青岛市政府采购

重要信息等级保护建设项目

货物类公开招标文件

（2018-5-31 示范文本）

采 购 人：胶州市人民法院

代理机构：昊金海建设管理有限公司（公章）

项目编号：JZZFCG2019072

日　　期：2019 年 4 月 4 日

目 录

第一章　招标公告

一、招标人：胶州市人民法院

地址：胶州市

联系方式：18562883616

采购代理机构：昊金海建设管理有限公司

地址：青岛市胶州市扬州支路 308 号

联系方式：82205307

二、项目名称：重要信息等级保护建设项目

采购项目编号：JZZFCG2019072

预算金额与最高限价：本项目预算金额为 1560000.00 元，其中：第 一 包 1560000.00 元。

投标人资格要求：

1 具有独立承担民事责任能力的法人。

2 招标公告发布之日前三年内无行贿犯罪等重大违法记录。

3 通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）、信用山东(www.creditsd.gov.cn) <http://www.creditsd.gov.cn)>及信用青岛（credit.qingdao.gov.cn）查询，未被列入失信被执行人、重大税收违法案件当事人、政府采购严重违法失信行为记录名单。

4 本项目不接受联合体投标。

三、项目概况：

重要信息等级保护建设项目。

四、公告媒介：

1. 招标公告在全国公共资源交易平台（山东省青岛市）青岛市公共资源交易电子服务系统（http://ggzy.qingdao.gov.cn）上发布。

2. 招标公告在中国青岛政府采购网（http://zfcg.qingdao.gov.cn）上发布。

五、获取招标文件：

开标时间前在全国公共资源交易平台（山东省青岛市）青岛市公共资源交易电子服务系统（http://ggzy.qingdao.gov.cn）本项目招标公告页面免费下载招标文件。代理机构不再发售纸质招标文件。

六、公告期限

招标公告发出之日起5个工作日。

七、投标文件递交：

投标人应当在投标截止时间前，通过【青岛市公共资源投标文件制作工具】上传投标文件。

八、投标截止时间、开标时间及地点：

投标截止时间、开标时间： 2019-04-29 14:00

开标地点：胶州市公共资源交易中心（胶州市行政服务中心西楼附楼二楼第2开标室）第二开标室

九、招标项目联系方式：

联系人（招标人）：吴主任

联系方式：18562883616

联系人（代理机构）：惠铭艳、臧石慧

联系方式：82205307

第二章　投标人须知前附表

序号	条款名称	编列内容
1	采购人	胶州市人民法院
2	采购代理机构	昊金海建设管理有限公司

3	项目名称	重要信息等级保护建设项目
4	分包情况	详见青岛市政府采购网（http://zfcg.qingdao.gov.cn）及全国公共资源交易平台（山东省•青岛市）青岛市公共资源交易电子服务系统（http://ggzy.qingdao.gov.cn）本项目招标公告页面。
5	资金来源以及资金构成	100%
6	是否接受联合体投标	√不接受 □接受
7	投标有效期	自投标截止之日起90个日历天。
8	踏勘现场	√不组织，自行踏勘 □组织
9	履约保证金	√不需要 □需要
10	采购代理服务费支付	□招标人支付 √中标人支付 □无需支付
11	构成招标文件的其他材料	
12	招标文件的澄清和修改	招标文件的澄清和修改内容详见青岛市政府采购网（http://zfcg.qingdao. gov.cn）及全国公共资源交易平台（山东省•青岛市）青岛市公共资源交易电子服务系统（http://ggzy.qingdao.gov.cn）本项目招标公告页面，投标人应密切关注上述公告页面的最新澄清信息。澄清和修改一经发布，视为投标人已收到。
13	投标截止时间	详见招标公告。
14	招标文件的质疑	招标公告公告期限届满之日起7个工作日内提出。
15	是否允许递交备选投标方案	√不允许 □允许
16	投标报价的范围	含税全包价。
17	投标报价的次数	本次投标报价为一次不得更改报价，投标人只有一次报价的机会。投标报价（即开标报价）不得有选择性报价和附有条件的报价，且不得高于预算金额或最高限价。
18	投标报价的方式	投标总报价（元）

19	进口产品投标	√不允许 □允许
20	样品	√不需要 □需要
21	投标保证金的交纳	□不需要交纳 √需要交纳 1.金额：人民币壹万伍仟陆佰元整（￥15600元） 2.缴纳截止时间，同投标截止时间。保证金缴纳账户信息请登录全国公共资源交易平台（山东省青岛市）青岛市公共资源交易电子服务系统（http://ggzy.qingdao.gov.cn）本项目招标公告页面点击“获取虚拟账号”。 3.投标保证金的交纳单位必须与投标人名称一致； 4.交纳形式： 4.1 以网银、银行电汇形式交纳的投标保证金须从其基本账户转出，以到账时间为准； 5.联合体投标的，投标保证金由牵头人交纳。
22	投标文件编制	投标人使用【青岛市公共资源投标文件制作工具】编制电子投标文件。
23	投标文件签章	在招标文件的第十章投标文件格式的附件中标示的 “公章”“印章”处，分别签单位公章、个人印章。操作详见“青岛市公共资源交易电子服务系统> 首页> 下载中心> 系统使用指南>电子签章操作说明”。
24	投标文件加密、上传	通过【青岛市公共资源投标文件制作工具】上传时，系统通过投标人当前使用的CA数字证书自动加密电子投标文件。 电子投标文件上传成功后，系统出具上传凭证，投标人可以下载保存。
25	投标人签到及电子投标文件解密	支持网上远程开标，投标人无需到现场参加开标会。若到现场开标，应携带上传投标文件的CA数字证书及可登陆互联网的电脑设备以确保网上开标。开标注意事项详见“青岛市公共资源交易电子服务系统>首页> 下载中心> 系统使用指南>电子投标开标注意事项” 1.投标人在线签到：在投标截止时间前1小时

		内通过CA数字证书进行在线签到，未在线签到的投标无效。 2．投标人接到解密提示后，应当在规定时限内通过CA数字证书对电子投标文件开始解密。
26	开标时间及开标地点	详见招标公告。
27	评标委员会	评标委员会共5人，其中：评审专家5人
28	评标方法	综合评分办法
29	是否授权评标委员会确定中标人	是　确定1个中标人，中标结果在青岛市政府采购网及全国公共资源交易平台（山东省　青岛市）青岛市公共资源交易电子服务系统公告，公告期限为1个工作日。
30	其他需补充的内容	
30.1	书面形式的定义	数据电文形式与纸质形式的招标投标活动具有同等法律效力。数据电文形式包括文字的打印或复印件、传真、信函、电传、电报、电子邮件等可以有形表现所载内容的电子文档，青岛市公共资源交易电子服务系统及青岛市政府采购网发布的招标公告、招标文件及发出的澄清、答疑、变更等各类公告。
30.2	相关评标标准认可要求	潜在投标人的业绩、荣誉（获奖）及相关附件须在青岛市公共资源交易电子服务系统上传并公示满5个工作日，且制作投标文件时上述材料需通过该系统选取，否则在电子评标时不予认可。
30.3	电子签名	可靠的电子签名与手写签名或者盖章具有同等的法律效力。电子签章是电子签名的一种表现形式，利用图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视效果。
30.4	分包和非主体、非关键性工作	√不允许 □允许
30.5	监督和管理	本次招标投标活动以及相关当事人应当接受财政部门依法实施的监督和公共资源交易综合管理部门的管理。
30.6	其他需补充的内容	1.供应商请在　2019年4月29日14时00分前在青岛市政府采购网　www.ccgp-qingdao.gov.cn　注册并登陆后进行网上投标报名（已注册用户可直接从【供应商报名】入口登陆后报名）。未在网上报名或网上报名不成功的，无资格参加投标。2.本项

		目招标公告在全国公共资源交易平台（山东省青岛市）青岛市公共资源交易电子服务系统（http://ggzy.qingdao.gov.cn）、青岛市政府采购网（http://zfcg.qingdao. gov.cn）及胶州市公共资源交易网<http://www.jzggzyjyzx.gov.cn/>，下同）上发布。3、招标文件的澄清和修改内容详见青岛市政府采购网（http://zfcg.qingdao.gov.cn）及全国公共资源交易平台（山东省青岛市）青岛市公共资源交易电子服务系统（http://ggzy.qingdao.gov.cn）和胶州市公共资源交易网本项目招标公告页面，投标人应密切关注上述公告页面的最新澄清信息。澄清和修改一经发布，视为投标人已收到。

第三章　投标人应当提交的资格证明文件

资格证明文件目录

序号	证明材料名称	提供形式	备注	必须提交
1	营业执照、登记证书、执业许可证等	电子文档	具有独立承担民事责任能力的企业或组织合法经营权的凭证（营业执照）	是
2	在经营活动中无重大违法记录和行贿犯罪记录的承诺	电子文档	在经营活动中无重大违法记录和行贿犯罪记录的承诺（详见附件 2）	是
3	政府采购诚信承诺书	电子文档	政府采购诚信承诺书（详见附件 17）	是
4	行贿犯罪档案查询结果告知函	电子文档	登陆中国裁判文书网（http://wenshu.court.gov.cn）查询投标人无行贿犯罪记录查询网页截图，并加盖公章	是
5	保证金缴纳凭证	电子文档	保证金缴纳凭证	是

资格证明文件备注：

开标时，必须提交的证明材料未提交或提交不全的视为资格审查不合格。

（1）缴纳税收的证明材料是指投标人税务登记证（或统一社会信用代码营业执照）和参加政府采购活动前一段时间内缴纳税收的凭据。缴纳社会保障资金的证明材料是指参加政府活动前一段时间内缴纳社会保险的凭据（专用收据或社会保险缴纳清单），其他组织和自然人也需要提供缴纳税收的凭据和缴纳社会保险的凭据。依法免税或不需要缴纳社会保障资金的投标人，应提供相应文件证明其依法免税或不需要缴纳社会保障资金。

（2）投标人的资格证明材料应当真实、有效、完整，字迹、印章要清晰。

第四章　采购需求

1.项目说明

1.1 本章内容是根据采购项目的实际需求制定的。

1.2 货物必须为合格产品，质量达到国家相关标准、行业标准、地方标准或者其他标准、规范，中标人供货时应当提供有关货物的合格证明材料等。

1.3 投标人应保证货物是全新、未使用过的合格产品。并完全符合合同规定的质量、规格和性能的要求。中标人应保证所提供的货物经正确安装、正常运转和保养后，在其使用寿命期内应具有满意的性能。在货物质量保证期内卖方应对由于设计、工艺或者材料的缺陷而发生的任何不足或者故障负责。所投产品应提供详细的技术资料，应有检测报告等详细资料。

1.4 进口产品是指通过中国海关报关验放进入中国境内且产自关境外的产品。

政府采购应当采购本国产品。采购人确需招标采购进口产品的，应在招投标活动开始前，按照财政部《政府采购进口产品管理办法》（财库〔2007〕119 号）文件规定办理审核手续，通过财政部门审核后，方可招标采购进口产品，否则采购人不得招标采购进口产品，投标人不得提供直接进口或者委托进口产品（包括已进入中国境内的进口产品）。

采购人或采购代理机构在采购进口产品时不得拒绝国产相同质量产品的制造商或代理商参与投标。

2.招标产品技术规格、要求和数量（包括附件、图纸等）

详见附录。

采购明细详细内容附件：

序号	设备名称	参数要求	单位	数量
1	下一代防火墙	1、系统架构：基于专用多核处理器硬件架构，Web界面可显示处理器核心数，且各核心均参与工作（提供截图证明）；主机系统采用具有自主知识产权的多核多线程 ASIC 并行操作系统平台（提供该操作系统软件著作权复印件加盖厂商公章的电子文	台	2

		档）；系统支持多系统引导（系统数量≥3），多系统设置可在 Web 界面上完成全部操作。 2、★标准 2U 机箱，双冗余电源；配置≥10 个 10/100/1000M Base-TX，≥4 个千兆 SFP 插槽；配置至少 2 个高速 USB2.0 接口，至少 1 个 RJ45 串口；整机吞吐量≥10Gbps，最大并发连接数≥320 万，每秒新建连接数≥8 万。 3、★必须开通病毒防护、IPSEC/SSL VPN、虚拟网关、动态路由、漏洞扫描、主动防御、反垃圾邮件、风险评估、抗拒绝服务攻击等功能；可扩展入侵防御、上网行为管理（含 URL 过滤、应用识别）功能模块。支持 IPv6 地址、地址组配置，支持 IPv6/IPv4 翻译策略技术，包括支持静态 NAT-PT、动态 NAT-PT 技术，支持双栈、6to4 隧道实现 IPv6 终端穿越 IPV4 网络的访问。 4、支持 IPv4 和 IPv6 双栈协议下的病毒扫描与防护，支持双防病毒引擎（标准引擎和增强引擎），杀毒强度可控，支持快速扫描、全面扫描模式；支持国内知名主流品牌病毒库，病毒库提供商通过 ICSA Labs 认证(提供证明电子文档)；支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性。 5、支持路由、透明、混合等各种工作模式下的网络病毒检测，支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个接口、多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境；支持应用协议自识别，可以实现 HTTP,SMTP,FTP,POP3,IMAP,FTP,WEBMAIL 多种应用协议下的病毒防护，支持自定义非标准端口下应用协议的病毒防护。 6、支持对病毒的云防护功能，可将检测出的病毒文件备份至云端进行分析；支持可疑文件检测功能，实现对 HTTP、FTP 以及邮件协议传输的文件进行可疑行为检测，支持病毒文件隔离，用于后续分析取证；支持全面的僵尸病毒检测，既可通过签名特征进行病毒的事前防护，也能基于行为特征进行事中防护，并且可针对至少三种病毒危害级别执行防护动作。 7、支持基于病毒防护规则，可以实现病毒隔离（仅在全面扫毒模式下,且为全局配置）、阻断、声音告警、记录日志，发送告警邮件等 5 种响应方式；系统内置 3 种病毒防护模板，支持自定义病毒防护模板，支持 gzip、rar、zip 等压缩格式的病毒扫描；支持过滤邮件病毒、文件病毒、恶意网页		

		代码、木马后门、蠕虫等多种类型的病毒。 8、内置 IPS 特征库，特征规则数量不少于 3,600 条，特征库可分组；支持 IP 碎片重组、TCP 流重组、会话状态跟踪、应用层协议解码等数据流处理方式；支持模式匹配、异常检测，统计分析，以及抗 IDS/IPS 逃逸等多种检测技术，采用业界领先的入侵检测技术，并取得相关专利。同时具有云计算相关专利技术的主动云防御，可实现全网计算资源、特征资源的共享。 9、流量管理：支持针对文件类型进行流量管理，至少支持 6 类如：电影类、音乐类、图片类、文本类、压缩类、应用程序类等。可以针对不同类型的 URL 配置不同的流量管理规则，包括最大带宽、保证带宽、协议流量优先级等；支持针对用户/用户组进行 URL、文件类型、应用的流量管理；为适应多出口环境，可以支持以网络安全区域为出接口的带宽保证策略；支持基于 IP、端口、用户/用户组、应用、时间等精准精确的流量统计（截图证明），支持对流量统计结果进行冻结和解冻。 10、支持 DMVPN，在增加一个新的分支节点网关后，不需要在中心网关更改任何配置，且支持路由推送，实现 spoke to spoke 互通，不必建立额外隧道；支持多 NAT 环境下的多用户 L2TP 认证加密接入。SSL VPN 默认支持不少于 30 个并发用户授权。 11、支持端口联动，支持上下行端口组的联动，可以实现单端口决定同组中的任意接口失效启动链路切换；自动同步、心跳接口多级（≥2 级）物理备份；支持链路备份、端口冗余、双机热备份、集群备份等,具备集群模式的发明专利（提供证明材料电子文档）。 12、支持一体化安全策略配置，可通过一条策略实现用户认证、IPS、病毒过滤、URL 过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能；支持对多种移动终端接入内网的行为进行防护，禁止非法外联；支持共享接入检测功能，可防止共享上网行为。 13、支持数据防泄密，可对 SMTP 协议主题、正文，HTTP 协议 POST 内容数据以及 FTP 协议文件内容进行敏感信息检测；支持对身份证号（包含港澳台）、银行卡号、手机号、护照号、邮箱、MD5 码等敏感信息进行安全防护。 14、内置 Web 服务攻击防护的特征库，支持对 SQL 注入、XSS 攻击的防护，支持 Webshell 恶意上传行		

		为并进行拦截；支持对 Web 恶意扫描行为的防护能力，至少包含对弱口令、版本探测、漏洞扫描三种行为的防护能力，支持 WEB 服务器错误信息替换，防止服务器信息泄露，提供功能设置、替换信息 Web 页面及生效日志。 15、支持反垃圾邮件功能，支持 SMTP，POP 协议下的垃圾邮件检测，支持邮件服务器地址黑名单、邮件地址、主题、正文、附件名、附件内容等进行关键字匹配过滤；支持防邮件炸弹功能，可设置 POP3、SMTP 的连接频率。 16、提供主动防御与主动扫描功能，支持 IPv4 和 IPv6 双栈协议下的主动防御，可主动屏蔽恶意地址、提前免疫包括病毒网站或者攻击源地址的攻击；要求支持主动扫描发现，支持对服务器、主机等资产的后门、服务探测、文件共享、Windows 系统补丁、认证等主动式扫描。 17、支持报表，可基于用户访问过网站、收发邮件、IM 聊天内容、论坛发帖、文件发送等的内容审计；支持风险评估智能报表，要求至少支持泄密风险、法律风险、工作效率、离职风险等智能报表；支持对 AV/IPS 等攻击事件的全球地图呈现，包含：基于经纬度、城市的攻击源、目地、攻击次数等，地图支持逐级缩放；支持国产化地图引擎（截图证明）。 18、要求产品提供三年原厂软、硬件质保和技术支持服务，并具有： 《计算机信息系统安全专用产品销售许可证》（增强级） 《涉密信息系统产品检测证书》 《中国国家信息安全产品认证证书》（ISCCC 第三级） 《国家信息安全测评信息技术产品安全测评证书》（EAL3+） 《电信设备进网许可证》 《IPv6 Ready Logo Certified》（IPV6 Ready 认证证书） 具有符合“GA243-2000《计算机病毒防治产品评级准则》”安全网关检测报告 具有国际 CVE 组织产品兼容证书，以上证书或证明材料须提供电子文档。		
2	日志审计系统	1、★一体化硬件架构，2U机架式设备，日处理性能3000EPS，配置不少于6个千兆电口，冗余双电源，有效存储空间不少于2T。 2、★配置设计数量≥500个，需涵盖互联网业务系	台	1

