2019年江干区数据安全建设和政务服务保障项目

公开招标文件

招标编号：ZJCT5-2019155

杭州市江干区数据资源管理局

浙江省成套工程有限公司

二〇一九年十一月

目　录

第一部分　招标公告

根据《中华人民共和国政府采购法》等有关规定，浙江省成套工程有限公司受杭州市江干区数据资源管理局委托，就2019年江干区数据安全建设和政务服务保障项目进行采购，欢迎国内合格的供应商前来参加。

一、招标编号：ZJCT5-2019155

二、采购组织类型：分散采购委托代理

三、采购方式：公开招标

四、招标项目概况（内容、用途、数量、简要技术要求等）：

序号	标项内容	数量	单位	预算金额（万元）	简要技术要求、用途	备注
1	2019年江干区数据安全建设和政务服务保障项目	1	项	539.5	详见招标文件	

五、投标供应商资格要求：

1、符合《中华人民共和国政府采购法》第二十二条的规定：

2、供应商未被列入失信被执行人名单、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，信用信息以信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）公布为准。

3、本次招标不接受联合体投标；

六、招标文件的发售时间、地点、售价：

1、发售时间：即日起至磋商截止时间 (双休日及法定节假日除外)，上午：09:00-11:30，下午：13:30-16:30。

2、发售地点：杭州市古墩路701号紫金广场A座1209室；

3、招标文件售价：人民币500.00元整，售后不退，汇款请在用途栏中注明项目编号：ZJCT5-2019155。

收款单位（户名）：浙江省成套工程有限公司；

开　户：杭州联合农村商业银行三墩支行

账　号：201000065548152

七、投标截止时间：2019年　月　日09：30

八、投标地点：杭州市古墩路701号紫金广场A座浙江省成套工程有限公司1505室

九、开标时间：2019年　月　日09：30

十、开标地点：杭州市古墩路701号紫金广场A座浙江省成套工程有限公司1505室

十一、投标保证金：不收取。

十二、其他事项：

1．供应商认为采购文件使自己的权益受到损害的，可以自收到采购文件之日（发售截止日之后收到采购文件的，以发售截止日为准）或者采购文件公告期限届满之日（招标公告为公告发布后的第 6 个工作日）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。

2.投标人购买标书时应提交的资料：

1）介绍信或法定代表人（单位负责人）授权书（原件）；

2）被授权人身份证（原件和复印件）；

3）有效的营业执照副本（或法人证书）等复印件（复印件加盖单位公章）；

3.对符合财政扶持政策的小微企业（或监狱企业）给予价格优惠扶持，供应商应为浙江政府采购网的正式入库供应商；

4.潜在供应商可在浙江政府采购网 http://www.zjzfcg.gov.cn 进行免费注册，具体详见浙江政府采购网供应商注册要求；

5.书面质疑受理地点：杭州市西湖区古墩路 701 号紫金广场 A 座 1209 室，联系人：小张，电话：0571-85058600；

6.政府采购监管部门：杭州市江干区财政局，监督投诉电话：0571-86438095；

7.采购人：杭州市江干区数据资源管理局；地址：杭州市庆春东路 1 号；联系人：张老师；联系电话：0571-86974690。

十三.联系方式：

采购代理机构名称：浙江省成套工程有限公司

地址：杭州市西湖区古墩路 701 号紫金广场 A 座 1209 室

联系人：章日

电话：0571-85058255

传真：0571-85058600

邮箱：zjct105@163.com

杭州市江干区数据资源管理局

浙江省成套工程有限公司

2019 年__月__日

第二部分　编制和提交投标文件须知

前 附 表

条款	内容规定
1	**项目说明** **一、项目名称：**2019 年江干区数据安全建设和政务服务保障项目 **二、采购要求、用途：**详见第三部分——项目技术规范和服务要求。 **三、项目实施地点：**杭州市江干区数据资源管理局及其指定地点。 **四、采购内容：**详见第三部分——项目技术规范和服务要求。 **五、项目进度要求：**项目内容必须在合同签订后 90 天内完成项目实施，并按照要求做好项目验收。 **▲六、采购预算：本项目总预算为 539.5 万元，其中建设费用预算为 508.5 万元；设备维护维保费用预算为 31 万元，总价不能超过总预算，分项价格不能超过对应的分项预算，超过预算为无效标。**
2	**合同名称**　《2019 年江干区数据安全建设和政务服务保障项目合同》
3	**投标有效期：**自投标截止日起 90 天。
4	**投标保证金数额：**不收取。
5	**付款方式：**合同签订后 10 天内支付合同总价的 20%；主要设备到货后支付合同总价的 25%；项目初验通过后支付合同总价的 30%；项目验收通过后支付合同总价的 25%。
6	**履约担保：**在合同签订后 10 天内，中标方向甲方缴纳合同总价 5%的履约保证金。项目通过验收后，履约保证金转为质量保证金，系统正常运行三个月，支持良好，无质量和服务问题，甲方无息退还中标方质量保证金。
7	**招标服务费：** 1、本项目代理服务费以中标金额为计算基数，按国家发展计划委员会计价格〔2002〕1980 号文件的标准向中标供应商收取,在领取中标通知书时一次性缴纳。 2、代理服务费支付： ① 代理服务费缴纳形式：汇票/支票/电汇/现金 ② 代理服务费汇入以下账户 ： 收款单位（户名）：浙江省成套工程有限公司； 开　户：杭州联合农村商业银行三墩支行 账　号：201000065548152 **3、增值税发票开票资料：单位名称、税号（统一社会信用代码）、开户行名称、**

条款	内容规定
	账号、地址及联系电话。
8	**投标文件份数：**正本壹份、副本肆份。
9	**投标截止时间：**2019 年__月__日 09 点 30 分。
10	**投标文件递交至单位：**浙江省成套工程有限公司； **投标文件递交至地点：**杭州市古墩路 701 号紫金广场 A 座浙江省成套工程有限公司 1505 室
11	**开标时间和地点：同投标截止时间与地点**
12	**带“▲”条款系指实质性要求条款。**
13	**注：**根据浙江省财政厅文件浙财采监[2015]13 号文件《关于印发浙江省政府采购活动现场组织管理办法的通知》要求，本项目按浙江省政府采购活动现场组织管理办法实施。
14	**本项目采用资格后审制。**
15	**投标供应商应为浙江政府采购网注册供应商，如尚未注册，请登录浙江政府采购网（http://www.zjzfcg.gov.cn）进行注册。**
16	根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》财库〔2016〕125 号的规定： 1）采购人或采购代理机构将对本项目供应商的信用记录进行查询。查询渠道为信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）； 2）截止时点：提交投标文件（响应文件）截止时间前 3 年内； 3）查询记录和证据的留存：信用信息查询记录和证据以网页截图等方式留存。 4）使用规则：被列入失信被执行人、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它不符合《中华人民共和国政府采购法》第二十二条规定条件的，其投标将被拒绝。 5）本项目不允许联合体投标。
17	现场勘查：投标人可在投标截止日 1 个工作日前，到江干区数据资源管理局现场踏勘，问询相关技术要求，做出有效的投标解决方案；因部分设备存在相关兼容性要求，为保证投标商利益，建议投标商根据技术参数要求自带相关设备产品进行现场测试，所投产品与测试产品应保持一致。 采购方联系人：张军　　联系电话：86974690 地点：杭州市庆春东路 1 号（江干区政府新大楼 W117）

一、总 则

1. 项目说明

1.1 项目说明见投标须知前附表(以下称“前附表”)第 1 项所述。

1.2 采购单位杭州市江干区数据资源管理局为本项目的招标人（合同中的甲方），浙江省成套工程有限公司为招标代理机构，浙江省财政厅政府采购监管处为政府采购监督管理部门，自愿参加本次项目投标的法人、其他组织为投标人，经评审产生并经批准的投标人为中标人，签订合同后的中标人为供应商(合同中的乙方)。

1.3 投标人一旦参与本次招标活动，即被视为接受了本招标文件的所有内容，如有任何异议，均已在答疑截止时间前提出。

1.4 投标人须对所投产品、方案、技术、服务等拥有合法的占有和处置权，并对涉及项目的所有内容可能侵权行为指控负责，保证不伤害招标人的利益。在法律范围内，如果出现文字、图片、商标和技术等侵权行为而造成的纠纷和产生的一切费用，招标人概不负责，由此给招标人造成损失的，供应商应承担相应后果，并负责赔偿。供应商为执行本项目合同而提供的技术资料等归招标人所有。

2. 采购方式

公开招标。

3. 定义

3.1 合格的投标人应具备的资格要求

详细见招标文件第一部分“招标公告”。

3.2代理机构

系指采购人委托的浙江省成套工程有限公司。

3.3投标人

系指向采购人提供投标文件所叙述的服务商。

3.4 服务

系指合同规定卖方须按文件上的要求提供的服务。

3.5 货物

“货物”系指供应商按竞争性磋商文件规定须向采购人提供的一切设备、机械、仪器仪表、材料、工具、及其它有关技术资料和材料。在本竞争性磋商文件及其合同条款中也称“材料”、“设备”。

4.投标费用

投标人需自行承担涉及投标的一切费用。

二、招标文件

5、招标文件的构成

5.1　招标文件包括下列文件及附件

- 第一部分　招标公告
- 第二部分　编制和提交投标文件须知
- 第三部分　项目技术规范和服务要求
- 第四部分　合同主要条款
- 第五部分　应提交的有关格式范例

5.2　投标人应认真审阅招标文件中所有的内容，包括编制和提交投标文件须知、项目技术规范和服务要求、采购合同主要条款、应提交的有关格式范例等。如果投标人编制的投标文件没有从实质上响应招标文件的要求，其投标文件将被拒绝。

6、招标文件的澄清

6.1 供应商认为采购文件使自己的权益受到损害的，可以自收到采购文件之日（发售截止日之后收到采购文件的，以发售截止日为准）或者采购文件公告期限届满之日起 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。

6.2 投标人一旦参与本次采购活动，即被视为接受了本招标文件的所有内容，如有任何异议，均已在答疑截止时间前提出。

7、招标文件的修改

7.1　招标文件澄清、答复、修改、补充的内容为招标文件的组成部分。当招标文件与招标文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的书面文件为准。

7.2　若有必要，招标代理机构将酌情延长递交投标文件的截止日期。

8、投标报价

8.1、报价

有关本项目所需的一切费用均计入报价。《开标一览表》是报价的唯一载体。招标代理机构将不接受有选择的报价。

8.2、其它费用处理

招标文件未列明，而投标人认为必需的费用也需列入报价。

8.3　投标货币

投标文件中价格全部采用人民币报价。报价应是唯一的，不接受有选择的报价。

8.4　投标人对在合同执行中，除上述费用及招标文件规定的由中标人负责的工作范围以外需要招标人协调或提供便利的工作应当在投标文件中说明。

8.5　其他注意事项：

投标人在投标活动中提供任何虚假材料，其投标无效，并报浙江省财政厅政府采购监管处查处。

8.6 中小企业（含中型、小型、微型）指符合中小企业划分标准（工信部联企业[2011]300号），在本项目政府采购活动中提供本企业提供的服务，或者提供其他中小企业提供的服务的企业。小型、微型企业提供中型企业提供的服务的，视同为中型企业。

监狱企业视同小微企业，参加本项目投标的，享受小微企业同等的价格扣除。

三、投标文件的编制

9、投标文件的语言

投标文件及投标人与采购有关的来往通知、函件和文件均应使用中文。

10、投标文件的组成

投标文件应当包括以下主要内容：**报价文件、技术文件、商务文件。（报价文件须单独密封装订）**

10.1　投标人的**报价文件**至少应包括以下内容：

（1）投标响应函；

（2）开标一览表；

（3）报价明细清单；

（4）其他文件（中小企业声明函（或监狱企业声明函）及其相关的充分的证明材料）。

10.2　投标人的**技术文件**至少应包括以下内容：

针对本项目的技术和服务响应方案，技术偏离说明表，招标文件要求提供的其他资料等（均需加盖公章）。

⑴投标人应提供针对项目的完整技术解决方案：

针对本项目的完整技术解决方案和实施方案；详细阐述项目方案的实现思路及关键技术；符合本项目对当前和未来发展的要求；以及对功能设计和实施计划的建议；

如果本项目涉及硬件设备采购，还需提供相关设备完整配置方案（设备名称、品牌、规格型号、数量、主要技术参数等），明确表示该项指标所涉及的软硬件是标准配置还是选择配置**（所有技术指标表述均应采用中文，如当前公布的技术指标只有英文表述的，必须由投标人作出中文注释，否则任何含糊不清的表述导致评标委员会技术扣分直至认定为投标无效都将是投标人的责任）**。

⑵投标人在投标文件技术偏离说明表中，应对项目技术规范和服务要求中所提出各项要求进行答复、说明和解释。

(3)针对本项目建设的详细实施计划。本项目详细工作实施组织方案，包括(但不限于)以下内容：组织机构、工作时间进度表、工作程序和步骤、管理和协调方法、关键步骤的思路和要点。

(4)项目验收之前、验收之后的维护方案；针对本项目的维护方案，包括本地(杭州)售后服务机构及人员情况等。投标人应以书面形式完整准确地表述售后服务承诺(范围、标准及期限等)、投标人可能增加的服务承诺等。并明示服务承诺可能涉及的前提设定和费用，否则将被认为是无条件和免费的。承诺质保期内均提供免费上门服务。

(5)投标人为完成本项目组建的工作小组名单，每个专业人员的情况和人员数应该明确表示，明确各阶段投入人数，在提交的投标文件中安排的人员，须为公司的固定职员；每个参加项目人员的履历表应随投标文件一并提交，主要内容包括学历、技术职称、工作特长、经验与业绩(包括从事相关项目的经验，对每一个项目有一个简要的描述，该人员参与的时间以及在项目中的责任)，资质情况等。

（6）优惠条件及特殊承诺；

(7)备品备件清单（含随机自带的备品备件和质保期后供采购人选择的备品备件及配套零部件，明细备品备件及价格，且供货价格不高于中标价格；中标货物设备应提供易损部件的备件和整机备品）；（如果有）

（8）培训计划；（如果有）

（9）验收方案；

（10）关于对招标文件中有关条款的拒绝声明；（如果有）

（11）投标人认为需要的其他技术文件或说明。

10.3 投标人的**商务文件**至少应包括以下内容：

1）法定代表人授权书(格式见附件)；

2）提供有效的营业执照复印件并加盖公司公章；事业单位的，则提供有效的《事业单位法人证书》副本复印件并加盖单位公章；自然人的，则提供有效的身份证复印件并签字；

3）企业资质证书

4）投标人单位情况表；

5）声明书 (格式见附件，含重大违法记录声明)；

6）提供自招标公告发布之日起至响应截止日内任意时间的“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）投标人信用查询网页截图。（以招标当日采购人或由采购人委托的评标委员会核实的查询结果为准）

