

# 新疆生产建设兵团 政府采购

## 招标文件 (答疑澄清文件) (货物类)

项目名称：第六师自然资源和规划局系统网络安全三级等保  
测评及整改项目（安全设备三级升级改造和密码  
安全防护）

项目编号：XJJY-[2023]政采云 003-02

采购代理机构：新疆建友友成工程管理咨询有限公司

日期：2023 年 03 月

# 目 录

第一部分 招标公告 .....	4
一、项目基本情况 .....	4
二、申请人的资格要求: .....	5
三、获取招标文件 .....	8
四、提交投标文件截止时间、开标时间和地点 .....	8
五、公告期限 .....	8
六、其他补充事宜 .....	8
七、对本次采购提出询问, 请按以下方式联系 .....	9
第二部分 投标人须知 .....	11
第三部分 采购需求 .....	47
一、要求 .....	47
二、设备清单 .....	48
三、具体参数要求 .....	51
(一) 政务外网设备要求 .....	51
(二) 专网设备要求 .....	79
(三) 互联网设备要求 .....	85
二、商务、服务要求 .....	102
1. 售后服务要求: .....	102
2. 交货期、交货地点及验收方式 .....	103
▲3、报价要求 (投标报价应包含完成招标文件规定的招标范围全部内容所需的全部费用) .....	106
4、付款方式 .....	106
▲5、知识产权 .....	106
6、附件、图纸 (若有) 及包装要求 .....	107
7、处罚条例: 签订合同时拟定 .....	107
第四部分 评审方法 (综合评分法) .....	108
第五部分 政府采购合同 .....	117
第六部分 投标文件格式 .....	123
招标文件确认书 .....	144
四、技术文件 .....	145
(一) 投标人自行编写的技术文件 .....	146
五、服务文件 .....	148
(一) 投标人自行编写的服务文件 .....	149
附件 1: .....	150

# 第一部分 招标公告

## 第六师自然资源和规划局系统网络安全三级等保测评及整改项目 (安全设备三级升级改造和密码安全防护)

### 项目概况

第六师自然资源和规划局系统网络安全三级等保测评及整改项目(安全设备三级升级改造和密码安全防护)的潜在投标人应在政采云平台 <https://www.zcygov.cn/> 获取采购文件,并于 2023年04月12日10:40 (北京时间)前提交响应文件。

### 一、项目基本情况

- 1、项目编号: XJJY-[2023]政采云 003-02
- 2、项目名称: 第六师自然资源和规划局系统网络安全三级等保测评及整改项目(安全设备三级升级改造和密码安全防护)
- 3、采购方式: 公开招标
- 4、预算金额(元): ¥5432591.00 元
- 5、货物需求: 安全设备三级升级改造和密码安全防护  
(详见招标文件“第三部分采购需求”)
- 6、合同履行期限: 签订合同后。按招标人要求所有设备 30 日历天内完成安装调试、培训、验收等。此次项目不另追加任何费用,中标人不得以任何理由,提出任何形式的增加合同价款或增加资金的要求。中标人规划并完成项目所需要用到的对接文档和接口协议,自行协调,若有费用需自行承担。
- 7、本项目不接受联合体投标。

## 二、申请人的资格要求：

### 1. 满足《中华人民共和国政府采购法》第二十二条规定：

(1) 具有独立承担民事责任的能力。①供应商法人营业执照（副本）或事业单位法人证书（副本）或个体工商户营业执照或有效的自然人身份证明，组织机构代码证扫描件（供应商按“三证合一”登记制度办理营业执照的，组织机构代码证和税务登记证（副本）以供应商所提供的营业执照（副本）扫描件为准）；②供应商法定代表人身份证明和法定代表人授权代表委托书扫描件。

(2) 具有良好的商业信誉和健全的财务会计制度。①提供审计机构或会计师事务所出具的上一年度（2022 年度或 2021 年度）财务审计报告（报告中须包括资产负债表、利润表、现金流量表及财务报表附注）的原件扫描件；②如供应商无法提供上年度审计报告，则需提供开户银行递交响应文件截止时间前三个月内基本账户银行出具的资信证明的原件扫描件，银行资信证明应能说明该供应商与银行之间业务往来正常，无不良记录，企业信誉良好等；③银行出具的存款证明不能作为银行资信证明；④新成立不满一年的供应商可不提供财务审计报告，只需提供财务报表即可。

(3) 具有履行合同所必需的设备和专业技术能力。提供具有履行合同所必需的设备和专业技术能力相关证明或提供具有履行合同所必需的设备和专业技术能力的承诺。

(4) 有依法缴纳税收和社会保障资金的良好记录。①提供（递交响应文件截止时间前）近 6 个月内任意 1 个月的缴纳税收的凭据证明

材料扫描件及缴纳社会保险的凭据证明材料扫描件；②新成立不满一个月的企业仅提供依法缴纳税收承诺书和依法缴纳社会保障资金承诺函即可；③如依法免税或依法不需要缴纳社会保障资金的，应提供的相应文件证明其依法免税或依法不需要缴纳社会保障资金。

(5) 参加政府采购活动前三年内，在经营活动中没有重大违法记录。①提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明，在开标日资格审查时由招标人或采购代理机构现场查询，供应商不能是被列入“信用中国”([www.creditchina.gov.cn](http://www.creditchina.gov.cn))严重失信主体名单；②不能是被列入“中国政府采购网”

([www.ccgp.gov.cn](http://www.ccgp.gov.cn)) 政府采购严重违法失信行为记录名单中仍在处罚期的，将拒绝其参加本次政府采购活动；③提供国家企业信用信息公示系统(<http://www.gsxt.gov.cn>)公示的基础信息、行政处罚信息、列入经营异常名录信息、列入严重违法失信名单(黑名单)信息、公告信息等查询记录。

(6) 法律、行政法规规定的其他条件。①投标文件是否含有招标人不能接受的附加条件；②是否违反国家法律、法规和采购文件规定的其他无效情形；③未与其他投标人串通投标，或者与招标人串通投标。

2. 落实政府采购政策需满足的条件：无

3. 采购项目需要落实的政府采购政策：(中小企业优惠、监狱企业、节能产品、环境标志产品等)

(1) 鼓励节能政策：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）、财政部、发展改革委《关于印发节能产品政府采购品目清单的通知》（财库【2019】19号）、《市场监管总局关于发布参与实施政府采购节能、环境标志产品认证机构名录的公告》（2019年第16号）；

（2）鼓励环保政策：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）、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）、《市场监管总局关于发布参与实施政府采购节能、环境标志产品认证机构名录的公告》（2019年第16号）；

（3）财政部、工业和信息化部文件关于印发《政府采购促进中小企业发展管理办法》（财库[2020]46号文）；

（4）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）；

（5）财政部、民政部、中国残疾人联合会文件《关于促进残疾人就业政府采购政策的通知》（财库[2017]141号）；监狱企业、残疾人福利性单位视同小型、微型企业，享受小型、微型企业评审中价格扣除的政府采购政策。

4. 本项目的特定资格要求：无

5. 其他要求：（1）单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同项下的政府采购活动。除单一

来源采购项目外,为采购项目提供整体设计、规范编制或者项目管理、  
监理、检测等服务的投标人,不得再参加该采购项目的其他采购活动。

(2) 投标保证金: ¥100000.00

### 三、获取招标文件

1、时间: 2023年03月14日到2023年03月21日(北京时间,法定节假日除外)

2、地点: 政采云平台 <https://www.zcygov.cn/>

3、方式: 供应商登录政采云平台 <https://www.zcygov.cn/>在线申请获取采购文件(进入“项目采购”应用,在获取采购文件菜单中选择项目,申请获取采购文件)

### 四、提交投标文件截止时间、开标时间和地点

1、提交投标文件截止时间: 2023年04月12日 10:40(北京时间)

2、投标地点: 政采云平台 <https://www.zcygov.cn/>

3、开标时间: 2023年04月12日 10:40(北京时间)

4、开标地点: 政采云平台 <https://www.zcygov.cn/>(不见面开标大厅)

### 五、公告期限

自本公告发布之日起不少于5个工作日。

### 六、其他补充事宜

1、本项目实行网上投标,采用电子投标文件。

2、各投标人应在开标前应确保成为政采云平台供应商,并完成CA

数字证书（符合国密标准）申领。因未注册入库、未办理 CA 数字证书等原因造成无法投标或投标失败等后果由投标人自行承担。有意向参与兵团区划电子开评标投标人，可访问新疆数字证书认证中心官方网站（<https://www.xjca.com.cn/>）或下载“新疆政务通”APP 自行进行申领。如需咨询，请联系新疆 CA 服务热线 0991-2819290。

3、投标人将政采云电子交易客户端下载、安装完成后，可通过账号密码或 CA 登录客户端进行投标文件的制作。在使用政采云投标客户端时，建议使用 WIN7 及以上操作系统。客户端请至新疆兵团政府采购网（<http://ccgp-bingtuan.gov.cn/>）下载专区查看，如有问题可拨打政采云客户服务热线 400-881-7190 进行咨询。如因投标人自身原因导致在规定时间内无法正常解密、签章等的（如：浏览器故障、未安装相关驱动、网络故障、CA 未绑定、加密 CA 与解密 CA 不一致等），代理机构不予异常处理，视为投标人自动弃标。

## 七、对本次采购提出询问，请按以下方式联系

### 1. 招标人信息

名称：新疆生产建设兵团第六师自然资源和规划局

地址：新疆五家渠市猛进北路 1699 号

联系人：程建军

电话：0994-5828151

### 2. 采购代理机构信息

名称：新疆建友友成工程管理咨询有限公司

地 址：五家渠长征东街青湖尚城小区 3 号商铺门面 A4-B4 部分

项目联系人：骆玉津

电 话：0994-5885765

### 3. 项目负责人联系方式

项目联系人：骆玉津

电 话：0994-5885765

新疆建友友成工程管理咨询有限公司

## 第二部分 投标人须知

序号	内容	说明与要求
1	项目名称	第六师自然资源和规划局系统网络安全三级等保测评及整改项目（安全设备三级升级改造和密码安全防护）
2	招标人	<p>名称：新疆生产建设兵团第六师自然资源和规划局</p> <p>地址：新疆五家渠市猛进北路 1699 号</p> <p>联系人：程建军</p> <p>联系电话：0994-5802539</p>
3	采购代理机构	<p>名称：新疆建友友成工程管理咨询有限公司</p> <p>地址：新疆五家渠二十四区长征东街 1659 号青湖尚城三号商铺 A4—B4 部分</p> <p>联系人：骆玉津</p> <p>联系电话：0994-5885765</p> <p>电子邮件：2122415327@qq.com</p>
4	采购内容	<p>安全设备三级升级改造和密码安全防护</p> <p>（详见招标文件“第三部分采购需求”）</p>
5	投标人资格要求	满足《中华人民共和国政府采购法》第二十二条规定应当具备的条件和特定资格条件
6	投标文件封	投标文件封面；

	<p>的组成部分</p>	<p>面</p> <p>1. 满足《中华人民共和国政府采购法》第二十二条规定：</p> <p>（1）具有独立承担民事责任的能力。①供应商法人营业执照（副本）或事业单位法人证书（副本）或个体工商户营业执照或有效的自然人身份证明，组织机构代码证扫描件（供应商按“三证合一”登记制度办理营业执照的，组织机构代码证和税务登记证（副本）以供应商所提供的营业执照（副本）扫描件为准）；②供应商法定代表人身份证明和法定代表人授权代表委托书扫描件。</p> <p>（2）具有良好的商业信誉和健全的财务会计制度。①提供审计机构或会计师事务所出具的上一年度（2022年度或2021年度）财务审计报告（报告中须包括资产负债表、利润表、现金流量表及财务报表附注）的原件扫描件；②如供应商无法提供上年度审计报告，则需提供开户银行递交响应文件截止时间前三个月内基本账户银行出具的资信证明的原件扫描件，银行资信证明应能说明该供应商与银行之间业务往来正常，无不良记录，企业信誉良好等；③银行出具的存款证明不能作为银行资信证明；④新成立不满一年的供应商可不提供财务审计报告，只需提供财务报表即可。</p> <p>（3）具有履行合同所必需的设备和专业技术能力。提</p>
--	--------------	---

		<p>供具有履行合同所必需的设备和专业技术能力相关证明或提供具有履行合同所必需的设备和专业技术能力的承诺。</p> <p>(4) 有依法缴纳税收和社会保障资金的良好记录。①提供（递交响应文件截止时间前）近6个月内任意1个月的缴纳税收的凭据证明材料扫描件及缴纳社会保险的凭据证明材料扫描件；②新成立不满一个月的企业仅提供依法缴纳税收承诺书和依法缴纳社会保障资金承诺函即可；③如依法免税或依法不需要缴纳社会保障资金的，应提供的相应文件证明其依法免税或依法不需要缴纳社会保障资金。</p> <p>(5) 参加政府采购活动前三年内，在经营活动中没有重大违法记录。①提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明，在开标日资格审查时由招标人或采购代理机构现场查询，供应商不能是被列入“信用中国”(<a href="http://www.creditchina.gov.cn">www.creditchina.gov.cn</a>)失信被执行人、重大税收违法案件当事人名单的供应商；②不能是被列入“中国政府采购网”(<a href="http://www.ccgp.gov.cn">www.ccgp.gov.cn</a>)政府采购严重违法失信行为记录名单中仍在处罚期的，将拒绝其参加本次政府采购活动；③提供国家企业信用信息公示系统(<a href="http://www.gsxt.gov.cn">http://www.gsxt.gov.cn</a>)公示的基础信息、行政处罚信息、列入经营异常名录信息、列入严</p>
--	--	---

		<p>重违法失信名单(黑名单)信息、公告信息等查询记录。</p> <p>(6) 法律、行政法规规定的其他条件。①投标文件是否含有招标人不能接受的附加条件;②是否违反国家法律、法规和采购文件规定的其他无效情形;③未与其他投标人串通投标,或者与招标人串通投标。</p> <p>2、落实政府采购政策需满足的资格要求: 无</p> <p>3、特定资质: 无</p> <p>4、其他要求: (1) 单位负责人为同一人或者存在直接控股、管理关系的不同投标人,不得参加同一合同项下的政府采购活动。除单一来源采购项目外,为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人,不得再参加该采购项目的其他采购活动。(2) 投标保证金证明(¥100000.00元)</p>
	<p>商务文件</p>	<p>☆投标函;</p> <p>☆开标一览表;</p> <p>☆投标报价明细表;</p> <p>☆售后服务承诺书;</p> <p>☆商务条款偏离说明表;</p> <p>投标人认为有必要提供的声明及文件资料;</p> <p>其他: /</p>
	<p>技术</p>	<p>投标人自行编写的技术文件:</p> <p>①货物主要技术指标和运行性能:</p>

		<p>文 件</p> <p>&lt;1&gt;☆技术明细表（详细描述货物技术指标及性能，包括采用的新工艺、新技术、新材料等）；</p> <p>&lt;2&gt;同货物型号一致的产品手册、彩页、说明书等技术文件(包括但不限于招标文件中要求提供的投标产品样本、使用保养说明书、图纸以及产品检测报告和认定证书等技术资料)；</p> <p>&lt;3&gt;☆货物技术规范偏离表；</p> <p>②货物配件、耗材、选件表和备件及特殊工具清单；</p> <p>③货物安装方案及验收标准；</p> <p>④质量保证措施和保证交货期措施；</p> <p>投标人认为有必要提供的声明及文件资料；</p> <p>其他： /</p>
7	是否允许联合体投标	<input checked="" type="checkbox"/> 否。
8	是否允许投报进口产品	<input checked="" type="checkbox"/> 否。
9	是否允许投标人将项目非主体、非关键性工作交由他人完成	<input checked="" type="checkbox"/> 否。
10	答疑接受时间	1、供应商认为采购文件、采购过程、中标或者成交结

果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向招标人、采购代理机构提出质疑。要求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，超过时间的质疑将不予接受。

接收部门：新疆建友友成工程管理咨询有限公司

联系人：骆玉津

联系电话：0994-5885765

提交方式：将投标人疑文件电子版（须为可编辑的WORD文档）与盖章的纸质版扫描件PDF版本发送至

2122415327@qq.com；如WORD文档内容与盖章的纸质版扫描件PDF内容不一致的，以盖章的纸质版扫描件PDF内容为准。

2、澄清、修改文件发出后（若有），投标人必须使用最新的澄清文件制作电子投标文件。

注：1、质疑函格式须按照《政府采购质疑和投诉办法》中华人民共和国财政部令第94号第十二条供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

（一）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（二）质疑项目的名称、编号；

- (三)具体、明确的质疑事项和与质疑事项相关的请求;
- (四) 事实依据;
- (五) 必要的法律依据;
- (六) 提出质疑的日期。

供应商为自然人的,应当由本人签字;供应商为法人或者其他组织的,应当由法定代表人、主要负责人,或者其授权代表签字或者盖章,并加盖公章。

依据:《中华人民共和国政府采购法实施条例》第五十三条政府采购法第五十二条规定的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。

《政府采购质疑和投诉办法》第十条供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的,可以在知道或者应知其权益受到损害之日起7个工作日内,以书面形式向招标人、采购代理机构提出质疑。采购文件可以要求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。第十一条提出质疑的供应商(以下简称质疑供应商)应当是参与所质疑项目采购活动的供应商。潜在供应商已依法获取其可质疑的

		采购文件的, 可以对该文件提出质疑。对采购文件提出质疑的, 应当在获取采购文件或者采购文件公告期限届满之日起7个工作日内提出。
11	投标有效期	自投标截止之日起 90 日历天。
12	投标截止时间 (开标时间)	截止时间: 2023 年 04 月 12 日 10: 40 (北京时间)
13	投标人在投标 截止时间前递 交的文件	投标文件 (具体要求见本表第 14 项)
14	投标文件份数	<p>采用网上不见面开标:</p> <p>1、本项目采用网上开标、投标人需要递交电子投标文件, 加密的电子投标文件, 在投标截止时间前通过政采云平台上传到指定位置。</p> <p>2、本项目采用远程不见面交易的模式。开标当日, 投标人无需到达开标现场, 仅需在任意地点通过网上开标系统 (登录地址详见网站操作手册) 完成远程解密、提疑澄清、开标唱标、结果公布等交互环节。投标人必须使用能正确解密投标文件的“CA 锁”在规定的时间内完成远程解密, 因投标人原因未能解密、解密失败或解密超时, 视为投标人撤销其投标文件, 系统内投标文件将被退回; 因招标人原因或网上招投标平台发生故障, 导致无法按时完成投标文件解密或开、评标工作无法进</p>

		<p>行的，可根据实际情况相应调整开、评标时间。</p> <p>3. 远程开标前，投标人务必在政采云平台 <a href="https://www.zcygov.cn/">https://www.zcygov.cn/</a> 查看。</p> <p>评标结束后，中标单位需提供壹正贰副的纸质版投标文件（需盖公章、法人章）</p>
15	开标时间及地点	<p>开标时间：<u>2023年04月12日10:40</u>（北京时间）</p> <p>开标地点：网上开标大厅，政采云平台 <a href="https://www.zcygov.cn/">https://www.zcygov.cn/</a>。（不见面开标大厅）</p> <p>网上开标默认解密时长：<b>20分钟</b>。</p> <p>投标人对报价开标记录表或报价开启程序确认，进行电子签章默认时长：<b>20分钟</b>。</p> <p>如解密过程中出现异常状况需经招标人允许投标单位才能将备份上传。</p>
16	评标委员会的组成	<p>评标委员会构成 <u>5</u> 人，其中招标人代表人 <u>1</u></p> <p>评委确定方式：<u>政采云平台专家库抽取</u></p>
17	投标保证金	<p>1、缴纳方式：<u>缴纳方式：电汇、网银转账、支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式交纳</u></p> <p>投标保证金的金额：<b>¥100000.00元</b></p> <p>收款单位：<b>五家渠建友工程管理咨询服务部</b></p> <p>开户银行：<b>五家渠国民村镇银行有限责任公司</b></p> <p>银行账号：<b>60222101303007901</b></p>

		<p>行 号：320885800018</p> <p>到账截止时间：<u>2023年04月12日10:40</u>之前（北京时间）</p> <p>注：（1）投标保证金以网银转账的形式由投标人的账户汇出（个体工商户除外），并汇入至招标代理公司保证金账户。</p> <p>（2）采用银行保函缴纳的，应出具保函的银行级别（应为国有商业银行或股份制商业银行的支行及其以上的银行）及保承的有效期。如有问题请联系400-903-9583，政采云金融管理人员。</p> <p>（3）投标人需自行评估因异地、跨行、公休日等因素造成的投标保证金到账延迟风险。投标保证金以汇入我公司账户时间为准。</p> <p>（4）将保证金电子凭证加盖公章附至投标文件中。</p> <p>以上情况导致否决投标，投标人自行承担责任。</p> <p>（5）退还保证金申请：供应商将单位名称、项目名称、金额、开户行信息发至我公司邮箱 2122415327@qq.com（具体详见附件，退保证金申请函）</p>
18	中小微型企业有关政策	<p>1、本项目非专门面向中小企业采购；</p> <p>2、本次采购所属行业为：软件和信息技术服务业</p> <p>（1）中小企业划分标准根据《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）</p>

		<p>执行，给予小型和微型企业产品或服务的价格给予10-20%的扣除，用扣除后的价格参与评审（监狱企业、残疾人福利性质单位视同为小微企业）。</p> <p>(2) 监狱企业、残疾人福利性单位视同为小、微企业。</p> <p>(3) 价格扣除办法:本项目对小型和微型企业货物的价格给予10%的扣除,用扣除后的价格参与价格分的评审。</p> <p>(4) 供应商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。</p> <p>2、投标人应出具采购文件中要求的《中小企业声明函》，否则评审时不予认可。</p> <p>说明：供应商应当对《中小企业声明函》、监狱企业证明文件、《残疾人福利性单位声明函》的真实性负责，上述材料与事实不符的，依照《政府采购法》第七十七条第一款的规定，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任。</p>
19	<p>技术部分是否采用“暗标”评</p>	<p><input checked="" type="checkbox"/> 否。</p>

