西安市高陵区医院网络安全等级保护建设项目

项目编号：DXZB-2022-0631

公 开 招 标 文 件

采购单位：西安市高陵区医院

代理机构：陕西德信招标有限公司

2022 年 6 月

目　录

第一部分 招标公告

西安市高陵区医院网络安全等级保护建设项目

招标公告

陕西德信招标有限公司受西安市高陵区医院的委托，经政府采购管理部门批准，按照政府采购程序，对西安市高陵区医院网络安全等级保护建设项目进行公开招标采购，欢迎符合资格条件的、有能力提供本项目所需货物和服务的供应商参加投标。

一、采购项目名称：西安市高陵区医院网络安全等级保护建设项目

二、采购项目编号：DXZB-2022-0631

三、采购人名称：西安市高陵区医院

地址：陕西省西安市高陵区上林二路 555

联系人：李先生

联系方式：029-86918870

四、采购代理机构名称：陕西德信招标有限公司

地址：陕西省西安市雁塔区南二环东段凯森盛世一号 A 座 5 层

联系人：赵恬钰

联系方式：029-82694900-9025

五、采购内容和要求：（共 1 包、具体技术参数详见招标文件）

采购内容：网络安全等级保护建设

项目预算：130 万元

项目用途：自用

项目性质：财政资金

六、投标人资格要求：

符合《中华人民共和国政府采购法》第二十二条之规定，有能力提供本次采购货物和服务，同时符合下列条件的供应商：

1、具有独立承担民事责任能力的法人或非法人组织或自然人，提供合法有效的统一社会信用代码的营业执照等证明文件；

2、提供法定代表人授权委托书及被授权人身份证（投标人为法定代表人时，须提交法定代表人证明书）；

3、提供 2021 年审计报告（至少应包含资产负债表、利润表和现金流量表）或投标截止日前半年内任意一个月的的财务报表（至少应包含资产负债表、利润表和现金流量表）或银行出具的资信证明；（成立时间至提交响应文件截止时间不足三个月的可不提供）；

4、提供投标截止日前半年内任意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，成立不足一年的公司提供自成立后至今连续缴存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，单据或证明上应有社保机构或代收机构的公章或业务专用章；（成立时间至提交响应文件截止时间不足三个月的可不提供）；

5、提供投标截止日前半年内任意一个月的纳税证明或完税证明，单据应有代收机构或税务机关的公章或业务专用章；依法免税的单位应提供相关证明材料；（成立时间至提交响应文件截止时间不足三个月的可不提供）；

6、具有履行合同所必需的设备和专业技术能力的书面声明；

7、提供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书面声明；

8、未被列入失信被执行人、税收违法黑名单、政府采购严重违法失信行为记录名单；以“信用中国”网站(www.creditchina.gov.cn)或中国政府采购网(www.ccgp.gov.cn) 查询结果为准；

9、本项目不接受联合体投标。

七、招标文件发售

1、文件售价：免费赠送。

2、缴纳地点：陕西省西安市雁塔区南二环东段凯森盛世一号 A 座五楼

3、缴纳时间：2022 年 06 月 22 日至 2022 年 06 月 28 日每天上午 9:00-12:00，下午 14：00-17：00（双休日及法定节假日除外）

4、报名须知：

供应商须在招标文件发售时间内携带介绍信和经办人身份证复印件(加盖公章）一套在陕西德信招标有限公司（陕西省西安市雁塔区南二环东段凯森盛世一号 A 座五楼）政府采购部进行确认。

备注：请各投标人购买招标文件后，按照陕西省财政厅《关于政府采购供应商注册登记有关事项的通知》要求，通过陕西省政府采购网注册登记加入陕西省政府采购供应商库。

八、投标文件递交截止时间及开标时间和地点：

投标文件递交截止时间：2022 年 07 月 12 日 14 点整

开标时间：2022 年 07 月 12 日 14 点整

投标地点：陕西德信招标有限公司开标室

九、采购项目需要落实的政府采购政策：

依据《中华人民共和国政府采购法》和《中华人民共和国政府采购法实施条例》的有关规定，落实政府采购政策，详见招标文件。

1、《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）、财政部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）；

2、《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号）；

3、《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）；

4、《财政部 国家发展改革委关于印发〈节能产品政府采购实施意见〉的通知》（财库〔2004〕185 号）；

5、《环境标志产品政府采购实施的意见》（财库〔2006〕90 号）；

6、《三部门联合发布关于促进残疾人就业政府采购政策的通知》(财库〔2017〕141 号）；

7、《关于运用政府采购政策支持乡村产业振兴的通知》（财库〔2021〕19 号）；

8、《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51 号）；

9、陕西省财政厅关于印发《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23 号）。

十、其他应说明的事项：

采购代理机构：陕西德信招标有限公司

联系人：赵恬钰

联系方式（电话/传真）：029-82694900 转 9025

陕西德信招标有限公司

2022 年 06 月 21 日

第二部分 投标人须知及前附表

一、投标人须知前附表

本表关于招标服务的具体要求是对投标人须知的具体补充和修改，如有矛盾，应以本表为准。

序号	内　　容
1	**买方名称：西安市高陵区医院** **地　址：陕西省西安市高陵区上林二路 555 号** **联系人：李先生** **联系电话：029-86918870**
2	**招标代理机构：陕西德信招标有限公司** **地　址：陕西省西安市雁塔区二环南路东段凯森盛世一号 A 座 5 层** **联系人：赵恬钰** **联系电话：029-82694900 转 9025**
3	**采购内容：网络安全等级保护建设** **采购预算：130 万元**
4	**该项目专门面向中小企业采购。**
5	投标有效期：90 天
6	投标语言：　中文
7	投标报价：人民币报价，最终目的地价。
8	评标方法：综合评分法，不保证最低价成交。
9	中标服务费账户： 开户名称：陕西德信招标有限公司 开户银行：西安银行东二环南段支行 账　号：209011580000073440
10	投标截止时间：2022 年 07 月 12 日 14 点整(北京时间)。 投标文件递交地点：陕西德信招标有限公司开标室。
11	开标时间：2022 年 07 月 12 日 14 点整(北京时间)。 开标地点：陕西德信招标有限公司开标室。
12	**投标文件的提交：** **正本一份，副本四份，电子版 Word 及加盖公章 PDF 文档各一份（U 盘）、报价表一份。**

13	**技术偏离表不得完全复制粘贴招标文件技术参数要求，否则视为无效投标。** **技术偏离表响应内容须提供相关技术支持资料。**
14	**落实的政府采购政策：** **1、对小型或微型企业参加政府采购投标的扶持：** 根据《政府采购促进中小企业发展管理办法》（财库[2020]46号）的规定，对于非专门面向中小企业的项目，对小型和微型企业产品的价格给予10%的扣除，用扣除后的价格参与评审；供应商可在投标文件中提供小型和微型企业声明； **2、对监狱企业、残疾人福利企业的扶持：** 根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）（提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件）、《三部门联合发布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，对监狱企业、残疾人福利企业给予10%的价格扣除，用扣除后的价格参与评审； **对同时属于小微企业、监狱企业或残疾人福利性单位，不重复享受政策。** **3、对节能、环保政策的支持** （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）和财政部、发展改革委发布的《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19号）的规定，若投标货物属于“节能产品政府采购清单”中品目的产品，供应商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，对获得证书的产品实施政府优先采购或强制采购。 （2）、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），及 财政部、生态环境部关于印发环境标志产品政府采购品目清单的通知》财库〔2019〕18号的规定，若投标货物属于“环境标志产品政府采购清单”中品目的产品，供应商提供国家确定的认证机构出具的、处于有效期之内的环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。 （3）、产品同时属于“非强制采购节能产品”、环境标志产品的，评审时只有其中一项能享受优先待遇（供应商自行选择，并在报价文件中填写相关信息及数据）。

15	**强制认证产品说明：** 所投产品属于国家强制认证产品的应获得强制认证且证书在有效期内，否则不得投标。不论查验与否，提供本应获得而未获得 CCC 认证产品的投标和中标（成交）将被取消。
16	为支持和促进中小企业发展，进一步发挥政府采购政策功能作用，有效缓解中小企业融资难等问题，根据财政部财库〔2011〕124 号文件的精神，陕西省财政厅制订了《陕西省政府采购信用担保试点工作实施方案（试行）》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，为参与陕西省政府采购项目的供应商提供政府采购信用担保，并按照程序确定了合作的担保机构。中标（成交）供应商如果需要融资贷款服务的，可凭中标（成交）通知书、政府采购合同等相关资料，按照文件规定的程序申请办理，具体规定可登陆陕西省政府采购网(www.ccgp-shaanxi.gov.cn/)重要通知专栏中查询了解。
17	**供应商注册登记提醒：** 根据“陕西省财政厅关于政府采购供应商注册登记有关事项的通知”，如所投本项目的供应商未在陕西省政府采购网（http：//www.ccgp-shaanxi.gov.cn/）注册登记加入陕西省政府采购供应商库的，应按要求及时办理注册登记，并接受财政部门监督管理。
18	**供应商信用信息查询说明：** 采购人、采购代理机构在供应商递交投标文件或响应文件时，在“信用中国”网站(www.creditchina.gov.cn)或中国政府采购网(www.ccgp.gov.cn)， 查询供应商信用是否合格并记录，将查询网页、内容截图或拍照，留档保存。此查询信息仅作为本项目使用。
19	**供应商如放弃本项目投标，应在递交投标（响应）文件截止时间前一日以电子邮件形式发送至 zhaotianyu989@foxmail.com 告知采购代理机构，否则采购代理机构可向财政部门反映情况并提供相应佐证。供应商一年内累计出现三次该情形，将被监管部门记录为失信行为。**
20	依据《政府采购货物和服务招标投标管理办法》（财政部令第 87 号）第四十三条，招标过程中经评审实质性响应招标文件要求的供应商只有 2 家时，经采购人书面请示政府采购管理机构同意后，现场转变采购方式为竞争性谈判，评审办法按照《政府采购非招标采购方式管理办法》（财政部令第 74 号）规定执行。

