（2021-02 竞争性磋商文件范本）

青岛市政府采购

崂山区电子政务外网安全提升服务项目（一）

采 购 人：青岛市崂山区电子政务和大数据中心

代理机构：青岛正嘉招标项目管理有限公司（公章）

项目编号：LSCG2021000072

日　　期：2021 年 03 月 28 日

目 录

第一章　磋商公告

项目概况

崂山区电子政务外网安全提升服务项目采购项目的潜在供应商应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）本项目采购公告页面免费获取磋商文件，并于2021年04月08日14点00分（北京时间）前提交响应文件。

一、项目基本情况

项目编号：LSCG2021000072

项目名称：崂山区电子政务外网安全提升服务项目

采购方式：□竞争性谈判 ☑竞争性磋商 □询价

预算金额：171.6万元

最高限价（如有）：/

采购需求：详见磋商文件第四章。

合同履行期限：具备服务能力，自验收合格之日起一年。

本项目□接受☑不接受联合体。

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。

2采购公告发布之日前三年内无行贿犯罪等重大违法记录。

3具有良好的商业信誉和健全的财务会计制度；具有依法缴纳税收和社会保障资金的良好记录。

4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）、崂山区公共资源交易信用监管平台查询，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、不良行为名单。

5 供应商请在开标截止时间前在青岛政府采购网 www.ccgp-qingdao.gov.cn 注册并登陆后进行网上报名。未在网上报名或网上报名不成功的，无资格参加投标或谈判。

6 投标人请在开标截止时间前在崂山政务网（http://www.laoshan.gov.cn）公共资源交易模块“诚信考核”注册，注册未成功的，无资格参加投标（或谈判）。

7 本项目不接受联合体投标。

三、获取采购文件

供应商须在开标前在青岛市政府采购网上注册并关注该项目。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）本项目采购公告页面免费下载电子磋商文件。代理机构不再发售纸质磋商文件。

四、响应文件提交

截止时间：2021 年 04 月 08 日 14 点 00 分（北京时间）

地点：通过【青岛市公共资源投标文件制作工具】上传响应文件。

五、开启

时间：2021 年 04 月 08 日 14 点 00 分（北京时间）

地点：青岛市崂山区仙霞岭路 20 号市民文化中心 D 座政务办理大厅 4 楼

六、公告期限

自本公告发布之日起 3 个工作日。

七、其他补充事宜

1. 公告媒介：本项目采购公告同时在中国青岛政府采购网（http://zfcg.qingdao.gov.cn）和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。预算金额在500万以上的项目，同时在中国政府采购网上发布。

2. 支持网上远程开标，供应商无需到现场参加开标会。

八、凡对本次采购提出询问，请按以下方式联系。

1.采购人信息

名　　称：青岛市崂山区电子政务和大数据中心

地　　址：青岛市崂山区仙霞岭路18号

联系方式：88996736

2.采购代理机构信息（如有）

名　　称：青岛正嘉招标项目管理有限公司

地　　址：青岛市延安三路114号金环大厦2单元503室

联系方式：18561231036

3.项目联系方式

项目联系人：宋欣雨

电　　话：18561231036。

如有询问，请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）本项目采购公告页面在线提交。询问及答复的内容在上述公告页面查看。

第二章　供应商须知前附表

序号	条款名称	编列内容
1	采购人	青岛市崂山区电子政务和大数据中心
2	采购代理机构	青岛正嘉招标项目管理有限公司
3	项目名称	崂山区电子政务外网安全提升服务项目
4	分包及成交规定	☑本项目不分包。 ☐本项目分为多个包，供应商可以选择多包响应，供应商成交包数不受限制。 ☐本项目分为多个包，供应商可以选择多包响应，但供应商最多只能成交_____个包。若同一供应商在 2 个及以上包的响应排名均第一的，按照以下规则确定成交供应商：_____
5	资金来源以及资金构成	预算金额为 1716000 元，其中财政资金为 1716000 元，其他资金为 0 元。
6	是否接受联合体磋商、报价	☑ 不接受 ☐ 接受，应满足下列要求：_____
7	报价有效期	自报价截止之日起 90 个日历天。
8	踏勘现场	☑ 不组织，自行踏勘 ☐ 组织，踏勘时间：_____ 踏勘地点：_____
9	履约保证金	☑不需要交纳 ☐需要交纳，履约担保的金额：成交合同金额的___%（履约保证金允许以担保支票、押金证明、保险单、保函、信用证等形式提交）
10	采购代理服务费支付	☐ 无需支付 ☐ 采购人支付 ☑ 成交人支付，代理费：2.0728 万元
11	构成磋商文件的其他材料	采购人依法依规对磋商文件所作的澄清和修改，构成磋商文件的组成部分。
12	磋商文件的澄清和修改	磋商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）本项目磋商公告页面，供应商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，视为供应商已收到。

13	是否允许递交备选报价方案	☑ 不允许 ☐ 允许。要求：只有成交供应商所递交的备选报价方案方可予以考虑。磋商小组认为成交供应商的备选报价方案优于其按照磋商文件要求的报价方案，采购人可以接受该备选报价方案。
14	响应报价的范围	含税全包价，包括产品的设计、制作、包装、保险、运输、装卸、安装、调试、培训、验收、保修等一切费用（即交钥匙工程）。
15	最后报价	报价次数由磋商小组根据磋商情况确定。 最后报价前必须告知所有参加磋商的供应商，在规定的时间内提交最后报价，并以最后报价为最终报价。 供应商未在规定时间内报价的，按其前一次报价进行评审。
16	面向中小企业预留情况及小微企业报价扣除标准	☐本包为面向中小企业预留份额的采购包，专门面向中小企业采购，有关要求详见采购公告和第三章。小微企业不享受价格折扣优惠。 ☐本包为面向中小企业预留份额的采购包，要求供应商以联合体形式参加采购活动，且联合体中中小企业承担的部分达到一定比例，有关要求详见采购公告和第三章。小微企业不享受价格折扣优惠。 ☐本包为面向中小企业预留份额的采购包，要求获得采购合同的供应商将采购项目中的一定比例分包给一家或者多家中小企业，有关要求详见采购公告和第三章。小微企业不享受价格折扣优惠。 ☑本包为非面向中小企业预留份额的采购包。小微企业报价扣除标准如下： 1.对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）规定的小微企业报价给予 10%（工程项目为 5%）的扣除，用扣除后的价格参与评审。 2.接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购包，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的，对联合体或者大中型企业的报价给予 3%（工程项目为 2%）的扣除，用扣除后的价格参加评审。
17	采购标的对应的中小企业划分标准所属行业	
18	响应文件编制	供应商使用【青岛市公共资源投标文件制作工具】编制电子响应文件。
19	响应文件盖章	在磋商文件的第十章响应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 2019 年 7 月 10 日版”。 特别提示：1、制作响应文件时，单项绑定 pdf（word）文件时无需再电子签章，单项绑定的 pdf（word）文件不再作为响应文件上传。 2、响应文件制作完成后，系统自动合成资格审查部分、商务部分、技术部分三个 pdf 响应文件。供应商需要按照磋商文件要求，在上述三个 pdf 响应文件上进行电子签章，并上传。（单项绑定的 pdf（word）不再上传）
20	响应文件加密、上传	通过【青岛市公共资源投标文件制作工具】上传时，系统通过供应商当前使用的 CA 数字证书自动加密电子响应文件。 电子响应文件上传成功后，系统出具上传凭证，供应商可以下载保存。
21	供应商签到及电子响应文件解密	支持网上远程开启响应文件，供应商无需到现场参加开启会议。若到现场开启响应文件，应携带上传响应文件的 CA 数字证书及可登陆互联网的电脑设备以确保网上开启。开启注意事项详见“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.供应商在线签到：在递交响应文件截止时间前 1 小时内通过 CA 数字证书进行在线签到，未在线签到的响应无效。 2.供应商接到解密提示后，应当在规定时限内通过 CA 数字证书对电子响应文件开始解密。
22	开启响应文件时间及地点	详见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本项目磋商公告页面及青岛市政府采购网。
23	磋商小组	磋商小组共1组，其中：第1组采购人代表1人，评审专家2人；－－－－－－ 。
24	评审方法	综合评分法
25	是否授权磋商小组确定成交供应商	☑ 是，确定一个成交供应商，成交结果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，公告期限为 1 个工作日。 ☐ 否，推荐的成交候选供应商个数：____
26	其他需补充的内容	
26.1	书面形式的定义	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磋商公告、磋商文件及发出的澄清、答疑、变更等各类公告。
26.2	相关评审标准认可要求	潜在供应商的资质、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（上传后将无法删除），制作响应文件时上述材料只能通过系统选取，否则在电子评审时不予认可。
26.3	分包和非主体、非关键性工作	☑ 不允许 ☐ 允许，供应商根据磋商文件载明的标的采购项目实际情况，拟在成交后将成交项目的非主体、非关键性工作交由他人完成的，应当在响应文件中载明。
26.4	监督和管理	本次竞争性磋商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。
26.5	关注	潜在供应商须递交响应文件截止时间前在青岛市政府采购网（www.ccgp-qingdao.gov.cn）上注册并关注该项目，否则无法上传电子响应文件。
26.6	采购文件是否包含可能实质性变动的技术、服务要求以及合同草案条款内容。	☑ 不包含 ☐ 包含，详见第四章带“◆”标注内容。

第三章　供应商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（如营业执照、登记证书、执业许可证等）	是
2	声明函	电子文档	在经营活动中无重大违法记录和行贿犯罪记录、具有良好商业信誉和健全财务会计制度、具有依法缴纳税收和社会保障资金良好记录的声明函	是
3	崂山区公共资源交易网	电子文档	供应商必须在开标截止时间前在崂山政务网（http://www.laoshan.gov.cn）公共资源交易模块“诚信考核”注册，提供加盖供应商公章的企业完成注册截图。	是
4	政府采购诚信承诺书	电子文档	政府采购诚信承诺书	是

备注：

1、必须提交的证明材料未提交或提交不全的视为资格性审查不合格。

2、供应商的资格证明材料应当真实、有效、完整，字迹、印章要清晰。

青岛汇嘉招标项目管理有限公司
3702030304367

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，质量达到国家有关标准，成交供应商供货时应当提供有关货物的合格证明材料等。

1.3 供应商应保证货物是全新、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。成交供应商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成交供应商应对由于设计、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。采购人确需采购进口产品的，应在采购活动开始前，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，方可采购进口产品，否则采购人不得采购进口产品，供应商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报价。

2.采购产品技术规格、要求和数量（包括附件、图纸等）

一、　项目背景

国家电子政务外网是根据中办发〔2002〕17号文件和〔2006〕18号文件要求建设的政务网络平台，是服务于各级党委、人大、政府、政协、法院和检察院等政务部门，满足其经济调节、市场监管、社会管理和公共服务等方面需要的政务公用网络。

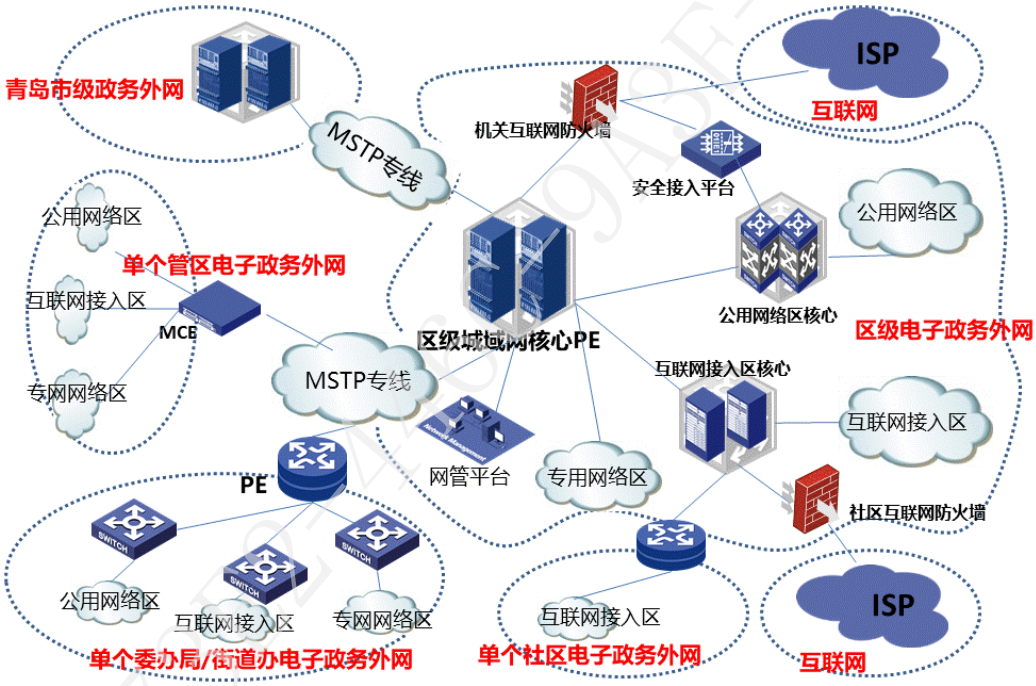
山东省电子政务外网是我省电子政务网络的重要组成部分，是国家电子政务外网在我省的延伸，目前山东省电子政务外网由外网公共服务域和行政服务域两部分组成。

青岛市于2015年根据国家电子政务外网的技术要求对市级电子政务外网公共服务域进行优化提升，通过启用BGP、MPLS VPN等技术和必要的安全措施，将市级政务外网公共服务域划分为公用网络区（金宏网对应公共服务域的公用网络区）和互联网接入区，

建成物理线路和设备共享、业务逻辑隔离的非涉密的电子政务基础网络平台，能够顺利承接国家和省延伸到我市的业务应用。公用网络区为非涉密的内部办公网，与国家、省电子政务外网公共服务域互联互通，市、区（市）、街道（乡镇）三级机关全面互联，与互联网通过数据安全交换平台进行数据交换，以便实现公共服务与内部业务流转的衔接。互联网接入区与互联网逻辑隔离，用于市级机关访问互联网，提供网上公共服务。

目前，崂山区按照青岛市政府的统一部署要求，顺利完成了电子政务外网改造。已将原有的社区外网、金宏网利用 MPLS VPN 技术，整合成崂山区电子政务外网。新的崂山区电子政务外网在网络层次机构中，属于崂山区城域网；同时改变了原有区属局委办、街道办、各个管区的网络接入方式。这些单位已经按照统一的规划，以 MPLS VPN 方式统一接入到崂山区新的电子政务外网中。电子政务外网已经涵盖了区政府，区属局委办，街道办，管区全部的金宏和互联网网络。

崂山区电子政务外网拓扑图如下：



从近两年崂山区电子政务外网运行情况来看，崂山区电子政务外网所实现的网络功能、网络响应效率，网络的健壮性、安全性和可靠性均已达到了原设计要求。但随着网络威胁形式的多样化和复杂化，现在的网络攻击和病毒等不仅扩散速度快，其攻击手段也越来越繁杂，攻击对象包括移动端、桌面端、嵌入式设备、网站和各种信息系统等。崂山区电子政务外网中已经部署的防火墙等常规安全设备所能提供的防御功能已经不

能满足当下网络安全需求。一段时间以来，崂山区电子政务和大数据中心多次收到上级相关部门转发的安全事件通报。另外，崂山区电子政务外网尚不具备对各类安全事件识别、报警和分析的能力，及对网络数据解码、检测、分析、诊断的能力。在目前日益严峻的信息安全大环境下，崂山区电子政务外网需要的不仅仅是一个综合的安全设备管理技术或管理工具，而是一个能够将整体的安全组织、安全策略、安全技术、安全风险、安全事件、安全操作等统一的管理并保证其运转有效的一个平台。在此平台下，通过威胁情报系统主动收集崂山区电子政务外网中所有业务相关安全风险，并与崂山区网络空间中的 IP 资产进行关联，分析出可能受影响的资产范围，提前了解网络系统可能遭受的攻击和潜在的安全隐患。结合监测对象的特征，第一时间实现应急闭环响应。根据不同业务特征，分别启动应急预案，包括：事件预防及预警机制、应急处置、应急响应保障措施等。

为了解决以上问题，本项目将在崂山区电子政务外网现有的基础之上，进行必要安全提升建设，以便能够充分应对新形势下安全攻击的威胁和风险。

二、 项目采购内容

2.1 采购要求

本次项目中，采购人以购买服务的方式，委托供应商对崂山区电子政务外网进行安全提升建设并进行后期的安全服务。

★供应商必须提供满足采购人标书中要求的性能、功能的软硬件设备来进行崂山区电子政务外网安全提升建设，加强崂山区电子政务外网的安全体系，不允许其它业务共享使用本项目内的相关设备。

本次项目内容包括优化提升崂山区电子政务外网安全所需要的全部安全软硬件设备、项目建设所需要的系统集成、软件开发、安全管理、安全服务，本次项目中使用到的各类安全设备、专用硬件以及各组成部分之间所必须的网络互联跳线等各类耗材费用，均计入本项目。

本项目共 1 包。供应商提供的安全设备必须根据采购人要求部署在指定位置。采购人以支付服务费的形式结算。与本次崂山区外网安全提升相关的技术实施工作内容将全部包含在本次服务费中，采购人不再单独支付相关费用。

2.2 项目要求

2.2.1 整体要求

（1）贴合实际，符合等保要求

根据目前崂山区电子政务外网进行实际综合安全分析考量，同时结合积极防御、综合防范的方针策略和等级保护的原则对这些系统进行整体设计，使得崂山区电子政务外网满足等保 2.0 中关于三级防护要求。必须确保外部安全问题进不来，内部安全问题出不去。

（2）注重整体，重视联动

结合崂山区电子政务外网现有情况，面向未来发展目标和需求，进行安全系统的体系建设，通过合理部署安全产品来进行有效的监测和防御，保证系统安全性不断增长的需要，确保崂山区整个电子政务外网系统安全可靠。

（3）注重落地，重视服务

在安全策略制定上，要尽量考虑安全机制的合理性，对重点信息资源，实现重点保护。在保证安全的前提下，尽量减少安全机制的规模和复杂性，使之具有可操作性，避免因过于复杂而导致安全措施难以执行。严格按照实际需求制定安全策略，保障网络信息系统安全可靠。提供统一的安全管理、安全运维、安全服务等手段，保障业务系统、监控系统、数据分析系统等可持续运行。

（4）注重预警，加强控制

对检测出来的安全事件，进行合规并有效的处理，强化安全管控细粒度。加强对网络攻击行为、应用攻击行为、数据窃取行为的防护和检测，及时发现和阻断外部恶意人员和内部违规人员的非法操作，并全面留存电子证据以备查证，确保非法人员非法操作走不脱。

（5）着眼未来，实现可持续安全运营

以崂山区电子政务外网 IT 资产为基础，以业务信息系统为核心，以维护体验为指引，从监控、审计、风险和运维四个维度建立起来的一套可度量的统一业务支撑平台，能够对业务信息系统进行可用性与性能的监控、配置与事件的分析审计预警、风险与态势的度量与评估、安全运维流程的标准化、例行化和常态化，最终实现业务信息系统的持续安全运营。