		统所有网络设备、安全设备、主机、数据库、中间件以及各种应用系统的告警、并对安全日志实现事件关联分析，集中展现; 3、部署方式：旁路部署; 4、综合展示：能够显示系统的基本管理信息; 5、资产管理：具有资产管理的功能，能够将被管理 IT 资产进行分组、分域出网络拓扑图，展示IT资产之间的逻辑拓扑连接关系，并能够自动进行多种拓扑布局；能够提供基于资产的拓扑视图，显示资产之间的逻辑连接关系。 6、拓扑管理：拓扑管理功能能够运行在 Linux 和 Windows 环境下，展示网络拓扑。 7、日志采集：无需另外安装软件组件，管理中心即可通过SNMPTrap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、NetBIOS、OPSEC等多种方式完成日志 收集功能。；特殊协议支持订制；针对文本格式的日志采集，支持本地文件、Windows共享和FTP获取三种采集方式. 8、事件统计分析：能够以实时统计策略的形式从各个维度进行安全事件进行实时统计分析。支持根据需要结合应用场景，能够重定义关联事件中一个或多个字段的值，比如某些原始事件触发了某一关联规则而产生新的关联事件，原本是一个自动不可干预的过程，关联事件重定义可以凭借安全专家经验，重定义及补全像事件类型、事件名称、摘要描述信息，起到修正、补正信息的作用; 9、事件关联分析：具有安全事件关联分析的能力，能够对不同的事件进行 相关性分析，支持多事件关联，对不同来源的安全事件进行相关性分析。应具备历史日志关联分析的能力；能够对指定时间范围内的不同的历史日志进行相关性分析，发掘潜在的信息；应支持观察列表，可根据关联分析的结果将可疑或者需要关注的信息加入观察列表，并可以对观察列表中的信息进行关联，也可以被任何规则引用; 10、威胁情报支持：应支持通过导入或者主动自动抓取的方式获取外部相关威胁情报信息，并能将这些威胁情报用于关联分析，主要威胁情报包括：恶意IP地址、恶意URL; 11、知识管理：提供开放的知识管理功能，内置安全知识。提供详尽的日志参考知识库，方便用户查询不同原始日志信息的错误ID号和详细描述信息;应提供Cisco PIX和交换机的事件编码知识库；应提供Windows、Linux、Solaris、AIX操作系统的事		

		件ID知识库（提供截图）；应提供Oracle、SQL Server、MySQL、Informix、DB2数据库的事件编码知识库；支持查看系统内置的事件库中事件类型名称及其描述信息。 12，产品资质：产品具备中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》；具备国家保密局涉密信息系统安全保密测评中心《涉密信息系统产品检测证书》；具备《（3C）中国国家信息安全产品认证证书（增强级）》；具有中国信息安全测评中心《信息技术产品安全测评证书》EAL3+级；具有《IPv6 Ready Logo Phase-2》认证证书，以上证书或证明材料须提供电子文档。		
3	网络准入设备	★产品需实现与上级单位做对接。 实现全网设备 NTP 服务同步，采用统一、精准的时间，全网各类型设备都能配置，时间精确，与标准时间同步。 提高 DNS/DHCP 的技术支持能力，消除 DNS/DHCP 服务单点故障，保证业务的连续性，避免设备出现单点故障。 实现集中式、有效的 IP 地址管理分配，通过 IP 开通自动化来控制操作成本；优化网络资源的使用率。 实现集中高效 DNS 域名解析服务，支持多线路 DNS 智能解析，实现服务器宕机检测，提高 DNS 系统安全性和可靠性。 实现非法 IP 接入控制，实现有线、无线网络终端集中管控，根据单位的 IP 规划，不同区域划分不同 VLAN，按需实现自动分配。 设备内嵌 WEB 认证服务，在实现基于 WEB 界面集中管理同时，在同台设备必须要实现 WEB Portal 认证服务，实现设备自服务注册。 灵活的网络端口安全扫描，实时分析服务器/终端提供了哪些应用和服务，能够有效的预先评估和分析终端所存在的安全隐患。 ★设备集成 DNS、DHCP、NTP、TFTP、内置 WEB Portal 认证服务、无线 BYOD 指纹识别控制、IP 地址管理审计、IP 地址接入控制、IP 地址调和、智能 DNS 解析、应用服务器宕机检测，终端服务端口扫描审计、全面支持 IPv6。 设备必须支持 HA（ high-availability）自动切换功能和 active-standby 模式。 联动交换机的 DHCP SNOOPING 和 DAI 功能，可以预防伪 DHCP 服务，避免 IP 地址冲突、ARP 病毒，防止私改 IP 地址。	台	1

		★用户界面支持中文，并具有纠错功能。 支持双因子登录鉴别，支持动态令牌+用户名/密码方式，防止密码重放性攻击。 针对管理员可进行细粒度的管理控制，要求能根据需求，将设备的管理权限分配给多管理员用户进行管理并进行审计；支持记录管理员的相关操作配置；要求支持账户保护功能（多次登陆失败则一段时间内禁止登陆，同时支持手动解锁功能）。 支持将 IP 或 DNS 等外部数据方便的导入，支持.xls 和.xlsx 格式。 支持将数据库内容实时备份和定时备份。 支持将设备的日志文件方便的导出。 设备支持 Telnet 或 ssh。 设备支持和主流的上网行为厂商（深信服、网康、锐捷 SMP、NETGEAR 网件）进行接口联动，实现 IP/MAC 全程审计（需提供上述厂家界面截图，加盖公章的电子文档）。 设备必须提供 WEB Services 接口，供二次开发，实现 DDI 系统与其他系统的整合 支持 SYSLOG 日志发送第三方日志服务器。 兼容同步多种接入设备的时钟，包括网络设备、服务器、PC、小型机等各类型设备，如 windows/ Linux/AIX/Solaris 等。 支持作为一级时间服务器，同步接入设备的时钟。 支持作为二级时间服务器，同步于外部 NTP 网络时间服务器。 支持配置多个外部 NTP 网络时间服务器，并可以灵活排序。 系统必须支持标准的 DNS 服务，支持反向 DNS 解析功能。 ★支持 OSPF+ANYCAST 方式部署，支持配置宣告物理网段。 支持泛域名解析，支持 DNS 轮询，实现 DNS 负载均衡。 支持中文域名，DNS 解析服务支持中文域名记录。 微软 AD 域支持，能够与微软 AD 域控结合，自动同步生成 NS、SRV、A 等记录，接管其 DNS 服务（需提供界面截图，加盖公章的电子文档）。 支持 DNS 智能解析，支持设定网通、电信、移动等 IP 地址段，针对不同的地址段解析不同的 IP，便于外部访问主页提高访问速度。 ★支持 DNS 业务健康检测，支持 Ping，TCP/端口，Http URL，Https URL，SNMP 等检测方式。 支持 DNS 域名过滤，可自定义域名 URL，实时生		

		效。 DHCP 服务：基于 IP/MAC 地址的静态绑定（IP 保留地址分配）；实现地址的动态分配和回收；支持所有 ISC 预定义的 DHCP option 空间（如 Option 1 到 Option 125）和客户化的 DHCP Option 空间（如 Option 126 到 Option 254）。 ★支持通过 DHCP 下发无线控制器信息，支持不同类型、厂家无线 AP 在子网/VLAN 内混合组网，智能引导各厂家无线 AP 自动注册，支持显示中文计算机名称（Windows 非标准字符），终端的计算机名称可配置为中文，通过 DHCP 显示中文计算机名。 支持 IP 地址强制释放功能，针对部分终端 DHCP 租期到了不会主动续约并继续使用过期 IP 的情况，实现手工和周期性强制释放 IP 地址，可定制定强制释放天数，以确保 IP 地址的利用率。 支持 DHCP 实时在线用户趋势分析、DHCP 响应包趋势分析、IP 数据利用率实时统计分析、DHCP 指纹数据实时统计等。 支持创建 DHCPv6 地址分配池。 支持 DHCPv6 有状态地址分配，支持自动发现设备 DUID 标识（需提供界面截图，加盖公章的电子文档）。 中央数据集中的 IP 管理控制台，支持 IPv4、IPv6 双栈地址管理 支持交换机自定义脚本配置功能，实现与交换机之间自动和交互式任务进行通信，提供快速开通配置交换机等功能 实时显示分配地址的状态和续租信息 实名制地址分配、回收和历史数据的审计分析 支持 DHCP 系统指纹技术，支持 BYOD（BringYourOwnDevice），自动识别智能手机、平板电脑等的系统指纹 。 支持 DHCP 指纹识别率 98%以上，支持快速对 DHCP 未知指纹进行识别及添加（需提供界面截图，加盖公章的电子文档）。 支持数据完整性检查，数据核查机制可以在系统部署前进行数据检查，提前发现系统配置的问题 ★支持 MAC 地址黑白名单，可以只对已授权 MAC 的设备分配 IP 地址。向 MAC 动态授权列表内临时添加新的记录，不需要重启 DHCPv4 服务进程。 灵活的 MAC 地址永久授权，及 MAC 地址活跃度分析。 ★内置 WEB　Portal 认证服务器，在实现基于 WEB 界面集中管理同时，在同台设备必须要实现 WEB		

		Portal 认证服务，实现设备自服务注册。 支持 IP 自助授权和管理员审批授权等多种方式，可通过后台配置进行灵活切换（需提供界面截图，加盖公章的电子文档）。 支持配置访客地址使用期限设定。 支持手动/定期解除已授权地址。 基于 Portal 的访客自服务注册信息录入和自动授权，针对于笔记本和手机终端支持响应式界面，既然页面自适应。 ★支持以旁路的方式接入网络中，使用标准 SNMP 协议对网络设备进行端口操作，开启或关闭。 支持发现同一 VLAN 内相同 IP 和 MAC 更换端口的操作，可进行一键端口关闭。 ★支持终端服务端口扫描功能，支持多种扫描方式，包括 TCP 同步扫描(TCP SYN)/TCP connect()扫描)/TCP ACK 扫描/TCP Window 窗口扫描/TCP Maimon 扫描/UDP 扫描。 支持终端端口状态变更审计，利于实时统计终端安全状态。 支持发现待清除核查状态，此状态表明此 IP 地址长时间没有被使用 支持发现未知 IP 核查状态，此状态表明此 IP 由于各种原因没有被记录在系统中，如非法接入、手动私设地址等。 支持设备端口和 MAC 扫描，自动周期性发现 IP 设备和交换机端口的对应关系，自动发现和显示 VLAN 信息，显示交换机端口的详细信息，包括端口速率，端口状态，端口信息描述等信息。 集成 Expect 编程工具语言，自动实现交互式任务。通过用户名和密码实现模拟登录过程，实现指令交互，支持定制计划任务，如脚本的执行时间、周期等（需提供界面截图，加盖公章的电子文档）。 提供软件著作权证书、软件产品登记证书、3C 认证证书、公安部等保三级评测报告、公安部销售许可证、中国泰尔实验室入网检测报告、原厂授权以及服务承诺函（以上证明材料须提供电子文档。）; 所供货 CNS 网络核心服务设备的厂商，应能提供 365 x 24 的标准技术支持服务，应包括但不限于客户服务网站/MAIL/电话热线服务 所供货 CNS 网络核心服务设备必须具有 NBD 服务，当硬件出现故障时，能够及时提供备品备件。		
4	数据库审计	1、系统采用专用硬件架构与专用安全操作系统；专用的安全操作系统具有自主知识产权；审计设备	台	1

		的存储支持RAID1阵列，空间不得少于4T。 2、★支持千兆网络环境监听，2U上架专用设备，双电源，≥6电口（含1个管理口）和1扩展槽，提供1个RJ45串口。 3、系统审计事件每秒入库速度至少在25000条/秒以上，日处理审计事件数至少15000万条; 4、采用旁路部署方式对原有网络不造成影响，网络审计产品的故障不影响被审计系统的正常运行;无需在被审计系统上安装任何代理。 5、支持对 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、MongoDB、Redis 数据库进行审计，支持人大金仓 KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase) (需提供功能截图的电子文档) 6、支持 FTP、Rlogin、Radius、NFS、X11 等协议审计(需提供功能截图电子文档) 7、针对异常场景自动生成审计结果，免配置; 8、异常场景包含且不限于: 异常账号访问审计、数据库异常审计、同账号多 IP 登陆、同账号上下班时间操作统计、访问时长异常审计、操作全审计等; 9、异常账号审计支持对数据库近一个月没有登陆账号突然登陆的异常行为进行审计;（截图证明电子文档） 10、数据库异常审计支持对于数据库异常信息的统计与发现，一键生成审计结果; 11、支持对于短时间内相同账号多个 IP 地址登陆的自动发现与审计，用以发现账号被盗用等异常; 12、支持对相同账号下班时间操作多于上班时间的异常操作自动发现和审计; 13、支持访问操作的全审计，自动生成审计策略，自动生成报表; (需提供功能截图电子文档) 14、产品需具备以下产品资质: 公安部销售许可证（增强级） 涉密信息系统产品检测证书 《中国国家信息安全产品认证证书》（3C 认证），以上证书或证明材料须提供电子文档。		
5	安全可视化管理平台 SOC	1、运行环境: 要求采用 B/S 架构; 集成数据库。支持 Windows 或 Linux 操作系统，支持 64 位操作系统; 事件处理性能平均每秒≥8000 条事件。 2、★管理节点数量≥1000 个，需涵盖互联网业务系统所有网络设备、安全设备、主机、数据库、中间件以及各种应用系统的告警、并对安全日志实现事件关联分析，集中展现;	台	1

		3、★部署方式：支持分布式部署和群集模式，多级、多点部署时，采用分布式存储；支持两个管理中心之间可以进行级联，形成大规模统一管理；为保证管理一致性，实现可视化信息统一管控。 4、综合展示：能够显示系统的基本管理信息； 5、资产管理：具有资产管理的功能，能够将被管理 IT 资产进行分组、分域出网络拓扑图，展示 IT 资产之间的逻辑拓扑连接关系，并能够自动进行多种拓扑布局；能够提供基于资产的拓扑视图，显示资产之间的逻辑连接关系。 6、拓扑管理：拓扑管理功能能够运行在 Linux 和 Windows 环境下，展示网络拓扑。 7、日志采集：无需另外安装软件组件，管理中心即可通过 SNMPTrap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、NetBIOS、OPSEC 等多种方式完成日志 收集功能。分别配置 XX 个分布式事件采集器和 XX 个分布式事件存储器。 8、事件统计分析：能够以实时统计策略的形式从各个维度进行安全事件进行实时统计分析。 9、事件关联分析：具有安全事件关联分析的能力，能够对不同的事件进行 相关性分析，支持多事件关联，对不同来源的安全 事件进行相关性分析。 10、知识管理：提供开放的知识管理功能，内置安全知识。 11、网络管理：对支持 SNMP 协议的主流网络设备和安全设备进行管理；支持主流版本的 Windows、Linux、UNIX 等主机和服务器；支持主流版本的 Oracle、DB2、Sybase、MySQL 等数据库；支持主流版本的 Weblogic、WebShpere、JBoss、Apache、Tomcat 等中间件；支持多种网络服务的运维和管理，包括 但不限于：SMTP、POP3、HTTP、FTP、TELNET、SSH、SSH2、DNS、DHCP、WINS、LDAP。 12、漏扫驱动：支持对漏扫引擎进行集中管理，并对漏扫引擎下发扫描任务，收集扫描结果，统一进行漏洞脆弱性分析；至少支持三种漏扫引擎的调度，必须明确列举出来；漏扫结果可以自动参与到弱点管理模块中，并参与脆弱性计算。 13、配置核查：系统应具有主动的配置安全核查功能，能够对核查对象的配置进行细粒度的安全符合性检查，并出具核查报告；系统支持多种核查调度策略，包括即时核查、定时核查、周期性核查和离线核查四种核查方式。 14、威胁态势分析：支持通过建立并针对一组关键		

		指标体系（KPI）计算得到一个威胁指数，以此来表征一段时间内、某个网络区域的网络安全威胁状态及其发展趋势；能够计算全网或者一级安全域的威胁态势指数，并自动描绘出态势指数曲线；能够描绘态势成因雷达图和帕累托图，展示出每种态势成因在态势指数中所占的比重；系统能够分析并展示当前态势指数与上个周期的态势指数的环比变化情况；能够展示一幅热点分析图，以三个同心圆的方式展示应用层、网络层和终端层的热点信息。 15、流安全分析：支持端口镜像与被动接收两种方式采集流数据，可接受支持 NetFlow、NetStream、Sflow 和 jflow 协议的采集；支持按业务场景进行流量分析，可自定义业务场景，至少包含总流量、数据包、top 端口、top 地址和 top 协议等维度，可以对业务场景流量进行 top 端口、top 地址、top 协议的排行分析与查看；支持协议流量分析，可分别分析应用层、传输层、网络层、链路层的不同层面的协议的流量情况。 16，产品资质要求：产品具备中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》；具备国家保密局涉密信息系统安全保密测评中心《涉密信息系统产品检测证书》；具备《（3C）中国国家信息安全产品认证证书（增强级）》；具有中国信息安全测评中心《信息技术产品安全测评证书》EAL3+级；具有《IPv6 Ready Logo Phase-2》认证证书，以上证书或证明材料须提供电子文档。		
6	入侵防御系统	1、系统架构：基于专用多核处理器硬件架构，Web 界面可显示处理器核心数，且各核心均参与工作；操作系统为 VSP 通用安全平台，具备高效、智能、安全、健壮、易扩展等特点。(提供 VSP 证明文件并加盖公章的电子文档) 2、标准 2U 机箱，双冗余电源；配置≥6 个 10/100/1000M Base-TX，≥4 个千兆 SFP 插槽；配置至少 2 个高速 USB2.0 接口，至少 1 个 RJ45 串口；整机吞吐量≥6Gbps，最大并发连接数≥320 万，每秒新建连接数≥8 万。 3、系统可检测的入侵防御事件库事件数量不少于 4000 条，系统应支持事件响应模版，能够批量修改事件响应动作，包括：事件级别、事件启用开关、动作、日志合并方式、日志开关、抓包取证。系统应支持弱口令检测功能，需支持至少 8 种网络协议并支持至少 7 种弱口令检测元素，文字说明支持的网络协议和定义弱口令的检测元素。	台	1

		4、系统应支持多种防 web 扫描能力，包括爬虫、CGI 和漏洞扫描等，并支持设置至少 5 个不同级别的扫描容忍度/扫描敏感度。系统应支持多种事件响应方式，满足客户的安全要求，需包括：重置、临时阻断、丢弃报文、丢弃会话等动作。系统应支持密码穷举探测功能，提供至少 16 种应用的密码穷举行为探测和阻断。 5、为保证病毒检测的可靠性，要求系统应至少支持双病毒引擎，需提供界面截图并提供防病毒引擎厂商合作证明，并加盖原厂公章的电子文档。 6、★系统支持具有云计算相关专利技术的主动云防御功能，实现全网计算资源、特征资源的共享。 7、系统应支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 50 万。 8、系统应支持 HTTP 协议和邮件协议防病毒，通过信息替换功能，用以通知用户病毒被阻断，管理员可以自行设置替换信息。 9、系统应提供扩展静态恶意代码（APT）检测引擎，针对 http、ftp、SMTP 等协议中包含的未知恶意文件进行检测。 10、★系统应支持可扩展恶意样本自学习功能，除通过网络文件捕获外，还支持通过系统直接上传文件，自动识别黑白文件并提供简要信息。 11、系统应支持与动态恶意代码（APT）检测系统联动功能，通过联动功能可将恶意样本发送到动态 APT 引擎进行深度检测，并将检测结果生成攻击特征样品进行动态拦截。 12、系统应支持可扩展未知 C&C 通道（隐蔽通道）检测功能，能够提供 C&C 通道的危险级别、连接建立时间、连接持续时间、控制端 IP 地址和端口、受控端 IP 地址和端口等 C&C 通道信息。 13、系统除具备可扩展的本地恶意代码检测功能外，还应具备云查杀、云检测等防御机制。 14、系统应支持 Web 过滤功能，至少支持黑白名单、关键字过滤、禁止 HTTP 代理、URL 分类过滤外，还支持 Script、 Java Applet 等过滤，并能通过统一模版设置。 15、系统应支持邮件内容过滤功能，有效防止恶意邮件及信息外泄。可根据邮件 SMTP 命令、发件人、主题、附件、IP 及邮件大小进行过滤。 16、系统应支持敏感信息防护功能，识别信息和文件中的关键字、身份证、手机号码、固定电话号码、银行卡、IP 地址等敏感信息，并支持文件指纹		