二、投 标 人 须 知

1、 适用范围

本招标文件仅适用于本次公开招标采购项目。

2、名词解释

2.1、采购人：西安市高陵区医院

2.2、采购代理机构：陕西德信招标有限公司

2.3、监督管理机构：西安市高陵区财政局

2.4、投标人：是指响应招标、参加投标竞争的法人、非法人组织或者自然人。

2.5、投标人代表：是指参加投标竞争中代表投标人的法定代表人或者是其被授权人，投标人代表是唯一的。

3、特殊情形

3.1、特殊情形：指具有独立承担民事责任能力的非法人组织或自然人。

3.2、特殊情形规定

3.2.1、非法人组织：

①、事业单位参加投标的，应参照本招标文件给出的投标文件格式制作，其中投标文件要求法人签字处可以是事业单位的法人签章；

②、分公司参加投标的（须提供总公司出具的法人授权），应参照本招标文件给出的投标文件格式制作，其中投标文件要求法人签字处可以是分公司的负责人签字；

③、个体户参加投标的，应参照本招标文件给出的投标文件格式制作，其中投标文件要求法人签字处可以是其经营者本人签字；

3.2.2、自然人：自然人投标的，应参照本招标文件给出的投标文件格式制作，其中投标文件要求盖公章处可以是自然人本人的手印；不接受自然人授权他人参加投标。

4、招标文件

4.1 招标文件的组成

（1）招标公告

（2）投标人须知及前附表

（3）商务部分（合同条款及合同格式）

（4）用户需求书（采购内容及要求）

（5）评标办法

（6）投标文件格式

4.2 招标文件质疑与投诉

4.2.1 投标人对本次招标采购活动有疑问的，按照国家《中华人民共和国政府采购法》及中华人民共和国财政部令第 94 号《政府采购质疑和投诉办法》的规定办理。

4.2.2 供应商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。

4.2.3 递交质疑函有关说明

4.2.3.1 接收方式：书面形式

4.2.3.2 联系部门：政府采购部

4.2.3.3 联系电话：029-82694900

4.2.3.4 通讯地址：陕西省西安市雁塔区南二环东段凯森盛世一号 A 座 5 层

4.3 招标文件的澄清

投标人若对招标文件有疑问，应将要求澄清的问题以书面形式通知招标机构。

4.4 招标文件的补充和修改

4.4.1 招标机构可以用书面补充通知的方式对招标文件进行补充和修改。

4.4.2 所颁发的补充通知将于投标截止时间前发往所有购买招标文件的投标人。该补充通知作为招标文件的一部分。投标人在收到该通知后须予以签收确认。

4.4.3 考虑到补充通知的影响，委托人和招标机构可决定推迟投标截止时间。

5、投标和招标总则

5.1 投标文件的编写

5.1.1 投标人应仔细阅读招标文件的所有内容，并按照招标文件的“投标文件格式”规定及要求的内容和格式，提交完整的投标文件。

5.1.2 投标语言和计量单位

投标文件和来往函件用中文书写（外文函件必须翻译为中文），计量单位应使用中华人民共和国法定计量单位。（除非招标文件中另有规定）。

5.1.3 投标人应按招标文件规定的投标范围进行投标。

5.1.4 投标人应用**人民币投标**。若由单价计算出的总价与投标总价不一致，以单

价计算出的总价作为投标总价。若中文文字形式表示的数值与数字形式表示的数值不一致，以中文文字形式表示的数值为准。

5.1.5 采购进口产品时，按照财库〔2007〕119号《政府采购进口产品管理办法》的相关规定实施。

5.2 投标文件的组成

5.2.1 投标人提交的投标文件至少应包括以下部分：

(1) 投标函；

(2) 投标报价表；

(3) 投标报价明细表；

(4) 商务条款偏离表；

(5) 技术规格偏离表；

(6) 法定代表人证明书或授权书；

(7) 资格证明文件；

(8) 具有履行合同所必需的设备和专业技术能力的书面声明；

(9) 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书面声明；

(10) 陕西省政府采购供应商拒绝政府采购领域商业贿赂承诺书；

(11) 项目业绩表；

(12) 优惠、培训、售后服务承诺；

(13) 其他证明材料；

缺以上任一项的投标将被视为无效投标。

5.2.2 投标人可在满足“用户需求书（采购内容及要求）”中对设备的整体要求的前提下，对设备中的软硬件配置提出合理化建议。

5.3 投标

5.3.1 投标人投标时间提交的全部材料必须密封，具体包括：

（1）投标文件一式5份（正本1份，副本4份）；

（2）投标文件电子版U盘一份（投标文件电子版提供Word及PDF版本各一份，将其作为投标文件的一部分，不予退还）；

（3）开标信封（内放开标一览表和投标文件电子版U盘）。

投标文件正本、副本的内容应当一致，如果正本与副本不符，以正本为准。

投标文件应由投标人的法定代表人或经正式授权并对投标人有约束力的代表在投标文件上签字。被授权代表需将以书面形式出具的“法人授权书”附在投标文件中。

任何行间插字、涂改和增删，必须由投标文件签字人在旁边签字才有效。

5.3.2 每本投标文件的内容应装订成册。

5.3.3 投标人应对投标服务提供完整的详细的技术说明，如果投标人对指定的技术要求建议做任何改动，应在投标文件中清楚的说明。投标人投标的内容与招标文件的技术、商务要求有偏离时，无论这种偏离是否有利于买方，投标人都应该按照附件的格式如实填写技术偏离表和商务条款偏离表。商务条款不可负偏离，否则视为无效投标。

5.3.4 投标人应按照要求提交资格文件，并对这些资格文件的真实性负责。

5.3.5 所有投标文件必须装入密封的信封或封套，并在每一信封或包装的封面上写明：

正本或副本；

项目名称；

项目编号；

开标时间；

投标人名称；

5.3.6 招标机构对因投标文件未装订成册而造成的投标文件的损坏、丢失不承担任何责任。

5.3.7 招标机构对不可抗力的事件造成的投标文件的损坏、丢失不承担任何责任。

5.4 投标的有效期

5.4.1 从投标截止日期起，投标有效期为 90 天。在特殊情况下，招标机构可于投标有效期满之前要求投标人同意延长有效期，要求与答复均以书面形式。

5.5 投标保证金

5.5.1 本次招标项目应提交投标保证金为**人民币 0 元整**。

5.5.2 合同备案

在结果公告公示后，请中标单位在合同签订后请将合同复印件一份送至代

理机构或将扫描件发至采购代理机构邮箱：zhaotianyu989@foxmail.com，以便及时归档）。

5.6　投标文件的修改：

在规定的时间内，投标人可以修改其投标文件的内容，但必须以书面形式通知招标机构。在招标规定的修改截止时间后，投标人不可以修改其投标文件的内容。

5.7　投标的撤回

在投标截止时间前投标人可以撤回其投标，但在投标截止后不允许撤回投标。

5.8　招标过程及评审

5.8.1 招标机构将在招标公告中规定的时间和地点接受投标。

5.8.2 评标委员会只对确定为实质上响应招标文件要求的投标进行评审。

5.8.3 实质上没有响应招标文件要求的投标文件将视为无效投标。出现但不限于下列情况之一的，其投标将视为无效投标：

（1）投标人未按招标文件要求的金额提交投标保证金的；

（2）投标文件不完整的；

（3）投标文件无法人代表签字或签字人未被法人授权的；

（4）投标有效期不足的；

（5）投标文件附有招标方不能接受条件的；

（6）投标总价超出项目预算或明显高于市场价格的；

（7）按招标文件要求其他不符合招标方要求的。

5.8.4 评标委员会将按已定的原则及方法进行评审，详见评标办法。

5.8.5 评标委员会在确定中标候选人以前有权按照有关法规拒绝任何或全部投标，对此造成对投标人的影响不负任何责任，不做任何解释。

5.8.6 确定中标人后，由招标机构发出中标通知书，中标人应 30 日内与采购人签约。

5.8.7 招标机构没有义务向未中标的投标人解释不中标的理由。

5.9　招标、评标过程的保密性。

5.9.1 接受投标后，直至中标商与买方签订合同后止，凡与招标、审查、澄清、评价、比较、授标意见有关的内容，任何人均不得向投标人及与评审无关的其

他人透露。

5.9.2 从投标截止日起到确定中标人止，投标人不得与参加招标、评审的有关人员私下接触。在评审过程中，如果投标人试图在投标文件审查、澄清、比较及推荐中标人方面对参与评审的有关人员和买方施加任何影响，其投标将被拒绝。

5.9.3 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本项目，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按照招标文件规定的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。

5.10 若投标人须知前附表中写明专门面向中小企业采购的，提供的货物全部由符合政策要求的中小企业制造；工程的施工单位全部为符合政策要求的中小企业承接（或者：服务全部由符合政策要求的中小企业承接）。否则其投标将被认定为投标无效。

6、签约及中标服务费

6.1 中标人须向招标机构缴纳足额中标服务费并领取中标通知书。

6.2 中标人应持中标通知书，在 30 日内与采购人签定合同。

6.3 中标人须向招标机构按如下标准和规定交纳中标服务费：

（1）中标服务费币种与中标通知书中标价的币种相同；

（2）中标服务费不列在投标报价表中；

（3）招标代理服务费参照国家计委关于印发《招标代理服务收费管理暂行办法》的通知（计价格〔2002〕1980 号）、《国家发展和改革委员会办公厅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）规定向中标（成交）供应商收取。

第三部分 商务部分（合同条款及合同格式）

（说明：本合同作为合同的基本格式，不作为最终合同，甲方有权在签订合同时对合同的相关条款及内容作进一步的细化和修改。）

商务部分

一、合同专用条款

本表关于招标服务的具体要求是对本合同条款的具体补充和修改，如有矛盾，应以本条款为准。

序 号	内　　容
1.	买方（采购人）名称：西安市高陵区医院
2.	卖方（中标人）名称：
3.	付款方式和条件：签订合同后货到验收合格后支付合同总金额的 50%，项安装调试合格后支付合同总金额的 45%，质保二年后支付合同总金额的 5%
4.	交付期：40 个日历日
5.	交货地点：西安市高陵区医院指定地点。
6.	应提供的伴随服务：选所有。
注：以上要求不可负偏离，否则视为无效投标。	

二、合同通用条款

1.定义

本合同下列术语应解释为：

1.1“合同”系指买卖双方签署的、合同格式中载明的买卖双方所达成的协议,包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

1.2“合同价”系指根据本合同规定，卖方在正确地完全履行合同义务后买方应支付给卖方的价格。

1.3“服务”系指根据合同规定，卖方提供的服务。

1.4“合同条款”系指本合同条款。

1.5“买方”系指在合同专用条款中指明的购买服务的单位。

1.6“卖方”系指签署本合同，提供本合同项下服务的单位。

1.7“服务地点”系指本合同(包括附件)指明的提供服务的地点。

1.8“天”指日历天数。

2.服务要求

2.1卖方提供服务应与本合同所指明的服务(包括合同附件)相一致。

2.2见合同专用条款。

3.专利权

卖方应保证买方在使用该服务或其任何一部分时免受第三方提出侵犯其专利权·商标权、工业设计权或其他知识产权的起诉。

4.服务地点和服务期限

见合同专用条款。

5.保险

卖方应为所提供服务的人员等购买保险。

6.付款

6.1本合同以人民币付款。

6.2卖方应按照双方签订的合同规定提供服务,服务成果由买方验收合格并出具验收书后，连同合同一并送政府采购管理部门办理结算。

6.3见合同专用条款。

7.质量保证及索赔

7.1 卖方应保证所供服务完全符合合同规定的要求。

7.2 在服务期限内，如果服务与合同有任何一项不符，买方应尽快以书面形式向卖方提出索赔。同时应向政府采购管理部门报告。

7.3 卖方在收到买方的通知后，应及时纠正。具体响应时限见专用合同条款。

7.4 如果卖方在收到通知后，没有在上述专用合同条款中规定的时限内及时纠正和弥补，买方可采取必要的补救措施，但其风险和费用将由卖方承担，买方根据合同规定对卖方行使的其它权力不受影响。买方亦可从合同款和卖方履约保证金中扣回索赔金额。

8. 检验和验收

8.1 服务成果，由采购单位根据合同规定的标准要求进行验收，并出具验收书。验收书应当包括履约情况。

9. 卖方履约延误

9.1 如卖方事先未征得买方同意并得到买方的谅解而单方面延迟提供服务的情况，将按违约终止合同。

9.2 在履行合同过程中，如果卖方遇到可能妨碍按时提供服务的情况，应及时以书面形式将拖延的事实，可能拖延的期限和理由通知买方。买方在收到卖方通知后，应尽快对情况进行评价，并确定是否通过修改合同，酌情延长服务期限或对卖方加收误期赔偿金。误期赔偿金以每周 0.5%计。

10. 违约终止合同

在卖方违约的情况下，买方报告政府采购管理部门后，有权终止合同，并依法向卖方进行索赔。

11. 适用法律

本合同应按照中华人民共和国的现行法律进行解释。

12. 合同生效及其它

12.1 本合同经买卖双方及招标单位授权代表签字盖章后生效。

12.2 如需修改合同内容，双方应签署书面修改或补充协议，该修改协议作为本合同的一个组成部分。

12.3 根据项目需求甲乙双方须按照《关键信息基础设施安全保护条例》的有关规定签订安全保密协议并作为合同附件。

12.4 本合同具有法律效力，受国家法律保护。

12.5 本合同一式伍份，买方(使用单位)贰份，卖方贰份，招标代理机构壹份。

三、合同格式（参考）

本合同与_____ 年_____ 月_____日由_____（以下简称“买方”）为一方和（卖方名称）（以下简称“卖方”）为另一方按下述条款和条件签署。

鉴于买方为获得以下服务(包括服务和伴随货物),即_____的公开招标，并接受了卖方以总金额_____（人民币、用文字和数字表示的合同价）（以下简称“合同价”）提供上述服务的投标。