	审方式	
20	评审方法	<p><input checked="" type="checkbox"/>资格后审                      <input checked="" type="checkbox"/>综合评分法</p> <p>注：综合评分法是指在最大限度地满足招标文件实质性要求前提下，按照招标文件中规定的评分细则评审后，以评标最终最高得分的投标人作为中标人的评标方法。每一投标人的最终得分为所有评委评分的算术平均值。得分相同的，报价较低的一方为中标人。得分且投标报价相同的，技术指标较优的一方为中标人。</p> <p>使用综合评分法的招标项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由招标人或者招标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，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。</p> <p>非单一产品招标项目，招标人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前款规定处理。</p>
21	履约保证金	<p>为保证成交供应商设备质量，采购文件要求成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或</p>

		者金融机构、担保机构出具的保函等非现金形式提交。
		交纳时间：签订合同后与招标人协商
		交纳金额：合同价的 10%
		收款单位：签订合同后与采购方协商 开户银行：签订合同后与采购方协商 银行账号：签订合同后与采购方协商
		项目完成验收合格无质量问题后退还。
22	代理服务费	<input checked="" type="checkbox"/> 交纳。（中标人支付） 交纳时间：领取中标通知书前 交纳金额：代理服务收费标准：本项目服务费按照差额定律累进计费方式计算，标准如下： 中标金额 100 万元以下的部分，货物类采购费率 1.50%， 中标金额 100 万元至 500 万元的部分，货物类采购费率 1.1%， 成交金额 500 万元至 1000 万元的部分，货物类采购费 0.8%。 收款单位： <u>五家渠建友工程管理咨询服务部</u> 开户银行： <u>中国农业银行股份有限公司五家渠青湖支行</u> 银行账号： <u>30716101040003098</u>
23	场地服务费	<input checked="" type="checkbox"/> 不交纳。
24	付款途径	转帐
25	付款方式	签订合同后，货物到达现场及系统安装后支付合同价的 10%，培训、实施、试运行正常且验收合格后甲方向乙

		方支付合同总额的 90%，质保条款按合同约定。（具体以签订合同为准）
26	交付日期	签订合同后。按招标人要求所有设备 30 日历天内完成安装调试、培训、验收等。此次项目不另追加任何费用，中标人不得以任何理由，提出任何形式的增加合同价款或增加资金的要求。中标人规划并完成项目所需要用到的对接文档和接口协议，自行协调，若有费用需自行承担。
27	实施地点	招标人指定地点
28	质保期	质保期三年
29	争议的解决	无
30	是否需要 递交样品	<input checked="" type="checkbox"/> 不需要
31	项目预算 (最高限价)	¥5432591.00。 大写：伍佰肆拾叁万贰仟伍佰玖拾壹元。 注：投标报价超过采购预算的否决投标
32	产品演示	<input checked="" type="checkbox"/> 需要 演示要求：根据招标文件要求需要产品演示，请各投标单位在递交投标文件截止时间（2023年04月12日10:40分）后10分钟内（2023年04月12日10:50分），将自己单位录制的演示视频（视频演示材料需要逐项进行视屏演示，时间控制在10分钟内，专家通过视频演

		示优劣进行评审) 发至代理公司邮箱号: 2122415327@qq.com。(必须注明单位名称) 评标时按递交视频文件顺序依次播放。
33	其他	在评标过程中, 投标人报价低于采购预算50%或者低于其他有效投标人报价算术均价40%, 有可能影响产品质量或者不能诚信履约的, 评标委员会应当要求其在评标现场合理的时间内提供质询, 需投标人确定并承诺后果。投标人书面说明应当按照国家财务会计制度的规定要求, 逐项就投标人提供的主营业务成本(应根据投标人企业类型予以区别)、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。投标单位回复说明应当签章, 否则无效。投标人回复后, 评标委员会应当结合采购项目采购需求、专业实际情况进行审查评价。投标人拒绝或者变相拒绝提供有效文件或者不能证明其报价合理性的, 评标委员会应当将其投标文件作为无效处理。
34	招标人补充的其他内容	逾期未上传的或者未上传至指定地点的投标文件, 招标人不予受理。 具体操作流程请各投标人在政采云平台下载中心下载《操作手册(投标人)》及网上开标流程视频学习。

## 投标人须知正文部分

### 一、总则

#### 1. 说明

1.1 本招标文件适用于本次招标采购项目的招标投标。

#### 2. 定义

2.1 “招标人”：新疆生产建设兵团第六师自然资源和规划局

2.2 “采购代理机构”：新疆建友友成工程管理咨询有限公司

2.3 “招标货物”指招标文件第三部分所述所有货物；“服务”指招标文件第三部分所述投标人应该履行的承诺和义务。

2.4 “潜在投标人”指符合招标文件各项规定的投标人。

2.5 “投标人”指满足《中华人民共和国政府采购法》第二十二条规定及特定资格的投标人。

2.6 “投标人公章”是投标文件中指与投标人标准公章一致

#### 3. 合格投标人的条件

3.1 具有本项目生产、生产厂、供应或实施能力，符合、承认并承诺履行本文件各项规定的国内法人、其他组织或自然人均可参加投标。

3.2 遵守有关的国家法律、法规和条例，具备《中华人民共和国政府采购法》和本文件中规定的条件：

- 1) 具有独立承担民事责任的能力；
- 2) 具有良好的商业信誉和健全的财务会计制度；
- 3) 具有履行合同所必需的设备和专业技术能力；

- 4) 具有依法缴纳税收和社会保障资金的良好记录；
- 5) 参加政府采购活动前三年内，在经营活动中没有重大违法记录；
- 6) 法律、行政法规规定的其他条件；
- 7) 具有本招标文件第二部分“投标人须知前附表”中规定的资格条件。

3.3 投标人之间如果存在下列情形之一的，不得同时参加同一包（标段）或者不分包（标段）的同一项目投标：

- 3.3.1 法定代表人为同一个人的两个及两个以上法人；
  - 3.3.2 母公司、全资子公司及其控股公司；
  - 3.3.3 参加投标的其他组织之间存在特殊的利害关系的；
  - 3.3.4 法律和行政法规规定的其他情形。
- 3.4 投标人须持有《法定代表人授权委托书》。
- 3.5 投标人按时足额交纳投标保证金。

#### 4. 投标费用

- 4.1 投标人应承担所有与准备和参加投标有关的费用。

#### 5. 纪律

- 5.1 投标人的投标行为应遵守中国的有关法律、法规和规章。
- 5.2 投标人不得相互串通投标报价，不得妨碍其他投标人的公平竞争，不得损害招标人或其他投标人的合法权益，投标人不得以向招标人、评标委员会成员行贿或者采取其他不正当手段谋取中标。

- 5.2.1 有下列情形之一的，属于投标人相互串通投标：

- 5.2.1.1 投标人之间协商投标报价等投标文件的实质性内容；
  - 5.2.1.2 投标人之间约定中标人；
  - 5.2.1.3 投标人之间约定部分投标人放弃投标或者中标；
  - 5.2.1.4 属于同一集团、协会、商会等组织成员的投标人按照该组织要求协同投标；
  - 5.2.1.5 投标人之间为谋取中标或者排斥特定投标人而采取的其他联合行动。
- 5.2.2 有下列情形之一的，视为投标人相互串通投标：
    - 5.2.2.1 不同投标人的投标文件由同一单位或者个人编制；
    - 5.2.2.2 不同投标人委托同一单位或者个人办理投标事宜
    - 5.2.2.3 不同投标人的投标文件载明的项目管理成员为同一人；
    - 5.2.2.4 不同投标人的投标文件异常一致或者投标报价呈规律性差异；
    - 5.2.2.5 不同投标人的投标文件相互混装；
    - 5.2.2.6 不同投标人的投标保证金从同一单位或者个人的账户转出。

## 6. 通知

6.1 对与本项目有关的通知，采购代理机构将以书面（包括书面材料、信函、传真等，下同）或在本次招标公告刊登的媒体上发布公告并在兵团政采云网平台内发送变更通知及/或答疑文件的形式，向潜在投标人发出，传真和电话号码以潜在投标人的登记为准。收到通知的投标人须立即予以回复确认，但投标人未回复或采购代理机构未

收到回复时，并不应当被理解为采购代理机构知道或应当知道投标人是否收到通知。因登记有误、传真线路故障或其它任何意外情形，导致所发出的通知延迟送达或无法到达投标人，采购代理机构不因此承担任何责任，有关的招标活动可以继续有效地进行。

## 二、招标文件

### 7. 招标文件组成

7.1 招标文件由招标文件目录所列内容组成。

### 8. 踏勘现场

8.1 本项目不组织踏勘（投标单位如有需要可自行踏勘）

### 9. 知识产权

9.1 投标人须保证，招标人在中华人民共和国境内使用投标生活物资、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，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或经济纠纷。如投标人不拥有相应的知识产权，则在投标报价中必须包括合法获取该知识产权的一切相关费用。如因此导致招标人损失的，投标人须承担全部赔偿责任。

9.2 投标人如欲在项目实施过程中采用自有知识成果，须在投标文件中声明，并提供相关知识产权证明文件。使用该知识成果后，投标人须提供开发接口和开发手册等技术文档。

### 10. 答疑及招标文件的澄清和修改

10.1 投标人如果对招标文件有疑问或要求进行澄清的，应按照招标文件第二部分“投标人须知前附表”规定向采购代理机构提出。

提出后，请投标人及时查看答疑文件或澄清文件。必要时，采购代理机构将组织相关专家召开答疑会，如召开，答疑会安排另行通知。

投标人在规定的时间内未对招标文件提出疑问或要求澄清的，采购代理机构将视其为同意，对在“答疑接受时间”后就招标文件内容提出的疑问及澄清要求将不予受理。

10.2 无论出于何种原因，采购代理机构主动或出于解答投标人疑问对已发出的招标文件进行必要澄清或修改的，应当在招标文件要求提交投标文件截止时间 15 日前，以当面交接、邮寄、传真或电子邮件、网站披露等其中至少一种方式，向潜在投标人发出澄清、修改的补充文件。需要为此调整投标文件提交截止时间的，应当重新确定，并就变更后的投标截止时间重新发出通知。

特殊情况下，采购代理机构发布澄清、修改文件后，征得投标人同意，可不改变投标截止时间和开标时间。

10.3 采购代理机构一旦对招标文件作出了澄清、修改，即刻发生效力，采购代理机构有关的补充文件，将作为招标文件的组成部分，对所有现实的或潜在的投标人均具有约束力，而无论是否已经实际收到上述文件。同时，采购代理机构和投标人的权利及义务将受到新的截止期的约束。

10.5 澄清、修改文件发出后，投标人必须使用最新的答疑、澄清文件制作投标文件。

### 三、投标文件

#### 11. 投标文件的语言及计量单位

11.1 投标人提交的投标文件（包括技术文件和资料、图纸中的说明）以及投标人与采购代理机构就有关投标的所有来往函电均应使用中文简体字。

11.2 除非招标文件另有规定，投标文件所使用的计量单位，应使用国家法定计量单位。

11.3 对违反上述规定情形的，评标委员会有权要求投标人限期提供相应文件或决定对其投标予以拒绝。

11.4 电报、电话、传真形式的投标概不接受。投标人的投标文件一律不予退还。

## 12. 投标文件组成及编制

12.1 投标文件分为资格审查资料、商务文件、技术文件。

商务文件指投标人提交的证明其有资格参加投标和中标后有履行合同的文件。技术和服务文件指投标人提交的能够证明其提供的货物及服务符合招标文件规定的文件。本次招标，投标人须按招标文件第二部分“投标人须知前附表”中第6项规定提交资格审查资料、商务文件、技术文件，其中加粗项目若有缺失或无效，将导致投标被拒绝且不允许在开标后补正。

12.2 投标人递交的投标文件及相关要求按照招标文件第二部分“投标人须知前附表”中的规定。

12.2.1 投标文件的编制

12.2.1.1 投标文件根据招标文件要求进行制作编制。投标文件制作时，按照招标文件中明确的投标文件目录和格式进行编制，保证

目录清晰、内容完整。

12.2.1.2 投标文件须使用投标人公章的以及法定代表人的签章。若无签章，则视为无效投标。

12.2.1.3 招投标文件具有法律效力，若投标文件与招标文件要求不一致，其内容影响中标结果时，责任由投标人自行承担。投标人递交的投标文件因投标人自身原因而导致无法评标，该投标文件视为无效投标文件，将导致其投标被拒绝。

### 13. 投标报价

13.1 报价及最高限价：最终总报价（完税法）（出厂价+货物到达最终目的地点的相关运输费、保险费、仓储费、装卸费、搬运设备费、人工费、安装费、和伴随服务费等）。不接受备选投标报价方案。

13.2 除非招标文件另有规定，不接受可选择或可调整的投标方案和报价，任何有选择的或可调整的投标方案和报价将被视为非响应性投标而被拒绝。

13.3 本项目是否允许投标人将项目的非主体、非关键性工作交由他人完成按照招标文件第二部分“投标人须知前附表”中的规定。如允许，投标人根据采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作交由他人完成，须在技术文件中载明。

13.4 投标人须严格按照报价明细表规定的内容填写货物单价以及其他事项。

13.5 投标人对投标报价若有说明应在投标文件中显著处注明。

除政策性文件规定以外，投标人所报价格在合同实施期间不因市场变化因素而变动。

#### 13.6 最低报价不能作为中标的保证。

### 14. 投标有效期

14.1 本项目的投标有效期按照招标文件第二部分“投标人须知前附表中”中的规定。投标有效期自开标之日起计算，短于规定期限的投标将按无效投标处理。

14.2 在特殊情况下，采购代理机构可与投标人协商延长投标有效期。这种要求和答复都应以书面形式进行。此时，规定的投标保证金的有效期也相应延长。投标人可以拒绝接受延期要求而不会被没收保证金。同意延长有效期的投标人除按照采购代理机构要求修改投标有效期外，不能修改投标文件的其他内容。

### 15. 投标内容填写说明

15.1 投标人应仔细阅读招标文件的全部内容。投标文件须对招标文件中的内容作出实质性和完整的响应，如果投标文件填报的内容不详，或没有提供招标文件中所要求的全部资料及数据，将可能导致投标被拒绝。

15.2 投标文件须严格按照招标文件第六部分规定的格式提交，并按规定的统一格式逐项填写，不准有空项；无相应内容可填的项，应填写“无”、“未测试”、“没有相应指标”等明确的回答文字。由于编排混乱导致投标文件被误读或查找不到，其责任由投标人承担。投标文件未按规定提交或留有空项，将被视为不完整响应的投标

文件，其投标有可能被拒绝。

15.3 开标一览表为在开标仪式上唱标的内容，要求按格式统一填写，不得自行增减内容。

15.4 投标人须注意：为合理节约政府采购评审成本，提倡诚实守信的投标行为，特别要求投标人应本着诚信精神，在本次投标文件的偏离表中，均以审慎的态度明确、清楚地披露各项偏离。若投标人对某一事项是否存在或是否属于偏离不能确定，亦必须在偏离表中清楚地表明该偏离事项，并可以注明不能确定的字样。任何情况下，对于投标人没有在偏离表中明确、清楚地披露的事项，包括可能属于被投标人在偏离表中遗漏披露的事项，一旦在评审中被发现存在偏离或被认定为属于偏离，则评标委员会有权视具体情形评审时予以处理，乃至对该投标予以拒绝。

15.5 投标人必须保证投标文件所提供的全部资料真实可靠，并接受采购代理机构或评标委员会对其中任何资料进一步审查的要求。

15.6 投标人在投标文件及相关文件的签订、履行、通知等事项的文件中的单位盖章、印章、公章等处均指与当事人全称相一致的电子签章或标准公章，不得使用其他形式（如带有“专用章”等字样的印章）。不符合本条规定的按无效投标处理。

#### **四、投标保证金**

#### **16. 投标保证金**

16.1 投标人应按照招标文件第二部分“投标人须知前附表”中第 18 项的规定交纳。投标保证金须于到账截止时间前到帐，并经采

购代理机构确认。

16.2 采购代理机构不接收以现金或汇票等其他形式递交的投标保证金。未按要求递交投标保证金的，将被视为无效投标。

16.3 未中标的投标人的投标保证金在中标通知书发出之日起5个工作日内退还；中标人的投标保证金将在交纳履约保证金并于合同生效后5个工作日内退还。

16.4 投标保证金退还一律采用网上银行转帐方式退还至投标人的汇款帐户，资金原路返回。

## 五、投标文件的递交

### 17. 投标文件的密封和标记

17.1 电子响应文件的内容通过数字证书进行加密并签章。未按要求加密和数字证书认证的响应文件，电子评标系统将无法接受，采购单位不予受理。

### 18. 投标文件的递交

18.1 投标人应在招标文件规定的响应文件递交截止时间前将电子响应文件上传到指定网站的指定栏目。未在响应文件递交截止时间前完成上传的电子响应文件视为逾期送达。逾期上传或未按规定方式上传的电子响应文件，采购单位不予受理。

18.2 投标人应在招标文件规定的响应文件递交截止时间前递交电子响应文件。

18.3 采购单位将拒绝并原封退回在规定的响应文件递交截止期后送达的任何响应文件。由于对网上招标操作不熟悉或自身电脑、网

络的原因导致不能在响应文件递交截止时间之前上传响应文件，代理机构不负任何责任。建议于开标前1个工作日完成响应文件的制作与上传。

## 19. 投标文件的修改和撤回

19.1 投标人在递交投标文件后，可以修改或撤回其投标，但这种修改和撤回，必须在规定的投标截止时间前。在投标截止时间后，投标人不得要求修改或撤回其投标文件。

## 六、开标

### 20. 开标

20.1 采购代理机构按照招标文件规定的时间、地点主持开标。投标人法定代表人或授权代理人应当参加开标并签到。

20.2 开标前，采购代理机构将会同监督人员或公证人员进行验标（检查网上招标系统正常与否，检查电子投标文件，检查投标人报名及保证金交纳情况），确认无误后开标。开标时，各投标人应对本单位的加密的电子投标文件进行解密，采购代理机构工作人员在监督人员或公证人员监督下解密所有投标文件。

20.3 开标时，采购代理机构将通过网上开标系统公布投标人名称、投标价格，以及采购代理机构认为合适的其它详细内容。

## 七、评标步骤和要求

### 21. 组建评标委员会

21.1 采购代理机构根据有关法律法规和本招标文件的规定，结合招标项目的特点组建评标委员会，对投标文件进行评估和比较。评

标委员会由五人以上单数组成，其中经济、技术等方面的专家不少于三分之二。

21.2 参与过本项目的论证专家不得作为评标专家参加评标，招标人不得以专家身份参与评标。

## 22、资格审查

22.1 公开招标采购项目开标结束后，招标人或者采购代理机构应当依法对投标人的资格进行审查。合格投标人不足3家的，不得评标。

## 23. 初步评审

23.1 评标委员会审查投标文件是否符合招标文件的基本要求：内容是否完整、资格证明文件是否合格、文件签署是否齐全、有无计算错误等。

23.2 评标委员会审查投标文件是否实质上响应招标文件的要求。

1) 实质上响应的投标是指与招标文件上的条款、条件和规格相符，没有重大偏离或保留，否则将视为无效投标。

2) 重大偏离或保留系指投标货物的质量、数量和交付日期等明显不能满足招标文件的要求，或者实质上与招标文件不一致，纠正这些偏离或保留将对其他实质上响应要求的投标人的竞争地位产生不公正的影响。包括但不限于：

A、招标文件第二部分“投标人须知前附表”“投标文件组成”部分中，如部分的证明文件不全或无效的；

B、投标文件未按招标文件的规定签章的；

- C、未按投标文件份数要求提交投标文件的；
- D、招标文件带加粗部分任意一款不满足要求的；
- E、报价超过项目预算或经评标委员会认定低于成本的；
- F、投标有效期不足的；
- G、联合体投标文件未附联合体投标协议书的；
- H、不符合招标文件中有关分包规定的；
- I、有串通投标或弄虚作假或有其他违法行为的；
- J、投标人递交的电子投标文件（加密电子投标文件和未加密电子投标文件）均无法满足正常开标、评标使用功能的；
- K、投标人名称或组织结构与报名时不一致且无有效变更证明的；
- L、不符合招标文件中规定的其他实质性要求。

23.3 投标文件的细微偏差是指在实质上响应招标文件要求，但在个别地方存在漏项或者提供了不完整的技术信息和数据等情况，并且补正这些遗漏或者不完整，不会对其他投标人造成不公正的结果。细微偏差不影响投标文件的有效性。

23.4 初步评审中，对明显的文字和计算错误按下述原则处理，若出现相互矛盾之处，应以排列在前的原则为准优先处理：

1) 投标文件中的开标一览表与明细表内容不一致的，以开标一览表为准。

2) 如果以文字表示的数据与数字表示的有差别，以文字为准修正数字。如果大写金额和小写金额不一致的，以大写金额为准；

3) 如果单价乘以数量不等于总价，以单价为准修正总价，但单

价金额小数点有明显错位的，应以总价为准，并修改单价。如果明细价格相加不等于汇总价格，以明细价格为准。

4) 调整后的数据对投标人具有约束力，投标人不同意以上修正，其投标将被拒绝。

23.5 评标委员会对投标文件的判定，只依据投标文件内容本身，不依据其他外来证明。

## 24. 投标的澄清

24.1 评标委员会有权要求投标人对投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误等内容作必要的澄清、说明或者补正。该要求应当采用书面形式，并由评标委员会成员签字。评标委员会不接受投标人主动提出的澄清、说明或者补正。

