

磋商文件

(服务类)

采购项目名称：碑林区政务服务中心网络安全升级项目

采购项目编号：**ZY2024-ZB-CS1110**

西安市碑林区行政审批局

陕西正翼项目管理咨询有限公司共同编制

2024年09月05日

第一章 竞争性磋商邀请

陕西正翼项目管理咨询有限公司（以下简称“代理机构”）受西安市碑林区行政审批局委托，拟对碑林区政务服务中心网络安全升级项目采用竞争性磋商采购方式进行采购，兹邀请供应商参加本项目的竞争性磋商。

一、项目编号：ZY2024-ZB-CS1110

二、项目名称：碑林区政务服务中心网络安全升级项目

三、磋商项目简介

碑林区政务服务中心网络安全升级项目

四、邀请供应商

本次采购采取公告征集邀请磋商的供应商。

公告征集：本次竞争性磋商在“陕西省政府采购网（www.ccgp-shaanxi.gov.cn）”上以公告形式发布，兹邀请符合本次采购要求的供应商参加本项目的竞争性磋商。

五、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：

执行政府采购促进中小企业发展的相关政策：

采购包1（碑林区政务服务中心网络安全升级项目）：属于专门面向中小企业采购。

（三）本项目的特定资格要求：

采购包1：

1、营业执照等主体资格证明文件：提供有效合格的具有统一社会信用代码的营业执照，其他组织经营的须提供合法凭证，自然人提供身份证明文件

2、财务状况报告：提供2023年度经审计的完整财务报告或磋商日期前三个月内其基本存款账户开户银行出具的资信证明。（如提供资信证明，须同时提供基本存款账户开户许可证或基本账户信息表）

3、税收缴纳证明：提供2024年1月至今已缴纳的至少一个月的纳税证明，依法免税的单位应提供相关证明材料

4、社会保障资金缴纳证明：提供2024年1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：具备履行合同所必须的设备和专业技术能力的书面声明

6、无重大违法记录：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

7、信用记录：供应商未被列入信用中国网站(www.creditchina.gov.cn)“失信被执行人、重大税收违法失信主体”；不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间

8、授权委托书：法定代表人授权委托书、被授权人身份证（法定代表人参加磋商时,只需提供法定代表人身份证）,非法人单位参照执行

六、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

七、竞争性磋商文件获取时间、方式及地址

(一) 磋商文件获取时间：详见采购公告或邀请书。

(二) 在磋商文件获取开始时间前，采购人或代理机构将本项目磋商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磋商文件。成功获取磋商文件的，供应商将收到已获取磋商文件的回执函。未成功获取磋商文件的供应商，不得参与本次采购活动，不得对磋商文件提起质疑。

成功获取磋商文件后，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响应文件编制的，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磋商文件，供应商应当重新获取磋商文件；澄清或者修改后的磋商文件发布日期距提交响应文件截止日期不足5日的，采购人或代理机构顺延提交响应文件的截止时间。供应商未重新获取磋商文件或者未按照澄清或者修改后的磋商文件编制响应文件进行响应的，自行承担不利后果。

注：获取的磋商文件主体格式包括pdf、word两种格式版本，其中以pdf格式为准。

八、首次响应文件提交截止时间及开启时间、地点、方式

(一) 提交首次响应文件截止时间及开启时间：详见采购公告或邀请书。

(二) 响应文件提交方式、地点：供应商应当在提交首次响应文件截止时间前，通过项目电子化交易系统提交响应文件。成功提交的，供应商将收到已提交响应文件的回执函。

九、磋商方式

本项目磋商小组与供应商通过项目电子化交易系统以在线方式进行磋商。磋商会议由磋商小组在线主持，供应商代表在线参加。供应商应随时关注项目电子化交易系统信息，及时参与在线磋商。供应商登录项目电子化交易系统，与磋商小组进行在线磋商、提交供应商响应表，供应商响应表应加盖供应商（法定名称）电子印章。

十、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，凭项目成交结果、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。

十一、联系方式

采购人：西安市碑林区行政审批局

地址：碑林区东大街8号

邮编：710000

联系人：彭老师

联系电话：029-89625901

代理机构：陕西正翼项目管理咨询有限公司

地址：陕西省西安市未央区西安经济技术开发区凤城一路6号利君V时代B座901、912室

邮编：710000

联系人：徐超、张晶

联系电话：029-86210100转803

采购监督机构：西安市碑林区政府采购管理股

联系人：郝天峰

联系电话：029-89625302

第二章 供应商须知

2.1 供应商须知前附表

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1：540,000.00元</p> <p>供应商采购包报价高于采购包采购预算的，其响应文件将按无效处理。</p>
2	最高限价（实质性要求）	<p>详见第三章。</p> <p>供应商的采购包响应报价高于最高限价的，其响应文件将按无效处理。</p>
3	评审方法	综合评分法(详见第六章)。
4	是否接受联合体	<p>采购包1：不接受</p> <p>如以联合体响应的，联合体各方均应当具备本磋商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磋商项目必备的条件，如相应的人力、物力、资金等。</p> <p>（2）磋商文件对供应商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较甲级更低的乙级，则该联合体资质等级为乙级。</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.本项目采购的/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，否则作无效响应处理。</p> <p>3.本项目采购的/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，本项目采购的/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）	<p>（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）根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）第九条和《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）的规定。</p> <p>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六章。</p> <p>（其他情形）不适用。</p>

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>提供相同品牌产品且通过资格审查、符合性审查的不同供应商参加同一合同项下采购活动的，按一家供应商计算，评审后得分最高的同品牌供应商获得成交供应商推荐资格；最后评审得分相同的，由采购人或者采购人委托磋商小组采取随机抽取方式确定一个供应商获得成交供应商推荐资格，其他同品牌供应商不作为成交候选人。</p> <p>核心产品清单详见第三章。</p> <p>在符合性审查、有效报价环节提供核心产品品牌不足3个的，视为有效响应供应商不足3家。</p>
8	不正当竞争预防措施（实质性要求）	<p>在磋商过程中，磋商小组认为供应商报价明显低于其他通过符合性审查供应商的报价，有可能影响产品质量或者不能诚信履约的，磋商小组应当要求其在合理的时间内通过项目电子化交易系统书面说明，必要时提交相关证明材料。供应商提交的书面说明和相关证明材料，应当加盖供应商公章，在磋商小组要求的时间内通过项目电子化交易系统进行提交，否则提交的相关材料无效，视为不能证明其响应报价合理性。供应商不能证明其响应报价合理性的，磋商小组应当将其响应文件作为无效处理。</p>
9	磋商保证金	缴交方式：否
10	标书费信息	免费获取
11	履约保证金（实质性要求）	采购包1：不缴纳
12	响应有效期（实质性要求）	提交首次响应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：以成交价格为基数，依据国家计委颁布《招标代理服务收费管理暂行办法》（计价格[2002]1980号）和国家发展改革委员会办公厅颁发的《关于招标代理服务收费有关问题的通知》（发改办价格[2003]857号）文件规定执行，定额收取人民币捌仟元整； 招标代理服务费缴纳信息： 名称：陕西正翼项目管理咨询有限公司 税号：91610132MA6U430T24 地址：西安经济技术开发区凤城一路6号利君V时代B座9楼901、912室029-86210100 开户行：中国民生银行股份有限公司西安经济技术开发区支行 账号：152605604</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	成交通知书	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成交供应商发出成交通知书；成交供应商通过项目电子化交易系统获取成交通知书。
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，采购人将本项目采购合同通过政府采购平台进行备案。</p>
17	进口产品	不允许
18	是否组织潜在供应商现场考察	采购包1：组织现场踏勘：否

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终止采购活动。</p>
----	------	--

2.2总则

2.2.1适用范围

一、本磋商文件仅适用于本次竞争性磋商采购项目。

二、本磋商文件的最终解释权由西安市碑林区行政审批局和陕西正翼项目管理咨询有限公司享有。对磋商文件中供应商参加本次政府采购活动应当具备的条件，磋商项目技术、服务、商务及其他要求，评审细则及标准由西安市碑林区行政审批局负责解释。除上述磋商文件内容，其他内容由陕西正翼项目管理咨询有限公司负责解释。

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。本次磋商的采购人是西安市碑林区行政审批局。

二、“供应商”是指在按照磋商公告规定获取磋商文件，拟参加响应和向采购人提供货物、工程或服务的法人、其他组织或自然人。

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正翼项目管理咨询有限公司。

四、“网上开启”是指供应商通过项目电子化交易系统在线完成签到、响应文件解密后，采购人或者采购代理机构通过项目电子化交易系统在线完成已解密响应文件的开启工作。

五、“电子评审”是指通过项目电子化交易系统在线完成资格审查小组、磋商小组组建，开展资格和符合性审查、比较与评价、出具磋商报告、推荐成交候选供应商等活动。

2.2.3响应费用（实质性要求）

供应商应自行承担参加竞争性磋商采购活动的全部费用。

2.3磋商文件

2.3.1磋商文件的构成

一、磋商文件是供应商准备响应文件和参加响应的依据，同时也是评审的重要依据。磋商文件用以阐明磋商项目所需的资质、技术、服务及报价等要求、磋商程序、有关规定和注意事项以及合同草案条款等。本磋商文件包括以下内容：

- （一）竞争性磋商邀请；
- （二）供应商须知；
- （三）磋商项目技术、服务、商务及其他要求；
- （四）资格审查；
- （五）磋商过程中可实质性变动的内容；
- （六）磋商办法；
- （七）响应文件格式；
- （八）拟签订采购合同文本。

二、供应商应认真阅读和充分理解磋商文件中所有的事项、格式条款和规范要求。供应商没有对磋商文件全面作出实质性

响应所产生的风险由供应商承担。

2.3.2磋商文件的澄清和修改

一、在提交首次响应文件截止时间前，采购人或者代理机构可以对已发出的磋商文件进行必要的澄清或者修改。

二、澄清或者修改的内容为磋商文件的组成部分，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，供应商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。更正内容可能影响响应文件编制的，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磋商文件，供应商应依据更正后的磋商文件编制响应文件。若供应商未按前述要求进行响应的，自行承担不利后果。

2.4响应文件

2.4.1响应文件的语言

一、供应商提交的响应文件以及供应商与磋商小组在磋商过程中的所有来往书面文件均须使用中文。响应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，磋商小组将其视为无效材料。

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供应商的不利后果，由供应商承担。

2.4.2计量单位

除磋商文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3响应货币

本次项目均以人民币报价。

2.4.4知识产权

一、供应商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，如存在前述情形，由供应商承担所有相关责任。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、供应商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，供应商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、如采用供应商所不拥有的知识产权，则在报价中必须包括合法使用该知识产权的相关费用。

四、构成本磋商文件的各组成部分，未经采购人书面同意，供应商不得擅自复印或用于非本磋商项目所需的其他目的。

2.4.5响应文件的组成（实质性要求）

供应商应按照磋商文件的规定和要求编制响应文件。

响应文件具体内容详见第七章。

2.4.6响应文件格式

一、供应商应按照磋商文件第七章中提供的“响应文件格式”填写相关内容。

二、对于没有格式要求的响应文件由供应商自行编写。

2.4.7响应报价（实质性要求）

一、供应商的报价是供应商响应磋商项目要求的全部工作内容的价格体现，包括供应商完成本项目所需的一切费用。

二、响应文件报价出现前后不一致的，按照磋商文件第六章磋商办法规定予以修正，修正后的报价经供应商通过项目电子化交易系统进行确认，并加盖供应商（法定名称）电子印章，供应商逾时确认的，其响应无效。

2.4.8响应有效期（实质性要求）

响应有效期详见第二章“供应商须知前附表”，响应文件未明确响应有效期或者响应有效期小于“供应商须知前附表”中响应有效期要求的，其响应文件按无效处理。

2.4.9响应文件的制作、签章和加密

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、供应商应按照客户端操作要求，对应磋商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磋商文件对应项的要求的，其响应文件作无效处理。