7）提供采购公告中符合投标人特定条件要求的有效的其他资质复印件并加盖公司公章及需要说明的资料。

8）代理服务费支付承诺书。

注：法定代表人授权委托书、声明书、报价明细表必须按招标文件格式要求正确签署并加盖投标人公章。投标文件中所需的各种证书、证件、证明资料如是复印件，需在复印件上加盖有效公章，原件备查。投标人的投标文件必须按照招标文件要求制作。

11、投标有效期

11.1 投标文件合格投递后，自投标截止日期起，至前附表所列的日期内有效。

11.2 在原定投标有效期之前，如果出现特殊情况，招标代理机构可以以书面形式通知投标人延长投标有效期。

12、投标保证金

不收取。

13、投标文件的编制和签署

13.1 投标人按本须知规定的语言和前附表规定的份数编制投标文件，并在封面上标明“正本”和“副本”。投标文件正本和副本如有不一致之处，以正本为准。

13.2 投标文件正本和副本均应使用不褪色的材料书写或打印，开标一览表必须加盖法人单位公章，按要求由法定（授权）代表人签字。

13.3 全套投标文件应无涂改和行间插字。如有修改，所修改处应由法定代表人或授权代表人签字予以确认。

四、投标文件的递交

14、投标文件的密封与标志

14.1 **投标文件分正本和副本，其中报价文件、技术文件及商务文件分别胶装并分别密封包装。没有密封包装的投标文件，将被当场拒绝。<u>如因包装问题导致报价信息在开标时发生泄漏，由供应商自行承担相关责任。</u>**

14.2 **包装封面物的正面应写明投标文件名称（商务文件、技术文件、报价文件）、项目名称、投标人全称与地址、邮政编码，封口处要密封并加盖投标人公章(或授权代表签章)。不论投标人中标与否，投标文件均不退回。**

14.3 **投标文件递交至前附表所述的单位和地址。**

15、投标截止期

15.1 投标人应按前附表规定的时间、地点将投标文件递交给招标代理机构，招标代理机构将拒绝接受逾期送达的投标文件。

15.2 招标代理机构可以按本须知规定以补充通知的方式，酌情延长递交投标文件的截止日期。在上述情况下，招标代理机构与投标人以前在投标截止期方面的全部权利、责任和

义务，将适用于延长至新的投标截止期。

16、投标文件的修改

16.1　投标人递交投标文件以后，在规定的投标截止时间之前，可以书面形式对投标文件进行补充、修改，修改文件须加盖单位公章，并由法定（授权）代表人签字盖章，在投标截止时间以后，不能修改、补充投标文件。

16.2　投标人的修改文件，应按本须知规定编制、密封、标志和递交，如果一份投标文件有几份函件时，应注明哪一份有效，否则所作修改视为无效。

16.3　在投标截止日期与招标文件中规定的有效期终止日之间的这段时间内，投标人不能撤回投标文件。

五、开 标

17、开标

17.1　招标代理机构将在规定的时间和地点进行开标，各投标人法定代表人或授权代表准时参加，携带本人有效证件及授权委托书，投标文件中要求提供授权委托书和个人身份有效证件（复印件加盖公章）。投标人如不参加开标大会的，事后不得对招标相关人员、开标过程和开标结果提出异议。投标人代表未到场签字确认或者拒绝签字确认的，不影响评标过程。

17.2　招标代理机构接收投标文件并登记，各投标人法定代表人或其授权代表对投标文件的递交记录情况进行签字确认。**对不符合装订要求的投标文件，由现场工作人员退还供应商代表。**

17.3 主持人宣布开标期间的有关事项；告知应当回避的情形，提请有关人员回避；组织供应商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》。

17.4 投标人或其当场推荐的代表，或者采购人委托的公证机构检查投标文件密封的完整性并签字确认。

17.5 招标代理机构根据各投标人递交投标文件时间，按后到先开的顺序当众拆封，宣读递交投标文件的供应商名单，清点投标文件正本、副本数量，并核对法定代表人或授权代表的身份信息。将其中密封的报价文件现场集中封存保管等候拆封，将拆封后的商务和技术文件由现场工作人员送至指定的评审地点。

17.6 商务和技术评审结束后，主持人宣告有效供应商的商务和技术得分情况，无效供应商代表可收回未拆封的报价文件并签字确认；

17.7 拆封供应商报价文件，宣读《开标一览表》有关内容，同时当场制作并打印开标记

录表，由投标人授权代表在开标记录表上签字确认（不予确认的应说明理由，否则视为无异议）。唱标结束后，现场工作人员将报价文件及开标记录表送至指定评审地点，由评标委员会对报价的合理性、准确性等进行审查核实。

六、评 标

18、评标组织

评审工作由招标人组建的评标委员会负责。评标委员会由招标人熟悉相关业务的代表，以及有关技术、经济等方面的专家组成，成员人数为五人及以上单数，其中技术、经济等方面的专家不得少于成员总数的三分之二。

19、评标原则

19.1 竞争优选；

19.2 坚持公平、公正、科学合理的原则；

19.3 价格合理，方案、产品先进可行；

19.4 反对不正当竞争。

20、投标文件审查

20.1 投标文件资格性审查：招标人依据法律法规和招标文件的规定，对投标文件中的资格证明等进行审查，以确定投标人是否具备投标资格。

20.2 投标文件符合性审查：评标委员会依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求作出响应。

21、修正原则

评标委员会对投标文件的商务报价文件进行审核，发现计算、书写等错误的，按以下原则进行修正：

（1）大写金额与小写金额不一致的，以大写金额为准；

（2）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；

（3）单价金额小数点有明显错位的，应以总价为准，并修改单价；

（4）以修正后的总价作为投标报价。

22、投标文件有下列情况之一者将视为无效：

22.1 开标时，发生下列情况之一的投标文件被视为无效：

（1）出现多个投标报价，并未说明以哪一个为准的；

（2）递交两份或多份内容不同的投标文件的；

（3）不符合法律、法规和招标文件中规定的其他实质性要求的。

22.2 在投标文件初审时，发生下列情况之一的投标文件被视为无效：

（1）投标人不满足资格要求的；

（2）投标文件无法定代表人或合法授权的委托人签署的；

（3）对投标文件的修正与澄清必须无法定代表人或合法授权的委托人签署的；

（4）投标有效期不足的；

（5）未按招标文件编制，字迹模糊不可辨，未按招标文件要求签署、盖章的；

（6）文件内容不完整，未按招标文件要求提供的商务文件、报价文件、技术文件。

（7）改变招标内容、服务内容的；

（8）技术条款重大偏离的；

（9）对“▲”条款不响应的；

（10）服务期、付款方式重大偏离的；

（11）投标人与招标人、招标机构有利害关系的；

（12）认定串标的。不同的投标人有以下行为之一的认定串标：投标文件内容存在非正常一致、错漏处一致、同一单位或者同一人编制、出现同一人员、相互混装、同一人或者同一中介机构为其提供咨询服务；

（13）不符合法律、法规和招标文件中规定的其他实质性要求的。

23、投标文件鉴定

（1）就本条款而言，实质上响应要求的投标文件，应该与招标文件的规定要求、条件、条款和规范相符，无显著差异或保留。

（2）如果投标文件实质上不响应招标文件的要求，将被视为无效，并且不允许通过修正或撤消不符合要求的差异或保留，使之成为具有响应性的投标。

（3）本项目采用资格后审制。经开标后递交至评标委员会的投标文件，仍需接受相关符合性的检查，并有可能在评标过程中被判断为无效。

24、评标办法

24.1、本项目采用综合评分法，总分为 100 分，其中商务分 6 分、技术分 64 分、价格 30 分。评标委员会将评审综合得分最高的前两名投标人作为中标侯选人向招标人推荐，得分最高的为第一中标候选人，得分次高的为第二中标候选人（得分相同时，报价低者优先；报价、得分都相同时，技术部分得分最高者优先）。

24.2、评标细则

24.2.1 商务分：6 分，评标委员会根据评审细则内容统一评审打分。

评审项目	标准分	评分内容及标准

同类项目业绩	3 分	自 2016 年以来，投标企业实施过政府部门系统集成，技术服务等项目，提供合同复印件作为证明（以签订时间为准，原件备查），每提供一个得 1.5 分，最多 3 分。（3 分）
企业资质	3 分	1.投标企业具备 AAA 级信用认证。（1 分） 2.投标企业具备 ISO9001 质量管理体系证书。（1 分） 3.投标企业具备 ISO14001 环境管理体系证书。（1 分）

相关证书须提供复印件并加盖投标人公章，证书所有者必须与投标人名称一致，否则无效。此项由评标委员会集体核实后统一打分。

24.2.2 技术分：64 分，评标委员会成员根据评审细则内容各自评审打分。如某个单项的打分超过所规定的分值范围，则该份打分表无效。投标人技术部分最后得分为所有评标委员会成员技术部分评分和的平均值。得分值小数点后保留两位，第三位四舍五入。

评审项目	标准分	评分内容及标准
投标方案的科学性和完整性	28 分	1.投标文件编制是否完整、格式规范、内容齐全、表述准确和条理清晰。（1 分） 2.投标方案与项目需求吻合采购人现状的程度，包括方案的科学性、先进性、可靠性、成熟性、经济性、合理性和扩展性；总体方案的功能实现以及设计方案配置的合理性等方面与采购人项目对应需求的满足程度等。（3 分） 3.投标人对江干区电子政务网络现状（包括设备型号、配置、运行环境、功能情况）以及问题和采购人的需求了解是否全面、详尽、准确。（3 分） 4.投标产品的可靠性及系统的技术水平、应用程度、系统结构和产品实际布局设计的先进性、科学性和合理性等是否满足采购人的需求。（4 分） 5.投标产品的知名度、销售量、市场占有率、使用现况和用户反馈情况，在同类产品中是否具有优势。（4 分） 6.投标方案与江干区政府现有设备系统的衔接、整合及统一管理方案，在保证现有资源充分利用的情况下进行高效的整合，确保原先系统的平稳运行。（6 分） 7.投标方案是否能结合采购人现状，具备完整有效的应急预案。（3 分） 8.投标方案中，结合采购人现状，对全国网站普查内容提出完整的解决方案，包括先进的检测手段，成熟的工具，详细的人工核查方案，技术培训方案。（3 分） 9.投标方案中，结合采购人现状，针对门户网站基础运维服务，提出详细渗透测试方案，给出风险评估报告，详细的服务流程。

		（1 分）
招标参数(产品技术与服务指标)符合程度	20 分	不打★的招标参数（技术与服务指标）负偏离每一项扣减 2 分，打★的招标参数（技术与服务指标）负偏离每一项扣 3 分，扣完为止。（20 分）
实施组织方案	4 分	1.实施组织方案是否能结合采购人现状，具有科学性、合理性、规范性和可操作性，包括系统集成、产品供货、验货、安装调试、试运行、测试、系统管理培训、系统运行维护培训等内容，以及组织机构、工作时间进度表、工作程序和步骤、管理和协调方法、关键步骤的思路和要点等。（2 分） 2.实施组织方案是否能结合采购人现状，具有完备的管理组织、项目实施规范和管理制度，并能有效实施。（2 分）
售后服务方案	10 分	1.具有本地化服务机构；（1 分） 2.售后服务方案是否能结合采购人现状，在完整、合理，响应时间方面满足要求；（1.5 分） 3.投标人是否能结合采购人现状，完整、科学合理地提供培训计划、地点、组织、人员配备、软硬件资料等内容是否完整、科学合理。（1.5 分） 4.投标主要设备（数据隔离网闸、数据容灾系统扩容、全区网络安全态势感知系统、数据库脱敏系统、云安全资源池、网络回溯分析系统）原厂质保期限及服务承诺是否满足采购需求，参考原厂质保服务承诺函。（6 分）
优惠措施	2 分	结合采购人现状，对江干区电子政务网络、政务云平台给出合理化的建议及具备实际意义的优惠方案。（2 分）

24.2.3 价格分 30 分，评标委员会对商务标、技术标评审结束后，对有效投标人统一打分。

商务报价评分将在有效投标人范围内进行，最高得 30 分，小数点后保留 2 位小数。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，其商务报价分为满分 30 分。其他投标人的价格分按照下列公式计算：商务报价分=(评标基准价 / 投标报价)×30。

根据浙江省财政厅浙江省中小企业局转发财政部工业和信息化部关于印发《政府采购促进中小企业发展暂行办法》的通知（浙财采监〔2012〕11 号文）及浙江省财政厅浙江省经济和信息化委员会浙江省中小企业局关于简化中小企业类别确认流程有关事项的通知（浙财采监〔2018〕2 号）规定，参加浙江省政府采购的中小企业供应商，应根据浙江省财政厅《关于开展政府采购供应商网上注册登记和诚信管理工作的通知》（浙财采监〔2010〕8 号文）

的要求，通过浙江政府采购网申请注册加入政府采购供应商库。

已注册入库且符合《政府采购促进中小企业发展暂行办法》规定的小微企业条件的，在参加浙江省政府采购活动时可享受《政府采购促进中小企业发展暂行办法》规定的优惠政策。供应商应按照浙江省财政厅浙江省中小企业局转发财政部工业和信息化部关于印发《政府采购促进中小企业发展暂行办法》的通知（浙财采监〔2012〕11 号文）规定，在商务文件中按照规定格式，提供《中小企业申明函》，并由审核单位进行核查，同时在商务文件中提供投标人注册加入政府采购供应商库的相应证明材料，才可享受价格扣除后参与评审的优惠。

本项目根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181 号）规定，对小型和微型企业的价格给予 6%的扣除，用扣除后的价格参与评审。监狱企业视同小型、微型企业。投标报价得分=(评标基准价 / (投标报价*94%))×10。

此项由评标委员会集体核实后统一打分。

24.3　投标人评标综合得分=价格分+技术分+商务分

注：以上所涉及的证明材料，需提供复印件，加盖公章，未提供的不得分，证书原件备查。报价是中标的一个重要因素，但最低报价不是中标的唯一依据。

25、评标内容的保密

25.1　公开开标后，直到宣布中标单位止，凡属于审查、澄清、评价和比较投标的所有资料，都不应向投标人或与评标无关的其他人泄露。

25.2　在投标文件的审查、澄清、评价和比较以及确定中标人过程中，投标人对招标人、招标代理机构和评标委员会施加影响的任何行为，都将导致取消资格。

26、投标文件的澄清

为了有助于投标文件的审查、评价和比较，评标委员会可以个别地要求投标人澄清其投标文件。有关澄清的要求和答复，应以书面形式进行。

27、废标

在采购中，出现下列情形之一的，应予废标：

(1)符合专业条件的供应商或者对招标文件作实质响应的供应商不足 3 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，招标人不能支付的；

(4)因重大变故，采购任务取消的。

七、定 标

28、定标

28.1　评标委员会将根据招标文件和有关规定，履行评标工作职责，以评标办法为标准，全面衡量各投标人对招标文件的响应情况。对实质上响应招标文件的投标人，以打分的方法，