24.2 投标人必须按照评标委员会通知的内容和时间做出书面答复，该答复经法定代表人或授权代理人的签字认可，将作为投标文件内容的一部分。澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。投标人拒不按照要求对投标文件进行澄清、说明或者补正的，评标委员会可拒绝该投标。

24.3 如评标委员会一致认为某个投标人的报价明显不合理，有降低质量、不能诚信履行的可能时，评标委员会有权决定是否通知投标人限期进行书面解释或提供相关证明材料。若已要求，而该投标人在规定期限内未做出解释、作出的解释不合理或不能提供证明材料的，经评标委员会取得一致意见后，可拒绝该投标。

24.4 公开招标采购项目开标结束后，招标人或者采购代理机构

应当依法对投标人的资格进行审查。合格投标人不足 3 家的，不得评标。

## 25. 详细评审

25.1 评标委员会只对实质上响应招标文件的投标进行评价和比较；评审应严格按照招标文件第二部分“投标人须知前附表”中第 22 项规定以及招标文件的要求进行。具体要求等详见招标文件第五部分“评审方法”。

25.2 评标委员会依法独立评审，严格遵守评审工作纪律。对需要共同认定的事项存在争议的，按照少数服从多数的原则作出评审结论。持不同意见的评标委员会成员应当在评标报告上签署不同意见并说明理由，不签署不同意见的视为同意。

## 26. 确定中标人

26.1 使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由招标人或者招标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，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

26.2 评标委员会根据评审结果及招标文件的规定确定中标人。

## 27. 评标过程要求

27.1 开标之后，直到签订合同止，凡是属于审查、澄清、评价和比较投标的有关资料以及定标意向等，均不向投标人或者其他与评

标无关的人员透露。

27.2 在确定中标人之前，投标人试图在投标文件审查、澄清、比较和评标时对评标委员会、招标人和采购代理机构施加任何影响都可能导致其投标无效。

### 27.3 电子招投标的应急措施

27.3.1 电子开标、评标如出现下列原因，导致系统无法正常运行或无法正常评标时，应采取应急措施。

- (1) 系统服务器发生故障，无法访问或无法使用系统；
- (2) 系统的软件或数据库出现错误，不能进行正常操作；
- (3) 系统发现有安全漏洞，有潜在的泄密危险；
- (4) 病毒发作或受到外来病毒的攻击；
- (5) 出现其他不可抗拒的客观原因造成开评标系统无法正常使用。

出现上述情况时，应对未开标的暂停开标。已在系统内开标、评标的立即停止。采取应急措施时，必须对原有资料及信息作出妥善保密处理。

## 28. 投标人瑕疵滞后发现的处理规则

28.1 无论基于何种原因，各项本应作拒绝处理的情形即便未被及时发现而使该投标人进入初审、综合评审或其他后续程序，包括已经签订合同的情形，一旦投标人被拒绝或该投标人的此前评议结果被取消，其现有的位置将被其他投标人依序替代，相关的一切损失均由该投标人承担。

## 29. 采购项目废标

29.1 在评标过程中，评标委员会发现有下列情形之一的，应对采购项目予以废标：

1) 符合专业条件的投标人或者对招标文件作实质响应的投标人数量不足，导致进入详细评审、打分阶段的投标人不足 3 家的；

2) 投标人的报价均超过了采购预算；

3) 出现影响采购公正的违法、违规行为的；

4) 因重大变故，采购任务取消的。

除前款第四项规定的情形外，项目废标后，如未变更采购方式，采购代理机构将依法重新组织招标。

## 八、履约保证金

### 30. 履约保证金

30.1 履约保证金按照招标文件第二部分“投标人须知前附表”中第 23 项规定，在签订合同前交纳。

30.2 中标人在中标公告发布后及时足额交纳履约保证金。

## 九、代理服务费

### 31. 代理服务费

31.1 代理服务费按照招标文件第二部分“投标人须知前附表”中的规定由中标人交纳，请投标人在测算投标报价时充分考虑这一因素。

## 十、签订、审核合同

### 32. 中标通知

32.1 中标人确定后,采购代理机构将在相关政府采购信息发布媒体上发布中标公告,并以书面形式向中标人发出中标通知书,但该中标结果的有效性不依赖于未中标的投标人是否已经收到该通知。中标人应按照上述第 29、30 条的规定交纳履约保证金、代理服务费和公证费并经采购代理机构确认后,委派专人持介绍信或授权书和身份证件前往采购代理机构领取中标通知书。中标通知书对招标人和中标人具有同等法律效力。中标通知书发出以后,招标人改变中标结果或者中标人放弃中标,应当承担相应的法律责任。

32.2 采购代理机构对未中标的投标人不作未中标原因的解釋,但中标结果的有效性不以未中标的投标人是否收到相应的通知为前提。

32.3 中标通知书是合同的组成部分。

### 33. 签订合同

33.1 中标人须在中标通知书发出之日起 30 日内与招标人签订采购合同。

33.2 中标人须按照招标文件、投标文件及评标过程中的有关澄清、说明或者补正文件的内容与招标人签订合同。中标人不得再与招标人签订背离合同实质性内容的其他协议或声明。

33.3 招标人如需追加与合同标的相同的货物,在不改变合同其他条款的前提下,提交追加合同的申请报经同级财政部门审核后,可与中标人签订补充合同,但所有补充合同的采购金额不得超过原合同金额的百分之十。

33.4 中标人一旦中标及签订合同后，不得转包，亦不得将合同全部及任何权利、义务向第三方转让。

33.5 中标人不履行合同的，招标人可在报经同级人民政府财政部门核准后，与排位在中标人之后的第一位中标候选投标人签订合同，以此类推；或在报经同级人民政府财政部门核准后重新组织采购。

33.6 违反 32.1 条、32.2 条的规定，给对方造成损失的，应承担赔偿责任。

#### 34. 审核合同

34.1 中标人持政府采购合同于签订合同之日起 3 个工作日内到财政局备案留存。

### 十一、处罚、询问和质疑

#### 35. 处罚

35.1 发生下列情况之一，投标人的保证金不予退还；情节严重的将其列入不良记录名单。

- 1) 开标后在投标有效期内，投标人撤回其投标；
- 2) 中标后无正当理由不与招标人签订合同的；
- 3) 中标人与招标人订立背离合同实质性内容的其他协议；
- 4) 将中标项目转让给他人，或者在投标文件中未说明，且未经采购代理机构同意，将中标项目分包给他人的；
- 5) 存在串通投标行为的；
- 6) 存在弄虚作假或提供虚假材料谋取中标的；
- 7) 投标人其他未按招标文件规定和合同约定履行义务的行为。

## 36. 询问

36.1 投标人对采购事项有疑问的，可以向招标人或采购代理机构提出询问。

## 37. 投标人有权就招标事宜提出质疑

37.1 投标人认为招标文件、采购过程和中标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，以书面形式提出质疑。

37.2 质疑应当按照《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》、《政府采购投标人投诉处理办法》等法律法规的相关规定，以书面形式向采购代理机构提出。

37.3 质疑书应当附上相关证明材料，否则质疑将视为无有效证据支持，将被予以驳回，并不得以上述理由要求延长质疑有效期。未递交投标文件的投标人，其未参加后续采购活动，不得对递交投标文件截止后的采购过程、采购结果提出质疑。

37.4 质疑人可以采取直接送达或者邮寄方式提交质疑书。采购代理机构收到质疑书后，对质疑书进行审查，对符合质疑条件的将办理签收手续，自签收质疑书之日起即为受理。

37.5 采购代理机构将在受理书面质疑后7个工作日内审查质疑事项，作出答复或相关处理决定，并以书面形式通知质疑人和其他相关投标人，但答复的内容不涉及商业秘密。

37.6 投标人进行虚假和恶意质疑的，采购代理机构将提请有关部门将其列入不良记录名单，在一至三年内禁止参加政府采购活动，

并将处理决定在相关政府采购媒体上公布。

37.7 质疑人对答复不满意以及采购代理机构未在规定的时间内作出答复的，可以在答复期满后 15 个工作日内向财政部门投诉。

## 十二、保密和披露

### 38. 保密和披露

38.1 投标人自领取招标文件之日起，须承担本招标项目保密义务，不得将因本次招标获得的信息向第三人外传。由招标人向投标人提供的图纸、详细资料、样品、模型、模件和所有其它资料，被视为保密资料，仅被用于它所规定的用途。除非得到招标人的同意，不能向任何第三方透露。开标结束后，应招标人要求，投标人应归还所有从招标人处获得的保密资料。

38.2 采购代理机构有权将投标人提供的所有资料向有关政府部门或评审标书的有关人员披露。

38.3 在采购代理机构认为适当时、国家机关调查、审查、审计时以及其他符合法律规定的情形下，采购代理机构无须事先征求投标人同意而可以披露关于采购过程、合同文本、签署情况的资料、投标人的名称及地址、投标文件的有关信息以及补充条款等，但应当在合理的必要范围内。对任何已经公布过的内容或与之内容相同的资料，以及投标人已经泄露或公开的，无须再承担保密责任。

## 第三部分 采购需求

### 一、要求

依据《网络安全等级保护基本要求》，落实安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理的要求。突出技术思维和立体防范，注重全方位主动防御、动态防御、整体防控和精准防护。

由于业务直接面向互联网用户，安全风险主要来源于外部网络攻击、内部程序脆弱、恶意用户行为、在线缴费四方面。建设规划应重点加强用户认证、传输安全、安全防护、漏洞检测等方式实现区域信息安全。

1、本项目要求需针对现业务提供全方位的安全体系保障，包括安全边界隔离、安全通信网络、安全计算环境、安全运营中心等。为深入贯彻落实平台安全防护责任，提供业务系统智能运维平台，可通过对平台的软硬件告警进行实时采集并上报至运维平台，实现智能告警分析，及时发现业务环境故障并主动提供闭环服务。

2、基于现有业务与网络状况分析，现有承载平台能够实现和本次建设内容实现联动处置，支持数据日志导出至安全运营中心做大数据分析 & 运行可靠性分析，可联动云平台进行关机、挂起等，联合保障业务运行安全。

3、确保业务数据完整性，有效规避业务系统在使用过程中的数据丢失风险，如数据重建优先级调整等，一旦发生安全事件，支持查

看数据重建任务列表信息，包括对象名称、对象类型、数据量和优先级等信息，可以实现不同业务的优先级对数据重建进行优先重建，保证重要的业务优先恢复数据的可靠性。

4、中标单位项目建设中，对甲方现有设备造成损坏，或数据丢失等事故，同时未能按合同完成进度要求和质量要求，甲方有权追究中标人的法律责任，造成的所以损失由中标单位承担。

5、本次建设中，对现有数据安全需重点考虑异地容灾条件下跨数据中心的数据恢复能力，在原有数据中心异地容灾基础上，实现每个数据中心均保存完整的数据副本，数据定期写入到两个数据中心，保障一个数据中心故障，数据零丢失，业务分钟级别恢复，实现 RPO=0、RTO 分钟级恢复。

## 二、设备清单

政务外网设备			
序号	设备名称	部署位置	数量（台）
1	链路负载均衡	政务外网出口	2
2	下一代防火墙	政务外网出口	2
3	准入控制	核心交换区	1
4	检测探针	核心交换区	1
5	Web 应用防火墙	核心业务域	2
6	数据库审计	核心业务域	1
7	统一认证平台	核心业务域	1
8	安全代理网关	核心业务域	1
9	下一代防火墙	终端接入域	3

10	运维管理系统	运维管理域	1
11	日志审计系统	运维管理域	1
12	漏洞扫描系统	运维管理域	1
13	安全态势感知系统	运维管理域	1
14	网络版防病毒	运维管理域	1套（150个PC、30个服务器端）
15	网闸	数据交换域	2
16	安全运营服务	电子政务外网	3年
17	安装调试及业务云升级	核心业务域	1
18	核心交换机	核心业务域	2
19	交换机扩展板卡	核心业务域	2
20	规则库升级	灾备机房	2
21	数据库审计	灾备机房	1
22	HBA卡	核心业务域	3
23	交换机	核心业务域	5
专网			
序号	设备名称	部署位置	数量（台）
1	下一代防火墙	三级专网出口	2
2	漏洞扫描系统	核心交换区	1
3	准入控制	核心交换区	1
4	检测探针	终端接入域	1
5	日志审计系统	终端接入域	1
6	网络版防病毒	终端设备	1套（50个PC）
7	核心交换机	核心业务域	2
8	技术安装调试	核心业务域	1
9	安全智能视频门禁	边界安全	1
10	门禁卡	边界安全	4

11	后台登录读卡器	边界安全	1
12	门禁管理后台一体机	边界安全	1
13	门禁控制器（通用）	边界安全	1
互联网			
	设备名称	部署位置	数量（台）
1	态势感知平台	运维管理域	1
2	链路负载均衡	互联网出口	2
3	下一代防火墙	互联网出口	2
4	漏洞扫描系统	核心交换区	1
5	准入控制	核心交换区	1
6	检测探针	核心交换区	1
7	下一代防火墙	终端接入域	1
8	日志审计系统	核心交换区	1
9	网络版防病毒	终端设备	1
10	数据库审计	核心业务域	1
11	堡垒机(核心交换)	核心业务域	1
12	WAF 应用防火墙	核心业务域	1
13	前置机	终端接入域	2
密码安全管理			
序号	设备名称	设备部署	数量
1	IPSec/SSL VPN 综合安全网关	政务网核心交换域	2
2	设备证书	IPSec/SSL VPN 综合安全网关	3
3	数字证书	证书服务费(含证书存储介质)	200
4	服务器密码机	核心业务域	2
5	签名验签和时间戳二合一服务器	核心业务域	1
6	技术安装调试	核心业务域	1

7	安全智能视频一体化服务系统	边界安全	1
8	USBKey	边界安全	2
9	一体化高清网络视频设备	边界安全	2
10	视频监控专用数字证书	边界安全	4

### 三、具体参数要求

#### (一) 政务外网设备要求

##### 1、链路负载均衡

具体要求
<p>性能参数：4层吞吐量（默认网口）<math>\geq 3\text{Gbps}</math>，四层并发连接数<math>\geq 8000000</math>，4层新建连接数 CPS<math>\geq 100000</math>，7层新建连接数 RPS<math>\geq 150000</math>。硬盘容量：<math>\geq 128\text{G}</math> SSD，接口<math>\geq 6</math>千兆电口+2千兆光口 SFP。</p> <p>◆部署方式支持双机热备形式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换；与现有负载均衡设备、以及链路之间的冗余互备，能够实现与现有设备部署双机热备功能；（出具厂商证明文件复印件并加盖公章）</p> <p>支持 PPPOE 和静态 IP 两种线路接入方式；</p> <p>支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略；</p> <p>支持链路负载情况的投屏展示，能够分别实现基于 ISP 流量、应用选路和链路监测进行投屏展示分析。ISP 流量展示基于运营商分类选择链路的示意图；链路监测展示链路的上下行带宽、健康状态、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；（需提供产品功能截图证明）</p> <p>内置智能告警系统,支持两种告警方式，管理员可基于业务安全所关注方面来</p>

选择告警触发事件与对应的告警方式，当业务网络环境中发生时（如服务器宕机、网络攻击、链路中断等故障场景），即会自动向管理员发送告警信息；

支持在同一个虚拟服务下同时配置多个 IPv4 和 IPv6 地址；

支持跨数据中心集群和跨数据中心会话保持

支持 SNMP v1/v2c/v3，提供标准的 MIB 库下载，可接受第三方网管平台的管理；

新疆建友友成工程管理咨询有限公司

## 2、下一代防火墙

### 具体要求

硬件参数：接口 $\geq 8$ 千兆电口+2万兆光口 SFP+。电源：冗余电源；规格：2U；性能参数：网络层吞吐量 $\geq 15\text{Gbps}$ ，应用层吞吐量 $\geq 8\text{Gbps}$ ，防病毒吞吐量 $\geq 1\text{Gbps}$ ，IPS 吞吐量 $\geq 1\text{Gbps}$ ，并发连接数 $\geq 200$ 万，HTTP 新建连接数 $\geq 9$ 万，IPSec VPN 最大接入数 $\geq 1000$ ，IPSec VPN 吞吐量 $\geq 700\text{M}$ 。

产品支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御。

支持勒索病毒检测与防御功能，需提供功能截图及关于“勒索病毒”的相关证书证明所投产品的功能有效性，证明证书不限于公安部计算机信息系统安全产品质量监督检验中心、中华人民共和国国家版权局、中国信息安全测评中心之中任意一家检测机构。

产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 80 万种，可识别主机的异常外联行为。

产品支持服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和封锁。

支持安全策略的生命周期管理，支持对安全策略修改的时间、原因、变更类型进行统一管理，发便于策略的运维与管理。（需提供产品功能截图证明）

◆支持与网络版防病毒软件统一管理，在防火墙产品完成防病毒软件策略设置和防病毒软件的统一管理。（需提供产品功能截图证明）

产品支持用户账号全生命周期保护功能，包括用户账号弱口令检测、多余入口检测、失陷账号检测、用户账号暴力破解检测，防止因账号被暴力破解导致的非法提权情况发生。

### 3、准入控制

#### 具体要求

硬件参数：硬盘容量 $\geq 128\text{G}$  SSD，接口 $\geq 4$  千兆电口

性能参数：网络层吞吐量（大包） $\geq 3\text{Gb}$ ，带宽性能 $\geq 200\text{Mb}$ ，支持用户数 $\geq 500$ ，准入终端数 $\geq 300$ ，准入终端数的扩容上限（支持客户端授权） $\geq 500$ ，每秒新建连接数 $\geq 2400$ ，最大并发连接数 $\geq 120000$ 。

◆支持对在网接入终端进行统一可视化管理，可视化内容包括终端详细信息、合规状态等，支持查看入网终端详细信息（类型、厂商，系统，端口等）（需提供产品功能截图证明）

支持 windows 终端安全检查，包括：杀软检查、登录域检查、操作系统检查、进程检查、文件检查、注册表检查、补丁检查、windows 账号检查、防篡改检查、客户端集成检查，对不满足检查要求的终端可弹窗提示、禁止上网、违规修复；支持 windows 终端调用管理员指定脚本或程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网；

支持存储设备、网络设备、蓝牙设备、摄像头、打印机的使用管控；

支持允许特定的外设（包括 U 盘/存储设备）在终端上使用，并提供批量获取硬件 ID 的工具；

◆支持对 Windows 终端外联行为进行检查，包括但不限于连接外网检查、PPPoE 拨号检查、双网卡行为检查、无线网卡检查、链接非法 WIFI 检查（可设置合法 WIFI 白名单）、4G 网卡检查、是否使用非法网关（可设置合法网关白名单）等场景，对不符合检查要求的终端强制断网，弹窗提示用户进行修复，并将告警消息通知系统管理员；（需提供产品功能截图证明）

支持根据访问的 URL 和网页关键字进行网页过滤，支持设置拒绝以 IP 访问网页行为；

能够与本次采购的“安全态势感知系统”产品兼容对接，完成数据上传，实现资产管理信息的同步；

#### 4、检测探针

具体要求
<p>性能参数：网络层吞吐性能<math>\geq 1.5</math> Gbps，应用层吞吐性能<math>\geq 500</math> Mbps。</p> <p>硬件参数：硬盘容量<math>\geq 256</math>GSSD，接口<math>\geq 6</math> 千兆电口+2 千兆光口 SFP。</p> <p>具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。</p> <p>支持 FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测</p> <p>支持 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞等网站攻击检测；</p> <p>◆为检测异常流量，需支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括威胁端口 3389、53、80/8080、21、69、443、25、110、143、22 等。（需提供产品功能截图证明）；</p> <p>支持 ICMP、UDP、SYN、DNS 等协议外发异常流量检测，支持自定义阈值。</p> <p>支持设备内置简单命令行管理窗口，便于基础运维调试；可实时监控设备的 CPU、内存、存储空间使用情况；</p>

## 5、Web 应用防火墙

### 具体要求

硬件参数：内存大小 $\geq 8\text{G}$ ，硬盘容量 $\geq 128\text{G}$  SSD，接口 $\geq 8$  千兆电口+2 万兆光口 SFP+。

性能参数：网络层吞吐量 $\geq 20\text{G}$ ，应用层吞吐量 $\geq 9\text{G}$ ，防病毒吞吐量 $\geq 1.5\text{G}$ ，IPS 吞吐量 $\geq 1.3\text{G}$ ，并发连接数 $\geq 200$  万，HTTP 新建连接数 $\geq 9$  万。

产品支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护等攻击类型。

产品内置不低于 10000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。（需提供产品功能截图证明）

◆产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。（需提供产品功能截图证明）

产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。

◆支持与网络版防病毒软件统一管理，在防火墙产品完成防病毒软件策略设置和防病毒软件的统一管理。（需提供产品功能截图证明）

要求所投产品具备国家信息安全漏洞库兼容性资质证书，提供有效证书原件扫描件。

## 6、数据库审计

### 具体要求

硬件参数：内存大小 $\geq 16G$ ，硬盘容量：2T SATA，接口 $\geq 6$ 千兆电口+2万兆光口 SFP+，规格：2U；冗余电源

性能参数：最大硬件吞吐量 $\geq 4Gbps$ ，最大纯数据库流量 $\geq 800Mb/s$ ，数据库实例个数 $\geq 50$ 个，SQL处理性能 $\geq 50000$ 条 SQL/s，日志检索性能 $\geq 1000000$ 条/秒。

要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、及用户手动升级系统补丁；

采用 B/S 管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务；

支持以图表方式（饼图、柱图、曲线图、清单列表）显示日志数据分布情况；

◆支持自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果。（需提供产品功能截图证明）

支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询。

支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行。

内置大量 SQL 安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、查询内置敏感表、篡改内置敏感表等；

