招 标 文 件

项目编号： XJCG-2022-GK005

项目名称： 仙居县公安局公共视频一体化及网络安全建设

采 购 人： 仙居县公安局

采购代理机构： 仙居县政府采购中心

2022 年 7 月

目　　录

第一章 公开招标公告

项目概况

仙居县公安局公共视频一体化及网络安全建设 招标项目的潜在投标人应在浙江政府采购网（网址 http：//zfcg.czt.zj.gov.cn/）获取（下载）招标文件，并于 2022 年 8 月 17 日 09 点 00 分（北京时间）前提交（上传）投标文件。

一、项目基本情况

项目编号：XJCG-2022-GK005

项目名称：仙居县公安局公共视频一体化及网络安全建设

预算金额（元）：24000000

最高限价（元）：23400000

采购需求：

标项序号	标项名称	简要技术需求	数量	单位	预算金额（元）	备注
1	仙居县公安局公共视频一体化及网络安全建设	见本招标文件中招标需求内容	1	项	24000000	

合同履行期限：本项目服务期限为三年，自项目初验完成之日起三周年

本项目不接受联合体投标。

二、申请人的资格要求

1.满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）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；

2.落实政府采购政策需满足的资格要求：无；

3.本项目的特定资格要求：具备《基础电信业务经营许可证》或《广播电视节目传送经营许可证》。

三、获取招标文件

时间：发布公告之日至2022年8月17日，每天上午00：00至12：00，下午12：00至23：59（北京时间，线上获取法定节假日均可）

地点（网址）：浙江政府采购网（http：//zfcg.czt.zj.gov.cn/）

方式：本项目招标文件实行网上获取，获取路径：浙江政府采购网—用户入驻/登录—用户登录—项目采购—获取采购文件管理（或者直接在公告下方选择“潜在供应商→获取采购文件”）。在浙江政府采购网采购公告附件中以“游客”身份（或仙居县人民政府 仙居县公共资源交易网）获取的招标文件仅供阅览，潜在供应商必须按已明确的“获取路径”获取招标文件，否则不得对招标文件提起质疑。

售价：0 元

四、提交投标文件截止时间、开标时间和地点

1.提交投标文件截止时间：2022 年 8 月 17 日 09：00（北京时间）

2.投标地点：

⑴电子加密投标文件：在“政府采购云平台”上传提交。“电子加密投标文件”成功上传提交后，投标人自行打印投标文件接收回执。

⑵备份投标文件：投标人自行确定是否提交。若提交请在投标文件截止时间前将备份投标文件打包压缩加密（未加密造成泄密的由投标人自行承担）后以电子邮件的形式发送至 jcbf2022@163.com 。

3.开标时间：2022 年 8 月 17 日 09：00（北京时间）

4.开标地点：仙居县公共资源交易中心开标室（四）（投标人无需在开标当天到达开标现场，但须准时在线参加）

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

1.《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》（浙财采监（2022）3 号）、《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22 号）已分别于 2022 年 1 月 29 日和 2022 年 2 月 1 日开始实施，此前有关规定与上述文件内容不一致的，按上述文件要求执行。

2.根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22 号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表:鼓励供应商在线提起

质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政府服务网-政府采购投诉处理-在线办理。

3.供应商认为采购文件使自己的权益受到损害的，可以自获取采购文件之日或者采购文件公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）起 7 个工作日内，以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、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作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

4.其他事项：⑴投标文件解密时间：开标时间后 60 分钟内供应商可以登录“政府采购云平台”的“项目采购-开标评标”，用制作电子标书的 CA 锁对电子加密投标文件进行解密。若供应商在规定时间内投标文件无法解密，或解密失败且备份文件读取失败（含未提交），则投标无效；

⑵本项目所有公告发布网站：浙江政府采购网（http：//zfcg.czt.zj.gov.cn）、仙居县人民政府 仙居县公共资源交易网（http：//www.zjxj.gov.cn/col/col1229347417/index.html）。项目如有更正或澄清公告，请各供应商自行及时登陆上述网站查看，采购代理机构不再作出书面通知；

⑶中标结果公告发出后，采购监管部门如发现供应商出现投标硬件异常的，若查证后存在违法事实的，将取消该供应商的中标资格，剩余供应商达 3 家及以上的，由采购人决定是否按中标顺位替补；不足 3 家的，该项目作废标处理。

七、对本次采购提出询问、质疑、投诉，请按以下方式联系

1.采购人信息

名称：仙居县公安局

地址：仙居县南峰街道环城南路 900 号

项目联系人（询问）：朱丹艳

项目联系方式（询问）：0576-89373601

质疑联系人：潘国星

质疑联系电话：0576-89373801

2.采购代理机构信息

名称：仙居县政府采购中心

地址：仙居县南峰街道泰和中路 6 号（吾悦广场东面）县人民政府行政服务中心二楼

项目联系人（询问）：应先生

项目联系方式（询问）：0576-89372058

质疑联系人：朱女士

质疑联系电话：0576-87716503

3.同级政府采购监督管理部门信息

名称：仙居县财政局

地址：仙居县南峰街道环城南路 500 号财政大楼

联系人：陈女士

监督投诉电话：0576-89375225

若对项目采购电子交易系统操作有疑问，可登录政采云（https://www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线 400-881-7190 获取热线服务帮助。

CA 问题联系电话（人工）：汇信 CA 400-888-4636；天谷 CA 400-087-8198。

仙居县政府采购中心

2022年7月26日

第二章 投标人须知

前附表

序号	项目	内容
1	联合体投标	☑ 不接受。 ☐ 接受。
2	现场踏勘	☑ 不组织。 ☐ 组织，详见第四章招标需求
3	答疑会	☑ 不召开。 ☐ 召开，详见第四章招标需求
4	分包	☑ 不允许。 ☐ 允许，但主体部分不得分包，详见第四章招标需求。
5	政府采购节能产品、环境标志产品	投标产品若属于节能（环境标志）产品的，请提供参与实施政府采购节能（环境标志）产品认证机构出具的认证证书或证书发布平台的投标产品认证证书查询截图；参与实施政府采购节能（环境标志）产品认证机构详见《市场监督管理总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告》（2019 第 16 号）；证书发布平台详见《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9 号）。产品属于政府强制采购节能品目的（详见《关于印发节能产品政府采购品目清单的通知》财库〔2019〕19 号），投标人须按上款要求提供节能产品认证证书或规定网站证书查询截图。**产品属于政府强制采购节能产品品目的，投标人未提供节能产品的，其投标将作无效标处理；本文件“第四章招标需求”另有规定的除外。**
6	小型、微型企业的价格扣除	1.对符合《政府采购促进中小企业发展管理办法》规定的小微企业报价给予 **20%** 的价格扣除；如项目接受联合体投标或者允许分包的，其中对于大中型企业与小微企业组成联合体或者大中型企业向一家或者多家小微企业分包的，对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，对其报价给予 **6%** 的价格扣除（组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策）。 2.投标人符合《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号）文件要求，并提供省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件（格式自拟），则视同小型、微型企业，享受小微企业价格扣除政策。 3.投标人符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）文件要求，并提供《残疾人福利性单位声

		明函》的，则视同小型、微型企业，享受小微企业价格扣除政策。 4.专门面向中小企业的项目，不享受价格扣除。
7	投标文件份数	1. 电子加密投标文件：政府采购云平台在线提交、上传一份； 2. 备份投标文件（政采云平台上最后生成的具备电子签章的备份投标文件，文件名后缀为备份文件四字的首字母）：电子邮件提交一份，由投标人自行确定是否提交；若提交请将备份投标文件打包压缩加密后以电子邮件的形式发送至jcbf2022@163.com。 注：投标人在线解密失败后，启用备份投标文件，否则不启用备份投标文件。
8	投标文件组成	投标文件由【资格证明文件】、【商务与技术文件】、【报价文件】三部分组成。
9	提交投标文件截止时间	见第一章公开招标公告
10	投标文件提交地点	见第一章公开招标公告
11	开标时间和地点	见第一章公开招标公告
12	投标有效期	自投标文件提交截止之日起 90 天内有效。
13	履约保证金	合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金（履约保证金要求详见“招标需求”内容）。采购人要求中标供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。
14	实质性条款	带“▲”的条款是实质性条款，投标文件须作出实质性响应，否则作无效投标处理。

一 、总则

（一）适用范围

本招标文件适用于本次项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

（二）定义

1.“采购人”系指委托采购代理机构采购本次项目的国家机关、事业单位和团体组织，具体见招标公告中采购人信息内容。

2.“采购代理机构”系指采购人委托组织招标的仙居县政府采购中心。

3.“投标人”系指按照本招标文件的规定参加并提交投标文件的自然人、法人或其他组织。

4.“产品”系指投标人按招标文件规定，须向采购人提供的一切产品（包括：虚拟产品），以及产品相关的保险、税金、备品备件、附件、耗材、工具、手册及其它有关技术资料和材料等。

5.“服务”系指投标人按招标文件规定应承担的送货上门、安装、调试、技术协助、维修、产品三包制度、校准、培训、技术指导以及其他类似的附随义务。

6.“项目”系指投标人按招标文件规定向采购人提供的产品和服务。

7.“书面形式”包括信函、传真等。

8.标有“▲”符号均属于“实质性条款”，不允许负偏离。

9.“电子交易平台”系指政府采购项目电子交易平台，即政府采购云平台（简称政采云平台）。

10.“电子投标文件”系指投标人通过“政采云电子交易客户端”编制的数据电文形式的“电子加密投标文件”。

11.“备份投标文件”系指与“电子投标文件”同时生成的数据电文形式的电子文件。

（三）采购组织类型

采购组织类型：政府集中采购。

（四）招标方式

本次招标采用公开招标方式进行。

（五）联合体投标

1.联合体投标：见投标人须知“前附表”内容；

2.联合体各方均符合政府采购法第二十二条第一款规定；

3.联合体中至少有一方符合本文件规定的特定资质要求。但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。

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。

5.联合体参与的，必须提供《联合体协议书》。

（六）投标费用

不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用。

（七）分包

1.分包：见投标人须知“前附表”内容。

2.若项目允许分包，投标人应根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

（八）政府采购政策

1.政府采购节能产品、环境标志产品：见投标人须知“前附表”中“政府采购节能产品、环境标志产品”内容。

2.根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）文件要求，中小企业参加政府采购活动，应当出具该办法规定的《中小企业声明函》（见附件），否则不得享受相关中小企业扶持政策。

属下列情形之一的给予价格扣除：

⑴对于非专门面向中小企业的项目，提供的货物全部由符合政策要求的小型和微型企业制造或服务全部由符合政策要求的小型和微型企业承接的，对其报价给予扣除，用扣除后的价格参与评审，价格扣除比例见投标人须知“前附表”中“小型、微型企业的价格扣除”内容；

⑵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项目，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扣除，用扣除后的价格参加评审，价格扣除比例见投标人须知“前附表”中“小型、微型企业的价格扣除”内容。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控

股、管理关系的，不享受价格扣除优惠政策。

3.投标人符合《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号）文件要求，并提供省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件（格式自拟），则视同小型、微型企业，享受小微企业价格扣除政策。

4.投标人符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）文件要求，并提供《残疾人福利性单位声明函》的，则视同小型、微型企业，享受小微企业价格扣除政策。

5.同一投标人（包括联合体），小微企业、监狱企业、残疾人福利性单位价格扣除政策只享受一次，不得重复享受。

6.专门面向中小企业的项目，不享受价格扣除。

（九）信用信息

投标人信用信息查询渠道及截止时点、信用信息查询记录和证据留存的具体方式、信用信息的使用规则：

1.查询渠道：中国政府采购网（网址：http：//www.ccgp.gov.cn）、信用中国（网址：http：//www.creditchina.gov.cn）；

2.查询截止时间：开标后评标前；

3.查询内容：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；

4.信用信息查询记录和证据留存的具体方式：信用信息查询记录和证据以网页页面打印（或截图）等方式进行留存；

5.使用规则：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供应商，将被拒绝其参与政府采购活动。

6.联合体成员存在不良信用信息记录的，视同联合体存在不良信用记录。

（十）特别说明

1.投标人投标所使用的采购项目实施人员必须为投标人员工（或投标人控股公司正式员工）。

2.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。

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。

（十一）质疑与投诉

1.投标人认为采购文件、采购过程、中标结果使自己的权益受到损害的，可以在知道或者应知其权益收到损害之日起七个工作日内，以书面形式向采购人、采购代理机构提出质疑（在法定质疑期内一次性提出针对同一采购程序环节的质疑）。

2.质疑函格式见《政府采购质疑和投诉办法》（财政部令第 94 号）附件范本，下载网址：浙江政府采购网(www.zjzfcg.gov.cn)，位置：“首页-下载专区-质疑投诉模板”。供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

a 供应商的姓名或者名称、地址、邮编、联系人及联系电话；

b 质疑项目的名称、编号；

c 具体、明确的质疑事项和与质疑事项相关的请求；

d 事实依据；

e 必要的法律依据；

f 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。质疑应明确阐述招标过程或中标结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理，质疑函不符合《政府采购质疑和投诉办法》相关规定的，应在规定期限内补齐的，自收到补齐材料之日起受理；逾期未补齐的，按自动撤回质疑处理。

3.质疑方式：质疑供应商可直接提交（含政采云平台在线质疑）、传真或邮寄方式提交质疑函（一式三份），以其他方式提出的质疑，采购人或采购代理机构将不予接受、答复。其中，以传真方式送达质疑书的，应及时将质疑书原件送达采购人或采购代理机构，采购人或采购代理机构以实际收到原件之日作为收到质疑的日期（在质疑期限届满前质疑书已经传真成功的，质疑不视为过期）；邮寄方式送达质疑书的，以采购人或采购代理机构实际收到邮件之日作为收到质疑的日期；通过政采云平台在线质疑（供应商需在线签章）和查看质疑答复，访问路径如下：政采云-项目采购-询问质疑投诉-质疑列表。

4.采购人或采购代理机构在收到质疑供应商的书面质疑后 7 个工作日内作出书面

答复（涉及项目资格要求和招标需求内容的由采购人答复）。

5.质疑供应商捏造事实、提供虚假材料进行质疑的，采购人或采购代理机构报告同级财政部门。情况属实的，列入不良行为记录并在指定的媒体上公告。

6.质疑供应商对采购人或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作出答复的，可以在答复期满后十五个工作日内向仙居县财政局投诉。

二、招标文件

（一）招标文件由招标文件总目录所列内容以及本项目招标文件的澄清、修改、补充的内容组成。

（二）招标文件的澄清或修改

1.采购人或采购代理机构可以对已发出的招标文件进行必要的澄清或者修改，澄清或者修改的内容可能影响投标文件编制的，采购代理机构应当在提交投标文件截止时间15日前，在原公告发布媒体上以更正公告的形式通知各潜在的投标人；不足15日的，采购代理机构有权顺延提交投标文件的截止时间。

2.澄清或者修改的内容作为招标文件的组成部分，对各投标人起同等约束作用。

3.当招标文件与澄清、修改、补充等文件就同一内容的表述不一致时，以最后发出的书面文件为准。

三、投标文件

（一）投标文件的形式和效力

1.投标文件形式：电子投标文件（包括“电子加密投标文件”和“备份投标文件”，“电子加密投标文件”和“备份投标文件”在投标文件编制完成后同时生成）。

2.投标文件的效力：“电子加密投标文件”和“备份投标文件”具有同等效力，数据电文内容应完全一致。

▲3.电子加密投标文件按时解密成功的，备份投标文件自动失效；电子加密投标文件解密失败，按时启动备份投标文件电子且有效的，以备份投标文件为准；电子加密投标文件解密失败，又未提交备份投标文件（包括提交备份投标文件未按时提供解密密码或密码错误的），视同放弃投标；仅提交备份投标文件的，投标无效。

（二）在线投标响应（电子投标）说明

1.本项目通过“政府采购云平台”实行电子投标，应按照本项目招标文件和政府采购云平台的要求编制。

2.标前准备：各投标人应及时完成CA数字证书办理，拿到CA后在政采云平台进行

绑定。因未办理 CA 数字证书等原因造成无法投标或投标失败等后果由投标人自行承担。

3.投标人通过“政府采购云平台”电子投标工具制作投标文件，电子投标工具请自行前往浙江政府采购网“下载专区-电子交易客户端”下载并安装，电子投标（政府采购项目电子交易管理操作指南-供应商）具体流程详见网址：https://service.zcygov.cn/#/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ8Na?keyword=政府采购项目电子交易操作指南，具体以政采云平台最新网址为准。

（三）投标文件的组成

投标文件由【资格证明文件】、【商务与技术文件】、【报价文件】三部分组成。

▲1.资格证明文件的组成：

⑴投标声明书；（见附件）

⑵授权委托书（法定代表人或营业执照中负责人亲自办理投标事宜的，提供法定代表人或营业执照中负责人有效的身份证）；（见附件）

⑶有效的营业执照（如事业单位参加投标的，则提供有效的《事业单位法人证书》）；

⑷具有良好的财务状况、依法缴纳税收和社会保障资金的承诺函（见附件）；

⑸具有履行合同所必需设备和专业技术能力的承诺函（见附件）；其中，电信、移动、联通等区域性分支机构参与投标的，还需提供总公司（总机构）授权（或出具总公司的有关文件或制度等能够证明总公司授权独立开展业务的证明）或提供房产权证或其他有效财产证明材料；

⑹提供招标公告中符合项目特定资格要求的有效资质证书（如有要求的，必须提供，其中电信、移动、联通等区域性分支机构参与投标的，必须提供总公司的《基础电信业务经营许可证》才能视为符合供应商特定资格要求）；

2.商务与技术文件的组成：

⑴投标人基本情况表；（见附件）

⑵投标方案描述：

A.对项目采购需求的了解及对应技术解决方案【包含且不限于对仙居公安现有网络基础情况了解程度、对仙居公安网络安全现状了解程度、技术解决方案、合理化建议等】；

B.项目服务方案【包含且不限于：1.针对招标需求中服务内容提出相应的服务方案（包括且不限于网络安全运营中心建设方案、等级保护测评服务方案、设备搬迁及临时开通方案、设备托管服务方案、售后服务方案及承诺等）；2.突发特殊情况下的应急保障方案（对自然灾害、安全事件等的服务应急预案及措施的详细表述）】；

C.项目组织实施方案（包含且不限于项目前期实施期限及实施进度安排、保证实施进度的措施、确保项目供货和质量的措施等）；

D.项目技术团队人员履历及能力说明（包含项目负责人及项目实施人员的资质、类似经验等，其中应明确中标后现场驻场技术人员情况）。（见附件）

⑶拟投入的主要软硬件设备情况；（见附件）

⑷投标人具有的质量管理和质量保证体系等等与本项目相关的认证证书或文件；（见附件）

⑸符合等保要求承诺书；（格式自拟）

⑹商务响应表；（见附件）

⑺近三年同类项目业绩（投标人同类项目业绩实施情况表、合同、中标（或成交）通知书以及验收报告（或验收证明）等）；（见附件）

⑻项目培训方案；

⑼投标人认为需要提供的其他资料（包括可能影响投标人商务与技术文件评分的各类证明材料）。

3.报价文件的组成

⑴报价文件由开标一览表、投标报价明细表、中小企业等声明函（如有，见附件），以及投标人认为其他需要说明的内容（包括政府采购优惠政策相关资料等，如有）组成。

⑵投标报价是包括与本服务项目相关的设备安装、调试、验收、培训合格之前所有含税费用、税金、光纤租赁费用、其他费用（包括质保期内的备品备件、易损件、专用工具等）、制造、包装、保险、运输、仓储、税金、验收、安装、售后服务、招标中规定的设备搬迁、各种人工费及技术支持等相关服务的费用、合同包含的所有风险责任等各项费用以及不可预见费等所需的全部费用，全部费用已包含在开标一览表的投标总报价中。

▲⑶投标文件只允许有一个报价（包含其它一切所要涉及到的费用），投标报价应按招标文件中相关附表格式填报，《开标一览表》的投标报价大写金额应与《投标报价明细表》的投标报价相等，明细出现“0”元，视同赠送。

（四）投标文件的编制、份数及提交要求

1.投标文件的编制要求

▲⑴本招标文件中若有多标项的，若参与多标项投标的，则按每个标项分别独立编制投标文件；

⑵电子投标文件编制请按政府采购云平台“政府采购项目电子交易管理操作指南-供应商”（网址：https://service.zcygov.cn/#/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAGOBFdiHxlNdQ8Na?keyword=政府采购项目电子交易操作指南，具体以政采云平台最新网址为准）和本招标文件要求编制并进行关联定位。

⑶投标人应按招标文件的要求提供相关资料，并对招标文件中提出的所有内容要求给予明确响应，须保证投标文件的准确、真实、明确。投标文件响应内容对招标文件要求如有偏离均应填写偏离表，如不填写，评标委员会有权视作投标文件不完全响应招标文件要求。

⑷投标文件编制时应有正确的索引目录及连续页码标注。因投标文件内容不完整、编排混乱导致投标文件被误读、漏读或者查找不到相关内容的责任由投标人自行承担。

⑸投标文件须清晰可辨，因模糊不清所引起的后果由投标人自行负责。与本次投标无关的内容请不要制作在内，确保投标文件有针对性、简洁明了。

⑹投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元）。

⑺投标文件以及投标人与采购代理机构就有关投标事宜的所有来往函电，均应以中文汉语书写，除签字、盖章、专用名称等特殊情形外。投标资料提供外文证书或者外国语视听资料的，应当附有中文译本，由翻译机构盖章或者翻译人员签名。

2.投标文件的份数及签署要求

⑴电子加密投标文件：政府采购云平台在线提交、上传一份；

⑵备份投标文件（政采云平台上最后生成的具备电子签章的备份投标文件，文件名后缀为备份文件四字的首字母）：电子邮件提交一份，由投标人自行确定是否提交；若提交请将备份投标文件打包压缩加密后以电子邮件的形式发送至 jcbf2022@163.com。

▲⑶投标文件内容中有要求盖章的地方，必须采用投标人 CA 签章。

3.投标文件的提交要求

⑴投标文件导入和加密

①投标人应当按照资格证明文件、商务与技术文件和报价文件三部分分别导入相应位置，各文件之间不得导错位置；

②投标文件编制好后应当生成电子加密投标文件，生成电子加密投标文件具体流程详见政府采购云平台“政府采购项目电子交易管理操作指南-供应商”，具体以政采云平台最新网址为准。