		识别和白名单功能。 17、系统应支持 WEB 登录图像验证码功能，防止暴力破解。 18、要求提供三年原厂软、硬件质保和技术支持服务、并提供三年特征库升级服务，同时要求产品具有: 《计算机信息系统安全专用产品销售许可证》（增强级） 《涉密信息系统产品检测证书》 《中国国家信息安全产品认证证书》（ISCCC 第三级） 《国家信息安全测评信息技术产品安全测评证书》（EAL3+） 《军用信息安全产品认证证书》（军 B 级） 《计算机软件著作权登记证书》 具有国际 CVE 组织产品兼容证书，以上证书或证明材料须提供电子文档。		
7	路由器	路由器机框、配置机箱附件、配置双电源、1 块灵活接口平台 300,1 HIM 插槽,12 端口 GE Combo ★1、支持与原有的路由器虚拟成一台逻辑设备使用，采用全分布式硬件架构；要求支持主控、业务板和交换网板物理分离；整机线卡采用母板+子卡架构形态，母板和子卡均可热拔插; 2、交换容量：≥70Tbps；包转发率：≥6000Mpps 3、整机框全物理尺寸的业务槽位数≥2，不含主控、交换网板槽位,非子卡槽位；支持独立交换网板。 4、支持 E1/T1、FE、GE、10GE、POS（155M/622M/2.5G）、CPOS、RPR、同步串口等广域网接口 5、内置硬件加密引擎，本次要求实际配置具备 IPsec VPN 功能的硬件板卡或功能 license; 6、要求支持 OTV/EVI 等数据中心虚拟机迁移二层协议技术，并可提供高安全的加密功能。 ★7、硬件支持 NAT 功能，本次要求实际配置具备 NAT 功能硬件板卡或功能 license; 8、支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合；虚拟化技术需提供权威机构出具的报告复印件加盖厂家公章的电子文档。 9、支持 L2TP、GRE，本次要求实际配置具备 L2TP、GRE VPN 功能的硬件板卡或功能 license; 10、支持与路由器一体化的防火墙、IPS（或 IDS）、ACG 业务板，以简化管理，消除单点故障。	台	1

		11、本次配置：⩾1 个主控；⩾2 个模块化电源；⩾12 个千兆光接口，⩾12 个千兆电接口。		
8	交换机	★1、支持与原有交换机冗余使用，业务插槽数⩾6；主控引擎模块⩾2；交换容量⩾85Tbps；转发性能⩾26400Mpps 2、以太网支持千兆电口，千兆光口，10GE 端口、40G 端口、100G 端口；单槽位线速万兆端口密度⩾16；单槽位线速 40G 端口密度⩾4；单槽位万兆端口密度⩾48；单槽位 40G 端口密度⩾8；单槽位 100G 端口密度⩾2；单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数⩾48；支持 FCoE 接口；支持 EPON OLT 接口；支持 RPR。支持 POE+，满足新一代园区网以太网供电需求，提供工信部权威第三方测试报告复印件加盖厂家公章的电子文档。 3、聚合组数⩾128 组，每组成员⩾8 个；支持跨设备链路聚合 4、多虚一技术(N:1)，支持 4 框虚拟化技术，一虚多技术（1:N），支持多虚一技术和一虚多技术的配合使用，提供工信部权威第三方测试报告提供工信部权威第三方测试报告复印件加盖厂家公章的电子文档。 5、支持 MACsec 6、提供工信部入网证,产品最早入网时间⩾3 年 ★7、本次配置要求：配置单主控；配置冗余电源；实配千兆电口⩾48，千兆光口⩾24，万兆光口⩾4；配置⩾10 个千兆多模光模块。 ★8、要求与核心路由器统一品牌	台	1
9	●运维平台	1、★1U 机架式一体设备，单电源，物理存储⩾2TB; 至少支持 6 个千兆电口，具有一个扩展插槽，可扩展 4 个千兆光口、8 个千兆光口、8 个千兆电口、4 个千兆光口+4 个千兆电口或 2 个万兆光口; 2、★字符协议不低于 1000 个，图形协议不低于 300 个，可管理设备数不低于 500 台; 3、专用安全操作系统，软硬件一体化，物理旁路，逻辑串联模式，不影响正常业务流量，A 双机热备，支持 NAT 地址映射部署，通过映射后的 IP 地址访问堡垒机，分布式部署：支持添加一台或多台协议代理服务器，分担审计中心性能压力；并支持通过不同的协议代理服务器节点访问不同的资源，多协议代理服务器节点可访问相同资源时实现自动负载均衡; 4、字符协议：SSHv1、SSHv2、TELNET、RLOGIN,	套	1

		图形协议：RDP、VNC、X11，文件传输协议：FTP、SFTP；数据库协议：支持 Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、TeraData 等数据库类型；支持通过应用发布进行协议审计，记录命令详情，包括字符协议和数据库协议等，审计回放支持协议回放和图形回放；支持通过应用发布进行协议扩展第三方客户端，并支持账号密码代填登录；支持通过应用发布对 http/https 的访问过程进行录像审计；支持 web 页面防跳转功能，进行 http/https 访问过程中，运维人员仅允许访问授权地址 5、支持 Oracle、postgresql、sybase、mysql、sqlserver 数据库下行返回行数和 oracle 数据库变量绑定； 6、支持运维客户端功能，运维操作过程不依赖浏览器和 JAVA 环境；通过堡垒机 web 页面内嵌 SSH、FTP、TELNET 运维工具访问目标资源；通过堡垒机 web 页面调用本地工具访问目标资源；户端菜单模式访问：用户可通过字符菜单（TELNET、SSH 协议）或图形菜单（RDP、VNC 协议）方式选择目标服务器并进行访问； 7、RDP 协议支持剪切板、本地磁盘映射功能，所有图形协议支持自适应本地浏览器窗口大小；windows 服务端开启安全层 SSL 加密，加密级别符合 FIPS 标准，允许运行使用网络级别身份验证的远程桌面的计算机连接； 8、支持 TELNET、SSH 协议使用 SecureCRT 工具批量登录目标资源；多种本地工具支持，支持 SecureCRT，WinSCP，SQLPlus，PLSQLDev，Toad4Oracle，Db2cmd（DB2），TightVNC，pgAdmin3，SqlAdvantage，Sqleditor，mysql，QuestCentral，SSMS，Xshell，dbvis，Navicat，SSH Secure Shell Client； 9、RDP 图形操作过程中键盘输入操作记录和鼠标点击行为记录，支持开启或关闭键盘输入审计功能，支持 RDP 窗口标题审计，并支持窗口标题内容检索定位回放 10、以 WEB 在线视频回放方式重现维护人员对服务器的所有操作过程，无须在客户端安装播放客户端软件，离线回放重现维护人员对服务器的所有操作过程（回放文件下载到本地播放）；倍速/低速播放、拖动、暂停、停止、重新播放会话协议回放空闲时间过滤，应用发布图像操作回放支持操作空闲		

		过滤（可设置无操作多长时间开始过滤）等播放控制操作；根据审计日志操作命令和RDP键盘输入命令开始回放； 11、支持按设备、系统帐号、计划开始时间、改密周期等信息配置改密计划，到期自动执行，随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并严格遵守密码强度设置；手工改密功能；支持自动改密结果发送到指定改密计划的管理员邮箱； 12、自动改密支持Linux、Unix、Windows（采用RPC方式）、AIX以及Oracle、SqlServer、PostgreSQL、MySql、DB2、Informix 、SYBASE的内置自身账号密码； 13、支持实时监控当前连接发生的所有会话信息和阻断功能，审计系统CPU、内存、磁盘的使用情况，记录审计系统自身的管理操作，保障审计系统自身安全，会话查询可定义条件，包括会话时间范围、用户、资源、操作命令关键字、指令策略等条件；以CSV、HTML方式生成并导出报表，管理员自定义审计报表，以日报、周报、月报的方式自动生成周期性报表 14、审计查询关键字和结果显示支持多种编码(UTF-8、Big5、EUC-JP、EUC-KR、GB2312、GB18030、ISO-8859-2、KOI8-R、KS_C_5601_1987、Shift_JIS、Window-874)，由用户自主选择； 15、支持数据备份，系统配置的导入、导出功能，配置和数据备份自动导出到FTP服务器、空间自管理功能，存储空间不足时能够自动清理历史数据，可自定义清理存储空间的阀值； 16、从WEB界面修改网卡IP设置、静态路由设置等内容，支持IPv6；支持网口聚合功能。		

采购人允许偏离范围或者幅度：

3.商务条件

3.1 交货期

合同签订后20日内交货并安装调试完毕。

3.2 交货地点

招标人指定地点。

3.3 付款方式

供货安装调试完毕并验收通过后一次性付清全部货款。

3.4 验收

3.4.1 货物运抵现场后，采购人将对货物数量、质量、规格等进行检验。如发现货物和规格或者两者都与招标文件、投标文件、合同不符，采购人有权限根据检验结果要求中标人立即更换或者提出索赔要求。

3.4.2 货物由中标人进行安装，完毕后，采购人应对货物的数量、质量、规格、性能等进行详细而全面的检验。安装完毕 7 日后，证明货物以及安装质量无任何问题，由采购人组成的验收小组签署验收报告，作为付款凭据之一。

3.5 质量保证期

3.5.1 质保期：自验收合格之日起 3 年，国家主管部门或者行业标准对货物本身有更高要求的，从其规定并在合同中约定，投标人亦可提报更长的质保期。

3.5.2 质量保证期内，如果证实货物是有缺陷的，包括潜在的缺陷或者使用不符合要求的材料等，中标人应立即免费维修或者更换有缺陷的货物或者部件，保证达到合同规定的技术以及性能要求。如果中标人在收到通知后 5 天内没有弥补缺陷，采购人可自行采取必要的补救措施，但风险和费用由中标人承担，采购人同时保留通过法律途径进行索赔的权利。

3.6 售后服务

3.6.1 中标人应提供及时周到的售后服务，应保证每季度至少一次上门回访、检修。

3.6.2 中标人在接采购人通知 1 小时做出响应，2 小时内到达现场，24 小时内维修完毕，不能在规定时间内修好的要免费提供备品（机）备件。

3.6.3 中标人免费为采购人提供中文操作手册并培训操作人员，其中包括讲解产品的结构以及原理、产品的使用以及维护保养，直至操作人员能够独立的操作使用。

注：上述要求以及标注中：

带“★”条款为实质性条款，投标人必须按照招标文件的要求做出实质性响应。

带“▲”标注的产品为政府强制采购产品，政府强制采购产品是指财政部、发展改革委最新发布“节能产品政府采购清单”中的政府强制采购节能产品。

带“※”标注的产品为投标人开标时需提供的样品，中标后投标人送至采购人指定地点封存。投标人提交的样品与投标文件不一致的，由投标人承担相关法律责任。

带“●”标注的产品为核心产品，系指在非单一产品采购项目中，采购人根据采购项目技术构成、产品价格比重等合理确定的产品。

第五章　评标办法

1.相关要求

1.1 技术汇总得分的计算方法：评标委员会成员技术评分的算术平均值。

1.2“同类项目”是指投标人已经完成的与本次采购要求相同或者类同的货物，并且签订合同一方必须是投标人，以相同或者类同部分的合同金额为准。

1.3 执行国家统一定价标准和采用固定价格采购的项目，其价格不列为评审因素。

1.4 依据《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）文件规定，残疾人福利性单位投标的须提供本单位的服务及《残疾人福利性单位声明函》并对声明函的真实性负责；残疾人福利性单位投标的视同小型、微型企业，按照本招标文件小型、微型企业的相关价格扣除标准执行。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

1.4.1 享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：

（1）安置的残疾人占本单位在职职工人数的比例不低于 25%（含 25%），并且安置的残疾人人数不少于 10 人（含 10 人）；

（2）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

（3）为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；

（4）通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；

（5）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）。

1.4.2 前款所称残疾人是指法定劳动年龄内，持有《中华人民共和国残疾人证》或者《中华人民共和国残疾军人证（1 至 8 级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或者服务协议的雇员人数。

1.4.3 符合条件的残疾人福利性单位在参加政府采购活动时，应当提供《残疾人福利性单位声明函》（见附件），并对声明的真实性负责。

1.4.4 中标、成交供应商为残疾人福利性单位的，采购代理机构应当随中标、成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。

1.4.5 投标人提供的《残疾人福利性单位声明函》与事实不符的，依照《政府采购法》第七十七条第一款的规定追究法律责任。

1.5 对于非专门面向中小企业或小型、微型企业采购的项目，中型、小型、微型企业应当同时符合以下条件：

1.5.1 依据财政部、工业和信息化部《政府采购促进中小企业发展暂行办法》（财库〔2011〕181 号）规定，中型、小型和微型企业投标的须提供《中小企业声明函》并对声明函的真实性负责；

1.5.2 按照《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300 号）规定，投标人应符合中小企业划分标准；所称中小企业划分标准，是指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。

1.5.3 提供本企业制造的货物、承担的工程或者服务，或者提供其他中小企业制造的货物。本项所称货物不包括使用大型企业注册商标的货物。

1.6 小型、微型企业提供中型企业制造的货物的，视同为中型企业。

1.7 小型和微型企业提供的货物中含有中型及以上企业的产品或者大中型企业提供货物中含有小型、微型企业产品的，均不给予价格扣除。

1.8 评分得分非整数的保留小数点后两位（小数点后第三位数四舍五入）。

1.9 监狱企业参与政府采购活动，均视同小型、微型企业，享受国家优惠政策。

2. 评分标准

评分项目		分数	评分标准
商务部分	投标报价	30	满足招标文件要求且投标价格(或者最终价格)最低的投 标报价为评标基准价，其价格分为满分。 其它报价得分=评标基准价÷(投标报价或者最终价格)×30。
	投标人业绩	2	自 2016 年 1 月 1 日至今(近三年)已完成的同类项目(合同金额 150 万元及以上的)，每份得 1 分。 须同时提供政府采购同一项目的中标通知书原件的电子文档、合同原件的电子文档、验收报告原件的电子文档，三项原件的电子文档缺一项不得分。同类项目时间以验收报告签署时间为准。
	售后服务机构	3	青岛地区注册或设有分支机构的得 3 分（提供营业执照原件的电子文档，未提供的不得分），或在青岛具有常驻售后服务机构的得 1 分（提

				供包含维修营业范围的售后维修机构营业执照原件的电子文档、双方协议书原件的电子文档，未提供或者提供不全的不得分)。
	质保期		3	在满足招标文件质保期的基础上，每增加一年得1分，满分3分（以商务响应表中的质保期为准)。
	政策加分优采	节能产品加分	4	提供的货物品牌、型号以及制造商等信息必须与财政部、发展改革委最新发布“节能产品政府采购清单”或者财政部、环境保护部最新发布“环境标志产品政府采购清单”一致。加分计算方法是： “节能产品政府采购清单”优采加分：加分=4×[所投“节能产品政府采购清单”(政府强制采购节能产品除外）中的产品价格在投标报价中所占比例]，总计最高加$(分值)分。 若所投产品同时列入最新发布“节能产品政府采购清单”和“环境标志产品政府采购清单”的，则应当优先于只列入其中一种最新发布政府采购清单的进行优采加分。 开标时，需提供产品所在最新发布的政府采购清单完整页，且在清单中标注所在位置，并加盖投标人公章的电子文档，否则不得分。
		环保产品加分	4	提供的货物品牌、型号以及制造商等信息必须与财政部、发展改革委最新发布“节能产品政府采购清单”或者财政部、环境保护部最新发布“环境标志产品政府采购清单”一致。加分计算方法是： “环境标志产品政府采购清单”优采加分：加分=4×[所投“环境标志产品政府采购清单”中的产品价格在投标报价中所占比例]，总计最高加$(分值)分。

				若所投产品同时列入最新发布“节能产品政府采购清单”和“环境标志产品政府采购清单”的，则应当优先于只列入其中一种最新发布政府采购清单的进行优采加分。 开标时，需提供产品所在最新发布的政府采购清单完整页，且在清单中标注所在位置，并加盖投标人公章的电子文档，否则不得分。
技术部分	响应情况		15	基础分为 10 分。 优于招标文件实质性要求的，每有 1 项加 1 分，最高加 5 分;对非实质性要求，每出现 1 条正偏离，加 0.5 分，最高加 2 分，(以上两项最高加 5 分)。 每出现 1 条负偏离，扣除基础分 2 分，出现 5 条及以上负 偏离的，响应情况项不得分。
	质量与性能		12	产品的市场占有率高、品牌信誉度好，得 6-1 分;产品的 性能先进、技术成熟，得 4-1 分;产品的配备备件和备选配件价格低，得 2-1 分。
	技术措施		5	有完善的供货组织方案、产品安装和调试的主要技术保证 措施，得 3-1 分;有完善的人员培训计划和应用技术支持，得 2-1 分。
	企业及产品认证		27	1、投标人通过 ISO14001 环境管理体系认证得 1 分，开标时提供证书原件的电子文档，未提供不得分。 2、投标人通过职业健康安全管理体系认证得 1 分；开标时提供证书原件的电子文档，未提供不得分。 3、投标人须具有省级或以上保密局颁发的涉密系统集成资质乙级或以上资质证书得 5 分；开标时提供证书原件的电子文档，未提供不得

			分。 4、投标人所投路由器、交换机生产厂商具备ISO50001 能源管理体系认证的得 3 分，需提供证书复印件并加盖厂商公章的电子文档，未提供不得分. 5、投标人所投路由器、交换机生产厂商具备健全的环保体系，通过 QC080000 有害物质过程管理体系认证得 3 分，需提供证书复印件并加盖厂商公章的电子文档，未提供不得分. 6、投标人所投路由器、交换机生产厂商具备科学、系统的知识产权管理体系得 2 分，提供《知识产权管理体系认证证书》复印件并加盖设备厂商公章的电子文档，不提供不得分。 7、所投防病毒安全网关厂家具备系统集成一级及涉密系统集成甲级资质得 3 分；提供相关资质证明复印件并加盖厂家公章的电子文档 8、所投安全管理可视化 SOC 产品的厂家在省法院系统具备一个“安全管理可视化 SOC”建设案例的得 3 分；（提供证明复印件并加盖厂家公章的电子文档）。 9、所投安全产品厂家在省法院系统具备相关建设案例的，提供一个百万级以上合同得 2 分，最高得 6 分。(提供证明复印件并加盖厂家公章的电子文档)。
	售后服务方案	3	技术人员配置、服务响应时间，得 1 分(提供常驻地行政 部门出具的社保证明原件的电子文档或社保网站打印的社保证明原件的电子文档，未提供或者提供不全的不得分);有详细的售后服务方案、质量 保证期内产品维护措施，得 2-1 分。