三、供应商完成响应文件编制后，应按照响应文件第1章明确的签章要求，使用互认的证书及签章对响应文件进行电子签章和加密。

四、磋商文件澄清或者修改的内容可能影响响应文件编制的，代理机构将重新发布澄清或者修改后的磋商文件，供应商应重新获取澄清或者修改后的磋商文件，按照澄清或者修改后的磋商文件进行响应文件编制、签章和加密。

2.4.10 响应文件的提交（实质性要求）

一、供应商应当在提交首次响应文件截止时间前，通过项目电子化交易系统完成响应文件提交。

二、在提交首次响应文件截止时间后，代理机构不再接受供应商提交响应文件。供应商应充分考虑影响响应文件提交的各种因素，确保在提交首次响应文件截止时间前完成提交。

2.4.11 响应文件的补充、修改（实质性要求）

响应文件提交截止时间前，供应商可以补充、修改或者撤回已成功提交的响应文件；对响应文件进行补充、修改的，应当先行撤回已提交的响应文件，补充、修改后重新提交。

供应商响应文件撤回后，视为未提交过响应文件。

2.5 开启、资格审查、磋商和确定成交供应商

2.5.1 磋商开启程序

一、本项目为竞争性磋商项目。网上开启的开始时间为响应文件提交截止时间。成功提交或解密电子响应文件的供应商不足3家的，不予开启，采购人或代理机构将终止采购活动。

二、磋商开启准备工作

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。

三、解密响应文件（实质性要求）

响应文件提交截止时间后，成功提交响应文件的供应商符合响应文件规定数量的，代理机构将启动响应文件解密程序，解密时间为30分钟；供应商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响应文件解密。供应商未在规定的解密时间内完成解密的，按无效响应处理。

开启过程中，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。供应商对开启过程和开启记录有疑义，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供应商提出的询问或者回避申请应当及时处理。

2.5.2 查询及使用信用记录

开启结束后，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）、“中国政府采购网”网站（www.ccgp.gov.cn）等渠道，查询供应商在响应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，以一个供应商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

详见磋商文件第四章。

2.5.4 磋商

详见磋商文件第六章。

2.5.5成交通知书

一、采购人或者磋商小组确认成交供应商后，代理机构在陕西省政府采购网发布成交结果公告、通过项目电子化交易系统发出成交通知书，成交供应商通过项目电子化交易系统获取成交通知书。

二、成交通知书是采购人和成交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、规章制度规定的成交无效情形的，将以公告形式宣布发出的成交通知书无效，成交通知书将自动失效，并依法重新确定成交供应商或者重新开展采购活动。

三、成交通知书对采购人和成交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、采购人应在成交通知书发出之日起三十日内与成交供应商签订采购合同。

二、采购人和成交供应商签订的采购合同不得对磋商文件确定的事项以及成交供应商的响应文件作实质性修改。

2.6.2合同分包和转包（实质性要求）

2.6.2.1合同分包

一、供应商根据磋商文件的规定和采购项目的实际情况，拟在成交后将成交项目的非主体、非关键性工作分包的，应当在响应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。分包供应商履行的分包项目的品牌、规格型号及技术要求等，必须与成交的一致。

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，不属于成交供应商的主要合同义务。

三、采购合同实行分包履行的，成交供应商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。履行分包项目事项应当具备法定资质规定要求的，分包供应商应当具备相应资质。

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。

2.6.2.2合同转包

一、严禁成交供应商将本采购项目采购合同转包。本项目所称转包，是指成交供应商签订政府采购合同后，不履行合同约定的责任和义务，将其全部工程转给他人或者将其全部工程肢解以后以分包的名义分别转给其他单位承包的行为。

二、成交供应商转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3合同公告

采购人应当自政府采购合同签订（双方当事人均已完成盖章）之日起2个工作日内，在陕西省政府采购网公告本项目采购合同，但合同中涉及国家秘密、商业秘密的内容除外。

2.6.4合同备案

采购人自政府采购合同签订（双方当事人均已完成盖章）之日起7个工作日内，将本项目采购合同通过报同级财政部门备案。

2.6.5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、工程或者服务的，在不改变合同其他条款的前提下，可以与成交供应商协商签订补充合同，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。

2.6.6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。

2.6.7履约验收方案

采购包1：

(1) 磋商文件、磋商响应文件、澄清表(函); (2) 本合同及附件文本; (3) 合同签订时国家及行业现行的标准和技术规范

2.6.8 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 磋商活动纪律要求

采购人、代理机构应保证磋商活动在严格保密的情况下进行, 采购人、代理机构、供应商和磋商小组成员应当严格遵守政府采购法律法规规章制度和本项目磋商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磋商过程和结果。

对各供应商的商业秘密, 磋商小组成员应予以保密, 不得泄露给其他供应商。

2.7.2 供应商不得具有的情形(实质性要求)

供应商参加响应不得有下列情形:

一、有下列情形之一的, 视为供应商串通响应:

- (一) 不同供应商的响应文件由同一单位或者个人编制;
- (二) 不同供应商委托同一单位或者个人办理磋商事宜;
- (三) 不同供应商的响应文件载明的项目管理成员或者联系人员为同一人;
- (四) 不同供应商的响应文件异常一致或者响应报价呈规律性差异;
- (五) 不同供应商的响应文件相互混装。

二、提供虚假材料谋取成交;

三、采取不正当手段诋毁、排挤其他供应商;

四、与采购人或代理机构、其他供应商恶意串通;

五、向采购人或代理机构、磋商小组成员行贿或者提供其他不正当利益;

六、在磋商过程中与采购人或代理机构进行协商磋商;

七、成交后无正当理由拒不与采购人签订政府采购合同;

八、未按照磋商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。

供应商有上述情形的, 按照规定追究法律责任, 具有前述一至十一条情形之一的, 其响应文件无效, 或取消被确认为成交供应商的资格或认定成交无效。

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供应商有下列利害关系之一的, 应当回避:

- (一) 参加采购活动前3年内与供应商存在劳动关系;
- (二) 参加采购活动前3年内担任供应商的董事、监事;
- (三) 参加采购活动前3年内是供应商的控股股东或者实际控制人;
- (四) 与供应商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;
- (五) 与供应商有其他可能影响政府采购活动公平、公正进行的关系。

供应商认为采购人员及相关人员与其他供应商有利害关系的, 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，供应商对采购文件中采购需求的询问、质疑由陕西正翼项目管理咨询有限公司负责答复；供应商对除采购需求外的采购文件的询问、质疑由陕西正翼项目管理咨询有限公司负责答复；供应商对采购过程、采购结果的询问、质疑由陕西正翼项目管理咨询有限公司负责答复。

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、不影响响应文件的编制的情形）。

四、供应商认为磋商文件、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（针对磋商文件提出的质疑，需提交从项目电子化交易系统获取的磋商文件回执单）。

接收质疑函方式：书面形式。

答复主体：代理机构

联系人：徐超、张晶

联系电话：029-86210100转803

地址：陕西省西安市未央区西安经济技术开发区凤城一路6号利君V时代B座901、912室

邮编：710000

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磋商文件、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时间内作出答复的，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 磋商项目技术、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

碑林区政务服务中心网络安全升级项目

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）：540,000.00

采购包最高限价（元）：540,000.00

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	碑林区政务服务中心网络安全升级	1.00	540,000.00	批	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：碑林区政务服务中心网络安全升级

参数性质	序号	技术参数与性能指标				
		<p>一、网络安全设备</p> <p>（一）防火墙设备2台，进行深度防御，以抵御恶意攻击和非法访问，保护我局内外网络的安全；WEB应用防火墙1台，识别各类高危Web攻击，保护正常Web访问；入侵检测与防御设备1台，实时监测网络流量，并对异常流量进行自动识别与告警，确保关键系统和数据的安全；上网行为管理设备1台，帮助网络管理员合理利用网络带宽、保障数据安全、提升工作效率和避免法律风险；终端安全管理1套，预防病毒和恶意代码的传播；日志审计设备1套，实现对信息系统日志的全面审计。</p> <p>（二）完成设备安装、调试、整改和平滑上线，配置防火墙策略、端口策略、行为管理策略、终端安全策略等工作，达到等保测评要求。</p> <p>（三）采购设备需满足国产化要求，质保期为项目终验之日起不少于三年，投标供应商提供设备售后服务承诺函，承诺投标产品提供不少于三年硬件保修服务，不少于三年软件升级服务(含特征库)。</p> <p>1、防火墙系统 数量：2台</p> <table border="1" style="width: 100%; margin-top: 10px;"> <thead> <tr> <th style="width: 20%;">指标项</th> <th>指标要求</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"></td> <td></td> </tr> </tbody> </table>	指标项	指标要求		
指标项	指标要求					

※硬件规格	国产化CPU: ≥2.6GHz, 4核; 操作系统: 国产系统; 内存≥8G; 硬盘≥1T; 接口类型和数量: 网络接口包括1个管理口、1个HA口、≥12*GE电口(支持对电口Bypass)和≥12*SFP光口(默认SFP接口不带光模块); 双交流电源; MTBF(小时)≥200,000; ≥1U机箱
性能要求	防火墙吞吐量: ▲整机网络层吞吐量(双向): ≥10G 整机应用层吞吐量(单向)≥3G
	TCP新建连接速率: IPv4: ≥5万/秒、IPv6: ≥5万/秒
	TCP并发连接数: IPv4: ≥500万、IPv6: ≥500万
安全业务	▲支持安全运营中心概览, 自动进行网络风险评估、监测分析和风险建议(提供证明材料并加盖公章)
	▲支持勒索专项防护, 展示勒索风险业务、攻击暴露面管理、弱口令检查(提供证明材料并加盖公章)
	支持业务安全概览, 展示业务风险、漏洞风险、全网热点事件展示
	支持用户安全概览, 展示不同风险级别和失陷风险用户、支持攻击趋势分布展示
	支持攻击者IP一键封锁和自定义封锁时间
安全能力	▲内置漏洞攻击特征库、应用特征库、URL特征库、病毒特征库、WEB应用防护库、数据泄密防护库、僵尸网络识别库、IP信誉库、热点时间预警与处置库、威胁情报等, 可在线/离线升级(提供证明材料并加盖公章)
	▲支持漏洞攻击防护、web应用防护、僵尸网络防护、内容安全防护、应用控制预置策略模版(提供证明材料并加盖公章)
	▲支持业务模型AI学习功能, 展示业务特征(提供证明材料并加盖公章)
访问控制	支持一体化安全策略配置, 可以通过一条策略实现五元组、源MAC、源区域、目的区域、域名、应用、服务、时间、长连接时间、最大活动会话数、策略优化场景、黑链检测、webshell检测、漏洞风险分析、配置风险分析、弱口令账户检测、漏洞攻击防护(上网管控场景、业务保护场景)、内容安全(文件过滤、邮件过滤、URL过滤、病毒检、弱口令检测)、WEB应用防护、网页防篡改、僵尸网络防护、APT高级威胁防护、流量控制防护、联动封锁、并发会话、WEB认证、审计日志开启等功能配置, 简化用户管理;(提供证明材料并加盖公章)
	▲支持策略标签化(提供证明材料并加盖公章)
	▲支持策略生命周期管理, 展示变更时间、变更原因、变更账号等信息(提供证明材料并加盖公章)
	支持失效策略检查
	支持模拟策略匹配
	▲支持策略优化自动分析及展示, 显示一般、严重等不同级别的问题策略(提供证明材料并加盖公章)
连接数控制	▲支持源、目的区域/对象的并发和新建数(提供证明材料并加盖公章)
端口镜像	支持将任意接口的数据完全镜像到设备自身的其他接口, 用于抓包分析
PPPOE接入	支持PPPOE接入, 最多支持4路ADSL接入
NAT功能	支持基于接口地址、地址池、VLAN接口、目标接口、目标地址的NAT、反向NAT及双向NAT
	可实现跨NAT的H.323通讯