本合同在此声明如下：

1. 本合同中的词语和术语的含义与合同条款中定义的相同。

2. 下述合同附件为本合同不可分割的部分并与本合同具有同等效力：

（1）服务范围及分项价格表

（2）招标文件、招标文件澄清文件

（3）投标文件、投标人在评标期间的承诺文件

（4）中标通知书

3. 考虑到买方将按照本合同规定向卖方支付款项，卖方再次保证全部按照合同的规定向买方提供服务并在质量保证期内承担质量保证责任。

4. 考虑到卖方提供的服务、货物并修补缺陷，买方在此保证按照合同规定的时间和方式向卖方支付合同价或其它按合同规定支付的金额。

双方在上述日期签署本协议。

（此页无正文）

买方名称：_____ 卖方名称：_____

买方代表姓名：_____ 卖方代表姓名：_____

买方代表签字：_____ 卖方代表签字：_____

地　　址：_____ 地　　址：_____

买方公章：_____ 卖方公章：_____

电　　话：_____ 电　　话：_____

传　　真：_____ 传　　真：_____

开户银行：_____ 开户银行：_____

账　　号：_____ 账　　号：_____

招标单位：**陕西德信招标有限公司**

地　　址：_____

电　　话：_____

邮　　编：_____

第四部分 用户需求书（采购内容及要求）

西安市高陵区医院网络安全等级保护建设项目

一、采购清单

序号	名称	数量
1	入侵防御	1台
2	入侵检测	1台
3	准入控制系统	1台
4	上网行为管理	1台
5	日志审计系统	1台
6	数据库审计系统	1台
7	堡垒机	1台
8	漏洞扫描	1台
9	网闸	2台
10	服务器	2台
11	测评	3项
12	机房改造	1项
13	机柜	1个

二、技术参数

一、入侵防御			
1	★配置要求	入侵防御系统，有液晶面板，≥1TB硬盘，标准配置≥千兆6个10/100/1000M自适应电口，≥2个扩展插槽，≥2组bypass，1个Console口，2个USB接口。报价中包含三年IPS特征库升级服务，三年硬件质保服务。	
2	★硬件架构	采用多核架构，支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件；	
3	★性能要求	网络层吞吐量≥5Gbps，IPS吞吐量≥2Gbps，最大并发连接数≥100万，每秒新建连接数≥5万/秒。	
4	★部署模式	产品提供多种部署模式，支持路由、透明接入、虚拟网线等部署方案的工作模式（请提供截图证明）	

5	★应用识别	产品具备应用识别特征库，提供 P2P 下载、网络电视、即时通讯、股票软件、流媒体、网络电话、手机应用等多种应用识别类型，特征库数量不少于 3000（请提供截图证明）	
6		产品具备自定义应用协议，提供除五元组之外的应用技术、应用属性、风险级别、类型、子类、协议、匹配内容、应用层长度等多项设置（请提供截图证明）	
7	ACL	产品具备访问控制功能，通过设置源及目的 IP、时间调度、用户、网络服务、流入接口、应用对象、源域、目的域等配置项实现访问限制	
8		★产品具备自定义访问控制功能，针对源及目的 MAC、报文头部信息（SYN 标志、分片标志、TTL、DSCP、Precedence、TOS）、内网域地址、外网域地址、长连接超时时间等细粒度的访问控制功能（请提供截图证明）	
9		★产品具备 ALG 协议类型过滤功能，支持 FTP、H.323、H.323GK、PPTP、MMS、RTSP、SIP、XDMCP、SQL*NAT/TNS 和 V2V 协议类型(请提供截图证明)	
10	安全策略	产品具备一体化安全策略模板功能，通过单条策略既可完成多项策略设置，可以配置源目的地址、国家地区、源目的域、源目的 MAC、时间对象、用户、虚拟身份、服务对象、URL 分类等对象，同时可在同一策略下，调用入侵防护、一体化防病毒、文件控制、URL 过滤、数据过滤防护、威胁情报、口令检测、挂马防护、僵尸网络等应用安全策略进行安全防护（请提供截图证明）	
11		产品具备配置向导功能，通过引导用户配置，包括拓扑图、桥接口配置、地址区域流、IPS、可视、概览等多项元素实现快速配置上线（请提供截图证明）	
12	病毒防护	★产品具备双病毒引擎功能，提供本地病毒引擎与云端第三方病毒引擎功能，支持 16 类 500 余万种病毒特征库（请提供截图证明）	
13		★产品具备病毒多种扫描模式，支持快速扫描和 16 层深度压缩文件的扫描模式，提供 HTTP、FTP、IMAP、POP3、SMTP 协议的病毒扫描功能（请提供截图证明）	
14		产品具备 7zip、avi、exe、mp3、gif、jpeg、mpeg 等 50 多种文件类型的病毒扫描策略（请提供截图证明）	
15		产品具备 MD5 黑白名单策略，通过检测文件 MD5 值判断文件安全性（请提供截图证明）	

16	入侵防护	品具备检测防逃逸技术，提供缓冲区溢出、SQL 注入、扫描刺探、间谍软件、拒绝服务、病毒、木马后门、漏洞攻击、潜在风险的入侵防御特征库	
17		★产品提供入侵防御特征库，特征数超过 10000 条。并提供基于正则表达式匹配方式的自定义特征策略功能（请提供截图证明）	
18	★情报威胁	产品具备云端威胁情报功能，提供僵尸网络、钓鱼网站、恶意网站等 10 大类的威胁情报并把相关数据运用到产品防御策略中（请提供截图证明）	
19		产品具备安全态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对威胁趋势图、风险主机 TOP10、威胁等级 、最新入侵事件 、设备运行状态 、资源监控、告警总数等信息统计展示（请提供截图证明）	
20	★系统管理	产品具备移动终端管理功能，无需安装 APP 和第三方插件，通过手机浏览器即可管理设备，并可查看设备 CPU、内存、硬盘使用情况（请提供截图证明）	
21		产品具备移动终端对设备的一键黑白名单功能，当突发应急事件时，提供一键黑名单应急处置功能（请提供截图证明）	
22		产品具备配置文件功能，提供配置文件的导入、导出功能，并可以指定下次启动的配置文件（请提供截图证明）	
23	★资质要求	中国国家信息安全产品认证证书	
24		国家信息测评中心 EAL 3+级资质	
25		IPv6 Ready Logo 测试认证证书	
26		国家信息安全漏洞库兼容性资质证书	
27		CVE 兼容性证书	
二、入侵检测			
1	★配置要求	1TB 硬盘，单电源，标准配置≥千兆 6 个 10/100/1000M 自适应电口，≥2 个扩展插槽，1 个 Console 口，2 个 USB 接口。报价中包含三年 IDS 特征库升级服务，三年硬件质保服务。	
2	★硬件架构	采用多核架构，支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的	

		历史配置文件；	
3	★性能要求	网络层吞吐量≥5Gbps，IDS 吞吐量≥2Gbps，最大并发连接数≥100 万，每秒新建连接数≥5 万/秒。	
4	★部署模式	产品提供多种部署模式，支持路由、透明接入、虚拟网线等部署方案的工作模式(请提供截图证明)	
5	★应用识别	产品具备应用识别特征库，提供 P2P 下载、网络电视、即时通讯、股票软件、流媒体、网络电话、手机应用等多种应用识别类型，特征库数量不少于 3000（请提供截图证明）	
6		产品具备自定义应用协议，提供除五元组之外的应用技术、应用属性、风险级别、类型、子类、协议、匹配内容、应用层长度等多项设置（请提供截图证明）	
7	ACL	产品具备访问控制功能，通过设置源及目的 IP、时间调度、用户、网络服务、流入接口、应用对象、源域、目的域等配置项实现访问限制	
8		★产品具备自定义访问控制功能，针对源及目的 MAC、报文头部信息（SYN 标志、分片标志、TTL、DSCP、Precedence、TOS）、内网域地址、外网域地址、长连接超时时间等细粒度的访问控制功能（请提供截图证明）	
9		★产品具备 ALG 协议类型过滤功能，支持 FTP、H.323、H.323GK、PPTP、MMS、RTSP、SIP、XDMCP、SQL*NAT/TNS 和 V2V 协议类型(请提供截图证明)	
10	安全策略	产品具备一体化安全策略模板功能，通过单条策略既可完成多项策略设置，可以配置源目的地址、国家地区、源目的域、源目的 MAC、时间对象、用户、虚拟身份、服务对象、URL 分类等对象，同时可在同一策略下，调用入侵防护、一体化防病毒、文件控制、URL 过滤、数据过滤防护、威胁情报、口令检测、挂马防护、僵尸网络等应用安全策略进行安全防护（请提供截图证明）	
11		产品具备配置向导功能，通过引导用户配置，包括拓扑图、桥接口配置、地址区域流、IPS、可视、概览等多项元素实现快速配置上线（请提供截图证明）	
12	病毒防护	★产品具备双病毒引擎功能，提供本地病毒引擎与云端第三方病毒引擎功能，支持 16 类 500 余万种病毒特征库（请提供截图证明）	

13		★产品具备病毒多种扫描模式，支持快速扫描和16层深度压缩文件的扫描模式，提供HTTP、FTP、IMAP、POP3、SMTP协议的病毒扫描功能（请提供截图证明）	
14		产品具备7zip、avi、exe、mp3、gif、jpeg、mpeg等50多种文件类型的病毒扫描策略（请提供截图证明）	
15		产品具备MD5黑白名单策略，通过检测文件MD5值判断文件安全性（请提供截图证明）	
16	入侵检测	品具备检测防逃逸技术，提供缓冲区溢出、SQL注入、扫描刺探、间谍软件、拒绝服务、病毒、木马后门、漏洞攻击、潜在风险的入侵防御特征库	
17		★产品提供入侵检测特征库，特征数超过10000条。并提供基于正则表达式匹配方式的自定义特征检测策略(请提供截图证明)	
18	★情报威胁	产品具备云端威胁情报功能，提供僵尸网络、钓鱼网站、恶意网站等10大类的威胁情报并把相关数据运用到产品防御策略中（请提供截图证明）	
19		产品具备安全态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对威胁趋势图、风险主机TOP10、威胁等级 、最新入侵事件 、设备运行状态 、资源监控、告警总数等信息统计展示(请提供截图证明)	
20	★系统管理	产品具备移动终端管理功能，无需安装APP和第三方插件，通过手机浏览器即可管理设备，并可查看设备CPU、内存、硬盘使用情况（请提供截图证明）	
21		产品具备移动终端对设备的一键黑白名单功能，当突发应急事件时，提供一键黑名单应急处置功能（请提供截图证明）	
22		产品具备配置文件功能，提供配置文件的导入、导出功能，并可以指定下次启动的配置文件（请提供截图证明）	
23	★产品资质	中国国家信息安全产品认证证书	
24		国家信息测评中心 EAL 3+级资质	
25		IPv6 Ready Logo 测试认证证书	
26		国家信息安全漏洞库兼容性资质证书	

27		CVE 兼容性证书	
三、准入控制系统			
1	★硬件参数	事件综合处理性能≥2000EPS，1TB 硬盘，本次≥25 准入单点授权。设备默认 1 个 Console 口，≥6 个千兆电口，≥4 个 SFP 插槽，≥2 个 SFP+插槽。配置 1500 准入客户端授权	
2	部署管理	设备采用旁路部署方式，避免串行设备部署导致单点故障	
3		★支持多台准入设备在同一管理平台集中管理，支持设备分组，策略分组下发，分权管理，设备的集中监测等。实现分布式部署，集中管理，满足大型网络环境下的部署要求。（提供产品界面截图）	
4		★不同区域采用不同组合认证技术方式，分支机构独立认证或混合认证管理机制（提供产品界面截图）	
5		★支持两种及以上准入技术，每种准入技术均具备完善的逃生机制，防止准入设备本身出现问题后对现有网络业务造成影响（包括但不限于测试报告、官网或功能截图等）；	
6	准入控制	★需支持集中管理方式，一体化“管理平台可集成杀毒、管控、审计、准入等模块，需对准入设备集中管理与监测，分权分域管理，实现分布式部署、集中管理的特点，满足大型网络环境下的部署要求。提供生产厂家出具的、相应的功能证明材料（包括但不限于测试报告、官网或功能截图等）；	
7		需支持和多种第三方认证源联动认证，至少支持 AD、LDAP、Email、HTTP 服务器联动认证，实现统一认证管理要求。提供生产厂家出具的、相应的功能证明材料（包括但不限于测试报告、官网或功能截图等）	
8		需支持准入接入点交换机列表，查看交换机端口状态，端口名称、使用端口、未使用端口、级联口、802.1x 开启端口，疑似 HUB 接入口状态查看，支持交换机端口状态清单的导出；	
9		需支持设备端口的流量监测，接受数据、发送数据、错误数据、丢弃数据等端口监测状态。提供生产厂家出具的、相应的功能证明材料（包括但不限于测试报告、官网或功能截图等）；	