3.政策加分以及计算方法

3.1 说明：

（1）投标人所提供的材料或者填写的内容必须真实、可靠，如有虚假或隐瞒，一经查实将导致投标被拒绝，并按照《中华人民共和国政府采购法》第七十七条第一款“提供虚假材料谋取中标、成交的”进行处罚，给采购人造成损失的应承担赔偿责任。

（2）以上评标标准中要求投标人提交相关证明材料原件（或复印件）的，未装订在投标文件中的不得分。

（3）投标单位以联合体的身份参与政府采购项目的，以商务部分加分最多的一家投标单位的加分为商务部分的加分。

（4）资产负债率=年末负债合计÷年末资产总计。

3.2 给予残疾人福利性单位价格扣除

3.2.1 给予残疾人福利性单位（包括相互之间组成的联合体）产品的价格 10%的扣 除；计算方法是： 最终价格＝投标报价×90%，按照最终价格计算其价格分得分。开标时，投标人须提供《残疾人福利性单位声明函》原件，否则不给予价格扣除。

3.2.2 大中型企业和其他自然人、法人或者其他组织与残疾人福利性单位组成联合 体投标，联合协议中约定，残疾人福利性单位的协议合同金额占到联合体协议合同金 额 30%以上的，可给予联合体 3%的价格扣除。计算方法是： 最终价格＝投标报价×97%，按照最终价格计算其价格分得分。 开标时，投标人须同时提供《残疾人福利性单位声明函》和联合体协议原件，否 则不给予价格扣除。

3.2.3 残疾人福利性单位属于小型、微型企业的，不重复享受政策。

3.3 给予小型和微型企业价格扣除

3.3.1 给予小型和微型企业（包括相互之间组成的联合体）产品的价格 10%的扣23 除；计算方法是： 最终价格＝投标报价×90%，按照最终价格计算其价格分得分。开标时，投标人须提供中小企业声明函原件，否则不给予价格扣除。

3.3.2 大中型企业和其他自然人、法人或者其他组织与小型、微型企业组成联合体 投标，联合协议中约定，小型、微型企业的协议合同金额占到联合体协议合同金额30% 以上的，可给予联合体 3%的价格扣除。计算方法是： 最终价格＝投标报价×97%，按照最终价格计算其价格分得分。 开标时，投标人须同时提供小型、微型企业中小企业声明函和联合体协议原件， 否则不给予价格扣除。

第六章　投标人须知

1.招标依据以及原则

1.1《中华人民共和国政府采购法》;

1.2《中华人民共和国政府采购法实施条例》;

1.3《政府采购货物和服务招标投标管理办法》;

1.4《政府采购质疑和投诉办法》;

1.5《山东省政府采购管理办法》;

1.6《中华人民共和国合同法》;

1.7 其他有关法律、行政法规以及省市规范性文件规定。

2.合格的投标人

2.1 符合《中华人民共和国政府采购法》第二十二条规定的条件;

2.2 符合本招标文件规定的资格要求，且按照要求提供相关证明材料;

2.3 单位负责人为同一个人的两个以及两个以上法人，母公司、全资子公司以及其控股公司或者存在管理关系的不同单位，都不得在同一包或者未划分包的同一招标项目同时投标;

2.4 投标人须知前附表规定接受联合体投标的，应符合以下规定:

2.4.1 联合体各方应按照招标文件提供的格式签订联合体协议书，明确联合体牵头人和各方权利义务;

2.4.2 联合体各方均应当符合《政府采购法》第二十二条第一款规定的条件;

2.4.3 联合体中有同类资质的投标人按照联合体分工承担相同工作的，应当按照资质等级较低的投标人确定资质等级。

2.4.4 以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他投标人另外组成联合体参加同一合同项下的政府采购活动。

2.4.5 联合体各方应当共同与采购人签订采购合同，就合同约定的事项对采购人承担连带责任;

2.4.6 鼓励大中型企业和其他自然人、法人或者其他组织与小型、微型企业组成联合体投标，但联合体各方均应符合上述规定。

2.5 除采购人拟采购进口产品通过财政部门审核外，投标人不得提供直接进口或者委托进口产品（包括已进入中国境内的进口产品）。

2.6 为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人，

不得再参加本项目的招标活动。

2.7 采购代理机构及其分支机构不得在所代理的采购项目中投标或者代理投标，不得为所代理的采购项目的投标人参加本项目提供投标咨询。

2.8 投标人提供的证明材料内容必须真实可靠。

符合上述条件的投标人即为合格投标人，具有参与公开招标的资格。

3. 保密

参与招标投标活动的当事人应对招标文件和投标文件中的商业和技术等秘密保密，违者应对由此造成的后果承担法律责任。

4. 语言文字、计量单位、时间单位、投标有效期以及投标费用

4.1 语言文字

除专用术语外，与招标投标活动有关的语言均使用简体中文。必要时专用术语应附有中文注释。如投标人提交的支持文件和印刷的文献使用另一种语言，应附有相应内容的中文翻译本，在解释投标文件时以中文翻译本为准。

4.2 计量单位

除招标文件另有规定外，计量均应采用中华人民共和国法定计量单位；所有报价一律使用人民币，货币单位为“元”。

4.3 时间单位

除招标文件中另有规定外，招标文件所使用的时间单位“天”、“日”均指日历天，时、分均为北京时间。

4.4 投标有效期

4.4.1 在投标人须知前附表规定的投标有效期内，投标文件以及其补充、承诺等部分均保持有效。

4.4.2 在招标文件规定的投标文件有效期满之前，如果出现特殊情况，采购人或者采购代理机构可在投标有效期内要求投标人延长有效期，要求与答复均以书面通知为准并作为招标文件和投标文件的组成部分；投标人可以拒绝上述要求而其投标保证金不被没收，拒绝延长投标文件有效期的，其投标失效；同意上述要求的，既不能要求也不允许其修改投标文件，有关退还和没收投标保证金的规定在投标有效期的延长期内继续有效。

4.4.3 投标有效期内投标人撤销投标文件的或开标时因投标人原因操作投标文件未解密的，采购人或者采购代理机构可以不退还投标保证金。

4.5 投标费用

投标人应自行承担其准备和参加投标活动发生的所有费用。

5.踏勘现场

5.1 踏勘现场：详见第二章投标人须知。

5.2 采购人向投标人提供的有关现场的资料和数据，是采购人现有的能使投标人利用的资料，采购人对投标人由此而做出的推论、理解和结论不负责任。

5.3 投标人可自行踏勘现场，但不得因此使采购人承担有关责任和蒙受损失。除采购人原因外，投标人应对踏勘现场而造成的死亡、人身伤害、财产损失、损害以及其它任何损失、损害和引起的费用和开支承担责任。

6.询问及答复

6.1 投标人对招标投标活动事项有疑问的，可以向采购代理机构提出询问；采购代理机构应当及时作出答复，但答复的内容不得涉及商业秘密。

6.2 询问在本项目的公告页面在线提交。

6.3 询问及答复的内容在本项目的公告页面查看。

7.偏离

采购人允许投标文件偏离招标文件某些非实质性要求的，偏离应当符合招标文件规定的偏离范围和幅度。

8.履约担保

8.1 在签订合同前，中标人应按照有关规定或者事先经过采购人书面认可的履约担保要求向采购人提交履约担保。除另有规定外，履约担保金额不超过中标合同金额的10%。

8.2 中标人未按照要求提交履约担保的，视为放弃中标，其投标保证金不予退还，给采购人造成的损失超过投标保证金的，中标人应当对超过部分予以赔偿。

9.采购代理服务费

见投标人须知前附表

10.招标文件

10.1 招标文件的组成

10.1.1 招标文件是用以阐明所需货物以及服务、招标程序和合同格式的规范性文件。招标文件主要由以下部分组成：

（1）招标公告；

（2）投标人须知前附表；

（3）投标人应当提交的资格、资信等证明文件；

（4）采购需求；

（5）评标办法；

（6）投标人须知；

（7）开标、资格审查、评标、定标；

（8）纪律和监督；

（9）签订合同、合同主要条款；

（10）投标文件格式；

（11）投标人须知前附表规定的其他材料。

10.1.2 根据本章第 10.2 款对采购文件所作的澄清和修改，构成采购文件的组成部分。

10.1.3 除非有特殊要求，招标文件不单独提供项目所在地的自然环境、气候条件、公用设施等情况，投标人被视为熟悉上述与履行合同有关的一切情况。

10.2 招标文件的澄清和修改

招标文件的澄清和修改及投标人确认，详见投标人须知前附表。

招标文件的澄清或者修改在同一内容的表述上不一致时，以最后发出的公告为准。

11. 投标文件的组成

11.1 投标人应按照招标文件的要求编制投标文件，并保证其真实性、准确性以及完整性，按照招标文件要求提交全部资料并做出实质性响应。

11.2 投标文件由商务文件、技术文件组成：

11.3 商务文件

11.3.1 投标函；

11.3.2 必须提交的资格资信证明材料；

11.3.3 法定代表人身份证明；

11.3.4 法定代表人授权委托书；

11.3.5 投标报价：

（1）报价一览表。是分项报价明细表的汇总表，投标报价（即投标报价总计金额）为各个分项报价金额之和。报价项不得空缺、删除或修改，也不可用“……”“--”“免费”“无”及“已包含在总价中”等表示。

（2）分项报价明细表。各分项报价小计名称应当与《报价一览表》中费用名称、金额对应，投标人应当对分项报价明细表中各分项逐一报价，无此项报价的不得删除、修改报价项，可用阿拉伯数字“0.00”表示，投标人认为《分项报价明细表》有漏项

的，可以增加分项报价。

（3）报价需要说明的其他文件、材料。投标人认为需要对《报价一览表》、《分项报价明细表》中有关报价进一步说明或者证明其报价的文件和材料等。

11.3.6 投标人同类项目实施情况一览表（若有）；

11.3.7 资格、资信证明文件；

11.3.8 商务响应表；

11.3.9 联合投标协议书（若有）；

11.3.10 联合投标授权委托书（若有）；

11.3.11 残疾人福利性单位声明函（若有）；

11.3.12 中小企业声明函（若有）；

11.3.13 节能、环保等的资质证书或者文件（若有）；

11.3.14 招标文件商务评标办法中要求提交的相关证明材料（若有）；

11.3.15 投标人认为应介绍或者提交的资料和文件（若有）。

11.4 技术文件

11.4.1 货物清单（包括产品彩页）；

11.4.2 技术响应表；

11.4.3 选配件、专用耗材、售后服务优惠表（若有）；

11.4.4 项目实施人员（主要从业人员以及其技术资格）一览表；

11.4.5 符合招标文件规定的技术资料：

（1）投标人应提交招标文件规定的有效技术（印刷体）支持资料，并作为投标文件的一部分。技术支持资料以制造商（或代理商）公开发布的印刷资料或者检测机构出具的检测报告为准。若制造商公开发布的印刷资料与检测机构出具的检测报告不一致，以检测机构出具的检测报告为准。

（2）证明货物和服务与招标文件要求相一致的文件可以是文字资料、图纸和数据，主要包括内容：

（2.1）技术方案；

（2.2）货物主要技术指标和性能的详细说明，并保证所供货物必须是全新的、未使用过的合格产品；

（2.3）保证货物在正常使用所需要的备品备件和专用工具清单以及其货源地与价格；

（2.4）对照招标文件技术规格、参数以及要求，逐条说明所提供货物与服务是否

做出了实质性响应，并按照招标文件中技术响应表和资信以及商务响应表如实填写具体响应的参数以及要求。采购人只接受相同或者优于技术条款中所规定的技术要求以及制造标准。

（2.5）当招标文件中的技术要求以及货物备品备件的互换性标准与国家标准或者行业标准等不一致时，应以国家标准或者行业标准等为准。

（3）投标人在详细阐述货物的主要技术指标和性能说明时，应注意招标文件第四章“采购需求”中的工艺、材料、货物标准和参照品牌以及文字说明，并无任何限制性，投标人可选用替代标准、品牌或者文字叙述，但这些替代要实质上满足技术规格、参数以及要求。

（4）如果采购人全部或者部分使用非中标人投标文件中的技术成果或者技术方案时，应书面征得其同意并给予一定的经济补偿后，方可使用。

（5）投标人必须对所提供货物和服务等知识产权方面的一切产权关系负全部责任，由此而引起的法律纠纷以及费用投标人须全部承担。

11.4.6 招标文件技术评标办法中要求提交的相关证明材料；

11.4.7 投标人认为应介绍或者提交的资料和文件。

12. 投标报价

12.1 投标报价的范围：见投标人须知前附表。

12.2 投标人应对所投包中的货物进行报价，对每一包货物的报价必须全部报齐。

12.3 投标报价的次数：见投标人须知前附表。

12.4 投标人不得以任何方式或者方法提供投标以外的任何附赠条款。

12.5 投标人应按照招标文件中要求的内容填写报价，并由法定代表人或者授权代表签署。

12.6 投标人须按照附件格式表中的各单项明细逐项填写，以方便评标委员会对各投标文件进行比较。

12.7 投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

（一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

（二）大写金额和小写金额不一致的，以大写金额为准；

（三）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

（四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

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

12.8 唱标时，采购代理机构只对按照招标文件要求编制的投标报价进行唱标。

12.9 投标人的中标价格在合同执行中是固定不变的，不得以任何理由予以变更，不得出现任何包含价格调整的要求。

12.10 采购人不接受未经中国海关报验放进入中国境内且产自关境外的货物报价。

12.11 投标人须知前附表未规定可以采购进口产品的，不允许进口产品参加投标。

13. 投标文件编制要求

13.1 投标文件应按所投包分别进行编制。

13.2 投标文件编制：见投标人须知前附表。

13.3 投标文件签章：见投标人须知前附表。

13.4 投标人可对供货现场以及其范围环境进行考察，以获取有关编制投标文件和签署实施合同所需的各项资料，投标人应承担现场考察的费用、责任和风险。

13.5 投标人编制投标文件时，应当如实在技术响应表和商务响应表中填写响应情况。

14. 投标文件的修改、撤回与撤销

14.1 投标人在招标文件要求提交投标文件截止时间前，可以修改或者撤回已上传的投标文件。

14.2 在提交投标文件截止时间后到招标文件规定的投标有效期终止之前，投标人不得补充、修改或者撤销其投标文件。投标人撤销投标文件的，采购人可以不退还投标保证金。

15. 投标文件加密、上传

见投标人须知前附表。

16. 投标文件的递交

16.1 投标人应在投标截止时间前递交投标文件。

16.2 投标人递交投标文件的要求： 投标人完成电子投标文件制作后，通过【青岛市公共资源投标文件制作工具】上传投标文件，系统即时向投标人发出上传回执通知。上传时间以上传回执通知载明的传输完成时间为准；逾期上传的投标文件，电子招标投标交易平台将予以拒收。

16.3 除投标人须知前附表另有规定外，不论招标过程和结果如何，投标人的投标文件均不退还。

17.投标保证金

17.1 投标保证金的交纳

17.1.1 投标保证金的交纳金额和形式：见投标人须知前附表。

17.1.2 投标保证金缴纳截止时间，同投标截止时间。

17.1.3 投标人为联合体的，联合体牵头人交纳的保证金对联合体各方均具有约束力。

17.2 投标保证金的退还

17.2.1 投标人在招标文件要求提交投标文件截止时间前撤回已提交的投标文件的，采购人或者采购代理机构自收到投标人书面撤回通知之日起5个工作日内，退还已收取的投标保证金，但因投标人自身原因导致无法及时退还的除外。

17.2.2 **未中标人的投标保证金于开标当天中标结果宣布后即可办理退款手续；中标人的投标保证金在签订合同经交易中心督查科备案并网上公示后即可办理退还手续，退还时提供合同原件2份（办理退还保证金时原账号退回，无需提供申请资料）。**17.3 投标保证金的不予退还

17.3.1 投标人有下列情形之一的，投标保证金将不予退还：

（1）提供的有关资料不真实或者提供虚假材料的；

（2）投标有效期内投标人撤销投标文件的；

（3）损害采购人或者采购代理机构合法权益的；

（4）投标人向采购代理机构、采购人、专家提供不正当利益的；

（5）经评标委员会认定有故意哄抬报价、串标或者其它违法行为的；

（6）中标人未按照招标文件规定签订合同或者未按照招标文件规定提供履约保证金的；

（7）法律、行政法规以及有关规定的其它情形。

17.3.2 不予退还的投标保证金应在规定时间内上缴国库。

18.质疑

18.1 **投标人对招标文件、踏勘现场有疑问需招标人答疑时，在全国公共资源交易平台（山东省•青岛市）青岛市公共资源交易电子服务系统（http://ggzy.qingdao.gov.cn）网站上提出质疑并采用信函或者直接送达的形式通知胶州市公共资源交易中心，并告知市公共资源交易中心工作人员（电话：82205638 联系人：李真）同时将电子版文件以电子邮件的形式发送至** lzzx1004@163.com**。招标人将对投标人提出的所有疑问进行综合答复，答疑内容应在招标文件规定范围内，不得对招标**

文件实质性条款进行改动，并形成书面文件报交易中心审查备案后，统一在全国公共资源交易平台（山东省•青岛市）青岛市公共资源交易电子服务系统（http://ggzy.qingdao.gov.cn）及胶州市公共资源交易网上公告。

潜在供应商已依法获取其可质疑的采购文件的，可以依法对该文件提出质疑。

18.2 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）对中标结果提出质疑的，为中标结果公告期限届满之日。

18.3 供应商应当在法定质疑期内一次性提出针对本项目同一采购程序环节的质疑。

18.4 质疑函内容应包括以下主要内容：

（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。否则采购人或者采购代理机构不予受理。

18.5 代理人提出质疑的，应当提交供应商签署的授权委托书。其授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。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、主要负责人签字或者盖章，并加盖公章。

18.6 采购人或者采购代理机构在收到质疑函后 7 个工作日内做出答复，并通过系统以电子文档形式通知质疑供应商和其他有关供应商，但答复不得涉及商业秘密。

19. 投诉

19.1 按照《中华人民共和国政府采购法》、财政部《政府采购质疑和投诉办法》（第 94 号令）以及相关的法律、法规及规定，质疑人对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内做出答复的，可以在答复期满后 15 个工作日内向同级监管部门提起投诉。投标人投诉按照采购人所属预算级次，由本级财政部门处理。