⑵投标文件的提交

①提交投标文件截止时间：见第一章公开招标公告；

②投标文件提交地点：

A.电子加密投标文件：电子加密投标文件在“政府采购云平台”上传提交。“电子加密投标文件”成功上传提交后，投标人自行打印投标文件接收回执。供应商应当在提交投标文件截止时间前完成电子加密投标文件的传输提交。

B.备份投标文件（政采云平台上最后生成的具备电子签章的备份投标文件，文件名后缀为备份文件四字的首字母）：投标人自行确定是否提交；若提交请将备份投标文件打包压缩加密（未加密造成泄密的由投标人自行承担）后以电子邮件的形式发送至jcbf2022@163.com ，备份投标文件在“电子加密投标文件”在线解密失败后启用，否则不予以启用；投标人确认“电子加密投标文件”在线解密失败后，将打包压缩加密的备份投标文件的解密密码在解密规定的时间内发送至上述邮箱，未在规定时间内发送造成的投标无效或失败由投标人自行承担。

⑶不予接收的投标文件情形

①提交投标文件截止时间前未完成传输的投标文件；

②未生成加密的投标文件；

⑷投标人所提交的投标文件不予退还。

⑸如有特殊情况，采购代理机构延长截止时间和开标时间，采购代理机构和投标人的权利和义务将受到新的截止时间和开标时间约束。

4.投标文件的补充、修改和撤回

⑴在提交投标文件截止时间前，投标人可对已提交的投标文件进行补充、修改或撤回。补充、修改投标文件的，应当先行撤回原文件，补充、修改后重新生成加密的投标文件并重新上传提交； 补充、修改后重新提交的投标文件应按招标文件的规定编制、加密、导入和提交。

⑵在提交投标文件截止时间后,投标人不得修改或撤回已提交的投标文件。

（五）备选投标方案

本项目不接受备选投标方案。

（六）投标文件的有效期

1.自投标截止日起 90 天投标文件应保持有效。有效期不足的投标文件将被拒绝。

2.在特殊情况下，采购人可与投标人协商延长投标文件的有效期，这种要求和答复

均以书面形式进行。

3.中标人的投标文件自开标之日起至合同履行完毕均应保持有效。

（七）投标诚实信用

1.投标人应当遵守诚实信用原则。

2.投标人有下列情形之一的，将会报告财政部门并按照相关规定处理：

⑴投标人在投标有效期内撤销投标文件的；

⑵未按规定提交履约保证金的；

⑶投标人在投标过程中弄虚作假，提供虚假材料的；

⑷中标人无正当理由不与采购人签订合同的；

⑸投标人有串通投标行为的；

⑹严重扰乱政府采购程序的；

⑺违反其他法律法规规定的情形。

四、开标

本项目开评标环节实行全流程电子化，采取政采云不见面开标大厅实现，投标人可自行登录政采云平台进入开标大厅观看现场直播画面。本项目通过政府采购云平台进行开标、资格审查、评审、询标，投标人均应当准时在线参加，否则产生的风险由投标人自行承担（投标人务必不要离开电脑太久，并留意手机短信，建议投标人提前做好检查“政府采购云平台”内，关于“项目采购”的岗位权限是否勾选）。

投标人可以登录“政府采购云平台”的“项目采购-开标评标”，在解密规定时间内用制作电子标书的CA锁对电子加密投标文件进行解密。

（一）开标事项

1.采购代理机构在“公开招标公告”规定的时间和地点进行开标。投标人的投标人代表应当在线参加，否则视同认可开标结果，事后不得对采购相关人员、开标过程和开标结果提出质疑。

2.评标委员会成员不得参加开标活动。

3.本次开标采用先评审资格证明文件和商务与技术文件，后评审报价文件的方式进行。

（二） 开标程序

1.开标会由采购代理机构工作人员主持，主持人宣布开标会开始，介绍参加开标会的相关人员。

2.宣布提交投标文件的投标人家数、投标人名称。

3.宣布开标纪律。

4.签署不存在影响公平竞争的《政府采购活动现场确认声明书》（见附件）。投标人应当通过邮件形式，将经授权代表签署的《政府采购活动现场确认声明书》发至采购代理机构电子邮箱 xjcg2009@163.com。

5.投标人进行在线解密（解密时间为开标时间后 60 分钟内）；解密未成功的，投标人应当在解密时间内向采购代理机构通过电子邮箱 jcbf2022@163.com 提供备份投标文件压缩解密密码，否则视为放弃投标。

6.采购人依法对资格证明文件进行审查，评标委员会对商务与技术文件进行评审。

7.商务与技术文件评审完成后，主持人宣告商务与技术文件评审无效投标人名称及理由，公布经商务与技术文件评审符合采购需求的投标人名单以及商务与技术文件得分情况。

8.开启各投标人报价文件，宣读《开标一览表》中的投标报价，以及采购代理机构认为有必要宣读的其他内容。

9.当场制作并打印开标记录表，由唱标人、记录人、监督人当场签字确认。投标人解密后可点击【查看开标记录】查看项目开标记录，并在规定时间内在线确认（投标人未确认的，不影响评标过程）。唱标结束后，由评标委员会对报价的合理性、准确性等进行审查核实。

10.评标结束后，主持人公布投标报价得分、综合得分以及推荐中标候选人排序名单。

11.开标会议结束。

五、评标

（一）组建评标委员会

本项目评标委员会由政府采购评审专家和采购单位评审代表组成。

（二）评标程序

1.资格审查

公开招标采购项目开标后，采购人应当依法对投标人的资格进行审查，对审查发现无效的进行必要的询标。

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，对审查发现无效的进行必要的询标。

3.比较与评价

⑴评标委员会依据招标文件的规定，对各投标人的商务与技术文件进行评价。若有演示环节要求的和商务与技术文件评审同步进行，并根据澄清、演示、样品等情况按评分标准进行独立打分；

⑵评标委员会依据招标文件的规定，对各投标人的报价的完整性、合理性进行审查，必要时可要求投标人对其报价做出澄清、说明（包括报价修正、政府采购政策价格扣除、报价明显偏低等等）；

⑶评标时，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。

4.得分确认及评审报告编写

⑴评标委员会对报价文件进行复核，对系统计算出的价格分及总得分进行确认，现场监督员应对评审结果签署监督意见。如发现分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致以及存在评分畸高、畸低情形的，应由相关人员当场改正或作出说明；拒不改正又不作说明的，由现场监督员如实记载后存入项目档案资料。

⑵评标委员会按评标原则及得分情况编写评审报告。

5.评价

采购代理机构对评审专家进行评价。

（三）澄清问题的形式

1.对于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，评标委员会应当通过政采云平台要求投标人作出必要的澄清、说明或者补正，给予投标人提交澄清说明或补正的时间不得少于 30 分钟，投标人已经明确表示澄清说明或补正完毕的除外。投标人务必在线等待，留意手机短信，及时通过政采云平台进行在线澄清、说明或补正。

2.投标人的澄清、说明或补正内容将作为投标文件的一部分。

（四）错误修正

1.“政府采购云平台”上开启的投标报价与电子投标文件中开标一览表（报价表）内容不一致的，以电子投标文件中开标一览表（报价表）为准。

2.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：

⑴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；

⑵大写金额和小写金额不一致的，以大写金额为准；

⑶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；

⑷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。修正应当通过电子交易平台交换数据电文，并加盖电子签章或者由法定代表人或其授权的代表签字。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。

（五）采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购组织机构可中止电子交易活动：

1.电子交易平台发生故障而无法登录访问的；

2.电子交易平台应用或数据库出现错误，不能进行正常操作的；

3.电子交易平台发现严重安全漏洞，有潜在泄密危险的；

4.病毒发作导致不能进行正常操作的；

5.其他无法保证电子交易的公平、公正和安全的情况。

出现前款规定情形，不影响采购公平、公正性的，采购组织机构可以待上述情形消除后继续组织电子交易活动，也可以决定某些环节以纸质形式进行；影响或可能影响采购公平、公正性的，应当重新采购。

（六）投标人存在下列情况之一的，投标无效

1.资格证明文件或商务与技术文件跟报价文件出现混装，或者在资格证明文件或商务与技术文件中出现投标报价的，或者报价文件中报价的货物跟商务与技术文件中的投标货物出现重大偏差的；

2.不具备招标文件中规定的资格要求的；

3.投标文件含有采购人不能接受的附加条件的；

4.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；

5.投标报价超过招标文件中规定的最高限价；

6.投标参数未如实填写，完全复制粘贴招标参数的；

7.投标人仅提交备份投标文件的；

8.电子加密投标文件解密失败或未按时解密的，且未在规定时间内提交备份投标文件的（包括未在解密规定时间内提供备份投标文件解密密码或密码错误的）；

9.投标文件提供虚假材料的；

10.不符合中华人民共和国财政部令第87号《政府采购货物和服务招标投标管理办法》第三十七条情形之一的，视为投标人串通投标，其投标无效，并移送采购监管部门：

⑴不同投标人的投标文件由同一单位或者个人编制；

⑵不同投标人委托同一单位或者个人办理投标事宜；

⑶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；

⑷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；

⑸不同投标人的投标文件相互混装；

11.不符合法律、法规以及招标文件中规定的无效标条款或其他实质性要求的（招标文件中打“▲”内容及被拒绝的条款）。

（七）有下列情况之一的，本次招标作为废标处理

1.符合资格要求的供应商或者对招标文件作实质响应的供应商不足三家的；

2.出现影响采购公正的违法、违规行为的；

3.投标人的报价均超过了采购预算，采购人不能支付的；

4.因重大变故，采购任务取消的；

5.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；

6.法律、法规和招标文件规定的其他导致评标结果无效的。

（八）评标原则和评标办法

1.评标原则。评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与投标人接触。

2.评标办法。具体评标内容及评分标准等详见《第三章 评标办法及评分标准》。

（九）评标过程的监控

1.本项目评标过程实行全程录音、录像监控，政府采购监管部门视情进行现场监督，投标人在评标过程中所进行的试图影响评标结果的不公正活动，可能导致其投标被拒绝。

2.评审过程中出现录音录像采集设备不能 正常运行的，应当立即封存评审资料、

中止评审活动，直至设备（或替代设备）运转正常或转移至符合条件的场所后继续进行评审工作。

六、定标

1.确定中标供应商。评标委员会根据采购单位的《授权意见确认书》，推荐中标候选人或确定中标人。其中推荐中标候选人的，采购代理机构在评审结束后 2 个工作日内将评审报告送采购人，采购人自收到评审报告之日起 5 个工作日内在评审报告推荐的中标候选人中按顺序确定中标人。

2.发布中标结果公告。采购代理机构应当自中标人确定之日起 2 个工作日内，在省级以上财政部门指定的媒体及相关网站上公告中标结果。中标结果公告将包括中标人名称、地址和中标金额，主要中标标的的名称、规格型号、数量、单价、服务要求以及评审专家名单等内容，但不包括国家秘密、商业秘密。

3.采购代理机构在发布中标结果公告的同时，通过政采云平台向中标人发放中标通知书。

4.中标通知书发出之日起至合同签订前，中标供应商不得开展项目实质性工作（如订货、施工等）。否则，造成的有关损失由中标供应商自行承担。

七、合同签订及公告

（一）签订合同

1.采购人应当自中标通知书发出之日起 30 日内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

2.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。

3.中标供应商无故拖延、拒签合同的，采购代理机构和采购人有权取消其中标资格。

4.中标供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。同时，拒绝与采购人签订合同的供应商，由同级财政部门依法作出处理。

5.询问或者质疑事项可能影响中标结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

（二）合同公告

采购人应当自政府采购合同签订之日起 2 个工作日内，在省级以上财政部门指定的政府采购信息发布媒体及相关网站上公告，但政府采购合同中涉及国家秘密、商业秘密

的内容除外。

八、验收

1.采购人组织对供应商履约的验收。大型或者复杂的政府采购项目，应当邀请国家认可的质量检测机构参加验收工作。验收方成员应当在验收书上签字，并承担相应的法律责任。如果发现与合同中要求不符，供应商须承担由此发生的一切损失和费用，并接受相应的处理。

2.采购人可以邀请参加本项目的其他投标人或者第三方专业机构及专家参与验收，相关验收意见作为验收的参考资料一并存档。

3.严格按照采购合同开展履约验收。采购人成立验收小组，按照采购合同的约定对供应商履约情况进行验收。验收时，按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料应当存档备查。

4.验收合格的项目，采购人将根据采购合同的约定及时向供应商支付采购资金、退还履约保证金。验收不合格的项目，采购人将依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。供应商在履约过程中有政府采购法律法规规定的违法违规情形的，采购人应当及时报告本级财政部门。

九、“政采贷”服务

为优化政府采购营商环境，缓解供应商资金难题，政采云平台已推广应用“政采贷”服务，中标供应商如有融资需求，可使用以下银行的政采贷服务。

银行名称	联系人	联系方式
中国工商银行	陈盈	13967614344
浙江泰隆商业银行	陈超	17858683697
浙江民泰商业银行	朱祖优	13858602876
中国建设银行	徐旭霞	15988932355
中国邮政储蓄银行	赵红芳	18968556112
农村商业银行	叶斌昇	13806593583
台州银行	朱翔	13819660917
中国农业银行	娄志伟	13958514828

十、履约保函、预付款保函相关说明

金融机构名称及意愿承担保函（保单）种类	保函（保单）收费情况	联系人及联系方式
机构名称：中国工商银行股份有限公司仙居支行 履约保函： 是 预付款保函：是	对外保函服务 1.开立及展期费担保费率： （1)融资性保函：期限在一年（含）以内，客户按担保额度 0.05-0.25%/月计收。最小计费周期为实际月（按实际发生天数，从保函生效之日至失效日计算，30 天为 1 月），期限不足 1 月的按 1 个月计收。最低 500 元 / 季。 （2)非融资性保函：期限在一年（含）以内，客户按 0.027-0.167%/月计收。最小计费周期为实际月（按实际发生天数,从保函生效之日至失效日计算,30 天为 1 月），期限不足 1 月的按 1 个月计收。最低 500 元 / 季。 （3)担保期限超过一年的,每增加一年整体费率提高 10%（单利）。若担保文本未明确确定的到期日或含有自动延展性质条款的，我行可按根据基础合同和担保文本的有关约定推算出的担保最长有效期调整对应的费率。 如企业划型为小微企业的，以上手续费全免。	陈盈 13967614344
机构名称：浙江泰隆商业银行台州仙居支行 履约保函：是 预付款保函：是 备注：我行目前只有线下模式	根据保证金比例不同，参照下述费率计收： 全额保证金，500 一年； 保证金比例 50%以下，保函敞口金额的 1.25‰/季，最低 500 元/季； 保证金比例 50%（含）以上，保函敞口金额的 1‰/季，最低 500 元/季。 涉及保函增额，增额部分参照开立保函收费标准另行收费，延期修改按照 300/次的标准另行收费； 按年收费项目不足一年按一年计收，超过一年三十天按照两年计收（从保函开立之日起 390 天（含）为一个年度三十天） 按季收费项目不足一季按一季度计收，超过一季度十天的按两季度计收（从保函开立之日起 100 天（含）为一个季度十天）	银行联系人：陈超 17858683697 具体保函业务办理客户经理：王英 17858683702
机构名称：仙居农商银行 履约保函：是 预付款保函：是	合同（质量）履约按履约保证金年费率万分之五，在出具保函前一次性收取。	李杭 13586233529
机构名称：仙居中国银行 履约保函：是 预付款保函：是	合同（质量）履约按履约保证金年费率 1%（1.5%），每单保函最低保险费为 500 元。	张弥 0576-87796908

机构名称：中国人民财产保险股份有限公司仙居支公司 履约保险：是 预付款保函：是	建设工程合同款支付保证保险，年费率 1.2%，每单最低保险费为 1000 元。 建设工程预付款保证保险，年费率 0.6%，每单最低保险费为 1000 元。	王巧红 13968483573
机构名称：中国大地财产保险股份有限公司仙居支公司 履约保函：是 预付款保函：否	合同（质量）履约按履约保证金年费率最低 0.5%，每单保函最低保险费为 1000 元。	吴琼 17858699170
机构名称：天安财产保险股份有限公司台州中心支公司仙居县营销服务部 履约保函：否 预付款保函：是	预付款保函：按预付款金额投保，年费率为 1%-2%，每单保函最低保险费为 500 元；保险期限最长不超过 5 年。	陶正鹏 13858613668
机构名称：仙居县台融融资担保有限公司 履约保函：是	合同（质量）履约按履约保证金年费率 0.2%，每单保函最低保险费为 800 元。	郭鹏飞 13819645716

第三章 评标办法及评分标准

根据《中华人民共和国政府采购法》等有关法律法规，结合本项目的实际需求，制定本办法。

一、总则

1.本项目评标采用综合评分法，总分为100分（商务与技术文件得分权重为 90 %，评分分值为 90 分；报价文件得分权重为 10 %，评分分值为 10 分）。各合格投标人的评标综合得分为其商务与技术文件得分与报价文件得分之和，中标候选资格按评标综合得分由高到低顺序排列，综合得分相同的，按投标报价由低到高顺序排列；综合得分且投标报价相同的，按技术分得分由高到低顺序排列。如合格投标人数量超过三家，原则上只推荐三家中标候选供商。

2.相同品牌认定标准。使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

非单一产品采购项目，多家投标人提供的核心产品品牌相同的，按前款规定处理。

3.评分过程中采用四舍五入法，并保留小数2位（以政采云系统计算为准）。

二、分值的计算

评标综合得分=商务与技术文件得分（商务资信分+技术分）+报价文件得分（价格分）。

1.商务与技术文件中的客观分由评标委员会统一意见后统一给分，其余在规定的分值内独立评定打分。

2.各有效投标人的商务与技术文件得分按照评标委员会成员的独立评分结果汇总后的算术平均值计算，计算公式为：

商务与技术文件得分=评标委员会所有成员评分合计数/评标委员会组成人员数。

3. 价格扣除（专门面向中小企业的项目，不享受价格扣除）：

因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。价格扣除比例见投标人须知“前附表”中“小型、微型企业的价格扣除”内容。

调整后的投标报价＝投标报价×（1-扣除比例）

4.评分内容及标准

序号	评分内容	评分标准	分值
一、商务资信分			**4 分**
1	认证证书	1.投标人具有有效期内的 ISO9001 质量管理体系认证证书，提供证书原件扫描件或复印件，有得 1 分，没有不得分。 2.投标人具有有效期内的信息安全管理体系认证证书，提供证书原件扫描件或复印件，有得 1 分，没有不得分。 3.投标人具有有效期内的信息技术服务管理体系认证证书，提供证书原件扫描件或复印件，有得 1 分，没有不得分。	3
2	业绩	投标人近三年内（自投标截止之日起往前追溯，以合同签订时间为准）具有同类服务项目合同业绩的，每个合同得 0.5 分，本项最高得 1 分。 **注：合同、中标（或成交）通知书、验收报告（或验收证明）必须同时编入商务与技术文件，否则不得分。**	1
二、技术分			**86 分**
3	对项目需求的了解及对应技术解决方案	1.投标人应充分了解仙居公安网络基础情况，包括网络拓扑、机房现状、现有设备情况，根据投标人对网络基础情况了解程度，从提供的网络现状拓扑图、机房基础设施情况、现有设备清单等情况由评标委员会判定评分，最高得 5 分。	5
		2.投标人应充分了解仙居公安网络安全现状情况，包括现有安全设备、当前存在的安全隐患,根据投标人对网络安全现状情况了解程度，从提供现有的网络安全设备清单、网络安全隐患、基础（电力、环境）保障问题等情况，由评标委员会判定评分，最高得 5 分。	5
		3.投标人应提供对应技术解决方案，提供建设后的网络拓扑图，明确建设内容，并对拓扑图各项建设内容进行阐述,根据投标人提供的对应技术解决方案与本项目需求的响应程度，从提供的拓扑图各项建设内容的针对性、合理性、科学性，由评标委员会判定评分，最高得 5 分。	5
		4.根据投标人提供针对项目的合理化建议，由评标委员会判定评分，最高得 2 分。	2
4	项目服务方案	网络安全运营中心建设方案：根据投标人提供的网络安全运营中心建设方案（重点内容为信息安全驾驶舱建设，通过建设信息安全驾驶舱，实现对仙居县信息安全态势的充分感知，并为领导决策提供有效依据，打造仙居网络安全亮点特色）进行评分，内容全面完整、科学合理的得 4 分。内容存在欠完整或欠合理的每项（次）扣 0.5 分，内容不完整或不合理的每项（次）扣 1 分，扣完为止。未提供或被评标委员会认定为无效的，此项不得分。	4

		等级保护测评服务方案：根据投标人提供的等级保护测评服务方案进行评分，内容全面完整、科学合理的得 4 分。内容存在欠完整或欠合理的每项（次）扣 0.5 分，内容不完整或不合理的每项（次）扣 1 分，扣完为止。未提供或被评标委员会认定为无效的，此项不得分。	4
		设备搬迁及临时开通方案：根据投标人提供的设备搬迁及临时开通方案进行评分，内容全面完整、科学合理的得 4 分。内容存在欠完整或欠合理的每项（次）扣 0.5 分，内容不完整或不合理的每项（次）扣 1 分，扣完为止。未提供或被评标委员会认定为无效的，此项不得分。	4
		设备托管服务方案：根据投标人提供的设备托管服务方案进行评分，内容全面完整、科学合理的得 4 分。内容存在欠完整或欠合理的每项（次）扣 0.5 分，内容不完整或不合理的每项（次）扣 1 分，扣完为止。未提供或被评标委员会认定为无效的，此项不得分。	4
		售后服务方案及承诺：根据投标人提供的售后服务方案、售后服务承诺的可行性、完整性以及服务承诺落实的保障措施，服务期内外的后续技术支持和服务维护能力情况等，由评标委员会判定评分，最高得 2 分。	2
		突发特殊情况下的应急保障方案：根据投标人提供的应急保障方案进行评分，内容全面完整、科学合理的得 2 分。内容存在欠完整或欠合理的每项（次）扣 0.5 分，内容不完整或不合理的每项（次）扣 1 分，扣完为止。未提供或被评标委员会认定为无效的，此项不得分。	2
5	项目组织实施方案	根据投标人提供的项目组织实施方案（包含且不限于项目前期实施期限及实施进度安排、保证实施进度的措施、确保项目供货和质量的措施等）进行评分，内容全面完整、科学合理的得 3 分。内容存在欠完整或欠合理的每项（次）扣 0.5 分，内容不完整或不合理的每项（次）扣 1 分，扣完为止。未提供或被评标委员会认定为无效的，此项不得分。	3
6	项目技术团队人员履历及能力说明	因本项目涉及多网络且对网络安全要求较高，因此要求投标人投入的项目总负责人具备有效的国家注册信息安全工程师（CISP）、信息系统项目管理师证书、智能化系统集成项目经理证书、网络工程师、PMP，具备三个及以上有效证书的得 2 分，不足三个的每少一个扣 1 分，扣完为止。 注：必须同时提供证书原件扫描件或复印件以及投标截止时间前近 6 个月内任意 1 个月的社保缴费证明，否则不得分。	2