排出推荐中标的投标人的先后顺序，并按顺序提出授标建议。评标结果报经招标人同意，最终确定中标人。

28.2　招标人应当根据评标委员会推荐的顺序确定中标人，不得在评标委员会推荐的中标候选人以外确定中标人。

28.3　未注册入库的供应商拟参与采购活动的，可以先获取采购文件，再补办注册登记手续，请在投标截止时间前完成注册入库。

28.4　政府采购法规、文件中另有规定的，按照相关规定执行。

八、合同签订及其他

29、中标通知书

29.1　确定中标人后，招标代理机构将在发布招标公告的网站上公布评标结果。

29.2　如中标人拒绝承担中标的项目，或提出招标方不能接受的条件，致使合同无法签订，招标方将取消其中标资格，并根据评标委员会推荐的中标候选人先后顺序，将下一顺序的中标候选人作为预中标人进行公示，或由招标方组织评标委员会复议后提出重新组织采购等建议。

29.3　在中标人签订合同并生效后，招标代理机构及时将未中标的结果通知其他投标人。

29.4　如签订合同并生效后，供应商无故拒绝或延期，除按照合同条款处罚外，列入不良行为记录一次，并给予通报。

30、合同的签订

中标人按规定的日期、时间、地点，由法定代表人或授权代表人与招标人代表签订合同。

31、付款方式

合同签订后 10 天内支付合同总价的 20%；主要设备到货后支付合同总价的 25%；项目初验通过后支付合同总价的 30%；项目验收通过后支付合同总价的 25%。

32、项目进度要求

项目内容必须在合同签订后 90 天内完成项目实施，并按照要求做好项目验收。

33、采购方式改变

在符合资格的投标人不足规定数量或投标人提供的服务及其报价、服务承诺等不能满足采购人要求，以及招标过程中出现其他不正常情况时，经批准，招标代理机构将根据《政府采购货物和服务招标投标管理办法》(财政部第 18 号令)第四十三条之规定，重新选择合适的方式进行采购。

34、质疑和投诉

根据《中华人民共和国政府采购法》和《财政部关于加强政府采购供应商投诉受理审查

工作的通知》(财库〔2007〕1 号)的规定，投标人对政府采购活动事项有疑问的，可以向招标人和招标代理机构提出询问，招标人和招标代理机构应当及时作出答复，但答复的内容不得涉及商业秘密。

35.1　供应商认为采购文件、采购过程和成交、成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向采购人、采购代理机构提出质疑。

（1）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日；

（2）对采购过程提出质疑的，为各采购程序环节结束之日；

（3）对成交结果提出质疑的，为成交结果公告期限届满之日。

35.2　采购人或者采购代理机构应当在 3 个工作日内对供应商依法提出的询问作出答复。

供应商提出的询问或者质疑超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知供应商向采购人提出。

政府采购评审专家应当配合采购人或者采购代理机构答复供应商的询问和质疑。

35.3　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管部门投诉。

35、解释权

招标文件的解释权均属于杭州市江干区数据资源管理局和浙江省成套工程有限公司。

第三部分　项目技术规范和服务要求

2019年江干区数据安全建设和政务服务保障项目需求

注：

1、**根据浙财采监字[2007]2号文件规定：除采购文件明确的品牌外，欢迎其他能满足本项目技术需求且性能与所明确品牌相当的产品参加。**

一、建设背景

根据省市2019年政府数字化转型工作任务要点，以及区委十届七次全会、2019年政府工作报告精神和我区全面深化改革的工作要求，为进一步推进我区“三化融合”工作，在区委区政府的高度重视下，我区高标谋划、积极对接、主动拥抱杭州城市大脑，着力推动政府数字化转型，提升社会治理现代化水平。

江干区已建成政务私有云和政务公有云“二云合一”的“混合云”平台，为区政府各部门提供应用服务。私有云平台为全区机关单位非涉密业务系统提供统一规范的机房运行环境、服务器存储资源、网络安全体系支撑和专业运行维护的“拎包式”入驻服务。目前，已部署有178台云主机，支撑着区政协办、区财政局等16个部门50个业务系统的运行。政务公有云平台目前已部署30台云主机，支撑着区委组织部、区人力社保局等8个部门10个业务系统的运行。政务云平台建设较好地解决了我区电子政务建设中采购周期长、部署上线慢、资源利用率低等问题，同时节省了大量的财政资金。但是，政务云平台建成后，各单位业务系统的大量集中，虚拟机资源、带宽资源集约化管理，在外部威胁和攻击手段不断升级的环境下，政务云平台极易成为攻击的对象，面临的威胁十分严峻，需要不断加强安全建设保障工作。同时也需要加强全国网站普查、政务服务网保障工作等业务，并且依据省市要求对整个网络定期进行风险评估，满足网络安全的相关要求。

二、建设目标

根据网络安全等级保护2.0版本（以下简称“等保2.0”）**及省市网络及数据安全检查要求，2019年江干区数据安全建设和政务服务保障项目主要建设目标如下：**

1.建设完善、先进的预警系统，完善的运维体系，完善的数据备份、灾备体系。特别是数据灾备，应采用本地和云端备份的方式来保障数据安全，并增强敏感数据的存储加密和共享脱敏手段。

2.建立信息安全服务云平台、云安全资源池平台，在区级层面打通云平台、信息系统和数据共享平台，做好数据安全备份，加强测试提高应用软件稳定性，加强对最新技术的跟踪，为江干区智慧电子政务提供全方位的安全保障。

3.依据上级要求，做好全国网站普查保障及信息系统等保测评相关工作，做好政务服务网保障工作、政务网络及系统的风险评估等。

4.进一步做好政务网络优化工作，完善网络架构，做好政务专网整合。并对前期已过保修期的设备购买原厂商安全特征库升级及硬件维保服务，保证电子政务的顺利推进。

三、建设内容

2019年江干区数据安全建设和政务服务保障项目主要包括以下几方面的内容:

(一)系统安全与数据安全建设

1.新增3台数据隔离网闸。用于政务网与互联网数据强隔离；政务网与公安视频专网数据交换隔离；智安小区数据分发平台与政务网数据交换。

2.数据容灾系统扩容。已实时保护的系统有智慧办公、智慧治理、基层治理四平台、共享融合平台，在此基础上扩容4个应用系统授权，建议为国民经管、城市大脑江干平台、城市大脑数字驾驶舱、浙政钉晾晒台，同时扩容相应硬件资源。

3.全区网络安全态势感知平台建设。一是总体上把握我区电子政务网络的安全态势，实时了解网络安全态势和网络安全问题，开展预警通报、应急处置和网络安全综合管理工作。二是对我区电子政务网、重要信息系统进行全面监测，对云安全资源池以及网络安全设备产生的数据进行安全态势分析；三是对全区安全态势进行大屏展示。

4.数据库脱敏系统建设。对数据库敏感数据进行脱敏，针对人员、权限、客户端、主机、时间等不同维度配置脱敏策略，对待脱敏数据可以进行替换、屏蔽、数据偏移、数字随机化等方式进行脱敏处理，保护敏感信息，不被违规查询泄露，防止恶意操作和误操作，提升数据安全性。

5.数据安全监管平台建设。基于实时流数据为用户提供安全分析能力和风险告警及多维度可视化展示。具有实时流数据分析系统、交互式在线分析系统、超大规模存储查询控制系统、用户行为分析（UEBA）系统、深度感知智能引擎、大数据可视化引擎，提供大规模数据存储、高压缩比及快速检索能力、追溯取证能力以满足合规要求。

(二)政务网络安全加固及优化

1.云安全资源池建设。2018年已建设云安全资源池终端防护平台CSSP，支持南北向安全防护，东西向安全隔离，覆盖30%云主机。本期建设将覆盖70%云主机，增加安全组件包（防火墙为主。并可选VPN,行为管理，运维审计，日志安全，数据库审计，应用交付，端点管理软件等），微隔离保障满足300台虚拟机。

2.虚拟化网络回溯分析系统。在云计算环境下对虚拟计算对象进行合规测评。对虚化区域进行回溯分析，实现硬件+虚拟相结合的方式对网络进行回溯分析，确保业务不间断的运行，出现故障时能及时定位故障点并快速排除，恢复业务系统正常运行。

3.数据安全检查整改（增加安全设备相关模块）。根据2018年杭州市数据安全检查的结果及要求，一是增加漏扫Web应用扫描模块，对Web应用提供专业的漏洞检测分析、授权可扫描总数量不少于128个无限制范围IP地址；二是增加漏扫数据库扫描模块，支持对Oracle、MSSQL、MySql、DB2、Informix、Postresql、达梦、人大金仓等数据库的专业漏洞检测分析、授权可扫描总数量128个，无限制范围IP地址；三是增加WEB应用防火墙网页防篡改功能模块。

(三)全国网站普查检查、门户网站基础运维服务、政务服务网江干分站检查、信息系统与网络等保测评、政务网络漏洞检查与数据安全检查评估服务。

1.全国网站普查检查。根据全国政府网站普查常态化要求，定期对江干区门户网站进行检查，确保通过上级部门组织的安全检查工作。

2.门户网站安全运维服务。一是网站错误修复；二是网站性能优化；三是解决网站BUG；四是解决突发性宕机故障；五是敏感信息清除；六是紧急事件响应；七是普查监控，实现按国家、地方或行业网站普查指标对目标网站进行24小时自动监测；八是攻击监控，对网站实行24小时不间断实时监控，及时发现安全问题，及时通知，及时处理。

3.政务服务网江干分站检查。按照2019年国办印发的政府网站与政务新媒体检查指标对浙江省政务网江干分站的所有办事要素进行全面检查，并提供详细的错误分析报告。

4.信息系统与网络等保测评。3个重要信息系统与1个网络等保测评，主要为智慧经管、数据共享融合、城市大脑江干平台数字驾驶舱和江干区电子政务外网。

5.政务网络漏洞检查与数据安全检查评估服务。根据《中华人民共和国网络安全法》的规定和省市安全检查工作要求，对江干区政务网络及数据进行漏洞检测、风险评估，协助进行数据安全检查,政务数据安全技术检查与整改,制度检查与管理体系建设,应急演练和专项培训等。

(四)政务专网整合及提升

1.政务网络专网整合CE设备。政务网络专网整合CE设备，根据省市部门专网整合的要求，新增3层交换机5台（含光模块）。新增2台交换机（含万兆上联口及光模块）用于江干区社会治理综合服务中心部门专网整合需求。

2.汇聚交换机。我区电子政务网络以南三楼中心机房两台思科7609设备为主核心节点，各楼层办公节点通过千兆链路接入锐捷S2910交换机，再千兆汇聚至思科3750汇聚交换机接入核心设备；两台锐捷S12010交换机做为大院外单位、社区（村）以及服务器的核心设备。因大院外单位、社区（村）网络节点（约200个左右）涉及终端多，不稳定因素较多，如病毒、环路等故障会对应用服务器网络造成影响,严重时会导致服务器网络瘫痪无法访问。为了保障业务系统稳定性和可靠性，建议将大院外单位、社区（村）应用网络和服务器网络

进行分离，保证各自业务之间不互相干扰。计划新增 2 台汇聚交换机，做为大院外单位、社区（村）网络的汇聚，通过光纤接入 7609 核心交换机。

3.TAP 交换机。随着网络安全、数据安全设备的增加，增加 1 台 TAP 交换机，捕获不同网络端口的流量，将汇聚流量进行复制、镜像，分发给多台安全设备进行分析处理。

4.无线认证扩容。无线 AP 接入认证新增 128 台授权；无线用户接入认证新增 5000 个。

5.UPS 电池。更换地下室 UPS 机房 100AH UPS 电池 32 节（已使用 8 年）及相关线路整理。

(五)安全设备特征库升级及设备维保。

安全设备特征库升级，对江干区数据中心已过免费质保期的设备购买原厂维保一年，保证政务网络及数据的安全性。

四、项目建设清单

序号	名称	数量
1	数据隔离网闸	3台
2	数据容灾系统扩容	1批
3	全区网络安全态势感知平台	1套
4	数据库脱敏系统	1套
5	数据安全监管平台	1套
6	云安全资源池建设	1批
7	网络回溯分析系统（虚拟化模块扩容）	1批
8	数据安全检查整改	1套
	漏洞扫描安全模块	1套
	WAF模块	1套
9	全国网站普查检查	1年
10	门户网站基础运维服务	1年
11	政务服务网江干分站检查	1年
12	信息系统等保测评	4个
13	政务网络漏洞检查与数据安全检查评估服务	1年
14	政务网络专网整合CE设备—大楼交换机（含模块）	2台
	政务网络专网整合CE设备—接入交换机（含模块）	5台
15	汇聚交换机（含模块）	2台
16	TAP交换机	1台

17	无线认证扩容	1批
18	UPS电池	32节
19	安全设备特征库升级及数据中心设备维保	1年

五、招标参数

1、数据隔离网闸

指标项	参数要求
基本要求	数据隔离网闸 3 台 标准 2U 机架式设备,冗余双电源;内、外网各标配 6 个 10/100/1000M Base-TX 网络接口，4 个 SFP 插槽，4 个 SFP+插槽，共 20 个千兆接口，8 个万兆接口；内、外网主机系统分别具有独立的管理口、HA 口（热备口）。
	★系统吞吐量不小于 9Gbps,并发连接数不小于 60 万。
系统架构	采用“2+1”系统架构，即由两个主机系统和一个隔离交换专用硬件组成，隔离交换矩阵基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为物理断开状态。
系统要求	内、外网主机系统分别支持多操作系统引导（大于或等于三操作系统，即 A,B,备份系统），并可在 WEB 界面上直接配置启动顺序，在 A 系统发生故障时，可以随时切换到 B 系统；且支持系统备份。提供截图。
	主机系统采用具有自主知识产权的多核多线程并行操作系统平台。
系统监控	支持设备健康状态实时自我检测，如散热系统状态，并能够进行正常/异常状态指示(非液晶屏显示)，且能在异常状态下进行声音报警；设备具有液晶面板，实时显示设备工作状态及配置信息。
强制访问控制	支持基于动态令牌的双因子认证方式。
	支持 WEB 认证方式和专用客户端两种认证方式。
	可对用户的操作系统和进程进行检查，进行准入控制。
功能模块	支持文件交换、FTP 访问、数据库传输、数据库同步、邮件传输、安全浏览、安全通道、消息传输等基本功能； 支持文件交换 IPv4、IPv6 双协议栈接入。 支持文件传输长度及 MD5 校验，并支持校验失败自动重传。
	支持文件格式特征过滤，并且不依赖于文件扩展名；支持文件类型检查可扩展模式，方便用户自主增加特定文件类型，并提供工具帮助用户识别不常见文件类型。