网络应用	支持802.1Q VLAN, PPPOE, DHCP Client, DHCP Server、IPX等协议
身份认证	▲支持本地认证, 支持本地认证、Radius认证、Tacacs认证、AD域认证、POP认证、LDAP认证等, 同时支持短信认证、硬件特征码认证
	▲支持操作系统版本、文件、进程、注册表、登录IP、登录时间等终端认证安全检查方式 (提供证明材料并加盖公章)
	支持WEB登录前、登录后安全检查, 支持SSL VPN登录前、登录后安全检查 (提供证明材料并加盖公章)
DDoS攻击 防御	支持外网对内攻击防护功能, 支持防御ARP洪水攻击、SYN Flood、UDP Flood、DNS Flood、ICMP Flood、ICMPv6 Flood、RST Flood、ACK Flood、HTTP Flood、IP地址扫描、端口扫描防御等攻击 (提供证明材料并加盖公章)
	▲支持内网对外攻击防护功能, 支持防御SYN Flood、UDP Flood、DNS Flood、ICMP Flood、ICMPv6 Flood、RST Flood、ACK Flood、HTTP Flood、IP地址扫描、端口扫描防御等攻击 (提供证明材料并加盖公章)
	支持DoS排除
入侵防御	内置入侵防御规则数≥7600
	支持可疑网络行为、尝试侦查行为、用户尝试攻击、RPC攻击、SHELL Code攻击、协议解析攻击、MISC攻击等攻击防御
病毒防护	支持木马查杀, 比如Trojan.agent, Trojan. Downloader, Trojan.Dropper等
上网行为管理	支持9700+种应用识别, 包括基本服务、HTTP、视频、P2P、流媒体、网络游戏、即时通讯、股票、网上银行、网络电话、网络存储、网页邮箱、软件更新、远程控制、网络货币、网上支付、生活服务、新闻媒体、社交通讯、旅游、贷款等
	▲支持限速、会话限制、阻断、警告等多种应用管控方式 (提供证明材料并加盖公章)
URL管控	支持URL过滤功能, 同时支持用户自定义URL库, 系统内置上万条的URL库
内容防泄漏	▲支持邮件、论坛发帖/回复、外发文件的内容识别 (提供证明材料并加盖公章)
	支持120+文件类型识别
	支持银行卡号、身份证号、手机号等默认防护规则
WEB攻击防护	支持900+WEB防护规则, 支持防御SQL注入、跨站脚本攻击、自动扫描防护、WEB爬虫防护、WEB服务器漏洞攻击、WEB插件漏洞、LDAP注入防护、SSI指令防护、XPath注入防护、命令行注入防护、路径穿越防护、远程文件包含防护、内容过滤、WEBShell防护、敏感信息过滤等类型
邮件过滤	支持SMTP、POP3、IMAP邮件过滤功能
	支持主题、正文、附件敏感词过滤功能
	▲支持钓鱼邮件检测 (提供证明材料并加盖公章)
VPN	支持IPSEC、SSLVPN、PPTP、L2TP、GRE等VPN
路由功能	支持静态路由和动态路由协议 (RIP、RIPNG、OSPFv2、OSPFv3、BGP) (提供证明材料并加盖公章)
	支持基于区域、ISP地址、国家/地址、应用、生效时间的策略路由
	▲支持路由测试配置, 模拟路由匹配结果 (提供证明材料并加盖公章)
IPv6	支持IPv6网络环境, 支持6to4转换、ISATAP等环境

威胁情报	▲支持内置威胁情报中心，可推送实时情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测检测，发现问题后支持一键生成防护规则发现问题后支持一键生成防护规则（提供证明材料并加盖公章）
工作模式	支持路由、透明、混合多种工作模式
	透明模式支持多桥接入，支持8个桥接入
应用代理	支持透明的应用代理，DNS、FTP、HTTP、POP3、SMTP以及TELNET等协议（提供证明材料并加盖公章）
高可用性	支持双机热备和负载均衡
	端口聚合：防火墙多个接口可以设置为聚合口，起到链路备份的功能
	支持双ISP出口热备：当一个出口线路出现故障，系统可以把网络数据流切换到运行状态良好的另一个接口和路由上；
负载均衡	支持服务器负载均衡，支持八种负载算法：轮流、根据权重轮流、最少连接、加权最少连接、局部性最少连接、带复制局部性最少连接、根据源地址做HASH查找、根据目的地址做HASH查找
流量带宽管理	支持基于网络、行为、业务及用户的流量控制，支持设置上行带宽、下行带宽和应用带宽
工作状态自检测	可以实时检测整机运行状态、接口工作状态，一旦有异常发生时，以日志、邮件等形式进行告警
可视化	支持应用风险系数、Top高风险应用、应用类型排行、应用流速趋势、Top应用、接口流量监控、最新威胁列表、最新流量排行、服务器安全、Top安全策略等模块实时监控
	支持应用/威胁/网址/内容过滤等内容统计分析
	▲支持资产风险态势展现，支持内网资产IP地址、风险等级查看（提供证明材料并加盖公章）
	▲支持威胁态势感知展现,包括威胁攻击地图、威胁类型排行、影响IP排行、威胁趋势和最新威胁列表（提供证明材料并加盖公章）
全面的诊断工具	系统提供实用的网络诊断工具，包括ping、tracert、dns及抓包工具
	提供连接管理功能，可根据当前连接状态诊断网络的使用情况
	可提供多种管理方式，包括WEBUI、CONSOLE、SSH
	提供远程集中监控管理功能：支持远程集中管理监控功能，在同一个管理平台下能够对所管理的网络中的防火墙设备进行管理和监控，提供远程升级和统一策略下发
管理	支持SNMP的v1、v2、v3等不同版本，并与当前通用的网络管理平台兼容；
	支持远程的FTP、HTTP的在线升级方式，同时支持本地的离线升级方式
	支持管理员的三权分立，系统提供配置管理员、审计管理员、日志管理员等三种类型的管理员
日志处理和	支持安全日志、应用控制日志、用户认证日志、SSL VPN日志、运行日志、性能日志等分类存储
	支持选择日志存储位置，支持本地存储、外发syslog、态势感知存储

备份	支持手动、自动日志备份
	支持自动合并同类日志和日志条数导出限制（提供证明材料并加盖公章）
报表	支持业务系统、终端IP报表定制，可自定义安全风险概况、业务安全分析、用户安全分析、安全评分细则和危害、安全漏洞分析、拦截率统计、报表名称、报表摘要、报备logo等；
产品联动	▲支持同品牌防火墙、漏扫、IDS、EDR、堡垒机、数审、安全管理中心、网站安全监测、准入等产品联动（提供证明材料并加盖公章）

2、WEB应用防火墙 数量：1台

指标项	指标要求
※硬件规格	国产化CPU：≥2.6GHz，4核；操作系统：国产系统；内存：≥8G；硬盘：≥1T； 接口类型和数量：网络接口包括1个管理口、1个HA口,4个扩展槽；单电源；MTBF（小时）：≥200,000；≥1U机箱
性能要求	HTTP应用层吞吐量(一对接口)≥976.267Mbps，HTTP最大请求速率≥2.498万/秒，HTTP最大并发连接数≥25.805万
安全防护	支持Referer+Cookie的盗链防护，WAF会为防护站点生成Cookie，只有当Referer和Cookie同时正确时，才能正常访问站点，否则，执行防护动作，达到对站点的防护目的。 支持对访问者的请求量统计、应答分布统计以及阈值告警统计，根据访问者对防护站点的访问量来识别攻击者并触发防护策略，实现对站点的安全防护。

<p>WEB应用 防火墙</p>	<p>▲支持配置ip黑白名单，通过对访问源ip进行过滤，同时可对攻击IP进行自动禁封管理，并且可以设置禁封时间和手动删除功能，有效抵御恶意用户（提供证明材料并加盖公章）</p> <p>http防护：支持针对HTTP协议的深度防护，可针对HTTP协议的方法，URL、User-Agent、Cookie、Referer、Accept等长度进行设置。</p> <p>▲支持攻击引擎的查看操作，可根据用户实际业务环境情况有选择的查看防护规则。（提供证明材料并加盖公章）</p> <p>支持CC攻击、HTTP反协议攻击的检测和防护</p> <p>支持虚拟补丁，可对扫描结果产生针对性的虚拟补丁，自动修复扫描结果暴露出的问题，支持内置扫描器的扫描结果、IBM的APPSCAN等扫描工具扫描结果的导入、识别、分析形成策略。</p> <p>▲WEB网页自学习：支持自动学习网页特征并根据学习内容配置防护规则</p> <p>支持WEB业务常规漏洞防护，并支持恶意代码过滤、URL敏感关键字过滤。</p> <p>支持针对URL的网关防篡改防护，支持对防护对象的篡改预警以及快速恢复。</p> <p>规则支持在线升级（自定义升级周期）、离线升级、升级历史信息查看，提供Web应用防护事件库的应急升级，提供重大、突发Web安全事件的响应。</p> <p>▲针对攻击行为防护规则可根据用户情况配置阻断、重定向到指定页面、拦截提醒等响应动作（提供证明材料并加盖公章）防护规则支持中文描述。</p> <p>▲日志中心提供系统和引擎运行日志，日志类型包括：流量日志、威胁日志、访问控制日志、性能监控日志、运行日志、系统日志、配置日志、用户认证日志、NAT日志等（提供证明材料并加盖公章）。</p> <p>支持将生成的报表以EXCEL、HTML、png等通用格式输出，可设置生成报表自动发送邮件。</p>
<p>抗DDoS</p>	<p>支持针对synflood攻击至少提供2种攻击检测方式，如：syn代理、首包丢弃；</p> <p>对于应用层的http协议发起的攻击进行防护：如pushflood、httpfloods等攻击进行防护；</p> <p>支持对多个端口的http同时进行防护；</p> <p>支持对DNS Query flood的攻击检测与防护；</p> <p>针对于指定的服务器可单独配置抗DDos策略；</p> <p>可设置全局的抗DDOS防护参数：可配置synflood、pushflood、udpflood、icmpflood系统紧急防护参数；可配置连接防护开关和防护参数；可配置DNS放大攻击防护参数；</p> <p>支持攻击特征自识别功能：可配置数据包采样参数，通过分析，自动抓取攻击特征；</p> <p>支持用户自定义攻击特征定义。</p>

其它	<p>支持直路部署，如路由/桥/多桥模式部署。</p> <p>支持服务器负载均衡，可根据用户需求和灵活的算法提供后端服务器的请求负载均衡。</p> <p>▲系统提供WEB方式的系统资源使用情况（CPU、内存、磁盘）、接口状态查看、引擎流量、运行态势、服务器监控日志等信息进行查看。</p> <p>▲提供磁盘诊断与修复工具</p> <p>提供WEB扫描功能</p> <p>▲WEB页面提供接口状态查看工具、进程状态查看工具、磁盘使用情况查看工具、系统路由查看工具、内核调试工具</p> <p>支持日志数据以ftp或sftp方式远程备份到其它存储设备</p> <p>信任主机支持MAC地址绑定</p>
----	--