		因本项目涉及网络安全和机房运维管理服务，拟投入项目组人员（除项目总负责人外）需具备： 1.根据拟投入项目技术负责人具备有效的高级工程师、信息安全工程师（或国家注册信息安全工程师）、信息系统项目管理师证书、网络工程师、互联网技术工程师、智能化系统工程师的情况进行评分。具备三个及以上有效证书的得 2 分；不足三个的，每少一个扣 1 分，扣完为止。 2.根据拟投入项目组成员人员具备有效的数据中心机房运维与管理工程师、弱电系统工程师、国家注册信息安全工程师（CISP）、系统集成项目管理工程师、信息系统项目管理师的情况进行评分。具备三个及以上有效证书的得 2 分；不足三个的，每少一个扣 1 分，扣完为止。 注：上述人员必须同时提供证书原件扫描件或复印件以及投标截止时间前近 6 个月内任意 1 个月的社保缴费证明，否则不得分。	4
7	项目培训方案	提供详细合理的项目培训方案（包括培训计划、方式、目标等），对投标人相关人员进行培训，确保人员能熟练掌握所提供设备和软件的操作技术、维护保养知识及常见故障排除方法等。根据投标人提供的方案由评标委员会判定评分，最高得 2 分。	2
8	驻场人员要求	根据业务需要，安排 2 名技术人员在服务期内提供驻场技术支撑服务。驻场人员中有一人需同时具备有效的网络工程师证书、信息安全工程师证书、网络安全工程师证书，另一人需具备有效的注册渗透测试工程师证书，驻场技术支撑人员的一切费用由中标供应商负责。 每提供一个符合要求的驻场人员得 2 分，最高得 4 分。 投标人必须同时提供驻场人员名单和相对应符合上述要求的证书原件扫描件或复印件，否则不得分。	4
9	拟投入的主要软硬件设备	符合招标文件明确指标参数的得 14 分。对标注“★”的指标参数属负偏离或缺漏项的每项扣 1 分，其他指标参数每项负偏离或缺漏扣 0.5 分，扣完为止。指标参数有实质性正偏离的，每项正偏离得 0.5 分，最高得 1 分。	15

10	讲解演示	网络安全运营中心演示 **（视频录制模拟演示，演示时间不超过 15 分钟）**	一、态势大屏 1.支持对接网络安全、数据安全、云安全、应用准入、边界安全等领域的安全管理中心，展示各中心部署引擎数和上报数据数，支持统计并展示选定任意日期和时间范围内的互联网暴露面，包括域名、IP、开放端口等，支持统计并展示安全运营现状，包括存在的高危漏洞、高危端口、高危违规、弱口令、防火墙阻断、安全处置等。 2.支持展示实时保障力量，包括团队规模、安全值守、机关单位、安全支撑单位、安全指挥长、总联络人。支持展示全链路安全监管对象，包括监管单位、监管系统、监管终端、安全设备、数据资产、用户档案等信息。 3.支持在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反应三层之间的关联关系，支持将攻击行为从网络空间映射到地图空间，再到单位拓扑。 上述 3 项功能全部能完整演示的得 3 分，其中每项功能能完整演示的得 1 分，每项功能只能部分演示的得 0.2 分，未提供或无法演示的该项功能得 0 分。	3
			二、实施监测、安全事件 1.支持网络和数据安全事件场景化验证，包括弱口令、挖矿、勒索病毒等场景，支持通过单位名称、IP 地址、时间等多字段组合查询场景内容。支持事件信息联想，通过事件数据关联同单位事件、同类型事件、同终端事件等联想方式。 2.支持通过“与“、“或”、“包含”等不低于 15 种语法分析研判，根据攻击类型和攻击信息进行数据聚合分析，支持不低于 13 种攻击类型分类，支持自定义攻击信息字段，支持详细展示攻击趋势、攻击链、攻击流向、实体信息等。 上述 2 项功能全部能完整演示的得 2 分，其中每项功能能完整演示的得 1 分，每项功能只能部分演示的得 0.2 分，未提供或无法演示的该项功能得 0 分。	2
			三、重保应急响应分级机制 1.支持对保障人员、保障单位、安保制度、安保组织、支撑单位、驻场小组等应急力量和物资的管理，支持重大活动保障前、中、后不同阶段里程碑节点管理，支持回放复盘历史保障过程。 2.支持通过应急作战台展示活动信息和近期重点工作，支持快速查看通报详情并处置，支持按不同等级的应急预案响应指令并联动移动端调度人员，支持驻场每日分班次上报平安情况。 上述 2 项功能全部能完整演示的得 2 分，其中每项功能能完整演示的得 1 分，每项功能只能部分演示的得 0.2 分，未提供或无法演示的该项功能得 0 分。	2

			四、重要部门应用安全画像 1.支持系统安全画像包括系统信息、系统拓扑、安全检测、防护情况、供应链、安全检查、等保信息、基础网络、人员信息、单位信息、档案时光轴等内容。 2.支持卡片式、缩略图方式展示系统信息，支持一键标记重要系统，一键查看系统事件隐患详情，快速下发系统扫描评估任务，支持系统域名到期提醒。 上述 2 项功能全部能完整演示的得 2 分，其中每项功能能完整演示的得 1 分，每项功能只能部分演示的得 0.2 分，未提供或无法演示的该项功能得 0 分。	2
			五、应用安全风险评估机制 1.支持现场检查、单位自查、远程检查三种方式开展安全风险评估工作，支持界面创建检测表单，上移下移调整检查项顺序，支持检查项类型包括填写、单选、多选、附件上传等。 2.支持设定考评范围的地区和行业、考评周期、考评起始时间、考评规则，支持将发生的安全事件、风险隐患级别和处置情况纳入考评并设定分值和权重。 上述 2 项功能全部能完整演示的得 2 分，其中每项功能能完整演示的得 1 分，每项功能只能部分演示的得 0.2 分，未提供或无法演示的该项功能得 0 分。	2
			六、安全隐患整改闭环服务 1.支持安全事件和风险隐患一键生成通报信息，通报详情支持显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。 2.通报支持进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒，针对已超时的通报进行超时显示，并显示具体超时时间。 上述 2 项功能全部能完整演示的得 2 分，其中每项功能能完整演示的得 1 分，每项功能只能部分演示的得 0.2 分，未提供或无法演示的该项功能得 0 分。	2
		信息安全驾驶舱演示 **（视频录制模拟演示，演示时间不超过 5 分钟）**	应急处突：展示紧急安全事件，基于驾驶舱，提供民警指派功能、事件状态调整功能、多部门协同通报功能等。 根据演示情况由评标委员会判定评分，最高得 2 分。	2
			信息预警：展示信息预警网络池，可随时调阅威胁和异常的详细信息，并通报网安大队民警进行处置。 根据演示情况由评标委员会判定评分，最高得 2 分。	2
			典型案例库：汇聚网络安全典型案例库，实际案例检索和调取。 根据演示情况由评标委员会判定评分，最高得 2 分。	2

三、价格分			
11	投标报价	报价得分采用低价优先法计算，即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，其报价得满分。其他投标人的投标报价得分按下列公式计算： 投标报价得分=(评标基准价／投标报价)×10%×100 。	10

第四章 招标需求

重要提示：

▲1.本项目仅允许非进口产品参与投标(注：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)。

一、招标项目一览表

本次招标共 1 个标项，具体内容如下表：

标项序号	标项名称	数量	单位	预算金额（万元）	最高限价（万元）	所属行业
1	仙居县公安局公共视频一体化及网络安全建设	1	项	2400	2340	软件和信息技术服务业

二、服务内容及要求

根据公安部相关文件和信息安全等级保护文件要求，结合仙居公安整体网络安全和公共视频一体化建设情况，对仙居公安的网络信息系统和视频接入进行统一整改。

1.对公共视频一体化升级扩容。搭建视频结构化平台，对动态人像识别系统授权以及存储设备进行扩容；

2.公安网、视频专网、取证网等 3 张网的网络安全等保建设。使得公安网和视频专网建设满足网络安全等级保护三级要求，且视频专网建设满足《台州市公共视频监控安全建设指南》的要求，取证网建设满足网络安全等级保护二级要求。实现大数据安全管理、0day 攻击预警、安全审计、违规外联处置等安全防护能力，建立一套安全、高效、可靠的安全运营中心体系；

3.网络边界建设，实现视频和数据安全交互能力，实现公安网、视频专网、网安网、取证网、政务网（互联网）等多张网络数据便捷传输交互；

4.建立实体网络安全运营中心，实现网络安全可视化、安全事件及时响应等；

5.等级保护测评服务；

6.设备搬迁及临时开通服务

由于台州市公安局仙居分局大楼目前电源系统及机房空间紧张，大楼电源系统及机

房空间无法满足后续视频专网新设备上线，计划将本项目涉及的天网安全设备及 8-10 期的存储服务器搬至供应商机房临时开通，等供应商新建的数据机房建成通过验收后，再将所有设备搬迁至供应商的数据机房，后续再将仙居分局天网机房的其他设备逐一搬迁至供应商的数据机房进行设备托管。

本次项目设备搬迁计划将仙居公安 15F 天网机房中视频存储服务器搬迁至中标供应商机房进行托管，本次搬迁设备为天网 8-10 期视频存储服务器 70 台，约 7 个综合架。

7. 设备托管服务

设备托管服务要求供应商新建机房并满足以下要求：

⑴机房地点在仙居县城区范围内，新建地点须获得采购人认可，并具备提供本项目相应标准机柜的服务能力。

⑵机房近期需满足：本次新建设备 150 台设备，约 12 个综合架；天网 8-10 期视频存储服务器约 70 套设备，约 7 个综合架；本项目需满足 19 个综合架。天网 4-6 扩容及搬迁设备 133 台，约 13 个综合架；约总计 32 个综合架的安装位置。

⑶新建数据中心机房至少需满足 32 个综合架的安装位置及后续扩容位置，机房面积至少保证 200 平米及以上，并配有相应的配线间、UPS 间、监控管理等；配线间至少保证两个不同光缆路由出局，新建数据机房要求在本次项目签订合同后 12 个月内完成验收。

⑷数据中心机房按 B 级标准、模块化一体化机房建设标准设计。包括机房装修、供配电系统（UPS 系统）、防雷接地系统、机房空调系统、机房环控、机房配线间等子系统。

⑸机房应远离无线电和强力电源干扰，避开地震区和其他震源，避开环境污染区、远离容易发生燃烧、爆炸、洪水地区和低洼地区。

⑹周边具有市政配套环境，网络通信资源丰富，提供各运营商线路接入支持。

⑺机房为独立建筑，与办公区域、库房区域、生活配套区域不在同一建筑内或具有有效分隔。

⑻数据中心机房应具有风险抵御能力，如地震、火灾、洪水、台风/暴风雨、鼠虫害、设备故障、操作风险等，确保基础设施的连续性。

⑼数据中心机房应具有安全性、可用性设计，包括建筑结构、系统冗余能力、物理安全考虑、人员设备控制、消防安全考虑、应急能力、防电磁辐射、防雷、防水、防静电等。

⑽建筑主体结构应具有耐久、抗震、防火、防止不均匀沉陷等性能，建筑结构安全等级为一级，抗震设防烈度不低于 8 度。

⑾数据中心机房在场地空间、电力容量、空调容量、通讯能力等方面都应有足够的余量，以满足采购人未来扩展需要。

总之，项目建成后完成公共视频一体化视频接入能力、人脸视频汇聚能力等，实现公安网和视频专网等级保护三级要求、取证网等级保护二级要求。使得仙居公安整体信息建设最终既可以满足信息安全等级保护和公共视频一体化相关要求，又能够全方面为仙居公安的业务系统提供立体、纵深的安全保障防御体系，保证信息系统整体的安全保护能力。

（一）需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

本项目执行的标准和规范包括但不局限于以下：

1.GB28181-2016 公共安全视频监控联网系统信息传输、交换、控制技术要求；

2.DB33/T 629.1-2011《跨区域视频监控联网共享技术规范》；

3.DB33/768-2009《安全技术防范系统建设技术规范》。

如有未特别注明需执行的国家相关标准、行业标准、地方标准或者其他标准、规范，则统一执行最新标准、规范。

（二）拟投入的主要软硬件设备情况

一级	二级	三级	指标参数	数量
公共视频一体化升级扩容	核心扩容	视频专网核心交换机	双主控，三交换网板，1*48 端口千兆以太网电接口模块，1*48 端口千兆以太网光接口模块，1*48 端口万兆以太网光接口模块，双电源，含 48 块千兆光模块，48 块万兆光模块。	2
		政务外网核心交换机	支持 48 个 10/100/1000BASE-T 端口,支持 4 个 10G/1G BASE-X SFP+端口,配置 8 端口万兆 SFP Plus 接口板，单电源，双风扇，含 12 块万兆光模块。	2
	扩容动态人脸识别系统授权	动态人像识别系统授权	解析能力：单套支持不低于 240 路动态人像图片流解析。 应用能力主要包括： 人脸结构化信息识别功能：人脸结构化信息提取，支持特征筛选。 系统支持对抓拍的路人图片进行属性识别。支持分析路人的年龄段，种族属性，性别，是否戴眼镜，是否维族人。 系统支持用机器学习的方法处理眼镜、长刘海、披肩发、胡须等装饰造成的特征缺失的补偿算法，提高不同环境下的通过率，误报率 1%时，通过率不低于 95%。 路人检索功能：支持上传查询照与路人库进行比对，分析出相似度高的路人数据。	3

			★人像识别算法（或产品）应具有快速的 1：N 算法速度，在 2,000 万人像库中以任意一张人像进行 1：N 比对，结果返回时间不超过 1 秒。 人像辅助识别查询：系统支持在网络端对过于模糊且无法识别的人像图片通过双目强制标注进行查询。 离线视频分析：对离线视频文件进行分析，截取出视频中出现的所有人脸照片，支持离线人脸数据的布控检索。 布控报警功能：支持三十万量级的人像库布控，支持根据时间查看的抓拍和报警信息，同时支持导出报警信息。 系统管理功能：支持人像库管理、离线视频管理、用户管理。 ★需与台州市公安局溯影人像平台无缝对接，投标时提供对接平台主管部门出具的无缝接入证明。	
	扩容存储设备	共享平台服务器	提供不低于以下配置 Xeon 4210 处理器/32G 内存/2*600G SAS 10K/RAID1/双口千兆网卡/冗余电源。	1
		视图库接口服务器	提供不低于以下配置 Xeon 4210 处理器及以上/32G 内存/2*600G SAS 10K/RAID1/双口千兆网卡/冗余电源。	1
		SSU 存储	采用 64 位多核处理器。内存≥4GB。标配 2 个千兆网卡。支持 24 块 SAS/SATA 硬盘，支持 SAS 和 SATA 磁盘混插，实现分层存储。支持 RAID 0，1，10，5，6。支持 CIFS、NFS、iSCSI。支持 RTSP、ONVIF、GB/T28181 等传输协议。采用冗余电源。冗余风扇。针对监控视频数据进行优化存储，优化磁盘使用模式，保障 I/O 为顺序读写。 数据安全：数据流块式组织，无碎片，无病毒。系统冗余：全局 N+（1~3）热备。 属性控制：SSU 可配置读写属性，包括“可读可写”和“只读”，保证全局数据安全。 统一网管：SSU 支持系统统一网管，系统的录像情况、运行状态一目了然。 录像完整率统计：精确记录每个摄像头的录像存储细节，多方位展示录像的统计信息。 包含了硬件级和固件级的电源故障数据保护功能，保证断电数据安全。带防断电模块。AC220V 电源。 ★无缝接入台州公安天网视频作战侦查平台，投标时提供对接平台主管部门出具的无缝接入证明。	3
		SSU 存储	采用 64 位多核处理器。内存≥4GB。标配 2 个千兆网卡。支持 24 块 SAS/SATA 硬盘，支持 SAS 和 SATA 磁盘混插，实现分层存储。支持 RAID 0，1，10，5，6。支持 CIFS、NFS、iSCSI。支持 RTSP、ONVIF、GB/T28181 等传输协议。采用冗余电源。冗余风扇。针对监控视频数据进行优化存储，优化磁盘使用模式，保障 I/O 为顺序读写。 数据安全：数据流块式组织，无碎片，无病毒。系统冗余：全局 N+（1~3）热备。 属性控制：SSU 可配置读写属性，包括“可读可写”和“只读”，保证全局数据安全。 统一网管：SSU 支持系统统一网管，系统的录像情况、运行状态一目了然。	10

			录像完整率统计：精确记录每个摄像头的录像存储细节，多方位展示录像的统计信息。 包含了硬件级和固件级的电源故障数据保护功能，保证断电数据安全。带防断电模块。AC220V 电源。 ★无缝接入台州公安天网视频作战侦查平台，投标时提供对接平台主管部门出具的无缝接入证明。	
	视频结构化平台	结构化智能服务器	硬件规格： 处理器：≥双颗 CPU（16 核，2.2GHz）。 GPU 卡：≥8 张高性能 GPU 卡。 内存：≥64GB DDR4 ，32 个内存插槽 。 硬盘：≥240G SSD ＊ 1。 数据接口：≥4 个千兆 RJ45 网口，≥1 个 RJ45 管理口，≥1 个 VGA 接口，≥4 个 USB 接口。 电源模块：1200W 1+1 高效冗余电源。 软件服务： 支持对视频进行目标分类（人、车、人和车分析处理）。 ★支持全分析功能，支持对视频或者图片进行人脸、人体、车辆的分析（提供公安部检测报告证明）。 支持根据需求进行硬件计算资源预分配，达到任务秒级处理。支持对突发的任务进行计算资源动态分配，算法资源动态管理。 ★支持通过界面展示查看每种算法已使用/预分配的总资源（提供公安部检测报告证明）。 如下性能为或的关系： 支持人脸分析：≥1280 张/S 或视频：≥256 路（1080P）。 支持车辆分析：≥3200 万张/天（200W~700W）。 支持视频结构化：≥256 路（1080P）。 支持治安场景图片分析性能（车辆、人体）：≥640 张/秒（200W）或≥256 张/秒（500W）或≥192 张/秒（800W）。 支持对视频和图片中车辆的类型进行识别。图片识别支持大型客车、大货车、轿车、皮卡、面包车、小货车、SUV/MPV、中型客车、二轮车/三轮车 9 种车型的识别。视频识别支持客车、大货车、轿车、面包车、小货车、SUV、中型客车 7 种车型的识别。光线正常，图片车辆类型识别正向准确率不低于 99%，背向准确率不低于 99%。 白天光照正常、夜间补光正常、车辆特征可辨识的情况下 1、车头方向：支持不少于 6000 种车辆子品牌及年款的识别 2、车尾方向：支持不少于 4400 种车辆子品牌及年款的识别。 30 万人脸库与 100 万底库进行人脸 N:N 比对，比对时间不超过 300 分钟。 人体属性：目标方向/大小/速度、上/下衣类型/颜色、年龄段、发型、性别、骑车、背包、戴眼镜、戴帽子、戴口罩、拎东西、骑车人数、骑车类型等。 支持实现对 1080P 视频流做实时结构化分析，并提供离线视频导入结构化分析能力。 支持目标追踪的结构化应用，基于视频结构化技术，对视频点位的录像或实时视频进行解析，通过对人脸及人体的实时布控，以视频接力的方式逐步还原出目标完整行动轨迹的应用。	5

			★支持与仙居县图像视频结构化处理多维立控指挥平台有效接入，投标时提供平台主管部门出具的接入测试证明文件，如涉及费用由投标人自理。 ★解析后的数据支持与台州市公安局视频 AI+平台进行对接，投标时提供与台州市公安局视频 AI+平台主管部门出具的测试对接证明文件，如涉及费用由投标人自理。	
		结构化数据库服务器	硬件规格： 处理器：≥双颗 CPU（16 核，2.2GHz）。 内存：≥256GB DDR4。 硬盘：≥240G M.2*1（系统）+240G SSD*1 + 480G SSD*6 + 2T 7.2K SATA *4(RAID10) + RAID 卡。 支持热插拔。 外部接口：≥2 个万兆光口，≥2 个千兆电口。≥4 个 USB 接口。 电源模块：高效能 800W 铂金 1+1 CRPS 冗余电源。 软件服务： 支持单台设备不少于 20 亿条数据存储。支持通过 SQL 等配置数据采集服务，消费数据入库，支持配置多个采集服务（提供公安部出具的检验报告）。 集成人脸、人体、车辆算法模型比对库，为下面的上层应用提供能力支撑： 支持分布式 SQL 查询，包括全文检索、精确查询、模糊查询。 支持第三方 Kerberos 身份认证，实现用户和服务的身份验证。支持用户密码的访问控制。支持数据权限控制。 支持多租户资源隔离功能，平台的资源包括计算资源和存储资源。 支持监控集群健康状态(组件状态、CPU 及内存使用率、网络流量、磁盘空间使用率、磁盘挂载情况、磁盘 IOPS 等）。支持查看集群中各节点运行状态，组件状态，集群告警信息等。 支持通过接口创建、删除、上传、下载文件等常规操作。 支持可视化的服务组件控制，包括服务添加、卸载、启动、停止、升级，支持服务升级失败后服务回滚。 支持存储功能组件：Hadoop(分布式文件系统 HDFS)、分布式协调 Zookeeper、NoSQL 数据库 Hbase、提供消息订阅 Kafka、全文检索 ElasticSearch、列示存储 Kudu、高性能 Key-value 数据库 Redis、时序数据库 STARTSDB、图数据库 Janusgraph、时空数据库 STRACK、日志收集 LOGGER、元信息管理 atlas。 ★支持与仙居县图像视频结构化处理多维立控指挥平台有效接入，形成结构化数据库，提供平台主管部门出具的接入测试证明文件，如涉及费用由投标人自理。 ★解析后的数据支持与台州市公安局视频 AI+平台进行对接，需要提供与台州市公安局视频 AI+平台主管部门出具的测试对接证明文件，如涉及费用由投标人自理。	3