## 7、统一认证平台

具体要求
<p>性能参数：最大理论并发用户数<math>\geq 3200</math>；本地认证理论应用鉴权请求新建 TPS（个/秒）<math>\geq 360</math>；本地认证理论新建用户数（个/秒）<math>\geq 90</math>。</p> <p>硬件规格：内存大小<math>\geq 16G</math>，硬盘容量<math>\geq 128GB</math> SSD，接口<math>\geq 6</math> 千兆电口+4 千兆光口 SFP。电源：冗余电源；</p> <p>支持中国商用密码标准，支持加密算法 SM2、SM3、SM4。</p> <p>支持使用商密密码卡进行加密，支持在控制台对密码卡进行管理（包括：激活、取消激活、密钥备份/恢复、管理 KEY 口令）</p> <p>应支持部署分离式架构的统一认证平台和安全代理网关，以实现控制面与执行面分离，提高系统安全性。</p> <p>为有效防止木马入侵系统后攻击服务器，系统内置常见攻击工具进程黑名单，管理员可基于内置的名单进行增减，匹配上此名单的进程访问零信任系统时会被打上标签，以方便快速定位排查问题终端。</p> <p>当检测到不符合安全条件时，支持设置如短信增强认证、告警等灵活的补救动作，实现灰度处置，且能配置处置有效时长，平衡员工访问体验和安全保障</p> <p>支持提供开放的 API，管理员可在控制台创建 API KEY，供单位与本项目中态势感知分析平台对接，形成统一的安全体系（需提供产品功能截图证明）</p> <p>支持将进程的可信状态作为访问控制评估条件，配置应用访问策略。限制仅可信的进程可访问指定的应用，或不可信的进程阻止访问。</p> <p>支持将用户访问控制器的加密流量解密后镜像给外部系统，如态势感知等</p> <p>◆支持终端环境诊断排查，提供终端诊断工具，支持对当前终端的基本环境进行扫描和一键修复，便于员工自行排查修复终端问题，减少 IT 运维人员工作（需提供产品功能截图证明）</p> <p>提供国家密码管理局商用密码检测中心出具的含有“访问控制系统”字样，符合 GM/T 0024 标准或 GM/T 0025 标准要求，以及符合 GM/T 0028 《密码模</p>

块安全技术要求》第二级的《商用密码产品认证证书》

新疆建友友成工程管理咨询有限公司

## 8、安全代理网关

### 具体要求

性能参数：最大理论加密流量 $\geq 450\text{Mbps}$ ；最大理论 https 并发连接数 $\geq 45000$ ；最大理论并发用户数 $\geq 4500$ ；

硬件参数：规格：内存大小 $\geq 16\text{G}$ ，硬盘容量 $\geq 128\text{G SSD}$ ，接口 $\geq 6$ 个千兆电口  
4个千兆光口；电源：冗余电源

支持接入 IP 限制（即接入控制台的 IP 白名单），限制后，从浏览器、SSH 或 SNMP 等方式接入管理台时，都必须在上述 IP 白名单范围内接入。

支持告警信息设置，包含以下几个方面：CPU 使用率超过 80%、内存使用率超过 80%、磁盘占用率超过 80%、序列号即将到期（提前 15 天提醒）、在线用户数已达购买授权数

支持在控制台上提供命令面板，内嵌常规的网络配置和排障命令，方便运维人员对设备进行维护，网络测试以及故障排查

◆为完善系统使用用户行为审计溯源能力，支持将用户访问安全代理网关的加密流量解密后镜像给本次招标的安全态势感知系统。

为证明所投产品的自身安全性，应具备国家计算机网络应急技术处理协调中心出具的安全众测无漏洞证明文件。

支持中国商用密码标准，支持加密算法 SM2、SM3、SM4。

支持使用商密密码卡进行加密；支持在控制台对密码卡进行管理（包括：激活、取消激活、密钥备份/恢复、管理 KEY 口令）

◆提供国家密码管理局商用密码检测中心出具的含有“访问控制系统”字样，符合 GM/T 0024 标准或 GM/T 0025 标准要求，以及符合 GM/T 0028《密码模块安全技术要求》第二级的《商用密码产品认证证书》

## 9、下一代防火墙

### 具体要求

硬件参数：硬盘容量 $\geq 128\text{G}$  SSD，接口 $\geq 8$  千兆电口+2 千兆光口 SFP。

性能参数：网络层吞吐量 $\geq 4\text{G}$ ，应用层吞吐量 $\geq 2\text{G}$ ，防病毒吞吐量 $\geq 600\text{M}$ ，IPS 吞吐量 $\geq 600\text{M}$ ，并发连接数 $\geq 200$  万，HTTP 新建连接数 $\geq 6$  万，IPSec VPN 最大接入数 $\geq 300$ ，IPSec VPN 吞吐量 $\geq 270\text{M}$ 。

产品支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护、Smurf 攻击防护等攻击类型。

支持勒索病毒检测与防御功能

产品内置不低于 10000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。

产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 80 万种，可识别主机的异常外联行为。

产品支持用户账号全生命周期保护功能，包括用户账号弱口令检测、多余入口检测、失陷账号检测、用户账号暴力破解检测，防止因账号被暴力破解导致的非法提权情况发生。

产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。

## 10、运维管理系统

### 具体要求

性能参数：默认包含运维授权数 $\geq 200$ ，最大可扩展资产数 $\geq 1000$ ，图形运维最大并发数 $\geq 200$ ，字符运维最大并发数 $\geq 350$ 。硬盘容量 $\geq 128G+2T$  SATA，接口 $\geq 6$  千兆电口+2 万兆光口 SFP+。规格：2U

系统各模块支持以 B/S 方式管理，采用 https 加密方式访问

内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴

口令变更至少支持 windows 系统、网络设备、linux/unix 系统、数据库等

支持命令黑名单，对字符型设备（如 linux/unix/网络设备）的高危命令执行进行阻断，如 rm、shutdown、reboot 等

支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人

图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放

支持提供系统内部操作审计，包括管理员和运维用户的登录、登出、对系统的配置操作、账号属性修改等系统管理操作

全面支持 Windows、linux、国产麒麟系统、Android、IOS、Mac OS 等客户端操作系统下的 H5 页面一站式运维，实现跨终端适应性 BYOD (Bring Your Own Device)

## 11、日志审计系统

### 具体要求

性能参数:默认包含主机审计许可证书数量 $\geq 100$ ,平均每秒处理日志数(eps)最大性能 $\geq 2500$ 。

支持软件部署,能够部署在现有云平台上,通过SSL加密对数据传输等进行处理、采用B/S架构,HTTPS访问

支持各类设备的日志采集要求,主要包括:安全设备:国内主流防火墙;操作系统:Linux、Windows、Windows Server、Unix等操作系统;数据库:Oracle、MySQL、SQLServer等;应用系统:如Apache、Tomcat、IIS、Weblogic等;网络设备:主流的路由器、交换机、负载均衡等网络设备等主流网络设备

支持对日志格式进行标准化操作时,不破坏原始日志内容。从不同设备或系统的日志中抽取相关片段准确和完整地映射至日志的标准字段中,统一格式。支持单条事件进行展开,显示事件详细信息和事件原始信息,支持事件详情中任意字段作为查询条件无限制进行二次检索分析。

支持对单个/多个日志源批量转发,支持定时转发,可通过syslog和kafka方式转发到第三方平台,并且支持转发原始日志和已解析日志的两种日志(需提供产品功能截图证明)

支持对每个日志源设置过滤条件规则,自动过滤无用日志,满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数,减少对网络带宽和数据库存储空间的占用。

## 12、漏洞扫描系统

### 具体要求

性能参数：系统漏扫授权 IP 数 $\geq 100$ ，WEB 漏扫授权 URL 数 $\geq 20$ ；主机漏扫最大并发 IP 数 $\geq 150$ ，WEB 漏扫最大并发 URL 数 $\geq 5$ 。

采用有自主知识产权的安全操作系统，采用 B/S 设计架构，支持软件化交付，部署在现有云平台上，并采用 SSL 加密通信方式，无须安装客户端，用户可通过浏览器远程方便的对产品进行管理。

支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描等 $\geq 4$ 种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。

◆提供检测结果综述分析，按照等保 2.0 的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。（需提供产品功能截图证明）

支持统一管理所有业务系统的合规情况，合规报告可导出。业务系统差距报告量化、可视化整改前后的符合情况和安全问题。

产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表。

系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果支持报表导出的格式包括 HTML、WORD、EXCEL 等格式。

### 13、安全态势感知系统

#### 具体要求

性能参数：存储容量 $\geq 21\text{T}$ ；在带宽性能 1Gbps 时存储时长 $\geq 1200$  天/1Gbps；  
硬件参数：规格 2U，电源：冗余电源；接口不少于 4 个千兆电口。

◆为更好地实现外网资产设备的管理管控，支持自定义资产多级分支管理，最多可至 15 级分支。支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等。（需提供产品功能截图证明）

弱密码检测规则支持高度自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web 空密码、账号白名单、密码白名单、txt 文件格式导入。

弱密码检测规则支持自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web 空密码、账号白名单、密码白名单、txt 文件格式导入。

支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力，综合运用威胁情报、IPS 特征规则和行为关联分析技术，如检测发现文件传输（上传下载）阶段的异常，对挖矿早期的准备动作即告警。

支持对网络安全设备规则，包括网络设备、安全设备、中间件、操作系统等；接入方式。支持文件、数据库、API、Syslog、FTP、Kafka 等方式进日志行接入，并支持用户对日志进行自定义解析规则，支持接入设备自动发现功能。

◆定期可提供安全风险报告，风险报告支持综合安全风险、主机安全风险、脆弱性感知、外部感知、工单、摘要、处置报告多种方式呈现，也支持自定义时间导出 PPT 形式报告，帮助管理员进行多维度的风险分析和辅助决策。（需提供产品功能截图证明）

具备实战化攻防中心，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面梳理。实战阶段的实时攻击分析，被攻击者 IP、攻击者 IP、攻击结果、攻击次数、事件类型、联动响应等级等 20 个以上类型。实战阶段的全过程可视溯源分析、总结阶段的值守报告等全过程流程。

内置多个处置策略模板，支持与本次招标下一代防火墙、防病毒软件、负载

均衡联动封锁、访问控制，支持与网络版防病毒软件联动一键查杀、进程取证

支持自动化编排的自定义处置流程策略的设置，灵活剧本设置，融入事件自动处置流程，节省运维处置时间，根据客户实际需要对接所需同品牌或者第三方品牌安全设备进行安全事件处置。

◆所投产品具备国家 IT 产品信息安全产品认证证书，提供有效证书复印件。

新疆建友友成工程管理咨询有限公司

## 14、网络版防病毒

### 具体要求

性能参数：终端桌面需要配置 $\geq 150$ 点，服务器终端安全响应需要配置 $\geq 50$ 点，终端安全检测响应平台需要支持不得少于接入200点。

采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能

支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量；

◆支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示（需提供产品功能截图证明）；

支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具

支持与同厂商的网络防火墙进行安全配置，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息

支持与本次投标的安全态势感知平台进行兼容，支持管理员在安全感知平台管理界面下发快速查杀任务及一键隔离指令，并支持查看任务状态、任务结果并进行协同终端所有连接进行阻断（需提供产品功能截图证明）

## 15、网闸

### 具体要求

性能参数：网络层吞吐量 $\geq 300\text{Mbps}$ ，最大并发连接数 $\geq 5$ 万，硬盘容量 $\geq 128\text{GB}$  SSD+128GB SSD（内网主机和外网主机各 128GB SSD），接口 $\geq 6$ 千兆电口，规格：2U；冗余电源

采用 2+1 系统架构即内网单元+外网单元+FPGA 专用隔离硬件。不能采用网线等形式直通。

设备支持透明、代理及路由三种工作模式，管理员可依据实际网络状况进行相应的部署。（需提供产品功能截图证明）

支持 Oracle、SQLServer、Mysql、Sybase、DB2、Mariadb、Postgresql 等多种主流国外数据库的同步和国产达梦、人大金仓、南大通用、神舟通用、优炫数据库的同步

支持 Oracle、DB2、SyBase、SQL Server、MySQL 等主流数据库的安全访问，实现内外网之间数据库及表内容安全传输。

支持 TCP 应用层数据单向传输的控制，保证 TCP 应用数据的零反馈，以满足二次防护对数据传输的安全性需求

系统提供 ping, traceroute, TCP 端口探测、抓包等工具方便管理员在配置策略或调整网络时排查问题

## 16、安全运营服务

### 1 服务总体要求：

◆（1）数据处理安全需求：因电子政务外网系统安全保障要求，安全运营服务数据接收和处理限于在电子政务外网内完成（出具厂商承诺说明并加盖厂商公章）。

（2）服务兼容性要求：安全服务处置维护数据需与安全态势感知进行数据对接。

（3）服务频率要求：为建立健全安全实战对抗能力，需开展7\*24小时持续安全对抗防护。

（4）专家上门要求：合同期内至少提供安全运营专家（不少于）6次上门安全服务。

### 2 服务水平协议 SLA 要求：

投标方对于以下服务水平需出具承诺，并作为项目验收考核标准：

（1）安全通告服务按照国家标准对安全事件的分类分级指南，达成以下服务水平：

科目	水平要求（通告）
重大安全事件	小于 30 分钟
一般安全事件	小于 1 小时
高级安全威胁	小于 2 小时
一般安全威胁	小于 2 小时

（2）在配备投标方的边界防护服务组件和终端防护服务组件的情况下，安全托管服务需达成以下服务水平：

科目	水平要求（遏制影响和处置完成）
重大安全事件	小于 1 小时
一般安全事件	小于 4 小时
高级安全威胁	小于 1 小时
一般安全威胁	小于 4 小时

（3）在未配备投标方的边界防护服务组件和终端防护服务组件的情况下，安全

托管服务需达成以下服务水平：

科目	水平要求（遏制影响和处置完成）
重大安全事件	小于 8 小时
一般安全事件	小于 24 小时
高级安全威胁	小于 24 小时
一般安全威胁	小于 24 小时

(4) 投标方在于安全漏洞服务工作上，需达成以下服务水平：

在配备投标方的漏洞定期扫描服务组件的情况下，漏洞扫描的频率不低于每 30 天扫描一次。

高危可利用漏洞从完成漏扫后发发现到推送漏洞报告的时间少于 2 个工作日。

高危可利用漏洞经服务人员确认后的准确率不低于 99%。

高危可利用漏洞的防护率达到 99%。

(5) 安全事件经过投标方安全托管服务人员的确认后，各类安全事件、高级安全威胁、一般安全威胁的判断准确率不低于 99%。

(6) 在配备了投标方的边界防护服务组件和终端防护服务组件的情况下，安全事件、高级安全威胁、一般安全威胁的闭环处置比例需达到 100%。

(7) 对于重大事故应启动应急响应机制，工作时间 15 分钟之内云端专家进行响应，非工作时间 30 分钟之内云端专家进行响应，省会 2 小时上门处置，省内 8 小时上门处置。

### 3 服务质量监督要求

业务安全状态监控：投标方需为招标人提供服务监控门户（或用户 Portal，非安全感知大屏展示类页面），在门户中招标人可查看业务和资产安全状态信息，至少包括服务资产安全评级、服务运营状态、成果、安全风险概览、最新情报、脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，已验证投标方所承诺的服务 SLA。

### 4 主要服务能力要求

投标方需基于以下服务能力要求，并围绕资产、漏洞、威胁、事件四个要素开展服务。

- 1) 投标方开展服务范围内资产全面梳理工作（梳理的信息包含：支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP 地址；应用开放协议和端口、应用系统管理方式、资产的重要性以及网络拓扑等信息），并将信息录入到安全托管运营平台中进行管理，当资产发生变更时，安全服务专家对变更信息确认与更新，并定期输出《资产管理表》交付招标人。
- 2) 投标方需在安全托管服务工作开展前进行安全现状评估工作，评估内容包括但不限于：系统与 Web 漏洞扫描、弱口令扫描、基线配置核查、蠕虫病毒检查、失陷主机分析、潜伏威胁分析、漏洞风险等，并输出《安全现状风险评估报告》；
- 3) 投标方需提供提供脆弱性验证服务，针对发现的脆弱性问题进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的脆弱性，自动生成工单，安全专家跟进修复状态，各个处理进度透明，便于招标人清晰了解当前脆弱性的处置状态，将脆弱性处理工作可视化，【需提供服务工具脆弱性工单截图证明，需展示当前脆弱性的处置状态。】；
- 4) 针对存在的漏洞提供修复建议，投标方能够提供精准、易懂、可落地的漏洞修复方案，【提供脆弱性修复方案样本证明，需包含多种修复方案以及修复过程中可能引发的其他问题的解决方案】；
- 5) 针对服务平台生成的工单，招标人可按需催单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置，督促投标方第一时间处理【提供服务平台脆弱性工单处置提醒的功能截图证明】；
- 6) 7\*24 小时实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件。
- 7) 投标方需支持招标人主动申请对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案，【提供在服务平台申请主动响应的实际界面截图证明】；
- 8) 投标方应面向招标人提供定期的勒索病毒入侵风险专项排查，投标方应按照勒索预防 Checklist 开展勒索风险评估，勒索预防 Checklist 应当包含勒索高危利用漏洞、端口、安全策略、攻击行为、勒索残留隐患几个纬度。【投标方应提供勒索预防 Checklist 清单，清单内容必须包含上述纬度，并注明每一项的更新时间】；

9) 投标方定期按照勒索预防 Checklist 开展勒索风险评估后应当每季度一次向招标人提供《勒索病毒风险排查报告》，报告中应包含全面的勒索风险分析和隐患加固处置的情况，并且投标方有义务按招标人要求进行远程或现场的成果汇报。【投标方应提供《勒索风险排查报告》模板，并承诺每半年输出一次报告并向招标人汇报】

10) 投标方安全托管服务平台应支持面向招标人按照勒索预防 Checklist 的一键风险排查，支持维度至少包含弱密码扫描、勒索高危利用漏洞扫描、高危利用端口扫描、勒索风险策略检查、勒索行为监测，并且投标方可按照招标人要求设置定时勒索风险排查任务。【提供服务平台具备勒索风险排查工具、支持自定义排查任务的截图证明】；

11) 支持面向招标人的安全态势展示，展示出当前招标人遭受的威胁事件信息以及脆弱性信息统计，并支持服务专家按照资产类别、威胁类型进行定制化筛选查看，能直观感受到招标人当前的风险态势情况。【提供服务平台漏洞表、事件表统计信息，并证明支持按照资产类别、威胁类型进行定制化筛选查看截图证明】；

12) 投标方安全托管服务平台支持面向招标人的安全报告与交付物管理，可生成、导出、下载各类安全报告，包括但不限于《安全服务值守日报》、《特殊时期值守报告》、《安全运营周报》、《安全运营月报》。【投标方提供服务平台支持上述交付物管理界面的截图】。

## 5 服务交付物要求

- 1) 交付物名称：《安全托管服务运营报告》，报告频率：每周一次；
- 2) 交付物名称：《首次威胁分析与处置报告》，报告频率：一次；
- 3) 交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数；
- 4) 交付物名称：《安全通告》，报告频率：按需触发，不限次数；
- 5) 交付物名称：《综合分析报告》，报告频率：每月一次；
- 6) 交付物名称：《勒索病毒风险排查报告》，报告频率：每季度一次；
- 7) 交付物名称：《季度汇报 PPT》，报告频率：每季度一次；
- 8) 交付物名称：《年度汇报 PPT》，报告频率：每年一次；

招标人有权要求拟中标人严格按照上述频率要求提供服务交付物，确保满足

招标人安全需求。如中标人未能按时提供，招标人有权终止服务合同，中间产生任何费用由中标人自行承担。

新疆建友友成工程管理咨询有限公司

## 17、安装调试及业务云升级

### 具体要求

含线材辅材等设备安装调试,服务器硬盘修复与更换,平台软件升级等,技术要求:

- 1、提供云平台安全中心,实现虚拟机安全防护,包括:主机终端防护的自动安装、病毒的隔离防护、被勒索后的应急恢复、漏洞管理、安全事件一键处置等。
- 2、配置流量镜像,支持虚拟网络内部流量镜像、虚拟网络流量镜像至物理网络、物理网口间流量镜像,满足用户安全审查、流量监控等场景。
- 3、配置网络可视化,支持对业务虚拟机之间的访问关系进行可视化管理,直观查看应用之间的非法访问与故障情况。通过脚本自动化实现大规模虚拟机的日常运维。
- 4、支持NTP服务、桌面云接入服务,两个服务端口管理能力,支持对接新特性的端口管理,满足客户合规性建设要求;支持优化告警设置功能:支持选择性屏蔽虚拟机告警,将用户认为不重要的虚拟机告警屏蔽掉;优化存储策略设置功能,支持用户为存储卷配置默认存储策略,满足用户为特殊业务配置共用的默认存储策略的需求。

## 18、核心交换机

### 具体要求

交换容量：76.8/336Tbps，包转发率：2880/25920Mpps；

模块化交换机，≥6 个业务插槽，双电源，双主控；≥48 个千兆电口+24 个千兆光口+24 个万兆光口（含 8 个万兆多模原装光模块）；

整机最大可管理 4K AP，支持虚拟交换网技术，可将横向和纵向的交换机虚拟成一台设备，支持超高万兆和 100G 端口密度，单台设备最大支持 288 个 10GE 端口，支持分布式 L2/L3 MPLS VPN 功能；