3、入侵防御系统 数量：1台

指标项	指标要求
※硬件规格	<p>国产化CPU：≥2.6GHz，4核；操作系统：国产系统；内存：≥8G；硬盘：≥1T；</p> <p>接口类型和数量：≥6*GE电口(3路Bypass),≥4*GE光口（不含模块），2个扩展槽；</p> <p>单电源；≥1U机箱</p>
性能要求	<p>▲满检速率：≥3601.268Mbps，TCP并发连接数：≥300万，设备具备3年IPS、防病毒、应用识别、防病毒、僵尸网络防御、威胁情况升级授权；</p>
安全业务	<p>▲支持安全运营中心概览，自动进行网络风险评估、监测分析和风险建议（提供证明材料并加盖公章）</p> <p>▲支持勒索专项防护，展示勒索风险业务、攻击暴露面管理、弱口令检查（提供证明材料并加盖公章）</p> <p>支持业务安全概览，展示业务风险、漏洞风险、全网热点事件展示</p> <p>支持用户安全概览，展示不同风险级别和失陷风险用户、支持攻击趋势分布展示</p> <p>支持攻击者IP一键封锁和自定义封锁时间</p>
安全能力	<p>▲内置漏洞攻击特征库、应用识别库、URL特征库、病毒防护库、WEB应用防护库、数据泄密防护库、僵尸网络防护库、实时漏洞分析识别库、IP地址库、热点时间预警与处置库、威胁情报等，可在线/离线升级（提供证明材料并加盖公章）</p> <p>▲支持漏洞攻击防护、web应用防护、僵尸网络防护、内容安全防护、应用控制预置策略模版（提供证明材料并加盖公章）</p>
访问控制	<p>▲能够基于区域、网络对象、服务、应用、地域、生效时间等多个元素进行访问控制（提供证明材料并加盖公章）</p> <p>▲支持策略标签化（提供证明材料并加盖公章）</p> <p>▲支持策略生命周期管理，展示变更时间、变更原因、变更账号等信息（提供证明材料并加盖公章）</p> <p>支持失效策略检查</p> <p>支持模拟策略匹配</p>

	<p>▲支持策略优化自动分析及展示，显示一般问题、严重问题和建议优化等不同级别的问题策略，支持对90天无匹配、任意权限、完全冲突、目的放通过大、完全冗余、影子策略、风险端口放行等策略问题分析（提供证明材料并加盖公章）</p>
连接数控制	支持源、目的区域/对象的并发和新建数（提供证明材料并加盖公章）
端口镜像	支持将任意接口的数据完全镜像到设备自身的其他接口，用于抓包分析
NAT功能	支持基于接口地址、地址池、VLAN接口、目标接口、目标地址的NAT、反向NAT及双向NAT
	可实现跨NAT的H.323通讯
身份认证	支持本地认证，支持本地认证、Radius认证、Tacacs认证、AD域认证、POP认证、LDAP认证等，同时支持IP/MAC绑定、硬件特征码绑定
	▲支持操作系统版本、文件、进程、注册表、登录IP、登录时间等终端认证安全检查方式（提供证明材料并加盖公章）
	支持WEB登录前、登录后安全检查
DDoS攻击 防御	▲支持外网对内攻击防护功能，支持防御ARP洪水攻击、SYN Flood、UDP Flood、DNS Flood、ICMP Flood、ICMPv6 Flood、RST Flood、ACK Flood、HTTP Flood、IP地址扫描、端口扫描防御等攻击（提供证明材料并加盖公章）
	▲支持内网对外攻击防护功能，支持防御SYN Flood、UDP Flood、DNS Flood、ICMP Flood、ICMPv6 Flood、RST Flood、ACK Flood、HTTP Flood、IP地址扫描、端口扫描防御等攻击（提供证明材料并加盖公章）
	支持DoS排除
入侵防御	内置入侵防御规则数≥9800
	支持network_device漏洞攻击、media漏洞攻击、dns漏洞攻击、ftp漏洞攻击、mail漏洞攻击、database漏洞攻击、telnet漏洞攻击、shellcode漏洞攻击、口令暴力破解、trojan漏洞攻击、spyware漏洞攻击、backdoor漏洞攻击等攻击防御
病毒防护	支持木马查杀、恶意软件、勒索病毒、挖矿、C&C通信、暗网、扫描器，比如Trojan.agent, Trojan. Downloader, Trojan.Dropper、Omni,CC攻击等
上网行为管理	支持9700+种应用识别，包括基本服务、HTTP、视频、P2P、流媒体、网络游戏、即时通讯、股票、网上银行、网络电话、网络存储、网页邮箱、软件更新、远程控制、网络货币、网上支付、生活服务、新闻媒体、社交通讯、旅游、贷款等
	▲支持限速、会话限制、阻断、警告等多种应用管控方式（提供证明材料并加盖公章）
URL管控	支持URL过滤功能，同时支持用户自定义URL库，系统内置上万条的URL库
内容防泄漏	▲支持邮件、论坛发帖/回复、外发文件的内容识别（提供证明材料并加盖公章）
	支持120+文件类型识别
	支持银行卡号、身份证号、手机号等默认防护规则
WEB攻击防护	支持1100+WEB防护规则，支持防御SQL注入、跨站脚本攻击、自动扫描防护、WEB爬虫防护、WEB服务器漏洞攻击、WEB插件漏洞、LDAP注入防护、SSI指令防护、XPATH注入防护、命令行注入防护、路径穿越防护、远程文件包含防护、内容过滤、WEBShell防护、敏感信息过滤等类型

邮件过滤	支持SMTP、POP3、IMAP邮件过滤功能
	支持主题、正文、附件敏感词过滤功能
	支持钓鱼邮件检测（提供证明材料并加盖公章）
路由功能	▲支持静态路由和动态路由协议（RIP、RIPNG、OSPFv2、OSPFv3、BGP）（提供证明材料并加盖公章）
	支持基于区域、ISP地址、国家/地址、应用、生效时间的策略路由
	▲支持路由测试配置，模拟路由匹配结果（提供证明材料并加盖公章）
IPv6	支持IPv6网络环境
威胁情报	▲支持内置威胁情报中心，可推送实时情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测检测，发现问题后支持一键生成防护规则发现问题后支持一键生成防护规则（提供证明材料并加盖公章）
工作模式	支持路由、透明、虚拟网线、旁路镜像、聚合、混合多种工作模式
	透明模式支持多桥接入，支持8个桥接入
应用代理	▲支持透明的应用代理，DNS、FTP、HTTP、POP3、SMTP以及TELNET等协议（提供证明材料并加盖公章）
高可用性	支持双机热备和负载均衡
	端口聚合：入侵防御多个接口可以设置为聚合口，起到链路备份的功能
	支持双ISP出口热备：当一个出口线路出现故障，系统可以把网络数据流切换到运行状态良好的另一个接口和路由上；
负载均衡	支持服务器负载均衡，支持八种负载算法：轮流、根据权重轮流、最少连接、加权最少连接、局部性最少连接、带复制局部性最少连接、根据源地址做HASH查找、根据目的地址做HASH查找
流量带宽管理	支持基于网络、行为、业务及用户的流量控制，支持设置上行带宽、下行带宽和子应用带宽
工作状态自检测	可以实时检测整机运行状态、接口工作状态，一旦有异常发生时，以日志、邮件等形式进行告警
可视化	支持应用风险系数、Top高风险应用、应用类型排行、应用流速趋势、Top应用、接口流量监控、最新威胁列表、最新流量排行、服务器安全、Top安全策略等模块实时监控
	支持应用/威胁/网址/内容过滤等内容统计分析
	▲支持资产风险态势展现，支持内网资产IP地址、风险等级查看（提供证明材料并加盖公章）
	▲支持威胁态势感知展现,包括威胁攻击地图、威胁类型排行、影响IP排行、威胁趋势和最新威胁列表（提供证明材料并加盖公章）
全面的诊断工具	系统提供实用的网络诊断工具，包括ping、traceroute、dns及抓包工具
	提供连接管理功能，可根据当前连接状态诊断网络的使用情况
	可提供多种管理方式，包括WEBUI、CONSOLE、SSH

	提供远程集中监控管理功能：支持远程集中管理监控功能，在同一个管理平台下能够对所管理的网络中的防火墙设备进行管理和监控，提供远程升级和统一策略下发
管理	支持SNMP的v1、v2、v3等不同版本，并与当前通用的网络管理平台兼容；
	支持远程的FTP、HTTP的在线升级方式，同时支持本地的离线升级方式
	支持管理员的三权分立，系统提供配置管理员、审计管理员、日志管理员等三种类型的管理员
日志处理和备份	支持安全日志、行为日志、用户日志、系统日志等分类存储
	支持选择日志存储位置，支持本地存储、外发syslog、态势感知存储
	支持手动、自动日志备份
	▲支持自动合并同类日志和日志条数导出限制（提供证明材料并加盖公章）
报表	支持业务系统、终端IP报表定制，可自定义安全风险概况、业务安全分析、用户安全分析、安全评分细则和危害、安全漏洞分析、拦截率统计、报表名称、报表摘要、报备logo等；
产品联动	▲支持同品牌IPS、漏扫、EDR、沙箱、安全管理中心等产品联动（提供证明材料并加盖公章）
分布式	支持分布式部署，通过将设备分为父节点和子节点实现分布式管理
	▲支持分布式架构通过拓扑展示，可在拓扑上点击配置分布式策略（提供证明材料并加盖公章）
	▲支持统一升级、配置同步、时钟同步、策略下发等功能，支持任务、通知、意见三种消息下发（提供证明材料并加盖公章）
安全助手	支持风险分析、web扫描、热点事件预警

4、上网行为管理 数量：1台

指标项	指标要求
※硬件规格	国产化CPU：≥2.3GHz，8核；操作系统：国产系统，内存≥8G，硬盘≥32G MSA TA+2T，接口类型和数量：网络接口≥6个千兆电口和≥2个万兆光口；冗余电源：≥1U机箱
性能要求	网络层吞吐量≥10G，应用层吞吐量≥3G，出口带宽≥1.5G，并发连接数≥500万；
即插即用模式	▲支持即插即用模式，无需干涉终端的任何IP地址设置（提供证明截图并加盖公章）
ARP表/邻居表	▲支持WEB管理ARP表查看，并支持指定静态ARP；支持WEB管理IPv6邻居表查看，并支持指定静态（提供证明截图并加盖公章）
智能DNS服务器	▲基于IP信息给不同的用户最合适的服务器IP（提供证明截图并加盖公章）
	▲支持智能DNS均衡策略，支持权重、上下行、总流量均衡算法（提供证明截图并加盖公章）
	▲支持A记录、Cname记录、Mx记录分配DNS策略（提供证明截图并加盖公章）

社交账号认证	支持企业微信，钉钉，Facebook，Gmail认证。（提供证明截图并加盖公章）
临时账号	▲支持申请临时账号申请，批量申请以及手动审核和自动审核（提供证明截图并加盖公章）
IP管理	▲支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量；（提供证明截图并加盖公章）
终端识别发现	▲自动发现网络里面的终端，并获取IP、Mac操作系统、开放服务、开放端口等信息，支持根据ip段、MAC、使用者过滤用户，以便和其他过滤方式一起组合来搜索或获取终端信息；（提供证明截图并加盖公章）
终端分类可视	1.对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 2.支持查看终端类型，以及终端详细信息（厂商，系统，端口等）； 3.支持查看终端类型分布； 设备必须支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，支持移动终端型号识别，至少识别不少于10种移动终端型号；
应用识别规则库	1.设备内置应用识别规则库，支持超过8000种以上的应用，并保持每两个星期更新一次，保证应用识别的准确率； 2.支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类； 3.支持给每个应用自定义标签； 4.支持根据标签选择一类应用做控制； 5.支持对每一种应用的定义和解释，帮助客户快速定位应用的分类； 6.支持给每一种应用列上图标，易于客户了解应用的特征。
资产识别库	▲支持网络设备、物联网设备、安全设备和计算机操作系统等设备类型识别（提供证明截图并加盖公章）
IP白名单	支持根据源IP，目的IP设置白名单，白名单流量可设置不做审计和流量控制，也可以设置为不做流量控制
URL白名单	URL白名单
广告拦截规则	通过终端插件拦截指定软件弹窗广告并上报日志到设备。
用户登录次数限制	支持每日登录次数，每次单次上线时间
基于每个端口实时统计	基于服务、用户的实时流量统计可以基于每个端口独立统计
syslog日志同步	支持日志同步至syslog服务器：上网行为日志、系统日志、时间日志等
刷卡认证	支持对接第三方刷卡器进行刷卡认证
DDOS防护	▲内网对外网攻击防护，基于源区域或源地址进行TCP最大连接数、最大攻击包次数等防护