		36 盘位云存储服务器	硬件规格： ≥两颗 64 位多核处理器。 ≥16GB 缓存。 ≥4 个千兆网口。 ≥1 个系统 SSD 盘。 ≥内置 1 颗 SSD 图片加速盘。 内置 36 块 6TB 企业级 SATA 硬盘。 软件服务： 支持聚合下载，即并发从多台存储节点中下载某一个时间段录像、图片、智能结构化数据、文件。 支持按毫秒级自定义时间段进行视频精准检索、回放、下载，回放支持豪秒级定位回放、关键帧回放、回放暂停、倍速快放、慢放等。 支持采用 RESTful 协议直存图片到云存储系统中。支持图片写入后 1s 内回显及下载。 支持前端设备和存储设备之间直接存储，采用块级存储，不生成文件（即不使用文件系统），无碎片。 支持按照设备可用容量实现负载均衡，各存储节点上存储的数据量在稳定状态下保持均衡，差距小于 5%。 云存储支持双控设备双 active 的工作方式，存储任务和压力平均分摊到两个控制器上面。 云存储系统采用模块化结构设计，业务系统可根据需要对配额进行调整，而不需要管理新增空间。 支持按照设备可用容量实现负载均衡，各存储节点上存储的数据量在稳定状态下保持均衡，差距小于 5%。 数据分散存储到存储节点上，数据呈离散式分布。 存储运维精细化：支持在运维监测功能页面显示存储硬盘的健康状态，便于存储硬盘的生命周期管理。 ★支持前端设备和存储设备之间直接存储，采用块级存储，不生成文件（即不使用文件系统），无碎片。（提供公安部出具的检验报告） 系统支持分域管理，当单个域中设备接入到同一个交换机时，可实现数据流分域控制管理，域内业务不受其他域影响。 ★支持与仙居县图像视频结构化处理多维立控指挥平台有效兼容，形成云存储集群管理，提供平台主管部门出具的接入测试证明文件，如涉及费用由投标人自理。	2
		云存储管理扩容	在图像视频结构化处理多维立控指挥平台的云存储管理系统上进行扩容，复用之前的云存储基础管理模块。系统可扩容，增加管理或存储节点。在多节点系统中，任何一个存储节点出现故障，应不影响数据的正常存取。 一套云存储系统可对外提供多种类型数据混合存储，同时支持分布式流式存储，分布式对象存储、分布式文件存储、分布式块存储。 支持利用软加密、加密卡、加密机方式对用户数据进行加密存储，兼容 AES、SM4 加密算法，兼容标准 KMS 系统对接。 支持存储设备维护模式状态下，读取业务（历史数据）不受影响可读取，新业务接管保证业务不中断。 支持云存储和虚拟化平台融合部署一套系统，支持通过唯一 IP 访问系统，支持各部分单独扩容，支持同时	1

			存储视频、图片、对象、文件融合存储，并支持存储、转发、分析、检索及应用等一体化服务。 支持磁盘故障、设备故障后，根据业务情况，调整设置重构的等级，分别调整为高速重构、中速重构、低速重构。支持重构速度展示。 ★支持与仙居县图像视频结构化处理多维立控指挥平台有效对接，对云存储系统扩容管控，提供平台主管部门出具的接入测试证明文件，如涉及费用由投标人自理。	
		通用服务器	CPU：≥1 颗 x86 架构 HYGON 处理器，核数≥24 核，频率≥2.2GHz。 内存:≥64G DDR4，16 根内存插槽，最大支持扩展至 2TB 内存。 硬盘：≥2 块 600G 10K 2.5 寸 SAS 硬盘。 阵列卡：SAS_HBA 卡，支持 RAID 0/1/10。 PCIE 扩展：最大可支持 6 个 PCIe 扩展插槽。 网口：≥2 个千兆电口。	2
		智能服务管理模块扩容	★支持切换查看基础目录及业务目录，资源以资源树形式展示，点击可查看下层资源及点位。（提供公安部检测报告） 支持根据用户业务需求，在基础目录树上创建更有业务针对性的业务目录区域，支持自定义新建及修改业务目录的名称、关联资源类型及关联目录标识，并支持针对业务目录进行修改、编辑、排序等管理。 支持录像分段回放功能，可以将录像文件等分成多个片段同时回放，通过分割点的图像差异，快速确定回放关键录像时段。 支持针对系统点位进行算法调度配置及视频结构化处理，包括人脸识别、人体识别、车辆识别及活动目标识别。 ★支持针对离线视频进行算法调度配置及视频结构化处理，包括人脸识别、人体识别、车辆识别及活动目标识别。（提供公安部检测报告） 支持勾选暂存架内文件，生成多类型目标混合的单条轨迹，并在地图上展示。 支持人脸名单布控、单张人脸图片布控、驾乘布控。 支持车辆名单布控、车牌布控、车辆模型布控。支持在 1 个预警中心的地图上实时展示人脸、车辆、的报警信息，并支持报警的进一步研判。 支持数据级联共享，支持将本级或下级域中的卡口、人脸、人体抓拍数据推送至上级域实现级联共享。 支持人脸、人体、车辆等结构化数据、特征值、图片的实时级联与跨网摆渡。 支持在查询结果中支持展示目标对象的关联信息，包括同步采集信息及与目标对象具有关联关系的对象信息 支持点位进行扩容到支持 15000 路视频接入或者级联能力。 ★支持与仙居县图像视频结构化处理多维立控指挥平台有效接入，提供平台主管部门出具的接入测试证明文件，如涉及费用由投标人自理。	1

		视讯指挥云终端设备	性能要求：云终端采用云终端采用低功耗 ARM 架构，提供≥四个物理算力单元、内存≥1 个物理内存单元、存储≥4G、USB≥6 个、1 个 VGA 或 HDMI，云终端与视讯指挥云平台计算中心同一品牌。要求每台云终端配备一个接入授权。 功能要求： 支持分组管理、批量移动、删除、关闭终端，支持配置定时开关机计划及加电自启动功能，支持自定义开机画面、配置自动登录和保存密码。 支持远程唤醒，管理员可以使用控制器或者第三方教学软件，远程开机瘦终端。 支持鼠标、键盘、打印机等常用外设，用户可以直接使用终端网络上的网络打印机正常完成打印。	40
		视讯指挥云平台计算中心	提供≥32 个物理算力单元。物理算力主频≥2.8GHz，≥512 个内存单元，盘位≥12*3.5 SATA/SAS 盘位，系统盘不低于 2 块 240G SSD 硬盘,缓存盘不低于 2 块 960G SSD 硬盘，数据盘不少于 10 块 4T 的 SATA 硬盘 ，接口配置≥6 个 GE 接口，≥2 个万兆光口，配置冗余双电源。平台出厂时必须预装各类视讯指挥云软件（含服务器虚拟化、存储虚拟化等），不允许提供裸机设备。 功能要求： 支持集群冗余技术，当硬盘故障时，HA 机制就会自动触发虚机迁移动作，实现毫秒级切换，对用户来讲基本是无感知的。主机或者网络故障，虚拟桌面可以快速切换到另一台服务器拉起，约 3-5 分钟。以保障用户稳定的使用。 单集群管理时无需部署集中管理平台，通过 Web 方式接入集群主服务器，实现对服务器、虚拟机、网络、存储虚拟化等进行统一管理。 支持个人盘加密技术，对个人数据进行加密保存，保障个人隐私安全。 内置防火墙，包括设置过滤规则、NAT 设置、访问监控、防 DOS 攻击。 可持续性检测并发现虚拟机、主机、集群相关的软硬件问题，检测出的问题按照严重程度做分级，并支持结合内置智能诊断库，进行自动化问题诊断，可直接在平台上以图文形式直接展示问题分析说明、问题举证分析、问题处置建议，管理员根据处置建议操作即可。 支持管控 PC 剪切板权限，通过策略组新增选项配置可以控制仅能拷贝文本内容，防止数据外泄。 支持虚拟机集中备份与恢复，可按需选择多个虚拟机或全部虚拟机备份至外置服务器（NAS、FTP、CIFS 等），支持设置备份策略，实现全自动化备份。 支持在管理组件中内置应用管控技术，实现全方位管控，在禁止名单中可以通过配置规则禁止指定应用或进程运行。在允许名单中通过配置规则只允许规则中的应用或进程运行。	2

		视讯云文件资源平台	用户机构管理。 系统参数设置。 文件集中存储，分类管理。 文件模板管理模式，根据需要自定义模板格式,文件材料按模板格式存放。 文件集由用户自行建立。 文件集权限由建立人管理，对不同文件集进行单独的权限设置，包括有浏览、创建、删除、编辑、预览、下载、打印等权限内容，根据应用情况，文件集所有者可以随时管理维护权限体系，赋予或收回权限。 文件上传下载，文件格式包括但不限于WORD,WPS,EXECL，PDF,图片文件，音视屏文件等。 个人中心：近期文件集、我的文件集、权限内的文件集。 文件集标签管理，根据文件集权限内用户自定义文件集标签，标签只针对个人。 文件资源搜索，可对文件集进行包含文件集名称、创建人、类型、标签、创建/修改时间进行条件搜索或组合查询并排序。 全文搜索引擎，为文件建立索引，能够根据索引搜索文本信息，对文件进行全文检索。 文件集文件列表。 在线文件预览，支持音频视频及文档各种格式文件WORD，EXCEL，PPT，JPG，MP4，PDF，PNG 等直接在线浏览和打印，无需下载。	1
网络安全等保建设	公安网	态势感知平台	支持单节点大数据一体机部署，服务器配置要求：CPU 2 路或更高 ，内存≥256GB，配置企业级存储磁盘总容量≥48TB。 支持横向平滑扩展，可以通过增加硬件服务器数量的方式增加平台集群的计算处理性能。 支持虚拟化部署：最低要求 6 节点，每个节点 CPU≥4 核，内存≥64G，硬盘≥4T。 单节点数据采集和处理性能≥20000EPS。 支持≥1000 个用户同时在线并发查询。 10 亿数据关键字查询结果响应时间<2 秒。 数据权限管理通过设置数据判断条件将数据划分到各归属单位、归属地区，数据判断条件支持与、或、非、In、Not In、exist、包含等方式灵活组合。 支持按资产重要程度、资产区域和组织架构将资产分级分类管理。 平台支持不低于 40 种单位行业属性标签，不低于 20 种单位类型属性标签，并支持多属性标签联合检索。 支持系统画像快速浏览，信息至少包括系统信息、安全检测、防护情况、供应链、检查督查、等保信息、基础网络、人员信息、单位信息、档案时光轴等字段。 通知举证信息支持一键溯源，包括溯源到资产档案、系统档案、情报信息、原始日志等。 ★需与台州市公安局关键信息基础设施态势感知平台无缝对接。出具平台主管部门出具的无缝接入证明及平台对接可行性方案，并提供台州市公安局关键信息基础设施态势感知平台接口文档。	1

		运维审计	软硬件一体化产品，2U、硬盘 1T*2、硬盘须配置 RAID1、至少配备 6 个 100/1000M 自适应电口、4 个 1000M 光口（含 2 个 SFP 多模模块），1+1 冗余电源。 可管理设备数量≥500 个，运维用户无限制。 单台堡垒机字符类并发会话≥500、图形类并发会话≥100 。 ★IE/Chrom 代填应用发布：HTTP/HTTPS 协议的 web 设备，且可以直接代填账号和密码），支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。（提供检测报告证明） 支持对数据库及 Web 应用的自动改密功能。 支持手机 APP 动态口令认证方式登录堡垒机，新用户首次登录后需强制绑定 APP 动态口令。支持 AD、LDAP、RADIUS、吉大正元、北京 CA 认证系统联动登录堡垒机，支持自动同步 AD/LDAP 用户。	1
		日志审计	工作管理口（6 个千兆电口，4 个千兆光口（配 2 个多模 SFP 光纤模块）），1 个 Console 口。 内存：16GB，磁盘：2T*2 raid1（支持 raid1、raid5）。双电源。 板载 CF 卡槽位，也可支持 CF 卡启动。 支持审计 200 个日志源。 平均处理能力（每秒日志解析能力 EPS）：9000 EPS。 峰值处理能力（每秒日志解析能力 EPS）：12000 EPS。 三维关联分析：支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。 通过在目标主机上安装 Agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。 ★资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。（提供检测报告证明） 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户。 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据。	1

		数据库审计	提供不低于以下配置：内存≥16GB DDR3 1600Mhz，硬盘≥4TB（2T*2），支持 RAID1，最大支持扩展到 4T*4 硬盘。 网络端口： 支持监听接口扩展，配备至少 2 个千兆电口管理口。 支持千兆网络环境下的监听能力，标配至少 4 个千兆电口和 4 个千兆光口。 支持的数据库实例个数：无上限。 审计性能：峰值 SQL 处理能力≥20000 条/秒。 硬件最大吞吐量 2000Mbps，最大纯数据库流量 200Mbps，标配日志存储数 20 亿条。 审计日志检索能力≥1500 万条/秒。 ★可在云环境操作系统中安装软件代理。 ★审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集。产品具有内置规则，规则类型有 sql 注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警。（提供检测报告证明） 支持内置安全规则单独升级。 ★可依据客户端工具名、数据库用户名、客户端 IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器 IP 等配置行为模型，并可查看相应告警日志。（提供检测报告证明） 支持在审计管理端批量安装、卸载、重新安装审计代理。 可监控 Agent 的转发速率，以及 Agent 所在数据库服务器的 CPU、内存利用率，并可设置 CPU、内存利用率的上线阈值，超阈值时 Agent 将自动停止转发数据。 可提供客户端访问 Web 服务器的 URL 和应用服务器访问数据库的 SQL 语句关联功能。	1
		高级威胁检测平台	软硬一体化 2U 标准机架式设备。 电源：双电源。 CPU：10 核 20 线程*2。 硬盘容量：2T*2，带 RAID1，可用磁盘空间不小于 2T。 内存：64G。 接口数量：管理口：Consle*1,USB*2,千兆 RJ45 网口*2。 业务口：千兆 RJ45 网口*4，千兆 SFP 光口*4（标配千兆多模光模块*2）。 接口扩展：（千兆 RJ45 网口*4 + 千兆 SFP 光口*4）或 千兆 RJ45 网口*8 或 千兆 SFP 光口*8 或 万兆 SFP 光口*2 或 万兆 SFP 光口*4。 扩展槽个数：3 个。 MTBF：大于 65000 小时。 支持将分析到的恶意文件攻击行为同步到 EDR，实现 APT 深度威胁分析与 EDR 联动查杀。 支持自定义与 EDR 联动的等待扫描时长，并将联动状态、样本执行结果、样本路径、EDR 病毒木马扫描结果等同步到 APT 设备。 支持 WEBSHELL 检测，可检测访问 webshell 的行为，包含具体对应的 URL、返回码、返回数据包内容等，可显示一句话类 webshell 后门是否植入成功。	1

			可添加或删除指定分离的文件类型，并可选择适用的协议类型（HTTP 可进一步按 GET、POST 来配置）。 支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现。 KAFKA 服务器配置支持 SASL 认证和 Kerberos 认证。 KAFKA 数据传输支持明文或 SSL 加密。	
		主机安全卫士	EDR 管理中心： 包含终端管理中心软件一套。实现对终端的统一管理和策略下发。CentOS 6.5 及以上系统。8G 及以上内存，四核及以上 CPU，200G 以上硬盘。 EDR 终端（含 100 套服务器安装授权）： 适用于各类型服务器防护。支持 Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、 Ubuntu 14 +等操作系统。 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。 支持基于 IP 及域名设置探测地址，实时感知违规外联行为，针对违规外联行为支持多种处置方式，包括不做处理、弹窗提醒用户，并关机、弹窗提醒用户并断网。 支持登录防护，包括以系统账号为粒度的异常登录防护、支持 4 个任意维度（任意 IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。 持对文件 HASH、IP、域名、邮箱等 IOC 指标进行动静态鉴定，通过和云端威胁情报进行碰撞，实时返回威胁结果。 联动威胁情报，支持对外联 IP、DNS 解析、可疑文件进行实时情报鉴定，实现风险一站式实时监测。 支持多引擎设置，包括默认引擎、深度扫描引擎。 针对 Windows 系统，提供内核级的数据防护能力，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程。	1
		漏洞扫描	软硬件一体化产品，标准 1U 硬件平台，硬盘 2T，内存 16G，配备至少 6 个 100/1000M 自适应电口，支持一个 4 光扩展，2*USB 口，单电源。提供 3 年硬件维保服务及特征库升级。 授权可扫描总数量不少于 500 个 IP 地址。 任务并发数≥10，单任务并发 IP 数≥90。 厂商漏洞特征库大于 200000 条。漏洞知识库与 CVE、CNNVD、Bugtraq、CNCVE、CNVD 等国际、国内漏洞库标准兼容。 具备弱口令扫描功能，支持弱口令扫描协议数量≥22 种，包括 FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP 等协议进行弱口令扫描，允许用户自定义用户、密码字典。 支持多种网站认证方式：支持包括 Basic、Digest、DigestIE、NTLM、GSS-Negotiate、Bearer 在内的认证方式，支持 HTTP 和 SOCKS 代理，并支持各种代理的认	1

			证方式。 支持 Oracle、Mysql、SQLServer、DB2、informix、PostgreSQL、Sybase、达梦、人大金仓的授权数据库漏洞扫描。 支持授权管理，对已知用户名、密码的资产可预先进行配置存放至授权管理，再下发扫描任务时能对该部分资产的授权信息同步。 提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。	
		运维管理调度中心	硬件要求：规格：2U，CPU≥10 核 2.4GHz，内存≥512GB DDR4 2933，系统盘≥2*240GB SATA SSD，数据盘≥4T，电源：冗余电源，接口≥2 个千兆电口+2 个万兆光口。 资产管理：提供资产分组功能，用户可建立自定义分组，设定分组包含的资产，并按照分组对资产进行导航。提供拖拽式拓扑绘制的功能，支持对绘制的节点进行分组，支持分组展开与折叠。提供 IP 基准功能，建立基准表，绑定 IP 与 MAC 的映射关系，发现未授权的设备接入。提供资产的硬件配置变动监测功能，并列表呈现所有的变动记录。 实现对物理服务器的工况信息进行监控，可支持以下监控项：电压、风扇转速、电源状态、硬盘状态、机箱温度等，服务流关联对应的服务工程师，工程师需具有主流服务器存储厂商认证，且人员为平台厂商的原厂工程师。 实现对 vmware 虚拟机的监控,可支持以下指标的监控：CPU 利用率、内存利用率、存储器信息、网口信息等，服务流关联对应的服务工程师，工程师需具有 VCP 认证或 OCP 认证，且人员为平台厂商的原厂工程师。 实现对网络设备的监控，可支持以下监控项：总流速、收包率、接收丢包率、接收错误率、发送利用率、发送丢包率、路由信息等，服务流关联对应的服务工程师，工程师需具有 HCIE 或 CCIE 或 H3CIE 级别以上认证，且人员为平台厂商的原厂工程师。 实现对安全设备的监控，涵盖防火墙、堡垒机、IDS、IPS、WAF 等，可支持以下监控项：接收流速、接收利用率、发包率、发送流速、发送错误率、CPU、内存利用率等，服务流关联对应的服务工程师，工程师需具有主流网络安全厂商的高级认证和 CISP 认证，且人员为平台厂商的原厂工程师。 实现对存储设备/系统的监控，涵盖 IPFCSAN、分布式 NAS 等存储服务器，可支持阵列、RAID 组和 LUN 级别的监控，可支持以下监控项：总速率、读速率、写速率、存储利用率、读写占比率等，服务流关联对应的服务工程师，工程师需具有主流服务器存储厂商认证，且人员为平台厂商的原厂工程师。 实现对 JVM 堆内存、活动线程、HTTP 线程、守护线程、启动线程的监控。 实现对操作系统，如 Windows、Linux、Unix 等系统的性能、容量、进程、连接、接口等进行监控，服务流关联对应的服务工程师，工程师需具有 RHCE 和 MCSE 级别以上的认证，且人员为平台厂商的原厂工程师。	1

			支持三权分立，系统管理员、审计管理员、安全管理员权限独立，避免一个用户权限最大没有制约给系统造成危害，由 ITIL 工程师负责运维流程设计、监督和执行，工程师需具有 ITIL foundation 认证证书，且人员为平台厂商的原厂工程师。	
		数据灾备	2U12 盘位机型，配置≥2 路八核心处理器，配置≥64GB 内存。配置≥1 片 200G SSD 系统盘，配置≥1 片 960G SSD 加速硬盘，配置 ≥8 片 4TB SATA 硬盘。冗余热插拔交流电源模块*2。 配置不少于 24TB 容量的实时备份可用容量授权许可。含本机性能允许下的无限节点容灾接管授权。	1
		WEB 应用防火墙	标准 X86 多核并行架构，2U 设备高度，至少配置 6 个千兆电口，4 个千兆光口，冗余电源，2 个扩展槽位，应用层吞吐≥2G，网络层吞吐≥10G，并发连接≥200 万。 支持透明（无 ip）模式串联部署和负载均衡模式部署旁路监听模式部署、代理模式部署。 支持 trunk 的多 VLAN 环境下部署。支持虚拟线从任一网络环境实现同设备不同端口间的数据转发。 Web 应用防火墙需全面支持 ipv6 环境，具有在 IPv6 网络中针对活跃 ip 进行检测能力，支持服务器健康检查，可以实时监测服务器的活跃状态，并且可定期备份健康记录。 支持 HTTP/HTTPS 站点防护，在代理模式下支持 HTTPS 加密流量解析，并兼容国家信息安全漏洞库（CNNVD），支持 SSL 卸载功能。 支持对请用户数据做合规性检查，包括请求头长度（需支持自定义）、最大 body 长度、最大 content-length、最大请求行、最大 header 行、最多 cookies、最多 header 头、最大 heade。 支持防护对 webshell 等后门上传攻击、支持防护对中国菜刀等工具对后门连接的阻断。 支持加密流量特征识别自学习功能，可以通过学习正常 URL 参数的长度、参数类型、请求方法等数据特点创建白名单模型，如果参数违反白名单模型则认为是非法流量直接阻断，开启自学习建模功能后可生成自学习网站参数的自学习结果报告。 支持应用层虚拟补丁功能，支持第三方的扫描器扫描结果进行 WEB 防护的规则的生成，并可对同类网站漏洞直接进行防护。 支持对多种应用层 WEB 漏洞进行扫描检测，如 SQL 注入攻击、脚本跨站、目录等。 无需在服务器中安装任何插件，即可对网站文件内容进行篡改防护，当检测到篡改后可以实时恢复篡改内容。也可通过将缓存的网站页面返回给客户端，从而保证客户端无法看到被非法篡改的页面，来做到网页篡改防护。	1