10		★支持有线、无线基于应用准入方式，准入配置支持保护服务器区域、例外终端等灵活的配置方式（包括但不限于测试报告、官网或功能截图等）；	
11		★支持基于应用协议的访问控制，可基于 IP、协议端口进行访问流量控制。（包括但不限于测试报告、官网或功能截图等）；	
12		支持基于 802.1x 认证的开机自动认证、支持账号和终端绑定认证，账号和接入点绑定认证，	
13		支持临时用户的访问申请，可限制临时用户访问时长和过期自动删除，并可限制临时用户入网时间长和过期自动删除	
14		支持 Web Portal 认证方式，核心服务器区访问准入，可采用账户口令方式进行认证，认证账号支持有效期设置，支持过期自动删除	
15		支持标准 802.1x 准入，支持动态 VLAN，支持账号接入有效时间限制，账号在线数量限制	
16		★支持通过自动审批和管理员手动审批两种方式进行用户申请审核，审批通过邮件进行通知（包括但不限于测试报告、官网或功能截图等）；	
17	合规检查	★支持健康合规检查策略，采用动态检测技术，需支持多种检查机制，至少支持入网检查、定时检查、周期检查机制，针对接入内部网络的计算机终端实行多种安全检查策略，支持分组策略下发控制，拦截不安全终端接入网络。（包括但不限于测试报告、官网或功能截图等）；	
18		★支持终端安全检查失败处置措施，可基于协议、特定端口、端口范围、特定地址、IP 范围、URL 来控制终端访问权限，从而无需操作交换机达到终端网络隔离目的，实现细粒度的访问控制管理（包括但不限于测试报告、官网或功能截图等）；	
19		★支持终端安全检查失败本地 ACL 隔离机制，可基于协议、特定端口、端口范围、特定地址、IP 范围、URL 来控制终端访问权限，从而无需操作交换机达到终端网络控制目的，实现细粒度的访问控制管理，支持不同终端修复区域定义。（包括但不限于测试报告、官网或功能截图等）；	
20		支持对关键位置注册表的检查，关键位置文件检查；检查指定的可疑文件或可疑注册表项	
21		支持非法外联检查，支持多个外联地址检查	

22		★支持对不合规的终端提供软隔离，不符合安全策略的计算机终端进行友好提示，提供终端修复向导，需支持引导修复和一键修复功能，并支持不同区域终端的修复区域定义，支持远程桌面检查（包括但不限于测试报告、官网或功能截图等）；	
23		★支持对文件共享检查，检查终端用户是否存在共享目录	
24		★外设使用安全检查，检查是否插入自动运行风险性 U 盘	
25		★支持对不合规的终端提供软隔离，不符合安全策略的计算机终端进行友好提示，提供终端修复向导，需支持引导修复和一键修复功能，并支持不同区域终端的修复区域定义。（包括但不限于测试报告、官网或功能截图等）；	
26	★联动能力	可支持与 AD、LDAP、Email、Http 第三方服务器联动认证，来完成用户鉴别功能，以达到终端用户实名制入网，统一认证管理，支持 LDAP 用户导入，用户映射关系、组织架构导入（提供产品界面截图）	
27		实时监测终端是否安装终端安全防护软件，快速引导安装，安装成功后执行合规检查，保障入网终端始终处于合规、可控范围内，实时上报安全动态及入网数据进行风险分析(提供产品界面截图)	
28		客户端具有防破坏和卸载能力，对服务、双进程、文件进行有效自我保护机制	
29	★资质要求	1. 提供公安部颁发的《计算机信息系统安全专用产品销售许可证》终端接入控制（一级）资质证书。 2. 具备该软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书。	
四、上网行为管理			
1	★配置要求	标配≥6 个千兆电接口；提供≥2 个扩展插槽；≥1T 硬盘；含专用操作系统与上网行为管理标准软件。含三年硬件质保服务和三年软件版本升级服务。	
2	★硬件架构	采用多核架构，设备必须提供物理硬件 bypass 按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅	
3		支持远程登录在界面实现 Bypass，并可进行切换（必须提供配置界面截图，加盖厂商公章）	

4	★性能要求	建议≥300M 带宽/2500 人网络环境使用；最大并发连接数≥100 万；最大新建连接数≥28000 个/秒	
5	功能要求	★设备在部署时支持模式选择，可设置为 Portal 模式，实现 Portal 服务器功能；（必须提供配置界面截图，加盖厂商公章）	
6		★可集中呈现上网行为风险等级和状态。行为风险等级包括安全等级、效率等级、合规等级和管控等级。（必须提供配置界面截图，加盖厂商公章）	
7		★支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对本地计算资源的消耗（必须提供配置界面截图，加盖厂商公章）	
8		支持通过恶意软件特征检测方式识别失陷主机并记录日志（必须提供配置界面截图，加盖厂商公章）	
9		★应用协议库包含的应用数量不低于 7100 种，应用规则总数不低于 30000 种。（必须提供配置界面截图，加盖厂商公章）	
10		★为覆盖工作无关应用，移动应用不少于 1000 种，即时消息应不低于 150 种，虚拟货币交易平台不低于 40 种；为规避外发类风险，论坛发帖应不低于 3000 种，网络存储不低于 100 种，代理隧道不低于 100 种。 （必须提供配置界面截图，加盖厂商公章）	
11		★当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈；（必须提供配置界面截图，加盖厂商公章）	
12		能够基于发件人、收件人、主题、内容、附件名维度进行过滤、记录、告警；能够支持 SSL 加密的 SMTP 邮件审计；必须提供配置界面截图，加盖厂商公章）	
13		支持对 Windows 百度网盘客户端的文件标题和内容审计，支持对 QQ、微信和百度网盘的 PC 客户端外发文件进行关键字过滤和封堵（必须提供配置界面截图，加盖厂商公章）	
14		★支持对微信 windows 版客户端进行聊天内容审计 支持对微信 Windows 版客户端的外发文件进行文件内容审计（必须提供配置界面截图，加盖厂商公章）	

15		★可审计、控制 Oracle，MySql，SqlServer，PostgreSQL 等数据库的访问与操作，包括添加、删除、修改、查询等。（必须提供配置界面截图，加盖厂商公章）	
16		★支持基于用户、时间、应用、源 IP、目的 IP 和服务创建流量控制策略(必须提供配置界面截图，加盖厂商公章）	
17		★支持配置禁用 PC 热点开启功能。禁用时 PC 仍可以使用网络，但是无法通过随身 wifi 或笔记本自带功能创建热点。（必须提供配置界面截图，加盖厂商公章）	
18		★支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制，避免超级管理员权限过大的弊端。系统管理员和审计员的账号创建，权限变更需要审核员审批才能生效。管理员和审计员的操作会形成日志受审核员监督。（提供审核员审批操作截图）	
19		支持管理员账号初始密码检测，如果发现管理员未更改初始密码，能够进行提醒，提供生产厂家出具的、相应的功能证明材料（必须提供配置界面截图，加盖厂商公章）	
20	★资质要求	1. 近 3 年在 IDC 国内安全内容管理市场占有率排名在前 3 证明材料 2. 中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，级别为 EAL3+ 3. 中华人民共和国工业和信息化部颁发的电信设备进网许可证 4. IPv6 ready 金牌认证资质证书 5. IT 产品信息安全认证证书	
五、日志审计系统			
1	★硬件规格	国产知名品牌，软硬一体形态，事件综合处理性能≥2000EPS。硬件规格：≥6 个千兆电口，≥2 个扩展插槽，≥2T 硬盘，1 个 Console 接口，220V 交流冗余电源。≥包含 25 个日志源授权。	
2	★网络环境支持	系统可同时支持 IPv4 和 IPv6 的网络环境下数据库的审计；	
3	管理范围	能够对企业和组织的 IT 资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、虚拟化、云计算、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。	

4	★日志采集与转发	支持通过 Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent 代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka 等多种方式完成各种日志的收集功能；(提供截图证明)	
5		支持按照 Syslog-NG 标准及自有格式进行转发，转发时包含原始日志源 IP 地址；	
6	资产管理	★支持对资产 IP 地址（含内网 IP）的地理信息进行管理，设置单 IP 及 IP 段行政区及经纬度，支持地图显示；	
7		★支持自定义资产类型及资产属性；支持对资产自定义标签，支持对标签内容进行查询和管理；	
8		支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。(提供截图证明)	
9		★支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息，并对资产进行 CIA 赋值，自动计算资产价值，设置等保等级；在资产管理界面可查看每个资产的属性信息，情境信息，本身产生的事件信息、关联告警信息；(提供截图证明)	
10	★日志解析	系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化，不需修改系统程序；(提供截图证明)	
11		日志解析字段内置大于 130 个字段，属性字段可扩展，用户可根据审计需要自行创建字段，字段类型包括 IP、字符串、整型等 6 种，可设定字段长度、选择字段操作符集，选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计；(提供截图证明)	
12	★日志分析	系统具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理，可将原始信息进行自动索引，快速搜索分析各类安全事件。系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件；(提供截图证明)	
13		系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表	

		达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件；（提供截图证明）	
14		能够在世界地图上实时定位事件源/目的 IP 地址（内网 IP）的地理位置；（截图证明）	
15		支持点击事件任意属性字段，可以该字段为条件对事件进行统计分析，并展示 Top 20 排序，排序支持正序和倒序，并可对统计内容进行点击下钻；（提供截图证明）	
16		可以以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。（提供截图证明）	
17		采用机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别，使审计人员清晰了解采集的日志构成；（提供截图证明）	
18		支持对保存在系统中的历史日志进行回溯关联分析，发现历史日志中的安全事件；（提供截图证明）	
19		支持对关联规则进行监控，了解该规则命中历史情况；（提供截图证明）	
20	★关联分析	具备完善的基于规则的关联分析引擎，能够提供逻辑关联、统计关联和递归关联三种关联分析能力。其中，逻辑关联支持与、或、非逻辑，支持丰富的逻辑表达式（包括并不限于大于、大于等于、小于、小于等于、不等于、包含、在……之间、属于、开始于、结束于、是否为空、通配符匹配、正则匹配等），支持逻辑嵌套；统计关联支持在统计的时候针对特定的一个或多个字段进行相同计数和不同计数，支持统计时长设置和触发次数设置，具备重复触发的抑制设置功能；（提供截图证明）	
21	★资质要求	提供中国信息安全认证中心《中国国家安全产品认证证书》（网专+3C），增强级； 国家信息安全测评中心《信息技术产品安全测试证书》EAL3+（以上证书需提供加盖厂商公章复印件） 提供至少三项产品相关专利	
六、数据库审计系统			
1	★硬件及性能要求	专用硬件平台和安全操作系统，事件处理≥12000 条/秒，内置≥4TB 磁盘存储空间。双电源；≥6 个千兆自适应电口，1 个 Console 口，支持两个扩展槽位，支持液晶屏。	

2	★部署方式	★支持通过 Agent 审计回环地址的流量	
3		可通过端口镜像（SPAN）或者分流器（TAP）模式旁路部署或 Agent 插件方式部署。	
4	审计功能	★支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓 kingbase 南大通用 Gbase,hadoop 架构下 Hbase，支持后关系型数据库 Cache、工控 IP21 的审计。（要求提供功能效果截图并厂家盖章证明）。	
5		★支持旁路阻断功能（非串联方式），阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源 IP 操作的所有请求直接阻断。（要求提供功能效果截图并厂家盖章证明）。	
6		★支持全文检索数据库 solr 的审计，可审计到 solr 的查询、插入行为的操作信息。（要求提供功能效果截图并厂家盖章证明）	
7		★支持 C/S 架构 COM、COM+、DCOM 组件的审计，可提取应用层工号（账号）的身份信息，精确定位到人；（要求提供功能效果截图并厂家盖章证明）。	
8		★全面支持后关系型数据库 Cache 的审计，包括 terminal、portal、studio、Sqlmanager、MedTrak 等工具访问的审计，Portal 可审计 Sql 语句、查询 Global 变量以及二者的返回内容，Terminal 可审计 M 语句及返回内容，MedTrak 可审计工号、操作报表以及二者的返回内容，studio 可审计到编译、代码更改等操作，Sqlmanager 可审计数据库账号和操作的 sql 语句。(要求提供功能效果截图并厂家盖章证明)。	
9	审计策略	★审计规则支持 24 种以上分项响应条件：支持规则类型(普通规则、组合规则)、风险级别(高、中、低、一般行为、关注行为五种级别)、数据库操作命令（包括 select、create、delete 等 40 种以上命令）；关键字审计、语句长度、语句执行回应（包含成功、失败、阻断等）、语句执行时间（支持配置 1-999999ms 阈值）、返回内容、返回行数（支持配置 1-9999 阈值）、数据库名、应用账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、时间（含开始结束日期）、数据库表、包、存储过程、函数、视图、字段、索引等条件（要求提供功能效果截图并厂家盖章证明）。	