	支持字段级数据库间的单向或双向同步（不改变用户的库结构）。支持同步库中初始数据功能；支持安全浏览模式下网页下载文件类型过滤；支持灵活的数据库冲突处理策略，当关键字数据发生冲突时可选择：覆盖/丢弃；支持数据容错处理，当数据同步失败时，用户可以查询、复位、删除未能正常传输的数据；支持数据库同步客户端的双机热备技术，为用户提供更高的冗余技术支持； 支持数据库 SQL 语句过滤功能;支持 FTP 协议命令的黑白名单控制；支持对邮件附件大小进行控制；支持附件格式过滤；邮件收发支持时段访问控制；时间段可以是一次性执行、周循环两种方式。
	支持客户端与网闸间的第三方数字证书方式的身份认证，确保只有被授权的合法用户才能运行。
病毒检测	可扩展支持病毒检测专用模块，支持自动/手动两种升级模式。
	采用高级的网关级病毒防护引擎，包括病毒检测引擎和病毒分析引擎。
入侵检测功能	★支持实时入侵检测功能，实现网络入侵特征配制方法及系统技术可设置自动阻断响应的技术，提供截图。
抗DDoS攻击	支持抗 DoS、DDoS 攻击功能。
安全管理	支持 HTTPS 的 Web 方式管理，实现远程管理信息加密传输； 支持配置文件以加密的方式导出。
防暴力破坏限制	支持系统防爆处理，对管理员登陆有密码次数限制，密码输入错误，超过限定次数，自动锁定设备，阻止非法管理员再次登录。根据限定期限，可自动解除锁定。
高可用性	通过独立的热备端口实现双机热备；支持抢占模式。
	支持配置同步；支持与多台网闸实现负载均衡，无需第三方软硬件支持。支持主、备状态实时展示。
日志审计	支持全中文日志显示，并能实现内外网主机日志同步； 日志实现按功能模块分组管理； 实现对日志的浏览、查询、导出、删除等操作；支持 FTP 方式上传日志；日志支持远程存储，能为第三方提供日志格式，实现日志数据分析；支持 SysLog 标准； 支持图表实时显示网口流量、CPU 状态、内存状态信息。
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年硬件质保函。
	三年产品原厂商质保服务；三年原厂商上门 7*24 小时现场服务支持。

2、数据容灾系统扩容

指标项	参数要求

配置要求	★因原有容灾系统已经备份有大量的数据，为确保重要数据的安全性，系统扩展软硬件必须与原有系统完全兼容。
	在原系统上增加 4 个实时容灾备份客户端。本次配置一个容灾系统扩展柜，2U12 盘位。
	配置≥4 个千兆的 iSCSI 接口;最大可扩展到 16 个 FC SCSI 端口和 16 个 1/10Gb iSCSI 端口； 配置 12 块 4T 3.5 英寸 NL-SAS（7.2K），支持 2.5 英寸 SSD、SAS（10K/15K）、NL-SAS（7.2K）、SATA（7.2K），3.5 英寸 SAS（15K）、NL-SAS（7.2K）、SATA（7.2K）″，12（3.5 英寸）/24（2.5 英寸），最大可扩展至 96 块硬盘。
	3.5 英寸盘位，单台机器需支持内置 16 块 3.5 英寸磁盘及 2 块系统盘并支持硬盘混插；2.5 英寸盘位，单台机器需支持 26 个 2.5 寸硬盘并支持硬盘混插； 支持硬件级 RAID 0，1，5，6，10 等多种 RAID 方式，并且不同 RAID 方式可以并存，热插拔冗余电源和风扇。
平台安全性	一体化数据存储备份系统完全基于 Linux 平台开发，嵌入式备份平台，安全可靠。
存储架构	支持以旁路方式快速部署，同时支持IP-SAN、FC-SAN存储组网，支持1Gb/10Gb IP-SAN、4Gb/8Gb FC-SAN。
实时保护	支持实体机、虚拟机的操作系统、数据库、应用及文件的一体实时保护；
	支持基于磁盘和卷的实时镜像保护，并且支持全盘复制与增量复制；
	支持>2TB的GPT卷、盘复制以及Windows NTFS卷精简复制；
	★支持VMWARE虚拟机一键备份（包括无代理和有代理的方式），将数据通过存储网络备份到磁盘备份存储中,对VMWare备份可同时实现异步增量备份和同步镜像备份；
	可同时备份Linux, Windows, AIX平台服务器中的多个数据库，如Oracle和DB2同时部署在一台AIX服务器中的情况；
CDP功能	块级CDP保护，基于数据块为系统及数据提供持续保护。可定制CDP策略，设定持续保护粒度，生产中心、容灾中心可独立设置CDP策略。
	支持CDP一致性组，提供磁盘或卷的一致性组保护功能：可以将涉及某个特定应用程序的所有LUN绑定到同一个一致性卷组中，基于同一策略进行保护，以确保所有LUN的快照点回滚保持一致，保证应用程序的有效恢复。
	支持分钟级、秒级增量快照，最大支持上亿个连续保护点，确保业务的连续运行。可根据时间段来恢复数据或直接读取数据。支持任意CDP快照点删除，可按策略对CDP快照点进行合并。
	支持CDP备份硬盘的分层功能，提升CDP备份系统的整体性能。
快速恢复	支持Windows、Linux系统、VMware虚机5分钟应急恢复，当服务器故障或宕机时，可一键恢复至容灾一体机或VMware虚拟机，或通过

	SANboot在备用实体机上快速恢复。
	支持数据2分钟快速找回，当生产数据出现丢失或损坏时，可以直接使用历史快照点数据快速恢复，无须还原恢复即刻使用，大大降低了业务停顿时间。
	支持卷、磁盘的快速应急恢复，支持P2P、P2V、V2V、V2P恢复，支持SAN BOOT和Live CD两种裸设备恢复方式。
远程容灾	支持基于IP的远程复制容灾，支持系统级、数据级别的远程复制容灾。
	支持数据复制链路的负载均衡，支持备份带宽限速；支持远程数据压缩加密。
	支持本地数据中心和容灾中心的scale-out，即支持容灾级别一对一、一对多与多对一的同步与异步复制，支持断点续传。
兼容性	支持对WINDOWS/LINUX/UNIX服务器系统进行实时保护和快速恢复。
	支持VMWare、Hyper-V、KVM、XEN实时备份，支持对VMWare虚拟机进行无代理备份，支持虚机数据块修改跟踪技术，支持虚机增量备份。
	支持Oracle、SQL Server、Exchange、Mysql DB2等主流数据库及应用。
设备管理	具有C/S管理方式，全中文GUI管理界面，通过同一个控制台界面即可集中管理所有功能，包括存储资源、备份计划、恢复操作等。
	提供卷、磁盘性能监控及容灾速率监控。
	支持不同权限的用户登录管理。
知识产权	厂家拥有完全自主知识产权，能提供可持续更新升级服务。
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年硬件质保函。
	三年产品原厂商质保服务;三年原厂商上门7*24小时现场服务支持。

3、全区网络安全态势感知平台

指标项	参数要求
安全态势感知平台	态势感知平台一套，含主机1台及探针1台
性能配置	主机：标准机架结构，设备接口：6个千兆电口，CPU：4核，物理内存≥32G，系统盘≥128G SSD盘，硬盘容量≥14.4TB。
兼容性要求	★产品支持兼容客户已有的的负载均衡及行为管理日志的采集与分析，提供证明材料。
资产识别与管理	支持自动识别资产，在不影响内部网络的前提下，通过主动发送微量包的扫描方式探测潜在的服务器以及学习服务器的基础信息，如：操作系统、开放的端口号等。
	支持自动识别已知服务器，通过被动检测机制，对经过探针的流量进行分析，识别已知服务器对外提供的所有服务、已开放端口及端口传输的协议/应用等。
脆弱性感知	支持通过镜像流量检测web流量中是否存在可截获的口令信息，分

	析web业务系统是否存在明文传输情况，避免因明文传输导致信息泄露的风险。
	支持不同视角展示全网态势，包括综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势等8个独立的大屏展示功能，并支持大屏轮播。
	支持基于流量实时漏洞功能，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、目录遍历漏洞、OpenLDAP等操作系统、数据库、Web应用等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。
高级威胁检测	具备僵尸网络识别能力，行为规则近40万条，并能够与CNCERT、VIRUSTOTAL等国内外权威机构共享威胁情报。
	支持DNSFlow分析引擎，利用机器学习算法结合威胁情报，能够从大量的样本中进行学习，总结其伪装的规律，从而发现伪装的恶意DNS协议。
	支持SMBFlow分析引擎，利用机器学习技术,发现主机传输可疑文件、恶意软件行为、文件或关键目录的可疑操作行为以及SMB暴力破解等。
	支持NetFlow分析引擎，利用UEBA方式来检测服务器外发异常，包括是否正在进行DoS攻击、网络内部的横向探测：如IP扫描、端口扫描、数据收集（如到其他服务器下载）或数据传输。
外联威胁检测	支持检测主机与C&C服务器通信行为，支持区分国内外区域。
	支持检测从未知站点下载可执行文件、访问恶意链接、使用IRC协议进行通信、浏览最近30天注册域名、下载文件格式与实际文件不符、基于行为检测的木马远控、比特币挖矿等可疑访问行为，支持区分国内外区域和显示可疑行为访问趋势。
	支持检测隧道、Tor暗网通信、端口反弹等对外通信方式，支持区分国内外区域。
	支持检测违规访问策略黑名单或违反了白名单，或者违反了下一代防火墙中的应用控制策略的行为。
	支持检测服务器对外发起的远程登录、远程桌面、数据库等风险应用访问。
	支持检测主机对外发起的攻击行为。
基础检测能力	支持记录用户网络当中南北向和东西向的访问信息，包括时间、五元组、具体应用、归属地、访问次数、流量大小等各类实时信息。
	支持识别应用类型超过1100种，应用识别规则总数超过3000条。
	支持自动识别所有访问关系，并能够将访问请求进行归类：正常访问、风险访问、违规访问等。
	依托于大数据检索能力，提供详细的日志查询功能，便于事后取证。
	支持对服务器、客户端的各种应用发起的漏洞攻击进行检测，包括20种攻击类型共9000+以上规则。

	支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP等）和数据库软件（MySQL、Oracle、MSSQL等）的口令暴力破解检测功能。
	支持检测针对WEB应用的攻击，如SQL注入、XSS、系统命令等注入型攻击。 支持跨站请求伪造CSRF攻击检测。 支持对ASP,PHP,JSP等主流脚本语言编写的webshell后门脚本上传的检测。 支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等的检测。
	要求具备独立的Web应用检测规则库，Web应用检测规则总数在3000条以上。
威胁感知监控	支持图形化大屏的横向威胁大屏展示，包括但不限于横向威胁趋势，威胁类型分布、被访问业务TOP5、攻击源TOP5、违规访问源TOP5、可疑访问源TOP5、风险访问源TOP5。
	支持以图形化大屏的服务器与漏洞实时态势，包括但不限于漏洞等级分布、TOP5漏洞、服务器操作系统分布、影响服务器的数量、被访问服务器TOP5、实时漏洞发现更新、业务对外开放TOP5端口。
	支持以图形化大屏的方式展示业务外连的实时动态地图，包括但不限于外连业务风险TOP10、外连态势、外连地址TOP10、最新事件等，支持国际、国内地图自主切换。
	支持以图形化大屏实时展示全网安全事件与网络攻击态势，包括但不限于攻击事件、攻击源、危害级别等进行统计与展示。
	支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机攻击了谁，被谁攻击了，帮助管理人员及时了解威胁的影响，并制定有效的处置动作。
	支持对风险业务、风险用户进行详细举证，详细举证为什么评判该主机为失陷级，并针对每个举证的安全事件进行详细的描述，如具体事件、该事件带来的危害、如何进行处置。
	支持基于威胁活动链的形式展现主机的安全状况，能够直观地展示主机正处于被黑客入侵的哪个阶段，是否已经被利用、以及威胁的程度。
	支持基于用户/业务维度的访问关系梳理，可呈现该用户/业务已经通过哪些应用、协议和端口访问了哪些业务，这些访问是否是攻击、违规、远程登陆等行为，IT人员可清晰的看出已对哪些业务存在影响，也能推导当前用户是否已失陷（或可疑）。
报表与日志管理	支持 TB级数据秒级查询。 支持检索接入设备传输过来的所有安全日志，可基于时间、攻击类型、严重等级等选择项进行组合查询，可基于具体设备、来源/目的所属、IP地址、特征ID、URL进行具体条件搜索；支持通过syslog等接收、存储第三方设备的日志，并提供详细的字段搜索能力。

	分析平台可对安全探针进行统一的升级管理，支持配置向导功能，通过系统检测功能，检测设备基础配置、设备资源、设备接入情况、设备流量等是否有异常，并导出上架检测报告，同时支持监控探针和各类安全组件的运行状态，包含日志传输模式、日志传输量、最近同步信息等，其中安全组件需包括上网行为管理、无线控制器、VPN、防火墙等设备。
威胁事件归档	支持对已处理威胁事件进行归档并导出，格式为excel或pdf，方便管理人员后续对已处理事件做统一分析。
探针要求	
性能指标	产品为标准1U机架式设备，需满足多核X86架构。标配4个千兆电口，2个千兆光口，并含2个高速USB2.0接口，1个RJ45串口，性能配置需满足：吞吐量≥1Gbps，并发连接数≥1,800,000，每秒新建连接数≥60,000，硬盘容量≥64G SSD盘。
基础检测功能	具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等，具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和域名记录,在特征事件触发时可以基于五元组和二元组(IP对)进行原始报文的录制。
监测识别规则库	能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上。
异常会话检测	可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内 的多场景网络异常通信行为分析能力。
深度监测能力	可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型; 支持对节点检测节点内部主机外发的异常流量进行检测; 支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为; 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解检测功能; 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测。
高级检测	支持同步DNS审计日志。
	支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。
Web应用安全检测能力	支持HTTP 1.0/1.1，HTTPS协议的安全威胁检测; 支持针对B/S架构应用抵御SQL注入、XSS、系统命令等注入型攻击; 支持跨站请求伪造CSRF攻击检测; 支持对ASP,PHP,JSP等主流脚本语言编写的webshell后门脚本上传的检测; 支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等的检测; （要求对以

	上列出的攻击类型进行逐条响应并提供相应的功能界面截图）； 产品应具备独立的Web应用检测规则库，Web应用检测规则总数在3000条以上； 支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤； 支持对被Web网站是否被挂黑链进行检测。
僵尸主机检测	支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 具备独立的僵尸主机识别特征库，恶意软件识别特征总数在40万条以上； 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告。
违规访问检测	能够针对IP，IP组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式，并对检测到的违规访问进行实时告警。
流量记录	能对网络通信行为进行还原和记录，以供进行取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为。
管理功能	可支持在线升级和离线升级，并依托安全感知平台进行统一管控； 可实时监控设备的CPU、内存、存储空间使用情况； 能够监控监听接口的实时流量情况。
集中管控	支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级。
部署	支持旁路部署，对镜像流量进行监听； 可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台；
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年硬件质保函。
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持。

