工作安排	针对项目组成员工作分配、项目实施进度等具有科学合理的安排措施，确保成员工作分配科学，进度安排科学紧凑。1、措施科学具体、合理可行，完全满足项目需求，计5分；2、措施较为详细，切合实际，基本满足项目需求，计3分；3、措施内容欠缺，进度安排可行性差，计1分；4、未提供的计0分。	5.0000	主观	投标方案说明-采购包2
	测评团队	投标人针对本项目拟派往现场的测评团队成员不少于6人，工作经验不少于1年，否则本项不计分。1、团队成员中至少6人为中级或以上测评师，其中高级测评师不少于4人，计5分；2、团队成员中5人为中级或以上测评师，其中高级测评师不少于3人，计3分；3、团队成员中4人为中级或以上测评师，其中高级测评师不少于2人，计2分；4、其余情况不计分。注：以相关证书、相关人员在本站的任职证明及全国网络安全等级保护网查询结果为准。	5.0000	客观	投标方案说明-采购包2
	项目经理	针对本项目的项目经理在高级测评师基础上具备以下证书（无高级测评师证书本项不计分）：1、信息安全工程师证书；2、注册信息安全专业人员证书（CISP）；3、信息安全保障人员-CISAW证书（风险管理）；4、网络安全服务能力评价证书；5、国家重要信息系统保护人员（CIIP-I）证书 每具备一个计1分，此项满分5分。注：以证书复印件及相关人员在本站的任职证明为准。	5.0000	客观	投标方案说明-采购包2

团队证书	拟派本项目团队（除项目经理）在具备中级及以上测评师证书基础上具备以下证书（无中级或以上测评师证书本项不计分）： <b>1</b> 、高级系统规划与管理师证书 <b>2</b> 、中级网络工程师证书 <b>3</b> 、注册网络安全渗透评估专业人员证书（NSATP-A）； <b>4</b> 、渗透测试工程师（高级）证书或注册渗透测试工程师CISP-PTE证书； <b>5</b> 、注册密码安全专业人员(NSATP-CSP)证书 每具备一个计 <b>1</b> 分，此项满分 <b>5</b> 分。注：以证书复印件及相关人员在本单位的任职证明为准。	5.0000	客观	投标方案说明-采购包2
售后服务	为保障测评项目结束后的信息安全，要求投标人提供完善的售后服务，包括应急响应服务、电话支持服务、配合检查服务、重保驻场服务、网络安全培训服务、应急演练服务等内容，能提供以上售后服务并做出相应服务说明。 <b>1</b> 、方案内容全面、细致详细、合理可行，完全满足项目需求，计 <b>5</b> 分； <b>2</b> 、方案内容基本全面、可行性一般，计 <b>3</b> 分； <b>3</b> 、方案内容欠缺，可行性差，计 <b>1</b> 分； <b>4</b> 、未提供的计 <b>0</b> 分。	5.0000	主观	投标方案说明-采购包2
培训方案	投标人针对本项目提供详尽的培训方案及培训计划，包括培训对象、培训方式、培训人数、培训时间等安排。 <b>1</b> 、方案内容完善，合理可行，针对性强，计 <b>5</b> 分； <b>2</b> 、方案内容基本完整、合理性、可行性、针对性一般，计 <b>3</b> 分； <b>3</b> 、方案内容欠缺，可行性差，计 <b>1</b> 分； <b>4</b> 、未提供的计 <b>0</b> 分	5.0000	主观	投标方案说明-采购包2

	企业实力	1、投标人具有中国网络安全审查技术与认证中心（CCRC）颁发的信息安全风险评估资质证书，一级资质计3分，二级资质计1分，其他情况不计分。2、投标人具有中国网络安全审查技术与认证中心（CCRC）颁发的信息安全应急处理资质证书，一级资质计3分，二级资质计1分，其他情况不计分。3、投标人具有中国网络安全审查技术与认证中心（CCRC）颁发的信息系统安全运维服务资质证书，一级资质计3分，二级资质计1分，其它情况不得分。4、投标人具备信息安全管理体系认证证书-ISO27001计1分，其它情况不得分。	10.0000	客观	投标方案说明-采购包2
	业绩	提供投标人2021年7月1日至今同类项目业绩合同，每份计2分，满分10分。	10.0000	客观	投标方案说明-采购包2
价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价 / 投标报价)×价格权值×100 计算分数时四舍五入取小数点后两位	10.0000	客观	开标一览表 标的清单 报价表、分项报价表

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------



1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.0000 %	<p>（1）根据《关于进一步加大政府采购支持中小企业力度的通知》财库〔2022〕19号的相关规定，对小型和微型企业的价格给予10%的扣除，用扣除后的价格参与评审。</p> <p>（2）根据《财政部民政部中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，对符合条件的残疾人福利性单位产品的价格给予10%的扣除，用扣除后的价格参与评审。小型、微型企业和监狱企业级符合财政部、民政部、中国残疾人联合会关于促进残疾人就业政府采购政策的通知，以上政策同时具备的仅对其进行一次10%的价格扣除，不重复扣除。</p>	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 报价表、分项报价表 监狱企业的证明文件
---	-----------------------	--------------------	-----------	---	--