10		审计规则针对访问工具、客户端 IP、客户端 MAC、操作系统主机名、操作系统用户名、应用账户名、数据库对象、SQL 语句执行回应等条件支持设置等于或不等于等条件	
11		★内置疑似 SQL 注入、跨站脚本攻击、字段猜测、代码更改、等近 500 种风险审计规则库，无需单独配置，直接调用。（要求提供功能效果截图并厂家盖章证明）。	
12		★支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警（要求提供功能截图并厂家盖章证明）。	
13	审计查询	★系统支持全库检索、条件检索和关键字检索，检索效率达到 1 亿条数据二十秒内检索出结果，快速定位相应的审计会话内容。	
14		★可根据包括时间范围（最近一分钟、五分钟、十分钟、半小时、一小时、十二小时、自定义时间等条件快速查询）、风险级别（高风险、中风险、低风险等级别）、保护对象、操作类型、客户端 IP（支持多个 IP 地址查询）、访问工具、数据库账户、应用账户、关键字过滤、规则名、规则组名、规则类型、客户端 MAC、客户端端口、操作系统主机名、操作系统用户名、服务端 IP（支持多个 IP 地址查询）、服务端端口、数据库名、语句长度、回应、语句执行时间、返回行数、返回结果、记录编号、会话 ID、处理状态等二十五种以上条件进行检索查询。（要求提供功能截图并厂家盖章证明）。	
15		事件回放支持以正序/倒序方式回放，并且支持设置回放时间，针对记录前后 1/2/5/30/60 分钟进行回放	
16	监控与告警	审计管理平台监控墙支持通过时间轴的方式以折线图展示当月每天的操作次数，支持通过时间范围检索登陆失败最多 IPTOP5 排行，登录次数最多的 IPTOP5 排行，和操作最多的功能模块 TOP5 排行信息	
17	系统管理	用户管理支持三权分立，系统提供了审计管理员、系统管理员、安全管理员分权的用户体系。	
18		支持根据保留天数和占用百分比自动清理，清理数据类型支持审计记录（高风险、中风险、低风险、一般行为、关注行为）、报表、后台日志及返回结果；	

19	★资质要求（备注：所有资质必须为数据库审计产品专有的资质）	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》，数据库安全审计国标-增强级；	
20		《计算机软件著作权登记证书》	
21		产品具备 IPv6 Ready Logo （Phase-2）认证	
22		具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》，级别 EAL3+，提供证书复印件；	
23		具备中国信息安全认证中心《中国国家信息安全产品认证证书》（CCRC 增强级）	
七、堡垒机			
1	★配置要求	国产知名品牌；≥6 个千兆电口；支持≥2 个接口扩展槽位；最大支持 150 路图形会话或 400 路字符会话并发，内置≥4TB 硬盘；冗余电源；支持液晶屏；本次配置 100 个管理授权；	
2	资源管理	支持 IPv4、IPv6 网络环境下的运维、操作审计；	
3		支持 SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin 等协议	
4		支持 Linux/Unix、Windows、H3C、Huawei、Cisco 等系统；	
5		可通过 windows 应用发布实现对 MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client、Radmin、dbisql 等应用程序/客户端的扩展支持，且图形界面支持分辨率设置；	
6		支持 SSH、RDP 协议文件管理与剪切板控制功能；	
7		★可通过 Linux 应用发布的方式实现对火狐浏览器的扩展支持；（提供截图配置截图）	
8		★支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure 云平台的资源（提供截图配置截图）	
9		不限操作客户端系统类型，无需安装任何客户端插件，使用 H5 即可直接运维 windows、Linux、网络设备等资源；	
10		运维过程中会话协同，可邀请其他用户参与、协助操作；会话协同过程中，参与者可以控制会话，创建者强制获取控制权；	

11	身份认证	★支持不同的用户配置不同的多因子认证方式，例如 user01 配置手机令牌、USB Key，user02 配置手机短信	
12		★支持微信小程序动态口令认证方式登录堡垒机，且当用户需要使用手机令牌登录时，需要强制绑定手机令牌	
13		★支持认证方式组合使用，例如使用 AD 域+手机短信、AD 域+Radius 认证、Radius 认证+手机令牌等多种组合方式登录（提供截图配置截图）	
14	策略管理	★针对核心设备可配置双人授权，需要管理员现场审批才能访问资源（提供截图配置截图）	
15		★针对核心设备，除可以配置双人授权外，也可以通过动态令牌进行授权，运维员需要拿到动态令牌才可以对资源进行运维	
16		★支持对 MySQL 和 Oracle 数据库的访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制（提供截图配置截图）	
17	访问和命令控制	按用户组和账户组多对多的资源访问授权，用户组和账户组内的新增成员可自动继承授权关系	
18		★预置 Linux 主机和网络设备的基本命令，支持正则表达式和通配符方式设置匹配规则，自定义命令黑白名单；（提供截图配置截图）	
19		★对MySQL和Oracle等数据库的访问操作控制，可基于库、表、命令实现对数据库操作的细粒度访问控制；	
20	自动运维	支持在页面上批量执行命令和脚本，实时查看命令和脚本的输出结果，实现快速运维，脚本类型支持 Python 和 Shell；	
21		★不限操作系统类型，无需安装任何客户端插件，使用浏览器通过 H5 方式即可直接运维 SSH、RDP、Telnet、VNC 和应用发布资源（提供截图配置截图）	
22		支持批量执行命令和脚本时，能够实时查看命令和脚本的输出，支持批量传输文件时，可以实时查看传输进度；	
23		★支持将执行命令、执行脚本和传输文件传操作灵活组合成运维任务，运维任务支持手动执行、定时执行和周期执行（提供截图配置截图）	
24		★支持以云盘形式在堡垒机上存储常用文件，实现操作端、堡垒机和目标资源三者之间文件共享（支持多文件和文件夹下载，文件展示最近修改时间和权限）（提供截图配置截图）	

25		★支持 SSH、RDP、TELNET、VNC 协议资源的批量登录功能，并且支持混合协议的批量登录，支持同时在一个页面运维不同协议的资源(提供截图配置截图)	
26	**★资质要求**	《公安部销售许可证》 《IPv6 证书》 《IT 产品信息安全证书》	
八、漏洞扫描			
1.	**★规格要求**	≥1T 硬盘，配置≥6 个 10/100/1000M 自适应电口，2 个扩展插槽,液晶面板显示，2 个 USB 口，1 个 Console 口。Web 扫描域名无限制，Web 扫描任务并发数≥5 个域名。系统扫描 IP 地址≥1024 个，支持扫描 A 类、B 类、C 类地址，系统扫描≥50 个 IP 地址并行扫描	
2.	**基本要求**	★能够提供系统扫描、WEB 扫描；（提供产品功能截图）	
3.		支持 IPV4、IPV6 环境部署管理、扫描；（提供产品功能截图）	
4.		支持多路扫描功能，设备所有网口均可用于扫描，支持同时对多个隔离子网进行扫描；	
5.	**部署要求**	支持分布式部署，管理中心统一下发策略、查看任务结果、导出报表，无需登录子引擎；支持从管理中心查看子引擎及其状态；管理中心、子引擎均可执行扫描任务	
6.		★网络配置需提供快速配置向导,支持快速部署上线；（提供产品功能截图）	
7.	**安全要求**	支持可信 IP 管理，自定义允许访问系统的 IP 范围；	
8.		支持自定义用户口令策略，包括密码更换周期、密码长度要求、密码复杂度要求。	
9.	**扫描策略管理**	★支持同时下发系统扫描、Web 扫描、弱口令扫描任务，无需单独下发扫描任务，扫描目标可以是 IP、域名、URL 的任一格式；（提供产品功能截图）	
10.		支持多主机、多线程扫描，可灵活调整参数以调整扫描速度；（提供产品功能截图）	
11.		★支持自适应网络扫描,根据网络状况自动控制发包速率，避免影响用户网络；（提供产品功能截图）	
12.		★支持针对已有任务做任务复制,快速生成一个相同任务，支持对复制出来的任务进行再编辑，包括：基本信息、策略、目标范围、调度、扫描	

		参数；（提供产品功能截图）	
13.		支持自定义立即执行、定时扫描、周期性扫描等多种扫描任务执行方式，可针对指定时间、执行对象自动执行扫描任务，并自动生成报告，时间可具体到某月、某天、某时、某分；	
14.	系统扫描	★支持检测的漏洞数大于 60000 条以上，涵盖漏洞标准包含 CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq6 种，CVSS 覆盖 CVSS2 和 CVSS3 版本；（提供产品功能截图）	
15.		支持扫描通用操作系统，涵盖 Windows 系列、苹果操作系统、Linux、AIX、HPUX、IRIX、BSD、Solaris 等；支持扫描交换路由设备，涵盖 Cisco、Juniper、华为、F5、Checkpoint、锐捷在内的主流厂商的设备；支持扫描安全设备，涵盖 Checkpoint、赛门铁克、Cisco、Juniper、Palo Alto、华为在内的主流厂商的防火墙等安全设备；	
16.		支持中间件漏洞扫描，涵盖 Apache、Resin、Nginx、Tomcat、TongWeb、BIND、DOMINO、WebSphere、IIS、Jboss、InforSuite 等；	
17.		★支持扫描国产系统、数据库扫描。国产操作系统包括中兴新支点、中标麒麟、凝思、华为欧拉、深度、红旗，国产数据库包括神通、人大金仓、南大通用、达梦（提供产品功能截图）	
18.		支持大数据组件框架漏洞检测，如 zookeeper、ElasticSearch、ActiveMQ 、Kibana、Hadoop 等；	
19.		★支持 SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP 协议的登录扫描；支持批量导入登录信息、批量登录验证；（提供产品功能截图）	
20.	Web 扫描	支持 Web 漏洞扫描，检测基于 OWASP Top10 标准定义扫描规则；	
21.		★支持自动探测指定网段中的 Web 站点，并可一键转为 Web 资产或一键下发 Web 扫描任务；（提供产品功能截图）	
22.		漏洞结果支持展示详细的 HTTP 请求头信息；	
23.		★支持 Web 登录扫描，支持 Cookie 认证、Form 认证、Basic 认证、NTLM 认证、Session 认证、Digest 认证、SSL，并支持 Web 登陆验证，确保 Web 登录成功；（提供产品功能截图）	