4、数据库脱敏系统

指标项	参数要求
硬件指标	数据库脱敏系统1台。2U机架式设备，双电源，板载6电口，16G以上内存，2T以上存储空间，1×扩展槽位。
脱敏性能	脱敏速度:不小于20000个数据单元/秒
数据库类型	支持多种数据源，包括：Oracle、DB2、SQL Server、MySQL、PostgreSQL、Sybase、Informix、GBase 、达梦、Hive等多种数据

	库及数据仓库；
平台支持	支持Windows、Linux、AIX、Solaris等多个主流数据库应用平台。
敏感数据自动发现	系统应支持敏感信息的自动发现能力，系统具有内置敏感数据特征库，能对身份证、银行卡号、电话号码（手机、座机）、中文姓名、中文地址、企业名称、email地址、ip地址、mac地址、车牌号、车架号等敏感信息自动识别。
	系统支持按照数据字典进行敏感数据发现的能力，凡是字段中数据都在数据字典内的，则该字段被发现为敏感字段。
定时任务	系统支持定时、定期自动执行脱敏任务的功能。支持按照日期、时间对任务进行定时。
数据对比	★系统支持通过查询单表数据实现脱敏后数据对比功能。(提供截图)
快捷模式	系统支持简化配置脱敏任务方式，适合对脱敏算法按默认策略配置，让“脱敏任务一键执行”。
异构脱敏	系统支持Oracle到SQLServer、Oracle到MySQL、Oracle到DB2、DB2到Oracle、dmp到oracle的异构脱敏。
数据关联	脱敏算法保持数据关联性，能够保持同一数据库中不同表字段之间的数据关联性，也能保持不同数据库之间的表字段间的数据关联性。
字段表达式	脱敏字段能满足表内其它字段的运算关系，如表内脱敏后数值字段1和字段2自动求和置入字段3。(提供截图)
分组字典	对含有分类字段的数据，可以根据分类内容按指定的分类对与分类数据关联的数据内容进行替换，保证数据替换范围在相关分类内。
脏数据脱敏	对不符合敏感类型格式的数据在脱敏时进行随机算法生成脱敏数据。
用户权限管理	具备完善、统一的权限管理体系，可以针对不同用户、不同角色、不同业务系统实现数据行级的权限控制，完成用户建立、用户分配、用户身份验证等管理功能，满足系统用户所有资源信息具备最小颗粒度的可配置、可分配的能力。
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年硬件质保函。
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持。

5、数据安全监管平台

指标项	参数要求
基本要求	数据安全监管平台软件1套； 基于实时流数据为用户提供安全分析能力和风险告警及多维度可视化展示。具有实时流数据分析系统、交互式在线分析系统、超大

	规模存储查询控制系统、用户行为分析（UEBA）系统、深度感知智能引擎、大数据可视化引擎，提供大规模数据存储、高压缩比及快速检索能力、追溯取证能力以满足合规要求。
系统平台性能要求	可支持 500*个日志源资产；可支持2*GB的镜像流量；内存：64GB，磁盘：4T*4 raid5；EPS：10000/秒 （峰值：14000/秒）
探针性能要求	可支持4个电口，1个console口；内存：64GB，磁盘：4T*4 raid5；EPS：10000/秒 （峰值：14000/秒）；双电源、非CF卡启动
安全监管服务要求	基础设施安全监测与评估服务要求： 1.安全服务团队专家利用安全监管监测平台对江干区政务外网内接入或已在线的服务器、系统、网络及安全设施的情况进行综合扫描与评估，评估内容包括系统的脆弱性、系统的可用性等。 2.安全服务团队里利用监管平台将江干区政务网内重要信息系统进行归类根据业务系统的类型、资产特性、风险等级等情况进行分类，并借助平台相关工具形成可视化的展现，方便各级用户进行整体安全把控。 3.对江干区政务网内的安全日志与流量情况进行综合分析，并将结果按照资产类型、事件等级、事件分布情况等进行整合与梳理，并将结果通过可视化的方式进行展示，并根据安全分析情况形成专家建议。 4.对江干区政务云、政务网等关键基础设施的安全评估情况形成评估报告，并通过可视化的方式对评估结果进行展示。 5.服务团队借助监管平台通过对江干区政务应用的不间断监测服务，实行网站漏洞监测、网页木马监测、篡改检测、可用性监测与关键字监测，提供详尽的数据与分析报告。
	安全通报与预警服务要求： 1.监管人员利用平台选择特定的用户或组织进行下发预警，预制好预警级别、标签等。针对未通报的事件，将根据事件信息，利用监管监测平台配置好的日常通报模板生成通报文件。 2.利用监管监测平台提供全局维度的安全分析通报，按照预警名称的维度对公开预警进行查询的功能，并可根据指定的查询条件，快速定位需要重点关注的公开预警。 3.监管人员通过平台提供的工单管理视图，并将工单指派给相应的处理人，经过各个环节的处理，工单记录状态未处理/处理中/已解决/已关闭，便于监督工单是否及时处理以及闭环。
	安全监管数据分析服务： 1.运用大数据的技术，汇总用户相关的历史、档案、行为得出个体和群体在一个长期时间范围内稳定的数据特征，从而描绘出用户的信息全貌。发现内部人员违规操作、越权使用等违规行为时，可以发起专项预警，对特定对象发送预警信息。 2.通过实体间网络关系的多级钻取，通过端口、协议、异常访问类型等进行综合分析过滤关联关系。

	3.在安全漏洞通报之后借助监管平台动对漏洞信息进行跟踪，周期性的检测漏洞是否被修复，且跟踪状态实时显示在平台上方便用户进行及时的查看。对于所有通报的安全漏洞和安全事件的状态进行跟踪记录，直至问题被完全修复。 4.对用户的各类日志进行综合审计分析，并以图表的形势展现在线服务的业务访问情况。通过对访问记录的深度分析，发掘出潜在的威胁，起到追根索源的目的，并且记录服务器返回的内容，便于取证式分析，以及作为事件的取证材料。 5.利用监管平台实现对核心应用系统的访问行为、连接行为、攻击行为以及应用系统性能进行审计分析，及时发现异常行为。 6.对终端用户的行为审计功能，主要包括终端的访问时间审计、访问地点审计、访问的应用系统审计、访问频率审计等。结合用户画像和资产画像，及时发现异常的终端行为。 7.对数据库的操作对象进行安全分析，分析对象包括对数据的访问用户包括远程应用访问用户等，对数据的恶意操作、删除、篡改等高风险操作行为进行安全分析和告警； 8.可以采集江干区政务网内目标系统的指纹信息，形成江干区专有的基础指纹信息库，当有重大安全事件或者0day漏洞爆发时，根据指纹匹配对用户进行快速的初步预警，并由监管服务人员利用监管平台及时通报相关情况。 9.对采集工具采集到的安全风险数据、攻击事件数据、安全状态数据、行为分析数据、审计和主机日志等内部安全数据，结合基于外部的各种攻防动态、攻击样本、黑客组织等情报数据，并通过完善的关联分析和数据挖掘方法去发现安全隐患与风险，并及时发布相关预警。
服务工具功能要求	可视化工具要求： 1.支持基于实时收集的安全日志和事件数据定义安全指标。 2.支持利用数据中的源地址、源端口、目的地址、目的端口、传输层协议、应用层协议等不少于50个字段进行指标过滤和分组。（提供截图） 3、指标算子包括求和、最大值、最小值、平均值等不少于6种。 4、支持利用安全指标数据建立不少于18种可视化图表以及通过可视化图表拖拽组装成不少于7种的仪表盘。
	安全分析工具要求： 1、支持自定义选择安全指标和AI机器学习算法部署AI训练模型。 2、多算法训练结果支持可视化对比分析。 3、支持异常事件的自动标注并基于事件的特征值和举证信息辅助用户发现潜在的安全风险。
	监管模型工具要求： 模型可通过串并联方式组合编排，前一个模型的输出可以作为后一个模型的输入，支持分析模型编排层级>10层（提供截图）。

	算法工具要求： 支持时间序列、UEBA、Bayes、随机森林等长周期高级机器学习算法； 平台内置不少于8种机器学习分析场景模型，可检测发现勒索挖矿告警数异常、安全设备日志数异常、网络会话数异常和域名请求数异常等特定场景条件下的安全态势异常。
服务人员要求	提供现场服务的人员需要具有专业的大数据安全分析团队和云安全团队，需提供至少3人由中国信息安全测评中心认证CISP-BDSA（大数据安全分析师）或由中国信息安全测评中心认证的CISP-CSE（云安全工程师）资质证书。（中标后合同签订前提供）。
服务保障	服务期限：1年

6、云安全资源池建设

指标项	参数要求
兼容要求	★本次招标产品和业主方之前的云安全服务平台可以无缝对接，云安全中的防火墙，行为管理，主机杀毒等组件可以联动。 产品为软件形态，支持部署于通用X86服务器平台，无需绑定底层操作系统即可搭建；
基本要求	1）平台具备安全接入（SSL VPN）、安全防护（访问控制、内容安全、入侵防御、Web应用防护、网站篡改防护、虚拟主机安全防护）、安全检测（僵尸网络检测、实时漏洞分析、Websheel检测、网站黑链发现）、安全审计（数据库审计、堡垒机、日志审计、上网审计）、安全应用（漏洞扫描、负载均衡）、终端响应与检测、安全运营等安全功能。 本次需提供8个安全组件的授权。 单个组件性能要求如下： 防火墙组件，吞吐量≥1000M，2个; 日志审计组件：主机授权≥200，1个 安全组件包：总数为5个组件授权，可灵活配置，各组件性能如下： 1、VPN组件(含20 SSL授权和20 Ipsec授权) 2、数据库审计组件（应用层吞吐200M／400M／600M） 3、应用交付组件（应用层吞吐200M／500M／1000M） 4、防火墙组件（应用层吞吐200M／500M） 5、上网行为管理组件（应用层吞吐200M／500M／1000M） 6、微隔离组件（含300端授权）
	具备独立可视化界面，具备面向安全合规的安全服务组合套餐，至少包含基础合规套餐与增强合规套餐，业务系统可自行选择匹配的合规套餐。

	安全资源运行状态、安全状态，租户可配置：当前所购买的安全资源，如VPN、下一代防火墙、数据库审计等安全功能的策略管控。平台支持关键安全组件双机功能保障安全组件高可用。
平台架构基本要求	★云安全服务平台底层基于架构，平台中计算资源、存储资源、网络资源、网络功能资源、安全功能等IT基础资源必须虚拟化，其中安全功能中必须具备虚拟VPN、虚拟应用负载均衡、虚拟下一代防火墙、虚拟数据库审计、网页防篡改、虚拟上网行为审计、主机杀毒等功能组件，且均为同一厂商品牌提供，保障平台的扩展性和兼容性；
部署方式	无需安装任何其他软件和专用设备硬件，采用基于X86服务器即可完成平台部署，采用旁路部署模式。
交付形态	资源池必须具备安全需求弹性扩展，安全灵活部署，按需交付。安全功能以基于不同安全需求以安全服务包的形式交付。
服务方式	1）平台必须支持租户与云平台管理方独立可视化界面。 2）租户界面必须支持安全组件自运维功能；支持在首页展示安全应用状态，以及业务遭受的入侵风险、僵尸主机风险及外发流量异常等相关安全信息； 3）平台侧界面必须支持安全组件分配功能，管理员可直接为各个租户分配安全资源。
系统管理	1）平台可根据实际业务环境定义业务安全区域，简化运维管理； 2）在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备。 3）支持应用的开关机操作，并支持迁移组件的运行位置与存储位置； 4）支持租户安全资源的服务链配置，通过灵活选择源、安全服务节点和目的，完成安全路径的自定义，安全服务节点的先后顺序可灵活调整。
性能优化	1）支持数据写入优化机制，将高速SSD作为写缓存，数据先写到SSD，再回写到机械硬盘，提升写IO性能。 2）支持配置内存回收机制，实现虚拟化平台内存资源的动态复用，保障虚拟机的性能。 3）支持通过SR-IOV技术对平台底层驱动进行优化，提升虚拟网卡和安全组件的性能。 4）支持通过任务队列框架，实现多任务并发处理，减少应用部署时间。用户可通过任务列表实时查看任务进度，优化客户体验。
可靠性	支持虚拟机卡死及蓝屏的检测功能并实现自动重启，无需人工干预减少运维工作量； 平台可以通过设置敏感时间度对集群服务器基础资源根据资源负载状态动态调度不同集群服务器的CPU、内存等资源；

	支持虚拟安全组件的HA功能。当物理服务器发生故障时，该物理服务器上的所有虚拟安全组件，可以在集群之内的其它物理服务器上重新启动，保障业务连续性； 支持对云安全服务平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态。
下一代防火墙功能要求	对虚拟防火墙分布式策略管控，策略内容可以针对IP、MAC地址或通讯端口，可防护所有基于IP五元组（TCP、 UDP、 ICMP 等）；
	支持静态路由，ECMP等价路由，支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议，支持多播路由协议，支持路由异常告警功能；
	提供基本的安全防御，包括但不限于4-7层访问控制、入侵防御、病毒过滤、网页防篡改等安全功能；
	对所有应用系统进行漏洞的攻击防护，包括防跨站、防SQL注入、防篡改、防木马、防黑客攻击等。
	支持根据国家/地区来进行地域访问控制；
	支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞；
	可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；
	支持生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证；
SSL VPN功能要求	支持对基于HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH等的所有B/S、C/S应用系统，支持基于TCP、UDP、ICMP等IP层以上的协议的应用，例如即时通讯、视频、语音、Ping等服务；
	支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows XP、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；
	支持用户登录界面、服务界面的完全自定义，上传单独的Web页面作为用户登录界面、服务界面；
	支持单点登录功能（SSO）,支持移动用户登录VPN后再登录内部B/S、C/S应用系统时不需要二次重复认证；
	提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作。
上网行为管理功能要求	支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限；
	支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如