支持 MPLS、VPLS、分层 VPLS、VLL，满足企业 VPN 等接入需求，主控、电源、风扇框等关键部件采用冗余设计，所有模块均支持热插拔；

软硬件平台均支持 IPv6，取得工信部 IPv6 入网认证和 IPv6 Ready 第二阶段认证，支持 IPv6 静态路由、RIPng、OSPFv3、BGP+、IS-ISv6、IPv6、组播、VXLAN 技术，支持 NetStream 业务分析功能，满足用户对网络流量实时采集、分析需要，创新节能芯片，实现按流量动态调整功率，支持端口休眠，无流量不耗电，支持 OPS 技术，OPS 是基于 Python 语言的开放可编程系统。IT 管理员可以通过 Python 脚本对交换机进行运维功能的编程，快速实现功能创新，实现智能化运维。为了方便管理，实现设备虚拟化技术，要求此交换机和系统原有交换机实现堆叠功能。

### 19、交换机扩展板卡

具体要求
4 端口万兆光口板卡，XFP 接口（含 4 个万兆多模原装光模块）

### 20、规则库升级（灾备机房）

具体要求
规则库升级*3 年

新疆建友友成工程管理咨询有限公司

## 21、数据库审计（灾备机房）

### 具体要求

硬件参数：内存大小 $\geq 16\text{G}$ ，硬盘容量：2T SATA，接口 $\geq 6$ 千兆电口+2万兆光口 SFP+。

性能参数：最大硬件吞吐量 $\geq 4\text{Gbps}$ ，最大纯数据库流量 $\geq 800\text{Mb/s}$ ，数据库实例个数 $\geq 50$ 个，SQL 处理性能 $\geq 50000$ 条 SQL/s，日志检索性能 $\geq 1000000$ 条/秒。

要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、及用户手动升级系统补丁；

采用 B/S 管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务；

支持以图表方式（饼图、柱图、曲线图、清单列表）显示日志数据分布情况；支持自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果。支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询。

支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行。

内置大量 SQL 安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、查询内置敏感表、篡改内置敏感表等；

## 22、HBA 卡

具体要求
用于原有设备服务器与存储数据接通，完成线路安装调试，保障存储数据管理与备份。承诺原有设备运行安全，并提供承诺函。

新疆建友友成工程管理咨询有限公司

## 23、交换机

### 具体要求

性能参数：交换容量 $\geq 400\text{Gbps}$ ，包转发率 $\geq 150\text{Mpps}$

硬件参数：千兆电口 $\geq 24$ 个，万兆 SFP+光口 $\geq 4$ 个；Console 口 $\geq 1$ 个

支持 MAC 地址 $\geq 16\text{K}$ ，

支持防网关 ARP 欺骗，支持端口保护、隔离、防止 ARP 泛洪攻击功能；要求提供具有 CMA 和 CNAS 认证章的第三方权威机构测试报告；

支持管理员分级管理；

支持 DHCP Snooping，支持交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应 DHCP 报文；

支持堆叠技术；

支持以下上线方式：支持二层广播自动发现网管中心平台；支持配置静态 IP 地址三层发现网管中心平台；

支持通过网管中心平台一键替换“按钮”即可完成故障设备替换。

支持终端类型库，基于指纹自动识别 PC、路由器、摄像头设备、无线 AP 等；

要求提供具有 CMA 和 CNAS 认证章的第三方权威机构测试报告；

支持基于终端类型自动识别结果，禁止非法终端(例如私接路由器)接入；要求提供具有 CMA 和 CNAS 认证章的第三方权威机构测试报告；

支持禁止通过内网 PC 端进行私接随身 WiFi 共享；

支持在交换机上创建东西向安全策略，实现全网安全风险拦截；

为提高系统兼容性对接，需支持联动第三方安全设备或平台，通过联动实现从系统及接入层交换机对风险终端 MAC 地址进行封堵；

## (二) 专网设备要求

### 1、下一代防火墙

具体要求
<p>硬件参数：内存大小<math>\geq 8\text{G}</math>，硬盘容量<math>\geq 128\text{G}</math> SSD，接口<math>\geq 8</math> 千兆电口+2 万兆光口 SFP+。</p> <p>性能参数：网络层吞吐量<math>\geq 20\text{G}</math>，应用层吞吐量<math>\geq 9\text{G}</math>，防病毒吞吐量<math>\geq 1.5\text{G}</math>，IPS 吞吐量<math>\geq 1.3\text{G}</math>，并发连接数<math>\geq 200</math> 万，HTTP 新建连接数<math>\geq 9</math> 万。</p> <p>产品支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护等攻击类型。</p> <p>产品内置不低于 10000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。</p> <p>产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。</p> <p>支持与网络版防病毒软件统一管理，在防火墙产品完成防病毒软件策略设置和防病毒软件的统一管理。</p> <p>要求所投产品具备国家信息安全漏洞库兼容性资质证书，提供有效证书原件扫描件。</p>

## 2、漏洞扫描系统

### 具体要求

性能参数：系统漏扫授权 IP 数 $\geq 100$ ，WEB 漏扫授权 URL 数 $\geq 20$ ；主机漏扫最大并发 IP 数 $\geq 150$ ，WEB 漏扫最大并发 URL 数 $\geq 5$ 。内存 $\geq 8G$ ，硬盘容量 $\geq 128GB$  SSD+ 2TB SATA，接口 $\geq 6$  千兆电口+2 千兆光口 SFP。

采用有自主知识产权的安全操作系统，采用 B/S 设计架构，采用 SSL 加密通信方式，无须安装客户端，用户可通过浏览器远程方便的对产品进行管理。

支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。

提供检测结果综述分析，按照等保 2.0 的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。

支持统一管理所有业务系统的合规情况，合规报告可导出。业务系统差距报告量化、可视化整改前后的符合情况和安全问题。

◆产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表。（需提供产品功能截图证明）

系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果支持报表导出的格式包括 HTML、WORD、EXCEL 等格式。

### 3、准入控制

#### 具体要求

硬件参数：硬盘容量 $\geq 128\text{G}$  SSD，接口 $\geq 4$  千兆电口

性能参数：网络层吞吐量（大包） $\geq 3\text{Gb}$ ，带宽性能 $\geq 200\text{Mb}$ ，支持用户数 $\geq 500$ ，准入终端数 $\geq 300$ ，准入终端数的扩容上限（支持客户端授权） $\geq 500$ ，每秒新建连接数 $\geq 2400$ ，最大并发连接数 $\geq 120000$ 。

支持对在网接入终端进行统一可视化管理，可视化内容包括终端详细信息、合规状态等，支持查看入网终端详细信息（类型、厂商，系统，端口等）

支持 windows 终端安全检查，包括：杀软检查、登录域检查、操作系统检查、进程检查、文件检查、注册表检查、补丁检查、windows 账号检查、防篡改检查、客户端集成检查，对不满足检查要求的终端可弹窗提示、禁止上网、违规修复；支持 windows 终端调用管理员指定脚本或程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网；

◆无需安装入网客户端，可通过获悉流量行为及状况检查行业主流杀毒软件的运行情况，对不满足检查要求的终端（未安装指定要求的杀毒软件或杀毒软件版本不符合要求）可进行下载页面重定向，帮助终端用户进行运行环境修复；（需提供产品功能截图证明）

支持存储设备、网络设备、蓝牙设备、摄像头、打印机的使用管控；

支持允许特定的外设（包括 U 盘/存储设备）在终端上使用，并提供批量获取硬件 ID 的工具；

支持对 Windows 终端外联行为进行检查，包括但不限于连接外网检查、PPPoE 拨号检查、双网卡行为检查、无线网卡检查、链接非法 WIFI 检查（可设置合法 WIFI 白名单）、4G 网卡检查、是否使用非法网关（可设置合法网关白名单）等场景，对不符合检查要求的终端强制断网，弹窗提示用户进行修复，并将告警消息通知系统管理员；

支持根据访问的 URL 和网页关键字进行网页过滤，支持设置拒绝以 IP 访问网页

行为；

能够与本次采购的“安全态势感知系统”产品兼容对接，完成数据上传，实现资产管理信息的同步；

新疆建友友成工程管理咨询有限公司

#### 4、检测探针

具体要求
<p>性能参数：网络层吞吐性能<math>\geq 1\text{Gbps}</math>，应用层吞吐性能<math>\geq 350\text{ Mbps}</math>。</p> <p>硬件参数：硬盘容量<math>\geq 128\text{GSSD}</math>，接口<math>\geq 6</math> 千兆电口+2 千兆光口 SFP。</p> <p>具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。</p> <p>支持 FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测</p> <p>支持 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞等网站攻击检测；</p> <p>为检测异常流量，需支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。</p> <p>支持 ICMP、UDP、SYN、DNS 等协议外发异常流量检测，支持自定义阈值。</p> <p>支持设备内置简单命令行管理窗口，便于基础运维调试；可实时监控设备的 CPU、内存、存储空间使用情况；</p>

## 5、日志审计系统

### 具体要求

性能参数：默认包含主机审计许可证书数量 $\geq 50$ ，平均每秒处理日志数（eps）最大性能 $\geq 2500$ 。内存 $\geq 16\text{GB}$ ，硬盘容量 $\geq 128\text{G minisata}+2\text{T SATA}^*2$ ，规格：2U；

支持软件部署，能够部署在现有云平台上，通过 SSL 加密对数据传输等进行处理、采用 B/S 架构，HTTPS 访问

支持各类设备的日志采集要求，主要包括：安全设备：国内主流防火墙；操作系统：Linux、Windows、Windows Server、Unix 等操作系统；数据库：Oracle、MySQL、SQLServer 等；应用系统：如 Apache、Tomcat、IIS、Weblogic 等；网络设备：主流的路由器、交换机、负载均衡等网络设备

支持对日志格式进行标准化操作时，不破坏原始日志内容。从不同设备或系统的日志中抽取相关片段准确和完整地映射至日志的标准字段中，统一格式。支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析。

◆支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志（需提供产品功能截图证明）

支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。

## 6、网络版防病毒

具体要求
<p>性能参数：终端桌面需要配置 50 点。</p> <p>采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能</p> <p>支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞及其各自影响的终端数量；</p> <p>支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示；</p> <p>支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具</p> <p>支持与同厂商的网络防火墙进行安全配置，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息</p> <p>◆支持对 Windows 停更的系统提供专项防护,包括 0day 漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能；（需提供产品功能截图证明）</p>

## 7、核心交换机

具体要求
<p>硬件要求：≥24 个千兆电口+4 个万兆光口（含 2 个万兆多模原装光模块），双电源插槽，默认含 1 个 AC 电源，一个扩展插槽，交换容量≥1.28 Tbps/12.8 Tbps，包转发率≥216/366Mpps。</p> <p>技术要求：支持完善的二、三层组播协议，支持 PIM SM、PIM DM、PIM SSM、MLD、IGMP Snooping 功能，支持 OSPF、ISIS、BGP、VRRP 等三层特性，机支</p>

持完善的 DoS 类防攻击、用户类防攻击，机支持超级虚拟交换网，可将多台设备虚拟成一台设备，机支持 SmartLink 功能。通过多条链路接入到多台汇聚交换机上，支持部署在纯 IPv4 或 IPv6 网络，也支持部署在 IPv4 与 IPv6 共存的网络，充分满足网络从 IPv4 向 IPv6 过渡的需求。

## 8、技术安装调试

### 具体要求

含安装调试光纤、跳线等辅材，各团场分局存在多个路由网关，调试至链路通畅，保障师局到各分局团场的双链路（政务外网、专网）文件的正常下发与接收。

## 9、安全智能视频门禁

### 指标要求

安全智能视频门禁是一款集刷卡、人脸识别、智能抓拍等功能为一体的门禁系统。产品是以 GM/T 0036 标准为基础，结合 GB/T 39786 等其他相关标准，采用国产密码算法对重要物理区域（如计算机集中办公区、设备机房等）出入人员的身份进行鉴别，同时对门禁记录的完整性进行保护，可应用于等保三级（及以上）信息系统的等保密评建设和整改需求。

1. 采用国产芯片，国产算法，保障门禁系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性要求；
2. 门禁系统满足 GB/T 0036 标准，提供商用密码认证证书原件扫描件；
3. 具有抓拍功能，除了抓拍正常刷脸或者刷卡开门照片上传到后台以外，还具有陌生人抓拍预警功能；
4. 支持人脸识别加刷卡双认证开门方式，保证人证合一，有效防止门禁卡被乱用或者盗用；
5. 内置双目近红外摄像头，基于光流分析的人脸识别技术，防止照片、视频攻击；
6. 一站式解决方案，整个方案设计、安装、部署、实施简单方便快捷；
7. 门禁基本参数：操作系统 Linux，CPU VC0718P，内存  $\geq 1G$ ，存储  $\geq 1G$  NANDFLASH+16G 扩展储存，验证开门方式不少于：刷卡、人脸识别、刷卡+人脸识别；人脸比对速度：白天  $\geq 500ms$  夜间  $\geq 900ms$ ，人脸特征值存储容量  $\geq 3000$  条，CPU 卡存储容量  $\geq 3000$  条，显示屏  $\geq 7$  寸，分辨率  $\geq 1024*600$ ，工作电压  $\geq 12V \pm 10\%$ ，工作电流  $\geq 1.5A$ ，门锁控制方式：RS485，使用环境： $-10^{\sim}+55^{\circ}C$ 。

## 10、门禁卡

指标要求
门禁卡卡内存放发行信息和卡片密钥。内置国密芯片。 门禁卡采用国家密码管理局认证的国密 CPU 卡，符合 GM/T 0028-2014《密码模块安全技术要求》（或 GB/T 37092-2018《信息安全技术密码模块安全要求》），符合 GM/T 0041-2015《智能 IC 卡密码检测规范》，安全等级第二级相关要求。提供商用密码安全二级认证证书原件扫描件。

## 11、后台登录读卡器

指标要求
用于登录门禁管理后台，通过管理员密码及国密卡硬件介质双重认证对后台登录人员进行身份认证，读卡器中内置国家密码局认证的安全芯片；需提供商用密码安全二级认证证书原件扫描件。

## 12、门禁管理后台一体机

指标要求
1. CPU $\geq$ 四核；硬盘 $\geq$ 256G SSD+1T 机械硬盘；内存 $\geq$ 8G；系统:Linux 系统； 2. 每台服务器可支持 $\geq$ 128 路门禁前端； 3. 包含门禁管理后台软件：安装门禁管理后台软件，实现门禁设备管理、人员管理、门禁记录存储，日志管理、角色管理等功能； 4. 后台系统与门禁前端通讯采用加密； 5. 服务器内置具有防拆功能的安全存模块，该安全模块采用一款 32 位多用途高性能安全芯片，符合 GM/T 008-2012《安全芯片密码检测准则》安全等级第二级相关要求。服务器密钥存储在安全芯片的密钥存储区，以此来保证服务器密钥的安全；提供商用密码安全二级认证证书原件扫描件； 6. 基于 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》，采用经商用密码认证机构认证合格的安全芯片进行密码运算，基于杂凑算法对门禁

记录定期进行完整性校验，若发现被保护数据的完整性被破坏，后台会产生告警。

7. 标配≥5 张后台管理员的登录国密卡。

### 13、门禁控制器

指标要求
门禁控制器是控制门锁的执行单元，内置国家密码局认证的安全芯片，采用国密算法与门禁机前端进行加密通讯； 功能：单/双门单门禁机（单向），单/双门双门禁机（双向），1 路门状态反馈，1 路报警输入，RS485 通讯方式； 门禁控制器包括：门禁控制模块、门禁电源、漏电开关、接地排，门禁机箱。

### （三）互联网设备要求

#### 1、安全感知平台

指标要求
产品形态：平台 SAAS 化形态交付，满足互联网区安全感知建设需要，无需要在数据中心进行任何下载和安装，通过账号密码在云端获取服务。 支持首页展示风险总览、包括安全事件总览、资产统计、接入设备展示、待处置安全事件 TOP5、攻击面 TOP5、脆弱性资产 TOP5、风险资产分布及风险资产发生趋势、待处置安全事件分布及安全事件发生趋势。可清晰明确下一步处置方向。 支持自定义可视化组件，包括资产范围、图表类型、聚合维度、度量模式、字段定义等。 支持自定义仪表盘，可圈定资产范围，内置安全告警试图、资产视图、脆弱性风险视图、风险资产视图等模板，展示图表样例包括文字、条形图、水平条形图、趋势图、饼图、表格、指标、markdown 等，可编辑背景及标题样式，可全

## 局预览

◆支持云端专家提供轻量安全服务，进行持续的威胁狩猎，发现潜在威胁；在有攻击事件生成后，进行二次确认，通过标签进行辨别，对热门威胁进行响应；（需提供产品功能截图证明）

支持对事件等级、威胁标签、数据源、处置状态等进行快速筛选，并提供简易模式和专家模式两种调查方式，简易模式可基于字段名称进行检索、专家模式采用 SPL 语句检索

支持查看 ATT&CK 攻击矩阵攻击命中全景图并匹配对应告警，可清晰了解安全事件中被黑客技战术利用的情况，提升研判效率。同时可查阅命中技术 ID、命中次数、技术描述和参考来源

支持通过安全事件详情查看攻击故事线、安全事件按照进程树的视角进行安全分析。可详细点开进程链中任意进程查看进程详情，包括基础信息、威胁告警、网络连接行为、文件行为、域名访问行为、模块加载行为，并且自带解码工具。（需提供产品功能截图证明）

◆支持对安全事件推送处置和响应建议，响应建议包括原理介绍、危害影响、处置建议。通过建议描述、业务影响标签和安全效果标签清晰明确指导下一步响应动作，可一键封禁 IP、隔离主机等。支持在线实时聊天框或离线留言咨询攻防专家，获取云端专家支持。（需提供产品功能截图证明）

支持展示资产基础信息包括基础信息、关联 IP、操作系统、设备信息、责任人；开放端口信息、账号信息及登录历史、应用软件信息、硬件信息及数据来源等。（需提供产品功能截图证明）

支持以资产视角，对终端遥测及网络遥测扫描到的资产脆弱性进行展示，可对资产修复优先级、风险类型、风险资产及资产组名、责任人等标签进行筛选，并通过图表进行统计展示资产修复优先级情况、脆弱性统计情况、资产脆弱性 TOP5

支持智能对抗功能，智能响应安全事件和安全告警中的关键威胁，外部攻击阶段式拦截，失陷实体自动遏制。对 IP、文件、域名等实体联动安全设备自动处置，可查看智能对抗记录，并且支持自定义对抗规则。

## 2、链路负载均衡

### 具体要求

性能参数：4层吞吐量（默认网口） $\geq 3\text{Gbps}$ ，四层并发连接数 $\geq 8000000$ ，4层新建连接数 CPS $\geq 100000$ ，7层新建连接数 RPS $\geq 150000$ 。硬盘容量： $\geq 128\text{G}$  SSD，接口：6千兆电口+2千兆光口 SFP。

部署方式支持双机热备形式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换；与现有负载均衡设备、以及链路之间的冗余互备，能够实现与现有设备部署双机热备功能；

支持 PPPOE 和静态 IP 两种线路接入方式；

支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略；

◆支持链路负载情况的投屏展示，能够分别实现基于 ISP 流量、应用选路和链路监测进行投屏展示分析。ISP 流量展示基于运营商分类选择链路的示意图；链路监测展示链路的上下行带宽、健康状态、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；（需提供产品功能截图证明）

内置智能告警系统，支持两种告警方式，管理员可基于业务安全所关注方面来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（如服务器宕机、网络攻击、链路中断等故障场景），即会自动向管理员发送告警信息；

支持在同一个虚拟服务下同时配置多个 IPv4 和 IPv6 地址；

支持跨数据中心集群和跨数据中心会话保持

支持 SNMP v1/v2c/v3，提供标准的 MIB 库下载，可接受第三方网管平台的管理；

### 3、下一代防火墙

#### 具体要求

硬件参数：内存大小 $\geq 8\text{G}$ ，硬盘容量 $\geq 128\text{G}$  SSD，接口 $\geq 8$  千兆电口+2 万兆光口 SFP+。

性能参数：网络层吞吐量 $\geq 20\text{G}$ ，应用层吞吐量 $\geq 9\text{G}$ ，防病毒吞吐量 $\geq 1.5\text{G}$ ，IPS 吞吐量 $\geq 1.3\text{G}$ ，并发连接数 $\geq 200$  万，HTTP 新建连接数 $\geq 9$  万。

产品支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护等攻击类型。

产品内置不低于 10000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。

◆支持 Cookie 攻击防护功能，日志能够记录 Cookie 被篡改。所投产品必须提供具备 CMA 认证的第三方权威机构关于“Cookie 攻击防护”功能项的产品检测报告。

产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。

产品支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。

产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。

支持与网络版防病毒软件统一管理，在防火墙产品完成防病毒软件策略设置和防病毒软件的统一管理。

要求所投产品具备国家信息安全漏洞库兼容性资质证书，提供有效证书原件扫描件。

#### 4、漏洞扫描系统

##### 具体要求

性能参数：系统漏扫授权 IP 数 $\geq 100$ ，WEB 漏扫授权 URL 数 $\geq 20$ ；主机漏扫最大并发 IP 数 $\geq 150$ ，WEB 漏扫最大并发 URL 数 $\geq 5$ 。

采用有自主知识产权的安全操作系统，采用 B/S 设计架构，支持软件化交付，部署在现有云平台上，并采用 SSL 加密通信方式，无须安装客户端，用户可通过浏览器远程方便的对产品进行管理。

支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描等， $\geq$ 四种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。

提供检测结果综述分析，按照等保 2.0 的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。

支持统一管理所有业务系统的合规情况，合规报告可导出。业务系统差距报告量化、可视化整改前后的符合情况和安全问题。

产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表。

系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果支持报表导出的格式包括 HTML、WORD、EXCEL 等格式。