24.		支持 Web 扫描会话录制，通过登录预录制方式扫描常规网页爬虫爬取不到的 URL；	
25.		★支持至少三种漏洞验证方式如浏览器验证、注入验证、通用验证；（提供产品功能截图）	
26.		支持 Web 扫描代理检测，能够使用 HTTP 代理和 SOCKS 代理方式；	
27.	资产管理	支持资产自动发现功能，支持利用历史扫描过程中发现的主机创建扫描任务；	
28.		支持资产统一管理，支持按照 IP、URL、网页编码、操作系统、MAC 地址、所属资产组、资产标签、资产评分对资产进行高级检索和分析；（提供产品功能截图）	
29.		支持对资产及资产检测结果进行备份恢复；	
30.	数据分析及报表管理	支持漏洞数据高级检索及分析，支持按照目标 IP 或 URL、操作系统、MAC 地址、资产评分、漏洞等级、漏洞名称、漏洞类别、漏洞评分、开放端口查看漏洞分布情况，并将检索结果导出；（提供产品功能截图）	
31.		支持资产历史扫描结果变化趋势展示，并可对比任意两次扫描结果，查看新增漏洞和减少漏洞；（提供产品功能截图）	
32.		支持离线导出报表或扫描任务结束后自动发送报表到指定邮箱，报表包含 5 种常见格式：Excel、Word、HTML、PDF、XML；（提供产品功能截图）	
33.		★支持导出同时包含系统扫描、Web 扫描、弱口令扫描结果的报表，可以统一分析网站漏洞、网站所在主机漏洞以及主机弱口令；（提供产品功能截图）	
34.		★支持自定义导出报表模板，可定制指定漏洞等级（高危、中危、低危等）、指定漏洞状态（新增、误报、已修复）、指定公司信息、公司 LOGO、指定报表标题以及章节内容的报表模板，并可在导出报表时灵活选择已经定义好的报表模板；（提供产品功能截图）	
35.		★支持扫描任务完成后发送告警，告警方式包含邮件告警、短信告警、SNMPtrap 告警、SYSLOG 告警、FTP 告警；（提供产品功能截图）	
36.	系统管理	★漏洞库支持在线升级、FTP 方式升级、本地导入升级，在线升级支持设置周期自动升级时间，支持通过代理方式进行升级；（提供产品功能截图）	

37.		支持自带诊断工具，包含 PING、WGET、端口探测、Tcpdump 抓包、故障信息收集、一键诊断修复等工具；	
38.	★资质要求	计算机信息系统安全专用产品销售许可证	
39.		中国国家信息安全产品认证证书书（增强级）	
40.		IPv6 Ready Logo 认证（Phase-2）	
41.		国家信息安全测评信息技术产品安全测评证书（EAL3+）	
九、网闸			
1	**★性能及服务要求**	系统吞吐量：≥600Mbps 硬件配置：标准 2U 机箱，冗余电源；支持液晶面板 内网接口：≥6 个 10/100/1000Base-T 端口，1 个 Console 口，2 个 USB 口；支持≥1 个扩展槽位； 外网接口：≥6 个 10/100/1000Base-T 端口，1 个 Console 口，2 个 USB 口；支持≥1 个扩展槽位 功能模块：数据库同步、文件交换、数据库访问、邮件访问、安全浏览、安全 FTP、定制模块、工控访问等； 可增配集中监控与数据分析中心（MDA）统一管控； 质保年限：默认包含三年维保；	
2	**功能要求**	★采用“2+1”模块结构设计，即包括外网主机模块、内网主机模块和隔离交换模块，内外端机为网络协议终点，彻底阻断各种网络协议；	
3		★自主研发的基于安全芯片的专用隔离部件，无操作系统，外部无法编程控制，全硬件交换；采用多核并行架构的自主研发安全操作系统；	
4		★采用基于 linux 内核的多核并行安全操作系统（提供软件著作权证书截图）	
5		★支持双系统冗余架构，可通过 WEB、console 口进行主备系统切换，当主系统发生故障可切换至备系统进行工作（提供功能截图并加盖原厂公章）；	
6		提供基于 https 的图形化安全管理，支持用户名/口令、RADIUS、数字证书、U-KEY 等多种认证管理方式；	
7		提供调制工具，至少包括：trace、ping、telnet、arp 等（提供功能截图并加盖原厂公章）；	
8		★文件交换、邮件访问、FTP 访问、安全浏览支持病毒检测功能，支持通过文件大小控制病毒查杀（提供功能截图并加盖原厂公章）；	
9		★支持 MySQL、ORACLE、SQLServer、DB2、SYBASE、POSTGRESQL 等数据库的同步（提供功能截图并加盖原厂公	

		章）
10		支持 TCP 定制服务，支持源地址绑定、网络接口地址绑定功能，支持源地址、源端口、目的地址、目的端口过滤功能
11		支持多种告警类型：病毒告警、攻击告警、硬件异常、系统异常、资源异常、配置变化、日志告警，支持状态日志配置，通过设置硬件信息使用率进行日志记录及暂停使用
12		支持入侵检测功能，可对网页攻击、缓冲区溢出攻击、后门/木马、P2P、病毒/蠕虫、拒绝服务攻击、扫描类攻击等多种攻击类型进行实时检测并记录日志，支持弱口令防护和攻击防护
13		支持双机热备，支持宕机切换、拔线切换等多种切换机制
14		支持 IPV4/IPV6 双栈接入
15		支持文件传输方向控制：单向传输和双向同步
16		支持根据时间、文件名、文件类型、数据库源表、目的表、IP、端口等条件查询数据从源到目的的整体轨迹信息
17		支持增配集中监控与数据分析中心统一管控，支持集中监管平台，可对多台网闸进行统一监控，记录每台设备的系统资源运行情况
18		★支持多种同步模式： 完全一致、完全复制、首次复制+新增、源端移动、源端删除等多种模式（提供功能截图并加盖原厂公章）
19		支持实时监控文件同步进度、同步状态、操作标识等同步信息，便于实时掌握文件传输过程（提供功能截图并加盖原厂公章）
20		★支持 SSL 隧道访问模式，针对 FTP 访问模块、数据库访问模块、邮件访问、定制模块等模块，通过网闸实现访问客户端认证、授权及访问链路加密，保证客户端访问合法性及访问链路的安全性（提供功能截图并加盖原厂公章）；
21		★支持多种告警类型：病毒告警、攻击告警、硬件异常、系统异常、资源异常、配置变化、日志告警，支持状态日志配置（提供功能截图并加盖原厂公章）
十、服务器		
1		外形：标准 2U 机架式服务器；
2		处理器：2 颗 Intel Xeon 4310(12C,120W,2.1GHz)处理器；
3		内存：64GB（2×32G）DDR4 ECC RDIMM 内存，内存插槽≥16 个 DDR4 内存；支持 RDIMM，LRDIMM 内存；

4	硬盘：4 块 600G 15K 企业级热插拔 SAS 盘，最大可扩展支持≥29 个 2.5 寸热插拔 SSD；最大可扩展支持≥12 个 3.5 寸 SATA/SAS 硬盘；最大可扩展支持≥12 个 U.2 NVMe SSD；后置可扩展支持≥2*E1.S 或 2*M.2；
5	RAID：独立 8 通道高性能 SAS RAID 卡，支持 RAID0/1/5/6/10/50 等；
6	网络：四千兆网口，四口万兆网卡（含光模块）；
7	HBA：2 块双口 16GB HBA 卡；
8	I/O 插槽：最大支持 5 个标准 PCIe 4.0，支持 1 个 Raid Mezz 卡，支持 1 个 200Gb/s OCP3.0 网卡，支持 4 个单宽 GPU；
9	管理：BMC 管理模块，支持 IPMI、KVM Over IP、虚拟媒体等；
10	电源及其他：2 个电源，电源功率≥550W；机架安装导轨及电源线；
11	服务：三年免费整机硬件质保，原厂工程师上门服务，提供原厂授权书及售后服务承诺函。

十一、测评服务

安全层面	安全控制点	测评指标（2.0）
安全物理环境	物理位置选择	a)机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；
		b)机房场地应避免设在建筑物的高层或地下室，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，并设置明显的不易除去的标识；
		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)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
		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；
		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。
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热冗余，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。
	集中管控	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；
		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。
	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；
		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；
		d）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；
		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。
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。
安全建设管理	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。
	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）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
		c）应制定代码编写安全规范，要求开发人员参照规范编写代码；
		d）应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。
安全运维管理	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。
	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；		
		d)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。		
十一、机房改造				
1	原吊顶拆除		㎡	75
2	机房窗封堵		㎡	9
3	机房窗封堵轻钢龙骨基层		㎡	76
4	机房窗封堵基层内填岩棉		㎡	9
5	机房窗封堵面层乳胶漆		㎡	9
6	机房窗封堵石膏板双面		㎡	76
7	机房外窗玻璃隔热膜		㎡	9
8	垃圾装袋搬运		㎡	75
9	垃圾装车外运		车	1
10	保洁打扫卫生		㎡	75
11	施工防护措施费		项	1
12	600X600 铝扣板吊顶		㎡	79
13	吊顶主龙骨		㎡	75
14	吊顶次龙骨		㎡	75
15	Φ8 吊杆、吊挂件		套	210
16	吊顶收边条		米	50

17	机房顶面漏水管道防水处理	项	1
18	顶面管道接水盘施工	米	15
19	顶面管道接水盘排水管路施工	项	1
20	隔墙吊顶上地板下封堵	项	1
21	施工辅材	项	1
22	综合布线及整理	批	1
23	主要核心系统测评（必须取得公安机关三级等保备案证）	年	1
24	机柜	个	1

第五部分 评标办法

1. 评标委员会

1.1 招标机构将按照《中华人民共和国政府采购法》、《中华人民共和国招标投标法》及有关规定组建评标委员会。

1.2 评标委员会由招标人代表及有关技术、经济等方面的专家组成。

1.3 评标委员会负责评标工作，对投标文件进行审查和评估，并向招标方提交书面评标报告。

1.4 评标方法：**综合评分法。**

1.5 投标文件的澄清

1.5.1 在评标期间，评标委员会可要求投标人对其投标文件中含义不明确的内容作必要的澄清或说明，但澄清或说明不得超出投标文件的范围或改变投标文件实质性内容。有关澄清的要求和答复均应以书面形式提交，澄清的内容为投标文件的组成部分。

2. 投标文件的初审（资格审查及符合性检查）

2.1 根据《中华人民共和国政府采购法》第二十三条 ，由采购人或采购人委托的采购代理机构对供应商的资格进行审查。评标委员会将审查投标文件是否完整。

2.2 算术错误将按以下方法更正：若单价计算的结果与总价不一致，以单价为准修改总价；若用文字表示的数值与数字表示的数值不一致，以文字表示的数值为准。如果投标人不接受对其错误的更正，其投标将被拒绝。

2.3 对于投标文件中不构成实质性偏差的不正规、不一致或不规则，招标方可以接受，但这种接受将影响投标人的综合得分。

2.4 在详细评标之前，评标委员会要审查每份投标文件是否实质上响应了招标文件的要求。实质上响应的投标应该是与招标文件要求的全部条款、条件和技术参数相符，没有重大偏离的投标。对关键条文的偏离、保留或反对将被认为是实质上的偏离。评标委员会决定投标的响应性只根据投标文件本身的内容，而不寻求外部的证据。

2.5 评标委员会不接受有选择的报价。

2.6 实质上没有响应招标文件要求的投标将被拒绝。

3. 投标文件的详细评审

3.1 评标委员会将只对确定为实质上响应招标文件要求的投标进行详细评审。

3.2 详细评审即以招标文件为依据，对所有实质上响应的投标分别从“技术”、“价格”、“商务”及“服务”等方面进行评审并按照百分制进行综合打分。

4.落实政府采购政策

4.1 中小企业政府采购政策

4.1.1 本项目执行《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）、财政部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），对符合政府采购关于中小企业扶持政策的小微企业投标人的报价给予10%的扣除，用扣除后的价格参与评审。

4.1.2 本招标文件所称中小企业，是指在中华人民共和国境内依法设立、依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。划分标准见《中小企业划型标准规定》（工信部联企业[2011]300 号）。

4.1.3 投标人提供的货物、工程或者服务符合下列情形的，享受前款办法规定的中小企业扶持政策：

（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动民法典》订立劳动合同的从业人员。

在货物采购项目中，投标人提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受本办法规定的中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

4.1.4 政府采购监督检查、投诉处理及政府采购行政处罚中对中小企业的认定，由货物制造商或者工程、服务投标人注册登记所在地的县级以上人民政府中小企业主管部门负责。

4.1.5 投标人需根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）、财政部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）和《中小企业划型标准规定》（工信部联企业〔2011〕300 号）对照自身情况及所提供产品的制造商、服务商的信息自行判断是否全部属于中小微企业。出具《中小企业声明函》（见投标文件格式）的小微企业，享受小微企业扶持，否则不享受相关中小企业扶持政策。投标人提供的《中小企业声明函》在公示中标结果时公开。