		蜜罐系统	软硬件一体机。 机箱高度：2U。 内存：64G。 电源：1+1 冗余电源。 硬盘：1*2T（加配硬盘后支持 RAID 1）。 网口：10 个（2*千兆电+4*千兆电+4*千兆光（光模块*2），出厂标配）。 网口可扩展槽：3 个（定制可选：4*千兆电+4*千兆光、8*千兆电、8*千兆光、2*万兆光、4*万兆光。）。 硬盘可扩展槽：1 个（2TB SATA 7.2k）。 支持 SDN 技术模拟蜜网，可自定义添加交换机、VLAN，规划蜜网结构。 支持 Web 类蜜罐，提供不低于 13 种蜜罐，包括但不限于 Jenkins、WordPress、Zabbix、OA、Nginx、Discuz 论坛、DokuWiki、渗透、邮箱、Webmin、Struts2、SugarCRM、Joomla 等。 支持数据库类蜜罐，提供不低于 8 种蜜罐，包括但不限于 MySQL、Oracle、PostgreSQL 、MongoDB、Redis、MemCached、Hive、HBase 等。 支持漏洞事件蜜罐，提供不低于 2 种蜜罐，包括但不限于 SonarQube 漏洞蜜罐、Log4j2 漏洞蜜罐等，并根据安全热点事件持续推出。 支持基于攻击事件聚合攻击行为，捕获某一攻击者对某一蜜罐/蜜饵产生的所有攻击，并按照时间轴形式详细展示攻击内容。 ★支持与外部 APT 等流量监测设备联动，对可疑样本进行沙箱深度分析，导出 HTML 格式的沙箱分析报告；对攻击蜜罐的流量进行深度分析。 支持与云端情报中心联动，对可疑样本进行云端情报匹配分析，导出 HTML 格式的云端情报分析报告。对攻击源 IP 进行云端情报分析，获得详细的云端 IP 情报。 支持与外部 APT 等流量监测设备联动，对可疑样本进行沙箱深度分析，导出 HTML 格式的沙箱分析报告。对攻击蜜罐的流量进行深度分析。 支持提供至少 3 种方式告警，包括但不限于：短信、邮件、钉钉等。	1
		网络资产与边界感知系统	采用标准机架式的 2U 硬件设备，全内置封闭式结构，专用安全加固 Linux 操作系统，冗余双电源。 12 个千兆电口，2 个万兆光口，4 个 USB 接口。 QPS（TPS）≥2000 个（IP 数量）。 并发处理数≥100 万（数据包）。 最大镜像流量≥4Gbps。 无需在主机上安装客户端软件，通过实时全量采集网络设备镜像口流量，以设备基准模型分析、主动扫描和基于数据的安全监管等技术为核心，实现对内外网互联、非授权外联、NAT 边界、移动设备接入等各类违规行为的自动发现与地址定位。能对 linux、unix 操作系统版本的服务器进行内外网互联、非授权外联等违规行为发现等。	1

		违规外联处置平台	硬件参数：2U 机架式设备，内存≥512G，硬盘≥24T，冗余电源，配置 1 个管理口，≥2 个千兆电口+2 个千兆光口。 设备准入：自动发现管理域内的设备接入行为，自动上报接入设备的 IP/MAC 地址、操作系统、厂商信息等信息至处置审计平台，根据需要实现设备自动准入（如视频网监控摄像头设备）或经管理员审计通过后接入内网。 出口 ip 地址池限制：检测网内所有终端的出口 ip 地址，需匹配 ip 地址池白名单列表，对非白名单 ip 的终端进行违规外联告警并断网处置。 日志审计：对终端接入内网的行为进行记录展示。记录内容包括：登录用户、IP 地址、登录地点、登录时间、登录系统、浏览器、操作（对记录删除）。它的功能有：根据登录用户或登录时间进行记录查询与对记录删除、导出。 行为监控：包括敏感词管理（查询、增加、编辑功能）、行为分析（根据敏感词提取的信息进行统计、查询、分析、展示）、文档查看（对于键盘输入文档提取的数据统计、查询等操作管理）、行为轨迹（对于鼠标点击截图进行提取的数据统计、查询等操作管理）、监控管理(对于异常的 IP 进行统计、查询等操作管理)。 违规外联：监测范围内终端的两网互通（同时连接内网和互联网）的行为，一旦发现，定位其终端地址（内网 IP 和互联网 IP）并及时阻断。监测任何手机接入计算机终端 USB 口的行为，对该计算机终端进行违规外联告警并断网下线。	1
		汇聚交换机（安全运维区）	支持 24 个 10/100/1000BASE-T 端口(8 个 SFP Combo)，支持 4 个 10G/1G BASE-X SFP+端口,配置 8 端口万兆 SFP Plus 接口板，单电源，双风扇，含 12 块万兆光模块。	2
		汇聚交换机(外联单位)	支持 24 个 10/100/1000BASE-T 电口,2 个 GE Combo 电口,2 个 100/1000BASE-X SFP Combo 光口,2 个 1000BASE-X SFP 光口,支持 AC，含 4 块千兆光模块。	1
		防火墙(外联单位、服务器区)	标准 X86 多核并行架构,1U 标准机架,双交流冗余电源,至少配置接口：8 个 GE 电口，2 个 SFP 光口，2 个 SFP+万兆光口,2 个扩展槽位,防火墙网络吞吐量≥10Gbps。并发连接数≥400 万，每秒新建 HTTP 连接数≥20 万。含三年 IPS 和防病毒模块。 支持路由、虚拟线、Listening、交换混合工作模式。支持静态路由、动态路由和 ISP 路由协议,支持 802.1Q、QinQ 模式。 支持手动添加绑定和 IP、接口的动态探测绑定，可实现跨三层 IP/MAC 绑定，绑定表可导入导出。 针对公安网大规模多路由接入环境，设备需支持芯片数据包缓存管理，实现多核平台下的多系统并行运行及数据共享，支持在一台物理设备上划分出 128 个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源。 支持基于 IP/IP 组、应用/应用组、服务/服务组、用户/用户组配置带宽策略，支持带宽策略优先级，可配	2

			置包含多级 5 层带宽策略，对流量进行细分管理，保证带宽的利用率。 可以通过 TCP 连接粘合实现应用代理加速。通过该技术可可实现 HTTP、FTP、POP3、SMTP、IM 等协议的病毒快速查杀，支持木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的精准查杀，可实现压缩文件解码查杀。 支持对基于最大并发连接数的单条访问控制策略进行限制。	
	视频网	态势感知平台	CPU ≥24 核 ，内存≥256GB，配置企业级存储磁盘总容量≥48TB（或磁盘可用容量≥40TB）。 接口要求：千兆电口*4（可选万兆双口 RJ45、千兆四口 RJ45、万兆双口光纤等多种网络接口）。 最低要求 6 节点，每个节点 CPU≥12 核，内存≥64G，硬盘≥4T。 数据采集和处理性能≥15000EPS，每条数据大小>1KB。10 亿数据关键字查询结果响应时间<2 秒。 应内置包括规则模型、关联模型、统计模型、情报模型、AI 模型等不少于 5 类安全分析模型。 平台内置不少于 4 种机器学习分析场景模型，可检测发现流量异常、网络会话数异常、网址访问失败异常、域名请求数异常等特定场景条件下的安全态势异常。 支持与云端威胁情报库实现在线对接，可跳转到云端和第三方威胁情报库交叉验证。支持通过离线导入方式，形成本地威胁情报，用户可自建行业情报库，并实现对情报库的增加、修改、查询、导入、导出等功能。情报记录包含情报置信度、类型、标签、运营商等信息，并支持统计情报源命中情报数量，针对单条无效情报可实现删除。 ★具有分析指标管理和构建功能，支持用户根据实际业务场景从安全日志中选取特定字段作为分析指标，可采用计数、求和、均值、最大值、最小值等策略统计相关特定字段数值，且分析指标可作为分析模型的创建条件。（提供检测报告证明） ★具有基于 IP 地址段为系统内资产划分安全域，可对每个安全域内的告警数和资产数进行实时统计，并支持安全域之间的横向互访关系在大屏中进行展示的功能。	1
		运维审计	提供不低于以下配置：软硬件一体化产品，2U、硬盘 1T*2、硬盘须配置 RAID1、至少配备 6 个 100/1000M 自适应电口、4 个 1000M 光口（含 2 个 SFP 多模模块），1+1 冗余电源。 可管理设备数量≥500 个，运维用户无限制。 单台堡垒机字符类并发会话≥500、图形类并发会话≥100 ★IE/Chrom 代填应用发布：HTTP/HTTPS 协议的 web 设备，且可以直接代填账号和密码。（提供检测报告证明） ★支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。 支持对数据库及 Web 应用的自动改密功能。	1

			支持手机 APP 动态口令认证方式登录堡垒机，新用户首次登录后需强制绑定 APP 动态口令。支持 AD、LDAP、RADIUS、吉大正元、北京 CA 认证系统联动登录堡垒机，支持自动同步 AD/LDAP 用户。	
		日志审计	10 个工作管理口（6 个千兆电口，4 个千兆光口（配 2 个多模 SFP 光纤模块）），1 个 Console 口。 内存：16GB，磁盘：2T*2 raid1（支持 raid1、raid5）。双电源。 板载 CF 卡槽位，也可支持 CF 卡启动。 支持审计 200 个日志源。 平均处理能力（每秒日志解析能力 EPS）：9000 EPS。 峰值处理能力（每秒日志解析能力 EPS）：12000 EPS。 三维关联分析。 ★支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。（提供检测报告证明） ★通过在目标主机上安装 Agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。（提供检测报告证明） 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户。 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据。	1
		数据库审计	提供不低于以下配置：内存≥16GB DDR3 1600Mhz，硬盘≥4TB（2T*2），支持 RAID1，最大支持扩展到 4T*4 硬盘。 网络端口： 支持监听接口扩展，配备至少 2 个千兆电口管理口。 支持千兆网络环境下的监听能力，标配至少 4 个千兆电口和 4 个千兆光口。 支持的数据库实例个数：无上限。 审计性能：峰值 SQL 处理能力≥20000 条/秒。 硬件最大吞吐量 2000Mbps，最大纯数据库流量 200Mbps，标配日志存储数 20 亿条。 审计日志检索能力≥1500 万条/秒。 可在云环境操作系统中安装软件代理。 ★审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集。（提供检测报告证明） 产品具有内置规则，规则类型有 sql 注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警。 支持内置安全规则单独升级。 可依据客户端工具名、数据库用户名、客户端 IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器 IP 等配置行为模型，并可查看相应告警日志。 支持在审计管理端批量安装、卸载、重新安装审计代理。 ★可监控 Agent 的转发速率，以及 Agent 所在数据库	1

			服务器的 CPU、内存利用率，并可设置 CPU、内存利用率的上线阈值，超阈值时 Agent 将自动停止转发数据。 可提供客户端访问 Web 服务器的 URL 和应用服务器访问数据库的 SQL 语句关联功能。	
		高级威胁检测平台	硬件外形：软硬一体化 2U 标准机架式设备。 电源：双电源。 CPU：10 核 20 线程*2。 硬盘容量：2T*2，带 RAID1，可用磁盘空间不小于 2T。 内存：64G。 接口数量：管理口：Consle*1,USB*2,千兆 RJ45 网口*2。 业务口：千兆 RJ45 网口*4，千兆 SFP 光口*4（标配千兆多模光模块*2）。 MTBF：大于 65000 小时。 支持将分析到的恶意文件攻击行为同步到 EDR，实现 APT 深度威胁分析与 EDR 联动查杀。 ★支持自定义与 EDR 联动的等待扫描时长，并将联动状态、样本执行结果、样本路径、EDR 病毒木马扫描结果等同步到 APT 设备。 支持 WEBSHELL 检测，可检测访问 webshell 的行为，包含具体对应的 URL、返回码、返回数据包内容等，可显示一句话类 webshell 后门是否植入成功。 可添加或删除指定分离的文件类型，并可选择适用的协议类型（HTTP 可进一步按 GET、POST 来配置）。 支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现。 KAFKA 服务器配置支持 SASL 认证和 Kerberos 认证。 KAFKA 数据传输支持明文或 SSL 加密。	1
		主机安全卫士	EDR 管理中心： 包含终端管理中心软件一套。实现对终端的统一管理和策略下发。CentOS 6.5 及以上系统。8G 及以上内存，四核及以上 CPU，200G 以上硬盘。 EDR 终端（含 140 套服务器安装授权）： 适用于各类型服务器防护。支持 Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、 Ubuntu 14 +等操作系统。 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。 支持基于 IP 及域名设置探测地址，实时感知违规外联行为，针对违规外联行为支持多种处置方式，包括不做处理、弹窗提醒用户，并关机、弹窗提醒用户并断网。 ★支持登录防护，包括以系统账号为粒度的异常登录防护、支持 4 个任意维度（任意 IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。 持对文件 HASH、IP、域名、邮箱等 IOC 指标进行动静态鉴定，通过和云端威胁情报进行碰撞，实时返回威胁结果。 联动威胁情报，支持对外联 IP、DNS 解析、可疑文件进行实时情报鉴定，实现风险一站式实时监测。	1

			支持多引擎设置，包括默认引擎、深度扫描引擎。 针对 Windows 系统，提供内核级的数据防护能力，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程。	
		漏洞扫描	软硬件一体化产品，标准 1U 硬件平台，硬盘 2T，内存 16G，配备至少 6 个 100/1000M 自适应电口，支持一个 4 光扩展，2*USB 口，单电源。提供 3 年硬件维保服务及特征库升级。 授权可扫描总数量不少于 500 个 IP 地址。 任务并发数≥10，单任务并发 IP 数≥90。 ★厂商漏洞特征库大于 200000 条。 提供详细的漏洞描述和对应的解决方案描述。漏洞知识库与 CVE、CNNVD、Bugtraq、CNCVE、CNVD 等国际、国内漏洞库标准兼容。 具备弱口令扫描功能，支持弱口令扫描协议数量≥22 种，包括 FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP 等协议进行弱口令扫描，允许用户自定义用户、密码字典。 支持多种网站认证方式：支持包括 Basic、Digest、DigestIE、NTLM、GSS-Negotiate、Bearer 在内的认证方式，支持 HTTP 和 SOCKS 代理，并支持各种代理的认证方式。 支持 Oracle、Mysql、SQLServer、DB2、informix、PostgreSQL、Sybase、达梦、人大金仓的授权数据库漏洞扫描。 支持授权管理，对已知用户名、密码的资产可预先进行配置存放至授权管理，再下发扫描任务时能对该部分资产的授权信息同步。 提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。	1

		运维管理调度中心	硬件要求：规格：2U，CPU≥10 核 2.4GHz，内存≥512GB DDR4 2933，系统盘≥2*240GB SATA SSD，数据盘≥4T，电源：冗余电源，接口≥2 个千兆电口+2 个万兆光口。 资产管理：提供资产分组功能，用户可建立自定义分组，设定分组包含的资产，并按照分组对资产进行导航。提供拖拽式拓扑绘制的功能，支持对绘制的节点进行分组，支持分组展开与折叠。提供 IP 基准功能，建立基准表，绑定 IP 与 MAC 的映射关系，发现未授权的设备接入。提供资产的硬件配置变动监测功能，并列表呈现所有的变动记录。 实现对物理服务器的工况信息进行监控，可支持以下监控项：电压、风扇转速、电源状态、硬盘状态、机箱温度等，服务流关联对应的服务工程师，工程师需具有主流服务器存储厂商认证，且人员为平台厂商的原厂工程师。 实现对 vmware 虚拟机的监控,可支持以下指标的监控：CPU 利用率、内存利用率、存储器信息、网口信息等，服务流关联对应的服务工程师，工程师需具有 VCP 认证或 OCP 认证，且人员为平台厂商的原厂工程师。 实现对网络设备的监控，可支持以下监控项：总流速、收包率、接收丢包率、接收错误率、发送利用率、发送丢包率、路由信息等，服务流关联对应的服务工程师，工程师需具有 HCIE 或 CCIE 或 H3CIE 级别以上认证，且人员为平台厂商的原厂工程师。 实现对安全设备的监控，涵盖防火墙、堡垒机、IDS、IPS、WAF 等，可支持以下监控项：接收流速、接收利用率、发包率、发送流速、发送错误率、CPU、内存利用率等，服务流关联对应的服务工程师，工程师需具有主流网络安全厂商的高级认证和 CISP 认证，且人员为平台厂商的原厂工程师。 实现对存储设备/系统的监控，涵盖 IPFCSAN、分布式 NAS 等存储服务器，可支持阵列、RAID 组和 LUN 级别的监控，可支持以下监控项：总速率、读速率、写速率、存储利用率、读写占比率等，服务流关联对应的服务工程师，工程师需具有主流服务器存储厂商认证，且人员为平台厂商的原厂工程师。 实现对 JVM 堆内存、活动线程、HTTP 线程、守护线程、启动线程的监控。 实现对操作系统，如 Windows、Linux、Unix 等系统的性能、容量、进程、连接、接口等进行监控，服务流关联对应的服务工程师，工程师需具有 RHCE 和 MCSE 级别以上的认证，且人员为平台厂商的原厂工程师。 支持三权分立，系统管理员、审计管理员、安全管理员权限独立，避免一个用户权限最大没有制约给系统造成危害，由 ITIL 工程师负责运维流程设计、监督和执行，工程师需具有 ITIL foundation 认证证书，且人员为平台厂商的原厂工程师。	1
		数据灾备	2U12 盘位机型，配置≥2 路八核心处理器，配置≥64GB 内存。配置≥1 片 200G SSD 系统盘,配置≥1 片 960G SSD 加速硬盘，配置 ≥8 片 4TB SATA 硬盘。冗余热插拔交流电源模块*2。 配置不少于 24TB 容量的实时备份	1

			可用容量授权许可。含本机性能允许下的无限节点容灾接管授权。	
		WEB 应用防火墙	标准 X86 多核并行架构，2U 设备高度,至少配置 6 个千兆电口，4 个千兆光口,冗余电源,2 个扩展槽位,应用层吞吐≥2G，网络层吞吐≥10G,并发连接≥200 万。 支持透明（无 ip）模式串联部署和负载均衡模式部署旁路监听模式部署、代理模式部署。 支持 trunk 的多 VLAN 环境下部署。支持虚拟线从任一网络环境实现同设备不同端口间的数据转发。 Web 应用防火墙需全面支持 ipv6 环境，具有在 IPv6 网络中针对活跃 ip 进行检测能力,支持服务器健康检查，可以实时监测服务器的活跃状态，并且可定期备份健康记录。 支持 HTTP/HTTPS 站点防护，在代理模式下支持 HTTPS 加密流量解析，并兼容国家信息安全漏洞库（CNNVD），支持 SSL 卸载功能。 支持对请用户数据做合规性检查，包括请求头长度（需支持自定义）、最大 body 长度、最大 content-length、最大请求行、最大 header 行、最多 cookies、最多 header 头、最大 header。 支持防护对 webshell 等后门上传攻击、支持防护对中国菜刀等工具对后门连接的阻断。 支持加密流量特征识别自学习功能，可以通过学习正常 URL 参数的长度、参数类型、请求方法等数据特点创建白名单模型，如果参数违反白名单模型则认为是非法流量直接阻断，开启自学习建模功能后可生成自学习网站参数的自学习结果报告。 支持应用层虚拟补丁功能，支持第三方的扫描器扫描结果进行 WEB 防护的规则的生成，并可对同类网站漏洞直接进行防护。 支持对多种应用层 WEB 漏洞进行扫描检测，如 SQL 注入攻击、脚本跨站、目录等。 无需在服务器中安装任何插件，即可对网站文件内容进行篡改防护，当检测到篡改后可以实时恢复篡改内容。也可通过将缓存的网站页面返回给客户端，从而保证客户端无法看到被非法篡改的页面，来做到网页篡改防护。	1
		视频监控网络安全管控中心	高度：2U。电源：1+1 冗余。CPU：6 核 6 线程。内存 64GB。硬盘：2*4TB。 端口：2 个千兆电口。处理能力支持接入：10,000 资产。 针对资产进行安全画像，以百分制的方式进行资产安全评分，展示近 7 天的安全状况，并展示资产的安全状态、基本信息、网络进程关系图、进程关关系、开放端口、以及隐患和告警趋势等。 支持隐患概览页面展示，包括漏洞数量、弱口令数量、漏洞等级分布、漏洞类型、漏洞资产品牌、弱口令资产品牌以及隐患趋势图展示等。 ★平台支持对视频监测引擎的一键管控。	1

		视频监测引擎	规格：2U 导轨式设备。内存：不低于 96GB。硬盘：不低于 24TB。电源：1+1 冗余电源。 网口数量：4*千兆电口+2*千兆光口,4 个USB2.0接口，2 个 USB3.0 接口,1 个 CONSOLE 口。 可进行自定义监测频率设置，并对全网设备进行安全检测。 漏洞扫描须实现与仙居县公安局视频网视频监控网络安全管控中心对接，出具平台厂家无缝接入证明及平台对接可行性方案。 ★行为取证——对行为进行取证并留存包括访问、站点访问、文件传输等行为信息。 ★恶意扫描——监测网络中频繁或大规模的访问其它主机设备、服务端口的行为，提供发起扫描的设备地址、被扫描最多主机、被扫描最多端口等详细信息。（提供检测报告证明） ★脆弱性——对使用弱口令、设备端口的安全风险隐患进行监测和发现。用户可以自定义扫描目标、类型、扫描时间策略。系统会根据设备类型进行漏洞扫描。（提供检测报告证明）	5
		违规外联处置平台	硬件参数：2U 机架式设备，内存≥512G，硬盘≥24T，冗余电源，配置 1 个管理口，≥2 个千兆电口+2 个千兆光口。 设备准入：自动发现管理域内的设备接入行为，自动上报接入设备的 IP/MAC 地址、操作系统、厂商信息等信息至处置审计平台，根据需要实现设备自动准入（如视频网监控摄像头设备）或经管理员审计通过后接入内网。 出口 ip 地址池限制：检测网内所有终端的出口 ip 地址，需匹配 ip 地址池白名单列表，对非白名单 ip 的终端进行违规外联告警并断网处置。 日志审计：对终端接入内网的行为进行记录展示。记录内容包括：登录用户、IP 地址、登录地点、登录时间、登录系统、浏览器、操作（对记录删除）。它的功能有：根据登录用户或登录时间进行记录查询与对记录删除、导出。 行为监控：包括敏感词管理（查询、增加、编辑功能）、行为分析（根据敏感词提取的信息进行统计、查询、分析、展示）、文档查看（对于键盘输入文档提取的数据统计、查询等操作管理）、行为轨迹（对于鼠标点击截图进行提取的数据统计、查询等操作管理）、监控管理(对于异常的 IP 进行统计、查询等操作管理)。 违规外联：监测范围内终端的两网互通（同时连接内网和互联网）的行为，一旦发现，定位其终端地址（内网 IP 和互联网 IP）并及时阻断。监测任何手机接入计算机终端 USB 口的行为，对该计算机终端进行违规外联告警并断网下线。	1
		汇聚交换机（安全运维区、交警接入）	支持 24 个 10/100/1000BASE-T 端口(8 个 SFP Combo)，支持 4 个 10G/1G BASE-X SFP+端口,配置 8 端口万兆 SFP Plus 接口板，单电源，双风扇，含 14 块万兆光模块。	4