2.2.2 公用网络区安全提升要求

崂山区电子政务外网公共服务域公用网络区出口边界处，包括崂山区电子政务外网与市电子政务外网边界、崂山区各委办局/街道办与区电子政务外网边界等处部署下一代防火墙设备，通过访问控制策略严格限制外部网络到内部网络的访问；在下一代防火

墙设备中增加IPS功能,对通过下一代防火墙过滤的数据流量再进行应用级的安全防护;部署上网行为管理设备，对网络流量进行审计，详细了解用户的一些网络行为，便于溯源和流量统计，为网络安全维护人员后续安全规则调整提供必要的依据。部署高级威胁网络防护系统保护网络流量的安全，检测并拦截进出崂山区政务外网数据流量的恶意行为，威胁攻击。确保外部安全问题进不来，内部安全问题出不去。在充分利用现有的网络防病毒系统基础上，增加终端准入设备。对于没有安装防病毒系统的终端和服务器将阻止其接入到公共网络区。

此区域安全提升所需设备参数要求如下：

公用网络区	
下一代防火墙（至少3台）	1、硬件指标：★双电源；最大吞吐量≥25Gbps，并发连接数≥500 万，标准配置≥6个10/100M/1000M自适应千兆电接口、≥4个千兆SFP接口（含光模块）及≥4个万兆SFP+。≥5个接口扩展槽。标配60G SSD硬盘； 服务期内提供入侵防御特征库升级授权及硬件维保； 2、访问控制：基于状态检测技术；支持路由、透明及混合模式； 可针对源接口、目的接口、协议类型、源地址、目的地址、服务和报文通讯时间等对象设定安全策略； 3、网络特性：支持静态路由、RIP、OSPF及BGP动态路由、策略路由和组播路由； 4、虚拟化：支持基于硬件Hypervisor技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的CPU、内存、接口等资源。提供虚拟防火墙Hypervisor层资源配置管理界面截图。每个虚拟防火墙均提供完整的安全功能,包括防火墙、入侵防御、防病毒、上网行为管理和流控、VPN、IPv4/IPv6双栈等。 5、开通入侵防御功能，支持路由、透明、混合等各种工作模式下的网络病毒检测;支持专利级的基于网络数据流的网络病毒检测方法;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。 6、高级持续威胁防御：支持扩展APT检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和0DAY攻击的有效防护。 7、威胁情报防护：支持基于威胁情报云的动态防护功能，防火墙支持将用户对互

	联网的访问信息发送至威胁情报云进行实时情报查询及防护。支持 IPv4 和 IPv6 环境下威胁情报查询和实时防护 8★安全联动：支持与现有网络中的入侵检测（IDS）设备的联动，可接收 IDS 产品发送的动态访问控制策略； 9、支持广域网双边优化，通过使用 TCP 动态拥塞控制、TCP 窗口处理机制优化、TCP 选择性应答、使用快速 TCP 协议传输以及数据压缩机制，实现对业务访问的有效加速。通过 WAN 虚拟化技术实现多条链路捆绑，同一个 session 数据可以在多条链路上同时传输，加速大文件复制业务； 10、集中管理：支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。 支持扩展集中策略分析模块，通过集中策略分析模块，实现：集中对所有防火墙安全策略进行冗余分析、宽松策略分析、命中频率分析、潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的，
上网行为管理（至少 2 台）	★1、网络吞吐量≥12Gb，应用层吞吐量≥2.2Gb，支持用户数≥10000，每秒新建数≥20000，最大并发数≥800000，2U 硬件设备，采用标准 x86 架构，设备接口≥6 个千兆电口，2 个万兆光口 ≥1 个串口(RJ45) ，内存≥8G，≥2 个 USB2.0，硬盘≥1TB；服务期内提供特征库升级授权及硬件维保； 2、Web 访问质量监测：针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向 web 访问质量检测。 3、共享接入管理（防共享）：设备能够发现私接路由（或者共享软件等）共享网络的行为：支持自定义配置终端数量和冻结时间，和添加信任列表；支持显示以 IP 或用户名的维度统计一段时间内的趋势图。支持例外排除功能：如指定例外条件为 1 台 PC，2 个终端。则只有当 PC 或终端数超过例外条件才会被判定为共享。 ★4、应用标签功能分类管理：（1）支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖 6 大类；（2）支持给每个应用自定义标签；（3）支持根据标签选择一类应用做控制；支持对每一种应用的定义和解释，帮助客户快速定位应用的分类；（4）支持给每一种应用列上图标，易于客户了解应用的特征。

	5、支持 SSL 加密内容审计和过滤：针对 SSL 加密的网站、论坛发帖、web 邮箱的内容进行关键字过滤和内容审计；支持 SSL 硬件加速卡解密，从而可提高 SSL 全流量解密性能；支持加密证书自动分发：审计 SSL 网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台 PC 单独安装证书的问题； 6、加密 SMTP 邮件过滤：支持对加密 HTTPS、SMTP-SSL、SMTP 的邮件进行关键字过滤；加密 SMTP、POP3 邮件审计：支持对加密 HTTPS、POP3-SSL 、POP3、IMAP 、IMAP-SSL、SMTP-SSL、SMTP 邮件内容的审计。 7、针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）；支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱 8、支持 PPS 异常、丢包异常、ARP 异常、内网 DOS 攻击等异常情况实时监测，显示每日异常事件个数及情况。支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略。支持针对用户认证的故障进行分析，给出错误详情以及处置建议。 9、支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。支持基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中。
高级威胁网络防护系统（至少 2 台）	★1、高级应用防护 ＋ 防病毒功能开启性能≥2Gbps ；最大并发会话数≥77 万；每秒新建会话数≥5 万；2×千兆电口,；可扩展 2 口/4 口 bypass 千兆电卡；或者 2 口/4 口 bypass 千兆光纤卡（含多模/单模光纤模块）；或者 2 口 bypass 万兆光纤卡（含多模/单模光纤模块）。支持设备故障检测、链接失败检测、故障直通、硬件状态检测。服务期内提供防病毒库升级授权及硬件维保； 2、支持防恶意软件功能：防已知恶意软件（病毒、木马、蠕虫、后门、加密勒索软件、间谍软件、灰色软件、Rootkits 等）；具有高级未知恶意程序侦测及分析能力，可提供详细高级未知恶意程序的分析报告，并且可以进一步进行拦截。 ★3、支持 APT 防护功能：C&C 违规外联及僵尸网络检测及拦截；已知文档漏洞检测及拦截；未知文档漏洞及零日文档漏洞检测及拦截；可与 APT 增强侦测模块 TDA 联动，获取 APT 增强侦测模块 TDA 侦测到的本地 C&C 黑名单，并阻止 C&C 违规外联；

	可提交可疑文件、URL、IP 及域对象至 APT 增强定制化沙箱模块 DDAn 做联动分析，并根据 DDAn 的分析结果做进一步处理。 4、防病毒文件扫描客户可自定义大小，最大可支持 2G 5、VPN 支持双因素认证，保证用户安全性 6、病毒识别码≥3,000,000+种病毒识别码，每年约新增 735,000+识别码；全球病毒实验室+本地病毒实验室支持；本地病毒特征码（至少百分之 20 是中国的特征码)。 7、支持基于策略（源和用户/目标/通讯类型/时段）的带宽控制；支持上行流量/下行流量的带宽控制； 支持最大带宽限制/最小带宽保证；支持带宽服务优先级。终端管理支持本地用户及 LDAP 用户（MS Active Directory 及 Open LDAP）管理；支持本地用户及 LDAP 用户认证和识别，支持网页认证及透明认证方式；支持不同用户分组利用策略分类管理。 8、部署可支持桥接模式、路由模式、监控模式（旁路模式)、混杂模式（桥接+路由）、多路 ISP & WAN 模式。 9、支持中文管理界面，支持 WEB 界面，通过加密的 SSL 访问控制台，支持 snmp 管理。 10、支持自动/手动在线升级，可配置自动升级周期;全球升级架构以及本地升级源的设计，降低升级带宽使用。 11、提供安全日志的查询/打印/导出；可按照时间，协议，威胁类型等查询条件查询日志；支持 Syslog 协议，可以实时传输日志到 Syslog 服务器。 报告系统提供日/周/月图形化报表，以及实时图形化报表；提供按源用户/源地址生成报告；提供恶意软件事件安全报告。 12、支持安全信息汇总/监控硬件异常/系统资源警告/预设更新等通知；CPU 阀值/数据分区阀值/硬盘容量阀值/交换内存阀值监视警告等；产品中所用的防病毒引擎，病毒代码，防病毒扫描原理，APT 侦测等都必需为厂商自有技术，非 OEM 或引入其他厂商技术，以保证服务支持的连续性，和技术维护的一贯性。
终端准入管理系统（1 套）	★1、设备配置 1 个串口，配置≥6 个千兆以太网电口，配置≥2 个万兆光口，设备提供≥3 个网卡扩展槽；设备存储空间≥2TB SATA 硬盘，提供冗余电源。设备吞吐量≥2Gbps，支持集成公用网络区已有病毒防护及终端管理软件，实现统一的合规

	管理、日志审计、访问控制等。配置的终端管控数量授权≥3000 终端，服务期内提供软件升级服务及硬件维保； 2、设备采用旁路部署方式，支持针对不同区域采用不同组合合规管控技术。支持有线、无线基于应用准入的合规管控，支持配置保护服务器区域、例外终端等灵活的配置方式； 3、支持健康合规检查策略，采用动态检测技术，需支持多种检查机制，至少支持入网检查、定时检查、周期检查机制，针对接入内部网络的计算机终端实行多种安全检查策略，支持分组策略下发控制，拦截不安全终端接入网络。支持终端安全检查失败处置措施，可基于协议、特定端口、端口范围、特定地址、IP 范围、URL 来控制终端访问权限，从而无需操作交换机达到终端网络隔离目的，实现细粒度的访问控制管理。支持对不合规的终端提供软隔离，不符合安全策略的计算机终端进行友好提示，提供终端修复向导，需支持引导修复和一键修复功能，并支持不同区域终端的修复区域定义。支持对文件共享检查，检查终端用户是否存在共享目录。支持对不同类别补丁完整性检查，检查类别：高危漏洞、软件安全更新、可选高危、其他及功能性补丁，并对未安装的 PC 进行引导安装，支持自定义必须安装和禁止安装补丁。支持外设使用安全检查，检查是否插入自动运行风险性 U 盘。支持对关键位置注册表的检查，关键位置文件检查；检查指定的可疑文件或可疑注册表项" 4、支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件。支持文件系统实时防护，间谍文件监控，局域网病毒拦截，宏病毒免疫，DLL 劫持免疫等功能。对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置。支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件；支持手工导入 MD5+SHA1 的黑白名单方式，支持 txt 批量导入方式。支持下发忽略白名单的病毒扫描。支持对 windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理。对敲诈者病毒提供专有的防护功能； ★5、支持文件操作的监控和防护，可设置包括但不限于读，写，执行，重命名，链接等权限的监控和防护。实现文件防篡改功能。支持例外列表。支持基于操作系统内核加固技术，针对操作系统核心资源，如注册表、系统文件、进程等资源进行有效防护。包括但不限于对更改系统可执行文件，监听原始套接字，添加定时任务，

	添加系统启动项等多种风险行为的监控和阻断。具有防暴力破解技术，能有效防御针对 RDP、SSH 的暴力破解，适用各类型的服务器； 6、支持按 CVE 编号查询漏洞，支持按 KB 号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况，如果还有未修复的终端则可立即下发修复任务。具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端 P2P 补丁分发加速，有效节省外网带宽资源。提供补丁的详细通告情况，包含不限于补丁号、补丁的级别、对应产品、漏洞影响、CVE-ID、是否被公开披露、是否已受攻击、漏洞被利用的概率等； 7、支持根据检查项通过率的百分比评定终端配置的脆弱程度，定性的标准可由管理员自定义。.风险评估检查项至少包括身份鉴别、安全审计、访问控制、资源控制、入侵防范几个方面，且可进行扩充。支持自定义网络安全访问控制、数据泄漏控制、账户访问控制、账户权限控制等方面的检查项配置，可有效预防未加固系统容易被攻击者在未授权的情况下访问或破坏系统的情况； 8、通过异常行为检测引擎，能够对终端异常行为（异常域名请求、非法 IP 访问、敏感命令执行、恶意启动项创建等）进行实时告警，并能够还原攻击路径。黑客通过沦陷终端进行勒索病毒投递行为，进行实时检测判断，能够对进程中产生勒索病毒行为特征进行实时告警，并能完整还原攻击路径。能够对常见黑客使用的无文件攻击行为，例如通过 cmd、powershell、wmic 等进程执行不落硬盘而直接在内存加载的攻击行为，提供威胁检测与告警能力。能够对常见本地账号密码凭证窃取的攻击行为进行检测，例如 mimikatz、hashdump 等。对可疑进程行为产生告警信息，并对攻击路径完整溯源，以树状结构展示所有的危害动作，以及产生的路径。帮助管理员对威胁告警进行威胁确认，以及影响评估。提供威胁情报能力，形式包括 IP、域名、hash 等。当采集数据与威胁情报进行匹配后，对恶意行为数据进行告警，并提供详细威胁上下文信息描述。" ★9、支持控制中心防暴力破解，采用手机 APP 动态令牌方式进行二次认证，针对控制中心高危操作支持动态口令验证，要求令牌 APP 自主研发。支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；客户端程序具备自保功能，避免被恶意篡改。

2.2.3 互联网接入区安全提升

崂山区电子政务外网互联网接入区中已经部署了相对完善的信息安全防护措施。但在新的网络安全形势下，仍然需要进一步的安全提升，以增强安全检测和防御能力。通过互联网接入区现有的设备日志数据分析，在目前已知发生安全事件的类型中，感染计算机病毒、蠕虫和木马程序依然十分突出，其次是网络攻击和端口扫描、网页篡改和垃圾邮件。

本项目将在互联网接入区部署下一代防火墙设备，替换现网中已经达到报废年限的防火墙设备。通过访问控制策略严格限制外部网络到互联网接入区的访问。下一代防火墙具备 IPS 功能，对通过下一代防火墙过滤的数据流量再进行应用级的安全防护；部署上网行为管理设备，替换现网中已经达到报废期的上网行为管理设备，对网络流量进行审计，详细了解用户的一些网络行为，便于溯源和流量统计，为网络安全维护人员后续安全规则调整；提供必要的依据部署高级威胁网络防护系统保护网络流量的安全，检测并拦截进出崂山区政务外网数据流量的恶意行为，威胁攻击。确保外部安全问题进不来，内部安全问题出不去；部署抗 DDoS 系统，使其与现网中已经部署的 DDoS 系统形成集群部署，在增加性能的基础上，对互联网接入区的 WEB 应用进行精准防护，特别是针对 HTTP/HTTPS、NTP、DNS 等应用层拒绝服务类和 TCP/UDP、ICMP 等网络层拒绝服务类攻击提供更佳的检测和防护；部署互联网接入区网络防病毒系统，增加终端准入设备。对于互联网接入区没有安装防病毒系统的终端和服务器将阻止其接入到互联网接入区网络。

此区域安全提升所需设备参数要求如下：

抗 DDoS 攻击系统（至少 2	★1、硬件规格：软硬一体设备，专用硬件平台和安全操作系统，整机抗攻击能力 4Gbps。2 个 GE 管理口，8 个 100/1000M Base-TX 业务口，4 个 SFP 插槽；5 个扩展槽，双电源。服务期内提供硬件维保和技术支持服务； 2、抗攻击功能：防御流量型 flood 攻击 ：SYN Flood 、SYN-ACK Flood、 ACK Flood、FIN/RST Flood、ICMP Flood、SIP Flood、UDP Flood、IP Fragment Flood、Stream flood 等。防御 UDP Flood 攻击：必须提供 2 层防护，要求包括 UDP 防御阈值设置以及丢弃 UDP 碎片。ACK Flood 攻击提供 TCP 防御阈值设置，同时必须提供 ACK 限速手段进行防护，开启时不影响客户在线业务。支持流量自学习功能，通过对正常网络环境中 SYN、ACK、UDP 及 ICMP 等协议流量的统计分析，根据内置的算法得到相应的防护策略，并可以生成防护群组模板，支持自动防护，系统开启自动防护后，无需撰写任何规则对所有

台）	服务器进行 DDoS 防护，也可针对特定服务器撰写特定防护规则。 3、支持 IPV4/IPV6 双栈流量清洗 4、异常流量管理：支持自定义包大小限制，自定义数据包大小、特征字符出现的频率限制，必须提供数据匹配或正则匹配选项，对匹配的数据包进行丢弃、放行、对源目 IP 加黑名单等操作。支持配置 url 访问控制策略，直接针对域名、IP 以及端口等对连接进行限制 支持基于源 IP、目的 IP、源端口、目的端口、协议的五元组抓包功能；必须支持对输入滤前/滤后、输出滤前/滤后、输入拦截、输出拦截、双向滤前、双向滤后、双向拦截等条件抓取指定数据包，指定抓包数量和抓包比例；串行部署时进行双向会话管控，能够设置从外到内的连接阈值，同时必须能够设置从内到外的连接阈值。 5、日志报表：提供攻击事件和攻击详情。提供攻击源 IP、被攻击 IP、防护域、攻击类型、攻击事件、总流量、攻击流量、峰值流量等信息；支持按被攻击 IP、防护域、攻击时间等查询特定的攻击事件；支持导出 DOC、EXCEL、PDF、HTML、RTF 格式的攻击事件和攻击详情。支持攻击动态地图展示，显示全球范围内攻击源目 IP 所在地理位置 可设置访问客户端 IP 黑白名单，对客户端 IP 进行访问控制，提供允许访问和不允许访问两种方式。支持微信告警，通过微信公众号发送防护 IP，接口，CPU，内存，磁盘等告警信息。 ★6、高可靠性：与现网中的 DDoS 设备实现集群部署，支持在大流量攻击发生时手动或自动启动集群，保证整个系统可用性；支持集群设备间数据状态同步、配置同步，支持集群无限扩容。
下一代防火墙（互联网主出口，至少 2 台）	★1、硬件指标：双电源；最大吞吐量≥25Gbps，并发连接数≥500 万，标准配置 6 个 10/100M/1000M 自适应千兆电接口、4 个千兆 SFP 接口（含光模块）及 4 个万兆 SFP+，5 个接口扩展槽。标配 60G SSD 硬盘；服务期内提供入侵防御特征库升级授权及硬件维保； 2、访问控制：基于状态检测技术；支持路由、透明及混合模式； 可针对源接口、目的接口、协议类型、源地址、目的地址、服务和报文通讯时间等对象设定安全策略；