## 5、准入控制

### 具体要求

硬件参数：硬盘容量 $\geq 128\text{G}$  SSD，接口 $\geq 4$  千兆电口

性能参数：网络层吞吐量（大包） $\geq 3\text{Gb}$ ，带宽性能 $\geq 200\text{Mb}$ ，支持用户数 $\geq 500$ ，准入终端数 $\geq 300$ ，准入终端数的扩容上限（支持客户端授权） $\geq 500$ ，每秒新建连接数 $\geq 2400$ ，最大并发连接数 $\geq 120000$ 。

支持对在网接入终端进行统一可视化管理，可视化内容包括终端详细信息、合规状态等，支持查看入网终端详细信息（类型、厂商，系统，端口等）

支持 windows 终端安全检查，包括：杀软检查、登录域检查、操作系统检查、进程检查、文件检查、注册表检查、补丁检查、windows 账号检查、防篡改检查、客户端集成检查，对不满足检查要求的终端可弹窗提示、禁止上网、违规修复；

◆支持 windows 终端调用管理员指定脚本或程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网；（需提供产品功能截图证明）

无需安装入网客户端，可通过获悉流量行为及状况检查行业主流杀毒软件的运行情况，对不满足检查要求的终端（未安装指定要求的杀毒软件或杀毒软件版本不符合要求）可进行下载页面重定向，帮助终端用户进行运行环境修复；

支持存储设备、网络设备、蓝牙设备、摄像头、打印机的使用管控；

支持允许特定的外设（包括 U 盘/存储设备）在终端上使用，并提供批量获取硬件 ID 的工具；

支持对 Windows 终端外联行为进行检查，包括但不限于连接外网检查、PPPoE 拨号检查、双网卡行为检查、无线网卡检查、链接非法 WIFI 检查（可设置合法 WIFI 白名单）、4G 网卡检查、是否使用非法网关（可设置合法网关白名单）等场景，对不符合检查要求的终端强制断网，弹窗提示用户进行修复，并将告警消息通知系统管理员；

支持根据访问的 URL 和网页关键字进行网页过滤，支持设置拒绝以 IP 访问网页行为；

能够与本次采购的“安全态势感知系统”产品兼容对接，完成数据上传，实现资产管理信息的同步；

新疆建友友成工程管理咨询有限公司

## 6、检测探针

具体要求
<p>性能参数：网络层吞吐性能<math>\geq 500</math> Mbps，应用层吞吐性能<math>\geq 160</math> Mbps。</p> <p>硬件参数：硬盘容量<math>\geq 128</math>GSSD，接口<math>\geq 6</math> 千兆电口。</p> <p>具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。</p> <p>支持 FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测</p> <p>支持 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞等网站攻击检测；</p> <p>为检测异常流量，需支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等。</p> <p>支持 ICMP、UDP、SYN、DNS 等协议外发异常流量检测，支持自定义阈值。</p> <p>支持设备内置简单命令行管理窗口，便于基础运维调试；可实时监控设备的 CPU、内存、存储空间使用情况；</p>

## 7、下一代防火墙

具体要求
<p>硬件参数：内存大小<math>\geq 8G</math>，硬盘容量<math>\geq 128G</math> SSD，接口<math>\geq 8</math> 千兆电口+2 万兆光口 SFP+。</p> <p>性能参数：网络层吞吐量<math>\geq 20G</math>，应用层吞吐量<math>\geq 9G</math>，防病毒吞吐量<math>\geq 1.5G</math>，IPS 吞吐量<math>\geq 1.3G</math>，并发连接数<math>\geq 200</math> 万，HTTP 新建连接数<math>\geq 9</math> 万。</p> <p>产品支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护等攻击类型。</p> <p>产品内置不低于 10000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。</p> <p>产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。</p> <p>产品支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。</p> <p>产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。</p> <p>支持与网络版防病毒软件统一管理，在防火墙产品完成防病毒软件策略设置和防病毒软件的统一管理。</p> <p>要求所投产品具备国家信息安全漏洞库兼容性资质证书，提供有效证书原件扫描件。</p>

## 8、日志审计系统

### 具体要求

性能参数:默认包含主机审计许可证书数量 $\geq 100$ ,平均每秒处理日志数(eps)最大性能 $\geq 2500$ 。支持软件部署,能够部署在现有云平台上,通过SSL加密对数据传输等进行处理、采用B/S架构,HTTPS访问

支持各类设备的日志采集要求,主要包括:安全设备:国内主流防火墙;操作系统:Linux、Windows、Windows Server、Unix等操作系统;数据库:Oracle、MySQL、SQLServer等;应用系统:如Apache、Tomcat、IIS、Weblogic等;网络设备:主流的路由器、交换机、负载均衡等网络设备。支持对日志格式进行标准化操作时,不破坏原始日志内容。从不同设备或系统的日志中抽取相关片段准确和完整地映射至日志的标准字段中,统一格式。支持单条事件进行展开,显示事件详细信息和事件原始信息,支持事件详情中任意字段作为查询条件无限制进行二次检索分析。

支持对单个/多个日志源批量转发,支持定时转发,可通过syslog和kafka方式转发到第三方平台,并且支持转发原始日志和已解析日志的两种日志。支持对每个日志源设置过滤条件规则,自动过滤无用日志,满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数,减少对网络带宽和数据库存储空间的占用。

## 9、网络版防病毒

### 具体要求

性能参数：终端桌面需要配置 $\geq 50$ 点，服务器终端安全响应需要配置 $\geq 20$ 点，终端安全检测响应平台需要支持不得少于接入200点。

采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能

支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量；

支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示；

支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具

支持与同厂商的网络防火墙进行安全配置，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息

支持对Windows停更的系统提供专项防护，包括0day漏洞防护、文件防护、爆破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能；（需提供产品功能截图证明）

支持与本次投标的安全态势感知平台进行兼容，支持管理员在安全感知平台管理界面下发快速查杀任务及一键隔离指令，并支持查看任务状态、任务结果并进行联动终端所有连接进行阻断

## 10、数据库审计

### 具体要求

硬件参数：内存大小 $\geq 8G$ ，硬盘容量 $\geq 2T$  SATA，接口 $\geq 6$  千兆电口+2 万兆光口 SFP+，规格：2U；冗余电源

性能参数：最大硬件吞吐量 $\geq 2Gbps$ ，最大纯数据库流量 $\geq 400Mb/s$ ，数据库实例个数 $\geq 30$  个，SQL 处理性能 $\geq 30000$  条 SQL/s，日志检索性能 $\geq 500000$  条/秒。要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、及用户手动升级系统补丁；

采用 B/S 管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务；

支持以图表方式（饼图、柱图、曲线图、清单列表）显示日志数据分布情况；支持自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果。支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询。

支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行。

内置大量 SQL 安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、查询内置敏感表、篡改内置敏感表等；

## 11、堡垒机

### 具体要求

性能参数：默认包含运维授权数 $\geq 50$ ，最大可扩展资产数 $\geq 150$ ，图形运维最大并发数 $\geq 100$ ，字符运维最大并发数 $\geq 200$ 。硬盘容量 $\geq 2T$  SATA，接口 $\geq 6$  千兆电口。规格：1U

系统各模块支持以 B/S 方式管理，采用 https 加密方式访问

内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴

口令变更至少支持 windows 系统、网络设备、linux/unix 系统、数据库等

支持命令黑名单，对字符型设备（如 linux/unix/网络设备）的高危命令执行进行阻断，如 rm、shutdown、reboot 等

支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人

图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放

支持提供系统内部操作审计，包括管理员和运维用户的登录、登出、对系统的配置操作、账号属性修改等系统管理操作

全面支持 Windows、linux、国产麒麟系统、Android、IOS、Mac OS 等客户端操作系统下的 H5 页面一站式运维，实现跨终端适应性 BYOD (Bring Your Own Device)

## 12、WAF 防火墙

### 具体要求

硬件参数：内存大小 $\geq 8G$ ，硬盘容量 $\geq 128G$  SSD，接口 $\geq 8$  千兆电口+2 万兆光口 SFP+。

性能参数：网络层吞吐量 $\geq 20G$ ，应用层吞吐量 $\geq 9G$ ，防病毒吞吐量 $\geq 1.5G$ ，IPS 吞吐量 $\geq 1.3G$ ，并发连接数 $\geq 200$  万，HTTP 新建连接数 $\geq 9$  万。

产品支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护等攻击类型。

产品内置不低于 10000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。

产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。

产品支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。

产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。

支持与网络版防病毒软件统一管理，在防火墙产品完成防病毒软件策略设置和防病毒软件的统一管理。

要求所投产品具备国家信息安全漏洞库兼容性资质证书，提供有效证书原件扫描件。

### 13、前置机

#### 具体要求

处理器：≥2 颗，主频≥2.9GHz；每个 CPU 核数≥16C；

内存：≥256GB 内存，≥24 条扩展插槽；

硬盘：本次配置≥2\*240G SSD 系统盘，缓存盘≥2\*960G SSD，数据盘≥2\*8T SATA

接口：千兆以太网电口≥6 个，≥2 个万兆光口，

电源：冗余电源，支持热插拔功能；

故障定位：标配 BMC 诊断模块，可实现对 CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊断。

包含 4 颗物理 CPU 的虚拟化授权，包含服务器虚拟化、网络虚拟化、存储虚拟化以及云计算管理平台等模块授权。

支持上传或利用现有云主机创建镜像，可对镜像进行管理、关联资源池等操作，可通过镜像实现一键快速创建云主机及安全组件

◆为尽可能保障数据中心断电场景下的业务，可在市电断电时通过 UPS 临时供应电量，当 UPS 电量过低时，按照虚拟机优先级先将不重要的虚拟机进行软关机（需提供产品功能截图证明）。

虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 MAC 地址等。

在管理平台界面上提供虚拟机删除、开关机、挂起与恢复、重启、关闭、关闭电源、克隆、迁移、备份、模板导出、快照、标签管理等功能，并支持批量操作。

支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用 License 激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能。

◆为保障实时备份功能与虚拟化平台的深度兼容，要求实时备份功能与虚拟化平台为统一品牌或第三方整合方案，要求实时备份配置与虚拟化平台统一管理，如果是第三方整合方案，要求投标人出具厂家兼容性报告，并加盖备份厂

商公章；

支持存储分卷功能，以物理主机为单位划分为不同的存储卷，如高性能卷，大容量卷，全闪存卷等，可使对存储性能和容量要求不同的业务运行在不同的存储卷上

支持针对卡慢盘、异常只读盘的自动检测、自动隔离及手动隔离，隔离分为临时拔盘、永久拔盘（注：永久拔盘后，需要手动替换磁盘，原有磁盘离线后无法上线），消除磁盘异常对业务影响

◆支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性（需提供产品功能截图证明）  
分布式防火墙基于监测虚机 IP 地址、MAC 地址和端口进行东西向流量隔离控制，并提供实时拦截日志，以及支持“数据直通 Bypass”功能，方便出现问题快速定位问题。

支持创建分布式虚拟防火墙，可基于虚拟机、虚拟机组、虚拟机标签、IP、IP 范围、IP 组构建安全防火墙，当虚拟机在不同的物理节点之间迁移时，安全策略随之移动

◆支持在同一虚拟化主机或集群上同时运行 VDI 虚拟机和业务虚拟机，并使用同一管理平台同时管理桌面云与业务虚拟机。（提供厂商出具的证明材料并加盖公章的复印件）

要求服务器与终端、服务器虚拟化软件、存储虚拟化软件、桌面云软件为同一品牌。

#### （四）密码安全管理设备要求

##### 1、IPSec/SSL VPN 综合安全网关

指标要求
2U 机架式硬件设备， 内置密码卡（密码卡必须具有商用密码认证证书）。

内存：≥4GB

1+1 冗余电源供电。

◆具备国家密码管理局颁发的商用密码产品认证证书。（提供证明材料。）

≥4 个 10/100/1000M 自适应网

≥4 个 SFP 千兆光插槽

≥2 个 USB

IPSec:

密文吞吐率 (SM4) : ≥800Mbps

最大隧道数: ≥3000

SSL:

每秒新建用户数 (SM2) : ≥200tps

最大并发连接数: ≥20000

最大并发用户数: ≥2000

密文吞吐率 (SM4) : ≥600Mbps

支持双主机热备部署，支持主备机自动切换。支持多机负载均衡，支持负载动态分配。

支持“多因子”身份鉴别与访问控制。认证因子至少包含 PIN 码、数字证书和口令。

SSL 自适应，搭配国密和非国密浏览器，实现 SSL 自适应，实现数据以 HTTPS 形式传输。

提供安全接入客户端。客户端支持银河麒麟操作系统、中标麒麟操作系统、UOS 操作系统等国产操作系统。

管理员登录支持数字证书 (SM2) + 口令的“双因子”认证方式。

提供整机商用密码产品认证证书。

## 2、设备证书

指标要求
由第三方电子认证机构 CA 系统签发给 IPSEC/SSL VPN 综合安全网关、签名验签与时间戳二合一服务器,标识设备的身份。

## 3、数字证书

指标要求
签发的数字证书服务符合国家商用密码管理规范； 通过国家密码管理局的相关产品资质认证，支持 PKI 应用； 支持 SM2 非对称加密算法，能够快速完成 SM2 算法的签名、签名认证、加密、解密运算。 提供服务网点，能够快速响应客户需求。

#### 4、服务器密码机

指标要求
<p>1. 配置指标</p> <p>标准 2U 机架式硬件设备；</p> <p>基于国产硬件平台、操作系统以及相关软硬件组成；</p> <p>≥2 个 100/1000M 自适应网口。</p> <p>◆具备国家密码管理局颁发的商用密码产品认证证书。（提供证明材料。）</p> <p>2. 性能指标</p> <p>SM2 算法：</p> <p>生密钥：29000 对/秒；签名速度 29000 次/秒；验签速度：24000 次/秒；</p> <p>加密速度：15500 次/秒；解密速度：19800 次/秒；</p> <p>SM4 算法加解密速度：700Mbps/700Mbps</p> <p>SM3 杂凑算法：790Mbps</p> <p>3. 功能指标</p> <p>1) 非对称算法加/解密：</p> <p>能够实现 256 位 SM2 算法的公钥加密和私钥解密功能；</p> <p>2) 数字签名/验证功能：</p> <p>提供基于 SM2 算法的数字签名和认证功能，可用于证书生成和验证、身份认证等。</p> <p>3) 对称密钥加/解密：</p> <p>提供国家标准的 SM1 算法和 SM4 算法，用于数据的加解密；</p> <p>4) 随机数生成：</p> <p>采用国家密码管理局批准的双 WNG-9 硬件物理噪声源生成真随机数，随机数质量高。</p> <p>5) 密钥生成与管理</p> <p>提供 256 位 SM2 密钥生成算法及密钥备份和恢复。有非对称密钥对导入、导出功能，便于密钥对的备份、恢复及多机并行工作时各密码机密钥对的一致。在</p>

密钥导入、导出时，私钥是密文的。

#### 6) 集群支持及性能扩展：

支持多线程、多任务和性能扩展。

多机热备和负载均衡。

支持通过 SNMP 协议监控设备状态，可反馈服务器密码机后台服务状态、业务连接数、密码机 CPU、内存使用量等。

支持 keystore 的配置和管理功能。

支持设备网口配置管理功能，可将网口设置为仅用于管理、仅用于提供服务或兼容三种状态。

支持服务器密码机日志完整性保护。

支持多版本备份恢复。

新疆建友友成工程管理咨询有限公司

## 5、签名验签和时间戳二合一服务器

指标要求
<p>1. 配置指标</p> <p>2U 机架式硬件设备；</p> <p>基于国产硬件平台、操作系统以及相关软硬件组成；</p> <p>◆具备国家密码管理局颁发的商用密码产品认证证书。（提供证明材料。）</p> <p>内置密码卡；</p> <p>硬盘：≥32GB 固态硬盘。≥2 个 100M/1000M Base-T RJ45 接口，≥1 个液晶显示屏，≥4 个 USB 接口</p> <p>符合 GM/T 0029-2014《签名验签服务器技术规范》、GM/T 0033-2014《时间戳接口规范》、GM/T 0028-2014《密码模块安全技术要求》第二级要求。</p>
<p>2. 性能指标</p> <p>SM2 算法：</p> <p>签名速度：≥11290 次/秒；验签速度：≥6040 次/秒；（测试方法依据 GM/T 0029-2014《签名验签服务器技术规范》中单包数字签名/验签相关要求）</p> <p>签名速度：≥4260 次/秒；验签速度：≥3960 次/秒；（测试方法依据 GM/T 0029-2014《签名验签服务器技术规范》中单包带消息数字签名/验签相关要求）</p> <p>SM3 杂凑算法：≥860Mbps</p> <p>数字证书验证速度：≥1500 次/秒；数字信封制作速度：≥2080 次/秒；数字信封解封速度：≥3060 次/秒</p> <p>SM2 签名密钥对数量：≥500 对 SM2 加密密钥对数量：≥500 对 对称密钥数量：≥1000 个</p> <p>时间戳签发速度：≥2700 次/秒</p> <p>时间戳验证速度：≥2600 次/秒</p> <p>授时精度：4G-LTE 时间源授时精度≤15ms,GPS/北斗授时精度≤10 μs</p>
<p>3. 功能指标</p> <p>数字签名/验证功能：</p>

提供基于 SM2 算法的数字签名和认证功能，可用于证书生成和验证、身份认证等。

支持双机热备部署。

支持 CPU 和内存的利用率、磁盘占用率、网络状态、用户登录状态等的实时监控。

时间戳签发和验证功能

支持基于 SM2 算法的时间戳服务，为应用系统提供时间戳签发、验证时间戳服务，实现对数据、消息、文件等多种格式原文数据的时间戳签发服务。

支持将用户签名证书、加密证书导入设备。

支持 OCSP 在线查询服务配置和 CRL 自动更新配置。

支持指定算法类型、密钥号等信息，生成 P10 申请文件并导出。

支持设备初始化功能，为防止误操作，支持对设备初始化功能进行启用和关闭控制。

在满足权限的情况下，支持将设备内的密钥等重要信息加密后进行备份，并且可以恢复到相同型号的设备中，备份采用 (3, 5) 门限方式，产生备份密钥并分割导出到 5 个智能密钥钥匙中。

支持数字证书有效性验证策略配置，至少包括验证证书有效期、验证证书签名有效性、验证证书是否在 CRL 中三种验证策略。

## 6、技术安装调试

### 指标要求

用户角色关联表、角色功能关联表的重要字段进行基于 SM3 算法的 HMAC 运算，实现对访问控制信息完整性保护。规划并完成项目所需要用到的对接文档和接口协议。

调用服务器密码机，内部对称加密接口 InternalSM4Enc 对敏感数据（根据业务系统性质判断，包括但不限于用户手机号、身份证号、住址等）做加密操作，然后将密文存储于数据库中。业务系统从数据库中读取已加密过的数据，调用服务器密码机，内部对称加密接口 InternalSM4Dec 做解密操作，然后将解密后的明文信息展示。

## 7、安全智能视频一体化服务系统

指标要求
采用 USBkey 处理密码；8 路(GB35114 C 级)前端接入；2U $\geq$ 8 盘位， $\geq$ 4 块 8T 硬盘；含一个客户端 UKEY； ◆信息安全标准支持 GB35114-2017，支持视频认证和加密，满足 GB/T 0028 标准安全二级要求，需提供证书原件扫描件； 内置国密 UKEY，全面符合国密标准，国密算法加密和认证，保证数据的安全性和真实性 8 路(GB35114 C 级)前端接入； 支持 SVAC2.0、H.264、H.265 编码； 接入 $\geq$ 32Mbps，储存 $\geq$ 32Mbps，转发 $\geq$ 16Mbps； 最大支持 4 路录像回放（单路 4Mbps 1080P）； WEB 单客户端最高 4 路 1080P 4M 码流解码； WEB 客户端支持 35114 验签及解密播放； 使用国密标准的 UKEY； 显示输出接口 $\geq$ 1 个 VGA，2 个 HDMI； 网口 $\geq$ 2 个千兆网口。

## 8、USBKey

指标要求
支持与 CA 系统协同颁发数字证书； 非对称运算（RSA）：签名：不低于 10 次/秒；验签不低于 20 次/秒； 非对称运算（SM2）：不低于 5 次/秒； 支持对称预算（SM4）：不等于 20Mbps/秒； 支持的操作系统：win7 32/64 位；Linux； ◆需提供商用密码安全二级认证证书原件扫描件。

## 9、一体化高清网络视频设备

指标要求
采用高性能 1/2.8 英寸图像传感器； 输出 200 万像素 1920x1080@25fps 高清视频编码； 内置 4 倍 2.8-12mm 电动调焦镜头，方便调试与维护； 内置 30 米红外补光，夜间看得更清楚； 支持国家编码(GB/T25724-2017 )，需提供检测报告； 信息安全标准支持 GB35114-2017，支持视频认证和加密； ◆内置国密芯片，全面符合国密标准，国密算法加密和认证，保证数据的安全性和真实性，满足密码测评要求，需提供商用密码安全二级认证证书原件扫描件； 支持 Micro SD 存储卡，最高支持 256G； 支持 GB/T.28181，ONVIF，ViSS 等互联协议； DC12V±10% 最大功耗 12W（补光灯开启）、8W（补光灯未开启） 工作温度 -35℃~+65℃ 工作湿度 20%~85%，无冷凝。

## 10、视频监控专用数字证书

指标要求
视频监控专用数字证书，国密双证书。

新疆建友友成工程管理咨询有限公司

注：1. 招标文件技术参数均为参考指标，并不局限于某一品牌或规格型号。供应商在投标中可以选用替代指标，但这些替代技术指标要实质上相当于或优于招标文件中的要求。以上所供内容不少于参数内容，但可增加，以保证达到正常使用。否则所有产生不良后果，由投标人自行承担。