服务器防护	HTTP异常检测将HTTP头部中的Referer、User-Agent、Host字段进行攻击的检测
web应用防护告警	检测到web应用行为，产生web应用防护告警记录，支持发送邮件通知管理员、syslog日志同步

5、终端安全管理系统 数量：1套

指标项	指标要求
终端管理中心	终端管理中心，实现对终端的统一管理、策略下发、安全监控、终端升级、分布式管理等，支持杀毒、EDR、桌管、数据防泄密功能，支持全网统一杀毒和升级、资产信息采集、终端行为采集、防暴力破解、异常告警、联动响应身份鉴别、访问控制、恶意代码防范等基线核查，支持网络管控、外设管控、移动存储管控、WIFI外连检测、违规外连检测溯源、屏幕水印等。
	220个点
	▲具备人工智能引擎，人工智能引擎支持PE/OFFICE/PDF常见文件类型威胁检测（提供证明截图并加盖公章）
	▲支持目录白名单、文件哈希白名单、签名证书白名单三种方式（提供证明截图并加盖公章）
	▲人工智能引擎支持Windows/Linux/国产操作系统（提供证明截图并加盖公章）
	▲人工智能引擎支持X86/ARM硬件平台
	▲支持扫描过程中动态切换扫描速度，支持多核极速、多核高速、单核节能三种工作模式（提供证明截图并加盖公章）
	Windows/Linux/国产操作系统提供相同的杀毒UI界面（提供证明截图并加盖公章）
	▲客户端界面支持中文/英文等多种语言切换，且切换时不需要重启软件（提供证明截图并加盖公章）
	▲客户端界面支持4K/2K/1080P分辨率下无失真显示（提供证明截图并加盖公章）
	▲具有持续记录终端进程活动的机制，包括包括进程启动和结束、模块加载、驱动加载等信息
	▲具有持续记录终端网络活动的机制，包括捕获网络连接行为信息、域名访问信息、URL（支持HTTP和HTTPS）访问信息、进程PID、进程路径等（提供证明截图并加盖公章）
	▲具有持续记录终端文件活动的机制，包括捕获文件的创建、重命名、删除信息、进程PID、进程路径等
	具有持续记录终端注册表活动的机制，包括键值和子键的创建、重命名、修改、删除信息、进程PID、进程路径等
	具有持续记录账号变化的机制，包括创建账号、删除账号、修改账号信息、修改账号密码、创建克隆账户等（提供证明截图并加盖公章）
	具有持续记录网络文件传输的功能，包括FTP文件传输、邮件文件传输、HTTP文件传输和文件共享传输、进程PID、进程路径等
	具有持续记录USB设备插拔、打印活动的机制

1

客户端	提供RDP、SMB、SSH协议暴力破解监测与自动阻断功能，支持自定义爆破阈值和封停时间
	▲支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源IP、暴力破解类型、被攻击IP地址、最近攻击时间、累计攻击次数、封停状态
	提供CPU、内存、磁盘、流量异常检测与告警功能
	▲支持对硬盘温度和硬盘故障状态提供告警，支持固态硬盘、机械盘等（提供证明截图并加盖公章）
	支持采集主流操作系统日志，包括包括格式化磁盘、切断网络、创建服务、创建计划任务、修改远程管理策略、修改系统防火墙状态、修改自带杀毒软件状态等（提供证明截图并加盖公章）
	支持采集第三方服务软件日志，包括主流数据库日志、主流中间件日志、FTP日志、邮箱系统日志等（提供证明截图并加盖公章）
	提供WIFI外联检测机制，发现WIFI能够设置告警、断网等违规处理手段（提供证明截图并加盖公章）
	提供取证服务器安装包，支持用户自己搭建部署取证服务器
	支持自定义印章标题和脚注作为屏幕内容水印显示，支持设置印章半径、颜色等内容
	支持自定义主机名、IP地址、MAC地址、时间作为屏幕内容水印显示，支持设置二维码大小、背景色、前景色等内容
	支持设置点阵水印圆点半径、间隔、描边色、填充色等内容，具有单独的点阵水印检索页面
	支持对文本水印、印章水印、二维码水印和点阵水印设置明水印和隐水印
	管理平台具备整体安全概览展示，包括威胁趋势、安全概况、防护概况、安全合规、高危终端TOP10、高危病毒TOP10、待办事项等
	支持病毒、勒索病毒、webshell、可疑账号、可疑文件、异常通信链路、隔离终端、暴力破解的全网数量统计

6、日志审计系统 数量：1台

指标项	指标要求
※硬件规格	国产化CPU：≥2.6GHz，4核；操作系统:国产系统；内存≥16GB,硬盘≥1TB,网络接口:≥8个千兆电口、≥4个千兆光口，冗余电源；≥2个扩展槽；≥1U机箱
性能要求	日志审计节点许可数量≥50个，支持授权扩展

工作模式	<p>独立完成审计日志采集，不依赖于设备或系统自身的日志系统；</p> <p>审计工作不影响被审计对象的性能、稳定性或日常管理流程；</p> <p>审计结果存储于独立存储空间；</p> <p>自身用户管理与设备或主机的管理、使用、权限无关联；</p> <p>提供全中文WEB管理界面，无需安装任意客户端软件或插件</p>
设备部署	<p>设备采用旁路部署，不影响业务环境；</p> <p>支持分布式部署模式（提供证明材料并加盖公章）；</p> <p>对复杂的网络环境，支持部署分析系统和多采集器配合使用形式；</p> <p>支持页面一键添加子节点资产，自动进行绑定添加；</p> <p>▲支持集中式管理和升级模式（提供证明材料并加盖公章）</p>
功能扩展	<p>▲支持kafka日志接收转发、大数据安全域同步等大数据联调功能（提供证明材料并加盖公章）</p> <p>▲支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器（提供证明材料并加盖公章）</p>
日志收集	<p>▲支持Http、Syslog、Snmpttrap、Tcp、Vflow、WMI、FTP、SFTP、SSH、TELNET、SCP、LEA、FILE、WebService、AGENT等日志采集方式（提供证明材料并加盖公章）</p> <p>支持使用代理方式提取日志并收集，代理类型包括Windows、Linux；</p> <p>▲支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等，内置超过500+规则，包括但不限于：Cisco(思科)、Juniper、联想网御/网御神州、F5、华为、H3C、微软、绿盟、飞塔(Fortinet)、Foundry、天融信、启明星辰、天网、趋势、东软、Nokia、CheckPoint、Hillstone(山石)、安恒信息、珠海伟思、BEA、中国电信、安氏、帕拉迪、APC、Arbor、Clam、戴尔（Dell）、Digium、东方电子、EMC、中国电力科学研究院、Eudora、Google、冠群金辰、Linksys、McAfee、Netapp、NAS（美国国家安全局）、永达、Sonicwall、Vigor、天存、西岭、Symantec（赛门铁克）、Hardened-PHP、Foundertech(方正)、三零盛安、Allot、蓝盾、IBM、金诺网安、网威、Nortel(北电)、Citrix(思杰)、Watchguard、中兴、阿帕奇、Windows系统日志、Linux/UNIX syslog、IIS、Apache等（提供证明材料并加盖公章）；</p> <p>支持常见的虚拟机环境日志收集，包括Xen、XenServer及Esxi等；</p> <p>▲支持syslog日志采集及转发加密传输（SM4、AES）和国密SM3签名（提供证明材料并加盖公章）</p>

日志分析

▲可以操作系统、域名、时间、国家、显示、维度等条件进行过滤（提供证明材料并加盖公章）；

支持对收集到的重复的日志进行自动的聚合归并，减少日志量；

支持可由用户定义和修改的日志的聚合归并逻辑规则；

支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；

支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展。

▲可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息等，支持设置解析处理线程数、计数器间隔（提供证明材料并加盖公章）；

▲支持基于内存的实时关联分析，跨设备的多事件关联分析，支持仅保存关联事件；

▲支持自定义条件的事件进行聚合，包括但不限于源地址、源端口、目的地址、目的端口等聚合属性；

▲支持自定义字段和策略的脱敏配置；（提供证明材料并加盖公章）；

▲内置主机异常、网络攻击、恶意软件、暴力破解、漏洞利用、权限异常等6大类59子类的安全分析场景（提供证明材料并加盖公章）；

关联分析的规则可定制；

资产管理	<p>▲支持Windows、Unix、Linux、Solaris、FreeBSD、HP-UX、虚拟化设备等主机类设备，路由器、交换机等网络设备，防火墙、网闸等网络安全设备，WEB服务器、数据库服务器等应用类设备，门禁、打印机、无线等设备进行资产管理（提供证明材料并加盖公章）；</p> <p>支持资产发现功能，资产信息包含组织架构字段；</p> <p>▲支持资产性质、机密性价值、可用性价值、完整性价值等资产属性（提供证明材料并加盖公章）；</p> <p>支持管理、组织架构管理、安全域管理、资产类型管理、业务管理等功能；</p> <p>支持资产视图功能，实时显示发送日志的资产数、被监控的资产数和审计组件等应用情况，支持分类视图、监控域视图、组织架构视图、网络视图、资产类型视图、地图视图、拓扑、安全域视图、业务视图等多种视图模式；</p> <p>支持日志源统计功能，统计各日志源活跃度、日志协议、事件数量、最后更新时间；</p> <p>支持资产监控功能，展示监控对象的信息，如名称、管理IP、MAC地址、监控状态、接口流入/流出速率、系统进程数、系统生产商、CPU/内存信息、平均CPU占用率、平均MEM占用率、磁盘总使用率、磁盘分区使用率、磁盘读取速率、磁盘写入速率等信息；</p> <p>▲支持资产导入导出格式，默认支持XML、CSV及Excel三种格式（提供证明材料并加盖公章）；</p> <p>▲支持脆弱性监控功能，支持漏扫报表导入，支持脆弱性监视状态统计、脆弱性等等级统计等图形展示结果（提供证明材料并加盖公章）；</p> <p>支持展示漏洞类型、漏洞来源、处理状态、最近发现时间功能；</p>
事件统计	<p>支持事件统计查看，支持分组事件总数、事件级别、事件趋势以及事件类型、资源类型等事件统计，显示和查看全部安全事件日志；</p> <p>▲支持基础查询、高级查询、专业查询三种查询模式；（提供证明材料并加盖公章）；</p> <p>支持可指定多个筛选条件进行组合查询，条件如时间、规则集、事件级别、类型、设备名称、IP等查询参数；</p> <p>支持显示列信息可以选择，列展示的先后顺序可以手工调整；</p> <p>支持事件级别有8种，分别为：调试、通知、注意、告警、错误、关键、报警及紧急；</p> <p>支持查看事件详情，事件详情包括时间信息、基本信息、来源信息、目标信息、事件分类信息、设备信息、关联事件、威胁信息（恶意文件/脚本）、资产详情及资产的弱点信息等；</p> <p>极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果；</p> <p>支持原始日志查看。</p>