	3、网络特性：支持静态路由、RIP、OSPF 及 BGP 动态路由、策略路由和组播路由； 4、虚拟化：支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。提供虚拟防火墙 Hypervisor 层资源配置管理界面截图。每个虚拟防火墙均提供完整的安全功能，包括防火墙、入侵防御、防病毒、上网行为管理和流控、VPN、IPv4/IPv6 双栈等。 5、开通入侵防御功能，支持路由、透明、混合等各种工作模式下的网络病毒检测；支持专利级的基于网络数据流的网络病毒检测方法；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。 6、高级持续威胁防御：支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 0DAY 攻击的有效防护。 7、威胁情报防护：支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。支持 IPv4 和 IPv6 环境下威胁情报查询和实时防护 8★安全联动：支持与现有网络中的入侵检测（IDS）设备的联动，可接收 IDS 产品发送的动态访问控制策略； 9、支持广域网双边优化，通过使用 TCP 动态拥塞控制、TCP 窗口处理机制优化、TCP 选择性应答、使用快速 TCP 协议传输以及数据压缩机制，实现对业务访问的有效加速。通过 WAN 虚拟化技术实现多条链路捆绑，同一个 session 数据可以在多条链路上同时传输，加速大文件复制业务； 10、集中管理：支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。支持扩展集中策略分析模块，通过集中策略分析模块，实现：集中对所有防火墙安全策略进行冗余分析、宽松策略分析、命中频率分析、潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的。

下一代防火墙（部门业务系统专线出口，至少 1 台）	★1、硬件指标：双路供电电源；最大吞吐量≥14Gbps，并发连接数≥300 万，标配 16 个 10/100/1000M 自适应千兆电接口，2 个千兆 SFP 接口及 4 个 SPF+万兆接口（含光模块）；标配 60G SSD 硬盘； 服务期内提供硬件维保； 2、访问控制：基于状态检测技术；支持路由、透明及混合模式； 可针对源接口、目的接口、协议类型、源地址、目的地址、服务和报文通讯时间等对象设定安全策略； 3、网络特性：支持静态路由、RIP、OSPF 及 BGP 动态路由、策略路由和组播路由； 4、虚拟化：支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源； 5、支持入侵防御和防病毒功能，支持路由、透明、混合等各种工作模式下的网络病毒检测；支持专利级的基于网络数据流的网络病毒检测方法；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； 6、高级持续威胁防御：支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 0DAY 攻击的有效防护； ★7、安全联动：支持与现有网络中的入侵检测（IDS）设备的联动，可接收 IDS 产品发送的动态访问控制策略； 8、支持广域网双边优化，通过使用 TCP 动态拥塞控制、TCP 窗口处理机制优化、TCP 选择性应答、使用快速 TCP 协议传输以及数据压缩机制，实现对业务访问的有效加速。通过 WAN 虚拟化技术实现多条链路捆绑，同一个 session 数据可以在多条链路上同时传输，加速大文件复制业务； 1、集中管理：支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。 支持扩展集中策略分析模块，通过集中策略分析模块，实现：集中对所有防火墙安全策略进行冗余分析、宽松策略分析、命中频率分析、潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的。

IPS（社区互联网出口，至少1台）	★1、硬件指标：最大吞吐量≥25Gbps，1个RJ-45 Console口，2个10/100/1000 Base-T带外管理口，4个具备BYPASS功能的10/100/1000Base-T接口，4个千兆光口（含光模块），2个具备bypass功能的万兆SFP+多模接口（含SFP+多模光口模块），1个扩展插槽，2个USB口，双电源，服务期内提供入侵防御特征库升级授权及硬件维保； 2、支持入侵防御事件库在线自动升级和手工导入，入侵事件特征库升级率不少于一周一次； ★3、支持扩展无线攻击检测和防护功能扩展，可手工或自动识别和区分内部AP和外部AP，也可以手工或自动识别合法终端，并基于此设定无线准入策略，通过射频信号阻止非法AP、终端的接入。支持无线扫描、欺骗、DoS、破解等常见无线网络攻击行为的检测、告警、阻断功能，同时支持多种类型流氓AP的检测与阻断。 4、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；系统需提供口令保护功能，能够探测和阻止恶意暴力口令猜测行为，要求支持至少16种应用的口令穷举猜测； 5、系统应支持威胁情报，通过获得第三方的威胁情报，提升防御能力； 6、支持重点资产和应用监控功能，通过对重点资产和应用的工作状态进行检测，当出现异常时，可以syslog和邮件进行告警，并可以记录日志； 8、提供WEB登录图像验证码功能，防止暴力破解；支持场景分析功能，提供进行更深入的分析能力，至少包括僵尸木马蠕虫的分布式攻击场景分析； 9、系统能够检测敏感信息的外泄行为并阻止传输行为，有效保护用户的知识资产，支持检测和防范的对象包括但不限于：信息和文件中的关键字，身份证、手机和固定电话号码、银行卡、IP地址等信息监控，重要数据文件保护等。并可以设置白名单。除关键字外，还需要支持文件指纹识别能力。
高级威胁网络防护系统（互联网主出口，	★1、产品性能配置：高级应用防护 ＋ 防病毒模块功能开启性能≥4Gbps；最大并发会话数≥200万；每秒新建会话数≥10万；2×千兆电口，2×10G 光含模块；可扩展2口/4口/6口 bypass千兆电卡；或者2口/4口 bypass千兆光纤卡（含多模/单模光纤模块）；或者2口/4口 bypass万兆光纤卡（含多模/单模光纤模块）。支持设备故障检测、链接失败检测、故障直通、

至少 2 台）	硬件状态检测。 2、支持防恶意软件功能：防已知恶意软件（病毒、木马、蠕虫、后门、加密勒索软件、间谍软件、灰色软件、Rootkits 等）；具有高级未知恶意程序侦测及分析能力，可提供详细高级未知恶意程序的分析报告，并且可以进一步进行拦截。 ★3、支持 APT 防护功能：C&C 违规外联及僵尸网络检测及拦截；已知文档漏洞检测及拦截；未知文档漏洞及零日文档漏洞检测及拦截；可与 APT 增强侦测模块 TDA 联动，获取 APT 增强侦测模块 TDA 侦测到的本地 C&C 黑名单，并阻止 C&C 违规外联；可提交可疑文件、URL、IP 及域对象至 APT 增强定制化沙箱模块 DDAn 做联动分析，并根据 DDAn 的分析结果做进一步处理。 4、防病毒文件扫描客户可自定义大小，最大可支持 2G 5、VPN 支持双因素认证，保证用户安全性 ★6、病毒识别码≥3,000,000+种病毒识别码，每年约新增 735,000+识别码；全球病毒实验室+本地病毒实验室支持；本地病毒特征码（至少百分之 20 是中国的特征码）。 7、支持基于策略（源和用户/目标/通讯类型/时段）的带宽控制；支持上行流量/下行流量的带宽控制；　支持最大带宽限制/最小带宽保证；支持带宽服务优先级。 终端管理支持本地用户及 LDAP 用户（MS Active Directory 及 Open LDAP）管理；支持本地用户及 LDAP 用户认证和识别，支持网页认证及透明认证方式；支持不同用户分组利用策略分类管理。 8、部署可支持桥接模式、路由模式、监控模式（旁路模式）、混杂模式（桥接+路由）、多路 ISP & WAN 模式。 9、支持中文管理界面，支持 WEB 界面，通过加密的 SSL 访问控制台，支持 snmp 管理。 10、支持自动/手动在线升级，可配置自动升级周期;全球升级架构以及本地升级源的设计，降低升级带宽使用。 11、提供安全日志的查询/打印/导出；可按照时间，协议，威胁类型等查询条件查询日志；支持 Syslog 协议，可以实时传输日志到 Syslog 服务器。

	12、报告系统提供日/周/月图形化报表，以及实时图形化报表；提供按源用户/源地址生成报告；提供恶意软件事件安全报告。 13、支持安全信息汇总/监控硬件异常/系统资源警告/预设更新等通知；CPU 阀值/数据分区阀值/硬盘容量阀值/交换内存阀值监视警告等； 14、产品中所用的防病毒引擎，病毒代码，防病毒扫描原理，APT 侦测等都必需为厂商自有技术，非 OEM 或引入其他厂商技术，以保证服务支持的连续性，和技术维护的一贯性。
高级威胁网络防护系统（社区互联网出口，至少 1 台）	★1、高级应用防护 ＋ 防病毒功能开启性能≥2Gbps ；最大并发会话数≥80 万；每秒新建会话数≥5 万；2×千兆电口,；可扩展 2 口/4 口 bypass 千兆电卡；或者 2 口/4 口 bypass 千兆光纤卡（含多模/单模光纤模块）；或者 2 口 bypass 万兆光纤卡（含多模/单模光纤模块）。支持设备故障检测、链接失败检测、故障直通、硬件状态检测。服务期内提供防病毒库升级授权及硬件维保； 2、支持防恶意软件功能：防已知恶意软件（病毒、木马、蠕虫、后门、加密勒索软件、间谍软件、灰色软件、Rootkits 等）；具有高级未知恶意程序侦测及分析能力，可提供详细高级未知恶意程序的分析报告，并且可以进一步进行拦截。 ★3、支持 APT 防护功能：C&C 违规外联及僵尸网络检测及拦截；已知文档漏洞检测及拦截；未知文档漏洞及零日文档漏洞检测及拦截；可与 APT 增强侦测模块 TDA 联动，获取 APT 增强侦测模块 TDA 侦测到的本地 C&C 黑名单，并阻止 C&C 违规外联；可提交可疑文件、URL、IP 及域对象至 APT 增强定制化沙箱模块 DDAn 做联动分析，并根据 DDAn 的分析结果做进一步处理。 4、防病毒文件扫描客户可自定义大小，最大可支持 2G 5、VPN 支持双因素认证，保证用户安全性 6、病毒识别码≥3,000,000+种病毒识别码，每年约新增 750,000+识别码；全球病毒实验室+本地病毒实验室支持；本地病毒特征码（至少百分之 20 是中国的特征码）。 7、支持基于策略（源和用户/目标/通讯类型/时段）的带宽控制；支持上行流量/下行流量的带宽控制；　支持最大带宽限制/最小带宽保证；支持带

	宽服务优先级。 终端管理支持本地用户及 LDAP 用户（MS Active Directory 及 Open LDAP）管理；支持本地用户及 LDAP 用户认证和识别，支持网页认证及透明认证方式；支持不同用户分组利用策略分类管理。 8、部署可支持桥接模式、路由模式、监控模式（旁路模式）、混杂模式（桥接+路由）、多路 ISP & WAN 模式。 9、支持中文管理界面，支持 WEB 界面，通过加密的 SSL 访问控制台，支持 snmp 管理。 10、支持自动/手动在线升级，可配置自动升级周期;全球升级架构以及本地升级源的设计，降低升级带宽使用。 11、提供安全日志的查询/打印/导出；可按照时间，协议，威胁类型等查询条件查询日志；支持 Syslog 协议，可以实时传输日志到 Syslog 服务器。报告系统提供日/周/月图形化报表，以及实时图形化报表；提供按源用户/源地址生成报告；提供恶意软件事件安全报告。 12、支持安全信息汇总/监控硬件异常/系统资源警告/预设更新等通知；CPU 阀值/数据分区阀值/硬盘容量阀值/交换内存阀值监视警告等；产品中所用的防病毒引擎，病毒代码，防病毒扫描原理，APT 侦测等都必需为厂商自有技术，非 OEM 或引入其他厂商技术，以保证服务支持的连续性，和技术维护的一贯性。
上网行为管理（社区互联网出口，至少 1 台）	★1、网络吞吐量≥5.5Gb，应用层吞吐量≥750Mb，支持用户数≥500，每秒新建数≥8000，最大并发数≥400000，1U 硬件设备，采用标准 x86 架构，设备接口≥6 个千兆电口，2 个千兆光口 ≥1 个串口(RJ45），内存≥4G，≥2 个 USB2.0，硬盘≥128GB; 2、Web 访问质量监测：针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向 web 访问质量检测; 3、共享接入管理（防共享）：设备能够发现私接路由（或者共享软件等）共享网络的行为：支持自定义配置终端数量和冻结时间，和添加信任列表;支持显示以 IP 或用户名的维度统计一段时间内的趋势图。支持例外排除功

	能：如指定例外条件为 1 台 PC，2 个终端。则只有当 PC 或终端数超过例外条件才会被判定为共享； ★4、应用标签功能分类管理：（1）支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖 6 大类；（2）支持给每个应用自定义标签；（3）支持根据标签选择一类应用做控制；支持对每一种应用的定义和解释，帮助客户快速定位应用的分类；（4）支持给每一种应用列上图标，易于客户了解应用的特征。 5、支持 SSL 加密内容审计和过滤：针对 SSL 加密的网站、论坛发帖、web 邮箱的内容进行关键字过滤和内容审计；支持 SSL 硬件加速卡解密，从而可提高 SSL 全流量解密性能；支持加密证书自动分发：审计 SSL 网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台 PC 单独安装证书的问题； 6、加密 SMTP 邮件过滤：支持对加密 HTTPS、SMTP-SSL、SMTP 的邮件进行关键字过滤；加密 SMTP、POP3 邮件审计：支持对加密 HTTPS、POP3-SSL 、POP3、IMAP 、IMAP-SSL、SMTP-SSL、SMTP 邮件内容的审计； 7、针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）；支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱 8、支持 PPS 异常、丢包异常、ARP 异常、内网 DOS 攻击等异常情况实时监测，显示每日异常事件个数及情况。支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略。支持针对用户认证的故障进行分析，给出错误详情以及处置建议。 9、支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。支持基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中。
终端准入管理系统	★1、设备配置 1 个串口，配置≥6 个千兆以太网电口，配置≥2 个万兆光口，设备提供≥3 个网卡扩展槽；设备存储空间≥2TB SATA 硬盘，提供冗余电源。

（1 套）	设备吞吐量≥2Gbps，支持并且配置的终端管控数量授权≥3000 终端，提供≥3000 防病毒客户端。服务期内提供设备维保服务及规则库升级服务； 2、设备采用旁路部署方式，支持针对不同区域采用不同组合合规管控技术。支持有线、无线基于应用准入的合规管控，支持配置保护服务器区域、例外终端等灵活的配置方式； 3、支持健康合规检查策略，采用动态检测技术，需支持多种检查机制，至少支持入网检查、定时检查、周期检查机制，针对接入内部网络的计算机终端实行多种安全检查策略，支持分组策略下发控制，拦截不安全终端接入网络。支持终端安全检查失败处置措施，可基于协议、特定端口、端口范围、特定地址、IP 范围、URL 来控制终端访问权限，从而无需操作交换机达到终端网络隔离目的，实现细粒度的访问控制管理。支持对不合规的终端提供软隔离，不符合安全策略的计算机终端进行友好提示，提供终端修复向导，需支持引导修复和一键修复功能，并支持不同区域终端的修复区域定义。支持对文件共享检查，检查终端用户是否存在共享目录。支持对不同类别补丁完整性检查，检查类别：高危漏洞、软件安全更新、可选高危、其他及功能性补丁，并对未安装的 PC 进行引导安装，支持自定义必须安装和禁止安装补丁。支持外设使用安全检查，检查是否插入自动运行风险性 U 盘。支持对关键位置注册表的检查，关键位置文件检查；检查指定的可疑文件或可疑注册表项" 4、支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件。支持文件系统实时防护，间谍文件监控，局域网病毒拦截，宏病毒免疫，DLL 劫持免疫等功能。对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置。支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件；支持手工导入 MD5+SHA1 的黑白名单方式，支持 txt 批量导入方式。支持下发忽略白名单的病毒扫描。支持对 windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理。对敲诈者病毒提供专有的防护功能； ★5、支持文件操作的监控和防护，可设置包括但不限于读，写，执行，重

	命名，链接等权限的监控和防护。实现文件防篡改功能。支持例外列表。支持基于操作系统内核加固技术，针对操作系统核心资源，如注册表、系统文件、进程等资源进行有效防护。包括但不限于对更改系统可执行文件，监听原始套接字，添加定时任务，添加系统启动项等多种风险行为的监控和阻断。具有防暴力破解技术，能有效防御针对 RDP、SSH 的暴力破解，适用各类型的服务器； 6、支持按 CVE 编号查询漏洞，支持按 KB 号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况，如果还有未修复的终端则可立即下发修复任务。具备漏洞集中修复过程中的流量控制和保证带宽，补丁分发支持服务端带宽限流与客户端 P2P 补丁分发加速，有效节省外网带宽资源。提供补丁的详细通告情况，包含不限于补丁号、补丁的级别、对应产品、漏洞影响、CVE-ID、是否被公开披露、是否已受攻击、漏洞被利用的概率等； 7、支持根据检查项通过率的百分比评定终端配置的脆弱程度，定性的标准可由管理员自定义。风险评估检查项至少包括身份鉴别、安全审计、访问控制、资源控制、入侵防范几个方面，且可进行扩充。支持自定义网络安全访问控制、数据泄漏控制、账户访问控制、账户权限控制等方面的检查项配置，可有效预防未加固系统容易被攻击者在未授权的情况下访问或破坏系统的情况； 8、通过异常行为检测引擎，能够对终端异常行为（异常域名请求、非法 IP 访问、敏感命令执行、恶意启动项创建等）进行实时告警，并能够还原攻击路径。黑客通过沦陷终端进行勒索病毒投递行为，进行实时检测判断，能够对进程中产生勒索病毒行为特征进行实时告警，并能完整还原攻击路径。能够对常见黑客使用的无文件攻击行为，例如通过 cmd、powershell、wmic 等进程执行不落硬盘而直接在内存加载的攻击行为，提供威胁检测与告警能力。能够对常见本地账号密码凭证窃取的攻击行为进行检测，例如 mimikatz、hashdump 等。对可疑进程行为产生告警信息，并对攻击路径完整溯源，以树状结构展示所有的危害动作，以及产生的路径。帮助管理员对威胁告警进行威胁确认，以及影响评估。提供威胁情报能力，形式包括 IP、域名、hash 等。当采集数据与威胁情报进行匹配后，对恶意行为数据进行告警，并提供

	详细威胁上下文信息描述。" ★9、支持控制中心防暴力破解，采用手机 APP 动态令牌方式进行二次认证，针对控制中心高危操作支持动态口令验证，要求令牌 APP 自主研发。支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；客户端程序具备自保功能，避免被恶意篡改。

2.2.4 网络回溯分析系统

崂山区电子政务外网当前复杂的运行环境中，同样对回查历史网络流量的原始数据，提供网络流量的原始数据包存储和回溯查询能力有着强烈的需求。电子政务外网内具备专业的网络分析系统，就可以对链路流量、应用流量、故障告警相关流量、指定主机流量进行精准的回溯分析。从多角度还原历史场景，重组完整的会话信息。多维度展示网络中的流量组成、网络和应用的性能指标以及网络行为。提供端到端的全流量行为、性能的可视化分析能力，为网络调整提供可信的决策依据。