19.2 投诉人提起投诉应符合下列条件：

（一）提起投诉前已依法进行质疑；

（二）投诉书内容符合本办法的规定；

（三）在投诉有效期限内提起投诉；

（四）同一投诉事项未经财政部门投诉处理；

（五）财政部规定的其他条件。

投标人投诉的事项不得超出已质疑事项的范围，但基于质疑答复内容提出的投诉事项除外。以联合体形式参加政府采购活动的，其投诉应当由组成联合体的所有投标人共同提出。

19.3 投诉人投诉时,应当提交投诉书和必要的证明材料，并按照被投诉采购人、采购代理机构和与投诉事项有关的投标人数量提供投诉书的副本。

19.4 投诉书应当包括以下主要内容：

（一）投诉人和被投诉人的姓名或者名称、通讯地址、邮编、联系人及联系电话；

（二）质疑和质疑答复情况说明及相关证明材料；

（三）具体、明确的投诉事项和与投诉事项相关的投诉请求；

（四）事实依据；

（五）法律依据；

（六）提起投诉的日期。

投诉人为自然人的，应当由本人签字；投诉人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。

19.5 代理人提出投诉的，应当提交供应商签署的授权委托书。其授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。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、主要负责人签字或者盖章，并加盖公章。

19.6 投诉人在全国范围 12 个月内三次以上投诉查无实据的，由财政部门列入不良行为记录名单。

投诉人有下列行为之一的，属于虚假、恶意投诉，由财政部门列入不良行为记录名单，禁止其 1 至 3 年内参加政府采购活动：

（一）捏造事实；

（二）提供虚假材料；

（三）以非法手段取得证明材料。证据来源的合法性存在明显疑问，投诉人无法证明其取得方式合法的，视为以非法手段取得证明材料。

20.其他需补充的内容

其他需补充的内容：见投标人须知前附表。

第七章　开标、资格审查、评标、定标

1.开标程序

1.1 宣布开标纪律；

1.2 宣布主持人、唱标人、记录人等有关人员姓名；

1.3 查看在线签到家数，少于三家开标会结束；不少于三家开标会继续进行；

1.4 投标人根据要求在限定时间内通过电子招标投标交易平台对已上传的电子投标文件开始解密；因投标人原因造成投标文件未解密的，视为撤销其投标文件，采购人或者采购代理机构可以不退还投标保证金。

1.5 投标人授权代表在开标记录上确认；在规定时限内未确认的，视为默认开标结果；

1.6 开标结束。

2.开标

2.1 开标应当在招标文件确定的提交投标文件截止时间的同一时间通过电子招标投标交易平台公开进行。所有投标人须在开标前规定时间内签到。

2.2 开标由采购代理机构指定专人负责，开标记录由投标人线上确认。

2.3 投标人代表对开标过程和开标记录有疑义，以及认为采购人、采购代理机构相关工作人员有需要回避的情形的，应当场(在线)提出询问或者回避申请。采购人、采购代理机构对投标人代表提出的询问或者回避申请应当及时处理。投标人未参加开标的，视同认可开标结果。

2.4 投标人不足 3 家的，不得开标。

2.5 在评审结束前，投标单位请保持在线登录状态。评标过程中，如果评审委员会要求投标人对投标文件进行澄清，投标单位需要通过电子平台【专家问题澄清】功能，限时在线发送澄清。

2.6 各投标人的评审得分与排序将在电子招标投标交易平台告知。

3.评标委员会

3.1 评标委员会的组成

采购人按照《中华人民共和国政府采购法》以及有关规定组建评标委员会。评标由依法组建的评标委员会负责。评标委员会评标专家组成，成员人数为 5 人以上单数。

评审专家对本单位的采购项目只能作为采购人代表参与评标，采购人可以自行选定相应专业领域评审专家的规定情形除外。采购代理机构在职工作人员不得以评审专家身份参与政府采购项目评审活动。

3.2 评审专家的抽取

3.2.1 采用随机抽取方式从省级以上财政部门设立的政府采购评审专家库中抽取评审专家。任何单位和个人都不得指定评审专家或干预评审专家的抽取工作。

3.2.2 参加评审专家抽取的有关人员对被抽取的专家的姓名、单位和联系方式等内容负有保密的义务。评标委员会成员的名单在中标结果确定前必须严格保密。

3.3 评审专家不得参加与自身存在利害关系的政府采购项目的评审及相关活动，与自己有利害关系的应当回避，已经进入的必须更换。

3.4 评标委员会负责对各投标文件进行评审、比较、评定，并按本招标文件的规定确定中标候选人名单，以及根据采购人委托直接确定中标人。

3.5 评标委员会具有依据招标文件进行独立评标的权力，且不受外界任何因素的干扰。评标委员会成员必须独立、负责地提出评审意见，并对自己的评审意见承担责任。对评标结果有不同意见的评标委员会成员应当以书面形式说明其不同意见和理由，评标报告应当注明不同意见。评审委员会成员拒绝评审或者拒绝在评标报告上签字并且又不书面说明其不同意见和理由的，视为同意评标结果。

3.6 评标委员会的职责：

3.6.1 审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；

3.6.2 要求投标人对投标文件有关事项作出澄清或者说明；

3.6.3 对投标文件进行比较和评价；

3.6.4 确定中标候选人名单，以及根据采购人委托直接确定中标人；

3.6.5 向采购人、采购代理机构或者有关部门报告评标中发现的违法行为。

3.7 评标委员会的义务：

3.7.1 遵纪守法，客观、公正、廉洁地履行职责；

3.7.2 提出真实、可靠的评审意见；

3.7.3 严格遵守评标纪律，不得向外界泄露评标情况；

3.7.4 发现投标人在招投标活动中有不正当竞争或者恶意串通等违规行为，应及时向监督部门报告并加以制止；

3.7.5 按照招标文件规定的评标方法和评标标准进行评标，对评标意见承担个人责任；

3.7.6 编写评标报告；

3.7.7 配合采购人或者采购代理机构答复投标人提出的质疑；

3.7.8 对评标过程和结果，以及采购人、投标人的商业秘密保密；

3.7.9 配合监管部门处理投诉；

3.8 评标委员会成员有下列情形之一的，应当回避：

3.8.1 投标人或者投标人主要负责人的近亲属；

3.8.2 各级财政部门政府采购监督管理在职工作人员；

3.8.3 参加过采购项目前期咨询论证的；

3.8.4 与自身存在利害关系的政府采购项目；

3.8.5 曾因在招标、评标以及其他与招标投标有关系活动中从事违法行为而受到行政处罚或者刑事处罚的；

3.9 评标中因评标委员会成员缺席、回避或者健康等特殊原因导致评标委员会组成不符合本办法规定的，采购人或者采购代理机构应当依法补足后继续评标。被更换的评标委员会成员所作出的评标意见无效。

无法及时补足评标委员会成员的，采购人或者采购代理机构应当停止评标活动，封存所有投标文件和开标、评标资料，依法重新组建评标委员会进行评标。原评标委员会所作出的评标意见无效。

采购人或者采购代理机构应当将变更、重新组建评标委员会的情况予以记录，并随采购文件一并存档。

4.资格审查、评标程序

4.1 资格审查

4.2 宣布评标纪律以及回避提示；

4.3 组织推荐评标委员会组长；

4.4 符合性审查；

4.5 技术和商务评审；

4.6 澄清有关问题；

4.7 比较与评价；

4.8 确定中标人或者推荐中标候选人名单；

4.9 编写评标报告；

4.10 宣布评标结果。

5.资格审查

5.1 评标委员会和采购人或采购代理机构依法对投标人的资格进行审查，以确定其是否符合招标文件的资格要求。未按招标文件第三章要求提供资格证明文件的，属于不合格投标人。

5.2 采购人、采购代理机构通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）、信用山东(www.creditsd.gov.cn)及信用青岛（credit.qingdao.gov.cn）查询投标人信用记录，查询时要将查询网页、内容进行截图或拍照，以作证据留存，截图或拍照内容要完整清晰，应包括网站网址、查询内容、电脑截屏时

间。采购人或者采购代理机构应当对投标人信用记录进行甄别，对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的投标人，应当拒绝其参加政府采购活动，其投标无效；两个以上的自然人、法人或者其他组织组成一个联合体，以一个投标人的身份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录，其投标无效。

信用信息查询记录及相关证据应当与其他采购文件一并保存。

5.3 在资格性审查时，评标委员会和采购人或采购代理机构按照投标人提供的《在经营活动中无重大违法记录和行贿犯罪记录的承诺》审查投标人及其法定代表人和项目负责人行贿犯罪情况；在发放中标通知书前，采购人、采购代理机构应通过中国裁判文书网（http://wenshu.court.gov.cn）核实中标供应商的行贿犯罪情况，并截图或拍照以作证据留存。

5.4 在资格性审查时，对属于不合格投标人，采购人或者采购代理机构必须提出不合格的事实依据并出具不合格说明。

6. 评标

6.1 采购人或者采购代理机构负责组织评标工作，并履行下列职责：

6.1.1 核对评审专家身份和采购人代表授权函，对评审专家在政府采购活动中的职责履行情况予以记录，并及时将有关违法违规行为向财政部门报告；

6.1.2 宣布评标纪律；

6.1.3 公布投标人名单，告知评审专家应当回避的情形；

6.1.4 组织评标委员会推选评标组长，采购人代表不得担任组长；

6.1.5 在评标期间采取必要的通讯管理措施，保证评标活动不受外界干扰；

6.1.6 根据评标委员会的要求介绍政府采购相关政策法规、招标文件；

6.1.7 维护评标秩序，监督评标委员会依照招标文件规定的评标程序、方法和标准进行独立评审，及时制止和纠正采购人代表、评审专家的倾向性言论或者违法违规行为；

6.1.8 核对评标结果，有以下情形的，要求评标委员会复核或者书面说明理由，评标委员会拒绝的，应予记录并向本级财政部门报告；

6.1.8.1 分值汇总计算错误的；

6.1.8.2 分项评分超出评分标准范围的；

6.1.8.3 评标委员会成员对客观评审因素评分不一致的；

6.1.8.4 经评标委员会认定评分畸高、畸低的。

6.1.9 评审工作完成后，按照规定向评审专家支付劳务报酬和异地评审差旅费，不得向评审专家以外的其他人员支付评审劳务报酬；

6.1.10 处理与评标有关的其他事项。

采购人可以在评标前说明项目背景和采购需求，说明内容不得含有歧视性、倾向性意见，不得超出招标文件所述范围。说明应当提交书面材料，并随采购文件一并存档。

6.2 符合性审查

评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。

在符合性审查时，对属于投标无效的投标人，评标委员会必须提出投标无效的事实依据，并出具投标无效说明。

6.3 技术和商务评审

6.3.1 评标委员会按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估（包括政府采购政策执行），综合比较与评价。

6.3.2 采用综合评分法的，评标委员会各成员应当独立对每个投标人的投标文件进行评价，并汇总每个投标人的得分。

6.3.3 评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的，应当停止评标工作，与采购人或者采购代理机构沟通并作书面记录。采购人或者采购代理机构确认后，应当修改招标文件，重新组织采购活动。

6.3.4 采用最低评标价法的采购项目，提供相同品牌产品（非单一产品采购项目，系指采购人确定的核心产品）的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会采取随机抽取的方式确定一个参加评标的投标人，其他投标无效。

6.3.5 使用综合评分法的采购项目，提供相同品牌产品（非单一产品采购项目，系指采购人确定的核心产品）且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会采取随机抽取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。

7.澄清有关问题

7.1 对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应以书面形式要求投标人做出必要的澄清、说明或者补正。投标人的澄清、说明或者补正应采取书面形式，由法定代表人或者授权代表签字或盖章。投标人的澄清、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。

7.2 评标委员会判断投标文件的响应性仅基于投标文件本身而不靠外部因素。未响应实质性条款的，评标委员会有权确定其投标无效，投标人不能通过修正、撤销或者澄清不符之

处而使其投标成为实质性响应的投标。

7.3 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，有可能影响产品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；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。

8.定标

8.1 评标委员会根据投标人须知前附表的规定确定中标候选人或直接确定中标人。

评标委员会确定中标候选人的，中标候选人数见投标人须知前附表。采购人应当自收到评标报告之日起5个工作日内，在评标报告确定的中标候选人名单中按顺序确定中标人。中标候选人并列的，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中标人；招标文件未规定的，采取随机抽取的方式确定。

8.2 本次招标评标办法：见投标人须知前附表。

8.3 采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

8.4 采用最低评标价法的，评标结果按投标报价由低到高顺序排列，投标报价相同的并列。投标文件满足招标文件全部实质性要求且投标报价最低的投标人为排名第一的中标候选人。

8.5 按照有关规定中标人因不可抗力或者自身原因不能履行政府采购合同的，报经同级财政部门同意后，可顺延排序第二的投标人中标；或者报同级财政部门同意后，做废标处理，由采购人依法重新组织招标。

8.6 以入围方式确定多个中标人的，入围中标人数量应当根据招标需要并在招标活动开始前确定，由评标委员会按照招标文件规定的评标办法确定各投标人排列顺序，依照顺序确定入围中标人。

8.7 评标委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。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及理由，否则视为同意评标报告。

8.8 评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

（一）分值汇总计算错误的；

（二）分项评分超出评分标准范围的；

（三）评标委员会成员对客观评审因素评分不一致的；

（四）经评标委员会认定评分畸高、畸低的。

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

8.9 评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告。

9. 中标公告以及中标通知书

9.1 评标结束后，不再现场宣布评标结果。采购人或者采购代理机构应当自中标人确定之日起 2 个工作日内，发出中标通知书，并在全国公共资源交易平台（山东省•青岛市）青岛市公共资源交易电子服务系统和青岛市政府采购网公告中标结果（公告期限为 1 个工作日），招标文件随中标结果同时公告；采用综合评分法评审的，还应当告知未中标人本人的评审得分与排序。

9.2 采购人或采购代理机构不按照规定发布中标公告或者发布中标公告后不签发中标通知书的，应当承担法律责任，给中标人造成经济损失的应承担赔偿责任。

9.3 中标通知书对采购人和中标人都具有法律效力。中标通知书发出后，采购人改变中标结果的，或者中标人放弃中标，应当依法承担法律责任。

10. 不合格投标人或投标无效

出现下列情形之一的，为不合格投标人或投标无效：

10.1 报价超过招标文件中规定的预算金额或者最高限价的；

10.2 对“★”条款未做出实质性响应或者发生负偏离的；

10.3 应提供而未提供带“▲”标注的政府强制采购节能、环保产品的；

10.4 对于不允许偏离的实质性要求和条件发生偏离的；

10.5 不按照招标文件规定报价、没有分项报价、拒绝报价、有多个报价（招标文件另有规定的除外）、有选择性报价、附有条件的报价或者拒绝修正报价的；

10.6 未按照招标文件的规定提交投标保证金的；

10.7 投标有效期不满足招标文件要求的；

10.8 投标超出营业执照经营范围的；

10.9 评标委员会判定投标人涂改证明材料或者提供虚假材料和承诺的；

10.10 投标文件未按招标文件要求编制、签署、盖章的；

10.11 投标文件含有采购人不能接受的附加条件的；

10.12 法律、法规和招标文件规定的其他无效情形。

对投标无效的认定，必须经评标委员会集体做出决定并出具投标无效的事实依据。

11. 废标

11.1 出现下列情形之一的，应予废标：

11.1.1 在投标截止时间后参加投标的投标人不足 3 家或者通过资格审查或符合性审查的投标人不足 3 家的；

11.1.2 出现影响采购公正的违法违规行为的；

11.1.3 投标人的报价均超过预算金额或者最高限价的；

11.1.4 因重大变故，采购任务取消的；

11.1.5 法律、法规以及招标文件规定的其他废标情形。

11.2 废标后，采购人或者采购代理机构应当将废标理由通知所有投标人。

12. 特殊情况处置程序

12.1 评标委员会成员的更换

12.1.1 评标委员会应当执行连续评标的原则，按照招标文件规定的程序、内容、方法、标准完成全部评标工作。出现评审专家临时缺席、回避等情形导致评审现场专家数量不符合法定标准的，采购人或者采购代理机构要按照有关程序及时补抽专家，继续组织评审。如无法及时补齐专家，则要立即停止评审工作，封存招标文件和所有投标文件，择期重新组建评标委员会进行评审。

12.1.2 退出评标委员会的成员，其已完成的评审行为无效。由采购人向监督人员提出更换评标委员会成员意见并获准后，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。

12.2 记名投票

在评标过程中，评标委员会发生分歧或者评审结论有异议需表决的，按照少数服从多数的原则，由评标委员会全体成员以记名投票方式表决。

13. 违法违规情形

13.1 有下列情形之一的，属于投标人相互串通投标：

13.1.1 投标人之间协商投标报价等投标文件的实质性内容；

13.1.2 投标人之间约定中标人；

13.1.3 投标人之间约定部分投标人放弃投标或者中标；

13.1.4 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；

13.1.5 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。

13.2 有下列情形之一的，视为投标人相互串通投标，评标委员会应当出具违法违规认定意见并作投标无效处理：

13.2.1 不同投标人的投标文件由同一单位或者个人编制；

13.2.2 不同投标人委托同一单位或者个人办理投标事宜；

13.2.3 不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

13.2.4 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；

13.2.5 不同投标人的投标文件相互混装；

13.2.6 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。

13.3 有下列情形之一的，属于采购人与投标人串通投标：

13.3.1 采购人在开标前开启投标文件并将有关信息泄露给其他投标人；

13.3.2 采购人直接或者间接向投标人泄露标底、评标委员会成员等信息；

13.3.3 采购人明示或者暗示投标人压低或者抬高投标报价；

13.3.4 采购人授意投标人撤换、修改投标文件；

13.3.5 采购人明示或者暗示投标人为特定投标人中标提供方便；

13.3.6 采购人与投标人为谋求特定投标人中标而采取的其他串通行为。

在评标过程中发现投标人有上述情形的，评标委员会应当认定其投标无效，并书面报告本级财政部门。

14.违规处理

投标人有下列情形之一的，列入不良行为记录名单，在一至三年内禁止参加青岛市政府采购活动：

14.1 提供虚假投标材料谋取中标、成交的；

14.2 采取不正当手段诋毁、排挤其他投标人的；

14.3 与采购人、其他投标人或者采购代理机构恶意串通的；

14.4 向采购人、采购代理机构行贿或者提供其他不正当利益的；

14.5 在招标采购过程中与采购人进行协商谈判的；

14.6 拒绝有关部门监督检查或者提供虚假情况的；

14.7 一年内累计三次以上投诉均查无实据，并带有明显故意行为的；

14.8 捏造事实或者提供虚假投诉材料的；

14.9 不按照规定程序以及正常途径质疑、投诉，采用匿名信、匿名电话、发短信息等手段，威胁、恫吓、辱骂、恶意中伤其他相关当事人的；

14.10 法律、法规和招标文件中规定的其他情形。

第八章 纪律要求

1. 对采购人的纪律要求

采购人应当按照行政事业单位内部控制规范要求，建立健全本单位政府采购内部控制制度，在编制政府采购预算和实施计划、确定采购需求、组织采购活动、履约验收、答复询问质疑、配合投诉处理及监督检查等重点环节加强内部控制管理。