	检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等；
	必须支持以USB-Key方式验证接入数据中心的管理员身份； 支持以USB-Key方式分配管理员的日志审计权限；
	支持把每一个外网IP作为通道内的用户，使得通道的用户间公平分配带宽，以及单用户最高带宽属性对外网IP有效；
	支持基于访问行为的目标IP/IP组实现带宽划分与分配；
	支持多种事件进行邮件告警，包括攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等；
数据库审计功能要求	采用B/S管理方式，无需在被审计系统上安装任何代理；
	支持多种数据库类型的审计，支持Oracle数据库审计、SQL-Server数据库审计、DB2数据库审计、MySQL数据库审计、Informix数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql数据库审计、sysbase数据库审计、cache数据库；
	支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌，白名单内容包括以下4个维度:SQL模板、业务系统、URL地址及数据库条件；
	支持自动基线学习数据库语义语法，并支持提取参数自动生成SQL模板，可以减少审计日志的重复写入和节省磁盘的存储空间；
	支持基于SQL命令的webshell检测，提供webshell日志查询； 可通过查看webshell攻击的时间、源IP、业务系统、webshell规则发现威；
日志审计功能要求	系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段；
	对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义；
	系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用。
主机杀毒功能要求	支持多语言安装方式，支持远程安装控制台和客户端；
	支持基于威胁情报的病毒md5值的全网终端定位搜索，适用于对变种流行病毒的快速响应，快速确认全网终端是否感染；
	支持多级系统中心，并能够对每级系统中心及所属客户端进行统一升级、统一管理；
	支持全网统一自动升级，不需要人为干涉，支持病毒库无缝主动式智能升级，增量升级，以减少升级时带来的网络流量；

	支持多种病毒报警方式，包括发送到管理控制台、声音报警、发送邮件、显示消息框、报告给上级系统中心等；
	支持内置高风险规则，防范维护人员执行no where 删除、truncate table等合法的授权的高危操作检测；
	支持基于自动学习的访问行为基线策略； 自动学习的特征有：数据库用户、源IP、目标数据库 、源应用程序、主机名、系统用户名、表与操作、查询组、特权操作等； 行为基线支持自动更新； 支持根据业务情况生成不同阶段的基线策略； 支持偏离基线时使用的动作、风险级别可配； 支持模型特征的总量配置； 支持用户名+客户端IP绑定的形式进行特征学习（针对CS架构情况下，多个终端使用相同的数据库用户）；
	超级白名单：支持数据库连接工具白名单功能，自动忽略数据库连接工具访问数据库的默认操作；
	默认高风险规则：支持内置高风险操作特征规则，包含：清表、删表、提权；
	敏感数据防护：支持基于敏感数据发现的敏感数据提取到规则。
	SQL注入：支持基于CVE的SQL注入漏洞检测；
	缓冲区溢出检测防护：支持特征方式的缓冲区溢出检测规则；
	具备基于多维度轻量级的无特征检测技术，多引擎协同工作，包括：基于AI技术的自研引擎、基于家族基因分析的特征检测引擎、基于虚拟执行和操作系统环境仿真技术的行为引擎、基于大数据分析平台的云查引擎。
	日志查询与告警：日志内容能够详尽的显示访问行为发生的具体特征，具体信息包括：访问时间、次数、源、目标、操作类型、敏感数据判断、SQL内容、响应状态等。
	流量监控：支持实时的网络流量监控，支持实时/历史的入库日志流量监控；
	查询告警：支持以相同的规则进行告警日志汇总显示，支持以引擎的方式对进行告警日志汇总显示，支持以风险等级、匹配的策略、时间、其他操作条件对告警日志进行查询；
漏洞扫描	主机类支持：Windows、Unix、Solaris、HP-Unix、AIX、 Linux等；
	网络设备支持：华为、H3C、Cisco、Juniper、中兴等，防火墙：华为、天融信、H3C、Fortigate、Cisco、Juniper、迪普防火墙等；
	数据库支持：Mysql、DB2、Oracle、Sqlserver、Sybase等，中间件：Tomcat、IIS、Webservices、Apache、Weblogic、Resin、Nginx等，虚拟化平台：VMware ESXi、VMware Center、XenServer；

	支持扫描器登录到目标系统中对特定应用进行深入扫描；
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年硬件质保函。
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持。

7、网络回溯分析系统（虚拟化模块扩容）

指标项	参数要求
基本要求及兼容性	为了保障资产的保值性，新模块必须和现有的网络回溯分析平台无缝对接，能实现数据库级别融合。如果无法实现，应标方需重新提供和新采购模块无缝对接的流量分析平台。本项目部署虚拟化探针5个，7层分析模块1套。
支持平台	必须能够支持VMware虚拟化平台东西向流量的获取。
部署方式	★支持ovf、qcow2方式部署于Vmware、KVM宿主机，获取宿主机环境中的所有东西向流量；每个软探针支持一台宿主机，分布式部署集中管理。
探针规格	单虚拟化探针处理能力：1Gbps，250Kpps，每秒处理TCP会话：20,000笔，4TB存储许可。
数据存储	支持流量报文存储为pcap格式文件，可按照VLAN、应用协议设定报文切片。
流量识别	支持VLAN、MPLS、MPLS EXP、DSCP、VxLAN、GRE、FB、PPPoE、Jumbo Frame流量识别与统计，可设定2层以上VLAN层级识别。
协议定义	支持根据客户端/服务器IP、端口，HTTP URL自定义应用协议。
会话统计	支持1秒颗粒度TCP会话指标统计：流量、速率、数据包数量、重传数量、零窗口数量、重传率、客户端延迟、服务器延迟、响应时间，且标注会话开始/持续时间。
分析维度	支持按照VLAN、IP段、应用、主机、TCP端口、UDP端口、IP对聚合会话统计指标。
建连失败分析	支持记录每笔建连失败会话，自动识别失败原因（FIN超时、RST等），并可图形化展示该会话的三次握手交互。
报文解码	支持系统中解码TCP会话，呈现客户端与服务器报文交互过程，显示单笔请求与响应耗时，并自动解码常见协议负载内容。
亚秒级分析	支持捕获接口、VLAN、IP段100ms/10ms/1ms颗粒度的流量趋势及IP对分析。
自定义视图	支持自定义分析视图，支持时序图、快照、TOP时序图、饼图等4中视图类型，用户可自定义视图的时长、对象及统计指标。
自定义拓扑	支持自定义监控拓扑，实时刷新显示节点组件的统计指标，用户可自定义显示4个统计指标。
报表	支持自动生成PDF日/周/月报，可登陆系统查看，或发送Email至用

	户。
告警	支持阈值与基线告警，可设定告警时间段，并支持syslog发送告警事件。
操作界面	B/S操作界面，支持全中文操作，支持至少20个用户并发操作。
数据接口	支持Restful、Kafka、ELK、Redis数据接口输出TCP会话、应用明细、应用/链路统计指标。
异常分析	提供异常分析，实时呈现资产被攻击与失陷的数量，支持Web攻击、SQL注入、钓鱼网站、木马病毒、僵尸网络、DGA域名、恶意网站等攻击类型分类统计，根据GoIP排序攻击来源，并支持对攻击、失陷事件的回溯与pcap取证分析。
模块化部署	可部署在流量分析系统的探针或者中控服务器上。
DDI协议分析	支持ARP请求的MAC与IP统计；支持DHCP的D.R.O.A的MAC与IP统计；支持ICMP通告返回码及IP统计；支持DNS请求类型、域名、IP地址统计。
Web协议分析	支持正则定义HTTP协议的URL匹配模型；支持HTTP的URL自动发现，并统计每笔URL请求的延迟、返回码、方法；支持正则定义HTTPS协议的域名匹配模型；支持HTTPS的域名自动发现，并统计每笔域名访问的延迟；支持导入SSL证书解码HTTPS报文为HTTP报文。
数据库分析	支持Oracle的方法、SQL语句、返回码统计，可查询高频SQL及慢SQL； 支持DB2的方法、SQL语句、返回码统计，可查询高频SQL及慢SQL； 支持MySQL的方法、SQL语句、返回码统计，可查询高频SQL及慢SQL； 支持PostgreSQL的方法、SQL语句、返回码统计，可查询高频SQL及慢SQL； 支持MongoDB的方法、SQL语句、返回码统计，可查询高频SQL及慢SQL；支持MS-SQL的方法、SQL语句、返回码统计，可查询高频SQL及慢SQL。
应用关联	支持单笔应用事务关联TCP流，并直接进行解码。
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年硬件质保函。
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持。

8、数据安全检查整改

指标项	参数要求
漏洞扫描系统应用模块	增加以下应用模块，要求与原设备完全兼容，不接受更换整体设备。 1、增加漏扫Web应用扫描模块，对Web应用提供专业的漏洞检测分

	析、授权可扫描总数量不少于128个无限制范围IP地址；
	2、增加漏扫数据库扫描模块，支持对Oracle、MSSQL、MySql、DB2、Informix、Postresql、达梦、人大金仓等数据库的专业漏洞检测分析、授权可扫描总数量128个，无限制范围IP地址。原设备为安恒漏洞扫描系统。
WEB应用防火墙网页防篡改模块	增加WEB应用防火墙网页防篡改功能模块。要求与原设备完全兼容，不接受更换整体设备。 原有设备：绿盟WEB应用防火墙；2U专用机架式硬件设备，系统硬件为全内置封闭式结构；含交流冗余电源模块，2*USB接口，1*RJ45管理口，1*RJ45串口，6*GE电口（BYPASS），1个接口扩展槽位。
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年质保函；
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持；

9、网站普查检查

指标项	参数要求
工作目标	根据2019年4月《国务院办公厅秘书局关于印发政府网站与政务新媒体检查指标、监管工作年度考核指标的通知》要求，对江干区政府网站中存在的“信息更新不及时、信息发布不准确、交流互动不回应、服务信息不实用”等突出问题进行常态化监测和人工核查，通过检查，及时发现各个网站存在的问题，指导督促对存在问题的网站进行整改，引导增强网站管理责任意识，加强日常运行维护，消除影响政府形象的问题，提升政府公信力和互联网影响力。确保江干区政府重要网站通过国办组织的抽查核查。
基本要求	列入本次网站普查的网站：江干区门户网站
	★普查方法:与国务院办公厅普查全国政府网站使用的软件功能及方法保持一致;普查指标必须与国务院办公厅关于全国政府网站普查指标体系一致。提供证明材料。
	检测深度：4级页面；常态化监测：每年7*24小时监测；人工检测：4次。
普查工作内容	开展网站普查咨询指导服务： 供应商需要提供相关咨询指导工作,组织江干区相关人员学习和掌握本次全国网站普查的具体要求、指标解释，以及普查工作重点和要点。后期针对网站自查、整改、评分等工作事项，根据实际普查检查监测情况和各单位整改情况,帮助各单位理解和掌握各阶段的工作要点和具体要求。
	建立专项咨询渠道： 网站普查过程中，每个阶段都会存在不同的问题，为了应对各单位的网站普查业务咨询需求,供应商需开通热线电话、即时通讯平台，如QQ群、电子邮箱等业务咨询渠道，由专人负责各单位的咨询答疑

	工作。
	常态化监测检查： 利用专业自动监测技术服务，7*24小时不间断对站点无法访问、网站不更新、栏目不更新、排版格式、错别字情况、错断链、附件下载、网站响应等方面进行扫描，出具数据报告或问题清单，提交至各单位联系人。
	人工核查： 针对系统自动化的不足，如无法实现对办事服务、互动回应等方面的全面性、准确性监测，以及自动化扫描结果与业务工作的核对等，需要通过人工监测的方式进行核对及其他问题的监测。 （1）监测数据的人工核实：通过人工监测对人事、统计、公告信息的实际更新情况、政策文件、规划计划等信息进行核实筛选。 （2）监测指标的全面覆盖：对系统扫描中无法覆盖到的问题进行补充，包括服务实用情况中的办事指南要素的完整性、准确性，政务咨询栏目使用情况，调查征集、互动访谈等活动开展情况。
	编制网站监测检查报告： 根据经人工核查的自动化监测检查数据，以及人工检查结果，针对江干区政府网站出具《网站监测检查报告》。
工作进度要求	1.常态化监测 由供应商对江干区政府门户网站及部门网站进行一年的常态化监测工作，提交各网站问题报告及整改建议。 2.问题整改及全面核查 组织对江干区政府门户网站进行一年四次的人工监测，提交网站问题报告及整改建议。
实施服务要求	针对本次全国政府网站普查工作国办已提供报送系统软件，为保证网站基础数据准确性，本项目所用网站检测工具软件要提取报送系统已有的网站基础数据。 1.实施经验要求 ★由于本次政府网站需要在较短时间内完成全部普查检查工作，普查工作量大、时间紧，投标商可以委托第三方服务商完成网站普查工作，第三方服务商须与上级政府网站普查服务商一致，须具有政府网站普查监测经验及案例（投标时提供合同复印件）。 2.网站普查培训服务要求 组织各单位学习和掌握本次全国网站普查的具体要求、指标解释，以及普查工作重点和要点。根据普查检查监测情况和各单位整改情况，适时开展专题性培训活动，帮助各单位理解和掌握各阶段的工作要点和具体要求。
检测工具要求	供应商须利用先进的网站监测工具软件提供自动检测服务，该软件必须具有软件著作权，以提升检测工作的效率和准确度。 具体要求如下： 1.能对网站内容进行自动检测，及时发现网站不更新、栏目不更新

	等情况； 2.要求能对检测结果数据进行维护管理； 3.对于工具无法自动检测的指标，系统支持手工录入检测结果； 4.能够自动生成检测报告。
站点无法访问	首页打不开的次数占全部监测次数的比例。
网站不更新	首页栏目信息更新情况。 如首页仅为网站栏目导航入口，则检查所有二级页面栏目信息的更新情况。
栏目不更新	1.动态、要闻、通知公告、政策文件等信息长期未更新的栏目数量； 2.网站中应更新但长期未更新的栏目数量； 3.网站中的空白栏目（有栏目无内容）数量。
严重错误	1.网站存在严重错别字及敏感信息。 2.网站存在虚假或伪造内容； 3.网站存在反动、暴力、色情等内容。
互动回应差	互动回应类栏目长期未回应的情况。
服务不实用	1、未提供办事服务。2办事指南要素缺失或不准确。
服务保障	服务期限：1年

10、门户网站基础运维服务

指标项	参数要求
基础服务	江干区门户网站建在省集约化平台，需要专业公司对门户网站进行系统性维护。包括不限于解决以下问题： 1.网站错误修复，提供网站错误修复服务的指导和支持。 2.产品性能优化，不定期对现有产品进行性能优化。 3.解决产品BUG。 4.解决突发性宕机故障。 5.敏感信息清楚，对网站上已发布的敏感信息，错误文章等进行撤稿或删除。 6.紧急事件响应，当产品出现无法使用或异常时，将立刻响应并在1小时内给出解决方案。
专员服务	定期巡检：每季度进行系统巡检，现场或远程对系统进行测试及优化，及时发现系统存在的故障或潜在的问题，确保系统安全、稳定和高效地运行。 网站错误修复：提供网站错误修复服务的指导和支持。 产品性能优化：不定期对现有产品进行性能优化。 产品BUG排除：解决产品BUG。