本次安全提升服务中对所需溯源分析系统参数要求如下：

网络回溯分析系统 （1 套）	★1、自带全流量数据存储空间≥32T、数据采集端口：≥2 个万兆光口+4 个光口；管理端口：≥2 个电口。数据流量处理能力不低于 5Gbps；数据包处理能力不低于 100 万 pps；TCP/UDP 会话处理能力不低于 20 万/秒； 2、支持实时全量数据包线速采集，分析及存储。 3、支持数据包采集过滤器配置，可基于源目的 MAC 地址、源目的 IP 地址、端口号、协议、数据包内容等多种条件对流量进行精细化过滤；支持多个过滤条件设置。 4、数据采集链路支持自定义多级目录，多链路数据聚合分析。 5、支持数据中心 MPLS、VXLAN 环境下数据采集分析，能自动识别 MPLS VPN、802.1q 和 Cisco ISL 的 VLAN 标记进行流量分类，并提供 MPLS VPN、VLAN 的单独视图显示。 6、支持数据包去重及截取功能，能按照任意数值自定义保留数据包长度。 ★7、支持原始通讯数据包回放，能提供服务端离线数据包导入模式，回放分析界面和功能与实时采集链路的相同。数据包格式包括并不限于：cap、pcap、cscpkt、rapkt 等主流数据包格式，而不需要借助第三方协议分析工具支持；

	8、支持采集设备独立部署独立工作，设备自身需具备图形化的数据分析界面，能够通过控制台软件对设备采集的数据进行精细化分析。 ★9、支持按照 1 秒钟、10 秒钟、1 分钟、10 分钟、1 小时，1 天等 6 种时间刻度进行数据回溯展现。 10、拖选时间窗口的任意时间段，能自动关联展现该时间段的概要统计、网络应用、IP 地址、物理地址、IP 会话、物理会话、TCP 会话、UDP 会话、警报日志等参数，并能对各指标参数 TOP N 升降序排名（同时展现的最大数量不少于 500,000）。 11、支持对任意网络对象的回溯分析，包括但不限于以下类型：IP 地址、移动终端、网络应用、IP 会话、TCP/UDP 会话。 12、支持提供网络中每个 IP 主机服务端口，服务端口的流量统计数据，并可以访问这些服务端口的所有客户端的流量信息。 13、支持统计分析所有 TCP 会话的通讯流量信息，包括接收发送流量，接收发送数据包等。能够分析会话的开始时间，持续时间，应用名称，应用协议类型，重传数量，分段丢失数量，重传率，分段丢失率，平均 ACK 时延，TCP 交易数量，最大响应时间，平均响应时间等，支持同时展现的 TCP 会话最大数量不少于 500,000。 14、提供针对 TCP 会话的时序图分析功能，能够图形化的显示 TCP 会话中的数据交互传输过程，能够图形化显示数据传输中的时间间隔。 15、提供针对 TCP/UDP 会话的流重组功能，将会话中的数据流重组显示。 16、应用响应时间测量和统计，包括：TCP 建立时间分析、客户端网络时延分析、服务器网络时延分析、应用响应时间分析，并能提供时延性能最差 TOPN 通信对（同时展现的最大数量不少于 500,000）。 17、应用响应结果统计：访问请求量、成功及失败响应量统计，访问量、成功及失败响应量 TOPN 服务器（同时展现的最大数量不少于 500,000）。 18、错误代码分布统计，错误种类包括：重传、Reset、TCP 窗口冻结等等 19、支持纳秒级的数据包记录与解码，实时监控刷新精度为 1 秒。刷新参数包括且不限于比特率、并发会话数、连接失败率、平均包长、TCP 重传率等； 20、能够针对特定域名，分析内网主机对该域名的解析详情，包括且不限于

	访问时间、IP 地址及访问成功与否，并能对该访问 IP 进行长时间的网络通讯会话还原。 21、能够对安全事件的网络流量通讯还原能力达到数据包级，可以追溯数据包 ASCII 编码内容、TCP 标志字段、TCP 选型、TCP 序列号、数据包时间戳。 22、支持自定义添加木马特征，包括 16 进制和 ASCII 码的特征，并能用偏移量，使用 tcp/udp 端口，网络协议，TCP 标志位，数据包大小等参数对特征进行严格匹配，减少误报。 23、提供独立的警报视图，用于同时展现流量警报、邮件敏感字警报、可疑域名警报、可疑 IP 警报、特征值警报。 24、警报触发时间间隔：1 秒钟、10 秒钟、1 分钟、10 分钟、1 小时，1 天.警报条件：能设定>=条件、<条件，多种参数条件的与或关系事件警报。 ★25、全面支持 IPv6 识别及分析。 26、支持对常见网络通信协议进行识别和解码分析，必须具备中英文双语协议解码能力，包括并不限于：各协议字段的名称的中英文展现，及字段内容的中英文注释。

2.2.5 安全态势感知平台

本项目需要建设一套面向崂山区电子政务业务信息系统，以业务为核心保障目标，致力于为崂山区提供全方位的态势感知能力的安全态势感知平台。

平台融合业界主流的大数据技术，结合 SQL、NewSQL 和 NoSQL 技术，实现对多元、异构、海量安全数据的高效可靠存储和高速检索。提供智能化关联分析、基于机器学习的行为分析，流安全分析技术，内建主动安全管理机制，通过主动的漏洞扫描和安全配置核查，及时发现业务系统隐患，并进行事前预警；结合内外部情报，提供更加准确和及时的安全分析。同时引入攻击链模型分析从侦查、渗透、攻陷、控制、破坏一整套攻击流程，利用最新的感知模型和可视化技术对分析结果进行多维度、多视角、细粒度的集中态势呈现。帮助掌控实时安全态势，动态感知隐患与威胁，为安全分析师和决策层提供强有力的支撑。

态势感知平台可灵活地对接崂山区电子政务外网中现有的安全设备或安全子系统，实现各类型多厂商安全监测防护资源的整合，通过现有及待建安全子系统的对接，态势感知系统可覆盖全网资产及业务运行信息、脆弱性信息、攻击行为信息、风险信息、异

常流量信息，同时结合威胁情报和并在此基础上进行综合分析呈现，通过攻击链的描绘，形成包括被攻击对象和攻击源识别、脆弱性识别、攻击过程及影响分析、安全风险态势等在内的多视角全方位的态势感知系统。

本次建设的态势感知是一个全面信息收集、融合处理感知安全状态及风险并进行态势可视化呈现的过程，该过程是动态持续的，通过连续的信息采集分析不断更新对目标网络安全态势的认知理解，掌握安全状态、了解发展规律、进行提前预警。因此态势感知系统要处理的是海量多维的信息，要进行多方位的关联及发掘分析，要呈现的也是多对象、多维度、多视角的安全态势。鉴于此，需要将安全态势涉及的各类安全要素和监视角度进行了梳理归纳，形成了由多个维度组合构成的态势感知体系。多个维度分别是资产态势、攻击态势、运行感知、脆弱性态势、风险态势、威胁态势、流态势，融合这多个感知体系形成有面向综合态势监视的态势总览。通过多个维度的感知，崂山区电子政务外网的态势感知平台可以呈现出一幅较为通用和完整的网络安全态势的全景图。并且在多个维度的专项分析呈现和扩展外延中，崂山区可以聚焦整合、按需搭配，形成适合自身业务需要和安全态势监控需要的态势感知系统。

本次安全提升服务中对所需安全态势感知平台要求如下：

态势感知平台	1、产品要求部署在 Linux 操作系统上，必须采用 64 位操作系统。涵盖网络设备、安全设备、主机、数据库、中间件以及各种应用系统；支持单级部署和级联部署，支持分布式部署。产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。数据库应可支持分布式弹性扩展，提供数据冗余存储。提供弹性扩展能力和数据高可靠冗余存储。包含系统平台框架、资产管理、安全事件管理、基础关联分析、标准脆弱性管理、风险评估、首页、标准的报表模块、标准的响应管理模块、权限管理、知识管理、系统自身管理、内置 1 个本地事件采集器（日志采集器）； ★2、在综合展示界面中能够显示系统的基本管理信息，包括最近 30 分钟告警状态雷达图、最近 1 小时事件趋势图、最近 24 小时的 10 条告警列表，能够显示最新 5 分钟内的事件一览、包括各类型事件数量和等级，最近 24 小时资产告警排行 Top10 等以及事件量曲线 3、系统提供基于资产的拓扑视图，可以显示资产之间的逻辑连接关系。系统可以按列表和拓扑两种模式显示资产拓扑节点，在资产拓扑上选择每个

	资产节点，可查看每个资产的基本属性、事件信息、告警信息、漏洞信息、风险信息、关联事件、访问配置数据等，并且支持向下钻取，直接进入事件列表、关联告警列表 ★4、日志方式化：系统必须具备日志范式化功能，实现对异构日志格式的统一化，范式化字段至少应包括事件接收时间 、事件产生时间、事件持续时间、用户名称、源地址、源 MAC 地址、源端口、操作、目的地址 、目的 MAC 地址、目的端口、事件名称、事件摘要 、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等； 5、日志可加密压缩传输，保证数据的完整性和机密性；日志可加密存储，支持大数据量存储；支持加密压缩方式转发，定时转发；系统可以统计不同采集器和不同安全域下的设备个数并以饼图展示，统计采集器或安全域中事件量 Top10 以柱图展示，配以统计列表； 6、事件分析模块：系统提供交互式事件分析模式，供用户按照自己的需求通过仪表盘与系统存储的所有事件进行交互，实现按需查询，支持查询嵌套，可任意回退，查询时间缩短至秒级。系统可将用户的查询条件保存为策略，供后期快速分析使用，支持策略的导入导出；可以对选中日志进行视网膜视图分析，以可视化方式展示日志的源 IP 与目的 IP 分布走向；可以多种形式展示动态事件移动图，包括折线图、柱状图、折柱混合图、等级堆积图等，并可进行选择切换；系统具有基于规则的安全事件实时关联分析的能力，能够对不同的事件进行相关性分析，发掘潜在的信息；系统提供基于图形化方式的关联规则编辑器；具有多级关联的能力，即一次关联后的事件可以跟其他事件再次关联，并不断的延展下去，二次关联，三次关联，四次关联，等等，深度不限 7、态势综合展示：系统提供网络安全态势功能，可对采集的信息进行分析和计算，将分析所得的网络安全态势可视化进行展示；可展示网络总体安全态势，包括 1 小时事件数、24 小时规则命中次数、24 小时规则命中 Top5、资产信息统计、24 小时告警统计、15 分钟攻击分布、资产核查信息、5 分钟威胁 KPI、1 小时业务健康度、资产漏洞 Top5、1 小时告警和事件趋势、攻击地图

	8、资产态势：可对资产进行分析，实时呈现网络资产的安全态势，包括：资产类型统计数据、资产日志接入态势、资产告警态势、资产漏洞态势、资产核查态势、高危资产态势、资产风险等级、攻击类型 Top5、资产风险态势、攻击风险趋势、漏洞端口 Top10、安全域维度数据、业务系统维度数据 9、攻击态势：可对网络面临的威胁和攻击进行分析，实时展示网络面临的攻击数量及趋势走向，外部和内部攻击的分布情况，攻击成功和失败的数量及分布，攻击类型与安全域、资产类型对应关系的走势情况，最近 15 分钟的各类攻击关系展示，各安全域及业务系统面临的攻击态势等 10、威胁告警态势：可综合全网依据告警策略所触发的各类告警信息进行态势展现，通过各类饼图、柱图、趋势图等形式辅助数据的直观展示；可在同一饼图中，显示告警类型和告警严重等级两个维度的对比关系；可展示不同区域内告警类型和告警严重等级的比对统计信息；支持不同区域的告警类型和严重等级的发生数量趋势图展示。 11、大数据分析子系统：大数据分析子系统需具备海量数据处理能力，采用基于分布式架构数据库进行数据整合和存储，采用分布式搜索引擎进行数据的查询和钻取，采用数据聚类、攻击链关联、机器学习、攻击模型构建等方法实现数据监测与交互分析、攻击路径分析、历史关联，实现对恶意代码、攻击入侵、扫描探测、违规行为、可疑行为、武器化部署阶段、远控阶段、侦查阶段的安全预警。 ★12、二阶数据、三阶梯数据利用：对安全管理平台以产生告警消息进行二阶段处理及三阶段处理，通过多级告警输出、关联最大限度提高告警消息精准度，通过对三阶告警消息进行处理生成可视化数据源；越权漏洞自动确认：通过对安全管理平台业务日志监控，引入基于业务模型的安全处理模型，通过深度学习算法，自动处置发现业务系统中存在的越权类业务逻辑漏洞；弱密码漏洞自动确认：通过深度学习算法及制定的密码安全策略，自动处理及确认弱密码类安全事件，并根据业务重要程度、账户权限等安全模型建立自动处理机制；规自动确认：通过深度学习算法，引入网络安全管理模型，通过程序对安全管理平台的高精准告警事件进行自动确

	认、自动分析和关联；任意文件攻击事件自动处置：基于业务逻辑的访问方式，构建网络安全访问模型，通过对违反安全模型行为的自动处置自动评估网络安全事件及影响；敏感信息泄露：通过深度学习的方法，引入系统安全监控措施，通过对系统交换过程进行自动化处置、确认评估系统信息泄露情况； ★13、提供至少 500 管理节点授权，服务期内提供升级维护服务。
态势感知平台流量探针	1、硬件要求：支持原始数据包镜像和被动接收 flow 两种采集方式。其中 flow 包括 netflow、netstream、jflow、cflow 等主流协议的各主流版本。2U 标准机架式，冗余电源，专用硬件平台和安全操作系统，最大可支持 10G 网络流量的实时接收采集（多路）。6 个电口，4 个光口，2 个万兆光口，存储容量 32T，支持 RAID50。服务期内提供硬件维保； 2、必须具备范式化功能，实现对异构流日志格式的统一成自定义协议 vflow 3、有独立的管理界面，通过浏览器可以登录到采集器上进行查看和配置，能够对当前采集器进行配置，能够监视采集器所在服务器的运行状况、设置采集器的时钟同步服务器。 采集器可分布式部署。 4、支持端口镜像与被动接收两种采集方式，被动接收支持 NetFlow、NetStream、Sflow 和 jflow 的采集
态势感知分布式分析探针	★1、硬件指标：2U 上架设备，最大吞吐量≥3Gbps，提供 4 个 1000M Base-T 网络接口，最多提供 7 个扩展槽位，冗余电源，96G 内存，32T 容量硬盘，服务期内提供硬件维保和规则库升级； 2、威胁感知：支持网络威胁感知，基于基础检测日志进行威胁分析，基础日志包括入侵检测日志、恶意样本日志、恶意域名日志；各种日志提供单独的视角展示；能够展示、查询各种日志的元数据。 3、攻击者、被攻击者视角支持展示对应的的地理位置或资产信息、对应的被攻击者、事件日志数量，对应数量可以进行跳转至对应数据以助于进一步分析； 4、应提供不少于 6 种的专业模型视角：攻击者视角、被攻击者视角、事件视角、样本视角、威胁情报视角、脆弱性分析视角等多维度的专业视角，

	并可进行线索分析钻取能力； 5、支持内网安全和外部攻击两个主线分析维度，内网提供：WEB 攻击、扫描探测、异常行为、暴力破解、僵木蠕分析五个场景；外网提供：WEB 攻击、扫描探测、异常行为、暴力破解四个场景 6、脆弱性感知：支持基于旁路网络流量发现内部的脆弱性，包括弱口令、漏洞和高危端口；支持根据登录成功的流量判断脆弱口令，支持 telnet、ftp、tds 协议脆弱口令检测，支持自定义脆弱口令以防止常用复杂口令被爆破；支持监测网络环境中在公网开放的高危端口，并记录高危端口连接记录；支持监测内部主机存在的漏洞，并记录存在对应的攻击行为； 7、资产感知：支持对网络资产进行感知分析，可配置多级资产分组，编辑资产分组范围，支持自动发现网络资产配置，可编辑资产的类型、标签、系统、位置、服务等信息；支持公网私用配置，可将非私有地址配置成内部资产，并可自定义资产的地理位置；支持发现失陷资产，支持基于 SMB 攻击行为、蠕虫传播行为、其他内网攻击以及用户手动确认攻击成功事件分析失陷主机，可以查看主机失陷判定事件的判定性质和处理流程；支持对单资产进行分析，基于时间轴展示资产受到攻击的全部事件 ★8、威胁情报：提供威胁情报视角，展示命中情报的数座数据，支持 IOC 一键云查，支持自定义威胁情报，可下载、导入情报库模板；支持基于时间轴展示威胁情报总览情况。 9、威胁处置：支持与 IPS、WAF、防火墙产品进行联动阻断，可通过目的主机信息、异常访问事件、告警级别、命中威胁情报等参数配置自动化阻断规则，可配置阻断时长信息 10、威胁展示：支持全局态势、威胁情报态势、沙箱监测态势、外部攻击态势、资产态势、横向攻击态势展示。
★态势感知需自定义开发内容	1、告警方式和内容定制：在态势感知平台原有告警消息推送的基础上对告警方式进行扩展，增加短信告警、邮件告警、其他即时消息接口定制开发等，确保安全管理平台在现场落地时能够满足用户使用需求。传统安全设备、安全平台推送告警描述过于专业部分接收者无法完全理解告警消描述内容，通过对安全事件规则、安全告警接收者等对象定制告警描述消息。

	如面向安全管理员发送详细专业的描述内容，面向领导进描述安全事件及事件处理方式等。 2、二阶数据、三阶梯数据利用：对态势感知平台以产生告警消息进行二阶段处理及三阶段处理，通过多级告警输出、关联最大限度提高告警消息精准度，通过对三阶告警消息进行处理生成可视化数据源。 3、越权漏洞自动确认：通过对态势感知平台业务日志监控，引入基于业务模型的安全处理模型，通过深度学习算法，自动处置发现业务系统中存在的越权类业务逻辑漏洞。 4、弱密码漏洞自动确认：通过深度学习算法及制定的密码安全策略，自动处理及确认弱密码类安全事件，并根据业务重要程度、账户权限等安全模型建立自动处理机制。 5、违规自动确认：通过深度学习算法，引入网络安全管理模型，通过程序对安全管理平台的高精准告警事件进行自动确认、自动分析和关联。 任意文件攻击事件自动处置。 6、基于客户业务逻辑的访问方式，构建网络安全访问模型，通过对违反安全模型行为的自动处置自动评估网络安全事件及影响。 7、敏感信息泄露：通过深度学习的方法，引入系统安全监控措施，通过对系统交换过程进行自动化处置、确认评估系统信息泄露情况。 8、各种控制台互联网登录入口识别：通过态势感知平台各种审计日志、告警消息等内容进行数据处理和分析，深度发现所有违反网络安全管理规范的应用，并对应用影响程度进行自动化确认。 9、可视化定制-攻击事件可视化视图，安全威胁可视化视图大屏展示。

2.2.6 TAP 交换机

目前崂山区电子政务外网的网络规模较大，网络安全监测的难度随着变大。网络中的某个安全监控盲点可以轻易对网络产生巨大影响。因此在崂山区电子政务外网中需要监控的网络端口越来越多，接入的安全监控设备也讲大幅增加，这就对网络管理提出更高的要求。在崂山区电子政务外网中使用传统接入监测方法（例如：在核心交换机中配置端口镜像）的成本非常高且会对被镜像设备造成非常大的压力。势必会影响崂山区电子政务外网的整体性能。