告警功能	<p>支持告警统计，支持告警级别、告警类别、资源类型、订阅告警、待告警事件、外部告警用户、自定义告警以及最新告警等类型告警统计；</p> <p>所有统计支持近1小时、近24小时、近7天、近30天等的事件等维度查看统计信息；</p> <p>可预设置安全告警策略；</p> <p>支持数据阈值设置，超过阈值将产生告警；</p> <p>▲可以通过邮件、短信、微信、钉钉、TCP订阅、FTP订阅、Kafka订阅、Syslog订阅等方式进行告警事件订阅（提供证明材料并加盖公章）；</p> <p>支持自动防止报警信息在短时间内大量发送(告警抑制)；</p> <p>具备报警合并和在一个时间段内抑制报警次数的能力。</p>
用户管理	<p>根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，系统管理员只负责完成设备的初始配置，安全配置员只负责审计规则的建立，审计管理员只负责查看相关的审计结果及告警内容；</p> <p>▲支持普通模式与涉密三权模式的切换功能（提供证明材料并加盖公章）；</p> <p>▲支持新建、启用和禁用账户，支持账户动态令牌登录（提供证明材料并加盖公章）；</p> <p>▲支持设置登录黑名单（提供证明材料并加盖公章）；</p> <p>▲支持登录密码策略设置，可匹配弱点库（提供证明材料并加盖公章）；</p> <p>▲支持查看设备登录会话，针对异常登录账户可进行强制下线（提供证明材料并加盖公章）；</p> <p>支持细粒度的记录账号操作日志记录。</p>
系统管理	<p>▲支持一键检测功能，检查采集程序、syslog端口号、数据库监控信息、系统CPU、MEM、Swap检测状态、资产总数等检查项（提供证明材料并加盖公章）；</p> <p>集成Ping、Traceroute、NetBios、SNMP连接测试、TCP端口扫描、抓包工具、实时抓包等多种工具；</p>
报表	<p>支持报表导出操作，导出类型包括word、pdf、Excel；</p> <p>▲支持查看报表统计信息，系统内置报表类型包括：综合分析、按认证操作分析、按授权操作分析、按账户操作分析、按访问控制分析、按设备异常分析、按配置变更分析和按攻击威胁分析等8大类型审计报告（提供证明材料并加盖公章）；</p> <p>支持自动生成日报、周报及月报。</p>
知识库	<p>支持内置弱点库；</p> <p>支持内置漏洞库，包括74000+漏洞信息（提供证明材料并加盖公章）；</p> <p>支持内置知识库，包括知识文章、安全专家、事故案例、漏洞库、病毒库、补丁库、安全基本要求、安全文档、应急预案库等类别知识；</p>

二、信息系统等保测评

采购人须对等保测评机构资质进行审核，供应商承担保测评费用，测评机构需要提前介入项目给予项目实施指导，供应商需配合等保测评机构工作，完成测评机构提出的设备配置、网络的优化调整等工作，主要服务内容：“一业一证”信息系统的网络安全等级保护二级测评服务。测评单位需要有国家信息安全测评信息安全服务资质证书，未经采购方同意，项目组成员不得更改。

服务	功能要求
----	------

基本 要求	<p>供应商须提供完善的测评实施方案和计划、测评方案，经我单位审核通过后实施，在项目实施期间由有丰富实施经验的信息安全等级保护测评中级及以上测评师为项目实施团队主要负责人和核心成员，全程参与项目实施。</p> <p>测评服务流程：</p> <p>(1)针对测评系统协助定级备案；</p> <p>(2)进行系统调研；</p> <p>(3)编制测评方案；</p> <p>(4)进行现场测评、渗透测试；</p> <p>(5)编制整改方案，并协助整改；</p> <p>(6)安全加固；</p> <p>(7)进行现场复测评；</p> <p>(8)形成测评报告、渗透测试报告；</p> <p>配合项目验收。</p>
其他 要求	<p>1.测评机构所提供的项目经理和实施人员应是具有丰富经验和专业技能的技术骨干，应有同类项目经验。</p> <p>2.在测评机构以往参与的项目中，应具有项目实施、熟悉项目需求和团队建设方面的优势。</p> <p>3.测评机构应在项目全过程中严格遵循各项管理制度的要求，确保项目顺利开展。</p>

三、网络安全服务

服务	子服务	具体要求
----	-----	------

1、网络安全管理咨询服务

- 1、网络安全定制辅导服务：在遵循国家的信息安全政策法规及相关管理标准规范下，梳理一套标准化，层次化，一体化的管控体系框架，以适应于我单位信息安全工作一体化的要求，提升政务中心安全管理体系的可用性、可行性和可落地性。完善及优化西安市碑林区政务服务中心的信息安全管理标准框架，强化西安市碑林区政务服务中心信息安全管理自我改进能力。频次1次/年。
- 2、网络安全管理规范建设服务：根据网络安全法、工作责任制等网络安全基本政策要求，协助用户建立、完善网络安全管理机构、具体工作职能部门和岗位；协助客户建立并梳理网络安全工作制度、表单等，构建基础的网络安全管理体系。频次：1次/年。
- 3、网络安全培训服务：依据国家网络安全法规、标准，开展包括安全意识教育培训、信息安全技术培训等工作，通过循序渐进的方式，从浅显的网络安全基础知识到网络安全的实战经验，使工作人员能够更容易的由浅入深掌握网络安全的相关内容。内容：安全意识教育培训，频次：2次/年；网络安全技能培训，频次：1次/年。
- 4、资料输出服务：服务期结束后，将年度相关资料分类整理，形成胶装文件、电子档案、分类档案。频次：1次/年。

网络安全服
务

2、网络安
全技术支持
服务

- 1、全策略优化服务：服务范围覆盖所有安全产品，评估当前的安全产品策略库是否遵从组织当前的安全方针，是否根据业务目标的变化进行了调整；跟踪访问控制主体和客体的变化，及时剔除过期和失效的安全策略；优化现有安全策略，进行分类和整合，以便于管理员的日常维护工作。1次/年。
- 2、网络安全巡检服务：硬件状态检查，包括设备电源状态、网络接口状态、设备所在物理环境状态等。性能负载检查，包括CPU、内存的占用率、日志存储空间的占用率等。安全策略检查更新，检查安全策略的有效性，更新安全产品的规则库。日志功能检查，检查日志功能的有效性，确保能正常生成日志。4次/年。
- 3、安全态势分析服务：通过对信息系统定期检测（工具扫描及安全专家人工检测），及时发现信息系统（网络架构、网络设备、服务器主机、操作系统、数据库和用户账号、口令等安全对象）存在的各种安全隐患，提出系统加固建议以及相关的应急措施。同时安全产品进行日志分析，对事件定制可读性强的专业报告，并针对报告中提出的问题提供修补建议。
- 4、设备数据备份及恢复演练服务：开展设备配置文件数据备份工作，提供独立可信保密介质，适时开展恢复演练工作。频次：2次/年。
- 5、网络安全应急响应服务：安全运维小组提供7*24响应服务，当网络系统发生黑客入侵、系统崩溃或影响业务正常运行的安全事件时，在第一时间对安全事件进行应急响应处理，使用户的网络系统或者业务系统在最短时间内恢复正常。
- 6、重保支撑服务：根据客户网络的实际情况，在国家重大政治活动和节假日期间，针对近期可能发生的网络安全威胁，提供相应的技术防护服务，确保客户处网络的安全可靠运行。
- 7、应急预案及演练服务：依据国家网络安全相关法规，从应急响应的实际问题出发，制定网络安全应急预案，频次：2次/年；根据工作进度适时开展应急演练工作，提交应急演练报告，频次：1次/年。
- 8、配合检查服务：配合迎检工作，包括上级主管部门、监管部门的网络安全检查工作。
- 9、对于新出现的安全风险事件，提早做出预防措施。
- 10、对于检测出的安全漏洞和病毒，及时进行处理和解决。

3、网络安全风险评估服务	以现场派驻人员和远程支持相结合的方式对被评估对象进行一系列的安全探测，以发现网络中和系统中可能存在的安全隐患。通过评估工具以远程扫描的方式对评估范围内的系统和网络进行安全扫描，查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。按照风险评估标准对用户网络存在的安全风险开展评估服务，提供具备网络安全检测资质的风险评估报告。频次：1次/年。
--------------	--

四、网络相关运维服务

服务	功能要求
网络运维服务	<p>1、网络基础构架运维服务，对网络调整优化需求和故障进行处理，包括：网络VLAN划分、网络故障分析与处理、客户所有服务器操作与管理（操作系统级别）、硬件设备的安装调试、硬件设备的送修服务等服务。</p> <p>2、网络设备维护：包括交换机、路由器、防火墙等网络设备的安装、配置、调试和维护，确保网络设备的正常运行。</p> <p>3、无线AP管理：管理和维护大厅无线WiFi，确保WiFi的稳定运行。</p> <p>4、网络巡检服务：每月进行一次巡检，巡检的对象包括服务器、交换路由设备、安全设备,形成书面报告，每年能形成全年性巡检服务汇总文档。</p> <p>5、容量规划：根据网络的当前使用情况和未来发展趋势，预测网络的容量需求，并据此规划网络的升级或扩展。</p> <p>6、为我单位提供相关的技术支持服务，协助大厅进行信息化、智能化、系统集成等项目的方案设计及实施；因其它项目建设，提出协助请求时（如长时间停电、系统切换、调整网络结构、线路迁移等），供应商须派专业技术人员到现场监控设备的运行情况和做相关配合工作。</p> <p>7、综合布线维护管理：对机房线路进行归置整理、对大厅网络线路的检查和测试、对机柜及配线架的线缆进行整理等、对网络线路、网络设备进行标注和设备的管理，负责机房、分机房和上网终端的维护，及时排查和解决网络问题。</p> <p>8、文档管理：编写和维护网络设备的配置文档、操作手册、故障处理指南等文档，为网络运维提供参考。</p> <p>9、合规性检查：确保网络运营符合相关的上级部门的法律法规和政策，比如数据保护法规、网络使用政策等。</p> <p>10、资产梳理：对大厅涉及的信息资产进行梳理，以及IP的梳理和动态管理，并形成文档资料。（频次：2次/年）</p> <p>11、其他维护管理：机房所需的相关管理制度、告示牌、机房设备整理等，对机房内上墙的网络拓扑图及相关制度进行更新优化。</p> <p>12、根据我单位工作实际情况，不限次数上门网络故障处理服务（24*7全天候）</p>

		<p>服务器运维</p> <ol style="list-style-type: none"> 负责整体大厅服务器的架构评估、规划设计、扩容改造及新项目上线实施工作等； 负责服务器等相关设备的每日巡检与维护工作，定期检查服务器系统日志、设备健康状态监控、故障响应、及处理漏洞修复、关闭非必要映射端口、保障数据安全和解决安全隐患等，保证大厅服务器正常运行； 负责大厅服务器安全监控策略体系建设、安全应急事件响应和复盘，不断提升服务器安全监控能力； 掌握服务器系统、MySQL数据库、Web服务器的攻防技术和安全配置，能够进行系统安全加固，定期查看数据库和服务器日志，定期对服务器数据进行备份冗余； 按照上级部门要求，排查和扫描相关漏洞，及时修复不安全的漏洞，并形成系统文档。 根据大厅实际需求，配置Nginx服务器，配置Apache Web服务器，确保各类服务稳定运行。 对于已上线的服务，可修改和调整前端代码（html、CSS、JS），可少量修改后端服务代码（PHP、JAVA）。 负责大厅服务器对应的域名配置和维护电信网络备案、确保我局域名和子域名解析准确无误，使用SSL证书加密传输（https）。 	
		<p>监控运维服务</p> <ol style="list-style-type: none"> 设备巡检：定期对安防监控系统的硬件设备进行巡检，包括摄像头、服务器、线路和存储阵列等，确保设备正常工作，防止故障和损坏。 故障修复：对于发现的设备故障或异常，及时进行排查和修复，以保证安防系统的连续可用性。 设备清洁：定期对设备进行清洁，如清理摄像头镜头、清理设备内部灰尘等，确保设备的正常运行。 设备扩容与升级：按照用户的需求完成安防系统的扩充服务，以满足更高的监控需求。 网络设备维护：对监控系统的网络设备进行保养和维修，包括路由器、交换机、防火墙等，确保监控网络通畅无阻。 网络安全防护：采取措施防范网络安全风险，如设置密码、加密通信、安装杀毒软件等，保护监控系统免受网络攻击。 实时监控：对安防监控系统的运行状态进行实时监控，包括设备的在线状态、存储空间情况、网络连接状态等，及时发现并解决可能出现的问题。 异常响应：对于设备故障、报警事件等异常情况，及时做出响应和处理，以保证安全和秩序。 	
<p>3.2.3人员配置要求 采购包1： 满足采购人要求</p>		<ol style="list-style-type: none"> 维保记录：对维护过程进行记录，并保存维护记录，方便后续查询和分析。 	