4.1.6 投标人应对其出具的《中小企业声明函》真实性负责，投标人出具的《中小企业声明函》内容不实的，属于提供虚假材料谋取中标。

4.2 监狱企业政策

4.2.1符合《财政部司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号）的监狱和戒毒企业，提供省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具属于监狱、戒毒企业的证明的，视同小型、微型企业享受 10%的价格扣除，监狱、戒毒企业属于小型、微型企业的，不重复享受价格优惠政策。

4.2.2 投标人为监狱企业且所投货物全部由监狱企业制造的，应当提供由省级以上监狱管理局、戒毒管理局出具的属于监狱企业的证明文件，未提供或出具证明文件的单位不符合要求的，不视为小型微型企业。

4.3 残疾人福利性单位政策

4.3.1 符合财政部、民政部、中国残疾人联合会下发的《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）并提供本单位制造的货物、承担的工程或者服务，或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）的投标人，视同小型、微型企业享受 10%的价格扣除。残疾人福利性单位属于小型、微型企业的，不重复享受价格优惠政策。

4.3.2投标人为残疾人福利性单位且所投货物全部由残疾人福利性单位制造的，应当提供《残疾人福利性单位声明函》，未提供的不视为小型微型企业。

4.4 节能环境标志产品政策

4.4.1 执行《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）《节能产品政府采购实施意见》（财库〔2004〕185号）《环境标志产品政府采购实施的意见》（财库〔2006〕90号）《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51号）等政府采购政策，对获得符合政府采购政策的产品实施政府优先采购或强制采购。

4.4.2 投标人可以提供所投产品经国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书扫描件。采购代理机构通过中国政府采购网（http：//www.ccgp.gov.cn/）对获证产品信息进行核对。

4.4.3 投标人所投产品属于下列情形之一的，本应属于优先采购的，不再享受优先采购政策；属于强制采购的，则按无效投标文件处理：

（1）未提供认证证书扫描件或经核对认证证书存在信息有误的；

（2）认证证书已过期。

4.4.4 享受中小企业政府采购扶持政策的投标人，可以同时享受节能产品、环境标志产品优先采购政策。

4.4.5 鼓励中标（成交）供应商在提供**货物（产品）**包装、运输按照《商品包装政府采购需求标准（试行）》（财办库〔2020〕）123号）、《快递包装政府采购需求标准（试行）》（财办库〔2020〕）123号）规定的环保要求进行包装。

5.对于符合政策性优惠的，其评标价按照以下规则进行计算调整。

5.1符合（财库〔2020〕46号）、（财库〔2022〕19号）文件规定的小微企业单位的评标价计算规则：

5.1.1 对符合规定的小型和微型企业（非联合体投标）报价给予10%的扣除，用扣除后的价格参加评审。

其评标价=投标报价*（1-10%）

5.1.2 对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体或者大中型企业的报价给予4%的扣除，用扣除后的价格参加评审。

其评标价=投标报价*（1-4%）

5.1.3 确认为小微企业（含小型、微型企业，下同）投标的，应当同时符

合以下条件：

5.1.3.1 符合国务院有关部门根据企业从业人员、营业收入、资产总额等指标制定的中小企业划型标准（工信部联企业〔2011〕300 号）；

5.1.3.2 在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

5.1.3.3 投标时须提供《中小企业声明函》；

5.2 符合（财库〔2017〕141 号）文件规定的残疾人福利性单位的评标价计算规则：

5.2.1 在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。向残疾人福利性单位采购的金额，计入面向中小企业采购的统计数据。报价给予 10%的扣除，用扣除后的价格参加评审。

其评标价=投标报价*（1-10%）

5.2.2 对于联合协议或者分包意向协议约定残疾人福利性单位的合同份额占到合同总金额 30%以上的，对联合体或者大中型企业的报价给予 4%的扣除，用扣除后的价格参加评审。

其评标价=投标报价*（1-4%）

5.2.3 确认为残疾人福利性单位投标的，应当同时符合以下条件：

5.2.3.1 符合（财库〔2017〕141 号）文件相关规定。

5.2.3.2 投标时提供本单位制造的货物、承担的工程或者服务（以下简称产品），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

5.2.3.3 投标人须提供《残疾人福利性单位声明函》。

5.3 符合（财库〔2014〕68 号）文件规定的监狱企业的评标价计算规则：

5.3.1 在政府采购活动中，监狱企业视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策。向监狱企业采购的金额，计入面向中小企业采购的统计数据。报价给予 10%的扣除，用扣除后的价格参加评审。

其评标价=投标报价*（1-10%）

5.3.2 对于联合协议或者分包意向协议约定监狱企业的合同份额占到合同总金额 30%以上的，对联合体或者大中型企业的报价给予 4%的扣除，用扣除后的价格参加评审。

其评标价=投标报价*（1-4%）

5.3.3 确认为监狱企业投标的，应当同时符合以下条件：

5.3.3.1 符合（财库〔2014〕68 号）文件相关规定。

5.3.3.2 投标时提供本单位生产的货物，或者提供其他监狱企业生产的货物。

5.3.3.3 投标人须提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

5.4 符合（财库〔2021〕19 号）文件规定的来自贫困地区提供农副产品的评标价计算规则：

5.4.1 在政府采购活动中，对于来自贫困地区提供农副产品的投标人，报价给予 5%的扣除，用扣除后的价格参加评审。

其评标价=投标报价*（1-5%）

5.4.2 确认为来自贫困地区提供农副产品的投标人，应当同时符合以下条件：

5.4.2.1 符合（财库〔2021〕19 号）文件相关规定，在 832 个国家级贫困县域内注册的企业、农民专业合作社、家庭农场等出产的农副产品。

5.4.2.2 投标时提供本单位生产的货物，或者提供其他贫困地区生产的货物。

5.4.2.3 投标人须提供相关证明文件。

5.5 符合节能产品文件规定的评标价计算规则：

5.5.1 投标货物涉及提供的所有投标产品进入“节能产品政府采购品目清单”（相关证书的颁发机构应来自《参与实施政府采购节能产品认证机构名录》）的，其评标价=投标报价*（1-3%）；（不是所有投标产品的不享受此项优惠）。

5.6 符合环境标志产品文件规定的评标价计算规则：

5.6.1 投标货物涉及提供的所有投标产品进入“环境标志产品政府采购

品目清单”（相关证书的颁发机构应来自《参与实施政府采购环境标志产品认证机构名录》）的，其评标价=投标报价*（1-3%）；（不是所有投标产品的不享受此项优惠）。

6、 中标人的确定

评标委员会对进入详细评审的投标人进行综合评分并作出排序，得分最高排名第一的投标人将被确认中标人。如果二个投标人得分相同时，取投标价格低者。

评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响服务质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；如果投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

评标因素	权值%	评价要素
价格	15 分	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。其他投标供应商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 符合政策性优惠的，按照招标文件中第五部分评标办法-第5条执行。
投标产品技术指标及功能评审内容	20 分	提供所投产品的主要技术指标相应的证明材料（包括但不限于产品资质、检测报告、官网功能截图、产品彩页等）须提供相应资料或截图证明加盖原厂公章，未提供者不得分。 依据各投标供应商主要技术指标、参数、性能等情况；全部满足参数要求得 20 分；技术参数“★”号项一项不满足扣 2 分，非“★”号项一项不满足扣 1 分，扣完为止。
项目响应方案	25 分	1、投标人对本项目的背景及整体设计思路的理解程度综合对比打分，从网络安全体系设计、产品部署方案、实施方案、运维方案、应急响应方案等方面进行描述，对项目需求分析思路清晰、理解透彻，计 6.1-10 分，对项目需求分析合理、理解较清楚，计 3.1-6 分；对项目需求分析思路不清、对项目理解欠缺，计 0-3 分； 2、投标人针对本项目的采购需求提供详细的安全咨询和解决方案，方案及所选用的产品先进、合理、完整，思路清晰，符合国家相关标准，完全满足项目需求及未来扩展整合计 3.1-5 分；比较了解项目情况，基本满足文件要求计 2.1-3 分；与采购需求出现偏差计 1-2 分，未响应不计分。 3、投标人针对本项目需求制定详细具体可行的售后服务方案，包括但不限于响应产品的保修时间、保修期内的保修内容与范围、项目交付采购人后出现故障的响应时间、解决故障时间、补救措施等，同时具有明确的售后服务承诺且符合采购人实际需求，对项目需求分析思路清晰、理解透彻，计 3.1-5 分，对项目需求分析合理、理解较清楚，

		计 2.1-3 分；对项目需求分析思路不清、对项目理解欠缺，计 0-2 分； 4、投标人针对本项目提供免费为使用单位进行技术指导及培训，并在投标文件中列出指导及培训的内容及方式，确保使用人员能够独立熟练操作、维护和正常使用，项目培训方案思路清晰、合理，计 3.1-5 分，项目培训方案较合理，计 2.1-3 分；项目培训方案思路不清，计 0-2 分；
人员配备	10 分	所投产品制造厂商项目保障人员中需具备针对本项目重要时期拟派遣的安全保障服务人员中具备 CISP-PTS（注册信息安全专业人员-注册渗透测试专家）资质人员，每提供 1 个得 2 分，不提供不得分，最高 10 分。 备注：须提供上述人员证书及近 6 个月在职社保证明，并加盖章原厂公章。
企业实力	25 分	本次网络安全产品主要产品为入侵防御、入侵检测、准入控制、上网行为管理、日志审计、堡垒机、漏洞扫描、网闸。 1、产品制造厂商需具备互联网安全研发中心和 OWASP 组织的应用安全联盟会员资格，并提供会员编号和相关资质证明；（具备一年得 1 分，具备三年得 3 分，具备五年得 5 分，不具备不得分。） 2、产品制造厂商具备信息安全等级保护关键技术国家工程实验室共建协议证明；（具备得 3 分，不具备不得分。） 3、产品制造厂商需具备 ITSS 运行维护符合性证书资质；（三级得 2 分，二级得 4.5 分，不具备不得分。） 4、产品制造厂商需具备以下资质，每个资质得 1.5 分，共 7.5 分。 （1）CCRC 信息安全服务资质一安全运维服务资质（一级）； （2）国测信息安全服务资质一风险评估类（二级）； （3）国测信息安全服务资质一安全工程类（三级） （4）CMMI 能力成熟度模型集成（五级） （5）CNCERT 网络安全应急服务支撑单位（国家级） 5、产品制造厂商具备公开发布的专门针对中国的 APT 攻击（高级可持续威胁攻击）事件研究报告或相关证明材料；（评标委员会根据提供报告数量与质量综合排名，第一名得 5 分；第二名得 3 分；第三名得 1 分；其它名次得 0.5；不提供不得分。） （备注：以上要求须提供资质证书复印件或证明材料并加盖原厂公章，未提供不得分。）

业绩	5 分	提供投标人的 2019 年 1 月 1 日至今同类项目业绩合同（以合同签订日期为准），每份计 1 分，满分 5 分，未提供者不得分。（投标文件须提供合同首页、金额所在页、签字盖章页并加盖投标人公章。）

第六部分 投标文件格式

西安市高陵区医院网络安全等级保护建设项目

项目编号：DXZB-2022-0631

投　标　文　件

投 标 单 位： _____

采购代理机构： _____

时　　间： _____

投标报价表、投标文件信封格式

请按以下内容填写投标报价表、投标文件信封抬头，并将黑框剪下，贴在投标报价表、投标文件信封外面，除非特殊情况，否则请不要更改信封格式：

投标文件 **正/副本**

致： 陕西德信招标有限公司

项目名称：

项目编号：

开标时间：

投标人名称： （盖章）

投标报价表和投标文件电子版 U 盘

致： 陕西德信招标有限公司

项目名称：

项目编号：

开标时间：

投标人名称： （盖章）

注：投标文件须密封完整，封口处加盖公章。

目　录

一、投标函

投　　标　　函

致：陕西德信招标有限公司

我方确认收到贵方提供_____*（项目编号）*_____*（项目名称）*招标文件的全部内容，我方：*（投标人名称）*作为投标者正式授权*（授权代表全名、职务）*代表我方进行有关本投标的一切事宜。