因此，本项目要求供应商通过提供 TAP 交换机的形式采集网络流量数据，并将流量复制到多个端口、或把多条数据汇聚到个别端口，再给后端需要对网络内容进行分析、监控的平台应用。

本次安全提升服务中对所需 TAP 交换机要求如下：

TAP 交换机 （至少 2 台）	★1、业务接口配置不少于 48 个万兆光口(兼容千兆)，含 24 个万兆接口模块；提供至少一个 Console 口、一个 GE RJ45 管理口；单系统处理性能不低于 460Gbps；复制性能不低于 460Gbps；所有端口支持 100%线速转发无丢包；配置交流冗余电源，电源模块支持热插拔；配置冗余风扇；服务期内提供硬件维保服务； 2、单台设备支持一对一、一对多、多对一、多对多等方式的流量汇聚和流量复制功能；支持最大复制份数仅受面板接口数量限制； 3、设备所有业务接口支持自定义配置输入/输出（I/O）模式；可配置为输入端口用于接收流量，也可配置为输出端口用于将流量输出到其他设备； 4、支持基于硬件的流量过滤功能，支持不少于 2K 条 IPv4/v6 的七元组（源/目的 IP 地址、源/目的 TCP 端口号、协议号、VLAN、物理端口）匹配规则； ★5、支持不少于 96 条的字符串匹配规则(匹配深度 128 字节，匹配长度 8 字节)； 6、支持 IPv4/IPv6 五元组与字符串组合匹配规则； 7、支持面向会话的负载均衡分流，基于源和目标 IP、源和目的端口、协议号等五元组条件组合的哈希算法； 8、支持同源同宿负载均衡输出； 9、支持故障容错的负载均衡保护机制； 10、支持负载均衡输出到链路组，支持负载均衡输出到带权重的链路组； 11、所有端口支持报文标记功能，按需给捕获到的数据包添加用户自定义 VLAN 标签，支持 VLAN 标记的增加和删除； 12、设备支持业务端口流量统计、历史峰值流量统计； 13、支持 Console、SSH、Telnet、Web 等多种方式登录系统；支持多台设备的图形化集中管理；支持 SNMP、SNMP Trap； 14、支持 REST API 接口；

	15、支持在线安全升级；

2.2.7 安全检查和测试服务要求

1、信息资产识别服务

供应商应依据相关国家标准或国际标准，对崂山区电子政务外网的信息资产进行全面梳理和识别，识别内容包含但不限于资产类型、IP 地址、业务部门、责任人、用途、操作系统、数据库、中间件等。资产识别方式包含但不限于：自研工具扫描探测、人工访谈调研和实地核查等。资产类别应按照相关规范分类，包含但不限于以下几大类：业务应用、网络结构、文档和数据、软硬件资产等；物理环境、组织管理、人力资源资产等。

供应商应根据资产识别结果，科学、合理的对资产进行重要性赋值，明确资产价值。应针对资产识别情况及问题及时汇报。每年进行资产梳理工作，并交付资产梳理清单。

2、基线核查服务

供应商应依据相关标准或规范、提交基线核查的标准，会同采购方各接口人进行沟通确认。对目标对象进行核查，目标对象包括但不限于：网络设备、操作系统、数据库及中间件等。供应商应组织相关人员对结果进行确认，分析提交科学、合理的整改建，并结合崂山区电子政务外网实际业务场景实施基线核查修复处置工作,并进行复测,提交基线修复报告。基线核查应包含但不限于以下内容：

网络设备： OS 安全、帐号和口令管理、认证和授权策略、网络与服务、访问控制策略、通讯协议、路由协议、日志审核策略、加密管理、设备其他安全配置等

操作系统：系统漏洞补丁管理、帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制、通讯协议、日志审核功能、剩余信息保护、其他安全配置等

数据库：漏洞补丁管理、帐号和口令管理、认证、授权策略、访问控制、通讯协议、日志审核功能、其他安全配置等

中间件：漏洞补丁管理、帐号和口令管理、认证、授权策略、通讯协议、日志审核功能、其他安全配置等。

3、渗透测试服务（不少于 5 次）

由采购方给出目标业务清单，供应商提供渗透测试服务方案和渗透测试申请，内容必须包括但不限于：渗透测试方法和流程、渗透测试工具、渗透测试面临的风险和规避

措施、渗透测试时间和地点、渗透测试人员。在得到采购方授权后，供应商服务团队应通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试。

渗透测试应至少包括以下方面的工作内容：WEB 应用系统渗透、主机操作系统渗透、数据库系统渗透。

供应商需针对每个业务提交渗透测试报告及整改建议，并对修复结果进行复测。

4、漏洞扫描服务

供应商在服务期间应按照采购方要求，不定期对崂山区电子政务外网关键应用进行漏洞扫描并对扫描结果进行人工分析，提交经过人工处理的漏洞扫描报告。漏洞探测内容应至少包括：操作系统漏洞、中间件漏洞、常用软件漏洞、应用程序漏洞、网络设备漏洞、数据库漏洞等。供应商服务团队须自行携带专用漏洞扫描工具，以支撑本次漏洞扫描服务工作，采购方不承担专用漏洞扫描工具所产生的费用。服务期结束后，供应商须彻底清除扫描工具中的数据。扫描结果保留给采购方，以待下一步处理。

2.2.8 安全支撑服务要求

1、 应急演练服务（至少 1 次）

供应商需帮助采购方通过应急演练最大限度地在安全事件发生前暴露预案和流程的缺陷，反馈应急资源的保障情况，改善各部门、机构、人员之间的协调性，增强应对突发安全事件的信心和意识，提高队伍人员的熟练程度和技术水平，进一步明确各自岗位职责，提高各级预案之间的协调性，提高应急反应能力。

供应商应结合崂山区电子政务外网网络安全要求制定对应的应急演练方案，经采购方评审后，组织相关人员开展应急演练，并对应急演练全过程进行记录。演练场景包含但不限于以下内容：有害程序传播处理演练；网络攻击应急演练；信息破坏应对；设备设施故障事件应急演练等。每次应急演练需交付文档应包含但不限于:《应急演练脚本》、《应急演练总结报告》。

2、 应急响应服务

供应商在服务期间需结合最新威胁情报，及时对流行威胁进行评估、风险通告预警（提供威胁情报预警实际案例），由安全专家排查是否对采购方资产造成威胁，通知并协助采购方及时修复或调整安全策略。

供应商服务必须积极响应采购方上级单位各安全类通报、通知、文件等，按照要求对相关系统进行隐患排查，提出处置方案，跟踪进度，确保安全隐患整改到位，并形成处置报告

供应商必须对崂山区电子政务外网出现的网络安全相关故障或问题进行排查，分析故障原因并给出处置建议，及时发现各类安全事件，自动生成工单。安全事件包括但不限于以下几类：WEB 安全事件、恶意程序事件、网络攻击事件、信息破坏事件等；

★应急响应和时间要求：供应商应提供 7*24 应急响应服务，根据事件发生的根因、影响范围，针对性给出安全加固方案，通过工具和方法对恶意文件、代码进行根除，快速恢复业务，消除或减轻影响。每次故障处理完毕 3 个工作日内提供详细的故障处理报告，要求供应商安全服务团队严格按照招标方要求对事件做出响应：

- 特别重大事件（Ⅰ级），5 分钟作出响应，提供远程 7*24 小时响应服务、1 小时到达现场进行应急响应服务；
- 重大事件（Ⅱ级），10 分钟作出响应，提供远程 7*24 小时、2 小时到达现场进行应急响应服务；
- 较大突发事件（Ⅲ级），30 分钟作出响应，提供远程 7*24 小时响应服务、4 小时到达现场进行应急响应服务；
- 一般性突发事件（Ⅳ级），30 分钟作出响应，提供远程 7*24 小时响应服务、远程无法解决时，在 4 小时到达现场进行应急响应服务。

2.2.9 安全运营服务要求

供应商需遵循等级保护系列标准、ITIL 和 ISO27000 系列服务标准，结合自身丰富的信息安全服务经验，组建专门的专家支持队伍，为采购方提供信息安全日常的维护支持，协助采购方开展信息安全保障和安全维护工作工作，减轻采购方的压力。

供应商派遣一名专业的安全运维人员提供 5*8 小时驻场运维服务。驻场运维人员至少具有两年以上安全服务经验，具有原厂技术能力认证证书，并提供加盖投标人公章的人员社保缴纳证明。驻场人员能够独立进行安全告警分析、恶意程序分析，当发生安全事件时能够独立进行应急响应。服务过程中需输出《驻场运维人员月报、季报》等交付物。

供应商应保证服务期采购标方所有网络安全设备稳定运行，设备包含：新部署设备、采购方原有网络安全设备（见下表）。供应商服务团队需定期查看设备运行状况，定期对安全设备配置进行备份；保证病毒库特征库等及时升级；对采购方新增资产、业务变更等，负责安全设备的调试、配置变更；对发生的故障进行分析处置。根据需要输出巡检结果、维护记录和设备故障处理报告等交付物。采购方原有网络安全设备清单如

下：

设备名	数量	购买日期	质保结束日期
负载均衡	1	2017.12	2020.11
上网行为管理	1	2017.12	2020.11
入侵检测	2	2018.07	2021.06
WEB 防火墙	1	2015.07	2018.06
防火墙	1	2017.12	2020.11
SSL VPN	2	2015.07	2018.06
IMC 网管平台	1	2015.07	2018.06

注：本项目服务期内，上表中安全设备超出质保期后，如出现损坏，或规格、性能等不再满足业务运行要求，供应商需提供满足需求的相关设备，且按需与其他设备、业务对接，保证业务运行。

供应商需对崂山区电子政务外网内相关核心资产提供立体防护措施，需要结合防火墙、入侵防御系统、入侵检测系统、WEB 应用防火墙等设备进行日志审计分析，日志保留六个月，检查策略是否有效、配置是否安全，在得到授权时对相应设备的安全防护策略进行调整。通过对事件的分析、处置、响应过程进行复盘，提取持续性威胁防御配置，发起安全策略配置变更流程，并持续监测配置变更有效性。

在采购方业务关键期、重要活动、重大会议期，指派专门的服务团队负责突发安全事件处理、重大活动期间安全保障和应急处理服务，完成事前安全巡检、事中 7*24 小时驻场值守保障、事后总结汇报工作。

2.2.10 安全合规服务要求

★服务期内，安全服务供应商需确保采购方网络系统安全符合国家网络安全法等安全法规要求，以及上级网络安全主管部门（网信办、大数据局、网警等）的各类安全技术指标和要求，不被通报。

2.2.11 安全咨询及培训要求

1、安全咨询服务

协助采购方制定安全管理流程，内容包括但不限于安全事件管理、安全问题管理、安全应急管理、变更管理、考核管理、合规管理、安全服务管理、重保管理等流程管理；

协助采购方制定安全管理制度及规范，涉及安全培训、安全检查、安全防护等内容，

从服务实施进度、实施过程、实施结果等方面，综合控制安全服务实施质量；

协助建立崂山区电子政务安全监测和安通报机制，发现问题及时通报整改，并持续关注情况。

2、安全培训服务（至少 2 次）

安全意识培训：提高采购方普遍的安全意识和人员安全防护能力，使相关人员充分了解既定的安全策略，并能够切实执行。培训内容包括信息安全形势、面临的威胁和风险、典型安全问题、常见的黑客攻击手法、病毒/木马侵害及解决方法、web 访问和邮件手法的安全问题及解决方法、个人安全防护意识、个人安全防护手段；

安全技术培训：掌握基本的安全攻防技术，提升其安全技术操作水平，培养解决安全问题和杜绝安全隐患的技能。培训内容包括典型的技术脆弱性、各种常见操作系统/网络设备/应用系统的安全配置要点、典型安全工具的运行、日常安全操作的管理、典型安全产品的介绍；

安全管理培训：提升采购方整体的信息安全管理水平和能力，帮助有效建立信息安全管理体系。培训内容包括信息安全管理体系、等级保护建设的意义、风险管理和评估、风险处理措施，信息安全管理相关标准（BS7799、ISO27001 等）。

3. 商务条件

3.1 服务期限

具备服务能力，自验收合格之日起一年。

3.2 服务地点

采购人指定地点。

3.3 付款方式

签订合同时具体约定。

3.4 服务成果验收

服务期满或完成服务成果后，采购人应对服务的成果进行详细而全面的检验。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。检验合格后，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。

3.5 服务保障

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。

注：上述要求以及标注中：

带“★”条款为实质性条款，供应商必须按照磋商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的产品。投标人所投产品必须提供经市场监管总局公布的认证机构出具的有效期内的节能产品认证证书原件的电子文档。

第五章　评审办法

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 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。

1.3 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，残疾人福利性单位参加磋商报价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；残疾人福利性单位参加磋商报价的视同小型、微型企业，按照本磋商文件小型、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。

1.3.1 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）。

1.3.2 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。

1.3.3 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。

1.3.4 成交供应商为残疾人福利性单位的，采购代理机构应当随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。

1.3.5 供应商提供的《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。

1.4 面向中小企业预留情况详见投标人须知前附表。

1.4.1 依据财政部、工业和信息化部《政府采购促进中小企业发展管理办法》（财库

〔2020〕46 号）规定，中型、小型和微型企业参加政府采购活动的须提供《中小企业声明函》（格式见附件），否则不得享受相关中小企业扶持政策；

1.4.2 企业划型标准按照《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）规定执行。

1.4.3 供应商提供的货物、工程或者服务符合下列情形的，享受《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）规定的中小企业扶持政策：

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

（二）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

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

在货物采购项目中，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。

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

1.5 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）。

1.6 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，应当提供由省级以上监狱管理局、戒毒管理局或新疆生产建设兵团出具的属于监狱企业的证明原件的扫描件，且对上述材料的真实性负责，否则不给予价格扣除。

2. 评分标准

评分因素	商务部分	技术部分	总分
分值比重	24分	76分	100分

评审项目		分数	评分标准
商务部分	投标报价	10分	满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。 其它报价得分=评标基准价÷（投标报价）×10
	企业业绩	6分	自2018年1月1日（以合同签订时间为准）以来已完成的同类（信息化运维服务）项目，每份得2分，最高得6分； 开标时投标文件中必须附合同电子扫描件加盖公章，否则不得分。

	产品实力	6 分	选用核心安全产品（态势感知平台）生产厂商具有《国家信息安全测评信息安全服务资质》（安全工程类三级及以上）证书、微软MAPP计划成员单位证书、CMMI 5认证证书，每提供1份得2分，最多得6分； **注：投标人须提供证书等证明材料扫描件加盖公章，同时投标文件中提供相应扫描件，否则不予计分。**
	企业信誉	2分	1.投标人自2017年1月1日至开标日截止获得过税务部门对企业纳税信用的A级评价的，有一年得1分，本项满分2分。须提供国家税务总局官网网上公示截图和查询网址，否则不予计分。 以上评分均需提供上述证明文件的扫描件，且扫描件应加盖投标人公章，否则不予计分。
技术部分	响应情况	10分	基础分为 8 分。 优于招标文件非实质性要求的，每有 1 条加 0.5 分，最高加 2 分；对实质性要求，每出现 1 条正偏离，加 1 分，最高加 2 分。（以上两项最高加 2 分）。 非实质性条款每出现一条负偏离扣除基础分 2 分，扣完基础分为止。
	安全功能现场演示	6 分	能够利用技术手段，将所投核心安全产品（态势感知平台）产生的安全事件信息自动对应到部门及业务系统，并通过金宏办公系统通知到相关责任单位。现场演示此功能，并通过现场登录金宏办公系统查验成功，得 6 分。演示时间控制在 10 分钟以内，演示超时评委有权直接叫停，未现场演示不得分。说明：演示设备须在投标截止时间前提交，供应商须提前自行调试相关演示设备。开标现场提供金宏网线。
	服务承诺	4 分	对要求的服务范围、服务内容、服务技术指标或等级保护级别标准、重点保障等响应程度或承诺进行综合评价： 完全响应或优于招标文件要求的，得 2 分；基本满足招标文件要求的，得 1 分，不满足招标文件要求的不得分。 投标人针对项目综合考虑，可提出招标要求外的优质附加服务承诺，优质的得 2 分，未提供不得分。

	服务方案	25分	服务商针对本项目组建专业的服务团队，对于服务团队组成、分工、业务能力、从业经验等表述真实完善的得 6-4 分；模糊简略的得 3-1 分；未提供不得分； 对崂山电子政务外网安全现状及需求描述准确详实的得 6-4 分；描述模糊的得 3-1 分；未提供不得分； 服务方案总体设计内容完整、结构合理、针对性强，符合招标文件实际需求的得 6-4 分；服务方案设计简略，部分满足招标需求的，得 3-1 分，未提供不得分。 文档资料交付方案内容全面，涵盖项目整个生命周期的资料交付模板内容符合招标实际需求的，得 4-3 分；方案模糊简略的，得 2-1 分；未提供不得分。 在满足招标文件要求的基础上，能结合崂山区实际情况及行业发展趋势，提出合理化的优化建议，充分展现投标人专业性的，得 3-1 分；未提供不得分
	售后服务	15分	整体售后服务方案合理、措施有力、切实可行的得 5-3 分；模糊简略的得 2-1 分；未提供不得分 组织机构及服务质量保证措施、保密措施等能做到机构健全，建立完整的工作台帐、工作信息收集、反馈等客户质量保证措施，得 5-3 分；模糊简略的，得 2-1 分；未提供不得分 制定详细的专业培训计划，培训方案内容全面、措施有力，具有完善的技术支持方案的得 5-3 分；培训方案内容完整，技术支持方案不完备的得 2-1 分；未提供不得分。
	服务团队人员	12分	对项目组组织结构、人员资格条件或技术能力、专业配置、从业经验等进行评价： 投标人安全服务团队至少 1 人拥有国家注册信息安全专业人员（CISP）认证证书且提供社保证明，得 2 分；投标人安全服务团队至少 1 人拥有高级信息系统项目管理师证书且提供社保证明的，得 2 分；投标人安全服务团队至少 1 人拥有 HCIE 或 H3CIE 证书且提供社保证明的，得 1 分；（提供上述证明文件的扫描件加盖投标人公章）

			安全厂商安全服务技术支持团队经理(明确指定 1 人)具备 PTE、ISO27001、ICSSE 证书且提供社保证明，每提供一份得 1 分，最多得 3 分；安全厂商安全服务技术支持团队成员 1 人具备 ICSSE 证书且提供社保证明得 1 分；安全厂商安全服务技术支持团队成员 1 人具备 CCIE 证书且提供社保证明得 1 分;安全厂商安全服务技术支持团队成员具备 PTE 证书且提供社保证明，每提供一份得 1 分，最多得 2 分;（提供上述证明文件的扫描件加盖原厂公章）
	应急保证	4 分	具有详细的应急保障方案得 2-0 分； 具有详细的应急流程，体现各类应急事件处理流程，应急管理架构清晰，人员职责分工明确得 2-0 分。