3.2.4设施设备要求
采购包1：
满足采购人要求

3.2.5其他要求

采购包1:

1. (响应文件格式-标的清单) 1.1服务范围: 碑林区政务服务中心网络安全升级项目; 1.2服务要求: 符合磋商文件有关技术、商务要求; 1.3服务标准: 符合国家和省、市有关行业标准及采购人的有关规定。 2.本项目采购的网络安全设备等硬件设备, 质保期为验收合格之日起不少于3年, 并提供不少于3年病毒库、特征库、规则库的升级服务。

3.3商务要求

3.3.1服务期限

采购包1:

合同签订后10个日历日交付网络安全设备要求的所有设备; 信息系统等保测评以采购人要求时间为准; 网络安全服务期限为合同签订之日起1年; 网络相关运维服务期限为合同签订之日起1年。

3.3.2服务地点

采购包1:

采购人指定地点

3.3.3考核(验收)标准和方法

采购包1:

1.由采购人和成交供应商共同对项目进行整体验收。其内容包括是否按照采购人要求进行服务、是否在规定时间内服务完毕。①系统累积无故障时长 ≥ 363 天②系统正常运行率 $\geq 98\%$ ③信息系统软件修复响应时间 ≤ 10 分钟。 2.其他事项: (1)验收合格后, 填写政府采购项目验收单作为对本服务的最终认可。(2)服务商向采购人提供服务过程中的所有资料, 以便采购人日后管理。(3)验收依据: ①磋商文件、磋商响应文件、澄清表(函); ②本合同及附件文本; ③国家相应的标准、规范。

3.3.4支付方式

采购包1:

分期付款

3.3.5支付约定

采购包1: 付款条件说明: 合同签订后, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包1: 付款条件说明: 本项目结束并经甲方验收合格后, 达到付款条件起 30 日内, 支付合同总金额的 60.00%。

3.3.6违约责任及解决争议的方法

采购包1:

1. 甲乙双方必须遵守本合同并执行合同中的各项规定, 保证本合同的正常履行。 2. 如因乙方工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害, 包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等, 乙方对此均应承担全部的赔偿责任。

3.4其他要求

3.4.1安全责任:乙方应对其工作人员在现场工作期间的一切行为负责, 如安全事故责任及因此发生的人身损害赔偿和其它费用由乙方承担。3.4.2保密条款:(1)成交供应商应严格遵守采购单位有关保密规定, 不得泄漏一切机密;(2)在技术服务期间, 成交供应商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。

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磋商文件的规定，对响应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。	响应函
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。	资格证明材料 响应函
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。	响应函

4.2 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
1	本采购包专门面向中小企业采购	参与的供应商（联合体）服务全部由符合政策要求的中小企业承接。	中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

4.3 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	营业执照等主体资格证明文件	提供有效合格的具有统一社会信用代码的营业执照，其他组织经营的须提供合法凭证，自然人提供身份证明文件	资格证明材料
2	财务状况报告	提供2023年度经审计的完整财务报告或磋商日期前三个月内其基本存款账户开户银行出具的资信证明。（如提供资信证明，须同时提供基本存款账户开户许可证或基本账户信息表）	资格证明材料
3	税收缴纳证明	提供2024年1月至今已缴纳的至少一个月的纳税证明，依法免税的单位应提供相关证明材料	资格证明材料

4	社会保障资金缴纳证明	提供2024年1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	资格证明材料
5	书面声明	具备履行合同所必须的设备和专业技术能力的书面声明	资格证明材料
6	无重大违法记录	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	资格证明材料
7	信用记录	供应商未被列入信用中国网站(www.creditchina.gov.cn)“失信被执行人、重大税收违法失信主体”；不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间	资格证明材料
8	授权委托书	法定代表人授权委托书、被授权人身份证（法定代表人参加磋商时,只需提供法定代表人身份证）,非法人单位参照执行	资格证明材料

第五章 磋商过程中可实质性变动的内容

磋商小组可以根据磋商文件和磋商情况实质性变动第三章“磋商项目技术、服务、商务及其他要求”、第八章“拟签订采购合同文本”，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

在磋商过程中，磋商小组根据项目实际需要制定磋商内容，在获得采购人代表确认的前提下，可以根据磋商情况实质性变动相关内容。磋商小组对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应及时通知所有参加磋商的供应商。

第六章 磋商办法

6.1 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》《政府采购竞争性磋商采购方式管理暂行办法》《陕西省政府采购评审专家管理实施办法》等法律法规，结合本采购项目特点制定本竞争性磋商评审方法。

二、评审工作由代理机构组织，具体评审事务由依法组建的磋商小组负责。

三、评审工作应遵循客观、公正、审慎的原则，并以相同的磋商程序 and 标准对待所有的供应商。

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。磋商小组成员、采购人、代理机构和供应商应当按照本磋商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审活动。

五、评审过程中的书面材料往来均通过项目电子化交易系统传递，评审委员会成员使用互认的证书及签章进行签名后生效，供应商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，评审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、评审过程应当独立、保密，任何单位和个人不得非法干预评审活动。供应商非法干预评审活动的，其响应文件将作无效处理；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审活动的，将依法追究其责任。

6.2 磋商小组

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。

一、磋商小组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、推荐磋商小组组长。采购人代表可以使用采购人代表专用签章确认评审意见。

二、磋商小组成员获取解密后的响应文件，开展评审活动。出现应当回避的情形时，磋商小组成员应当主动回避；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响应文件，按规定重新组建磋商小组，解封响应文件后，开展评审活动。

三、磋商小组按照磋商文件规定的磋商程序、评分方法和标准进行评审，并独立履行下列职责：

- （一）熟悉和理解磋商文件；
- （二）审查供应商响应文件等是否满足磋商文件要求，并作出评价；
- （三）根据需要要求采购组织单位对磋商文件作出解释；根据需要要求供应商对响应文件有关事项作出澄清、说明或者更正；
- （四）推荐成交候选供应商，或者受采购人委托确定成交供应商；
- （五）起草资格审查报告、评审报告并进行签署；
- （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。

6.3 评审程序

6.3.1 熟悉和理解磋商文件和停止评审

一、磋商小组正式评审前，应当对磋商文件进行熟悉和理解，内容主要包括磋商文件中供应商资格条件要求、采购项目技术、服务和商务要求、磋商办法和标准、政府采购政策要求以及政府采购合同主要条款等。

二、本磋商文件有下列情形之一的，磋商小组应当停止评审：

- （一）磋商文件的规定存在歧义、重大缺陷的；

- (二) 磋商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，但是磋商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，但是磋商文件未依法体现促进中小企业发展相关规定的；
- (五) 磋商文件将供应商的资格条件列为评分因素的；
- (六) 磋商文件载明的成交原则不合法的；
- (七) 磋商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审情形的，磋商小组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，磋商小组不得以任何方式和理由停止评审。

出现上述应当停止评审情形的，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。采购组织单位认为磋商小组不应当停止评审的，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。

6.3.2 符合性审查

一、磋商小组依据本磋商文件的实质性要求，对符合资格的响应文件进行审查，以确定其是否满足本磋商文件的实质性要求。本项目的符合性审查事项必须以本磋商文件的明确规定的实质性要求为依据。

二、在符合性审查过程中，如果出现磋商小组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磋商文件规定。

三、磋商小组对所有响应文件进行审查后，确定参加磋商的供应商名单。

符合性审查标准见下表：

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.在磋商过程中，磋商小组认为供应商的报价明显低于其他实质性响应的供应商报价，有可能影响产品质量或者不能诚信履约的，磋商小组应当要求其在评审现场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，逐项就供应商提供的货物、工程和服务的主营业务成本（应根据供应商企业类型予以区别）、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.供应商提交的相关证明材料，应当加盖供应商（法定名称）电子印章，在磋商小组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。供应商不能证明其报价合理性的，磋商小组应当将其响应文件作为无效处理。	标的清单 报价表

2	磋商响应文件完整性	磋商响应文件构成无重大缺项（详细评审除外），按照磋商文件要求的格式编写磋商响应文件	响应文件封面 分项报价表 中小企业声明函 残疾人福利性单位声明函 资格证明材料 标的清单 服务内容及服务要求应答表 报价表 商务要求应答表 陕西省政府采购投标人拒绝政府采购领域商业贿赂承诺书 响应函 监狱企业的证明文件
3	磋商响应文件报价	报价唯一，且没有高于采购预算的	分项报价表 标的清单 报价表
4	磋商响应文件有效性	磋商响应文件的签署、盖章符合磋商文件要求，供应商递交的磋商响应文件与本项目名称一致	响应文件封面 分项报价表 中小企业声明函 残疾人福利性单位声明函 资格证明材料 标的清单 报价表 响应函 监狱企业的证明文件
5	磋商有效期、授权有效期	文件递交截止之日起90日历日	响应文件封面 资格证明材料
6	服务期	服务期限响应磋商文件要求	标的清单
7	其他	无磋商文件中规定的无效情形	供应商认为需要补充的其他内容

6.3.3磋商

一、磋商小组按照磋商文件的规定与邀请参加磋商的供应商分别进行磋商，磋商顺序由磋商小组确定。

二、磋商小组所有成员集中与单一供应商对技术、服务、合同条款等内容分别进行一轮或多轮的磋商。在磋商中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

三、磋商小组可以根据磋商文件和磋商情况实质性变动第三章“磋商项目技术、服务、商务及其他要求”、第八章“拟签订采购合同文本”，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

四、对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应通过项目电子化交易系统，将变动情况同时通知所有参加磋商的供应商。磋商过程中，磋商小组可以根据磋商情况调整磋商轮次。

五、磋商过程中，磋商文件变动的，供应商应当按照磋商文件的变动情况和磋商小组的要求就磋商文件变动部分，以“供应商响应表”形式在线提交磋商小组。“供应商响应表”作为响应文件的组成部分，响应文件应加盖供应商（法定名称）电子印章，否则无效。

六、经最终磋商后，响应文件仍有下列情况之一的，应按照无效响应处理：

- （一）响应文件仍不能实质响应磋商文件可实质性变动的实质性要求的；
- （二）响应文件中仍有磋商文件规定的其他无效响应情形的。

七、磋商小组对供应商在磋商、评审过程中的书面交换材料，未按要求加盖电子印章或签字的，视同未提交书面交换材料。

八、磋商小组在最终磋商后，对所有响应文件的有效性、完整性和响应程度进行审查后，确定最后报价的供应商名单。

九、磋商过程中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

十、磋商过程中，磋商小组发现或者知晓供应商存在违法行为的，应当磋商报告中予以记录，并向本级财政部门报告，依法将该供应商响应文件作无效处理的，应当作无效处理。

6.3.4最后报价

一、方案评审

采购包1：磋商/谈判/协商文件能够详细列明采购标的的技术、服务要求，磋商/谈判/协商结束后，磋商/谈判/协商小组可以根据磋商/谈判/协商情况要求所有实质性响应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。