在此提交的投标文件，正本__份，副本__份，投标报价表、电子版U盘各一份。包括如下等内容：

（一）投标报价表；

（二）投标报价明细表；

（三）商务条款偏离表；

（四）技术规格偏离表；

（五）法定代表人证明书或授权书；

（六）资格证明文件；

（七）具有履行合同所必需的设备和专业技术能力的书面声明；

（八）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书面声明；

（九）陕西省政府采购供应商拒绝政府采购领域商业贿赂承诺书；

（十）中小企业声明函；

（十一） 残疾人福利性单位声明函；

（十二） 监狱企业证明文件；

（十三） “节能产品”、“环境标志产品”证明材料；

（十四） 项目业绩表；

（十五） 优惠、培训、售后服务承诺；

（十六） 技术服务方案；

（十七） 其他证明材料。

我方已完全明白招标文件的所有条款要求，并重申以下几点。

（一）我方决定参加：_____*（项目编号）*_____*（项目名称）*的投标。

（二）全部服务及有关货物、工程供应的投标总价为：_____（大、小写）。

（三）本投标文件的有效期在_____年___月___日至_____年___月___日有效，如中标，有效期将延至合同终止日为止。

（四）我方已详细研究了招标文件的所有内容包括修正文（如果有）和所有已提供的参考资料以及有关附件并完全明白，我方放弃在此方面提出含糊意见或误解的一切权力。

（五）我方明白并愿意在规定的开标时间和日期之后、投标有效期之内撤回投标，则投标保证金将被贵方没收。

（六）我方同意按照贵方可能提出的要求而提供与投标有关的任何其它数据或信息。

（七）我方理解贵方不一定接受最低标价或任何贵方可能收到的投标。

（八）我方如果中标，将保证履行招标文件及其补充文件中的全部责任和义务，按质、按量、按期完成《合同书》中的全部任务。

（九）如我方中标，我方将在收到中标通知书之前，参照国家计委〔2002〕1980 号、发改委〔2003〕857 号文件规定标准向陕西德信招标有限公司交纳中标服务费。

（十）所有与本招标有关的函件请发往下列地址：

投标人名称(加盖公章)：_____

联系地址：_____

投标人授权代表职务：_____

投标人授权代表签字：_____

联系电话：_____

电子邮件：_____

传 真：_____

日 期：_____

二、投标报价表

投标报价表

项目名称：_____

项目编号：_____

序号	服务/货物名称	规格型号（如有）	数量	单价(元)	投标总价(元)	服务商/制造商名称	交付期/服务期	备注
合计	（大写）：_____ （小写）：_____							

投标人（盖章、签字）：_____

日期：_____年_____月_____日

注： 此投标报价表应按“投标人须知”的规定密封标记密封**单独提交。**

投标报价应包括服务费用、验收、安装部署费用、调试费用、人员培训及投标等全部费用。

三、投标报价明细表

（投标人根据投标产品自行编制格式）

四、商务条款偏离表

〔说明〕供应商应根据其提供的服务，对照招标文件合同专用条款要求逐条响应，商务条款不可负偏离，否则视为无效投标。

项目名称：_____ 项目编号：_____

序号	招标文件要求	投标文件内容	偏离	备注

注：请对招标文件商务要求内容逐条响应。

投标人（公章）：_____

授权代表（签名或盖章）：_____

日期：_____

五、技术规格偏离表

〔说明〕技术偏离表不得直接复制粘贴招标文件技术参数要求，否则视为无效投标。技术偏离表响应内容须提供相关技术支持资料。

项目名称：_____ 项目编号：_____

序号	招标文件要求	投标文件内容	偏离	备注

注：请对招标文件采购内容及要求内容逐条响应。

投标人（公章）：_____

授权代表（签名或盖章）：_____

日期：_____

六、法定代表人证明书或授权书

（一）法定代表人证明书格式（投标人为法定代表人时须出具）

<table>
<tr><td colspan="5">致：陕西德信招标有限公司</td></tr>
<tr><td rowspan="5">企业法人</td><td>企 业 名 称</td><td colspan="3"></td></tr>
<tr><td>法 定 地 址</td><td colspan="3"></td></tr>
<tr><td>邮 政 编 码</td><td colspan="3"></td></tr>
<tr><td>网 址</td><td colspan="3"></td></tr>
<tr><td>统一社会信用代码</td><td colspan="3"></td></tr>
<tr><td rowspan="3">法定代表人</td><td>姓 名</td><td></td><td>性 别</td><td></td></tr>
<tr><td>职 务</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传 真</td><td colspan="3"></td></tr>
<tr><td rowspan="2">法定代表人身份复印件</td><td colspan="2" rowspan="2">二代身份证正、反两面

（粘贴处）</td><td colspan="2">（法定代表人签字）</td></tr>
<tr><td colspan="2">（企业公章）

年 月 日</td></tr>
</table>

（二）法定代表人授权书格式（投标人为授权代表时须出具）

致：陕西德信招标有限公司

本授权书声明：注册于_____（国家或地区）的_____（投标人名称）的在下面签字的_____（法定代表人姓名、职务）代表本公司授权在下面签字的_____（被授权人的姓名、职务）为本公司的合法代表人，就**陕西德信招标有限公司**（项目名称、项目编号为_____）招标文件的投标和合同执行，以我方的名义处理一切与之有关的事宜。

本授权书____年___月__日至____年___月__日签字生效，特此声明。

投标人名称：（公章）

地址：

法定代表人：（签名或盖章）

职务：

被授权人：（签名或盖章）

职务：

法人代表与被授权人身份证（复印件）需附在投标文件中。

被授权人需携带身份证原件至开标现场。

七、资格证明文件

1、具有独立承担民事责任能力的法人或非法人组织或自然人，提供合法有效的统一社会信用代码的营业执照等证明文件；

2、提供法定代表人授权委托书及被授权人身份证（投标人为法定代表人时，须提交法定代表人证明书）；

3、提供 2021 年审计报告（至少应包含资产负债表、利润表和现金流量表）或投标截止日前半年内任意一个月的的财务报表（至少应包含资产负债表、利润表和现金流量表）或银行出具的资信证明；（成立时间至提交响应文件截止时间不足三个月的可不提供）；

4、提供投标截止日前半年内任意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，成立不足一年的公司提供自成立后至今连续缴存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，单据或证明上应有社保机构或代收机构的公章或业务专用章；（成立时间至提交响应文件截止时间不足三个月的可不提供）；

5、提供投标截止日前半年内任意一个月的纳税证明或完税证明，单据应有代收机构或税务机关的公章或业务专用章；依法免税的单位应提供相关证明材料；（成立时间至提交响应文件截止时间不足三个月的可不提供）；

6、未被列入失信被执行人、税收违法黑名单、政府采购严重违法失信行为记录名单；以“信用中国”网站(www.creditchina.gov.cn)或中国政府采购网(www.ccgp.gov.cn) 查询结果为准；

八、具有履行合同所必需的设备和专业技术能力的书面声明

（格式自拟）

九、提供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书面声明

无重大违法记录声明

陕西德信招标有限公司：

我_____*（投标人名称）*以下简称“我公司”参加项目编号为_____*（项目编号）*_____*（项目名称）*的投标，本公司郑重声明，我公司参加本项目招标活动前___年内_____*（如实填写有或无）*重大违法记录，符合法律法规的有关规定，我公司对此声明负全部法律责任。

特此声明！

投标人名称：_____（公章）

_____年___月___日

十、陕西省政府采购供应商拒绝政府采购领域商业贿赂承诺书

为响应党中央、国务院关于治理政府采购领域商业贿赂行为的号召，我公司在此庄严承诺：

1、在参与政府采购活动中遵纪守法、诚信经营、公平竞标。

2、不向政府采购人、采购代理机构和政府采购评审专家进行任何形式的商业贿赂以谋取交易机会。

3、不向政府采购代理机构和采购人提供虚假资质文件或采用虚假应标方式参与政府采购市场竞争并谋取中标、成交。

4、不采取“围标、陪标”等商业欺诈手段获得政府采购定单。

5、不采取不正当手段诋毁、排挤其他供应商。

6、不在提供商品和服务时“偷梁换柱、以次充好”损害采购人的合法权益。

7、不与采购人、采购代理机构政府采购评审专家或其它供应商恶意串通，进行质疑和投诉，维护政府采购市场秩序。

8、尊重和接受政府采购监督管理部门的监督和政府采购代理机构招标采购要求，承担因违约行为给采购人造成的损失。

9、不发生其他有悖于政府采购公开、公平、公正和诚信原则的行为。

投标人名称：

公章：

授权代表签字：

十一、中小企业声明函（如有）

请各位投标商根据实际情况提供，没有则不提供。投标人声明函将随结果公告一同公布，接受社会监督。

本公司郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司参加*（单位名称）*的*（项目名称）*采购活动，服务全部由符合政策要求的中小企业承接相关企业的具体情况如下：

1.*（标的名称）*，属于*（采购文件中明确的所属行业）*；承接企业为*（企业名称）*，从业人员____人，营业收入为____万元，资产总额为__万元，属于*（中型企业、小型企业、微型企业）*；

2.*（标的名称）*，属于*（采购文件中明确的所属行业）*；承接企业为*（企业名称）*，从业人员____人，营业收入为____万元，资产总额为___万元，属于*（中型企业、小型企业、微型企业）*；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日　　期：

1.从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

2.填写前请认真阅读《工业和信息化部　国家统计局　国家发展和改革委员会　财政部关于印发中小企业划型标准规定的通知》(工信部联企业（2011）300 号)和《财政部、工业和信息化部关于印发〈政府采购促进中小企业发展管理办法〉的通知》（财库〔2020〕46 号）相关规定。

十二、残疾人福利性单位声明函（如有）

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，由供应商自行申明，并对申明真实性负责。如有虚假，将依法承担相应责任。

本单位郑重声明，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，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供服务。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日　　期：

十三、监狱企业证明文件（如有）

根据财政部、司法部《关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）的规定，监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

单位名称（盖章）：

日　　期：

十四、“节能产品”、“环境标志产品”证明材料（如有）

供应商提供的产品属于下列情形的，提供产品列入“节能产品”、“环境标志产品”所在页的复印件（该页包含制造商或企业名称或申请单位名称、规格型号、有效期截止日期等内容），并加盖供应商单位公章。

（1）符合政府采购强制采购政策的财政部、环境保护部发布的《节能产品政府采购清单》中标记的“强制采购节能产品”。

（2）符合政府采购强制采购政策的财政部、环境保护部发布的《环境标志产品政府采购清单》中标记的的“环境标志产品”。

注：本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日　　期：

十五、项目业绩表

2019年1月1日至今同类项目业绩合同（以合同签订日期为准）

序号	项目名称	项目地址及电话	合同内容	签订日期

注：须提供合同首页、金额所在页、签字盖章页并加盖投标人公章。

十六、优惠、培训、售后服务承诺

16.1 优惠条件承诺书

致：

经仔细阅读你们的招标文件，我们同意招标文件中有关优惠条件的要求，对所投标项目向贵单位特作如下优惠条件承诺：

（1）…

（2）…

（3）…

…

特此承诺！

承诺方授权代表签字：_____

职　　务：_____

承诺方名称：_____

承诺方印章：_____

地址：_____

邮编：_____

电话：_____

传真：_____

日期：　　年　　月　　日

16.2 培训计划承诺

致：

经仔细阅读你们的招标文件，我们同意招标文件中有关培训计划的要求，对所投标项目向贵单位特作如下培训计划承诺：

（1）…

（2）…

（3）…

…

特此承诺！

承诺方授权代表签字：_____

职　　务：_____

承诺方名称：_____

承诺方印章：_____

地址：_____

邮编：_____

电话：_____

传真：_____

日期：　　年　　月　　日

16.3 售后服务承诺

报价人应详细说明售后服务保证内容，备品备件供应情况，出现故障响应时间及售后服务人员情况，并填写下表：

售后服务承诺

投标人（电话、地址、联系人）
现行售后服务的主要内容：（可附宣传材料）
售后服务技术人员简历：（姓名，性别，年龄，身份证号，学历，毕业院校，专业，联系电话，资格或培训证明，从事与本次采购相关项目的售后服务技术工作经历）

特此承诺!

承诺方授权代表签字：_____

职　　务：_____

承诺方名称（公章）：_____

日期：　　年　　月　　日

十七、技术服务方案

十八、其他证明材料