3.政策加分以及计算方法

3.1 说明：

3.1.1 供应商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。

3.2 小微企业价格扣除优惠标准详见投标人须知前附表。

3.3 按照财政部等四部委联合印发《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》〔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、财政部生态环境部《关于印发环境标志产品政府采购品目清单的通知》财库〔2019〕18 号的规定，属于节能、环境标志优先采购产品的，享受政府采购优先政策：

3.3.1 评审时，对节能、环境标志产品分别给予一定幅度的加分或价格折扣（详见评分标准）。

3.3.2 投标人必须提供经市场监管总局公布的认证机构出具的有效期内的节能产品、环境标志产品认证证书原件的电子文档。

第六章　供应商须知

1. 采购依据以及原则

1.1《中华人民共和国政府采购法》;

1.2《中华人民共和国合同法》;

1.3《中华人民共和国政府采购法实施条例》;

1.4《政府采购非招标采购方式管理办法》;

1.5《政府采购质疑和投诉办法》;

1.6《山东省政府采购管理办法》;

1.7 其他有关法律、行政法规以及省市规范性文件规定。

2. 合格的供应商

2.1 符合《中华人民共和国政府采购法》第二十二条第一款规定的条件;

2.2 符合本磋商文件规定的资格要求，且按照要求提供相关证明材料;

2.3 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

2.4 供应商须知前附表规定接受联合体报价的，应符合以下规定:

2.4.1 联合体各方应按照磋商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供应商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供应商确定资质等级。

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供应商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报价，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，供应商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、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

2.7 供应商提供的证明材料内容必须真实可靠。

符合上述条件的供应商即为合格供应商，具有参与竞争性磋商的资格。

3. 保密

参与竞争性磋商活动的当事人应对磋商文件和响应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、报价有效期以及参与采购活动费用

4.1 语言文字

除专用术语外，与竞争性磋商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。如供应商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，在解释响应文件时以中文翻译本为准。

4.2 计量单位

除磋商文件另有规定外，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

除磋商文件中另有规定外，磋商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 报价有效期

4.4.1 在供应商须知前附表规定的报价有效期内，响应文件以及其补充、承诺等部分均保持有效。

4.4.2 在磋商文件规定的响应文件有效期满之前，如果出现特殊情况，采购人或者采购代理机构可在报价有效期内要求供应商延长有效期，要求与答复均以书面通知为准并作为磋商文件和响应文件的组成部分；供应商可以拒绝上述要求，拒绝延长响应文件有效期的，其响应失效；同意上述要求的，既不能要求也不允许其修改响应文件。

4.5 参与采购活动费用

供应商应自行承担其准备和参加采购活动发生的所有费用。

5. 踏勘现场

5.1 供应商须知前附表规定组织踏勘现场的，采购人必须按照规定时间、地点组织供应商踏勘项目现场，以便供应商获取有关编制响应文件和签署合同所涉及现场的资料。供应商承担踏勘现场所发生的自身费用。

5.2 采购人向供应商提供的有关现场的资料和数据，是采购人现有的能使供应商利用的资料，采购人对供应商由此而做出的推论、理解和结论不负责任。

5.3 供应商经过采购人允许，可以进入项目现场踏勘，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，供应商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 供应商对竞争性磋商活动事项有疑问的，可以向采购人或采购代理机构提出询问；采购人或采购代理机构应当在 3 个工作日内作出答复，但答复的内容不得涉及商业秘密。

6.2 询问在青岛市公共资源交易网本项目的公告页面在线提交。

6.3 询问及答复的内容在青岛市公共资源交易网本项目的公告页面查看。

7. 偏离

采购人允许响应文件偏离磋商文件某些非实质性要求的，偏离应当符合磋商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，成交供应商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成交合同金额的 10%。采购人根据项目特点、供应商诚信等情况可免收履约保证金或降低收取比例。

8.2 成交供应商未按照要求提交履约担保的，视为放弃成交资格，成交供应商应当对采购人造成的损失给予赔偿。

9. 采购代理服务费

见供应商须知前附表。

10. 磋商文件

10.1 磋商文件的组成

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

（1）磋商公告；

（2）供应商须知前附表；

（3）供应商应当提交的资格证明文件；

（4）采购需求；

（5）评审办法；

（6）供应商须知；

（7）开启响应文件、磋商、成交；

（8）纪律要求；

（9）签订合同、合同主要条款；

（10）响应文件格式；

（11）供应商须知前附表规定的其他材料。

10.1.2 根据本章第 10.2 款对磋商文件所作的澄清和修改，构成磋商文件的组成部分。

10.1.3 除非有特殊要求，磋商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，供应商被视为熟悉上述与履行合同有关的一切情况。

10.2 磋商文件的澄清和修改

磋商文件的澄清和修改及确认，详见供应商须知前附表。

磋商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. 响应文件的组成

11.1 供应商应按照磋商文件的要求以及格式编制响应文件，并保证其真实性、准确性以及完整性，并按照磋商文件要求提交全部资料并做出实质性响应。

11.2 响应文件由资格审查文件、商务文件、技术文件文件组成：

11.3 资格审查部分

11.3.1 营业执照或登记证书等（第三章序号 1 要求的内容）；

11.3.2资格证书（如有）；

11.3.3在经营活动中无重大违法记录和行贿犯罪记录、具有良好商业信誉和健全财务会计制度、具有依法缴纳税收和社会保障资金良好记录的声明函(见附件1)

11.3.4 磋商文件要求的其他必须提交的资格证明材料。

11.4 商务文件

11.4.1 报价函；

11.4.2 法定代表人身份证明

11.4.3 法定代表人授权委托书（若授权）；

11.4.4 响应报价：

（1）报价一览表。是分项报价明细表的汇总表，响应报价（即响应报价总计金额）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，供应商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，供应商认为《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。供应商认为需要对《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。

11.4.5 供应商同类项目实施情况一览表（若有）；

11.4.6 商务响应表；

11.4.7 联合投标协议书（若有）；

11.4.8 联合投标授权委托书（若有）；

11.4.9 残疾人福利性单位声明函（若有）；

11.4.10 中小企业声明函（若有）；

11.4.11 监狱企业的证明（若有）；

11.4.12 节能、环保等的资质证书或者文件（若有）；

11.4.13 磋商文件要求和供应商认为应介绍或者提交的资料和文件（若有）。

11.5 技术文件

11.5.1 货物清单（包括产品彩页）；

11.5.2 技术响应表；

11.5.3 选配件、专用耗材、售后服务优惠表（若有）；

11.5.4 项目实施人员（主要从业人员以及其技术资格）一览表；

11.5.5 货物合格证明和符合磋商文件规定的技术资料；

（1）供应商应提交证明其拟提供货物的合格性符合磋商文件规定的有效技术（印

刷体）支持资料，并作为响应文件的一部分。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）证明货物和服务与磋商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（若是环保、节能产品须详细描述并提交相关证明材料原件）并保证所供货物必须是全新的、未使用过的合格产品；

（2.3）保证货物在质保期内正常、连续使用所必须的备品备件和专用工具清单以及其货源地与价格；

（2.4）对照磋商文件技术规格、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，并按照磋商文件中技术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）当磋商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）供应商在详细阐述货物的主要技术指标和性能说明时，应注意磋商文件第四章“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，供应商可选用替代标准、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成交供应商响应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）供应商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供应商须全部承担。

11.5.6 磋商文件要求和供应商认为应介绍或者提交的资料和文件。

12. 响应报价

12.1 响应报价的范围：见供应商须知前附表。

12.2 供应商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 响应报价的次数：见供应商须知前附表。

12.4 供应商不得以任何方式或者方法提供报价以外的任何附赠条款。

12.5 供应商应按照磋商文件中要求的内容填写报价，并由法定代表人或者被授权代表签署。

12.6 供应商须按照附件格式表中的各单项明细逐项填写，以方便磋商小组对各响应文件进行比较。

12.7 开启响应文件时，响应文件中《报价一览表》内容与《分项报价明细表》内容不一致的，以《报价一览表》为准。大写金额和小写金额不一致的，以大写金额为准；总价金额与按照单价汇总金额不一致的，以单价金额计算结果为准；单价金额小数点有明显错位的，应以总价为准，并修改单价；对不同文字文本响应文件的解释发生异议的，以中文文本为准。按照以上原则对错误报价的修正，供应商应书面确认。

12.8 唱价时，采购代理机构只对按照磋商文件要求编制的响应报价进行唱价。

12.9 供应商的成交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 供应商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报价。

13. 响应文件编制要求

13.1 响应文件应按所投包分别进行编制。

13.2 响应文件编制：见供应商须知前附表。

13.3 响应文件签章：见供应商须知前附表。

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

13.5 供应商编制响应文件时，应当如实在技术响应表和商务响应表中填写响应情况。

14. 响应文件的加密、上传

见供应商须知前附表。

15. 响应文件的递交

15.1 供应商应在递交响应文件截止时间前递交响应文件。

15.2 供应商递交响应文件的要求：供应商完成电子响应文件制作后，通过【青岛市公共资源投标文件制作工具】上传响应文件，系统即时向供应商发出上传回执通知。上传时间以上传回执通知载明的传输完成时间为准；逾期上传的响应文件，电子招标投标

交易平台将予以拒收。

15.3 除供应商须知前附表另有规定外，不论采购过程和结果如何，供应商的响应文件均不退还。

16. 响应文件的修改与撤回

16.1 供应商在磋商文件要求提交响应文件截止时间前，可以补充、修改、替代或者撤回已提交的响应文件。补充、修改的内容为响应文件的组成部分。

16.2 在提交响应文件截止时间后到磋商文件规定的报价有效期终止之前，在磋商文件没有变动的情况下，供应商不得补充、修改、替代或者撤销其响应文件。

17. 质疑

17.1 参加本次政府采购活动的供应商认为磋商文件、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道其权益受到损害之日起 7 个工作日内，向采购人或者采购代理机构提出质疑。

潜在供应商已依法获取其可质疑的磋商文件的，可以依法对该文件提出质疑。

17.2 供应商应知其权益受到损害之日，是指：

（一）对可以质疑的磋商文件提出质疑的，为收到磋商文件之日或者磋商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。

17.3 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。

17.4 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。

17.5 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。

17.6 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。

18. 投诉

18.1 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。供应商投诉按照采购人所属预算级次，由本级财政部门处理。

18.2 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）投诉书内容符合财政部《政府采购质疑和投诉办法》（第 94 号令）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。

供应商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供应商共同提出。

18.3 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供应商数量提供投诉书的副本。

18.4 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。

18.5 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。

18.6 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。

19. 其他需补充的内容

其他需补充的内容：见供应商须知前附表。

第七章　开启响应文件、磋商、成交

1. 开启响应文件程序

1.1 宣布开启响应文件纪律；

1.2 宣布主持人、唱价人、记录人等有关人员姓名；

1.3 查看在线签到家数，除市场竞争不充分的科研项目、以及需要扶持的科技成果转化项目和政府购买服务项目（含政府和社会资本合作项目）等特殊规定，提交最后报价的供应商可以为 2 家外，少于三家开启响应文件会议结束；不少于三家开启响应文件会议继续进行；

1.4 供应商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响应文件开始解密；

1.5 供应商授权代表在开启记录上确认；在规定时限内未确认的，视为默认开启响应文件结果；

1.6 开启响应文件结束。

2. 开启响应文件

2.1 开启响应文件应当在磋商文件确定的提交响应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；所有供应商须在开启响应文件前规定时间内签到。

2.2 开启响应文件由采购代理机构指定专人负责，开启响应文件记录由供应商线上确认。

2.3 供应商代表对开启响应文件过程和开启响应文件记录有疑义，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、采购代理机构对供应商代表提出的询问或者回避申请应当及时处理。供应商未参加开启响应文件的，视同认可开启响应文件结果。

2.4 供应商不足 3 家的，不得开启响应文件。

2.5 在评审结束前，供应商请保持在线登录电子交易平台状态。评标过程中，如果磋商小组要求供应商对响应文件进行澄清、说明或者补正，要求供应应商按照磋商文件的变动情况重新提交响应文件、最终设计方案或解决方案，要求供应商提交最后报价时，供应商需要通过电子交易平台【专家问题澄清】功能，限时在线提交上述内容。系统不接受超时提交的澄清、材料和报价。

2.6 各供应商的最终评审得分和排序将在电子招标投标交易平台告知。

3. 磋商小组

3.1 磋商小组的组成

采购人按照《中华人民共和国政府采购法》以及有关规定组建磋商小组。磋商由依法组建的磋商小组负责。磋商小组由采购人代表和评审专家共同组成，成员人数为三人以及以上单数，技术、经济等方面的评审专家不得少于成员总数的三分之二。

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确定磋商小组成员。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。磋商小组成员的名单在评审结果确定前必须严格保密。

3.3 磋商小组成员不得参加与自己有利害关系的评审活动，与自己有利害关系的应当回避，已经进入的必须更换。

3.4 磋商小组负责对各响应文件进行评审、比较、评定，并按本磋商文件的规定确定成交供应商或者推荐中标候选人。

3.5 磋商小组具有依据磋商文件进行独立评审的权力，且不受外界任何因素的干扰。磋商小组成员必须独立、负责地提出评审意见，并对自己的评审意见承担责任。对评审结果有不同意见的磋商小组成员应当以书面形式说明其不同意见和理由，评审报告应当注明不同意见。磋商小组成员拒绝评审或者拒绝在评审报告上签字并且又不书面说明其不同意见和理由的，视为同意评审结果。

3.6 磋商小组的职责：

3.6.1 审查响应文件是否符合磋商文件要求，进行资格性审查和符合性审查，并做出评价；

3.6.2 要求供应商对响应文件有关事项做出解释或者澄清；

3.6.3 推荐中标候选人名单，或者受采购人委托按照事先确定的办法直接确定成交供应商；

3.6.4 向采购人、采购代理机构或者有关部门报告非法干预评审工作的行为。

3.6.5 对围、串标等违法违规行为作出认定。

3.7 磋商小组的义务：

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 严格遵守评审纪律，不得向外界泄露评审情况；

3.7.4 发现供应商在招报价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 按照磋商文件规定的评审方法和评审标准进行评审，对评审意见承担个人责任；

3.7.6 编写评审报告；

3.7.7 配合采购人或者采购代理机构答复供应商提出的质疑；

3.7.8 对评审过程和结果，以及采购人、供应商的商业秘密保密；

3.7.9 配合监管部门处理投诉；

3.8 磋商小组成员有下列情形之一的，应当回避：

3.8.1 供应商或者供应商主要负责人的近亲属；

3.8.2 参加过采购项目前期咨询论证的；

3.8.3 自身与政府采购项目存在利害关系的；

4. 评审程序

4.1 宣布评审纪律以及回避提示；

4.2 组织推荐磋商小组组长；

4.3 资格性审查；

4.4 符合性审查；

4.5 澄清有关问题；

4.6 磋商

4.7 供应商提交最后报价

4.8 磋商小组进行综合评分；

4.9 确定成交供应商或者推荐成交候选人名单；

4.10 编写评审报告；

4.11 宣布评审结果。

5. 评审

5.1 资格性审查

5.1.1 磋商小组依据法律法规和磋商文件的规定，对响应文件中的资格证明等进行审查。

5.1.2 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)、信用青岛（credit.qingdao.gov.cn）及崂山区公共资源交易信用监管平台（崂山政务网公共资源交易模块“诚信考核”http://qdls.ggzyjyxypt.com/）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、不良行为名单及其他不符合《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。

5.1.3 在资格性审查时，磋商小组依据供应商提供的《声明函》(见附件 1)审查供应商及其法定代表人和项目负责人行贿犯罪情况。

5.2 符合性审查

磋商小组依据磋商文件的规定，从响应文件的有效性、完整性和对磋商文件的响应程度进行审查，以确定是否对磋商文件的实质性要求作出响应。符合性审查内容详见附录。

5.3 在资格性和符合性审查同时，对属于不合格或响应无效的供应商，磋商小组必须提出不合格或者响应无效的事实依据，并出具不合格或者响应无效说明。

6.澄清有关问题

磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。磋商小组要求供应商澄清、说明或者更正响应文件应当以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人或其授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

7.磋商、最后报价、综合评审

磋商小组成员应当按照客观、公正、审慎的原则，根据磋商文件规定的评审程序、评审方法和评审标准进行独立评审。未实质性响应磋商文件的响应文件按无效响应处理，磋商小组应当告知提交响应文件的供应商。

7.1 磋商程序

7.1.1 磋商小组所有成员应当集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

7.1.2 在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款。实质性变动的内容，须经采购人代表确认，磋商小组应当及时以书面形式同时通知所有参加磋商的供应商，并要求其重新提交由法定代表人或授权代表印章的响应文件。由其授权代表印章的，应当附法定代表人授权书；供应商为自然人的，应当由本人印章并附身份证明。

7.2 供应商提交最后报价

7.2.1 磋商文件能够详细列明采购标的的技术、服务要求的，磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于 3 家。

7.2.2 磋商文件不能详细列明采购标的的技术、服务要求，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后，磋商小组应当按照少数服从多数的原则投票推荐 3 家以上供应商的设计方案或者解决方案，并要求其在规定时间内提交最后报价，最后报价是供应商响应文件的有效组成部分。

已提交响应文件的供应商，供应商在提交最后报价之前，可以根据磋商情况退出磋商。对于未在限时内提交最后报价、退出磋商的供应商，按其前一次报价进行评审。

市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目，提交最后报价的供应商可以为 2 家。

7.3 磋商小组进行综合评分

经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。

评审时，磋商小组各成员应当独立对每个有效响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。

7.4 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、符合性审查的不同供应商参加同一合同项下磋商、报价的，按一家供应商

计算，评审后得分最高的同品牌供应商获得成交供应商推荐资格；评审得分相同的，由采购人或者采购人委托磋商小组采取随机抽取的方式确定一个供应商获得成交供应商推荐资格，其他同品牌供应商不作为成交供应商候选人。

8. 成交

8.1 磋商小组根据供应商须知前附表的规定确定成交供应商候选人或直接确定成交供应商。

磋商小组确定成交供应商候选人的，成交供应商候选人数见供应商须知前附表。采购人应当在收到评审报告后5个工作日内，从评审报告提出的成交候选供应商中，按照排序由高到低的原则确定成交供应商。

8.2 竞争性磋商采用综合评分法，磋商小组应当根据综合评分情况，按照评审得分由高到低顺序对供应商进行排序。评审得分相同的，按照最后报价由低到高的顺序排序。评审得分且最后报价相同的，按照技术指标优劣顺序排序。

8.3 对于分包采购的项目，供应商可以选择多包响应但限制成交包数的，成交人的选择按照供应商须知前附表“分包及成交规定”确定。

8.4 磋商小组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。持不同意见的磋商小组成员应当在评审报告上签署不同意见及理由，否则视为同意评审报告。

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

8.6 磋商小组根据全体小组成员签字的原始评审记录和评审结果编写评审报告。

8.7 磋商结果应通知所有参加磋商的供应商。

9. 成交结果公告以及成交通知书

9.1 采购人或者采购代理机构应当自成交人确定后立即发出成交通知书，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成交结果（公告期限为1个工作日）。