采购包3:

评审因素		评审标准			
分值构成		详细评审90.0000分 报价得分10.0000分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式

	项目理解	根据投标人对项目的理解进行打分，包括但不限于项目需求、测评对象、测评标准、测评范围及内容、密码需求分析、密码应用安全、密钥安全、安全管理制度等内容。1、项目理解充分，内容合理，描述全面、准确、细致，计10分；2、项目理解较充分，内容较合理，描述较全面准确，计7分；3、项目理解基本充分，内容基本合理，描述基本全面准确，计3分；4、项目理解不充分，描述不全面，不够准确，计1分；5、未提供的计0分。	10.0000	主观	投标方案说明-采购包3
	测评工作方案	根据测评工作方案专业性、科学性 & 合理性进行打分，内容包括但不限于测评流程、测评方法、实施计划、项目组织、项目交付、培训方案等。1、方案内容完整，架构清晰完整，可操作性、可实现性强，计15分；2、方案内容较完整，架构较清晰完整，可操作及可实现性较强，计10分；3、方案内容基本完整，架构基本清晰，可操作性、可实现性一般，计5分；4、方案内容简单，架构不够清晰，可操作性、可实现性较差，计1分；5、未提供的计0分。	15.0000	主观	投标方案说明-采购包3
	质量管控	方案需详细说明本测试项目的质量管控措施、过程控制及监控手段等内容，能保证技术人员按照相应的操作指导规范实施测评。1、措施详细具体、合理可行，完全满足项目需求，计8分；2、措施较为全面详细，切合实际，较能满足项目需求，计6分；3、措施基本全面合理，可行性一般，计3分；4、措施内容欠缺，可行性差，计1分；5、未提供的计0分。	8.0000	主观	投标方案说明-采购包3

详细评审

进度安排	<p>供应商针对本项目提供进度安排，包括但不限于明确合理的项目实施周期和进度计划表、相应的进度保障措施等。 1、进度计划安排合理，可行性强，计6分； 2、进度计划合理性、可行性一般，计3分； 3、进度计划合理性、可行性较差，计1分； 4、未提供计0分。</p>	6.0000	主观	投标方案说明-采购包3
风险防范措施	<p>根据供应商提供的项目实施过程中的风险防范措施，并明确保密责任与赔偿承诺。 1、措施合理、可行、完善，针对性强，计6分； 2、措施基本合理、可行、完善，针对性一般，计3分； 3、措施合理性、可行性及针对性不足，计1分； 4、未提供计0分。</p>	6.0000	主观	投标方案说明-采购包3
团队技术能力	<p>1、项目技术负责人具备商用密码应用安全性评估人员（计2分）、注册密码技术专家（CISP-CTE）（计2分）、高级网络安全等级保护测评师证书（计2分）、信息安全保障人员（CISAW）风险管理方向认证证书（计2分），共8分； 2、项目技术团队人员具有信息系统项目管理师（高级）证书的，每有一份计2分，最高8分。注：以证书复印件及相关人员在本单位的任职证明为准。</p>	16.0000	客观	投标方案说明-采购包3

	售后服务方案	为保障测评项目结束后的信息安全，要求投标人提供完善的售后服务，包括应急响应服务、电话支持服务、配合检查服务、安全咨询服务、安全培训服务等内容，能提供以上售后服务并做出相应服务说明。 1、方案内容全面、细致详细、合理可行，完全满足项目需求，计9分； 2、方案内容基本全面、合理性、可行性一般，基本满足项目需求，计6分； 3、方案内容欠缺，可行性差，计3分； 4、未提供的计0分。	9.0000	主观	投标方案说明-采购包3
	企业实力	1、投标人具有质量管理体系认证ISO9001，计2分。 2、投标人具有信息安全管理体系统证书ISO/IEC27001，计2分。 3、投标人具备信息技术服务管理体系认证ISO/IEC20000，计2分。 4、投标人具有市场监督管理部门颁发的检验检测机构资质认定证书（CMA），计2分。 5、投标人具有有效的中国合格评定国家认可委员会实验室认可（CNAS）证书,计2分。	10.0000	客观	投标方案说明-采购包3
	业绩	提供投标人2021年7月1日至今同类项目业绩合同，每份计2分，满分10分。	10.0000	客观	投标方案说明-采购包3
价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： 投标报价得分=(评标基准价 / 投标报价)×价格权值×100 计算分数时四舍五入取小数点后两位	10.0000	客观	开标一览表 标的清单 报价表、分项报价表

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.0000 %	<p>（1）根据《关于进一步加大政府采购支持中小企业力度的通知》财库〔2022〕19号的相关规定，对小型和微型企业的价格给予10%的扣除，用扣除后的价格参与评审。</p> <p>（2）根据《财政部民政部中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，对符合条件的残疾人福利性单位产品的价格给予10%的扣除，用扣除后的价格参与评审。小型、微型企业和监狱企业级符合财政部、民政部、中国残疾人联合会关于促进残疾人就业政府采购政策的通知，以上政策同时具备的仅对其进行一次10%的价格扣除，不重复扣除。</p>	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 报价表、分项报价表 监狱企业的证明文件
---	-----------------------	--------------------	-----------	---	--