	宕机处理：解决突发性宕机故障。 现场服务：对于无法远程解决的故障，提供现场协助。 紧急事件响应：当产品出现无法使用或异常时，将立刻响应，并在1小时内给出解决方案。
其他服务	协助工作：当第三方软件在网站挂接时，提供必要的技术配合。 数据统计：提供数据统计信息。便于网站数据考核。 用户培训：针对业主方工作人员更换或调整等情况，提供针对性的培训。
重大节日值守	提供重大节日专人值守服务，解决重要政府会议期间出现系统无法正常访问、系统出错、宕机和网站错误等问题，并跟踪到故障处理完全结束。
集约化监控	网站集约化监测平台可实现按国家、地方或行业网站普查指标对目标网站进行24小时自动监测，平台支持多站点监测管理，监测范围涵盖信息、页面、应用和搜索引擎，通过自定义检查条件、检查时间为用户提供实时详尽的动态监测图表，并提供详细监测报告下载。辅助用户推进政府网站信息内容建设有关工作，提高政府网站信息发布、互动交流、便民服务水平，全面提升政府网站的权威性和影响力，维护政府公信力。 基于云端部署，无需额外增加安全设备，对目标网站实行24小时不间断实时监控，及时发现安全问题。同时拦截针对网站发起的Web通用攻击(如SQL注入、XSS跨站等，以多种形式图表展现检测结果，自由选择微信、短信、邮件等多种方式警告安全问题，及时通知，及时处理。
服务保障	服务期限：1年

11、政务服务网江干分站检查

指标项	参数要求
基础服务	按照2019年国办印发的政府网站与政务新媒体检查指标对浙江省政务网江干分站的所有办事要素进行全面的检查，并提供详细的错误分析报告。主要包括以下检查要求：

	1、办事指南检查：对每个办事指南检查其重点要素类别（包括事项名称、设定依据、申请条件、办理材料、办理地点、办理机构、收费标准、办理时间、联系电话、办理流程）是否缺失； 办理材料格式要求是否明确的； 是否存在表述含糊不清的情形（如“根据有关法律法规规定应提交的其他材料”等表述）； 是否存在办事指南中提到的政策文件仅有名称、未说明具体内容的。
	2、内容准确性：办事指南，信息（如咨询电话、投诉电话等）是否存在错误，或与实际办事要求不一致的。
	3、表格检查：是否存要求办事人提供申请表、申请书等表单但未提供规范表格获取渠道。
专人服务	报告咨询服务：针对上级部门检查要求，安排专人对评测报告结果提供咨询服务。
服务保障	服务期限：1年

12、信息系统等保测评

指标项	参数要求
招标内容	依照国家标准GB/T22239《信息安全等级保护基本要求》中二级的标准，对3个重要信息系统与1个网络进行等保测评。（智慧经管、数据共享融合、城市大脑江干平台数字驾驶舱和电子政务外网）等级保护测评，出具测评报告，并协助完成测评工作。
测评等级	2级
安全技术测评	物理安全、网络安全、主机系统安全、应用安全、数据安全；
安全管理测评	安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理；
测评原则	1、保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标人的行为，否则招标人有权追究投标方的责任；
	2、标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。
	3、规范性原则：测评工作过程中的文档，具有良好的规范性，便于项目的跟踪和控制。
	4、可控性原则：测评服务的进度要严格进度表的安排。
	5、整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。
	6、最小影响原则：测评工作对系统和网络的影响必须在可控范围内，测评工作不能对现有信息系统的的正常运行、业务的正常开展产生任何影响。

整体要求	1、描述本次等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。
	2、描述测评人员的组成、资质及各自职责的划分。安排有经验的测评人员进行本次等级保护测评工作。
	3、描述安全测评需要的运行环境（如场地、网络环境等）及运行环境的具体要求。
	4、本次等级保护测评实施过程中所使用到的各种工具软件由投标方提供。
	5、安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由投标方推荐，经招标人确认后由投标方提供并在测评中使用。
	6、投标方应对所有正式交付件的综合质量审查负责，指定各交付件的相关责任人，明确相关职责。
	7、投标方应提供培训服务及售后服务。
安全测评报告	1、投标方协助招标人完成信息安全等级保护测评相关工作，出具最终信息安全等级保护测评报告。该项目过程中产生的文档，归招标方所有。
	2、对本次测评系统不符合信息安全等级保护有关管理规范和技术标准的，投标方出具行之有效的整改方案并协助招标人进行整改，并完成整改项的再次测评服务。
	3、投标方协助招标人办理信息系统安全保护等级备案手续，并取得备案证书。

13、政务网络漏洞检查与数据安全检查评估服务

指标项	参数要求
(一)协助数据安全监管检查	
期限及频率	一年2次
服务范围	江干区数据资源管理局相关业务系统
服务内容	协助江干区数据资源管理局对相关业务系统开展数据安全监督检查。服务内容包括： 1、主机漏洞扫描 采用专业安全扫描工具，通过定制的扫描规则，形成安全扫描策略文档，对服务器、网络设备、安全设备等进行自动化安全扫描，人工验证扫描结果并输出安全扫描报告及修复建议。 2、Web应用漏洞扫描 采用专业Web应用扫描器，通过定制的扫描规则，形成安全扫描策

	略文档，对指定网站进行自动化安全扫描，人工验证扫描结果并输出安全扫描报告及修复建议。 3、Webshell检查 采用专业的Web后门检查工具，针对网站所有的文件进行安全扫描，发现网站上可能存在的Webshell、网页后门等恶意文件。 4、渗透测试服务 通过模拟黑客使用的工具、分析方法对网站进行安全测试，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误以及其他专项内容。 5、制度检查 检查对象包括数据安全相关的制度文件、管理办法、操作规程，包括组织架构文件、人员、资产、采购、外包、系统建设与运维、备份、应急等方面的政务数据安全管理制度，以及业务系统相关变更、运维、运行等活动开展形成的记录表单。
交付物	《数据安全检查报告》
（二）政务数据安全技术检查与整改	
期限及频率	一年2次
服务范围	江干区数据资源管理局信息系统
服务内容	对江干区数据资源管理局相关信息系统开展数据安全技术检查及整改，服务内容包括： 1、主机漏洞扫描 采用专业安全扫描工具，通过定制的扫描规则，形成安全扫描策略文档，对服务器、网络设备、安全设备等进行自动化安全扫描，人工验证扫描结果并输出安全扫描报告及修复建议。 2、Web应用漏洞扫描 采用专业Web应用扫描器，通过定制的扫描规则，形成安全扫描策略文档，对指定网站进行自动化安全扫描，人工验证扫描结果并输出安全扫描报告及修复建议。 3、Webshell检查 采用专业的Web后门检查工具，针对网站所有的文件进行安全扫描，发现网站上可能存在的Webshell、网页后门等恶意文件。 4、渗透测试服务 通过模拟黑客使用的工具、分析方法对网站进行安全测试，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误以及

	其他专项内容。 5、协助安全整改 针对安全漏洞和安全配置评估中发现的安全漏洞和配置缺陷，提供加固意见和方案，配合客户完成配置修复。
交付物	《政务数据安全技术检查与整改报告》
（三）制度检查与管理体系建设	
期限及频率	一年2次
服务范围	江干区数据资源管理局
服务内容	对江干区数据资源管理局的数据安全管理制度及落地执行情况开展全面检查。检查对象包括数据安全相关的制度文件、管理办法、操作规程，包括组织架构文件、人员、资产、采购、外包、系统建设与运维、备份、应急等方面的政务数据安全管理制度，以及业务系统相关变更、运维、运行等活动开展形成的记录表单。此外，还需协助江干区数据局完善或重新建立不符合要求的数据安全管理制度。
交付物	《制度检查报告》、《数据安全管理制度》
（四）应急演练和专项培训	
期限及频率	一年2次
服务范围	江干区数据资源管理局
服务内容	1、应急演练：根据江干区数据资源管理局信息系统实际情况，编制应急演练方案，确定演练主题，明确职责分工，搭建类似信息系统的测试环境。在测试环境以模拟攻防演练方式开展，以检验应急预案的完整性、可行性，提高安全防护意识和应急处理能力。 2、专项培训：根据网络安全发展趋势，结合江干区数据资源管理局网络安全现状，制定培训计划，明确培训内容，开展面向全区的网络安全培训。主题可包括政务数据安全、攻防技术培训、网络安全意识培训、法律法规宣贯等方面，并形成培训记录。
交付物	《应急演练方案》、《培训PPT》
整体服务时间	合同签订之日起，一年。

14、政务网络专网整合 CE 设备

按照上级要求，对专网进行整合，提供相应技术支持及相应配件。主要设备如下：

（1）大楼交换机 2 台

指标项	参数要求
基本要求	
硬件性能	单台配置如下：（单台含8个千兆单模模块，4个万兆单模模块及相应配件） 要求≥24×10GE SFP+端口，2×40GE QSFP+端口，一个扩展插槽，支持4×40GE QSFP+插卡,插拔双电源，支持交流或者直流供电；包转发率：≥720 Mpps,交换容量：≥2.56Tbps/23.04Tbps；标配双电源。
VLAN特性	支持4K个VLAN，支持Guest VLAN、Voice VLAN，支持基于MAC/协议/IP子网/策略/端口的VLAN。
IPv4路由	静态路由、RIP V1/2、ECMP、支持URPF，OSPF、IS-IS、BGP，支持VRRP，支持策略路由，支持路由策略
IPv6特性	支持ND（Neighbor Discovery），支持PMTU，支持IPv6 Ping 支持6to4 、ISATAP 、手动配置隧道，支持基于源IPv6 地址、目的IPv6 地址、四层端口、协议类型等ACL，支持MLD v1/v2 snooping
安全性	支持防止DOS、ARP攻击功能、ICMP防攻击；支持IP、MAC、端口、VLAN的组合绑定；支持端口隔离、端口安全、Sticky MAC； 支持MAC地址强制转发（MFF）；支持MAC地址学习数目限制； 支持IEEE 802.1X认证，支持单端口最大用户数限制；支持AAA认证，支持Radius、HWTACACS、NAC等多种方式；支持SSH V2.0； 支持HTTPS；支持CPU保护功能； 支持黑名单和白名单。
超级虚拟交换	支持将下联交换机纵向虚拟为一台设备管理，并支持2层Client架构
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年硬件质保函；
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持；

（2）接入交换机 5 台

指标项	参数要求
基本要求	单台配置如下：单台含6个千兆单模模块及配件 交换容量≥598G/5.98Tbps s，转发性能≥222Mpps。
端口类型	28个千兆SFP,4个复用的千兆10/100/1000Base-T以太网端口Combo,4个万兆SFP+,单子卡槽位,含1个150W交流电源)
链路层与接口功能	支持端口聚合，每个聚合组至少8个端口；支持跨设备链路聚合。

二层功能	MAC地址≥32K；支持静态、动态、黑洞MAC表项； 支持DHCP Client, DHCP Server，DHCP Relay，支持Option 82； 支持4K VLAN；支持QinQ，灵活QinQ；支持1：1，N：1 VLAN mapping； 支持端口VLAN，协议VLAN，IP子网VLAN；支持Super VLAN； 支持Voice VLAN；支持组播VLAN；支持IEEE 802.1d(STP),802.w(RSTP), 802.1s(MSTP)；支持VLAN内端口隔离； 支持Smart link；支持LLDP；支持VCT，端口环路检测；支持Jumbo ≥9K。
MEF	支持MEF9、MEF14；支持MEF2.0。
三层功能	路由表≥12K；静态路由、RIP v1/v2、OSPF、BGP，ISIS；支持IPv6 支持IPv4/IPv6双栈，IPv6 over IPv4隧道，IPv4 over IPv6隧道； 支持ND, RIPng，OSPFv3，ISISv6，BGP4+；支持策略路由； 支持路由策略；支持ECMP；支持uRPF；支持VRRP；支持BFD for OSPF，BGP，IS-IS，Static Route，VRRP。
	支持IPv6，并提供IPv6 Phase II认证,要求提供IPv6 Ready网站的链接。
组播	三层组播组数≥2048；
镜像功能	支持多个物理端口的流量镜像到一个端口；支持流镜像；支持远程端口镜像（RSPAN）。
访问控制	支持基于第二层、第三层和第四层的ACL；支持双向ACL；支持VLAN ACL和IPv6 ACL；支持IP/Port/MAC的绑定功能。
QoS	至少具备8个队列；支持SP, DWRR，SP+DWRR调度方式；支持双向端口限速，限速粒度64K；提供广播风暴抑制功能；双向流限速。
安全功能	用户分级管理和口令保护，支持防止DOS、ARP攻击功能、ICMP防攻击，支持IP、MAC、端口、VLAN的组合绑定支持端口隔离、端口安全、Sticky MAC,支持MFF ,支持黑洞MAC地址 ,支持MAC地址学习数目限制 ,支持IEEE 802.1x认证，支持单端口最大用户数限制 支持AAA认证,支持Radius、HWTACACS 等多种方式 ,支持NAC功能 ,支持SSH v2.0 ,支持HTTPS支持CPU保护功能 ,支持黑名单和白名单,支持对ND、DHCPv6、MLD 等IPv6 协议报文进行攻击溯源和惩罚 ,支持用户认证点和策略执行点分离 ,支持IPSec 对管理报文加密
可靠性	支持以太网OAM 802.3ah和802.1ag
	支持 BFD for BGP/IS-IS/OSPF/静态路由
超级虚拟交换网（SVF）	支持作为SVF Client零配置即插即用，支持自动加载Client的大包和补丁 ，支持业务一键式自动下发 ，Client支持独立运行

管理协议	支持SNMP v1/v2/v3、Telnet、RMON、SSHv2；支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；支持NQA；支持基于IPv6的管理；支持集群管理；支持SFlow； 支持带外管理以太网口。
设备维护	支持自动配置，支持NAP远程开局。
服务保障	签订合同前必须提供原厂商针对本项目的授权函，提供原厂商针对本项目的三年硬件质保函；
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持；

（3）汇聚交换机 2 台

指标项	参数要求
基本要求	单台配置如下：（单台含4个万兆模块，8个千兆模块及相应配件） 基本引擎交流组合配置(含一体化总装机箱,MCUA主控板*2,800W交流电源*2)1套
	16端口万兆以太网光接口和16端口千兆以太网光接口板(X2S,SFP+)1张
	24端口十兆/百兆/千兆以太网电接口板(FA,RJ45)1张
基本参数	交换容量≥7.68Tbps
	包转发率≥5760Mpps
	业务槽位≥6，高度≤10U
	最大槽位带宽≥320Gbps
端口密度	整机万兆端口密度≥240个
单板要求	支持40GE单板。
	整机线速万兆端口密度≥72个，支持全分布式转发
硬件要求	支持无源背板
	支持风扇1+1冗余，支持风扇模块分区管理，支持风扇自动调速，支持热拔插，单个风扇框在线更换过程中，系统仍有独立风扇框保持运行。 且同一系列、不同款型间风扇可以通用，采用非左右风道或后出风风道。
	支持颗粒化电源，支持M+N电源冗余（AC和DC均支持）,电源个数≥3，首次配置在满足主备电源的情况下，后期扩容可以新增电源模块，无需更换电源模块。
	支持标准SFP，XFP，SFP+模块（支持标准SFP，XFP）
虚拟化技术	★支持将多台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合
	支持交换网集群，不占用业务槽位，集群卡和主控物理分离，集群