		汇聚交换机（机房服务器）	48 个 10G BASE-X SFP Plus 端口,2 个 QSFP Plus 端口,2 个 Slot，含 48 块万兆光模块。	2
		防火墙(机房服务器、交警服务器、天网乡镇、天网城区)	标准 X86 多核并行架构,1U 标准机架,双交流冗余电源,至少配置接口：8 个 GE 电口，2 个 SFP 光口，2 个 SFP+万兆光口,2 个扩展槽位,防火墙网络吞吐量≥10Gbps。并发连接数≥400 万，每秒新建 HTTP 连接数≥20 万。含三年 IPS 和防病毒模块。 能够基于时间、端口、域名组、用户/用户组/安全组、应用层 IP 地址、URL 分类、实现视频流的安全策略配置。 支持策略的快速（模糊）查询，策略组，策略规则标签，便于策略的管理及运维。 视频网多链路接入环境防火墙需支持过滤规则匹配技术，支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略。 支持链路实时动态监控功能，当发现异常可自动切换到可用链路，确保网络正常的通信。 视频网多链路接入环境下支持检测防火墙冲突规则技术，提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在 WEB 界面显示检测结果：红色为冗余策略，绿色为冲突策略。 具有网络流量阈值检测技术,支持 UDP DDOS 防护功能,支持基于报文大小限制、阀值检查、源/目的限流方式综合进行 UDP 报文、UDP FLOOD、UDP FRAG FLOOD 防护。支持基于 IP、用户的最大连接数限制，防护服务器。支持 SIP、H.323 等多种监控媒体协议,设备满足《安全防范视频监控联网系统信息传输、交换、控制技术要求（GB/T 28181-2016）》规范技术要求。	3
	取证网	运维审计	提供不低于以下配置：软硬件一体化产品，2U、硬盘 1T*2、硬盘须配置 RAID1、至少配备 6 个 100/1000M 自适应电口、4 个 1000M 光口（含 2 个 SFP 多模模块），1+1 冗余电源。 可管理设备数量≥500 个，运维用户无限制。 单台堡垒机字符类并发会话≥500、图形类并发会话≥100 。 ★IE/Chrom 代填应用发布：HTTP/HTTPS 协议的 web 设备，且可以直接代填账号和密码。（提供检测报告证明） 支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。 ★支持对数据库及 Web 应用的自动改密功能。 支持手机 APP 动态口令认证方式登录堡垒机，新用户首次登录后需强制绑定 APP 动态口令。支持 AD、LDAP、RADIUS、吉大正元、北京 CA 认证系统联动登录堡垒机，支持自动同步 AD/LDAP 用户。	1

		日志审计	10 个工作管理口（6 个千兆电口，4 个千兆光口（配 2 个多模 SFP 光纤模块）），1 个 Console 口。 内存：16GB，磁盘：2T*2 raid1（支持 raid1、raid5）。双电源。 板载 CF 卡槽位，也可支持 CF 卡启动。 支持审计 200 个日志源。 平均处理能力（每秒日志解析能力 EPS）：9000 EPS。 峰值处理能力（每秒日志解析能力 EPS）：12000 EPS。 ★三维关联分析，支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。 ★通过在目标主机上安装 Agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。（提供检测报告证明） 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户。 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据。	1
		数据库审计	提供不低于以下配置：内存≥16GB DDR3 1600Mhz，硬盘≥4TB（2T*2），支持 RAID1，最大支持扩展到 4T*4 硬盘。 网络端口： 支持监听接口扩展，配备至少 2 个千兆电口管理口。 支持千兆网络环境下的监听能力，标配至少 4 个千兆电口和 4 个千兆光口。 支持的数据库实例个数：无上限。 审计性能：峰值 SQL 处理能力≥20000 条/秒。 硬件最大吞吐量 2000Mbps，最大纯数据库流量 200Mbps，标配日志存储数 20 亿条。 审计日志检索能力≥1500 万条/秒。 ★可在云环境操作系统中安装软件代理。（提供检测报告证明） ★审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集。 产品具有内置规则，规则类型有 sql 注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警。 支持内置安全规则单独升级。 可依据客户端工具名、数据库用户名、客户端 IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器 IP 等配置行为模型，并可查看相应告警日志。 支持在审计管理端批量安装、卸载、重新安装审计代理。 ★可监控 Agent 的转发速率，以及 Agent 所在数据库服务器的 CPU、内存利用率，并可设置 CPU、内存利用率的上线阈值，超阈值时 Agent 将自动停止转发数据。（提供检测报告证明） 可提供客户端访问 Web 服务器的 URL 和应用服务器访问数据库的 SQL 语句关联功能。	1

		主机安全卫士	EDR 管理中心： 包含终端管理中心软件一套。实现对终端的统一管理和策略下发。CentOS 6.5 及以上系统。8G 及以上内存，四核及以上 CPU，200G 以上硬盘 EDR 终端（含 100 套服务器安装授权）： 适用于各类型服务器防护。支持 Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、 Ubuntu 14 +等操作系统 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。 ★支持基于 IP 及域名设置探测地址，实时感知违规外联行为，针对违规外联行为支持多种处置方式，包括不做处理、弹窗提醒用户，并关机、弹窗提醒用户并断网。 支持登录防护，包括以系统账号为粒度的异常登录防护、支持 4 个任意维度（任意 IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。 持对文件 HASH、IP、域名、邮箱等 IOC 指标进行动静态鉴定，通过和云端威胁情报进行碰撞，实时返回威胁结果。 联动威胁情报，支持对外联 IP、DNS 解析、可疑文件进行实时情报鉴定，实现风险一站式实时监测。 支持多引擎设置，包括默认引擎、深度扫描引擎。 针对 Windows 系统，提供内核级的数据防护能力，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程。	1
		违规外联处置平台(政务网办公区)	硬件参数：2U 机架式设备，内存≥512G，硬盘≥24T，冗余电源，配置 1 个管理口，≥2 个千兆电口+2 个千兆光口。 设备准入：自动发现管理域内的设备接入行为，自动上报接入设备的 IP/MAC 地址、操作系统、厂商信息等信息至处置审计平台，根据需要实现设备自动准入（如视频网监控摄像头设备）或经管理员审计通过后接入内网。 出口 ip 地址池限制：检测网内所有终端的出口 ip 地址，需匹配 ip 地址池白名单列表，对非白名单 ip 的终端进行违规外联告警并断网处置。 日志审计：对终端接入内网的行为进行记录展示。记录内容包括：登录用户、IP 地址、登录地点、登录时间、登录系统、浏览器、操作（对记录删除）。它的功能有：根据登录用户或登录时间进行记录查询与对记录删除、导出。 行为监控：包括敏感词管理（查询、增加、编辑功能）、行为分析（根据敏感词提取的信息进行统计、查询、分析、展示）、文档查看（对于键盘输入文档提取的数据统计、查询等操作管理）、行为轨迹（对于鼠标点击截图进行提取的数据统计、查询等操作管理）、监控管理(对于异常的 IP 进行统计、查询等操作管理)。 ★违规外联：监测范围内终端的两网互通（同时连接内网和互联网）的行为，一旦发现，定位其终端地址	1

			（内网 IP 和互联网 IP）并及时阻断。监测任何手机接入计算机终端 USB 口的行为，对该计算机终端进行违规外联告警并断网下线。	
	互联网	高级威胁检测平台	硬件外形：软硬一体化 2U 标准机架式设备。 电源：双电源。 CPU：10 核 20 线程*2。 硬盘容量：2T*2，带 RAID1，可用磁盘空间不小于 2T。 内存：64G。 接口数量：管理口：Consle*1,USB*2,千兆 RJ45 网口*2。 业务口：千兆 RJ45 网口*4，千兆 SFP 光口*4（标配千兆多模光模块*2）。 MTBF：大于 65000 小时。 ★支持 WEBSHELL 检测，可检测访问 webshell 的行为，包含具体对应的 URL、返回码、返回数据包内容等，可显示一句话类 webshell 后门是否植入成功。 可添加或删除指定分离的文件类型，并可选择适用的协议类型（HTTP 可进一步按 GET、POST 来配置）。 支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现。 KAFKA 服务器配置支持 SASL 认证和 Kerberos 认证。 KAFKA 数据传输支持明文或 SSL 加密。	1
		上网行为管理	提供不低于以下配置：网络层吞吐量≥5 Gbps，应用层吞吐量≥1.2 Gbps，IPSec VPN 性能≥800 Mbps，最大并发连接数≥250 万，每秒新建连接数≥3 万，IPSec VPN 隧道数≥1024，SSL VPN 接入数≥400。 标准 1U 机柜型硬件平台，内置交流单电源，硬盘容量≥1TB HDD。 10*GE 电口，4*Combo 口。支持千兆接口总数≥14 个机架式独立硬件设备，系统硬件为全内置封闭式结构，多核架构设计 MIPS 架构，功能采用模块化结构设计。 接口支持配置从属 IP 地址,每个接口要求支持至少 200 个从属 IP。 支持 4G USB 插卡接入，实现 4G 连接与有线链路之间互为备份。并支持在 4G 接口上运行 IPSec VPN。 ★支持基于入接口、源地址、目标地址、用户、服务、应用、时间、域名的策略路由。（提供检测报告证明） 支持 DNS 透明代理，支持指定 DNS 或继承链路 DNS 配置，针对多链路支持基于优先级、权重、流量算法进行 DNS 负载。 ★支持针对搜索引擎、HTTP、网页内容进行关键字过滤并实时生成日志记录，日志级别包括但不少于紧急、告警、严重、通知、信息、调试、不记录等，方便管理员快速区分用户上网行为属性和定位日志级别。 支持文件缓存，缓存文件形式不限于视频、APP 等。设备智能解析用户流量，针对域名或者文件请求，设备推送文件至终端，帮助用户缓解互联网出口压力，实现文件下载加速的效果。	1

		违规外联处置平台	硬件参数：2U 机架式设备，内存≥512G，硬盘≥24T，冗余电源，配置 1 个管理口，≥2 个千兆电口+2 个千兆光口。 设备准入：自动发现管理域内的设备接入行为，自动上报接入设备的 IP/MAC 地址、操作系统、厂商信息等信息至处置审计平台，根据需要实现设备自动准入（如视频网监控摄像头设备）或经管理员审计通过后接入内网。 出口 ip 地址池限制：检测网内所有终端的出口 ip 地址，需匹配 ip 地址池白名单列表，对非白名单 ip 的终端进行违规外联告警并断网处置。 日志审计：对终端接入内网的行为进行记录展示。记录内容包括：登录用户、IP 地址、登录地点、登录时间、登录系统、浏览器、操作（对记录删除）。它的功能有：根据登录用户或登录时间进行记录查询与对记录删除、导出。 行为监控：包括敏感词管理（查询、增加、编辑功能）、行为分析（根据敏感词提取的信息进行统计、查询、分析、展示）、文档查看（对于键盘输入文档提取的数据统计、查询等操作管理）、行为轨迹（对于鼠标点击截图进行提取的数据统计、查询等操作管理）、监控管理(对于异常的 IP 进行统计、查询等操作管理)。 ★违规外联：监测范围内终端的两网互通（同时连接内网和互联网）的行为，一旦发现，定位其终端地址（内网 IP 和互联网 IP）并及时阻断。监测任何手机接入计算机终端 USB 口的行为，对该计算机终端进行违规外联告警并断网下线。	1
网络边界建设	取证网-县视频专网	防火墙	标准 X86 多核并行架构，2U 硬件平台,至少配置 8 个千兆电口，2 个千兆光口,4 个 SFP+万兆接口，冗余电源，1 个扩展插槽,防火墙吞吐≥22G，并发连接≥800 万，每秒新建连接≥50 万，含三年 IPS 和防病毒模块。 能够基于时间、用户/用户组/安全组、应用层协议 IP 地址、端口、域名组、URL 分类、实现视频流的安全策略配置。 支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维。 支持防火墙过滤规则匹配技术，支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议。 支持实时链路监控，发现异常可启动功能自动切换到可用链路，确保网络的正常通信。 支持检测防火墙冲突规则技术，提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在 WEB 界面显示检测结果：红色为冗余策略，绿色为冲突策略。 具有网络流量阈值检测技术，支持 UDP DDOS 防护，采用报文大小限制、阀值检查、源/目的限流方式综合进行 UDP 报文、UDP FLOOD、UDP FRAG FLOOD 防护。 支持每 IP， 每用户的最大连接数限制，防护服务器。 支持用户流量配额管理。 支持 SIP、H.323 等多种监控媒体协议,设备满足《安	2

			全防范视频监控联网系统信息传输、交换、控制技术要求（GB/T 28181-2016）》规范技术要求支持 SIP、H.323 等多种监控媒体协议,设备满足《安全防范视频监控联网系统信息传输、交换、控制技术要求（GB/T 28181-2016）》规范技术要求。	
		数据安全交换系统(三件套)	标准 2U 机架式，由信任端服务器及非信任端服务器、安全隔离与信息交换系统组成。 信任端服务器及非信任端服务器服务器各具备 100/1000Mbase-TX 以太接口不少于 2 个，万兆光纤接口不少于 2 个，安全隔离与信息交换系统具备 100/1000Mbase-TX 以太接口不少于 2 个，万兆光纤接口不少于 2 个。 为满足客户业务需求，数据数据交换系统应用层吞吐不低于 8Gbps，单数据表映射最大字段数不低于 1024，单数据库交换业务并发表不低于 4096。（提供检测报告证明） 可对业务系统进行智能检测分析，并输出数据源检测结果、数据积压检测结果、服务器自身异常检测情况，对业务运行情况实时智能检测，便于运维人员快速定位业务系统故障及性能指标。 系统支持 kafka 同步，认证方式包含：PLANTEXT、SASL_PLANTEXT、KERBEROS。 数据交换系统支持接入业务多个优先级配置，保证实时性高的业务能优先传输，多个业务同时运行，各业务之间能够独立的启停，单个业务的故障不会影响到其它业务的数据交换。 能够在 IPV4 协议和 IPV6 协议环境下，支持 Mysql 等数据库间数据源交换，支持单向、双向数据交换，支持增量与全量两种交换方式。能够在 IPV4 协议和 IPV6 协议环境下，支持两个不同网络区域 ftp 文件传输。	1
	县视频专网-市视频专网	防火墙	标准 X86 多核并行架构,2U 硬件平台,至少配置 8 个千兆电口，2 个千兆光口,4 个 SFP+万兆接口，冗余电源，1 个扩展插槽,防火墙吞吐≥22G，并发连接≥800 万，每秒新建连接≥50 万，含三年 IPS 和防病毒模块。 能够基于时间、端口、域名组、用户/用户组/安全组、应用层 IP 地址、URL 分类、实现视频流的安全策略配置。 支持策略的快速（模糊）查询，策略组，策略规则标签，便于策略的管理及运维。 视频网多链路接入环境防火墙需支持过滤规则匹配技术，支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议。 支持链路实时动态监控功能，当发现异常可自动切换到可用链路，确保网络正常的通信。 视频网多链路接入环境下支持检测防火墙冲突规则技术，提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在 WEB 界面显示检测结果：红色为冗余策略，绿色为冲突策略。 具有网络流量阈值检测技术，支持 UDP DDOS 防护功能，支持基于报文大小限制、阀值检查、源/目的限流方式	2

			综合进行 UDP 报文、UDP FLOOD、UDP FRAG FLOOD 防护。 支持基于 IP、用户的最大连接数限制，防护服务器。 支持 SIP、H.323 等多种监控媒体协议,设备满足《安全防范视频监控联网系统信息传输、交换、控制技术要求（GB/T 28181-2016）》规范技术要求。	
	取证网-政务云	防火墙	标准 X86 多核并行架构,1U 标准机架,双交流冗余电源,至少配置接口：8 个 GE 电口，2 个 SFP 光口，2 个 SFP+万兆光口,2 个扩展槽位,防火墙网络吞吐量≥10Gbps。并发连接数≥400 万，每秒新建 HTTP 连接数≥20 万。含三年 IPS 和防病毒模块。 能够基于时间、用户/用户组/安全组、应用层协议 IP 地址、端口、域名组、URL 分类、实现视频流的安全策略配置。 支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维。 接口的 MAC 地址应答，实现保护内网主机。 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议。 政务云连接防火墙需全面支持 ipv6 环境，具有在 IPv6 网络中针对活跃 ip 进行检测能力。 支持服务器负载均衡，保证关键服务的有效性。 策略路由支持的匹配条件：源 IP/目的 IP、用户(组)，入接口。 支持实时链路监控，发现异常可启动功能自动切换到可用链路，确保网络的正常通信。 支持防火墙环境下动态负载均衡的网络地址转换，同时具有独立 DNSDoctoring 功能，可将来自内网的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡。	2
		数据交换服务系统（四件套）	标准 2U 机型，由数据交换前置机、数据交换后置机、单向导入光闸、单向导出光闸组成，标配冗余电源。 数据交换服务器各具备 100/1000Mbase-TX 以太接口不少于 3 个，万兆光纤接口不少于 3 个，单向导入光闸、单向导出光闸各具备 100/1000Mbase-TX 以太接口不少于 4 个，万兆光纤接口不少于 4 个。 交换能力≥3.5Gbps。文件性能≥1800Mbps，数据库触发性能≥16000 条/s。 支持 Kafka 协议消息队列数据交换，支持 PlainTEXT、SASL/PlainTEXT、Kerberos 等多种安全认证方式。 支持负载功能，多设备负载配置，系统中任意设备故障或宕机不影响任务的正常运行，具备极高的系统可用性。且可以通过负载模式提高边界交换的性能。 系统显示集群设备情况，包含设备总署、正常设备数、异常设备数、启用设备数、停用设备数，同时显示各节点设备 IP 地址、CPU、内存、磁盘使用率。	1

	视频专网-公安网	防火墙	标准 X86 多核并行架构，2U 硬件平台,至少配置 6 个千兆电口,4 个千兆光口,4 个 SFP+万兆接口，冗余电源,1 个扩展槽位,防火墙吞吐≥45G，并发连接≥800 万，每秒新建连接≥80 万，含三年 IPS 和防病毒模块，需同时满足视频网及公安网防护需求。 支持路由、虚拟线、Listening、交换混合工作模式。 支持静态路由、动态路由和 ISP 路由协议,支持 802.1Q、QinQ 模式。 支持手动添加绑定和 IP、接口的动态探测绑定，可实现跨三层 IP/MAC 绑定，绑定表可导入导出。 针对公安网大规模多路由接入环境，设备需支持芯片数据包缓存管理，实现多核平台下的多系统并行运行及数据共享，支持在一台物理设备上划分出 128 个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源。 支持基于 IP/IP 组、应用/应用组、服务/服务组、用户/用户组配置带宽策略，支持带宽策略优先级，可配置包含多级 5 层带宽策略，对流量进行细分管理，保证带宽的利用率。 可以通过 TCP 连接粘合实现应用代理加速，通过该技术可可实现 HTTP、FTP、POP3、SMTP、IM 等协议的病毒快速查杀，支持木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的精准查杀，可实现压缩文件解码查杀。 支持对基于最大并发连接数的单条访问控制策略进行限制。 能够基于时间、用户/用户组/安全组、应用层协议 IP 地址、端口、域名组、URL 分类、实现视频流的安全策略配置。 支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维。 视频网多链路接入环境防火墙需支持过滤规则匹配技术，支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议。 支持实时链路监控，发现异常可启动功能自动切换到可用链路，确保网络的正常通信。 视频网多链路接入环境下支持检测防火墙冲突规则技术，提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在 WEB 界面显示检测结果：红色为冗余策略，绿色为冲突策略。 具有网络流量阈值检测技术，支持 UDP DDOS 防护，采用报文大小限制、阀值检查、源/目的限流方式综合进行 UDP 报文、UDP FLOOD、UDP FRAG FLOOD 防护。 支持每 IP， 每用户的最大连接数限制，防护服务器。 支持用户流量配额管理。 支持 SIP、H.323 等多种监控媒体协议,设备满足《安全防范视频监控联网系统信息传输、交换、控制技术要求（GB/T 28181-2016）》规范技术要求。	2

		视频安全交换系统（三件套）	标准 2U 机架式，由信任端服务器及非信任端服务器、安全隔离与信息交换系统组成。 信任端服务器及非信任端服务器服务器各具备 100/1000Mbase-TX 以太接口不少于 2 个，万兆光纤接口不少于 2 个，安全隔离与信息交换系统具备 100/1000Mbase-TX 以太接口不少于 2 个，万兆光纤接口不少于 2 个。 ★为满足客户业务需求，视频交换系统吞吐量不低于 9.8Gbps，并发连接数不低于 400000 个。（提供检测报告证明） 为满足市场各品牌对接需求以及便于配置人员对接业务，产品支持配置不同视频厂商产品适配的模板文件，快速生成视频传输通道。（提供检测报告证明） 根据网络 IP 升级需要，视频交换系统能够在 IPV4 和 IPV6 协议环境下，对视频流使用用户、源端 IP 地址、目的端 IP 地址、访问时间进行控制。可对视频流进行丢帧、插帧处理。可对信令协议做 register、play 等关键字过滤，控制操作类型。	1
		数据安全交换系统（三件套）	标准 2U 机架式，由信任端服务器及非信任端服务器、安全隔离与信息交换系统组成。 ★信任端服务器及非信任端服务器服务器各具备 100/1000Mbase-TX 以太接口不少于 2 个，万兆光纤接口不少于 2 个，安全隔离与信息交换系统具备 100/1000Mbase-TX 以太接口不少于 2 个，万兆光纤接口不少于 2 个。 ★为满足客户业务需求，数据数据交换系统应用层吞吐不低于 8Gbps，单数据表映射最大字段数不低于 1024，单数据库交换业务并发表不低于 4096。（提供检测报告证明） 可对业务系统进行智能检测分析，并输出数据源检测结果、数据积压检测结果、服务器自身异常检测情况，对业务运行情况实时智能检测，便于运维人员快速定位业务系统故障及性能指标。 系统支持 kafka 同步，认证方式包含：PLANTEXT、SASL_PLANTEXT、KERBEROS。 数据交换系统支持接入业务多个优先级配置，保证实时性高的业务能优先传输，多个业务同时运行，各业务之间能够独立的启停，单个业务的故障不会影响到其它业务的数据交换。 ★能够在 IPV4 协议和 IPV6 协议环境下，支持 Mysql 等数据库间数据源交换，支持单向、双向数据交换，支持增量与全量两种交换方式。 ★能够在 IPV4 协议和 IPV6 协议环境下，支持两个不同网络区域 ftp 文件传输。	1
		请求服务系统	由内网数据服务器和外网数据服务器组成，用于实现跨网数据请求与响应。可与数据交换系统、单向导入系统无缝对接，保证传输数据、内网网络环境安全。 单主机硬件配置为：10/100/1000Mbps 以太网络接口不少于 2 个，SFP+万兆光纤网络接口不少于 2 个。 图片传输性能≥500 张/秒（1M），系统吞吐量（数据吞吐量）：≥5Gbps，服务请求并发性能≥15000，延	1