采购人不得向投标人索要或者接受其给予的赠品、回扣或者与采购无关的其他商品、服务。

2. 对投标人的纪律要求

投标人应当遵循公平竞争的原则，不得恶意串通，不得妨碍其他投标人的竞争行为，不得损害采购人或者其他投标人的合法权益。

3. 对评标委员会成员的纪律要求

评标委员会及其成员不得有下列行为：

（一）确定参与评标至评标结束前私自接触投标人；

（二）接受投标人提出的与投标文件不一致的澄清或者说明，法律规定允许澄清或说明的情形除外；

（三）违反评标纪律发表倾向性意见或者征询采购人的倾向性意见；

（四）对需要专业判断的主观评审因素协商评分；

（五）在评标过程中擅离职守，影响评标程序正常进行的；

（六）记录、复制或者带走任何评标资料；

（七）其他不遵守评标纪律的行为。

评标委员会成员有前款第一至五项行为之一的，其评审意见无效，并不得获取评审劳务报酬和报销异地评审差旅费。

4. 对与评标活动有关的工作人员的纪律要求

与评标活动有关的工作人员不得收受他人的财物或者其他好处，不得向他人透漏对投标文件的评审和比较、中标候选人的确定情况以及评标有关的其他情况。在评标活动中，与评标活动有关的工作人员不得擅离职守，影响评标程序正常进行。

第九章　签订合同、合同主要条款

1. 签订合同

1.1 采购人应当自中标通知书发出之日起三十日内，按照招标文件和中标人投标文件的约定，与中标人签订书面合同。所签订合同不得对招标文件和中标人投标文件作实质性修改。

1.2 签订的合同原则以本章第 4 条的规定为基础，并根据评标、答疑情况进行修改补充，但该款并不限制采购人以其他方式签订合同的权利。采购人不得向中标人提出任何不合理的要求，作为签订合同的条件，不得与中标人私下订立背离合同实质性内容的协议。

1.3 招标文件、投标文件、书面承诺和中标通知书均作为经济合同的一部分，且具有法律效力。中标人应严格履行经济合同所规定的各项义务和责任，否则将依法处理。

1.4 有关法规或者招标文件明确不允许分包方式履行合同的，中标人不得分包履行合同，否则将依法承担法律责任。招标文件明确允许分包方式履行合同的，按照招标文件相关规定执行。

当中标人放弃中标结果或者因被质疑、投诉，经查属实或者因不可抗力而不能履行合同的，采购人可从推荐中标候选人名单中按顺序重新确定中标人，但应符合相关规定；否则采购人应重新组织招标。

1.5 采购人应当自采购合同签订之日起 7 个工作日内，将采购合同副本报同级财政部门和有关部门备案。

1.6 法律、行政法规规定应当办理批准、登记等手续后生效的合同，依照其规定。

2. 追加合同金额

政府采购合同履行中，采购人需要追加与合同标的相同的货物的，在不改变合同其他条款的前提下并且在签订合同后 1 年内，经采购人报同级财政部门批准后，可以与中标人协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的 10%，否则采购人应重新组织招标。

采购合同双方当事人不得擅自变更、中止或者终止合同。采购合同继续履行将损害国家利益和社会公共利益的，双方当事人应当变更、中止或者终止合同。有过错的一方应当承担赔偿责任，双方都有过错的，各自承担责任。

3. 货物质量与验收

3.1 招标文件中的货物按照国标、部标、行业标准或者双方技术协议或者招标文件、投标文件、书面承诺的技术要求制造。货到后，由采购人组织验收小组对货物进行验收（以《项目验收报告单》为准）。如对货物质量有争议，采购人可委托国家认定的相关部门对货物进行质量检验，并以质检部门出具的检验报告为准，并由责任方承担全部责任。

3.2 货物制造完毕经出厂检验合格后方能发货，并提供货物合格证书。

3.3 货物的表面涂漆颜色：由采购人和中标人商定。

3.4 货物包装按照国标、部标以及有关标准执行。

4.合同主要条款

合同编号：_____

签 订 地：_____

甲方（采购人）：_____

住所地：_____

乙方（中标人）：_____

住 所 地：_____

乙方于20___年___月___日参加了__（采购代理机构）__组织的“__（项目名称及项目编号）__”政府采购活动，经评标委员会评审确定乙方为__（包及包名称）__中标人，按照《中华人民共和国合同法》、《中华人民共和国政府采购法》和相关的法律法规规定，以及招标文件规定，经甲乙双方协商一致，签订本政府采购合同。

第一条 货物条款

乙方向甲方提供以下货物

货物名称	品牌、规格型号（技术参数）	单价	数量	小 计
合 计				

注：如上述表格不适用相关货物的，具体品牌、数量、规格型号（技术参数）及质保期等可用附件形式列明，作为本合同组成部分。

……

第二条 合同总金额

合同总金额为人民币（大写）：_____（￥_____）

此价格为合同执行不变价，不因国家政策变化而变化，该价款包括了货物及与之配套的设计、制造、正版软件、检验、包装、运输、保险、税费以及安装、组织验收、培训、技术服务（包括技术资料、图纸提供等）、质保期服务等全部价款，除此之外，甲方不再向乙方支付其他任何费用。

……

第三条　质量要求及技术标准

1.货物原产地：

2.货物的质量要求：

……

3.货物的技术标准：

……

第四条　交货

1.交货日期：

2.交货地点：

……

第五条　包装、装运及运输

1.乙方负责包装、装运和运输，由于不适当的包装、装运和运输造成货物有任何损坏均由乙方负责。

2.包装费、运费及相关费用已包含在合同总金额内。

……

第六条　货款支付

1.货物运到交货地点，经甲乙双方共同验收合格后由甲方负责办理货款支付手续。

2.属国库集中支付资金，甲方应按照双方约定的付款期限，及时向同级财政部门报送资金支付申请，同级财政部门对支付申请审核无误后，将货款直接支付至乙方账户。

3.付款方式

可采用一次性付款方式，也可以采用分期付款方式，具体由甲乙双方协商约定。采用一次性付款方式的，应约定支付的时间；采用分期付款方式的，应约定首付、分期支付的时间、条件及支付资金的比例；甲方根据采购货物的具体情况确定是否预留质保金。首付款比例原则上不低于合同总金额的30%，验收合格后付至____%，质保金的比例原则上不得超过10%。

……

第七条　履约保证金

1.乙方须向甲方交纳人民币(大写)_____（￥_____） 作为本合同的履约保证金。

2.履约保证金用于补偿甲方因乙方不能履行或不能完全履行合同义务而蒙受的损失。

3.履约保证金在货物交付验收合格_____月无质量问题后，填写《青岛市政府采购项目履

约保证金退付表》、《青岛市政府采购项目验收单》和资金往来收款收据交监督部门审核后20个工作日内退还。

……

第八条　售后服务及承诺

1.乙方有完善的服务体系，有能力提供持续的、本地化售后服务。

2.乙方负责系统安装和调试以及操作人员培训，并制定详细的培训计划，使操作人员能独立进行管理、操作、维护和故障处理等工作，做好相关记录及技术文档收集整理，待验收合格后移交给甲方。

3.供货及服务范围：乙方负责货物的供应、运输、安装调试、免费培训、售后服务。

……

第九条　验收

1.货物运抵现场后，采购人将对货物数量、质量、规格等进行检验。如发现货物和规格或者两者都与合同不符，采购人有权限根据检验结果要求中标人立即更换或者提出索赔要求。

2.开箱检查设备外观，如有损伤或质量缺陷，乙方应及时更换。

3.依据合同设备清单，对设备品牌、规格型号（技术参数）、数量、质保书等必备附件进行检查。

4.货物由中标人进行安装，完毕后，采购人应对货物的数量、质量、规格、性能等进行详细而全面的检验。安装调试完毕___日内，证明货物以及安装质量无任何问题，甲乙双方共同确认设备正常运行后，由采购人组成的验收小组签署验收报告，作为付款凭据之一。

……

第十条　知识产权

1.乙方保证，甲方在使用该货物或者货物的任何一部分时，免受第三方提出的侵犯其专利权、商标权或其他知识产权的起诉。如发生此类纠纷，由乙方承担一切责任；如因此给甲方造成损失的，乙方负责全额赔偿。

2.乙方为执行本合同而提供的技术资料或者其他相关资料、软件等由甲方永久免费使用。

……

第十一条　甲方责任

1.及时办理付款手续。

2.负责提供工作场地，协助乙方办理有关事宜。

3.对合同条款及所知悉的乙方商业秘密负有保密义务。

……

第十二条　乙方责任

1.保证所供货物均为投标文件承诺的货物，符合相关质量检测标准，具有该产品的出厂标准或国家鉴定证书,保证其全部部件为全新的未使用的且符合相关质量要求。

2.保证货物的售后服务，严格依据投标文件及相关承诺，对货物及系统进行保修、维护等服务。

3.保证其所供货物不存在侵犯第三方知识产权的行为，否则由此产生的损失由乙方承担。

……

第十三条　违约责任

1.甲乙双方任意一方无故终止合同的，违约方应当按照合同总金额的20%向守约方支付违约金。

2.乙方逾期交付货物时，每逾1日乙方向甲方支付合同总金额0.5‰的滞纳金。逾期交货超过30日的，甲方有权决定是否继续履行合同，如甲方决定终止履行合同的，乙方应按照第1款的规定赔偿甲方违约金。

3.乙方所供货物品牌、规格型号、质量等不符合合同约定标准，甲方有权拒收，以及甲方收货后，发现产品出现质量问题不能使用的，甲方有权终止合同，同时，乙方向甲方支付合同总金额20%的违约金，如果违约金不足以支付甲方所受损失的，甲方有权要求其赔偿。

4.在质保期内产品出现质量问题，乙方必须在接到甲方通知后___小时内到达现场解决，否则甲方有权另请单位解决，由此产生的费用由乙方承担，甲方有权从质保金中扣除相关费用，产生的损失由乙方赔偿。

5.甲乙双方违背其他合同条款，违约方赔偿对方损失。

……

第十四条　不可抗力

甲乙双方的任何一方由于不可抗力不能履行合同时，应当及时通知对方不能履行或不能完全履行的情况和理由；在取得有关主管机关证明后，允许延期履行、部分履行或者终止履行合同的，根据情况可部分或全部免予承担违约责任。

……

第十五条　保密

乙方在合同履行期间知悉甲方的工作秘密（包括相关业务信息），不得透露或以其他方式提供给合同双方以外的其他方（包括乙方内部与本合同无关的任何人员），乙方的保密责任不因本合同的终止而终止。

乙方违反本合同所规定的保密义务，应按照本合同总金额的10%支付违约金。

……

第十六条　争议解决

甲乙双方在合同履行中发生争议，应通过协商解决。如协商不成，可以向合同签订地法院提起诉讼。

……

第十七条　合同生效及其它

1.除招标文件规定且甲方事先书面同意外，乙方不得部分或者全部转让、分包履行其应履行的合同项下的义务。

2.合同由甲、乙双方法定代表人（或者授权代表）签字并加盖单位公章，以最后一方签字日期为合同生效日期。

3.本合同一式六份，甲方一份，乙方一份，采购代理机构二份，市财政局一份，市公共资源交易管理办公室一份。

……

第十八条　本合同附件

1.中标通知书；

2.政府采购招标文件（含招标文件的澄清、修改等）；

3.乙方投标文件；

4.中标人在评标过程中做出的有关澄清、说明、承诺或者补正文件（材料）；

……

甲　　方：	乙　　方：
单位名称(公章)：	单位名称(公章)：
法定代表人（授权代表）签字：	法定代表人（授权代表）签字：
电　　话：	电　　话：
年　月　日	年　月　日

第十章　投标文件格式

投标文件

包：第　包

商务部分

项目名称：

项目编号：

投标单位名称（公章）：

二〇　　年　月　日

商务文件目录

1、投标函(见附件1)；

2、在经营活动中无重大违法记录和行贿犯罪记录的承诺(见附件2)；

3、法定代表人身份证明(见附件3)；

4、法定代表人授权委托书(见附件4)；

5、报价一览表(见附件5)；

6、分项报价明细表(见附件 6)；

7、资格、资信证明材料；

8、投标人情况介绍（主要产品、技术力量、生产规模、经营业绩等)；

9、投标人同类项目实施情况一览表(见附件7)（若有)；

10、类似成功案例业绩证明（投标人同类项目中标通知书、合同、验收报告)（若有)；

11、商务响应表(见附件8)；

12、联合投标协议书（若有）(见附件9)；

13、联合投标授权委托书（若有）(见附件10)；

14、残疾人福利性单位声明函（若有）(见附件11)；

15、中小企业声明函（若有）(见附件12)；

16、节能、环保等的资质证书或者文件（若有)；

17、招标文件商务评标办法中要求提交的相关证明材料（若有)；

18、招标文件其它规定或者投标人认为应介绍或者提交的资料、文件和说明（若有)。

附件1：

投标函

（采购代理机构）：

（投标人名称）系中华人民共和国合法企业，经营地址_____。

我（姓名）系（投标人名称）的法定代表人，我方愿意参加贵方组织的（招标项目名称）（编号为_____）的投标，为此，我方就本次投标有关事项郑重声明如下：

1、我方已详细审查全部招标文件，同意招标文件的各项要求。

2、我方向贵方提交的所有投标文件、资料都是准确的和真实的。

3、若中标，我方将按照招标文件规定履行合同责任和义务。

4、我方不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司以及其附属机构没有任何联系。

5、投标文件自开标日起有效期为90日历日。

6、以上事项如有虚假或者隐瞒，我方愿意承担一切后果。

投标人名称（公章）：

投标人法定代表人或者授权代表（印章）：

日　　期：_____年___月___日

备注：本投标函由授权代表印章的，应附法定代表人印章的授权委托书。

附件 2：

在经营活动中无重大违法记录和行贿犯罪记录的承诺

我方在参加_____（项目名称）政府采购活动前 3 年内，我方被公开披露或查处的违法违规行为有：_____，但在经营活动中：

1、没有重大违法记录（重大违法记录指投标人因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚）。

2、没有行贿犯罪记录（查询内容：①投标人_____、组织机构代码证或统一社会信用代码_____ ；②法定代表人_____、身份证号码_____ ；③项目负责人_____、身份证号码_____ ）。

以上承诺若与实际情况不符，我方自愿承担一切法律后果。

投　标　人：_____（公章）

日　　期：_____年___月___日

备注：1.投标人没有被公开披露或查处违法违规行为的，注明“无”即可。

2.采购文件未要求项目负责人的，项目负责人一栏可删除。

附件3：

法定代表人身份证明

投标人名称：_____

单位性质：_____

地址：_____

成立时间：_____年_____月_____日

经营期限：_____

姓名：_____ 性别：_____ 年龄：_____职务：_____

系_____（投标人名称）的法定代表人。

特此证明。

附：法定代表人身份证复印件。

附件4：

法定代表人授权委托书

（采购代理机构）：

我（姓名）系（投标人名称）法定代表人，现授权委托我公司的（姓名）为我公司本次项目的授权代表，代表我方办理本次投标、签约等相关事宜，签署全部有关的文件、协议、合同并具有法律效力。授权代表联系方式_____。

在我方未发出撤销授权委托书的书面通知以前，本授权委托书一直有效。授权人（代表）签署的所有文件（在授权书有效期内签署的）不因授权撤销而失效。

授权代表无权转让委托权。特此授权。

本授权委托书于_____年_____月_____日签字生效,特此声明。

(附法人代表身份证以及授权代表身份证复印件)

授权代表姓名：　　性 别：　　年 龄：

单　位：　　部 门：　　职 务：

投标人名称（公章）：

法定代表人（印章）：

日 期：　　年　月　日

附件5：

报价一览表

投标包：第_____包　　包名称：_____

序号	产品名称	含税总报价
1		
总计		小写：
		大写：

注：采购代理服务费由采购人支付的，投标人报价中无需考虑此费用。

时间：_____年_____ 月___日

附件 6：

分项报价明细表

投标包：第_____包　　包名称：_____

序号	货物名称	品牌	产地	规格型号	单 价	数量及单位	合计
1							
2							
3							
	……						
合计总报价（元）							

时间：_____年_____ 月___日

附件7：

投标人同类项目实施情况一览表

投标包：第_____包　　包名称：_____

采购单位名称	设备或项目名称	采购数量	单价	合同金额（万元）	采购单位联系人及电话

附件8：

商务响应表

投标包：第_____包　　包名称：_____

项目	招标文件要求	是否响应	投标人的承诺或者说明
售后服务保障要求			
备品备件以及耗材等要求			
质保期			
交货时间以及地点			
付款条件			
……			
政策性加分条件			
质量管理、企业信用要求			
能力或者业绩要求			
……			

附件9：

联合投标协议书

甲方：

乙方：

（如果两个以上的自然人、法人或者其他组织组成一个联合，可按照甲、乙、丙、丁…序列增加）

联合体各方经协商，就响应（采购人名称）组织实施（项目名称）（项目编号）的招标活动联合进行投标之事宜，达成如下协议：

一、联合体各方一致决定，以 _____为主办人进行投标，并按照招标文件的规定分别提交资格文件。

二、在本次投标过程中，主办人的法定代表人或者授权代理人根据招标文件规定以及投标内容对采购人所作的任何合法承诺，包括书面澄清以及响应等对联合体各方均有约束力。如果中标并签订合同，则联合体各方将共同履行对采购人或者采购代理机构所负有的全部义务，并就采购合同约定的事项对采购人承担连带责任。

三、联合体各方保证对主办人为响应本次招标而提供的产品和服务提供全部质量保证以及售后服务支持。

四、本次联合投标中，联合体各方承担的工作和义务：

甲方承担的工作和义务为：

乙方承担的工作和义务为：

五、有关本次联合投标的其他事宜：

六、本协议提交采购人或者采购代理机构后，联合体各方不得以任何形式对上述实质内容进行修改或者撤销。

七、本协议共份，联合体各方各持一份，并作为投标文件的一部分。

甲方名称：　　（公章）　　乙方名称：　　（公章）

法定代表人：　　（印章）　　法定代表人：　　（印章）

日期：年月日　　日期：年月日

附件10：

联合投标授权委托书

（如果两个以上的自然人、法人或者其他组织组成一个联合，可按照甲、乙、丙、丁…序列增加）

本授权委托书声明：根据_____（甲方名称）与_____（乙方名称）签订的《联合投标协议书》的内容，主办人_____的法定代表人_____现授权_____为联合投标代理人，代理人在投标、开标、评标、合同谈判过程中所签署的一切文件和处理与这有关的一切事务，联合投标各方均予以认可并遵守。

特此委托。

主办人的法定代表人：_____（印章）　　职合投标代理人：_____（印章）：

日期：年月日　　日期：年月日

甲方名称：_____（公章）　　乙方名称_____（公章）

法定代表人：_____（印章）　　法定代表人：_____（印章）

日期：年月日　　日期：年月日

附件11：

残疾人福利性单位声明函

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_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），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）。

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。

投标人名称：

日　期：

附件12：

中小企业声明函

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

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

2.本公司参加 （采购人） 的 （项目名称） 采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他（请填写：中型、小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人名称：