9.2 采购人或采购代理机构不按照规定发布成交结果公告或者发布成交结果公告后不签发成交通知书的，应当承担法律责任，给成交供应商造成经济损失的应承担赔偿责任。

9.3 成交通知书对采购人和成交供应商都具有法律效力。成交通知书发出后，采购人改变成交结果的，或者成交供应商放弃成交，应当依法承担法律责任。

10. 响应无效

出现下列情形之一的，响应无效：

10.1 响应报价高于采购预算或采购最高限价的；

10.2 对“★”条款未做出实质性响应或者发生负偏离的；

10.3 对“◆”条款经磋商小组实质性变动、采购人代表确认内容不响应的。

10.4 应提供而未提供带“▲”标注的政府强制采购节能产品的；

10.5 对允许偏离的非实质性条款，偏离磋商文件规定的偏离范围和幅度的；

10.6 不按照磋商文件规定报价、没有分项报价、拒绝报价、有多个报价（磋商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；

10.7 报价有效期不满足磋商文件要求的；

10.8 磋商小组判定供应商涂改证明材料或者提供虚假材料和承诺的；

10.9 响应文件未按磋商文件规定编制、签章的；

10.10 磋商文件第三章规定供应商应当提交的资格证明文件未提供、提供不齐全的；

10.11 响应文件含有采购人不能接受的附加条件的；

10.12 响应文件存在记录的 MAC 地址、CPU 序列号、硬盘序列号中两项及以上相同的；

10.12 不符合法律、法规和磋商文件中规定的其他要求的。

对响应无效的认定，必须经磋商小组集体做出决定并出具响应无效的事实依据。

11. 废标

11.1 出现下列情形之一的，应予废标：

11.1.1 除市场竞争不充分的科研项目、需要扶持的科技成果转化项目外，在报价截止时间结束后参加报价的供应商不足 3 家，符合磋商文件规定条件的供应商不足 3 家或者对磋商文件作实质性响应的供应商不足 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 供应商的报价均超过采购预算或采购控制价的；

11.1.4 因重大变故，采购任务取消的；

11.1.5 法律、法规以及磋商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供应商。

12. 特殊情况处置程序

12.1 磋商小组成员的更换

12.1.1 磋商小组应当执行连续评审的原则，按照磋商文件规定的程序、内容、方法、标准完成全部评审工作。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，封存磋商文件和所有响应文件，择期重新组建磋商小组进行评审。

12.1.2 退出磋商小组的成员，其已完成的评审行为无效。由采购人向监督人员提出更换磋商小组成员意见并获准后，根据本磋商文件规定的磋商小组成员产生方式另行确定替代者进行评审。

12.2 记名投票

在评审过程中，磋商小组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，由磋商小组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，属于供应商相互串通报价：

13.1.1 供应商之间协商响应报价等响应文件的实质性内容；

13.1.2 供应商之间约定成交供应商；

13.1.3 供应商之间约定部分供应商放弃报价或者成交；

13.1.4 属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同报价；

13.1.5 供应商之间为谋取中标或者排斥特定供应商而采取的其他联合行动。

13.2 有下列情形之一的，视为供应商相互串通报价，磋商小组应当出具违法违规认定意见并作响应无效处理：

13.2.1 不同供应商的响应文件由同一单位或者个人编制；

13.2.2 不同供应商委托同一单位或者个人办理报价事宜；

13.2.3 不同供应商的响应文件载明的项目管理成员为同一人；

13.2.4 不同供应商的响应文件异常一致或者响应报价呈规律性差异；

13.2.5 不同供应商的响应文件相互混装；

13.3 有下列情形之一的，属于采购人与供应商串通报价：

13.3.1 采购人在递交响应文件截止时间前开启响应文件并将有关信息泄露给其他供应商；

13.3.2 采购人直接或者间接向供应商泄露标底、磋商小组成员等信息；

13.3.3 采购人明示或者暗示供应商压低或者抬高响应报价；

13.3.4 采购人授意供应商撤换、修改响应文件；

13.3.5 采购人明示或者暗示供应商为特定供应商中标提供方便；

13.3.6 采购人与供应商为谋求特定供应商中标而采取的其他串通行为。

在开启响应文件、评审过程中发现以上违法违规情形的，首先由磋商小组作出认定，对认定确有以上违法违规情形的供应商，按无效报价处理，再进入正常评审程序。

14. 违规处理

供应商有下列情形之一的，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 提供虚假报价材料谋取中标、成交的；

14.2 采取不正当手段诋毁、排挤其他供应商的；

14.3 与采购人、其他供应商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 拒绝有关部门监督检查或者提供虚假情况的；

14.6 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；

14.7 捏造事实、提供虚假材料或者以非法手段取得证明材料进行投诉的；

14.8 法律、法规和磋商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

采购人不得泄漏竞争性磋商活动中应当保密的情况和资料，不得与供应商串通损害国家利益、社会公共利益或者他人合法权益。

2. 对供应商的纪律要求

供应商不得互相串通或者与采购人串通报价，不得向采购人或者磋商小组成员行贿谋取中标；不得以他人名义报价或者以其他方式弄虚作假骗取中标；供应商不得以任何方式干扰、影响评审工作。

3. 对磋商小组成员的纪律要求

磋商小组成员不得收受他人的财物或者其他好处，不得向他人透漏对响应文件的评审和比较、中标候选人的推荐情况以及评审有关的其他情况。在评审活动中，磋商小组成员应当客观、公正地履行职责，遵守职业道德，不得擅离职守，影响评审程序正常进行，不得使用超出本磋商文件有关规定的评审因素和评审标准进行评审。

4. 对与评审活动有关的工作人员的纪律要求

与评审活动有关的工作人员不得收受他人的财物或者其他好处，不得向他人透漏对响应文件的评审和比较、中标候选人的推荐情况以及评审有关的其他情况。在评审活动中，与评审活动有关的工作人员不得擅离职守，影响评审程序正常进行。

第九章　签订合同、合同主要条款

1. 签订合同

1.1 采购人应当自成交通知书发出之日起 10 个工作日内，按照磋商文件和成交供应商响应文件的约定，与成交供应商签订书面合同。所签订合同不得对磋商文件和成交供应商响应文件作实质性修改。

1.2 签订的合同原则以本章第 4 条的规定为基础，并根据评审、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。采购人不得向成交供应商提出任何不合理的要求，作为签订合同的条件，不得与成交供应商私下订立背离合同实质性内容的协议。

1.3 磋商文件、响应文件、书面承诺和成交通知书均作为采购合同的一部分，且具有法律效力。成交供应商应严格履行采购合同所规定的各项义务和责任，否则将依法处理。

1.4 有关法规或者磋商文件明确不允许分包方式履行合同的，成交供应商不得分包履行合同，否则将依法承担法律责任。磋商文件明确允许分包方式履行合同的，按照磋商文件相关规定执行。

当成交供应商放弃成交结果或者因被质疑、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成交供应商，但应符合相关规定；否则采购人应重新组织采购。

1.5 采购人应当自采购合同签订之日起 2 个工作日内，将采购合同在青岛市政府采购网上公开，并同步完成政府采购合同备案工作。

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。

1.7 甲方支持乙方按照《青岛市财政局青岛市民营经济发展局关于进一步做好政府采购合同信用融资工作的通知》（青财采〔2019〕20 号）规定享受信用融资政策。如乙方按照文件规定向政府采购合同信用融资平台合作金融机构申请贷款，甲方承诺无条件允许乙方将本合同约定的收款账号变更为相应贷款合同约定的还款账号，为信用融资业务的顺利开展提供便利。变更账号应当在政府采购合同信用融资平台备案锁定。

1.8 依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）规定享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

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，可以与成交供应商协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的 10%，否则采购人应重新组织采购。

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 磋商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磋商文件、响应文件、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：由采购人和中标供应商商定。

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

第一条 合同标的

服务名称：

服务内容：

……

技术标准：

……

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，该价款包括了服务价格及与之配套的设计、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　服务交付

1、交付日期：

2、交付地点：

……

第四条　交付验收

1、甲方应当根据国家、行业验收标准，以及合同约定验收方案，明确验收时间、方式、程序和内容等事项，组成验收小组，在收到乙方项目验收建议之日起7个工作日内，对采购项目进行实质性验收（验收建议有明显不当的除外）。乙方应对提交的服务成果作出全面检查和整理，并列出清单，作为甲方验收和使用技术条件依据，清单应随提交的服务成果交给甲方。

2、对大型或复杂的政府采购项目，甲方应当邀请国家认可的质量检测机构参与验收工作，并出具验收报告，相关费用负担由甲乙双方约定。

3、乙方在指定地点提交服务成果后，甲乙双方应依据招标文件、投标文件等文件材料的要求共同验收，并且出具书面验收报告，履约验收报告应当依法依规及时在青岛市政府采购网公开发布。

……

第五条　所有权归属

乙方将服务成果交付甲方，并且经甲乙双方共同验收合格后所有权转移给甲方，在所有权转移之前，标的物损毁、灭失的风险归乙方，乙方保证所交付的服务成果的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

如乙方交付的服务成果有产权瑕疵的，视为乙方违约，乙方须向甲方支付20%的违约金；如果合同总金额价款已经支付完毕或者开始支付合同价款时才发现产权有瑕疵的，乙方仍须支付上述违约金并且赔偿甲方由此所遭受的一切损失。

第六条　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。

……

第七条　款项支付

1、服务成果交付甲方，经甲乙双方共同验收合格后由甲方负责办理支付手续。

2、允许并鼓励乙方提供电子发票，甲方自收到发票之日起5个工作日内支付资金，并不得附加未经约定的其他条件。

3、付款方式

3.1 预付款比例：____%，于政府采购合同签订生效并具备实施条件后 5 个工作日内支付。

……

第八条　履约保证金

1、乙方须向甲方交纳人民币（大写）_____（￥_____）元作为本合同的履约保证金。允许以银行、保险公司出具的担保支票、押金证明、保险单、保函、信用证等形式提交履约保证金。

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、履约保证金在服务交付验收合格____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后20个工作日内退还。

……

第九条　售后服务及承诺

1、服务质量保证期限自提交服务验收合格之日起_____年，在质量保证期内，乙方应对服务出现的问题负责处理并承担一切费用，并且赔偿甲方的损失。

2、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。

3、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，待验收后移交。

4、服务范围：负责招标文件所涉及到的所有服务。

……

第十条　知识产权

1、乙方保证，甲方在享受服务或者服务的任何一部分时，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、保证所提供服务为投标文件承诺服务，符合相关法律法规规定并且满足甲方的需求，保证其配套项目部件为全新的未使用的且符合相关的质量要求。

2、保证所提供服务的售后服务，严格依据投标文件及相关承诺，对服务以及与之配套的项目进行保修、维护等服务。

3、保证其所供服务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、乙方所供服务成果及与之配套项目等不符合合同约定标准，甲方有权拒收。同时，乙方向甲方支付合同总金额20%的违约金。

2、乙方不能交付服务成果时，乙方向甲方支付合同总金额20%的违约金。

3、乙方逾期交付服务成果时，每逾1日乙方向甲方支付合同总金额3‰的滞纳金。逾期交付超过30日，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，乙方向甲方支付合同总金额20%的违约金，并且赔偿甲方因此所遭受的损失。

4. 甲方逾期退还履约保证金的违约责任：_____。

5. 甲方逾期支付资金的违约责任：_____。

6. 因甲方原因导致变更、中止或者终止政府采购合同的，甲方对供应商受到的损失予以赔偿或者补偿：_____。

7、因甲方过错而给乙方造成的损失，由甲方负担。

……

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以后，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　合同生效及其他

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（或者被授权代表）签字并加盖单位公章。

3、本合同一式六份，甲方一份，乙方一份，采购代理机构二份，同级财政部门一份，青岛市崂山区行政审批服务局一份。

……

第十八条　服务期限

本合同服务期限为__年；服务期限自 ____年____月___日起至___年___月___日止。本合同期限届满，如需续签，根据《政府采购目录》有关规定，经财政部门批准，双方可以根据法律及各项规定另行签订书面合同。

第十九条　下列文件为本合同不可分割部分

1、政府采购招标文件（包括澄清、修改）；

2、乙方投标文件；

3、中标（成交）通知书；

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；

5、政府采购委托协议书；

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

第十章　响应文件格式

响应文件

包：第　包

资格审查部分

项目名称：

项目编号：

供应商名称（公章）：

二〇　　年　　月　　日

资格审查文件目录

1、营业执照或登记证书等（第三章序号1要求的内容)；；

2、资格证书（如有)；

3、在经营活动中无重大违法记录和行贿犯罪记录、具有良好商业信誉和健全财务会计制度、具有依法缴纳税收和社会保障资金良好记录的声明函(见附件1)；

4、磋商文件要求的其他资格证明材料。

附件 1：

声明函

一、我方在参加_____（项目名称）政府采购活动前 3 年内，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供应商_____、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_____）。

二、我方在参加本项目活动前一段时间内具有良好的商业信誉和健全的财务会计制度、具有依法缴纳税收和社会保障资金的良好记录。

若以上声明不实，我方自愿承担一切法律后果。

供应商名称：_____

日 期：_____年___月___日

备注：1.磋商文件未要求项目负责人的，项目负责人一栏可删除。

政府采购诚信承诺书

青岛市崂山区行政审批服务局，（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：_____）响应文件，自愿参加本次采购，现就有关事项做出郑重承诺如下：

一、诚信投标，材料真实。我公司保证所提供的全部材料、投标内容均真实、合法、有效，保证不出借或者借用其他企业资质，不以他人名义投标，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；不向磋商小组、采购人提供利益以牟取成交。

三、若成交后，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投标资格、记入信用档案、媒体通报、1-3年内禁止参与政府采购等处罚；如已成交的，自动放弃成交资格，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(公章)：

法定代表人（印章）：

年 月 日

响应文件

包：第　包

商务部分

项目名称：

项目编号：

供应商名称（公章）：

二〇　　年　　月　　日

商务文件目录

1、报价一览表(见附件2)；

2、所提供安全服务所需设备清单(见附件3)；

3、报价函(见附件4)；

4、法定代表人身份证明（见附件5）；

5、法定代表人授权委托书(见附件6)；

6、供应商同类项目实施情况一览表(见附件7)；

7、投标人同类项目业绩证明材料（若有）；

8、投标人荣誉（获奖）情况一览表；(见附件8) （若有）

9、投标人荣誉（获奖）证明材料；(若有)

10、商务响应表(见附件9)；

11、联合投标协议书（若有）(见附件10)；

12、联合投标授权委托书（若有）(见附件11)；

13、中小企业声明函（若有）(见附件12)；

14、残疾人福利性单位声明函（若有）(见附件13)；

15、监狱企业的证明（若有）；

16、节能、环保等的资质证书或者文件（若有）；

17、磋商文件其它规定或者供应商认为应介绍或者提交的资料、文件和说明（若有）。

附件2：

报价一览表

报价包：第_____包　　包名称：_____

序号	服务名称	说明	含税总报价（万元/年）	备注（取费依据、收费标准等）
1	崂山区电子政务外网安全提升服务费	包括崂山区电子政务外网安全提升所需要的全部设备、相关的二次开发、系统集成、安全管理、安全服务，使用到的各类安全软硬件设备、专用设备以及各组成部分之间所必须的各类互联线路、耗材费用，计入本项目。本次崂山区外网安全提升改造相关的技术实施工作内容将全部包含在本次服务费中，采购人不再单独支付相关费用		
总计		大写：		
		小写：		

注：

采购代理服务费由采购人支付的：供应商报价中无需考虑此费用。

时间：_____年_____ 月___日

附件 3：

所提供安全服务所需设备清单

投标包：第_____包　　包名称：_____

序号	设备名称	品牌	产地	规格型号	数量及单位
1					
2					
3					
	……				

时间：_____年_____ 月___日

附件4：

报价函

（采购人）：

（供应商名称）系中华人民共和国合法企业，经营地址_____。

我（姓名）系（供应商名称）的法定代表人，我方愿意参加贵方组织的（项目名称）（编号为_____）的报价，为此，我方就本次报价有关事项郑重声明如下：

1、我方已详细审查全部磋商文件，同意磋商文件的各项要求。

2、我方向贵方提交的所有响应文件、资料都是准确的和真实的。

3、若中标，我方将按照磋商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、响应文件自开启响应文件日起有效期为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。

供应商名称（公章）：

法定代表人（印章）：

日 期：_____

附件5：

法定代表人身份证明

供应商名称：_____

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_____（供应商名称）的法定代表人。

特此证明。

附：法定代表人身份证复印件。

附件6：

法定代表人授权委托书

（采购人）：

我（姓名）系（供应商名称）法定代表人，现授权委托我公司的（姓名、职务或者职称）为我公司本次_____项目的授权代表，代表我方办理本次报价、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。

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。被授权人签署的所有文件（在授权书有效期内签署的）不因授权撤销而失效。

被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被授权代表身份证复印件）

被授权代表姓名：　　性　别：　　年　龄：

单　位：　　部　门：　　职　务：

供应商名称（公章）：

法定代表人（印章）：

日　期：　　年　　月　　日

附件7：

供应商同类项目实施情况一览表

报价包：第_____包　　包名称：_____

序号	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）	附件电子文档是否上传			
						成交通知书	合同	验收报告	采购单位联系人及电话

附件8：

投标人荣誉（获奖）情况一览表

投标包：第_____包　　包名称：_____

序号	荣誉（获奖）名称	荣誉（获奖）内容	颁发机构	获奖时间

时间：_____年_____ 月___日

附件9：

商务响应表

报价包：第_____包　　包名称：_____

项目	磋商文件要求	是否响应	供应商的承诺或者说明
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10：

联合投标协议书(若有)

甲方：

乙方：

（如果有的话，可按照甲、乙、丙、丁…序列增加）

联合体各方经协商，就响应 _____组织实施的编号为_____号的采购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，并按照磋商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磋商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采购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，并作为响应文件的一部分。

甲方单位：　　（公章）　　乙方单位：　　（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：

联合投标授权委托书(若有)

本授权委托书声明：根据 _____与_____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、评审、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。

授权人（印章）：

日期：　　年　月　日

代理人（印章）：

日期：　　年　月　日

联合体甲方单位：　　（公章）

法定代表人：　　（印章）

日期：　　年　月　日

联合体乙方单位：　　（公章）

法定代表人：　　（印章）

日期：　　年　月　日

附件12：

中小企业声明函（工程、服务）

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，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

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

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

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

2.《中小企业声明函》由参加政府采购活动的供应商出具。以联合体形式参加政府采购活动或者合同分包的，声明函中需填写联合体中的中小企业或签订分包意向协议的中小企业相关信息，供应商应当在声明函“项目名称”部分标明联合体中中小企业承担的具体内容或者中小企业的具体分包内容。

附件13：

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。

供应商名称：

日　期：

响应文件

包：第　包

技术部分

项目名称：

项目编号：

供应商名称（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、技术响应表以及产品彩页等图片介绍资料（见附件：14）；

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）（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、供应商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、磋商文件技术评审办法中要求提交的相关证明材料复印件；