2. 供应商中标后，须提供符合技术参数要求的有效检测报告（格式自拟），签订合同时需提供技术参数中要求的检测报告及相关证明材料，相关证明材料原件作为合同附件的一部分，同时供应商对已提交的材料的真实性负责，如供应商提供虚假材料谋取中标，则承担相应法律责任。

▲3. 本项目为交钥匙工程，《设备或软件需达到正常使用，若有任何问题中标单位自行承担）完成等保三级测评后存在的软件漏洞升级，达成等保三级的测评要求，中标人负责对所供设备进行安装和调试及后期设备维保等工作，所需的安装配件及辅材等由中标人提供；最终报价含前期踏勘（供应商如有需要可自行踏勘）、采购、运输、进口关税、安装、调试、校正、培训费、网络信息维护、一切配件附件费及不可预见的费用等。并对上述要求予以承诺证明。（承诺格式自拟）

## 二、商务、服务要求

### 1. 售后服务要求：

(1) 投标人应响应本次招标项目服务要求并在投标文件中提供详

细具体的售后服务条款及保证。投标产品由制造商（指产品生产制造商，或其负责销售、售后服务机构，以下同）负责标准售后服务的，应当在投标文件中予以明确说明，并附制造商售后服务承诺。

（2）（验收完毕后）承诺三年内免费质保，终生维护。三年后提供有偿的售后服务。若某项设备或产品的质保期在技术参数中有规定的从其规定，国家另行规定的以国家规定为准。

（3）投标产品属于国家规定“三包”范围的，其产品质量保证期不得低于“三包”规定。供应商的质量保证期承诺优于国家“三包”规定的，按供应商实际承诺执行。

（4）消耗品和零配件供应及时，特殊情况下可提供备产品。

（5）投标人提供7×24小时的电话热线咨询服务，30分钟内响应。如电话不能解决，则在4小时内工程技术人员到达现场维修。对于重大的技术问题，对所供设备有一定的配件及替换产品，确保招标人正常使用。（具体要求签订合同时拟定）

（6）免费提供每年不少于2次的现场预防性服务和跟踪服务。保修期内免费更换零配件、免工时费。（招标人需要由原投标人或制造商提供本项目货物采购所涉及的备品备件及易损件应为原厂配件，未经招标人同意不得使用非原厂配件。）

## 2、交货期、交货地点及验收方式

### （一）交货期

▲签订合同后。按招标人要求所有设备30日历天内完成安装调试、培训、验收等。此次项目不另追加任何费用，中标人不得以任何

理由，提出任何形式的增加合同价款或增加资金的要求。中标人规划并完成项目所需要用到的对接文档和接口协议，自行协调，若有费用需自行承担。

## （二）交货地点及实施单位

招标人指定地点

## ▲（三）验收方式

（1）中标人应提供货物的技术文件，包括但不限于设备配置清单、产品说明书、图纸、操作手册、维护手册（含维修密码及接口数据）、质量保证文件、服务指南等。文件应随货物一并交付至招标人指定地点。

（2）提供的货物必须为全新、经检验合格的产品。产品如需要计量检定的应提供招标人当地相关计量检定部门出具的合法检定报告（如有）。

（3）中标人负责将货物安全无损运抵招标人指定地点，并承担设备的包装、运输、保险、装卸、安装调试、培训、商检及计量检测、关税、增值税和进口代理等所有费用（如有）。

（4）货物到达现场后，应由中标人代表和招标人组成验收小组对产品进行开箱检查，共同清点、检查外观，以确认货物是否符合合同规格的要求，做出开箱记录，双方签字确认。

（5）招标人不承担额外的费用。如果发现所交货物与投标文件中所承诺的不符或存在质量、技术缺陷等，招标人可以拒绝接收该货物，投标人应在3天内采取补足、更换或退货等措施，以满足规格的要

求，由此发生的一切损失和费用由投标人承担。中标人应在货物验收后半个月内完成安装调试完毕。

(6) 中标人应提供完备的技术资料、装箱单和合格证等，并派遣专业技术人员进行现场安装调试。安装调试完毕后，由中标人代表、派遣的专业技术人员和招标人、招标人邀请的专业技术专家及国家认可的质量检测机构专家组成验收小组，共同对产品进行验收，验收标准按照国家规定标准执行。经检验设备正常运行符合要求后，才作为最终验收，并签署验收报告，产品保修期自验收合格之日起算。验收合格条件如下：

1. 设备技术参数与采购合同一致，性能指标达到规定的标准。
2. 货物技术资料、装箱单、合格证等资料齐全。
3. 系统软件（如有）运营良好、稳定。在设备试运行期间所出现的问题得到解决，并运行正常。
4. 检验技术支持和系统维护服务的运行过程符合采购需求。
5. 在规定时间内完成交货并验收，并经招标人确认。
6. 中标人若为代理商（关键产品），在项目实施验收时需提供所投产品生产厂家授权书及售后服务承诺函原件。
7. 招标人需要制造商对中标人交付的产品（包括质量、技术参数等）进行确认的，制造商应予以配合，并出具书面意见。
8. 产品包装材料归招标人所有。
9. 投标人应当在投标文件中列出完成本项目并通过验收所需的所有各项服务等明细表及全部费用，罗列与分项报价中。中标人必须

确保整体通过用户方及有关主管部门验收，所发生的验收费用由中标人承担；中标供应商应提供设备之前踏勘现场，如中标供应商因未及时踏勘现场而导致无法按时完工，投标人供应商自行承担一切后果。

**▲3、报价要求**（投标报价应包含完成招标文件规定的招标范围全部内容所需的全部费用）。

（1）本次报价须为人民币报价，报价包括但不限于产品的设计、制造（开发）、运输（含包装、运输和货到现场的二次装卸）、保险（交货验收前）、现场保管、仓储、搬运设备、通讯、安装（含安装人员现场住宿、伙食）、安装调试等所涉及到的软硬件费用、材料费用、施工费用、检验、验收（含第三方验收）、培训、税费、备品备件、技术资料、技术服务和保修期内的所有费用。因中标人自身原因造成漏报、少报皆由其自行承担责任，招标人不再补偿。

（2）投标人应仔细阅读招标文件，招标文件中所包括的内容，均为本次招标供货范围。如投标人未将招标文件中一项或多项项目进行报价，招标人将视为投标人已将未列入的项目报价包含在已报项目报价中，招标人不再另行支付。

#### **4、付款方式**

签订合同后，货物到达现场及系统安装后支付合同价的 10%，培训、实施、试运行正常且验收合格后甲方向乙方支付合同总额的 90%，质保条款按合同约定。（具体以签订合同为准）

#### **▲5、知识产权**

1. 投标人应保证招标人在使用该货物或其任何一部分时，免受第

三方提出的侵犯其专利权、商标权、著作权或其它知识产权的起诉。投标人保证所提供软件的合法性，所发生的任何知识产权纠纷与招标人无关，由此而引起的一切法律责任和费用由投标人承担。

2. 招标人购买产品后，有权对该产品与其他设备进行配套、整合或适当改进，而免受侵犯专利权的起诉。

#### 6、附件、图纸（若有）及包装要求

所有产品按照厂家规定的包装和随机标准附件为准。

#### 7、处罚条例：签订合同时拟定

注：技术与商务部分标注“▲”条款不满足（负偏离），视为不满足招标文件要求，给予废标处理。（允许无偏离、正偏离：优于）

## 第四部分 评审方法（综合评分法）

本项目评审方法见招标文件第二部分“投标人须知前附表”中的规定。如果采用综合评分法，评分细则如下：

评分因素	评分点	评分标准	评审意见	
			是	否
初步 评审	资格 检查	<p>满足《中华人民共和国政府采购法》第二十二条规定应当具备的条件</p> <p>《1. 满足《中华人民共和国政府采购法》第二十二条规定：</p> <p>（1）具有独立承担民事责任的能力。①供应商法人营业执照（副本）或事业单位法人证书（副本）或个体工商户营业执照或有效的自然人身份证明，组织机构代码证扫描件（供应商按“三证合一”登记制度办理营业执照的，组织机构代码证和税务登记证（副本）以供应商所提供的营业执照（副本）扫描件为准）；②供应商法定代表人身份证明和法定代表人授权代表委托书扫描件。</p> <p>（2）具有良好的商业信誉和健全的财务会计制度。</p> <p>①提供审计机构或会计师事务所出具的上一年度（2022年度或2021年度）财务审计报告（报告中须包括资产负债表、利润表、现金流量表及财务报表附注）的原件扫描件；②如供应商无法提供上年度审计报告，则需提供开户银行递交响应文件截止时间前三个月内基本账户银行出具的资信证明的原件扫描件，银行资信证明应能说明该供应商与银行之间业务往来正常，无不良记录，企业信誉良好等；③银行出具的存款证明不能作为银行资信证明；④新成立不满一年的供应商可不提供财务审计报告，只需提供财务报</p>		

		<p>表即可。</p> <p>(3) 具有履行合同所必需的设备和专业技术能力。提供具有履行合同所必需的设备和专业技术能力相关证明或提供具有履行合同所必需的设备和专业技术能力的承诺。</p> <p>(4) 有依法缴纳税收和社会保障资金的良好记录。  ①提供（递交响应文件截止时间前）近6个月内任意1个月的缴纳税收的凭据证明材料扫描件及缴纳社会保险的凭据证明材料扫描件；②新成立不满一个月的企业仅提供依法缴纳税收承诺书和依法缴纳社会保障资金承诺函即可；③如依法免税或依法不需要缴纳社会保障资金的，应提供的相应文件证明其依法免税或依法不需要缴纳社会保障资金。</p> <p>(5) 参加政府采购活动前三年内，在经营活动中没有重大违法记录。①提供参加政府采购活动前3年内，在经营活动中没有重大违法记录的书面声明，在开标日资格审查时由招标人或采购代理机构现场查询，供应商不能是被列入“信用中国”（www.creditchina.gov.cn）严重失信主体名单；②不能是被列入“中国政府采购网”（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单中仍在处罚期的，将拒绝其参加本次政府采购活动；③提供国家企业信用信息公示系统（http://www.gsxt.gov.cn）公示的基础信息、行政处罚信息、列入经营异常名录信息、列入严重违法失信名单（黑名单）信息、公告信息等查询记录。</p> <p>(6) 法律、行政法规规定的其他条件。①投标文件是否含有招标人不能接受的附加条件；②是否违反国家法律、法规和采购文件规定的其他无效情形；③未</p>		
--	--	--	--	--

			与其他投标人串通投标,或者与招标人串通投标。		
	特 定 资 格		无		
符 合 性 检 查	投 标 报 价		投标报价超过预算金额（最高限价）的为无效投标		
	投 标 人 名 称		是否与营业执照、税务登记证、资质证书一致		
	投 标 文 件 签 署		投标文件上法定代表人或其授权代理人的签章、招标文件要求在指定区域加盖单位公章		
	其 他 要 求		满足招标文件要求（如：投标保证金）		
	技 术 与 商 务 条 款		技术与商务部分标注“▲”条款不满足（负偏离），视为不满足招标文件要求，给予废标处理。（允许无偏离、正偏离：优于）		
	投 标 文 件 按 照 招 标 文 件 规 定 的 内 容 、 格 式 填 写 ， 字 迹 清 晰 可 辨		投标文件是否响应实质性响应文件，按照招标文件规定的内容、格式填写，字迹清晰可辨		
	投 标 有 效 期		符合投标人须知前附表的规定		
	招 标 技 术 要 求		投标文件未附有招标人不能接受的条件或不符合招标文件的其他要求，未存在明显不符合技术规格、技		

			术标准的要求，未有重大偏离		
	<b>评分因素</b>	<b>评分点</b>	<b>评分标准</b>		<b>分值</b>
<b>详细 评审</b>	价格 评审	投标报价 (30分)	评标基准价=有效投标报价的最低值，有效投标报价等于基准值的得满分，投标报价得分=(评标基准价/投标报价)×价格权重×100。有效投标报价为通过初步审查的供应商报价		30分
	商务 标 评审	业绩(5分)	投标人在近三年(2020年1月至本采购活动招标公告日期，中标(成交)通知书及合同或协议签字日期为准)承担类似项目业绩(例如：安全应用信息化或商用密码应用信息化)每提供一个业绩得1分；满分为5分。 <b>注：投标人需提供采购中标(成交)通知书及合同(含首页、项目内容、签字盖章页)复印件，否则业绩不予认可。</b>		20分
		售后保障 方案(8分)	1、提供售后服务承诺(1)响应时间，(2)修复时间，(3)售后服务承诺，(4)售后服务团队)全部响应得2分；每缺少一项或每有一项内容不合理的扣0.5分，扣至0分为止。(格式不限) 2、投标单位若中标(成交)后能有本地化服务能力的承诺函(包括但不限于：(1)售后服务团队的人员(岗位分工明确)。(2)所投设备厂家技术支撑(包括但不限于虚拟化软件平台原厂售后；厂商平台对接承诺)。(3)售后服务总负责人证明(格式自拟)。(4)售后服务设备或工具、维修配件(易耗品)等不再收取任何费用等)。(5)重大活动现场保障承诺(格式自拟)。(6)每年例行巡检说明或方案。全部响应得6分；每缺少一项或每有一项内容不合理的扣1分，扣至0分为止。(格式不限)		

		<p>注：投标单位对自己的方案具有法律责任，请根据自己得实际情况编辑，若有不切实际得情况，专家有权在对应的项目上视为不满足并对应扣分。</p>	
	投标人实力 (6分)	<p>投标企业或投标产品生产厂商具备：</p> <p>(1) 信息安全管理证书 (ISO27001)；得 0.5 分。</p> <p>(2) 质量管理体系认证证书 (ISO9001)；得 0.5 分。</p> <p>(3) ITSS 信息技术服务标准证书；得 1 分。</p> <p>(4) 电子认证服务许可证；得 1 分。</p> <p>(5) 电子认证服务密码使用许可证；得 1 分。</p> <p>(6) 拟配备项目工程师具备 CISP 注册信息安全认证，得 1 分。</p> <p>(7) 拟投入实施人员具备 CISA 认证 (认证覆盖的业务范围与安全相关) 或国家认可的计算机相关高级资格证书，得 1 分。</p> <p>注：提供相关证明材料，未提供不得分。</p>	
	投标文件制作要求 (1分)	<p>(1) 电子投标文件制作是否完整 (结合招标文件评标办法及投标格式提供的内容) 及电子关联点是否相对应关联；</p> <p>(2) 是否有正确的目录页码。</p> <p>以上全部符合的得 1 分，否则每一项扣 0.5 分。</p>	
技术标评审	产品参数、性能响应程度 (30分)	<p>“第三部分-采购需求” 产品参数、性能响应程度全部满足得 30 分：</p> <p>(1) 标注“◆”的参数全部满足得 20 分；标注“◆”的参数有一条不满足 (负偏离) 扣 2 分；扣完为止。</p> <p>(2) 未标注“◆”的参数全部满足得 10 分；未标注“◆”的参数一条不满足 (负偏离) 扣 1 分，扣完为止。</p>	50 分

		<p>注、需提供技术参数中“◆”条款要求提供的相关证明文件并加盖厂商鲜章。标注“◆”的参数需要按顺序点对点应答，并将证明文件标注页码。</p>	
	<p>质量保证 (3分)</p>	<p>1、产品一致性:为确保项目顺利开展和各产品的互相兼容,投标人所投 IPSec/SSL VPN 综合安全网关、签名验签与时间戳二合一服务器、服务器密码机,需要具有良好的适配性和兼容性并提供证明。全部满足得1分,否则不得分。</p> <p>2、完整性保护需求:为保证密码产品的设备自身安全 IPSec/SSL VPN 综合安全网关、签名验签与时间戳二合一服务器、服务器密码机使用的密码卡须支持实模式,确保开机启动系统镜像的完整性检验,防止系统被恶意篡改(提供相关证明文件)。全部满足得1分,否则不得分。</p> <p>3、运维安全需求:IPSec/SSL VPN 综合安全网关、签名验签与时间戳二合一服务器、服务器密码机支持国密 SSH、国密 FTP,保证整机运维安全要求。全部满足得1分,否则不得分。</p> <p>注:投标单位对自己得保证具有法律责任,请根据自己得实际情况编辑,若有不切实际得情况,专家有权在对应的项目上视为不满足并对应扣分。</p>	
	<p>安全运维 服务方案 (4分)</p>	<p>投标人提供的安全运维服务方案包括但不限于:(1)建设标准、建设目标理解清晰,建设后的安全防护体系出具真实性的安全服务计划。(2)提供不少于1名安全运维服务人员,并具备信息安全保障人员认证证书,且为本投标单位在职人员(提供近6个月内的社保证明或相关证明),并承诺(格式自拟)36个月的驻场服务。(3)对服务范围、服务内容、服务</p>	

		<p>流程、服务质量管理。（4）服务培训内容详细的描述、并符合用户实际需求。满分为4分；每项表达逻辑不清晰，未能突出重点和不切实际扣1分；扣完为止。</p> <p>投标单位对自己的方案具有法律责任，请根据自己得实际情况编辑，若有不切实际得情况，专家有权在对应的项目上视为不满足并对应扣分。</p>	
	<p>项目实施 方案（5 分）</p>	<p>1、投标人提供的项目实施方案包括但不限于：（1）根据招标文件中的采购需求对现有的安全问题进行研判分析，充分考虑现有的安全现状和此次建设的安全目标。（2）项目实施体现整体拓扑图。满分为2分；每项表达逻辑不清晰，未能突出重点和不切实际扣1分；扣完为止。</p> <p>投标单位对自己得方案具有法律责任，请根据自己得实际情况编辑，若有不切实际得情况，专家有权在对应的项目上视为不满足并对应扣分。</p> <p>2、投标单位承诺对此项目具有专业技术人员负责整个项目的实施过程，来保障项目能顺利实施，投标单位具有至少一名总负责人且为本单位在职人员（提供至少6个月的社保证明或相关证明相）；得1分。未提供不得分。</p> <p>3、总负责人需具备信息系统项目管理或系统集成项目管理工程师高级专业技术资格证明文件；得2分。未提供不得分。</p>	
	<p>视频演示 （8分）</p>	<p>视频演示每项均满足要求得8分，单项不满足扣2分，不演示不得分。</p> <p>演示内容包括：</p> <p>1、为应对新型安全威胁，态势感知平台检测到僵尸</p>	

		<p>网络时自动调用超融合平台的分布式防火墙进行虚拟机隔离；检测到勒索病毒自动对虚拟机存储进行快照备份；态势感知平台可以设置触发策略与超融合进行特定类型安全事件的处置。</p> <p>2、为保障终端防护效果，网络版防病毒需基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，提供勒索专区展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御。</p> <p>3、为确保平台的安全性，云安全中心需集成在虚拟化平台中一体化方式交付，无需第三方平台承载，必须能够提供虚拟主机安全防护安全能力，并对检测的恶意活动可实现分布式防火墙隔离虚拟机、虚拟机快照等有效防护手段。</p> <p>4、网络版防病毒支持与本次投标的防火墙、安全态势感知平台进行安全兼容，支持将终端安全软件客户端检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到安全态势感知平台，安全态势感知平台进行分析和展示；同时满足管理员在安全态势感知平台管理界面下发快速查杀任务和下发一键隔离指令，对终端所有连接进行阻断，并查看任务状态、结果并进行处置，防止病毒进一步扩散。</p> <p><b>注：投标单位对自己得视频具有法律责任，请根据自己得实际情况录制，若有不切实际得情况，专家有权在对应的项目上视为不满足并对应扣分。</b></p>	
	合计	100 分	
注：评分分值计算保留小数点后两位，小数点后第三位“四舍五入”。			

1、经评标委员会认可小、微企业产品和产品报价后，投标人相应产品政策计算公式如下：

中小微企业产品价格扣除后的投标人报价=投标人总报价-中小微企业产品报价\*扣除幅度。（以价格扣除后的投标人报价作为评审依据）

2、评标委员会应当执行连续评标的原则完成全部评标工作。只有发生不可抗力导致评标工作无法继续时，评标活动方可暂停。发生评标暂停情况时，评标委员会应当封存全部投标文件和评标记录，待不可抗力的影响结束且具备继续评标的条件时，由原评标委员会继续评标。

3、除非发生下列情况之一，评标委员会成员不得在评标中途更换：(1)因不可抗拒的客观原因，不能到场或需在评标中途退出评标活动；(2)根据法律法规规定，某个或某几个评标委员会成员需要回避。退出评标的评标委员会成员，其已完成的评标行为无效。根据本招标文件规定的评标委员会成员产生方式另行确定替代者进行评标。

4、在任何评标环节中，需评标委员会就某项评审结论做出表决的，由评标委员会全体成员按照少数服从多数的原则，以记名投票方式表决。

5、如果出现得分相同的供应商，以报价低优先、若得分、报价均相同以技术优先。

## 第五部分 政府采购合同

一、合同格式：

### 政府采购合同

(此合同仅做参考)

项目名称：第六师自然资源和规划局系统网络安全三级等保测评及整改项目（安全设备三级升级改造和密码安全防护）

项目编号：XJJY-[2023]政采云 003-02

合同编号：\_\_\_\_\_

甲 方：\_\_\_\_\_

乙 方：\_\_\_\_\_

甲方：

合同签订地点：五家渠市

乙方：\_\_\_\_\_

乙方在\_\_\_\_\_组织的（ ）采购中，通过公平竞争，成功成交。

供货周期： 年 月 日至 年 月 日。现依据《中华人民共和国民法典》、《中华人民共和国政府采购法》、订立合同，以便共同遵守。

依据采购文件（含补充、修改文件）和乙方的谈判响应文件（含澄清、补充答疑文件），乙方向甲方提供下列全新的标的（物资/工程/服务）。

序号	货物名称	品牌/型号	单价（元）	数量	合计（元）
1					
合计金额（小写）： ¥					
合计金额（大写）： 元整					

### 1. 保修期

乙方提供设备的质量保证期为自交货验收合格之日起 年止（人为损坏、易损件、第三方配套设施导致的设备损坏及耗材除外）。在保证期内因设备本身的质量问题发生故障，乙方应负责免费修理更换零部件。应对设备出现的质量及安全问题负责处理解决。期满后可同时提供终身（有偿）维修保养服务。