日　期：

投标文件

包：第　包

技术部分

项目名称：

项目编号：

投标单位名称（公章）：

二〇　　年　月　日

技术文件目录

1、项目总体架构以及技术解决方案；

2、货物清单（见附件13）；

3、原厂出厂配置表以及原厂中文使用说明书；

4、技术响应表（见附件14）以及产品彩页等图片介绍资料；

5、选配件、专用耗材、售后服务优惠表（若有）（见附件15）；

6、项目实施人员（主要从业人员以及其技术资格）一览表（若有）（见附件16）；

7、保证供货周期的组织方案以及人力资源安排；

8、投标人在青岛市的售后服务维修机构数量以及分布情况；

9、技术服务、技术培训、售后服务的内容和措施；

10、招标文件技术评标办法中要求提交的相关证明材料；

11、投标人需要说明的其他文件和说明（格式自拟）。

附件13：

货物清单

投标包：第_____包　　包名称：_____

序号	设备名称	品牌	产地	规格 型号	性能以及指标
1					
2					
3					
4					
5					
6					

附件14：

技术响应表

投标包：第_____包　　包名称：_____

序号	招标文件要求	投标文件响应	偏离情况
1			
2			
3			
4			
5			
6			

注：

1、投标人应根据投标设备的性能指标、对照招标文件技术指标要求，如实逐条一一对应填写响应情况，如有未响应技术指标，评标委员会有权视其为负偏离；

2、请投标人在“偏离情况”一栏详细描述存在正偏离或负偏离技术指标，并标明偏离情况；

3、招标文件技术指标未做要求的，不视为正偏离。

附件15：

选配件、专用耗材、售后服务优惠表（若有）

投标包：第_____包　　包名称：_____

序号	优惠内容	适用机型	单价	备　　注
1				
2				
3				
4				
5				
6				

附件16：

项目实施人员（主要从业人员以及其技术资格）一览表

投标包：第_____包　　包名称：_____

姓　名	职务	专业技术资格	身份证号码	参加本单位工作时间

注：在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行制表填写。

附件17：

政府采购诚信承诺书

胶州市公共资源交易中心，（采购人），（采购代理机构）：

我公司_____（供应商名称）已详细阅读了_____项目（项目编号：_____采购文件，自愿参加本次报价，现就有关事项做出郑重承诺如下：

一、诚信报价，材料真实。我公司保证所提供的全部材料、报价内容均真实、合法、有效，保证不出借或者借用其他企业资质，不以他人名义报价，不弄虚作假；

二、遵纪守法，公平竞争。不与其他供应商相互串通、哄抬价格，不排挤其他供应商，不损害采购人的合法权益；不向谈判小组、采购人提供利益以牟取中标。

三、若中标后，将按照规定及时与采购人签订政府采购合同，不与采购人订立有悖于采购结果的合同或协议；严格履行政府采购合同，不降低合同约定的产品质量和服务，不擅自变更、中止、终止合同，或者拒绝履行合同义务；

若有违反以上承诺内容的行为，我公司自愿接受取消报价资格、记入信用档案、没收保证金、媒体通报、1-3年内禁止参与政府采购等处罚；如已中标的，自动放弃中标资格，并承担全部法律责任；给采购人造成损失的，依法承担赔偿责任。

供应商名称(盖公章)：

法定代表人（签字）：

年　月　日

附件18：

政府采购项目验收单

<table>
<tr><td>用　户</td><td></td><td>合 同 号</td><td></td><td colspan="2">合 同</td></tr>
<tr><td rowspan="2">招标项目</td><td rowspan="2"></td><td rowspan="2">验收项目</td><td rowspan="2"></td><td>合 计</td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">验收意见：

负责人：
（组织验收单位盖章）
年　月　日</td><td colspan="2">验收意见：

负责人：
（用户盖章）
年　月　日</td><td colspan="2">验收意见：

负责人：</td></tr>
<tr><td colspan="2">验收小组成员签名</td><td colspan="4"></td></tr>
</table>

附录1

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
1	下一代防火墙	1、系统架构：基于专用多核处理器硬件架构，Web界面可显示处理器核心数，且各核心均参与工作（提供截图证明）；主机系统采用具有自主知识产权的多核多线程ASIC并行操作系统平台（提供该操作系统软件著作权复印件加盖厂商公章的电子文档）；系统支持多系统引导（系统数量≥3），多系统设置可在Web界面上完成全部操作。 2、★标准2U机箱，双冗余电源；配置≥10个10/100/1000M Base-TX，≥4个千兆SFP插槽；配置至少2个高速USB2.0接口，至少1个RJ45串口；整机吞吐量≥10Gbps，最大并发连接数≥320万，每秒新建连接数≥8万。 3、★必须开通病毒防护、IPSEC/SSL VPN、虚拟网关、动态路由、漏洞扫描、主动防御、反垃圾邮件、风险评估、抗拒绝服务攻击等功能；可扩展入侵防御、上网行为管理（含URL过滤、应用识别）功能模块。支持IPv6地址、地址组配置，支持IPv6/IPv4翻译策略技术，包括支持静态NAT-PT、动态NAT-PT技术，支持双栈、6to4隧道实现IPv6终端穿越IPV4网络的访问。 4、支持IPv4和IPv6双栈协议下的病毒扫描与防护，支持双防病毒引擎（标准引擎和增强引擎），杀毒强度可控，支持快速扫描、全面扫描模式；支持国内知名主流品牌病毒库，病毒库提供商通过ICSA Labs认证(提供证明电子文档）；支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性。 5、支持路由、透明、混合等各种工作模式下的网络病毒检测，支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个接口、多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境；支持应用协议自识别，可以实现HTTP,SMTP,FTP,POP3,IMAP,FTP,WEBMAIL多种应用协议下的病毒防护，支持自定义非标准端口下应用协议的病毒防护。 6、支持对病毒的云防护功能，可将检测出的病毒文件备份至云端进行分析；支持可疑文件检测功能，实现对HTTP、FTP以及邮件协议传输的文件进行可疑行为检测，支持病毒文件隔离，用于后续分析取证；支持全面的僵尸病毒检测，既可通过签名特征进行病毒的事前防护，也能基于行为特征进行事中防护，并且可针对至少三种病毒危害级别执行防护动作。 7、支持基于病毒防护规则，可以实现病毒隔离（仅在全面扫毒模式下,且为全局配置）、阻断、声音告警、记录日志，发送告警邮件等5种响应方式；系统内置3种病毒防护模板，支持自定义病毒防护模板，支持gzip、rar、zip等压缩格式的病毒扫描；支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒。 8、内置IPS特征库，特征规则数量不少于3,600条，特征库可分组；支持IP碎片重组、TCP流重组、会话状态跟踪、应用层协议解码等数据流处理方式；支持模式匹配、异常检测，统计分析，以及抗IDS/IPS逃逸等多种检测技术，采用业界领先的入侵检测技术，并取得相关专利。同时具有云计算相关专利技术的主动云防御，可实现全网计算资源、特征资源的共享。	台	2	否	

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
		9、流量管理：支持针对文件类型进行流量管理，至少支持6类如：电影类、音乐类、图片类、文本类、压缩类、应用程序类等。可以针对不同类型的URL配置不同的流量管理规则，包括最大带宽、保证带宽、协议流量优先级等；支持针对用户/用户组进行URL、文件类型、应用的流量管理；为适应多出口环境，可以支持以网络安全区域为出接口的带宽保证策略；支持基于IP、端口、用户/用户组、应用、时间等精准精确的流量统计（截图证明），支持对流量统计结果进行冻结和解冻。 10、支持DMVPN，在增加一个新的分支节点网关后，不需要在中心网关更改任何配置，且支持路由推送，实现spoke to spoke互通，不必建立额外隧道；支持多NAT环境下的多用户L2TP认证加密接入。SSL VPN默认支持不少于30个并发用户授权。 11、支持端口联动，支持上下行端口组的联动，可以实现单端口决定同组中的任意接口失效启动链路切换；自动同步、心跳接口多级（≥2级）物理备份；支持链路备份、端口冗余、双机热备份、集群备份等,具备集群模式的发明专利（提供证明材料电子文档）。 12、支持一体化安全策略配置，可通过一条策略实现用户认证、IPS、病毒过滤、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能；支持对多种移动终端接入内网的行为进行防护，禁止非法外联；支持共享接入检测功能，可防止共享上网行为。 13、支持数据防泄密，可对SMTP协议主题、正文，HTTP协议POST内容数据以及FTP协议文件内容进行敏感信息检测；支持对身份证号（包含港澳台）、银行卡号、手机号、护照号、邮箱、MD5码等敏感信息进行安全防护。 14、内置Web服务攻击防护的特征库，支持对SQL注入、XSS攻击的防护，支持Webshell恶意上传行为并进行拦截；支持对Web恶意扫描行为的防护能力，至少包含对弱口令、版本探测、漏洞扫描三种行为的防护能力，支持WEB服务器错误信息替换，防止服务器信息泄露，提供功能设置、替换信息Web页面及生效日志。 15、支持反垃圾邮件功能，支持SMTP, POP协议下的垃圾邮件检测，支持邮件服务器地址黑名单、邮件地址、主题、正文、附件名、附件内容等进行关键字匹配过滤；支持防邮件炸弹功能，可设置POP3、SMTP的连接频率。 16、提供主动防御与主动扫描功能，支持IPv4和IPv6双栈协议下的主动防御，可主动屏蔽恶意地址、提前免疫包括病毒网站或者攻击源地址的攻击；要求支持主动扫描发现，支持对服务器、主机等资产的后门、服务探测、文件共享、Windows系统补丁、认证等主动式扫描。 17、支持报表，可基于用户访问过网站、收发邮件、IM聊天内容、论坛发帖、文件发送等的内容审计；支持风险评估智能报表，要求至少支持泄密风险、法律风险、工作效率、离职风险等智能报表；支持对AV/IPS等攻击事件的全球地图呈现，包含：基于经纬度、城市的攻击源、目地、攻击次数等，地图支持逐级缩放；支持国产化地图引擎（截图证明）。 18、要求产品提供三年原厂软、硬件质保和技术支持服务，并具有： 《计算机信息系统安全专用产品销售许可证》（增强级） 《涉密信息系统产品检测证书》				
		《中国国家信息安全产品认证证书》（ISCCC第三级） 《国家信息安全测评信息技术产品安全测评证书》（EAL3+） 《电信设备进网许可证》 《IPv6 Ready Logo Certified》（IPV6 Ready认证证书） 具有符合“GA243-2000《计算机病毒防治产品评级准则》”安全网关检测报告 具有国际CVE组织产品兼容证书，以上证书或证明材料须提供电子文档。				

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
2	日志审计系统	1、★一体化硬件架构，2U机架式设备，日处理性能3000EPS，配置不少于6个千兆电口，冗余双电源，有效存储空间不少于2T。 2、★配置设计数量≥500个，需涵盖互联网业务系统所有网络设备、安全设备、主机、数据库、中间件以及各种应用系统的告警、并对安全日志实现事件关联分析，集中展现； 3、部署方式：旁路部署； 4、综合展示：能够显示系统的基本管理信息； 5、资产管理：具有资产管理的功能，能够将被管理 IT 资产进行分组、分域出网络拓扑图，展示IT资产之间的逻辑拓扑连接关系，并能够自动进行多种拓扑布局；能够提供基于资产的拓扑视图，显示资产之间的逻辑连接关系。 6、拓扑管理：拓扑管理功能能够运行在 Linux 和 Windows 环境下，展示网络拓扑。 7、日志采集：无需另外安装软件组件，管理中心即可通过SNMPTrap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、NetBIOS、OPSEC等多种方式完成日志收集功能。；特殊协议支持订制；针对文本格式的日志采集，支持本地文件、Windows共享和FTP获取三种采集方式. 8、事件统计分析：能够以实时统计策略的形式从各个维度进行安全事件进行实时统计分析。支持根据需要结合应用场景，能够重定义关联事件中一个或多个字段的值，比如某些原始事件触发了某一关联规则而产生新的关联事件，原本是一个自动不可干预的过程，关联事件重定义可以凭借安全专家经验，重定义及补全像事件类型、事件名称、摘要描述信息，起到修正、补正信息的作用； 9、事件关联分析：具有安全事件关联分析的能力，能够对不同的事件进行 相关性分析，支持多事件关联，对不同来源的安全事件进行相关性分析。应具备历史日志关联分析的能力；能够对指定时间范围内的不同的历史日志进行相关性分析，发掘潜在的信息；应支持观察列表，可根据关联分析的结果将可疑或者需要关注的信息加入观察列表，并可以对观察列表中的信息进行关联，也可以被任何规则引用； 10、威胁情报支持：应支持通过导入或者主动自动抓取的方式获取外部相关威胁情报信息，并能将这些威胁情报用于关联分析，主要威胁情报包括：恶意IP地址、恶意URL； 11、知识管理：提供开放的知识管理功能，内置安全知识。提供详尽的日志参考知识库，方便用户查询不同原始日志信息的错误ID号和详细描述信息；应提供Cisco PIX和交换机的事件编码知识库；应提供Windows、Linux、Solaris、AIX操作系统的事件ID知识库（提供截图）；应提供Oracle、SQL Server、MySQL、Informix、DB2数据库的事件编码知识库；支持查看系统内置的事件库中事件类型名称及其描述信息。 12、产品资质：产品具备中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》；具备国家保密局涉密信息系统安全保密测评中心《涉密信息系统产品检测证书》；具备《（3C）中国国家信息安全产品认证证书（增强级）》；具有中国信息安全测评中心《信息技术产品安全测评证书》EAL3+级；具有《IPv6 Ready Logo Phase-2》认证证书，以上证书或证明材料须提供电子文档。	台	1	否	

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
3	网络准入设备	★产品需实现与上级单位做对接。 实现全网设备NTP服务同步，采用统一、精准的时间，全网各类型设备都能配置，时间精确，与标准时间同步。 提高DNS/DHCP的技术支持能力，消除DNS/DHCP服务单点故障，保证业务的连续性，避免设备出现单点故障。 实现集中式、有效的IP地址管理分配，通过IP开通自动化来控制操作成本；优化网络资源的使用率。 实现集中高效DNS域名解析服务，支持多线路DNS智能解析，实现服务器宕机检测，提高DNS系统安全性和可靠性。 实现非法IP接入控制，实现有线、无线网络终端集中管控，根据单位的IP规划，不同区域划分不同VLAN，按需实现自动分配。 设备内嵌WEB认证服务，在实现基于WEB界面集中管理同时，在同台设备必须要实现WEB Portal认证服务，实现设备自服务注册。 灵活的网络端口安全扫描，实时分析服务器/终端提供了哪些应用和服务，能够有效的预先评估和分析终端所存在的安全隐患。 ★设备集成DNS、DHCP、NTP、TFTP、内置WEB Portal认证服务、无线BYOD指纹识别控制、IP地址管理审计、IP地址接入控制、IP地址调和、智能DNS解析、应用服务器宕机检测，终端服务端口扫描审计、全面支持IPv6。 设备必须支持HA（ high-availability）自动切换功能和active-standby模式。 联动交换机的DHCP SNOOPING和DAI功能，可以预防伪DHCP服务，避免IP地址冲突、ARP病毒，防止私改IP地址。 ★用户界面支持中文，并具有纠错功能。 支持双因子登录鉴别，支持动态令牌+用户名/密码方式，防止密码重放性攻击。 针对管理员可进行细粒度的管理控制，要求能根据需求，将设备的管理权限分配给多管理员用户进行管理并进行审计；支持记录管理员的相关操作配置；要求支持账户保护功能（多次登陆失败则一段时间内禁止登陆，同时支持手动解锁功能）。 支持将IP或DNS等外部数据方便的导入，支持.xls和.xlsx格式。 支持将数据库内容实时备份和定时备份。 支持将设备的日志文件方便的导出。 设备支持Telnet或ssh。 设备支持和主流的上网行为厂商（深信服、网康、锐捷SMP、NETGEAR网件）进行接口联动，实现IP/MAC全程审计（需提供上述厂家界面截图，加盖公章的电子文档）。 设备必须提供WEB Services接口，供二次开发，实现DDI系统与其他系统的整合 支持SYSLOG日志发送第三方日志服务器。 兼容同步多种接入设备的时钟，包括网络设备、服务器、PC、小型机等各类型设备，如windows/ Linux/AIX/Solaris等。 支持作为一级时间服务器，同步接入设备的时钟。 支持作为二级时间服务器，同步于外部NTP网络时间服务器。 支持配置多个外部NTP网络时间服务器，并可以灵活排序。 系统必须支持标准的 DNS 服务，支持反向DNS解析功能。 ★支持OSPF+ANYCAST方式部署，支持配置宣告物理网段。 支持泛域名解析，支持DNS轮询，实现DNS负载均衡。 支持中文域名，DNS解析服务支持中文域名记录。 微软AD域支持，能够与微软AD域控结合，自动同步生成NS、SRV、A等记录，接管其DNS服务（需提供界面截图，加盖公章的电子文档）。	台	1	否	

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
		支持DNS智能解析，支持设定网通、电信、移动等IP地址段，针对不同的地址段解析不同的IP，便于外部访问主页提高访问速度。 ★支持DNS业务健康检测，支持Ping，TCP/端口，Http URL，Https URL，SNMP等检测方式。 支持DNS域名过滤，可自定义域名URL，实时生效。 DHCP服务：基于IP/MAC地址的静态绑定（IP保留地址分配）；实现地址的动态分配和回收；支持所有ISC预定义的 DHCP option 空间（如Option 1 到Option 125）和客户化的DHCP Option空间（如Option 126 到Option 254）。 ★支持通过DHCP下发无线控制器信息，支持不同类型、厂家无线AP在子网/VLAN内混合组网，智能引导各厂家无线AP自动注册，支持显示中文计算机名称（Windows非标准字符），终端的计算机名称可配置为中文，通过DHCP显示中文计算机名。 支持IP地址强制释放功能，针对部分终端DHCP租期到了不会主动续约并继续使用过期IP的情况，实现手工和周期性强制释放IP地址，可定制定强制释放天数，以确保IP地址的利用率。 支持DHCP实时在线用户趋势分析、DHCP响应包趋势分析、IP数据利用率实时统计分析、DHCP指纹数据实时统计等。 支持创建DHCPv6地址分配池。 支持DHCPv6有状态地址分配，支持自动发现设备DUID标识（需提供界面截图，加盖公章的电子文档）。 中央数据集中的IP管理控制台，支持IPv4、IPv6双栈地址管理 支持交换机自定义脚本配置功能，实现与交换机之间自动和交互式任务进行通信，提供快速开通配置交换机等功能 实时显示分配地址的状态和续租信息 实名制地址分配、回收和历史数据的审计分析 支持DHCP系统指纹技术，支持BYOD（BringYourOwnDevice），自动识别智能手机、平板电脑等的系统指纹 。 支持DHCP指纹识别率98%以上，支持快速对DHCP未知指纹进行识别及添加（需提供界面截图，加盖公章的电子文档）。 支持数据完整性检查，数据核查机制可以在系统部署前进行数据检查，提前发现系统配置的问题 ★支持MAC地址黑白名单，可以只对已授权MAC的设备分配IP地址。向MAC动态授权列表内临时添加新的记录，不需要重启DHCPv4服务进程。 灵活的MAC地址永久授权，及MAC地址活跃度分析。 ★内置WEB Portal认证服务器，在实现基于WEB界面集中管理同时，在同台设备必须要实现WEB Portal认证服务，实现设备自服务注册。 支持IP自助授权和管理员审批授权等多种方式，可通过后台配置进行灵活切换（需提供界面截图，加盖公章的电子文档）。 支持配置访客地址使用期限设定。 支持手动/定期解除已授权地址。 基于Portal的访客自服务注册信息录入和自动授权，针对于笔记本和手机终端支持响应式界面，既然页面自适应。 ★支持以旁路的方式接入网络中，使用标准SNMP协议对网络设备进行端口操作，开启或关闭。 支持发现同一VLAN内相同IP和MAC更换端口的操作，可进行一键端口关闭。 ★支持终端服务端口扫描功能，支持多种扫描方式，包括TCP同步扫描(TCP SYN)/TCP connect()扫描)/TCP ACK扫描/TCP Window窗口扫描/TCP Maimon扫描/UDP扫描。 支持终端端口状态变更审计，利于实时统计终端安全状态。				