			时≤1s。 系统访问服务时，可对请求 URL、请求 IP、请求时间、请求数据和回应数据等进行检查和过滤。 ★系统提供服务时，对客户端必须进行身份验证，认证过程中支持时间、IP 等规则设置。（提供检测报告证明）	
	县公安网-市公安网	防火墙	标准X86多核并行架构,1U标准机架,双交流冗余电源,至少配置接口：8 个 GE 电口，2 个 SFP 光口，2 个 SFP+万兆光口，2 个扩展槽位,防火墙网络吞吐量≥10Gbps。并发连接数≥400 万，每秒新建 HTTP 连接数≥20 万。含三年 IPS 和防病毒模块。 支持路由、虚拟线、Listening、交换混合工作模式。支持静态路由、动态路由和ISP路由协议,支持802.1Q、QinQ 模式。 支持手动添加绑定和 IP、接口的动态探测绑定，可实现跨三层 IP/MAC 绑定，绑定表可导入导出。 针对公安网大规模多路由接入环境，设备需支持芯片数据包缓存管理，实现多核平台下的多系统并行运行及数据共享，支持在一台物理设备上划分出 128 个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源。 支持基于 IP/IP 组、应用/应用组、服务/服务组、用户/用户组配置带宽策略，支持带宽策略优先级，可配置包含多级 5 层带宽策略，对流量进行细分管理，保证带宽的利用率。 可以通过 TCP 连接粘合实现应用代理加速，通过该技术可可实现 HTTP、FTP、POP3、SMTP、IM 等协议的病毒快速查杀，支持木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的精准查杀，可实现压缩文件解码查杀。 支持对基于最大并发连接数的单条访问控制策略进行限制。	2
	视频专网-视联网	视频安全交换系统（三件套）	标准 2U 机架式，由信任端服务器及非信任端服务器、安全隔离与信息交换系统组成。 信任端服务器及非信任端服务器服务器各具备 100/1000Mbase-TX 以太接口不少于 2 个，万兆光纤接口不少于 2 个，安全隔离与信息交换系统具备 100/1000Mbase-TX 以太接口不少于 2 个，万兆光纤接口不少于 2 个。 为满足客户业务需求，视频交换系统吞吐量不低于 9.8Gbps，并发连接数不低于 400000 个。 为满足市场各品牌对接需求以及便于配置人员对接业务，产品支持配置不同视频厂商产品适配的模板文件，快速生成视频传输通道。 ★根据网络 IP 升级需要，视频交换系统能够在 IPV4 和 IPV6 协议环境下，对视频流使用用户、源端 IP 地址、目的端 IP 地址、访问时间进行控制；可对视频流进行丢帧、插帧处理；可对信令协议做 register、play 等关键字过滤，控制操作类型。（提供检测报告证明）	1

	分机房-视频专网	防火墙	标准X86多核并行架构,1U标准机架,双交流冗余电源,至少配置接口：8个GE电口，2个SFP光口，2个SFP+万兆光口,2个扩展槽位,防火墙网络吞吐量≥10Gbps。并发连接数≥400万，每秒新建HTTP连接数≥20万。含三年IPS和防病毒模块。 能够基于时间、用户/用户组/安全组、应用层协议IP地址、端口、域名组、URL分类、实现视频流的安全策略配置。 防火墙支持芯片硬件加速，基于专用防火墙专用芯片实现防火墙底层硬件加速机制，整体提升防火墙处理性能。 支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维。 支持循环事件实时监控并存取技术，对指定地址的ARP清求使用 指定接口的 MAC地址应答，实现保护内网主机。 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议。 支持用户服务器的负载均衡，保证用户关键服务的有效性。 策略路由支持的匹配条件：源IP/目的IP、用户(组),入接口。 支持实时链路监控，发现异常可启动功能自动切换到可用链路，确保网络的正常通信。 支持防火墙环境下动态负载均衡的网络地址转换，同时具有独立DNSDoctoring功能，可将来自内网的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡及对应功能。	3
	县WA网-市WA网	防火墙	标准X86多核并行架构，1U硬件平台，设备自带电源。至少配置6*GE电口。网络吞吐性能≥2Gbps，最大并发连接数≥100万，每秒新建HTTP连接数≥3.5万。SSL VPN并发用户数≥400。含三年IPS和防病毒模块。 能够基于时间、端口、域名组、用户/用户组/安全组、应用层IP地址、URL分类、实现视频流的安全策略配置。 支持策略的快速（模糊）查询，策略组，策略规则标签，便于策略的管理及运维。 视频网多链路接入环境防火墙需支持过滤规则匹配技术，支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略。 支持链路实时动态监控功能，当发现异常可自动切换到可用链路，确保网络正常的通信。 视频网多链路接入环境下支持检测防火墙冲突规则技术，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在WEB界面显示检测结果：红色为冗余策略，绿色为冲突策略。 具有网络流量阈值检测技术，支持UDP DDOS防护功能，支持基于报文大小限制、阀值检查、源/目的限流方式综合进行UDP报文、UDP FLOOD、UDP FRAG FLOOD防护。 支持基于IP、用户的最大连接数限制，防护服务器。	1

			支持 SIP、H.323 等多种监控媒体协议,设备满足《安全防范视频监控联网系统信息传输、交换、控制技术要求（GB/T 28181-2016）》规范技术要求。	
网络安全运营中心建设	信息安全驾驶舱	信息安全驾驶舱	信息预警:通过安全管理中心，搜集网络安全情报收集归纳整理后，用于构建仙居县内网络安全信息预警池。 应急处突驾驶舱 ：针对已经发生的紧急安全事件，可通过应急处突驾驶舱指派民警赶往事发单位或下发至单位进行处置反馈，跟踪事件发起、取证、处置、触发状态，及时掌握急处置情况。并联合多部门协同处置、加强应急处突能力。 典型案例库：相关典型案例进行统一汇总后形成网络安全典型案例库。 安全通报：进行统一网络安全检通报。构建仙居县内网络安全监测预警技术平台。 安全检查：针对不同部门，进行统一网络安全检查，构建仙居县内网络安全监测预警技术平台。 指数评估：安全评估指数。 数据资源中心建设：对接态势感知系统。对接 IRS 系统。 管理平台：开发管理平台，实现数据资源存储与管理、数据资源详细调阅。	1
		云租费	在台州政务云上提供 8VCPU/16G 内存/1000G 硬盘的云主机一台（包含三年云资费）。	1
	安全运维人员驻点服务	驻点技术支撑	为安全运营中心提供技术现场驻场技术支撑，2 人。了解常见网络安全设备，分析安全设备的告警日志,熟悉主流网络攻击技术和安全漏洞原理,掌握 Burp、sqlmap、nmap、MSF、Nessus 等常用工具,熟悉 WVS、AppScan、Fortify、BurpSuite 等工具的使用。	1
		网络安全可视化服务	为确保项目顺利推进，投标人需提供 3 名具有软件开发工程师证书的人员驻场仙居县公安局至少 6 个月进行项目开发。 安全可视化——信息公开。 支持将所有安全设备信息运行状态及实时安全风险统一展示。	1
		运维数据资源共享平台	支持在处理安全事件流程及响应情况结果，可自动生成报告，并支持推送下属机构。 支持将安全事件年度处理结果展示。 安全大数据整合——现有资源复用，避免投资浪费，充分发挥已有设备能效。 收集现有安全设备日志信息，实现监控、防护、阻断等多维度日志整合，通多单一平台解决运维重复、复杂难题。 制定日志筛选策略规则，分不同场景可通过筛选快速查看有效日志信息。 日志信息归档与统一保存，实现空间自由与保存时间要求。 安全事件响应自动化——自动化实现。 提供安全响应流程，可通过策略一件下发安全通知及处理报告分配给安全运营厂商和服务商，以及实施处理流程。 提供已有安全设备自动化部署流程指导，如态势感知	

			通知自动策略至终端安全管理快捷链接方式或操作指引。 针对每年度新产生的安全事故及安全问题，同样支持自定义流程，以通知应急单位做到反馈及响应。 安全管理合规化——框架完善。 平台支持录入当前单位合规性要求，如软件开发源代码规范、如网络使用规范、等保要求，相关服务单位负责通过账户填写支持信息以及项目信息，确保后期项目建设从根本上符合合规要求，用户方通过需通过审核方可进行项目建设。 提供一体化在线安全培训展示（文档、视频），可协助完成年度培训任务及发布安全培训信息，提高单位整体安全技能以及使用人员基础安全技能。 攻防演练、渗透攻击、应急演练等专业化安全活动录入，此类活动确保年度安全活动合规。	
	相关安全服务	威胁监测与主动响应服务	安全威胁分析：结合安全感知日志和威胁情报进行深度分析，研判网络中存在的威胁和攻击行为，明确对业务的影响和危害。 安全事件处置：对安全事件进行处置，清除恶意文件、快速恢复业务。 事件溯源分析：深入分析安全事件的成因，发现存在的薄弱点，溯源攻击路径 。 安全加固建议：根据事件发生的根因、影响范围，针对性给出安全加固建议。	1
		漏洞管理服务	在漏洞发现的基础上，有效地追踪资产漏洞全生命周期，清楚地掌握资产的脆弱性状况，实现漏洞全生命周期的可视、可控和可管。 提供最新漏洞预警、排查与响应服务。 漏洞协助修复服务。 服务交付 漏洞分析与管理服务：《漏洞管理报告》《紧急漏洞通告》。 最新漏洞预警与响应服务：《漏洞分析与管理服务资产表》《最新漏洞预警》《最新漏洞分析与管理报告》。 漏洞协助处置服务：《漏洞协助处置报告》。	
		诱捕防御服务	为保证仙居公安网络安全的运行环境，需采用有效的技术手段，实现如伪装欺骗环境或安全隔离技术，如遇网络攻击，可使攻击者增加攻击成本，通过信息收集与反制功能，平衡攻防不对等的网络安全环境现状，定期对内部资产进行黑盒测试，主动发现网络环境的脆弱点，做好安全管理提前量，由被动转为主动，需实现以下功能： 配置软件探针≥40 个。 支持伪装常用危险端口的服务，并可对攻击行为进行溯源排查。 对接精准的云端威胁情报，可对 APT 攻击进行更准确的研判。 可下发系统任务，分析系统信息，进行攻击溯源和攻击漏洞排查。 可通过反制平台对攻击源进行反制。 兼容市面主流安全产品，自动化、高度集成收集公安	

			网内部脆弱点，在公安网已部署的安全设备日志和告警信息中快速梳理出安全运营所需要的信息并分析结果，辅助公安管理更高效的处理安全事件。 自动生成相关服务报告。 服务报告支持生成 PDF 格式导出，提供在线打印功能，服务报告的频次最小可设置为 1 次/天。	
		漏洞扫描服务	使用系统漏洞扫描工具对 数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描，扫描完成后由技术人员对漏洞进行确认，提出整改建议，协助开发人员整改。 利用专业级 WEB 应用扫描工具对被评估对象进行应用检测，以发现网站应用层面可能存在的技术漏洞。包括 WEB 容器识别，如：Apache、tomcat、Weblogic、WebSphere 和 Ngix 等。支持多种服务端语言探测，如：PHP、JSP、ASP、ASPX 和.NET 等。支持 WEB 前端框架探测，如：jQuery、Bootstrap、HTML5 等。支持 WEB 后端开发框架探测，如：Django、Rails、ThinkPHP、Struts 等。 支持 WEB 业务应用探测，如：BBS、CMS 和 BLOG 等（备注：逻辑类漏洞主要通过人工渗透测试完成）。 支持扫描对象包括：B/S 架构类应用漏洞，主要包括：SQL 注入、XSS 跨站脚本攻击、应用系统弱口令、敏感文件下载、后台用户枚举等。	
		安全加固	针对巡检和评估过程中存在安全脆弱点的网络架构、网络设备、操作系统、应用系统和数据库系统，根据安全加固工程师制定的安全加固方案进行现场安全加固，并提供加固报告。	
		渗透测试服务	通过模拟黑客可能使用的攻击技术和漏洞发现技术，采用黑盒测试的方法对目标系统的安全做深入的探测，发现系统最脆弱的环节，了解自身网络所面临的问题。 渗透测试内容： 主机操作系统渗透：包括 WINDOWS、SOLARIS、AIX、LINUX、SCO、SGI 等。 数据库系统渗透：包括 MS-SQL、ORACLE、MYSQL、INFORMIX、SYBASE、DB2 等。 应用系统渗透:对各种应用系统进行渗透测试,如 WWW、E-mail、DNS、FTP 等。 渗透测评完成之后，将会详细的说明渗透测评过程中的得到的数据和信息、并且将会详细的纪录整个渗透测评的全部操作过程和数据统计分析结果。	
		安全风险评估	风险评估通过识别资产现有的脆弱性，可能面临的威胁，并充分调研已有的安全控制措施，以综合判断存在的风险，帮助用户预知可能发生的安全事件。 资产数量=业务系统数量+服务器数量（含虚拟机）+安全设备+关键网络设备（核心和汇聚交换机）。 服务交付物：《xx 风险评估报告》。	

		应急响应	当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题根除、协助业务恢复的服务，能够协助用户快速止损，最大化降低安全事件带来的影响。 事件处理完毕后，根据整个事件情况进行分析汇总并提交《安全应急响应报告》，针对安全事件现象、处理过程、处理结果进行陈述，同时对入侵原因进行分析，并给出相应的安全加固建议和安全防御体系建设指导。	
		基线核查	基线核查服务就是针对漏洞扫描工具不能有效发现的方面（网络设备的安全策略弱点和部分主机的安全配置错误等）进行安全辅助的一种有效评估手段。服务范围包括各种网络设备、安全设备、主机操作系统、数据库、常见中间件及网络服务应用等。基线核查的服务内容主要集中在设备的账号管理、口令管理、认证授权、日志配置、进程服务、外部端口等几个方面，覆盖了与安全问题相关的各个层面。	
		安全培训服务	通过开展信息安全培训工作，使客户最终达到强化安全意识，理解安全理论，掌握安全技术，获得安全实践经验，使得信息安全人员能够掌握安全方面必要的专业理论和技能，全面提升从事信息安全工作人员的管理和技术水平，保证其能够胜任相应的岗位，且能够融会贯通并应用于企业的安全建设当中。	
		应急演练	通过应急演练，并协助各级单位开展预案演练，提高应对安全事件的处置能力，预防和减少安全事件造成的危害和损失。应急演练是应急响应事件发生的场景模拟，通过对事件频发、危害性高、影响范围大的特定信息安全事件进行演练，以期在遇到此类信息安全事件应急响应处置过程中，发现问题，及时响应，快速处置的目的。	
等级保护测评服务	三级等保测评	公安网	一年一次，共三次（经过专业检测公司的检测，且出据通过检测报告）	3
		视频专网	一年一次，共三次（经过专业检测公司的检测，且出据通过检测报告）	3
	二级等保测评	取证网	两年一次，共一次（经过专业检测公司的检测，且出据通过检测报告）	1
供应商须保证所供货物是全新的、未使用过的原厂合格正品。本项目服务期届满后，拟投入的软硬件设备的所有权归采购人所有。				

▲（三）等保要求

本项目建成后应满足各网络等保2.0中相应内容的要求，取证网内所建内容符合二级等保要求，公安网和视频专网内所建内容符合三级等保要求，且视频专网内建设符合《台州市公共视频监控安全建设指南》的要求。**投标人须在商务与技术文件中作出相应符合等保要求承诺书。**

（四）项目售后服务要求

1.本项目软硬件设备的质保期至少为三年（从项目初验完成之日起开始计算）。在此质保期内，如在正常使用过程中出现的问题，供应商须负责免费维修或调换。质保期届满后，中标供应商终身维护，仅收取零配件成本费用，免人工费、差旅费。

2.本项目售后服务响应时间符合省厅、市局的考核要求。提供 7*24 小时故障电话服务热线。7*24 小时响应，故障申告后：1 小时内响应，1 小时到现场，如遇重、特大事故需紧急抢修的，特殊处理。

（五）项目驻场人员要求

中标供应商应在接到中标通知书后，即刻安排2名技术人员到仙居县公安局提供项目服务期内驻场技术支撑,驻场服务期间按采购人工作时间要求上下班。根据业务需要，驻场人员中有一人需同时具备网络工程师证书、信息安全工程师证书、网络安全工程师证书，另一人需具备注册渗透测试工程师证书，驻场技术支撑人员服务期内不得更换，且驻场技术支撑人员的一切费用由中标供应商负责。**投标人应在投标文件中明确相应的驻场技术人员，提供相关证明材料。**经采购人同意后才能变更相应驻场技术人员。

（六）项目培训要求

投标人需要提供详细合理的项目培训方案（包括培训计划、方式、目标等），对投标人相关人员进行培训，确保人员能熟练掌握所提供设备和软件的操作技术、维护保养知识及常见故障排除方法等。

三、考核办法

服务项	服务子项	服务细项	指标	评分
驻场人员服务	技术人员 1	同时具备网络工程师证书、信息安全工程师证书、网络安全工程师证书	服务期间人员不得更换	8
	技术人员 2	具备注册渗透测试工程师证书	服务期间人员不得更换	8
机房环境	基本环境采集量	温度	24 度（范围相对值 15%）	2
		湿度	55%（范围相对值 20%）	2
		供电、防水、防雷、门磁	正常	2
		烟雾探测、UPS 过载	正常	2
		精密空调状态	正常	2
现场管理服务	常规巡检服务	客户机房环境巡检	每月一次	10
		主机、存储、网络设备硬件运行状态巡检		

		接入辅助设备巡检		
		物理链路巡检		
	现场操作服务	线路插拔、介质更换	正常	5
		设备开关机（物理）	正常	5
	现场管理服务报告		月度	10
系统监管服务	设备线路监控	网络、安全设备监控	正常	4
		主机、存储等设备监控		
		互联情况监控		
	系统监控服务	数据库监控	正常	5
		Web 服务监控		
		系统日志监控		
	监控分析报告		月度	10
系统维护服务	系统高级操作	系统安装、更新及升级	正常	5
		数据库等软件安装及升级		
	系统健康性检查	网络设备巡查	每月一次	5
		主机、存储设备巡查		
	系统维护服务报告		月度	15
总分				100
故障处理	故障处罚要求	第Ⅰ级，重大事件	次/季度	扣季度付款总额*50%
		第Ⅱ级，较大事件	次/季度	扣季度付款总额*30%
		第Ⅲ级，一般事件	次/季度	扣季度付款总额*10%

备注：事件定级要求根据“台州市公安局网安部门处置网络安全事件应急处置规定”、“浙江省公安厅网安部门处置网络安全事件应急处置规定。”

四、讲解演示要求

1.本项目须进行讲解演示，演示次序以投标文件解密时间先后次序为准，总时间不超过 20 分钟。各投标人不允许出现相同的演示人员。投标人演示参与人员不超过 2 人，参与演示人员必须符合当地防疫要求，同时提交“讲解演示委托书”（见附件）。

2.疫情防控要求：因近期疫情防控需要，近 14 天到达或途经国内疫情中高风险地区的人员无法进入公共场所;其余人员需持 7 天内核酸检测阴性证明和绿色双码进入场所（如有疫情防控新政策，按新政策执行）。

3.投标供应商演示时自带电脑，须提供双份演示方案存储介质（以 U 盘和光盘不同介质存储）。演示结束后供应商现场向采购人提交全部演示方案存储介质。

4.中标供应商演示方案存储介质由采购人保管封存，作为履约验收的参考。

五、商务需求

（一）服务期限：本项目服务期限为三年，自项目初验完成之日起三周年。

（二）项目前期实施期限及实施地点

1.项目前期实施期限：自合同签订之日起 40 个日历天 内将设备运抵采购人指定地点，并在设备运抵后 50 个日历天 内安装调试完毕（包括原有设备搬迁及机房临时开通）。

2.项目实施地点：采购人认可的地点。

（三）项目其他要求

▲1.本项目“19 个综合架的设备托管服务”的每架每季度服务费报价≤16500 元/架/季度。服务期届满后 5 年内，采购人需额外采购托管服务的，中标供应商报价不得高于本次“每架每季度服务费”报价。

2.产品包装应符合国家或行业标准规定。产品交付时，产品须与“拟投入的主要软硬件设备情况”一致，同时附产品合格证书、产品说明书、装箱单、易损件（如有）、备件及专用工具清单（如有）等一套完整的技术文件资料。

3.中标供应商须对送货、安装、调试等工作人员的安全文明施工负责，必须按项目需求及国家有关规范标准进行施工，确保施工现场的安全生产和文明施工；根据疫情防控工作要求，承诺确保工作人员符合当地疫情防控标准。中标供应商在项目施工过程中如造成人员伤亡、财产损失的，有关责任均由中标供应商承担。

4.中标供应商应建立完善的运维管理系统、运维团队架构、故障处理流程、电子化工单及考核体系、其他运维相关的业务流程规范和制度。

（四）项目验收

1.本项目验收参照 GB28181-2016 公共安全视频监控联网系统信息传输、交换、控制技术要求、DB33/T 629.1-2011《跨区域视频监控联网共享技术规范》、DB33/768-2009《安全技术防范系统建设技术规范》等相关标准。