### 2. 专利权

2.1 乙方须保障甲方在使用其所提供的货物、服务及其任何部分时，不受到第三方关于侵权的指控，如果出现此类情况由乙方与第三方交涉并承担可能发生的一切经济和法律责任（包括但不限于甲方因此支付的律师费、公证费、鉴定费、保全费、诉讼费、邮寄送达费）。

### 3. 货物条款

3.1 甲、乙双方应将、投标文件及评标小组确认的货物名称、规格型号、技术要求、质量标准、数量和交货日期等作为本条款的基础。

### 4. 技术条款

4.1 乙方向甲方提供所招标采购的货物、服务及有关技术资料。

## 5. 包装

5.1 乙方交付的所有货物要符合国家主管机关的规定，具有适合长途运输和装卸的坚固包装。包装应保证在运输、装卸过程中完好无损，并有减振、防冲击及防磨损措施。包装应按设备特点，按需要分别加上防潮、防锈、防腐蚀的保护措施，以保证货物在没有任何损坏和腐蚀的情况下安全运抵设备安装现场。设备装货和包装前，乙方负责对其进行检查和清理，不留异物，并保证零部件齐全。

5.2 乙方应将所提供货物的装箱清单、配件、随机工具、用户使用手册、原厂保修卡等资料交付给甲方；乙方不能完整交付货物及本款规定的单证和工具的，必须负责补齐，否则视为未按合同约定交货。

## 6. 质量保证

6.1 乙方须提供全新的货物（含零部件、配件等），表面无划伤、无碰撞痕迹，且权属清楚，不得侵害他人的知识产权。

6.2 货物必须符合或优于国家（行业）标准，以及本项目招标文件的质量要求和技术指标与出厂标准（各标准不同时，以最严格标准为准）。

6.3 乙方须在本合同签订之日起3日内送样稿给甲方确认，在甲方出具确认后，乙方才能按样生产；每台货物上均应有产品质量检验合格标志。

6.4 货物制造质量出现问题，乙方应负责三包（包修、包换、包退），费用由乙方负担，甲方有权到乙方生产场地检查货物质量和生产进度。

6.5 如货物经乙方3次维修仍不能达到合同约定的质量标准，甲方有权退货，并视作乙方不能交付货物而须支付违约赔偿金给甲方，甲方还可依法追究乙方的违约责任。

## 7. 检验与索赔

7.1 在交货前，乙方应就商品的质量、规格、及数量做出准确和全面的检查，并出具商品符合合同的证明书（包括实验记录和书面报告）。

7.2 货物运抵甲方后，双方应一同对其进行检验，如发现货物规格质量、及数量与合同不符，须出具检验证书，并由乙方负责更换或赔偿，此项赔偿总额不超过合同总价的30%。

7.3 在合同规定的质量保证期满前如果发生货物的质量或规格与合同不符，或发生货物无论任何原因引起的缺陷，包括潜在的缺陷或使用不良材料，甲方有

权向乙方索赔。

7.4 乙方收到甲方索赔通知后如在 5 日内不答复，应视为乙方同意甲方提出的一切索赔。

## 8. 索赔解决方法

8.1 如货物不符合合同规定由乙方负责。乙方取得甲方同意后，应按下列方式之一理赔：

(1) 同意拒收货物，向甲方退还所拒收货物的货款，并承担全都损失和费用，包括利息、银行费用、运输、检验费等。

(2) 根据货物所受损坏的程度、下降的等级和甲方所受损失的价值，经乙方和甲方达成协议，降低货物的价款。

## 9. 合同变更

9.1 甲方可以在任何时间，在合同总的范围内，采取多种方式如书面、邮件、电话、短信、微信多种方式向乙方发出书面变更通知。

9.2 如果上述的变更通知导致乙方履行合同项下的任何工作部分的成本或时间的增加或减少，经双方协商一致，可以对合同价格或交货时间表或两者做公正的调整。乙方在本条项下的任何调整要求必须在收到甲方变更通知后的 7 天内书面提出。

## 10. 人力不可抗拒事件的处理

10.1 由于受到战争、严重水灾、洪水、台风、地震等不可抗力的影响不能执行合同时，履行合同的期限应予以延长，延长期限应相当于事故所影响的时间。不可抗力事故系指甲乙双方在缔结合同时不能预见的，并且它的发生及其后果是无法克服的。

10.2 人力不可抗拒的事件导致乙方交货延迟或不能交货时，责任不在乙方，但乙方应立即将事件通知甲方，并与事件发生后 7 日内，将事件发生地政府主管机关出据的事故证明书，邮寄给甲方审阅确认，即使在上述情况下，乙方仍负有采取一切必要措施从速交货的责任。如果事件持续超过 30 天，甲方有权撤消合同。

## 11. 违约和罚款

11.1 如乙方迟交货物，除人力不可抗拒事件外，乙方应按合同法规定付给

迟交违约金为每逾期一天，按逾期部分货款的3%计算，但此项总额不超过全部迟交货物总值的10%。此项迟交违约金应由乙方将款项交入甲方指定账户。

11.2 如迟延供货超过10天时，甲方有权终止合同，但乙方应向甲方付以上规定之违约金，不得推诿或延迟。

11.3 乙方提供货物不符合招标文件要求或者出来质量问题，甲方有权解除合同，由此产生的一切费用由乙方负责，并需支付合同价款30%的违约金。

## 12. 履约保证金

12.1 履约保证金的有效期限直到货物验收及提供合格为止。

12.2 当乙方没有履行合同规定的某项义务时，甲方有权从履约保证金中获取相应赔偿金。

## 13. 争议解决

执行合同或合同有关事项所发生的全部争执，应经双方友好协商加以解决，如协商不成，则提交甲方所在地法院起诉。

14. 交货期：合同签订后 天。

15. 交货地点：甲方指定

## 16. 验收方式：

16.1 甲方对乙方送交的货物进行现场检查验收，验收合格后，甲方在《新疆生产建设兵团第六师五家渠市政府采购项目验收结算单》上签字及加盖单位印章；

16.2 在检验、验收过程中应遵守有关标准和验收规范进行；

16.3 设备按照现行国标、部标、或者行业标准制造；

16.4 原装进口产品须提供报关单原件；

16.5 对检验及验收不达标的设备，所发生的一切费用及给采购单位造成的经济损失，均由中标人承担；采购单位保留追究其经济及法律责任的权利。

17. 付款方式：合同签订后，货到甲方指定地点，安装调试完毕，验收合格后由甲方根据使用单位签字及加盖单位印章的《新疆生产建设兵团第六师五家渠市政府采购项目验收结算单》及乙方按照甲方要求提供合法发票后：

17.1 付货款总价的\_\_\_\_的合计¥ 元（ 元整），签订合同日 年后当日，支付剩余\_\_\_\_\_的余款（剩余不计息）合计¥ 元（ 元整）；

## 18. 售后服务

18.1 所有设备质保期内出现质量问题，乙方在接到通知后 2 小时内响应，8 小时内完成维修或更换，并承担修理调换的费用；如货物经乙方 3 次维修仍不能达到本合同约定的质量标准，视作乙方未能按时交货，甲方有权退货并追究乙方的违约责任。

18.2 所有设备和系统质保金均在质保期结束，无质量问题的情况下，甲方向乙方无息返还。

18.3 乙方须指派专人负责与甲方联系售后服务事宜。运输风险及费用均由乙方承担，且甲方不再向乙方支付安装调试的费用。乙方自行为乙方人员购买工伤保险，如发生工伤事故或其他意外情况，相关责任均由乙方承担

### 19 其他：

19.1 本次采购，凡涉及知识产权问题，由乙方负责。

19.2 合同应在甲方、乙方双方签字盖章后开始生效。

19.3 在执行本合同的过程中，招标文件、中标人的投标文件、答疑记录、中标通知书及所有经买卖双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分。

19.4 合同一式 份，甲方 份、乙方 份。

甲 方：

乙 方：

法定代表人：

法定代表人：

委托代理人：

委托代理人：

手机/电话：

手机/电话：

时 间： 年 月 日

时 间： 年 月 日

## 第六部分 投标文件格式

### 目 录

- (一) 投标文件封面
  - (一) ☆营业执照、组织机构代码证、税务登记证
  - (二) ☆法定代表人身份证明及授权委托书
  - (三) ☆投标保证金
  - (四) 小、微企业声明函（小、微型企业产品价格需扣除的须提供）
  - (五) 投标人认为有必要提供的声明及文件资料
  - (六) 《中华人民共和国政府采购法》第二十二条应当具备的条件；
  - (七) 不参与围标串标承诺书
  - (一) ☆投标函
  - (二) ☆开标一览表
  - (三) ☆投标报价明细表
  - (四) ☆售后服务承诺书
  - (五) 商务条款偏离说明表
  - (六) 投标人认为有必要提供的其他资料
  - (一) 投标人自行编写的技术文件
  - (一) 投标人自行编写的服务文件
- 其他材料

## 一、投标文件格式

新疆建友友成工程管理咨询有限公司

(一) 投标文件封面

\_\_\_\_\_ (项目名称)

\_\_\_\_\_ (包号)

# 投标文件

投标人\_\_\_\_\_ (电子签章)

法定代表人\_\_\_\_\_

日期\_\_\_\_\_ (年/月/日)

## 二、资格审查材料

新疆建友友成工程管理咨询有限公司

(一) ☆营业执照、组织机构代码证、税务登记证

新疆建友友成工程管理咨询有限公司

## (二) ☆法定代表人身份证明及授权委托书

法定代表人资格证明文件

(代理机构名称)：

兹有\_\_\_\_\_同志为\_\_\_\_\_公司法定代表人，代表我公司办理一切社会公务事宜，具有法律效力。

附法定代表人基本情况：

姓名：\_\_\_\_\_性别：\_\_\_\_\_年龄：\_\_\_\_\_职务：\_\_\_\_\_

身份证号码：\_\_\_\_\_

通讯地址：\_\_\_\_\_

电话号码：\_\_\_\_\_ 邮政编码：\_\_\_\_\_

法定代表人《居民身份证》扫描件

投标人名称（电子签章）：\_\_\_\_\_

法定代表人（电子签名）：\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日

法定代表人授权书

（代理机构名称）：

兹授权\_\_\_\_\_同志为我公司参加贵单位组织的编号为（项目编号）的（项目名称）采购活动的投标代表人，全权代表我公司处理在该项目采购活动中的一切事宜。代理期限从\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日起至\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日止。

投标人（电子签章）：\_\_\_\_\_

法定代表人（电子签名）：\_\_\_\_\_

签发日期：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日

附：

代理人工作单位：\_\_\_\_\_

职务：\_\_\_\_\_ 性别：\_\_\_\_\_

身份证号码：\_\_\_\_\_

粘贴被授权人身份证（扫描件）

(三) ☆投标保证金

新疆建友友成工程管理咨询有限公司

#### （四）小、微企业声明函

### 小、微企业声明函（货物类）

（小、微型企业产品价格需扣除的须提供）

本公司（联合体）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（联合体）参加（单位名称）的（项目名称）采购活动，提供的货物全部由符合政策要求的中小微企业制造。相关企业（含联合体中的中小微企业、签订分包意向协议的中小微企业）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）行业；**制造商为**（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）行业；**制造商为**（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。

**价格扣除办法：**本项目对小型和微型企业货物的价格给予10%的扣除，用扣除后的价格参与价格分的评审。

供应商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。

企业名称（盖章）：

日期：

### (五) 投标人认为有必要提供的声明及文件资料

附：类似项目业绩表

采购项目编号：\_\_\_\_\_

采购项目名称：\_\_\_\_\_

项目名称	
项目单位名称	
项目单位联系人姓名及联系方式	
合同金额	
项目负责人姓名	
项目实施时间	
项目内容说明	

说明：1. 附上相关证明材料，否则专家在评审时将不予采信；

2. 项目内容请详细说明所承担的具体工作内容

投标人法定代表人（电子签名）：\_\_\_\_\_

投标人名称（电子签章）：\_\_\_\_\_

日期：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日

**(七)《中华人民共和国政府采购法》第二十二条应当具备的条件；**

- ①具有独立承担民事责任的能力；
- ②具有良好的商业信誉和健全的财务会计制度；
- ③具有履行合同所必需的设备和专业技术能力；
- ④有依法缴纳税收和社会保障资金的良好记录；
- ⑤参加政府采购活动前三年内，在经营活动中没有重大违法记录；
- ⑥法律、行政法规规定的其他条件；

新疆建友友成工程管理咨询有限公司

## (八) 不参与围标串标承诺书

### 不参与围标串标承诺书

本人作为(单位名称)\_\_\_\_\_的法人,清楚知晓我公司本项目投标活动,对以下事项作出承诺:

一、我单位遵循公开、公平、公正、诚实守信的原则,依法依规参与本项目竞标。

二、我单位在本项目招标投标活动中,未参与围标串标。

三、我单位如被查实在本项目招标投标活动中存在围标串标的,递交投标文件行为作为实施串通投标违法行为的关键环节,本人承担直接责任人员法律责任,接受相应行政处罚和失信惩戒。

项目编号:

标段号:

投标人单位名称:

投标人法人签名:

盖 章

年 月 日

### 三、商务文件

新疆建友友成工程管理咨询有限公司

## (一) ☆投标函

\_\_\_\_\_:

\_\_\_\_\_ (投标人名称) 授权\_\_\_\_\_ (投标人授权代理人姓名)\_\_\_\_\_ (职务、职称) 为我方代表, 参加贵方组织的\_\_\_\_\_ (项目名称、项目编号、包号) 招标的有关活动, 并对此项目进行投标。为此:

1、我方同意在本项目招标文件中规定的投标有效期内遵守本投标文件中的承诺且在此期限期满之前均具有约束力。

2、我方承诺已经具备《中华人民共和国政府采购法》中规定的参加政府采购活动的投标人应当具备的条件:

- 1) 具有独立承担民事责任的能力;
- 2) 具有良好的商业信誉和健全的财务会计制度;
- 3) 具有履行合同所必需的设备和专业技术能力;
- 4) 有依法缴纳税收和社会保障资金的良好记录;
- 5) 参加此项采购活动前三年内, 在经营活动中没有重大违法记录;
- 6) 法律、行政法规规定的其他条件。

3、以招标文件须知前附表要求为准。

4、按招标文件要求提供和交付的货物及相关服务的投标报价详见开标一览表。

5、保证忠实地执行双方所签订的合同, 并承担合同规定的责任和义务。

6、我方承诺完全满足和响应招标文件中的各项技术和服务要求, 若有偏差, 已在投标文件偏离表中予以明确特别说明。

7、我方承诺: 完全理解投标报价若超过项目预算时, 投标将被拒绝。

8、我方承诺: 与在本项目中设计编制技术规格的机构及其附属机构无任何直接隶属关系和利益关联。

9、如果在开标后规定的投标有效期内(90个日历日)撤回投标, 我方的投标保证金可被贵方没收。

10、我方完全理解贵方不一定接受最低价的投标或收到的任何投标。

11、我方承诺：投标文件所提供的一切资料及“政采云”平台申报资料均真实、及时、有效。由于我方提供资料不实而造成的责任和后果由我方承担。我方同意按照贵方提出的要求，向贵方提供任何与本项投标有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

12、我方已详细审核全部投标文件，包括投标文件修改书（如有的话）、参考资料及有关附件，确认无误。

13、我方承诺：招标人若需追加采购本项目招标文件所列货物及相关服务的，在不改变合同其他实质性条款的前提下，按相同或更优惠的折扣率保证供货。

14、我方承诺：如所报货物属国家强制认证产品的，均已通过认证且在有效期内，否则，由此产生的一切法律责任由我方承担。

15、我方承诺：接受招标文件中的全部条款且无任何异议，保证遵守招标文件的规定。

16、我方将严格遵守《中华人民共和国政府采购法》的有关规定，若有下列情形之一的，将被处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动；有违法所得的，并处没收违法所得；情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

- 1) 提供虚假材料谋取中标、成交的；
- 2) 采取不正当手段诋毁、排挤其他投标人的；
- 3) 与招标人、其他投标人或者采购代理机构工作人员恶意串通的；
- 4) 向招标人、采购代理机构工作人员行贿或者提供其他不正当利益的；
- 5) 在采购过程中与招标人进行协商谈判的；
- 6) 拒绝有关部门监督检查或提供虚假情况的。

17、

与本投标有关的一切往来通讯请寄：

地址：\_\_\_\_\_

邮编：\_\_\_\_\_

电话：\_\_\_\_\_

传真：\_\_\_\_\_

投标人法定代表人或授权代理人联系电话，e-mail：\_\_\_\_\_

投标人法定代表人电子签名：

投标人公章：

日期：

说明：除可填报项目外，对本投标函的任何修改将被视为非实质性响应投标，从而导致该投标被拒绝。

新疆建友友成工程管理咨询有限公司

## (二) ☆开标一览表

包号：\_\_\_\_\_

价格单位：元

分包名称	_____
投标总价	小写：_____元 大写：_____元
合同履行期限	_____
质保期	
备注：	_____

说明：1、投标人严格按照规定的格式填写。投标总价为优惠后报价，并作为评审及定标的依据。

2、任何有选择或有条件的投标总价或表中某一包填写多个报价，均将导致投标被拒绝。

### (三) ☆投标报价明细表

项目编号、包号：\_\_\_\_\_

价格单位：元

项 序 号	1  产品名称	2  品牌、型号	3  价格		
			单价	数量	小计
1					
2					
3					
4					
5	...				
	货物费用小计				
	安装调试费用				
	维护与技术支持费用				
	培训费用				
	备品备件费用				
	运输与保险费用				
	其他				
	合计				

说明：投标人必须填写报价明细表，否则将导致投标被拒绝。

注：投标报价超过采购预算及单价限价的否决投标

年 月 日

(四) ☆售后服务承诺书

(五) 企业实力

新疆建友友成工程管理咨询有限公司

### (六) 商务条款偏离说明表

序号	招标文件条款号	招标文件的服务条款	投标文件对应位置（细化描述）	偏差（正偏离或者负偏离）	备注

新疆建友友成工程管理咨询有限公司

(七) 投标人认为有必要提供的其他资料

新疆建友友成工程管理咨询有限公司

## 招标文件确认书

\_\_\_\_\_（招标人名称）：

我方已经详细阅读整个招标文件的内容，对本招标文件的内容没有任何异议，全部同意并接受且我方保证在开评标活动结束后不对本招标文件的任何内容提出异议。

投标人：\_\_\_\_\_（加盖公章）

授权代表签章：\_\_\_\_\_

2023 年\_\_\_\_\_月\_\_\_\_\_日

#### 四、技术文件

新疆建友友成工程管理咨询有限公司

## (一) 投标人自行编写的技术文件

① 物主要技术指标和运行性能：

<1>☆技术明细表（详细描述货物技术指标及性能）；

项目编号、包号：\_\_\_\_\_

项	1	2	3
序号	产品名称 品牌、型号	技术规格	备注
1			
2			
3			
4			
5			
6	...		

说明：1. 投标人必须填写技术明细表。如果此表中所列内容无法满足招标文件中提出的要求或者与投标人在技术文件中提供的内容不一致，投标有可能被拒绝。

2. 技术规格不得完全复制招标文件内容，否则按无效投标处理。

年 月 日

〈3〉货物技术规范偏离表

项目编号、包号：\_\_\_\_\_

序号	货物名称及编号	数量	招标文件技术规范、要求	投标文件对应位置(细化描述)	偏差(正偏离或者负偏离)	备注

注：投标单位所货物或设备的技术参数有任何偏离（偏差）说明需与“第三部分-采购需求”里的参数要求按顺序点对点编制（包括但不限于招标文件中要求提供的投标产品样本、产品手册、彩页、说明书等技术文件、图纸（如有）以及产品检测报告和认定证书等技术资料或其他证明材料（格式不限））。

年 月 日

②货物配件、耗材、选件表和备件及特殊工具清单；

③实施方案；

④产品及软件安全；

## 五、服务文件

新疆建友友成工程管理咨询有限公司

## （一）投标人自行编写的服务文件

①货物售后服务：

<1>货物的保修期和售后服务的程序、内容及措施；

<2>响应时间和技术支持情况；

<3>培训方案及内容；

## 七、投标人认为有必要提供的其他资料

新疆建友友成工程管理咨询有限公司

---

附件 1:

### 投标保证金退款申请函

新疆建友友成工程管理咨询有限公司:

我公司于\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日向贵单位以\_\_\_\_\_形式提交\_\_\_\_\_元投标保证金,参与\_\_\_\_\_项目的投标工作。现中标结果已经公布,我公司因:(1、中标且已签合同;2、未中标;3、其他情形),特向贵公司提出申请退还保证金。以下是我公司提供的退还款项的账户信息(帐户信息必须和汇入帐户信息一致):

户名:

账号:

开户行:

行号:

联系电话:

公司名称(盖公章):

注:1.未成交投标人请于成交结果公告发出后5个工作日内办理退还保证金程序,成交投标人请于与采购单位签订采购合同后5个工作日内办理退还保证金程序还需单独提供合同原件(加盖公章的)至代理机构。

2.为简化手续,优化流程,在符合上述条件要求的前提下,退还投标保证金时按原路退回,此申请函信息填完整后打印盖章将扫描件发至我公司邮箱2122415327@qq.com进行退款。