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
		支持发现待清除核查状态，此状态表明此IP地址长时间没有被使用 支持发现未知IP核查状态，此状态表明此IP由于各种原因没有被记录在系统中，如非法接入、手动私设地址等。 支持设备端口和MAC扫描，自动周期性发现IP设备和交换机端口的对应关系，自动发现和显示VLAN信息，显示交换机端口的详细信息，包括端口速率，端口状态，端口信息描述等信息。 集成Expect 编程工具语言，自动实现交互式任务。通过用户名和密码实现模拟登录过程，实现指令交互，支持定制计划任务，如脚本的执行时间、周期等（需提供界面截图，加盖公章的电子文档）。 提供软件著作权证书、软件产品登记证书、3C认证证书、公安部等保三级评测报告、公安部销售许可证、中国泰尔实验室入网检测报告、原厂授权以及服务承诺函（以上证明材料须提供电子文档。）； 所供货CNS网络核心服务设备的厂商，应能提供365 x 24的标准技术支持服务，应包括但不限于客户服务网站/MAIL/电话热线服务 所供货CNS网络核心服务设备必须具有NBD服务，当硬件出现故障时，能够及时提供备品备件。				
4	数据库审计	1、系统采用专用硬件架构与专用安全操作系统；专用的安全操作系统具有自主知识产权；审计设备的存储支持RAID1阵列，空间不得少于4T。 2、★支持千兆网络环境监听，2U上架专用设备，双电源，≥6电口（含1个管理口）和1扩展槽，提供1个RJ45串口。 3、系统审计事件每秒入库速度至少在25000条/秒以上，日处理审计事件数至少15000万条； 4、采用旁路部署方式对原有网络不造成影响，网络审计产品的故障不影响被审计系统的正常运行；无需在被审计系统上安装任何代理。 5、支持对Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、MongoDB、Redis数据库进行审计，支持人大金仓KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase) (需提供功能截图的电子文档) 6、支持FTP、Rlogin、Radius、NFS、X11等协议审计(需提供功能截图电子文档) 7、针对异常场景自动生成审计结果，免配置； 8、异常场景包含且不限于：异常账号访问审计、数据库异常审计、同账号多IP登陆、同账号上下班时间操作统计、访问时长异常审计、操作全审计等； 9、异常账号审计支持对数据库近一个月没有登陆账号突然登陆的异常行为进行审计；（截图证明电子文档） 10、数据库异常审计支持对于数据库异常信息的统计与发现，一键生成审计结果； 11、支持对于短时间内相同账号多个IP地址登陆的自动发现与审计，用以发现账号被盗用等异常； 12、支持对相同账号下班时间操作多于上班时间的异常操作自动发现和审计； 13、支持访问操作的全审计，自动生成审计策略，自动生成报表；(需提供功能截图电子文档) 14、产品需具备以下产品资质： 公安部销售许可证（增强级） 涉密信息系统产品检测证书 《中国国家信息安全产品认证证书》（3C认证），以上证书或证明材料须提供电子文档。	台	1	否	

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
5	安全可视化管理平台SOC	1、运行环境：要求采用 B/S 架构；集成数据库。支持 Windows或Linux操作系统，支持64位操作系统；事件处理性能平均每秒≥8000条事件。 2、★管理节点数量≥1000个，需涵盖互联网业务系统所有网络设备、安全设备、主机、数据库、中间件以及各种应用系统的告警、并对安全日志实现事件关联分析，集中展现； 3、★部署方式：支持分布式部署和群集模式，多级、多点部署时，采用分布式存储；支持两个管理中心之间可以进行级联，形成大规模统一管理；为保证管理一致性，实现可视化信息统一管控。 4、综合展示：能够显示系统的基本管理信息； 5、资产管理：具有资产管理的功能，能够将被管理 IT 资产进行分组、分域出网络拓扑图，展示IT资产之间的逻辑拓扑连接关系，并能够自动进行多种拓扑布局；能够提供基于资产的拓扑视图，显示资产之间的逻辑连接关系。 6、拓扑管理：拓扑管理功能能够运行在 Linux 和 Windows 环境下，展示网络拓扑。 7、日志采集：无需另外安装软件组件，管理中心即可通过SNMPTrap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、NetBIOS、OPSEC等多种方式完成日志收集功能。分别配置XX个分布式事件采集器和XX个分布式事件存储器。 8、事件统计分析：能够以实时统计策略的形式从各个维度进行安全事件进行实时统计分析。 9、事件关联分析：具有安全事件关联分析的能力，能够对不同的事件进行 相关性分析，支持多事件关联，对不同来源的安全 事件进行相关性分析。 10、知识管理：提供开放的知识管理功能，内置安全知识。 11、网络管理：对支持 SNMP 协议的主流网络设备和安全设备进行管理；支持主流版本的 Windows、Linux、UNIX 等主机和服务器；支持主流版本的Oracle、DB2、Sybase、MySQL等数据库；支持主流版本的 Weblogic、WebShpere、JBoss、Apache、Tomcat等中间件；支持多种网络服务的运维和管理，包括 但不限于：SMTP、POP3、HTTP、FTP、TELNET、SSH、SSH2、DNS、DHCP、WINS、LDAP。 12、漏扫驱动：支持对漏扫引擎进行集中管理，并对漏扫引擎下发扫描任务，收集扫描结果，统一进行漏洞脆弱性分析；至少支持三种漏扫引擎的调度，必须明确列举出来；漏扫结果可以自动参与到弱点管理模块中，并参与脆弱性计算。 13、配置核查：系统应具有主动的配置安全核查功能，能够对核查对象的配置进行细粒度的安全符合性检查，并出具核查报告；系统支持多种核查调度策略，包括即时核查、定时核查、周期性核查和离线核查四种核查方式。 14、威胁态势分析：支持通过建立并针对一组关键指标体系（KPI）计算得到一个威胁指数，以此来表征一段时间内、某个网络区域的网络安全威胁状态及其发展趋势；能够计算全网或者一级安全域的威胁态势指数，并自动描绘出态势指数曲线；能够描绘态势成因雷达图和帕累托图，展示出每种态势成因在态势指数中所占的比重；系统能够分析并展示当前态势指数与上个周期的态势指数的环比变化情况；能够展示一幅热点分析图，以三个同心圆的方式展示应用层、网络层和终端层的热点信息。	台	1	否	
		15、流安全分析：支持端口镜像与被动接收两种方式采集流数据，可接受支持NetFlow、NetStream、Sflow和iflow协议的采集；支持按业务场景进行流量分析，可自定义业务场景，至少包含总流量、数据包、top端口、top地址和top协议等维度，可以对业务场景流量进行top端口、top地址、top协议的排行分析与查看；支持协议流量分析，可分别分析应用层、传输层、网络层、链路层的不同层面的协议的流量情况。 16，产品资质要求：产品具备中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》；具备国家保密局涉密信息系统安全保密测评中心《涉密信息系统产品检测证书》；具备《（3C）中国国家信息安全产品认证证书（增强级）》；具有中国信息安全测评中心《信息技术产品安全测评证书》EAL3+级；具有《IPv6 Ready Logo Phase-2》认证证书，以上证书或证明材料须提供电子文档。				

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
6	入侵防御系统	1、系统架构：基于专用多核处理器硬件架构，Web界面可显示处理器核心数，且各核心均参与工作；操作系统为VSP通用安全平台，具备高效、智能、安全、健壮、易扩展等特点。(提供VSP证明文件并加盖公章的电子文档) 2、标准2U机箱，双冗余电源；配置≥6个10/100/1000M Base-TX，≥4个千兆SFP插槽；配置至少2个高速USB2.0接口，至少1个RJ45串口；整机吞吐量≥6Gbps，最大并发连接数≥320万，每秒新建连接数≥8万。 3、系统可检测的入侵防御事件库事件数量不少于4000条，系统应支持事件响应模版，能够批量修改事件响应动作，包括：事件级别、事件启用开关、动作、日志合并方式、日志开关、抓包取证。系统应支持弱口令检测功能，需支持至少8种网络协议并支持至少7种弱口令检测元素，文字说明支持的网络协议和定义弱口令的检测元素。 4、系统应支持多种防web扫描能力，包括爬虫、CGI和漏洞扫描等，并支持设置至少5个不同级别的扫描容忍度/扫描敏感度。系统应支持多种事件响应方式，满足客户的安全要求，需包括：重置、临时阻断、丢弃报文、丢弃会话等动作。系统应支持密码穷举探测功能，提供至少16种应用的密码穷举行为探测和阻断。 5、为保证病毒检测的可靠性，要求系统应至少支持双病毒引擎，需提供界面截图并提供防病毒引擎厂商合作证明，并加盖原厂公章的电子文档。 6、★系统支持具有云计算相关专利技术的主动云防御功能，实现全网计算资源、特征资源的共享。 7、系统应支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于50万。 8、系统应支持HTTP协议和邮件协议防病毒，通过信息替换功能，用以通知用户病毒被阻断，管理员可以自行设置替换信息。 9、系统应提供扩展静态恶意代码（APT）检测引擎，针对http、ftp、SMTP等协议中包含的未知恶意文件进行检测。 10、★系统应支持可扩展恶意样本自学习功能，除通过网络文件捕获外，还支持通过系统直接上传文件，自动识别黑白文件并提供简要信息。 11、系统应支持与动态恶意代码（APT）检测系统联动功能，通过联动功能可将恶意样本发送到动态APT引擎进行深度检测，并将检测结果生成攻击特征样品进行动态拦截。 12、系统应支持可扩展未知C&C通道（隐蔽通道）检测功能，能够提供C&C通道的危险级别、连接建立时间、连接持续时间、控制端IP地址和端口、受控端IP地址和端口等C&C通道信息。 13、系统除具备可扩展的本地恶意代码检测功能外，还应具备云查杀、云检测等防御机制。 14、系统应支持Web过滤功能，至少支持黑白名单、关键字过滤、禁止HTTP代理、URL分类过滤外，还支持Script、 Java Applet等过滤，并能通过统一模版设置。 15、系统应支持邮件内容过滤功能，有效防止恶意邮件及信息外泄。可根据邮件SMTP命令、发件人、主题、附件、IP及邮件大小进行过滤。 16、系统应支持敏感信息防护功能，识别信息和文件中的关键字、身份证、手机号码、固定电话号码、银行卡、IP地址等敏感信息，并支持文件指纹识别和白名单功能。 17、系统应支持WEB登录图像验证码功能，防止暴力破解。	台	1	否	
		18、要求提供三年原厂软、硬件质保和技术支持服务、并提供三年特征库升级服务，同时要求产品具有： 《计算机信息系统安全专用产品销售许可证》（增强级） 《涉密信息系统产品检测证书》 《中国国家信息安全产品认证证书》（ISCCC第三级） 《国家信息安全测评信息技术产品安全测评证书》（EAL3+) 《军用信息安全产品认证证书》（军B级） 《计算机软件著作权登记证书》 具有国际CVE组织产品兼容证书，以上证书或证明材料须提供电子文档。				

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
7	路由器	路由器机框、配置机箱附件、配置双电源、1块灵活接口平台300,1 HIM 插槽,12端口GE Combo ★1、支持与原有的路由器虚拟成一台逻辑设备使用，采用全分布式硬件架构；要求支持主控、业务板和交换网板物理分离；整机线卡采用母板+子卡架构形态，母板和子卡均可热拔插； 2、交换容量：≥70Tbps；包转发率：≥6000Mpps 3、整机框全物理尺寸的业务槽位数≥2，不含主控、交换网板槽位,非子卡槽位；支持独立交换网板。 4、支持E1/T1、FE、GE、10GE、POS（155M/622M/2.5G）、CPOS、RPR、同步串口等广域网接口 5、内置硬件加密引擎，本次要求实际配置具备IPsec VPN功能的硬件板卡或功能license； 6、要求支持OTV/EVI等数据中心虚拟机迁移二层协议技术，并可提供高安全的加密功能。 ★7、硬件支持NAT功能，本次要求实际配置具备NAT 功能硬件板卡或功能license； 8、支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合；虚拟化技术需提供权威机构出具的报告复印件加盖厂家公章的电子文档。 9、支持L2TP、GRE，本次要求实际配置具备L2TP、GRE VPN功能的硬件板卡或功能license； 10、支持与路由器一体化的防火墙、IPS（或IDS）、ACG业务板，以简化管理，消除单点故障。 11、本次配置：≥1个主控；≥2个模块化电源；≥12个千兆光接口，≥12个千兆电接口。	台	1	否	
8	交换机	★1、支持与原有交换机冗余使用，业务插槽数≥6；主控引擎模块≥2；交换容量≥85Tbps；转发性能≥26400Mpps 2、以太网支持千兆电口，千兆光口，10GE端口、40G端口、100G端口；单槽位线速万兆端口密度≥16；单槽位线速40G端口密度≥4；单槽位万兆端口密度≥48；单槽位40G端口密度≥8；单槽位100G端口密度≥2；单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48；支持FCoE接口；支持EPON OLT接口；支持RPR。支持POE+，满足新一代园区网以太网供电需求，提供工信部权威第三方测试报告复印件加盖厂家公章的电子文档。 3、聚合组数≥128组，每组成员≥8个；支持跨设备链路聚合 4、多虚一技术(N:1)，支持4框虚拟化技术，一虚多技术（1:N），支持多虚一技术和一虚多技术的配合使用，提供工信部权威第三方测试报告提供工信部权威第三方测试报告复印件加盖厂家公章的电子文档。 5、支持MACsec 6、提供工信部入网证,产品最早入网时间≥3年 ★7、本次配置要求：配置单主控；配置冗余电源；实配千兆电口≥48，千兆光口≥24，万兆光口≥4；配置≥10个千兆多模光模块。 ★8、要求与核心路由器统一品牌	台	1	否	

采购明细表

序号	货物名称	技术参数	单位	数量	是否为政府强制采购产品	备注
9	●运维平台	1、★1U机架式一体设备，单电源，物理存储≥2TB； 至少支持6个千兆电口，具有一个扩展插槽，可扩展4个千兆光口、8个千兆光口、8个千兆电口、4个千兆光口+4个千兆电口或2个万兆光口； 2、★字符协议不低于1000个，图形协议不低于300个，可管理设备数不低于500台； 3、专用安全操作系统，软硬件一体化，物理旁路，逻辑串联模式，不影响正常业务流量，A双机热备，支持NAT地址映射部署，通过映射后的IP地址访问堡垒机，分布式部署：支持添加一台或多台协议代理服务器，分担审计中心性能压力；并支持通过不同的协议代理服务器节点访问不同的资源，多协议代理服务器节点可访问相同资源时实现自动负载均衡； 4、字符协议：SSHv1、SSHv2、TELNET、RLOGIN，图形协议：RDP、VNC、X11，文件传输协议：FTP、SFTP；数据库协议：支持Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、TeraData等数据库类型；支持通过应用发布进行协议审计，记录命令详情，包括字符协议和数据库协议等，审计回放支持协议回放和图形回放；支持通过应用发布进行协议扩展第三方客户端，并支持账号密码代填登录；支持通过应用发布对http/https的访问过程进行录像审计；支持web页面防跳转功能，进行http/https访问过程中，运维人员仅允许访问授权地址 5、支持Oracle、postgresql、sybase、mysql、sqlserver数据库下行返回行数和oracle数据库变量绑定； 6、支持运维客户端功能，运维操作过程不依赖浏览器和JAVA环境；通过堡垒机web页面内嵌SSH、FTP、TELNET运维工具访问目标资源；通过堡垒机web页面调用本地工具访问目标资源；户端菜单模式访问：用户可通过字符菜单（TELNET、SSH协议）或图形菜单（RDP、VNC协议）方式选择目标服务器并进行访问； 7、RDP协议支持剪切板、本地磁盘映射功能，所有图形协议支持自适应本地浏览器窗口大小；windows服务端开启安全层SSL加密，加密级别符合FIPS标准，允许运行使用网络级别身份验证的远程桌面的计算机连接； 8、支持TELNET、SSH协议使用SecureCRT工具批量登录目标资源；多种本地工具支持，支持SecureCRT，WinSCP，SQLPlus，PLSQLDev，Toad4Oracle，Db2cmd（DB2），TightVNC，pgAdmin3，SqlAdvantage，Sqleditor，mysql，QuestCentral，SSMS，Xshell，dbvis，Navicat，SSH Secure Shell Client； 9、RDP图形操作过程中键盘输入操作记录和鼠标点击行为记录，支持开启或关闭键盘输入审计功能，支持RDP窗口标题审计，并支持窗口标题内容检索定位回放 10、以WEB在线视频回放方式重现维护人员对服务器的所有操作过程，无须在客户端安装播放客户端软件，离线回放重现维护人员对服务器的所有操作过程（回放文件下载到本地播放）；倍速/低速播放、拖动、暂停、停止、重新播放会话协议回放空闲时间过滤，应用发布图像操作回放支持操作空闲过滤（可设置无操作多长时间开始过滤）等播放控制操作；根据审计日志操作命令和RDP键盘输入命令开始回放；	套	1	否	
		11、支持按设备、系统帐号、计划开始时间、改密周期等信息配置改密计划，到期自动执行，随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并严格遵守密码强度设置；手工改密功能；支持自动改密结果发送到指定改密计划的管理员邮箱； 12、自动改密支持Linux、Unix、Windows（采用RPC方式）、AIX以及Oracle、SqlServer、PostgreSQL、MySql、DB2、Informix、SYBASE的内置自身账号密码； 13、支持实时监控当前连接发生的所有会话信息和阻断功能，审计系统CPU、内存、磁盘的使用情况，记录审计系统自身的管理操作，保障审计系统自身安全，会话查询可定义条件，包括会话时间范围、用户、资源、操作命令关键字、指令策略等条件；以CSV、HTML方式生成并导出报表，管理员自定义审计报表，以日报、周报、月报的方式自动生成周期性报表 14、审计查询关键字和结果显示支持多种编码(UTF-8、Big5、EUC-JP、EUC-KR、GB2312、GB18030、ISO-8859-2、KOI8-R、KS_C_5601_1987、Shift_JIS、Window-874)，由用户自主选择； 15、支持数据备份，系统配置的导入、导出功能，配置和数据备份自动导出到FTP服务器、空间自管理功能，存储空间不足时能够自动清理历史数据，可自定义清理存储空间的阀值； 16、从WEB界面修改网卡IP设置、静态路由设置等内容，支持IPv6；支持网口聚合功能。				