11、供应商需要说明的其他文件和说明（格式自拟）。

附件13：

货物清单（如有）

报价包：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

报价包：第_____包　　包名称：_____

序号	磋商文件要求	响应文件响应	偏离情况
1			
2			
3			
4			
5			
6			

注：

1、供应商应根据报价设备的性能指标、对照磋商文件技术指标要求，如实逐条一一对应填写响应情况，如有未响应技术指标，磋商小组有权视其为负偏离；

2、请供应商在“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、磋商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）

报价包：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

报价包：第_____包　　包名称：_____

姓　名	职务	专业技术资格	证书编号	参加本单位工作时间	劳动合同编号

注：在填写时，如本表格不适合供应商的实际情况，可根据本表格式自行制表填写。

附件 17：

_____项目政府采购履约验收(服务类样本)

<table>
<tr><td>采购单位</td><td colspan="2"></td><td>项目名称</td><td colspan="2"></td><td>合同名称</td><td colspan="2"></td></tr>
<tr><td>供应商</td><td colspan="2"></td><td>项目及合同编号</td><td colspan="2"></td><td>合同金额</td><td colspan="2"></td></tr>
<tr><td>分期验收</td><td colspan="2">是☐　否☐</td><td>分期情况</td><td colspan="4">共分　期，此为第　期验收</td></tr>
<tr><td>验收时间</td><td colspan="2"></td><td>验收地点</td><td colspan="2"></td><td>验收组织形式</td><td colspan="2">☐自行简易验收
☐验收小组验收</td></tr>
<tr><td rowspan="2">验收内容</td><td>服务质量</td><td>服务进度</td><td>人员、设备
配备情况</td><td>安全标准</td><td>服务承诺实现</td><td colspan="3">合同履约时间、
地点、方式</td></tr>
<tr><td>合　格☐
不合格☐</td><td>按　时☐
不按时☐</td><td>合　格☐
不合格☐</td><td>合　格☐
不合格☐</td><td>合　格☐
不合格☐</td><td colspan="3">合　格☐
不合格☐</td></tr>
<tr><td>专业检测机构
情况说明</td><td colspan="8"></td></tr>
<tr><td>存在问题
和改进意见</td><td colspan="8"></td></tr>
<tr><td>最终结论</td><td colspan="4">合　格☐</td><td colspan="4">不合格☐</td></tr>
<tr><td>验收小组
成员签字</td><td colspan="8"></td></tr>
<tr><td colspan="4">采购代理机构意见</td><td colspan="5">采购单位意见</td></tr>
<tr><td colspan="4">经办人：　　负责人：　　（采购代理机构公章）</td><td colspan="5">经办人：　　负责人：　　（采购单位公章）</td></tr>
<tr><td colspan="9">供应商确认：
（单位公章或授权代表签字）</td></tr>
</table>

说明：1.该表为服务类项目履约验收的参考样表，采购人或采购代理机构可以根据工作实际进行调整。

2.“采购代理机构意见”，履约验收工作由采购人自行组织的，无需填写该项内容。

附录　　符合性审查内容

序号	符合性审查内容	对应响应文件位置
2.1	响应文件不存在记录的 MAC 地址、CPU 序列号、硬盘序列号中两项及以上相同的情形	
2.2	响应文件响应谈判文件以下技术/服务要求	技术部分——技术响应表/服务响应表
2.2.1	★……	
2.2.2	★……	
2.3	按照谈判文件要求报价且不超过预算金额或最高限价	商务部分——报价一览表
2.4	响应有效期满足谈判文件要求	商务部分——报价函
2.5	响应文件响应谈判文件以下商务要求	商务部分——商务响应表
2.5.1	★……	
2.5.2	★……	
2.6	响应文件按照谈判文件要求编制、签章	资格审查——
2.7	响应文件未发现含有采购人不能接受的附加条件	
2.8	未发现供应商提供虚假材料、恶意串通、以行贿手段谋取中标等情形	
2.9	未发现法律、法规和谈判文件规定的其他无效情形	

备注：以上内容请根据谈判文件中实质性条款的规定和响应无效的情形填写完善。

附录1

通用竞磋服务类（综合评分法） 评分办法

序号	标题	分值	评分标准
通用竞磋服务类（综合评分法）［100.00］			
1	资格性审查［合格制］		
1.1	营业执照、登记证书、执业许可证等	合格制	具有独立承担民事责任的企业或组织合法经营权的凭证（如:营业执照、登记证书、执业许可证等）
1.2	声明函	合格制	在经营活动中无重大违法记录和行贿犯罪记录、具有良好商业信誉和健全财务会计制度、具有依法缴纳税收和社会保障资金良好记录的声明函
1.3	崂山区公共资源交易网	合格制	供应商必须在开标截止时间前在崂山政务网（http://www.laoshan.gov.cn）公共资源交易模块"诚信考核"注册，提供加盖供应商公章的企业完成注册截图。
1.4	政府采购诚信承诺书	合格制	政府采购诚信承诺书
2	符合性审查［- -］		
2.1	投标文件雷同检查	合格制	投标文件不存在记录的MAC地址、CPU序列号、硬盘序列号中两项及以上相同的情形
2.2	对招标文件的技术/服务要求响应情况［合格制］		
2.2.1	对招标文件的技术/服务要求响应情况1	合格制	投标文件响应招标文件以下技术/服务要求（对应投标文件技术部分——技术响应表/服务响应表）
2.2.2	对招标文件的技术/服务要求响应情况2	合格制	★……
2.3	投标报价	合格制	按照招标文件要求报价且不超过预算金额或最高限价（对应投标文件商务部分——报价一览表）
2.4	投标有效期	合格制	投标有效期满足招标文件要求（对应投标文件商务部分——投标函）
2.5	对招标文件的商务要求响应情况［合格制］		
2.5.1	对招标文件的商务要求响应情况1	合格制	投标文件响应招标文件以下商务要求（对应投标文件商务部分——商务响应表）
2.5.2	对招标文件的商务要求响应情况2	合格制	（货物：交货期、交货地点、付款方式、售后服务要求、验收……） （服务：服务期限或者提供服务起止时间、服务保障要求……）
2.6	对招标文件的编制、签章要求响应情况	合格制	投标文件按照招标文件要求编制、签章
2.7	其他1	合格制	投标文件未发现含有招标人不能接受的附加条件
2.8	其他2	合格制	未发现投标人提供虚假材料、恶意串通、以行贿手段谋取中标等情形
2.9	其他3	合格制	未发现法律、法规和招标文件规定的其他无效情形
3	商务部分［24.00］		
3.1	投标报价	10.00	评标基准价C=所有有效标书投标报价(或最终价格)中的最低投标报价。 最终报价： 1、对于小型和微型企业制造的货物(服务)，给予小型和微型企业包括相互之间组成的联合体的产品 10% 的价格扣除，扣除后的价格为最终报价 2、大中型企业和其他自然人、法人或者其他组织与小型、微型企业组成的联合体，联合体协议中约定，小微企业的协议合同金额占比30% 以上的，给予 3% 的价格扣除，扣除后的价格为最终报价 报价得分 = 评标基准价 ÷（投标报价或者最终价格）× 满分
3.2	企业业绩	6.00	自2018年1月1日（以合同签订时间为准）以来已完成的同类（信息化运维服务）项目，每份得2分，最高得6分； 开标时投标文件中必须附合同电子扫描件加盖公章，否则不得分。

通用竞磋服务类（综合评分法） 评分办法

序号	标题	分值	评分标准
3.3	产品实力	6.00	选用核心安全产品（态势感知平台）生产厂商具有《国家信息安全测评信息安全服务资质》（安全工程类三级及以上）证书、微软MAPP计划成员单位证书、CMMI 5认证证书，每提供1份得2分，最多得6分； 注：投标人须提供证书等证明材料扫描件加盖公章，同时投标文件中提供相应扫描件，否则不予计分。
3.4	企业信誉	2.00	1.投标人自2017年1月1日至开标日截止获得过税务部门对企业纳税信用的A级评价的，有一年得1分，本项满分2分。须提供国家税务总局官网网上公示截图和查询网址，否则不予计分。 以上评分均需提供上述证明文件的扫描件，且扫描件应加盖投标人公章，否则不予计分。
4	**技术部分［76.00］**		
4.1	**响应情况［10.00］**		
4.1.1	基本分	8.00	基础分为8分。 优于招标文件非实质性要求的，每有1条加0.5分，最高加2分；对实质性要求，每出现1条正偏离，加1分，最高加2分。（以上两项最高加2分）。 非实质性条款每出现一条负偏离扣除基础分2分，扣完基础分为止。
4.1.2	正偏离	2.00	优于招标文件非实质性要求的，每有1条加0.5分，最高加2分；对实质性要求，每出现1条正偏离，加1分，最高加2分。（以上两项最高加2分）。
4.1.3	负偏离	0.00	非实质性条款每出现一条负偏离扣除基础分2分，扣完基础分为止。
4.2	安全功能现场演示	6.00	能够利用技术手段，将所投核心安全产品（态势感知平台）产生的安全事件信息自动对应到部门及业务系统，并通过金宏办公系统通知到相关责任单位。现场演示此功能，并通过现场登录金宏办公系统查验成功，得6分。演示时间控制在10分钟以内，演示超时评委有权直接叫停，未现场演示不得分。说明：演示设备须在投标截止时间前提交，供应商须提前自行调试相关演示设备。开标现场提供金宏网线。
4.3	**服务承诺［4.00］对要求的服务范围、服务内容、服务技术指标或等级保护级别标准、重点保障等响应程度或承诺进行综合评价： 完全响应或优于招标文件要求的，得2分；基本满足招标文件要求的，得1分，不满足招标文件要求的不得分。 投标人针对项目综合考虑，可提出招标要求外的优质附加服务承诺，优质的得2分，未提供不得分。**		
4.3.1	**对要求的服务范围、服务内容、服务技术指标或等级保护级别标准、重点保障等［2.00］对要求的服务范围、服务内容、服务技术指标或等级保护级别标准、重点保障等响应程度或承诺进行综合评价： 完全响应或优于招标文件要求的，得2分；基本满足招标文件要求的，得1分，不满足招标文件要求的不得分。**		
4.3.1.1	对要求的服务范围、服务内容、服务技术指标或等级保护级别标准、重点保障等	2.00	对要求的服务范围、服务内容、服务技术指标或等级保护级别标准、重点保障等响应程度或承诺进行综合评价：投标人针对项目综合考虑，可提出招标要求外的优质附加服务承诺，优质的得2分，未提供不得分。
4.3.2	投标人针对项目综合考虑，可提出招标要求外的优质附加服务承诺，优质的得2	2.00	对要求的服务范围、服务内容、服务技术指标或等级保护级别标准、重点保障等响应程度或承诺进行综合评价：投标人针对项目综合考虑，可提出招标要求外的优质附加服务承诺，优质的得2分，未提供不得分。
4.4	**服务方案［25.00］服务商针对本项目组建专业的服务团队，对于服务团队组成、分工、业务能力、从业经验等表述真实完善的得6-4分；模糊简略的得3-1分；未提供不得分； 对崂山电子政务外网安全现状及需求描述准确详实的得6-4分；描述模糊的得3-1分；未提供不得分； 服务方案总体设计内容完整、结构合理、针对性强，符合招标文件实际需求的得6-4分；服务方案设计简略，部分满足招标需求的，得3-1分，未提供不得分。 文档资料交付方案内容全面，涵盖项目整个生命周期的资料交付模板内容符合招标实际需求的，得4-3分；方案模糊简略的，得2-1分；未提供不得分。 在满足招标文件要求的基础上，能结合崂山区实际情况及行业发展趋势，提出合理化的优化建议，充分展现投标人专业性的，得2-1分；未提供不得分**		

通用竞磋服务类（综合评分法） 评分办法

序号	标题	分值	评分标准
4.4.1	**服务商针对本项目组建专业的服务团队，对于服务团队组成、分工、业务能力、［6.00］服务商针对本项目组建专业的服务团队，对于服务团队组成、分工、业务能力、从业经验等表述真实完善的得6-4分；模糊简略的得3-1分；未提供不得分；**		
4.4.1.1	对崂山电子政务外网安全现状及需求描述准确详实的得6-4分；描述模糊的得3-1	6.00	对崂山电子政务外网安全现状及需求描述准确详实的得6-4分；描述模糊的得3-1分；未提供不得分；
4.4.2	对崂山电子政务外网安全现状及需求描述准确详实的得6-4分	6.00	对崂山电子政务外网安全现状及需求描述准确详实的得6-4分；描述模糊的得3-1分；未提供不得分；
4.4.3	服务方案总体设计内容完整、结构合理、针对性强，符合招标文件实际需求的得	6.00	服务方案总体设计内容完整、结构合理、针对性强，符合招标文件实际需求的得6-4分；服务方案设计简略，部分满足招标需求的，得3-1分，未提供不得分。
4.4.4	文档资料交付方案内容全面，涵盖项目整个生命周期的资料交付模板内容符合招	4.00	文档资料交付方案内容全面，涵盖项目整个生命周期的资料交付模板内容符合招标实际需求的，得4-3分；方案模糊简略的，得2-1分；未提供不得分。
4.4.5	在满足招标文件要求的基础上，能结合崂山区实际情况及行业发展趋势，提出合	3.00	在满足招标文件要求的基础上，能结合崂山区实际情况及行业发展趋势，提出合理化的优化建议，充分展现投标人专业性的，得3-1分；未提供不得分
4.5	**售后服务［15.00］整体售后服务方案合理、措施有力、切实可行的得5-3分；模糊简略的得2-1分；未提供不得分 组织机构及服务质量保证措施、保密措施等能做到机构健全，建立完整的工作台帐、工作信息收集、反馈等客户质量保证措施，得5-3分；模糊简略的，得2-1分；未提供不得分 制定详细的专业培训计划，培训方案内容全面、措施有力，具有完善的技术支持方案的得5-3分；培训方案内容完整，技术支持方案不完备的得2-1分；未提供不得分。**		
4.5.1	整体售后服务方案合理、措施有力、切实可行的得5-3分；模糊简略的得2-1分；	5.00	整体售后服务方案合理、措施有力、切实可行的得5-3分；模糊简略的得2-1分；未提供不得分
4.5.2	组织机构及服务质量保证措施、保密措施等能做到机构健全，建立完整的工作	5.00	组织机构及服务质量保证措施、保密措施等能做到机构健全，建立完整的工作台帐、工作信息收集、反馈等客户质量保证措施，得5-3分；模糊简略的，得2-1分；未提供不得分
4.5.3	制定详细的专业培训计划，培训方案内容全面、措施有力，具有完善的技术支	5.00	制定详细的专业培训计划，培训方案内容全面、措施有力，具有完善的技术支持方案的得5-3分；培训方案内容完整，技术支持方案不完备的得2-1分；未提供不得分。
4.6	**服务人员团队［12.00］对项目组组织结构、人员资格条件或技术能力、专业配置、从业经验等进行评价： 投标人安全服务团队至少1人拥有国家注册信息安全专业人员（CISP）认证证书且提供社保证明，得2分；投标人安全服务团队至少1人拥有高级信息系统项目管理师证书且提供社保证明的，得2分；投标人安全服务团队至少1人拥有HCIE或H3CIE证书且提供社保证明的，得1分；（提供上述证明文件的扫描件加盖投标人公章） 安全厂商安全服务技术支持团队经理(明确指定1人)具备PTE、ISO27001、ICSSE证书且提供社保证明，每提供一份得1分，最多得3分；安全厂商安全服务技术支持团队成员1人具备ICSSE证书且提供社保证明得1分；安全厂商安全服务技术支持团队成员1人具备CCIE证书且提供社保证明得1分；安全厂商安全服务技术支持团队成员具备PTE证书且提供社保证明，每提供一份得1分，最多得2分；（提供上述证明文件的扫描件加盖原厂公章）**		

通用竞磋服务类（综合评分法） 评分办法

序号	标题	分值	评分标准
4.6.1	投标人安全服务团队至少1人拥有国家注册信息安全专业人员（CISP）认证证书	2.00	对项目组组织结构、人员资格条件或技术能力、专业配置、从业经验等进行评价：投标人安全服务团队至少1人拥有国家注册信息安全专业人员（CISP）认证证书且提供社保证明，得2分
4.6.2	投标人安全服务团队至少1人拥有高级信息系统项目管理师证书且提供社保证明	2.00	对项目组组织结构、人员资格条件或技术能力、专业配置、从业经验等进行评价：投标人安全服务团队至少1人拥有高级信息系统项目管理师证书且提供社保证明的，得2分；提供上述证明文件的扫描件加盖投标人公章
4.6.3	投标人安全服务团队至少1人拥有HCIE或H3CIE证书且提供社保证明的，得1分；	1.00	对项目组组织结构、人员资格条件或技术能力、专业配置、从业经验等进行评价：投标人安全服务团队至少1人拥有HCIE或H3CIE证书且提供社保证明的，得1分；（提供上述证明文件的扫描件加盖投标人公章）
4.6.4	安全厂商安全服务技术支持团队经理(明确指定1人)具备PTE、ISO27001、ICSSE	3.00	对项目组组织结构、人员资格条件或技术能力、专业配置、从业经验等进行评价：安全厂商安全服务技术支持团队经理(明确指定1人)具备PTE、ISO27001、ICSSE证书且提供社保证明，每提供一份得1分，最多得3分；提供上述证明文件的扫描件加盖原厂公章
4.6.5	安全厂商安全服务技术支持团队成员1人具备ICSSE证书且提供社保证明得1分；	1.00	对项目组组织结构、人员资格条件或技术能力、专业配置、从业经验等进行评价：安全厂商安全服务技术支持团队成员1人具备ICSSE证书且提供社保证明得1分；（提供上述证明文件的扫描件加盖原厂公章）
4.6.6	安全厂商安全服务技术支持团队成员1人具备CCIE证书且提供社保证明得1分；（	1.00	对项目组组织结构、人员资格条件或技术能力、专业配置、从业经验等进行评价：安全厂商安全服务技术支持团队成员1人具备CCIE证书且提供社保证明得1分；（提供上述证明文件的扫描件加盖原厂公章）
4.6.7	安全厂商安全服务技术支持团队成员具备PTE证书且提供社保证明，每提供一份	2.00	对项目组组织结构、人员资格条件或技术能力、专业配置、从业经验等进行评价：安全厂商安全服务技术支持团队成员具备PTE证书且提供社保证明，每提供一份得1分，最多得2分；（提供上述证明文件的扫描件加盖原厂公章）
4.7	**应急保证［4.00］具有详细的应急保障方案得2-0分； 具有详细的应急流程，体现各类应急事件处理流程，应急管理架构清晰，人员职责分工明确得2-0分。**		
4.7.1	具有详细的应急保障方案得2-0分；	2.00	具有详细的应急保障方案得2-0分；
4.7.2	具有详细的应急流程，体现各类应急事件处理流程，应急管理架构清晰，人员职	2.00	具有详细的应急流程，体现各类应急事件处理流程，应急管理架构清晰，人员职责分工明确得2-0分。

其他注意事项

控制价　　：0.00

专家个数　　:3

投标人报价方式　　:总价（元）

定标方式　　:确定中标人