2.中标供应商应按本项目招标文件要求完成所有工作内容，项目终验时应提供竣工报告、第三方专业机构检测报告及监理报告等验收文本。

3.中标供应商提供本项目所有服务中涉及的软硬件产品必须与投标文件产品一致。

4.托管服务项数据机房需达到 B 级标准、模块化一体化机房建设标准设计。

（五）付款条件

1.合同签订之日起 7 个工作日内，采购人向中标供应商支付项目预付款，项目预付款为合同金额的 30%。

2.项目最终验收合格后，采购人将根据考核结果按季度支付剩余款项。采购人每季度第一个月的 5 日前将上一季度的考核结果抄送至中标供应商，采购人收到发票后并于每季度第一个月的 15 日前结算上季度的服务费用。每年付款金额不超过 800 万元。

季度实际付款=每季度根据监理及采购人打分（即每季度考核总分数÷3 月÷100）×每季度平均付款[（中标投标报价-预付款）÷3 年÷4 季度]

（六）履约保证金

项目履约保证金为合同金额的1%（向采购人交纳，具体详见“前附表”），项目最终验收合格之日起7个工作日内由采购人退还（不计息）。

第五章 拟签订的合同文本

项目名称： 项目编号：

甲方：（采购单位） 所在地：

乙方：（中标供应商） 所在地：

甲、乙双方根据仙居县政府采购中心关于（填写项目编号及项目名称）项目公开招标的结果，签署本合同。

一、合同文件：

1.合同条款。

2.中标通知书。

3.更正补充文件。

4.招标文件。

5.中标供应商投标文件。

6.其他。

上述所指合同文件应认为是互相补充和解释的，但是有模棱两可或互相矛盾之处，以其所列内容顺序为准。

二、合同内容及服务标准

合同内容及服务标准：具体见招标需求

三、合同金额

本合同金额为（大写）：_____元（￥_____元）人民币。

四、甲乙双方责任和义务

（一）甲方的权利和义务

1.监督、管理托管设备的安装、调试，并负责验收。

2.对乙方履行托管责任的情况进行监督与检查，对存在的问题提出改进意见、要求或建议。

3.按照约定交纳托管费用。

4.有权通过远程系统对托管的服务器进行配置、管理以及更新内容等操作。

5.甲方有权要求乙方运出自己的服务器以便甲方维护。

（二）乙方责任和义务

1.提供放置信息服务器所需的标准机房环境，包括：照明系统、电力系统、恒温恒湿系统、监控系统、门禁系统、消防系统、防静电地板、服务器系统安全等。

2.提供实现服务器托管业务所需的标准网络环境，包括标准交换机接口、互联网络出口、空间环境等，并配备专业的网管工程师为甲方提供服务。

3.保证甲方的服务器设备可持续获得电力供应，每月持续电力供应时间在 99%以上。

4.负责甲方信息服务器的设备的安全管理，以保证客户信息服务器的正常运行。

5.向甲方提供场地环境日常维护，包括：机器表面的清洁、机房卫生；电源配电系统的定期检查。

6.向甲方提供托管设备的一般性日常维护，包括：7*24 小时系统运行状态监测，网络设备系统状态日常检查、维护管理与技术支持。响应时间：当乙方接到甲方服务请求时，在 1 小时内到达现场。

五、技术资料

1.乙方应按招标文件规定的时间向甲方提供有关技术资料。

2.没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

六、知识产权

1.乙方应保证提供服务过程中不会侵犯任何第三方的知识产权。

2.若侵犯,由乙方赔偿甲方因此遭受的损失（包括但不限于应对及追偿过程中所支付的律师费、差旅费、诉讼费、保全费、鉴定费、评估费等）。

七、履约保证金

本项目履约保证金为合同金额的__1__% 。[履约保证金交至采购人处，在项目最终验收合格之日起7个工作日内无息退还]。

八、转包或分包

1.本合同范围的服务，应由乙方直接供应，不得转让他人供应；

2.除非得到甲方的书面同意，乙方不得将本合同范围的服务全部或部分分包给他人供应；

3.如有转让和未经甲方同意的分包行为，甲方有权解除合同，没收履约保证金并追究乙方的违约责任。

九、合同履行时间、履行方式及履行地点

1.履行时间：

2.履行方式：

3.履行地点：

十、拟投入软硬件设备的质量规格及质保期

为完成服务拟投入软硬件设备的质量和规格应符合公开招标的招标文件、投标文件及乙方询标过程中做出的书面说明及承诺，质保期_____年（从项目初验完成之日起开始计算）。

十一、款项支付

1.合同签订之日起 15 日内，甲方向乙方支付项目预付款，项目预付款为合同金额的 30%。

2.项目最终验收合格后，甲方将根据考核结果按季度支付剩余款项。甲方每季度第一个月的 5 日前将上一季度的考核结果抄送至乙方，甲方收到发票后并于每季度第一个月的 15 日前结算上季度的服务费用。每年付款金额不超过 800 万元。

季度实际付款=每季度根据监理及甲方打分（即每季度考核总分数÷3 月÷100）×每季度平均付款[（中标投标报价-预付款）÷3 年÷4 季度]

十二、税费

本合同执行中相关的一切税费均由乙方负担。

十三、质量保证及售后服务

1.乙方应按招标文件规定向甲方提供服务。

2.乙方提供的服务成果在服务质量保证期内发生故障，乙方应负责免费提供后续服务。对达不到要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴赔偿处理；

⑵解除合同。

3.如在使用过程中发生问题，乙方在接到甲方通知后在____小时内到达甲方现场。

4.在服务期内，乙方应对出现的质量及安全问题负责处理解决并承担一切费用。

十四、验收

1.本项目验收参照 GB28181-2016 公共安全视频监控联网系统信息传输、交换、控制技术要求、DB33/T 629.1-2011《跨区域视频监控联网共享技术规范》、DB33/768-2009《安全技术防范系统建设技术规范》等相关标准。

2.乙方应按本项目招标文件要求完成所有工作内容，项目终验时应提供竣工报告、第三方专业机构检测报告及监理报告等验收文本。

3.乙方提供本项目所有服务中涉及的软硬件产品必须与投标文件产品一致。

4.托管服务项数据中心机房达需到 B 级标准、模块化一体化机房建设标准设计。

十五、考核办法

服务项	服务子项	服务细项	指标	评分
驻场人员服务	技术人员 1	同时具备网络工程师证书、信息安全工程师证书、网络安全工程师证书	不得更换	8
	技术人员 2	具备注册渗透测试工程师证书	不得更换	8
机房环境	基本环境采集量	温度	24 度（范围相对值 15%）	2
		湿度	55%（范围相对值 20%）	2
		供电、防水、防雷、门磁	正常	2
		烟雾探测、UPS 过载	正常	2
		精密空调状态	正常	2
现场管理服务	常规巡检服务	客户机房环境巡检	每月一次	10
		主机、存储、网络设备硬件运行状态巡检		
		接入辅助设备巡检		
		物理链路巡检		
	现场操作服务	线路插拔、介质更换	正常	5
		设备开关机（物理）	正常	5
	现场管理服务报告		月度	10
系统监管服务	设备线路监控	网络、安全设备监控	正常	4
		主机、存储等设备监控		
		互联情况监控		
	系统监控服务	数据库监控	正常	5
		Web 服务监控		
		系统日志监控		
	监控分析报告		月度	10
系统维护服务	系统高级操作	系统安装、更新及升级	正常	5
		数据库等软件安装及升级		
	系统健康性检查	网络设备巡查	每月一次	5
		主机、存储设备巡查		
	系统维护服务报告		月度	15
总分				100

故障处理	故障处罚要求	第Ⅰ级，重大事件	次/季度	扣季度付款总额*50%
		第Ⅱ级，较大事件	次/季度	扣季度付款总额*30%
		第Ⅲ级，一般事件	次/季度	扣季度付款总额*10%

备注：事件定级要求根据“台州市公安局网安部门处置网络安全事件应急处置规定”、“浙江省公安厅网安部门处置网络安全事件应急处置规定。”

十六、托管机房要求

1.机房地点在仙居县城区范围内，新建地点须获得采购人认可，并具备提供本项目相应标准机柜的服务能力。

2.数据中心机房至少满足 32 个综合架的安装位置及后续扩容位置，机房面积至少保证 200 平米及以上；并配有相应的配线间、UPS 间、监控管理等；配线间至少保证两个不同光缆路由出局，机房要求在本次项目签订合同后 12 个月内完成验收。

3.数据中心机房按 B 级标准、模块化一体化机房建设标准设计。包括机房装修、供配电系统（UPS 系统）、防雷接地系统、机房空调系统、机房环控、机房配线间等子系统。

4.机房应远离无线电和强力电源干扰，避开地震区和其他震源，避开环境污染区、远离容易发生燃烧、爆炸、洪水地区和低洼地区。

5.周边具有市政配套环境，网络通信资源丰富，提供各运营商线路接入支持。

6.机房为独立建筑，与办公区域、库房区域、生活配套区域不在同一建筑内或具有有效分隔。

7.数据中心机房应具有风险抵御能力，如地震、火灾、洪水、台风/暴风雨、鼠虫害、设备故障、操作风险等，确保基础设施的连续性。

8.数据中心机房应具有安全性、可用性设计，包括建筑结构、系统冗余能力、物理安全考虑、人员设备控制、消防安全考虑、应急能力、防电磁辐射、防雷、防水、防静电等。

9.建筑主体结构应具有耐久、抗震、防火、防止不均匀沉陷等性能，建筑结构安全等级为一级，抗震设防烈度不低于 8 度。

10.数据中心机房在场地空间、电力容量、空调容量、通讯能力等方面都应有足够的余量，以满足甲方未来扩展需要。

十七、违约责任

1.甲方无正当理由拒绝接受服务的，甲方向乙方偿付合同款项的 百分之五 作为违约金。

2.甲方无故逾期验收和办理款项支付手续的，甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3.乙方未能如期提供服务的，每日向甲方支付合同款项的千分之六作为违约金。乙方超过约定日期_____个工作日仍不能提供服务的，甲方可解除本合同。乙方因未能如期提供服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值 5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

十八、不可抗力

1.在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2.不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3.不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十九、争议的解决

如双方在履行合同时发生纠纷，应协商解决；协商不成时，可提请政府采购管理部门调解；调解不成的通过_____方式解决（两种解决方式只能择其一）：

⑴ 提交台州仲裁委员会仲裁。

⑵ 依法向人民法院提起诉讼。

二十、合同生效及其它

1.合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

2.本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

3.本合同一式四份。甲、乙双方各执一份，采购组织机构及同级人民政府财政部门各执一份。本项目未尽事宜以招标文件、投标文件及澄清文件等为准。

甲方（公章）	乙方（公章）
法定代表人或授权代表：	法定代表人或授权代表：
联系电话：	联系电话：
开户银行：	开户银行：
帐号：	帐号：

地址及邮编：

签订日期：　　年　　月　　日

地址及邮编：

签订日期：　　年　　月　　日

第六章 投标文件格式附件

附件一：

投标文件

投 标 文 件 名 称： 资格证明文件

采 购 编 号：

项 目 名 称：

标 项：（若有）

投标人全称（盖章）：

投 标 人 地 址：

年 月 日

目录(资格证明文件)

1.投标声明书

2.授权委托书（法定代表人或营业执照中负责人亲自办理投标事宜的，提供法定代表人或营业执照中负责人有效的身份证）

3.营业执照等证明文件

4.具有良好的财务状况、依法缴纳税收和社会保障资金的承诺函

5.具有履行合同所必需设备和专业技术能力的承诺函；其中，电信、移动、联通等区域性分支机构参与投标的，还需提供总公司（总机构）授权（或出具总公司的有关文件或制度等能够证明总公司授权独立开展业务的证明）或提供房产权证或其他有效财产证明材料

6.招标公告中符合项目特定资格要求的有效资质证书（如有要求的，必须提供，其中电信、移动、联通等区域性分支机构参与投标的，必须提供总公司的《基础电信业务经营许可证》才能视为符合供应商特定资格要求）

注：以上内容相关要求见“第二章 投标人须知”中“投标文件”组成内容。

附件二：

投标声明书

致仙居县政府采购中心 ：

我（姓名）系 （投标人全称） 的法定代表人（或营业执照中的负责人），我方愿意参加贵方组织的 （项目名称）（项目编号） 的投标。为此，我方就本次投标有关事项郑重承诺如下：

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、我方承诺已经具备《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》中规定的参加政府采购活动的投标人应当具备的条件，并真实提供相关材料。

4、若中标，我方将按招标文件规定履行合同责任和义务。

5、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及其附属机构没有任何联系。

6、投标文件自开标日起有效期为 90 天。

7、我方参加本项目投标活动前三年内无重大违法记录（重大违法记录是指供应商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），符合《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》的规定。

8、我方保证，采购人在中华人民共和国境内使用我方投标货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，如有第三方向采购人提出侵犯其专利权、商标权或其它知识产权的主张，该责任由我方承担。我方的投标报价已包含所有应向所有权人支付的专利权、商标权或其它知识产权的一切相关费用。

9、以上事项如有虚假或隐瞒，我公司愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

与本投标有关的一切往来通讯请寄：

地址：_____ 邮编：_____

电话：_____ 传真：_____

投标人（盖章）：

日 期：

注：▲必须按照本声明书要求填报。

附件三：

授权委托书

仙居县政府采购中心 **：**

我 法定代表人姓名（或营业执照中负责人姓名）系 （投标人全称） 的法定代表人（或负责人），现授权委托本单位在职职工 （姓名） 以我方的名义参加就贵方组织的 （项目名称）（项目编号） 的投标活动，并代表我方全权办理针对上述项目的投标、开标、评审、签约等具体事务和签署相关文件。

我方对全权代表的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。全权代表在授权委托书有效期内签署的所有文件不因授权的撤销而失效。

全权代表无转委托权，特此委托。

全权代表姓名：_____职务：_____联系电话_____ 。

全权代表身份证号码：_____。

法定代表人或营业执照中单位负责人签名（或签名章）：_____

投标人（盖章）： **日 期：**

附：法定代表人（或营业执照中单位负责人）身份证复印件

法定代表人（或营业执照中单位负责人）身份证复印件粘帖处（正面）	**法定代表人（或营业执照中单位负责人）身份证复印件粘帖处（反面）**

附：全权代表身份证复印件

全权代表身份证复印件粘帖处 （正面）	全权代表身份证复印件粘帖处 （反面）

附件四：

具有良好的财务状况、依法缴纳税收和社会保障资金的承诺函

仙居县政府采购中心：

我方参与的（项目名称）（项目编号）的投标活动，我方郑重承诺，我方具有良好的财务状况，有依法缴纳税收和社会保障资金的良好记录，不存在欠税、偷税、逃税和欠缴、逃避社会保障资金等方面的相关记录。如有虚假，采购组织机构可取消我方任何资格（投标/中标/签订合同），我方对此无任何异议。

特此承诺！

投标人（盖章）：

日　期：

附件五：

具有履行合同所必需设备和专业技术能力的承诺函

仙居县政府采购中心 ：

我方参与的（项目名称）（项目编号）的投标活动，我方郑重承诺，我方承诺具有履行合同所必需设备和专业技术能力。如有虚假，采购组织机构可取消我方任何资格（投标/中标/签订合同），我方对此无任何异议。

特此承诺！

投标人（盖章）：

日 期 ：

附件六：

投标文件

投 标 文 件 名 称： 商务与技术文件

采 购 编 号：

项 目 名 称：

标 项：（若有）

投标人全称（盖章）：

投 标 人 地 址：

年 月 日

目录（商务与技术文件）

注：以上内容相关要求见“第二章投标人须知”中“投标文件”组成内容。

附件七：

投标人基本情况表

单位名称						
注册地址						
联系方式	联系人			电话		
	传真			网址		
法定代表人	姓名		技术职称		电话	
成立时间			员工总人数			
统一社会信用代码			高级职称人数			
注册资金			中级职称人数			
开户银行			初级职称人数			
账号			技工人数			
经营范围						
发展历程及主要荣誉						
企业综合情况介绍						

投标人（盖章）：

日 期 ：

附件八：

项目实施人员一览表

序号	姓名	职务	岗位职责	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	类似经验	备注

要求：

1.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划表填写；

2.附人员证书及其他相关材料；

投标人（盖章）：

日 期 ：

附件九：

项目负责人资质情况表

姓名		**近年来主要工作业绩**
性别		注：业绩证明应提供旁证材料（供货合同或中标通知书）。
年龄		
职称		
毕业时间		
学校专业		
联系电话		
最近一年工作状况		
拟在本项目中担任主要工作		

投标人（盖章）：

日 期 ：

附件十：

拟投入的主要软硬件设备情况

序号	产品名称	规格型号	招标参数	投标参数	偏离情况	备注

要求：

1.投标人应根据本招标文件第四章“招标需求”内容，按实填写投标产品的性能指标、服务指标等内容（**完全复制粘贴招标需求内容的，作无效标处理**），并在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

2.对于投标产品的技术偏离情况需严格按照招标文件的技术要求一一比对给出，未达到技术要求中规定的数值应以负偏离标注。若因技术实现方式等其他问题而导致的理解不同未标注负偏离的，需在备注中具体说明；若未按要求标注负偏离又未予以说明的，评标委员会将视偏离程度给予扣分或认定为虚假应标。

投标人（盖章）：

日 期 ：

附件十一：

证书一览表

证书名称	发证单位	证书等级	证书有效期

要求：

1.填写投标人获得资质、认证证书；

2.附所列证书或其他证明材料。

投标人（盖章）：

日 期 ：

附件十二：

商务响应表

条款名称	招标文件要求	投标文件的响应内容	是否响应
……			

注：投标人应根据本招标文件第四章“招标需求”中“商务需求”内容逐条响应，按实填写响应内容。

投标人（盖章）：

日 期 ：

附件十三：

投标人同类项目业绩实施情况表

序号	项目名称	项目地址	合同总价	实施时间	项目单位名称及其联系人电话
1					
2					
3					
…					

要求：业绩证明应提供证明材料（合同可提供首页、含金额页、含采购产品内容页、盖章页，中标（或成交）通知书以及验收报告（或验收证明））。

投标人（盖章）：

日　期：

附件十四：

投标文件

投标文件名称：报价文件

采购编号：

项目名称：

标项：（若有）

投标人（盖章）：

投标人地址：

年 月 日

目录（报价文件）

附件十五：

开标一览表

项目编号：XJCG-2022-GK005

项目名称：仙居县公安局公共视频一体化及网络安全建设

[货币单位：人民币元]

投标报价(元)	大写	
	小写	

注：投标报价是包括与本服务项目相关的设备安装、调试、验收、培训合格之前所有含税费用、税金、光纤租赁费用、其他费用（包括质保期内的备品备件、易损件、专用工具等）、制造、包装、保险、运输、仓储、税金、验收、安装、售后服务、招标中规定的设备搬迁、各种人工费及技术支持等相关服务的费用、合同包含的所有风险责任等各项费用以及不可预见费等所需的全部费用，全部费用已包含在开标一览表的投标总报价中。

投标人（盖章）：

日　　期：

附件十六：

投标报价明细表

[货币单位：人民币元]

序号	服务内容	每架每季度服务费	三年服务费（总价）
1	仙居县公安局公共视频一体化及网络安全建设（设备托管服务费用除外）		
2	19 个综合架的设备托管服务		
……			
合计投标总报价			￥_____

注：

▲1.“19 个综合架的设备托管服务”的每架每季度服务费≤16500 元/架/季度。服务期届满后 5 年内，采购人需额外采购托管服务的，中标供应商报价不得高于本次“每架每季度服务费”报价。

2.合计投标总报价＝仙居县公安局公共视频一体化及网络安全建设（设备托管服务费用除外）三年服务费（总价）＋19 个综合架的设备托管服务三年服务费（总价）。

3.“投标报价明细表”中的投标总报价应与“开标一览表”中的投标总报价相一致。

投标人（盖章）：

日　　期　：

附件十七：

中小企业声明函（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，提供的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）行业；承接企业为（企业名称），从业人员__人，营业收入为____万元，资产总额为____万元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）行业；承接企业为（企业名称），从业人员__人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

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

监狱企业声明函

提供省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，格式自拟

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，且本单位参加仙居县政府采购中心 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。

单位名称（盖章）：

日 期 ：

附件十八：

政府采购活动现场确认声明书

仙居县政府采购中心 ：

本人经由＿＿＿＿＿＿＿＿＿＿＿＿＿＿（单位）负责人＿＿＿＿（姓名）合法授权参加＿＿＿＿＿＿＿＿＿＿＿＿＿＿项目（编号：＿＿＿＿＿＿＿＿）政府采购活动，经与本单位法人代表（负责人）联系确认，现就有关公平竞争事项郑重声明如下：

一、本单位与采购人之间 □不存在利害关系 □存在下列利害关系＿＿＿＿＿＿：

A.投资关系　　B.行政隶属关系　　C.业务指导关系

D.其他可能影响采购公正的利害关系＿＿＿＿＿＿（如有，请如实说明）＿＿＿＿＿＿。

二、现已清楚知道参加本项目采购活动的其他所有供应商名称，本单位 □与其他所有供应商之间均不存在利害关系 □与＿＿＿＿＿＿（供应商名称）＿＿＿＿＿＿之间存在下列利害关系＿＿＿＿＿＿：

A.法定代表人或负责人或实际控制人是同一人

B.法定代表人或负责人或实际控制人是夫妻关系

C.法定代表人或负责人或实际控制人是直系血亲关系

D.法定代表人或负责人或实际控制人存在三代以内旁系血亲关系

E.法定代表人或负责人或实际控制人存在近姻亲关系

F.法定代表人或负责人或实际控制人存在股份控制或实际控制关系

G.存在共同直接或间接投资设立子公司、联营企业和合营企业情况

H.存在分级代理或代销关系、同一生产制造商关系、管理关系、重要业务（占主营业务收入50%以上）或重要财务往来关系（如融资）等其他实质性控制关系

I.其他利害关系情况＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿。

三、现已清楚知道并严格遵守政府采购法律法规和现场纪律。

四、我发现＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿供应商之间存在或可能存在上述第二条第＿＿＿＿＿＿项利害关系。

供应商代表签名：

2022年月日

附件十九：

讲解演示委托书

仙居县政府采购中心 **：**

我 法定代表人姓名（或营业执照中负责人姓名）系 （投标人全称） 的法定代表人（或负责人），现授权委托 （讲解演示代表姓名） 为我方参与 仙居县公安局公共视频一体化及网络安全建设 项目投标讲解演示代表。

讲解演示代表姓名：_____联系电话：_____ 。

讲解演示代表身份证号码：_____。

法定代表人或营业执照中单位负责人签名（或签名章）：_____

投标人名称：_____**（盖章）** **委托日期：**

附：讲解演示代表身份证复印件

讲解演示代表身份证复印件粘帖处（正面）

讲解演示代表身份证复印件粘帖处（反面）