二、磋商小组开启报价后，供应商应随时关注项目电子化交易系统信息提醒，登录项目电子化交易系统，通过“等候大厅”进行报价并签章后提交。

三、供应商在未提高响应文件中承诺的标准情况下，其最后报价不得高于对该项目之前的报价，否则，磋商小组将对其响应文件作无效处理，并通过电子化交易系统告知供应商，说明理由。

四、供应商最后报价属于明显低价不正当竞争的，磋商小组应按照“供应商须知前附表”第8项规定处理。

五、供应商未在响应文件提交截止时间内提交报价或未按要求进行报价的，视为无效响应，由供应商自行承担不利后果。

六、供应商未按磋商小组要求在规定时间内提交最后报价的，视为其退出磋商。

七、最后报价一旦提交后，供应商不得以任何理由撤回。

八、最后报价为有效报价应符合下列条件：

- （一）供应商所提供的最后报价是在规定的时间内提交。
- （二）供应商的最后报价应加盖供应商（法定名称）电子印章。
- （三）供应商的最后报价应符合磋商文件的要求。
- （四）最后报价唯一，且不高于最高限价。

九、最后报价出现下列情况的，不需要供应商澄清，按以下原则处理：

- （一）报价中的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；
- （二）单价金额小数点或者百分比有明显错位的，应以总价为准，并修改单价；
- （三）总价金额与按单价汇总金额不一致的，以单价汇总金额计算结果为准；

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的最后报价经加盖供应商（法定名称）电子印章后产生约束力，供应商不确认的，其最后报价无效。

6.3.5解释、澄清有关问题

一、评审过程中，磋商小组认为磋商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磋商文件的原义或者影响公平、公正，解释事项如果涉及供应商权益的以有利于供应商的原则进行解释。

二、对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，磋商小组应当要求供应商作出必要的澄清、说明或者更正，并给予供应商必要的反馈时间。供应商应当按磋商小组的要求进行澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。澄清不影响响应文件的效力，有效的澄清、说明或者更正材料是响应文件的组成部分。

三、供应商的澄清、说明或者更正需进行电子签章，应当不超出响应文件的范围、不实质性改变响应文件的内容、不影响供应商的公平竞争、不导致响应文件从不响应磋商文件变为响应磋商文件的条件。下列内容不得澄清：

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

四、响应文件报价出现前后不一致的情形，按照本章前述规定予以处理，不需要供应商澄清。

五、代理机构宣布评审结束之前，供应商应通过项目电子化交易系统随时关注评审消息提示，及时响应磋商小组发出的澄

清、说明或更正要求。供应商未能及时响应的，自行承担不利后果。

六、磋商小组应当积极履行澄清、说明或者更正的职责，不得滥用权力。

6.3.6比较与评价

磋商小组应当按照磋商文件规定的评标细则及标准，对符合性检查合格的响应文件进行商务和技术评估，综合比较和评价。

6.3.7复核

评审结束后，磋商小组应当进行复核，特别要对拟推荐为成交候选供应商的、报价最低的、响应文件被认定为无效的的重点复核。

评审结果汇总完成后，磋商小组拟出具磋商报告前，代理机构应当组织2名以上的工作人员，在采购现场监督人员的监督之下，依据有关的法律制度和磋商文件对评审结果进行复核，出具复核报告。代理机构复核过程中，磋商小组成员不得离开评审现场。

除资格检查认定错误、分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致、经磋商小组一致认定评分畸高、畸低的情形外，采购人或者代理机构不得以任何理由组织重新评审。采购人、代理机构发现磋商小组未按照磋商文件规定的评审标准进行评审的，应当重新开展采购活动，并同时书面报告本级财政部门。

6.3.8推荐成交候选供应商

磋商小组应当根据综合评分情况，按照评审得分由高到低顺序推荐如下成交候选供应商，并编写磋商报告。

采购包1： 3家； 评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术方案评审优劣顺序推荐。评审得分且最后报价且技术方案得分均相同的，由采购人采取随机抽取的方式确定成交供应商。

6.3.9编写磋商报告

磋商小组推荐成交候选供应商后，应向代理机构出具磋商报告。磋商报告应当包括以下主要内容：

- （一）邀请供应商参加采购活动的具体方式和相关情况；
- （二）响应文件开启日期和地点；
- （三）获取磋商文件的供应商名单和磋商小组成员名单；
- （四）评审情况记录和说明，包括对供应商响应文件审查情况、磋商情况、报价情况等；
- （五）提出的成交候选供应商的排序名单及理由。

磋商报告应当由磋商小组全体人员签字或加盖电子签章认可。磋商小组成员对磋商报告有异议的，磋商小组按照少数服从多数的原则推荐成交候选供应商，采购程序继续进行。对磋商报告有异议的磋商小组成员，应当在报告上签署不同意见并说明理由，由磋商小组记录相关情况。磋商小组成员拒绝在磋商报告上签字或加盖电子签章又不书面说明其不同意见和理由的，视为同意磋商报告。

6.3.10评审争议处理规则

在磋商过程中，对于符合性审查、对响应文件作无效响应处理的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，但不得违背磋商文件规定。持不同意见的磋商小组成员应当在磋商报告中签署不同意见及理由，否则视为同意评审报告。持不同意见的磋商小组成员认为认定过程和结果不符合法律法规或者磋商文件规定的，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。

6.4评审办法及标准

一、磋商小组只对通过资格审查的响应文件，根据磋商文件的要求采用相同的评审程序、评分办法及标准进行评价和比较。

二、磋商小组成员应依据磋商文件规定的评分标准和方法独立对每个有效响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。

6.4.1评分办法

本次评审采用综合评分法，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

6.4.2 评分标准

采购包1:

评审因素		评审标准			
分值构成		详细评审85.0000分 报价得分15.0000分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式
	技术方案	结合本次项目特点提出技术方案，方案内容包括但不①总体架构②项目实施③测试计划等。以上3项方案内容描述详细、条理清晰、符合本项目采购需求，每项得4分；以上分项每缺少一项内容扣4分；有某一项不完整或不符合实际要求或不满足实施要求或套用其他项目内容的每项得0.1-3.5分；未提供不得分。	12.0000	主观	技术部分
	技术参数响应	根据网络安全设备产品技术参数、性能、功能的满足程度赋分：产品优于或完全符合、响应磋商文件要求，没有负偏离计25分；※项号参数（5项）为重要技术指标，每负偏离一项扣1分；▲项参数（100项）每负偏离一项扣0.2分，扣完为止。需提供相关证明材料进行佐证，否则视为负偏离。	25.0000	客观	服务内容及服务要求 应答表 技术部分

详细评审	进度保障、重难点分析及解决、应急预案	结合项目采购需求，提供以下方案： 1、提供具体的服务进度保障措施，接到采购人任务后，反应迅速，时间安排合理。 2、针对本项目实际情况及采购人要求，提出重难点分析与解决方案。 3、针对本项目提出突发事件的应急预案。 评审标准：（1）以上3项方案描述详细，条理清晰，切实可行，满足评审标准每项得4分；（2）基本满足评审标准的，每项得2分；（3）不能满足评审要求得，每项得1分；未提供的，该项不得分。	12.0000	主观	技术部分
	网络运维方案	1、提供大厅整体网络的规划、梳理和管理的详细运维方案。方案科学，可操作性强得3分；方案基本合理得1分。未提供方案不得分。 2、提供服务器和监控的详细运维方案。方案科学，可操作性强得3分；方案基本合理得1分。未提供方案不得分。	6.0000	主观	技术部分
	网络安全运维	1、提供网络安全运维方案，梳理标准化、层次化、一体化的管控体系方案。方案科学，可操作性强得3分；方案基本合理得1分。未提供方案不得分。 2、提供网络安全管理规范建设服务，建立并梳理网络安全工作制度、巡检表单、制度建设等，构建完整的网络安全管理体系，提供相关运维材料。方案科学，可操作性强，资料齐全得2分；方案基本合理得1分。未提供方案不得分。 3、提供网络安全培训方案，方案内容齐全、简单易懂，服务目标明确，培训次数达标，架构完整、层次清楚，完全满足项目整体要求。方案科学，可操作性强，资料齐全得2分；方案基本合理得1分。未提供方案不得分。	7.0000	主观	技术部分

	质量保证措施	针对本项目制定详细的质量保证措施，措施内容包含①质量控制制度②质量控制标准③质量控制程序④与采购人配合方案及响应情况保障措施⑤设备保障措施。保证措施内容全面详细、阐述条理清晰详尽、符合本项目采购需求得5分；以上分项每缺少一项内容扣1分；有某一项不完整或不符合实际要求或不满足实施要求或套用其他项目内容的每项得0.1-0.5分；未提供不得分。	5.0000	主观	技术部分
	售后服务	供应商提供对本项目的售后服务方案，方案内容包含但不限于①售后时间及响应时间②管理制度③服务流程④维保能力。以上4项方案描述详细，条理清晰，切实可行，满足采购需求，每项得2分；某一项不完整或不符合实际要求或不满足实施要求或套用其他项目内容的每项得0.1-1.5分 以上分项每缺少一项内容扣2分	8.0000	主观	技术部分
	业绩	近三年(2021年1月1日至今)类似项目业绩，每份业绩得1分，最高10分。（以合同签订日期为准） 评审依据：提供合同复印件并加盖公章。	10.0000	客观	供应商业绩情况
价格分	价格分	价格分统一采用低价优先法计算，即满足磋商文件要求且磋商价格最低的最终磋商报价为磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：磋商报价得分=(磋商基准价 / 最终磋商报价)×价格权值×100计算分数时四舍五入取小数点后两位	15.0000	客观	报价表 标的清单 分项报价表 中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

价格扣除

序号	情形	适用对象	比例	说明	关联格式
无					

6.5 终止采购活动

出现下列情形之一的，采购人或者代理机构应当终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

- （一）因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；
- （二）出现影响采购公正的违法、违规行为的；
- （三）除《政府采购竞争性磋商采购方式管理暂行办法》第二十一条第三款规定的情形外，在采购过程中符合要求的供应商或者报价未超过采购预算的供应商不足3家的（财政部另有规定的除外）；
- （四）法律法规规定的其他情形。

6.6 确定成交供应商

- 一、评审结束后，代理机构在评审结束之日起2个工作日内将磋商报告及有关资料送交采购人。
- 二、采购人在收到磋商报告后5个工作日内，在磋商报告确定的成交候选供应商名单中按顺序确定成交供应商。成交候选供应商并列的，由采购人采取随机抽取的方式确定成交供应商。
- 三、采购人逾期未确定成交供应商且不提出异议的，视为确定磋商报告提出的排序第一的供应商为成交供应商。
- 四、根据采购人确定的成交供应商，代理机构在陕西省政府采购网上发布成交结果公告，同时向成交供应商发出成交通知书。

6.7 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。

6.8 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）评审前，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）评审过程中，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）评审过程中，不得干预或者影响正常评审工作，不得发表倾向性、引导性意见，不得修改或细化磋商文件确定的评审程序、评审方法、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审意见，不得拒绝对自己的评审意见签字确认。
- （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。

第七章 响应文件格式

采购包1:

分册名称: 投标响应文件分册

详见附件: 响应文件封面

详见附件: 响应函

详见附件: 报价表

详见附件: 标的清单

详见附件: 分项报价表

详见附件: 资格证明材料

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: 服务内容及服务要求应答表

详见附件: 商务要求应答表

详见附件: 技术部分

详见附件: 供应商业绩情况

详见附件: 供应商认为需要补充的其他内容

详见附件: 陕西省政府采购投标人拒绝政府采购领域商业贿赂承诺书

第八章 拟签订采购合同文本

详见附件：合同条款.docx