说明：

- 1、评分的取值按四舍五入法，保留小数点后两位；
- 2、评分标准中要求提供的证明材料须清晰可辨。

（最低评标价法适用）采用最低评标价法的，投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人。采用最低评标价法评标时，除了算术修正和落实政府采购政策需进行的价格扣除外，不能对投标人的投标价格进行任何调整。

## 5.7废标

本次政府采购活动中，出现下列情形之一的，予以废标：

- 一、符合专业条件的投标人或者对招标文件作实质响应的投标人不足三家的；
- 二、出现影响采购公正的违法、违规行为的；
- 三、投标人的报价均超过了采购预算，采购人不能支付的；
- 四、因重大变故，采购任务取消的；

废标后，代理机构将在陕西省政府采购网上公告。对于评标过程中废标的采购项目，评标委员会应当对招标文件是否存在倾向性和歧视性、是否存在不合理条款进行论证，并出具书面论证意见。

## **5.8定标**

### **5.8.1 定标原则**

采购人在评标报告确定的中标候选人名单中按顺序确定**1**名中标人。中标候选人并列的，由采购人采取随机抽取的方式确定中标人。

### **5.8.2定标程序**

一、评标委员会在项目电子化交易系统中编制评标情况，生成评标报告。

二、代理机构在评标结束之日起**2**个工作日内将评标报告送采购人。

三、采购人在收到评标报告后**5**个工作日内，按照评标报告中推荐的中标候选人顺序确定中标供应商。逾期未确认的，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标供应商。

四、根据确定的中标供应商，代理机构在陕西省政府采购网上发布中标结果公告，通过项目电子化交易系统向中标供应商发出中标通知书。

## **5.9评审专家在政府采购活动中承担以下义务**

（一）遵守评审工作纪律；

（二）按照客观、公正、审慎的原则，根据采购文件规定的评审程序、评审方法和评审标准进行独立评审；

（三）不得泄露评审文件、评审情况和在评审过程中获悉的商业秘密；

（四）及时向监督管理部门报告评审过程中的违法违规情况，包括采购组织单位向评审专家作出倾向性、误导性的解释或者说明情况，供应商行贿、提供虚假材料或者串通情况，其他非法干预评审情况等；

（五）发现采购文件内容违反国家有关强制性规定或者存在歧义、重大缺陷导致评审工作无法进行时，停止评审并通过项目电子化交易系统向采购组织单位书面说明情况，说明停止评审的情形和具体理由；

（六）配合答复处理供应商的询问、质疑和投诉等事项；

（七）法律、法规和规章规定的其他义务。

## **5.10评审专家在政府采购活动中应当遵守以下工作纪律**

（一）遵行《中华人民共和国政府采购法》第十二条和《中华人民共和国政府采购法实施条例》第九条及财政部关于回避的规定。

（二）评标前，应当将通讯工具或者相关电子设备交由采购组织单位统一保管。

（三）评标过程中，不得与外界联系，因发生不可预见情况，确实需要与外界联系的，应当在监督人员监督之下办理。

（四）评标过程中，不得干预或者影响正常评标工作，不得发表倾向性、引导性意见，不得修改或细化招标文件确定的评标程序、评标方法、评审因素和评审标准，不得接受供应商主动提出的澄清和解释，不得征询采购人代表的意见，不得协商评分，不得违反规定的评审格式评分和撰写评标意见，不得拒绝对自己的评标意见签字确认。

（五）在评审过程中和评审结束后，不得记录、复制或带走任何评审资料，不得向外界透露评审内容。

（六）服从评审现场采购组织单位的现场秩序管理，接受评审现场监督人员的合法监督。

（七）遵守有关廉洁自律规定，不得私下接触供应商，不得收受供应商及有关业务单位和个人的财物或好处，不得接受采购组织单位的请托。

## 第6章投标文件格式

### 6.1 投标文件封面格式

#### 采购包1:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：开标一览表

详见附件：标的清单

详见附件：报价表、分项报价表

详见附件：服务内容及服务要求应答表

详见附件：商务条款响应说明

详见附件：投标人资格条件证明文件-采购包1

详见附件：投标方案说明-采购包1

详见附件：投标人承诺书

详见附件：保证金交纳凭证

#### 采购包2:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：开标一览表

详见附件：标的清单

详见附件：报价表、分项报价表

详见附件：服务内容及服务要求应答表

详见附件：商务条款响应说明

详见附件：投标人资格条件证明文件-采购包2

详见附件：投标方案说明-采购包2

详见附件：投标人承诺书

详见附件：保证金交纳凭证

#### 采购包3:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：开标一览表

详见附件：标的清单

详见附件：报价表、分项报价表

详见附件：服务内容及服务要求应答表

详见附件：商务条款响应说明

详见附件：投标人资格条件证明文件-采购包3

详见附件：投标方案说明-采购包3

详见附件：投标人承诺书

详见附件：保证金交纳凭证



## 第7章 拟签订采购合同文本

详见附件：合同范本.docx