	卡可单独插拔，能达到单向≥100Gbps集群带宽。 支持业务口集群,集群带宽≥480G 。
MAC	支持整机MAC地址≥512K；
VLAN	支持4K VLAN，支持1：1，N：1 VLAN mapping，支持端口VLAN，协议VLAN，IP子网VLAN；支持Super VLAN;支持Voice VLAN;支持 PVLAN或类似技术
二层功能	支持IEEE 802.1d(STP)、 802.w(RSTP)、 802.1s(MSTP)，支持VLAN内端口隔离，支持端口聚合，支持MC-LAG，支持1:1, N:1端口镜像；支持流镜像；支持远程端口镜像（RSPAN）；支持ERSPAN, 通过GRE隧道实现跨域远程镜像;支持VCT,端口环路检测,支持DHCP Client, DHCP Server，DHCP Relay；支持Option 82；
路由表项	路由转发表项≥512K，IPv6路由转发表项≥256K。
单播路由协议	支持静态路由；支持RIP V1、V2, OSPF, IS-IS，BGP；支持IP FRR 支持路由协议多实例，支持GR for OSPF/IS-IS/BGP，支持策略路由。
组播协议	支持IGMP Snooping V1,V2,V3；支持PIM-SM/DM/SSM；支持MLD V1，V2；支持IGMP Proxy；支持组播频道预览。
IPV6	支持IPV6，并提供IPV6 Phase II认证,要求提供IPV6 Ready网站的链接。支持IPv6路由协议 RIPng ISISv6 OSPFv3 BGPv4+ 支持IPv6过渡技术，IPv4/IPv6双栈、6over4隧道、4 over6隧道，支持IPv6 DHCP SERVER, IPv6 DHCP Relay, DHCP Snooping，支持IPv6 Souce Guard，IPv6 ACL规格≥64K。
MPLS	支持MPLS，支持MPLS TE，支持MPLS OAM，支持RSVP
VPN	支持MCE，支持L3VPN，支持L2VPN 包括VLL VPLS，支持GRE隧道，支持MPLS 隧道入出方向的Qos
ACL表项	ACL表项数量≥70K
访问控制	支持基于第二层、第三层和第四层的ACL，支持双向ACL；支持VLAN ACL和IPv6 ACL；支持IP/Port/MAC的绑定功能
QoS协议	支持SP, WRR,DWRR,SP+WRR, SP+DWRR调度方式；支持双向CAR； 提供广播风暴抑制功能；风暴控制支持shutdown端口或拒绝转发的安全策略下发；支持WRED；
安全性	支持DHCP Snooping trust, 防止私设DHCP服务器； 支持DHCP snooping binding table (DAI, IP source guard), 防止ARP攻击、DDOS攻击、中间人攻击；支持BPDU guard, Root guard。支持802.1X；MAC地址认证；支持硬件防火墙插卡，支持硬件IPsec VPN插卡，支持自动隔离攻击源技术。
可靠性	支持VRRP 支持BFD for VRRP，支持GR for 路由协议
	支持独立的硬件监控模块, 控制平面和监控平面物理槽位分离，支持1+1备份，能集中监控板卡、风扇、电源、环境，能调节能耗
	支持G.8032开放环或SEP、REP半环协议,可与其他厂商设备混合组

	网
	支持G.8032环网保护技术，可与其他厂商设备混合组网，要求倒换时间为≤50ms
	支持BFD/OAM，遵循协议标准，3.3ms稳定均匀发包检测，50ms内完成故障倒换,保证设备高可靠性
	支持Y.1731端到端时延的检测和监控，支持NQA测试
	支持IP 快速重路由,MPLS TE FRR,MPLS VPN FRR
增值业务	支持独立负载均衡板卡，可实现服务器负载均衡功能，支持独立防火墙插卡，支持独立IPSEC板卡
管理特性	支持SNMP V1/V2/V3、Telnet、RMON、SSHV2，支持通过命令行、中文图形化配置软件等方式进行配置和管理，支持基于Ipv6的管理，支持集群管理
流量分析	支持Sflow，支持NetStream
绿色节能	支持能效以太网功能
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年硬件质保函；
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持；

（4）TAP 交换机 1 台

指标项	参数要求
硬件性能	TAP交换机1台； 24个(16个固定千兆电口和8个千兆SFP插槽)，背板带宽：24Gbps，电源模块：冗余电源模块，支持热插拔
	★要求64-1518字节下线速无丢包；BYPASS切换时长≤50ms，网络侧时延<2us。
	应用过滤规则对性能无影响，满足数据包到达入口的顺序和转发至出口的顺序一致。
	支持link-reflect，网络侧一端down后TAP会反射状态到另一侧。
其他功能	流量采集模式：支持分光单纤部署，支持SPAN流量部署模式
	系统安全：系统采用定制化OS，关闭了非必要的功能，并对服务端口完成安全加固，应保证管理数据安全。
	网管功能：trap方式向网管系统发送trap信息； 日志功能：支持向日志服务器发送系统日志信息； 配置备份：配置信息备份；
	管理角色划分：系统角色可按需划分等级权限，系统提供身份认证；

	管理方式：支持RS232串口管理，支持web图形化管理，支持Telnet管理，并可以在命令行下配置所有过滤条件，支持对命令的复制/粘帖操作，支持设备配置的明文格式查看、导出、备份等。
	端口复用：支持按需定义设备端口输入或输出功能； 流量复制：可将捕获的网络流量进行复制并分发给不同的工具处理；
	流量汇聚并复制：可将通过不同网络端口捕获的网络流量进行汇聚，并分发给单台工具处理；可将通过不同网络端口捕获的流量进行汇聚，随后将汇聚流量进行复制，分发给多台工具处理。
	流量过滤：可根据数据流量特征，对数据包进行有效过滤，只将满足条件的流量分发给工具，过滤条件应支持L2-L4
	基于端口的流量过滤：可以基于端口配置流量过滤功能；
	流量汇聚、过滤、复制：支持将汇聚后的流量按需过滤后，复制分发给不同工具处理；
	流量汇聚、过滤、分类输出：
	可将流量按照不同的连接分别发送给不同的工具处理，保证会话完整性；
流量全复制	在不影响端口已有过滤规则流量的情况下，将未过滤流量全部复制至目的端口。
L2-L4负载均衡	要求能够将过滤后的流量，基于L2-L4层负载均衡，发送给工具处理。
过滤规则条目	单台设备支持同时启用2K以上条过滤规则条目。
端口流量统计、报表	支持端口流量计数，包括：正常数据包、错误数据包等。
允许、拒绝规则	支持允许过滤规则，支持拒绝过滤规则；支持按DSCP/TOS值配置过滤条件。
以太网类型	支持按以太网类型配置过滤条件；支持按IP分帧标志配置过滤条件；支持按TCP标志位配置过滤条件；支持按IP地址配置过滤条件。
源目的端口、协议	支持按L4层端口配置过滤条件；支持按IP协议配置过滤条件。
过滤条件拒绝	支持按指定过滤标准，将数据包丢弃；
Pass All 规则	支持不影响原输入端口过滤条件的前提下，将该输入口流量无过滤的输出至工具口；

负载均衡	流量负载均衡：设备支持复制均衡能力，设备本身支持31组负载均衡；负载均衡端口：每组负载均衡最多支持23个端口；负载均衡算法：支持按L2/L3/L4层配置负载均衡条件，支持按各个层及多层结合配置条件；负载均衡算法应用：支持按每个负载均衡组分配负载均衡算法，设备同时支持多组算法同时启用；动态均衡负载：支持端口失效后将流量分配至组内其它端口。
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年硬件质保函；
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持；

15、无线认证扩容

指标项	参数要求
基本要求	1.在原有江干区政府无线统一认证系统License基础上增加5000个终端授权许可。
	2.AC控制器许可授权：在原江干区政府2台AC上增加128个AP管理授权。
服务保障	中标后签订合同前必须提供原厂商针对本项目的三年质保函；
	三年产品原厂商质保服务；三年原厂商上门7*24小时现场服务支持；

16、UPS 电池

指标项	参数要求
基本要求	电池规格：12V100AH，数量32节。 业主方UPS供电系统中电源后备电池更新，避免安全隐患。
基本参数	1.免维护的专业设计 高可靠的专业阀控密封式设计，有效确保电池不漏（渗）液、无酸雾、不腐蚀充电时产生的气体基本被回收还原成电解液，使用时无需加水、补液和测量电解液比重； 2.超长的使用寿命 独有配方，有效抵抗极板腐蚀；卓越的大电流放电特性，可靠的快速充电性能，优越的深度放电恢复能力，确保电池的使用寿命，浮充设计寿命可达8年以上（25℃）； 3.极小的自放电电流； 优质高纯度材料，每月小于4%的自放电电流，减轻电池维护工作； 极宽的工作温度范围 可在-15℃～+40℃的温度条件下工作；电池内阻小于常规电池，可进行大电流放电；

	4.合理的安装和结构设计 采用最新国际化结构设计，安装方便，易于维护。
	同时对UPS输入输出线路进行优化，消除隐患。
售后服务	电池提供三年保修及上门技术服务。

17、安全设备特征库升级及数据中心设备维保

指标项	设备名称
安全和网络设备已过免费维护期，购买原厂商维保服务（包括安全设备特征库升级及硬件设备质保一年）	启明星辰天玥网络安全审计系统 FA3000SE-R 1套；
	启明星辰天镜配置核查系统 CVS-2700 1套；
	思福迪 LogBase-D3600 数据库审计 1套；
	安恒明鉴远程安全评估系统 DAS-RAS-H1020 1套；
	安恒明御运维审计与风险控制系统 DAS-USM260（堡垒主机）1套；
	锐捷RG-WALL 1600-B-DE高性能板卡 2块；
	绿盟WEB应用防火墙WAFNX3-P1000B 1套；
	深信服上网行为管理AC8000 1套；
	锐捷RG-PowerCache X5E广域网加速缓存1套；
	锐捷M12000-24SFP/12GT-EA24光口核心板卡2块；
	锐捷RG-S5750-24GT/8SFP-E汇聚交换机2台；
	锐捷XG-SFP-SR-MM850万兆多模模块12块；
	Mini-GBIC-LX千兆多模模块34块；
	思科10Gbase-LR 1个，思科10Gbase-SR 6个；
	锐捷RG-WS6812无线核心AC控制器1台；
	锐捷RG-EG2000GE无线综合网关1台；
	锐捷RG-SMP 2.X专业版 License-10000（3套）；
	锐捷RG-S5750C-28SFP4XS-H无线核心交换机1台；
	锐捷Mini-GBIC-SX光模块14个；
	锐捷RG-S2910C-48GT2XS-HP-E POE交换机2台。
服务要求	1、远程支持服务； 2、安全设备特征库升级，硬件保修； 3、现场技术支持：7*24*4小时； 4、备件提供与更换：7*24*4小时； 5、客户服务经理； 6、服务计划与总结； 7、关键时刻值守保障； 8、疑难问题升级机制； 9、软件版本建议与升级支持； 10、网站知识中心；

	11、在线自助培训； 注：1.“7*24”小时响应维保服务的含义指：一年365天，全天24小时向用户提供故障维护服务。 2.维保时间一年；原厂维保信息需在原厂商官方网站可查，如因原厂商原因信息无法查询需提供服务承诺函。中标后合同签订前提供原厂商售后服务承诺函。

第四部分　合同主要条款

（以最终合同为准）

甲方（招标人）：

乙方（供应商）：

鉴证方：

经_____公开招标，确立_____公司为_____项目（编号：　　）的中标单位，根据《中华人民共和国政府采购法》等法律法规和采购文件，甲、乙双方经协商，达成如下合同条款：

第一条　合同价格　　金额单位：元

序号	项目名称	单价	数量	总价	备注

注：　以上费用报价含税。总价包含所需的一切费用。

第二条　服务时间

项目内容必须在合同签订后 90 天内完成项目实施，并按照要求做好项目验收。

第三条　服务地点

江干区人民政府。

第四条　服务内容

详细见招标需求。

第五条　服务要求

详细见招标需求。

第六条　费用的支付

合同签订后 10 天内支付合同总价的 20%；主要设备到货后支付合同总价的 25%；项目初验通过后支付合同总价的 30%；项目验收通过后支付合同总价的 25%。

第七条　保密条款

在执行合同时，乙方未经甲方同意，不得将所接触到的技术或业务资料、数据用作其他用途或以任何形式泄露，否则乙方将承担由此引起的法律责任和甲方损失。甲、乙双方对所有本外包项目的有关资料，不得向第三方透露。

第八条　违约责任

乙方逾期履行合同的，自逾期之日起，向甲方每日偿付合同总价万分之二的滞纳金；乙方逾期30日不能履行合同的，应向甲方支付合同总价百分之五的违约金。甲方有权终止合同并追究乙方的违约责任。

第九条　争议的解决

本合同为政府采购之合同，本合同中所指甲方享有与见证方同等权力，在发生服务不到位等问题时，甲方有权直接向乙方索赔，签订必要的书面处理协议。如协商不成，任何一方有权在甲方所在地选择诉讼的途径解决。

第十条　合同的生效

1、合同经甲、乙双方法定代表人或受委托人签字并加盖单位公章、鉴证方加盖单位公章后生效。

2、本合同一式伍份，甲、乙双方各执贰份，鉴证方执壹份。

第十一条　相关说明

甲方（盖章）：
法定代表人
（签字）：
或受委托人
地　　址：
邮　　编：
电　　话：
传　　真：
开户银行：
帐　　号：

乙方（盖章）：
法定代表人
（签字）：
或受委托人
地　　址：
邮　　编：
电　　话：
传　　真：
开户银行：
帐　　号：

鉴证方（盖章）：
法定代表人
（签字）：
或受委托人
地　址：

签约时间：　　年　月　日

签约地点：杭州市江干区人民政府

第五部分　应提交的有关格式范例

一、投标人提交投标文件须知：

1、投标人应严格按照以下顺序填写和提交下述规定的全部格式文件以及其他有关资料，混乱的编排导致投标文件被误读或评标委员会查找不到有效文件是投标人的风险。

2、所附表格中要求回答的全部问题和/或信息都必须正面回答。

3、本声明书的签字人应保证全部声明和问题的回答是真实的和准确的。

4、评标委员会将应用投标人提交的资料作出自己的判断。

5、投标人提交的材料将在一定期限内被保密保存，但不退还。

6、全部文件应按投标人须知中规定的语言和份数提交。投标文件组成漏项或未按规定的格式编制或投标文件正、副本份数不足，内容不全或内容字迹模糊辨认不清的情况，**将有可能被评标委员会认定为投标无效。**

二、投标文件编制格式及规范要求：

报价文件、技术文件、商务文件三部分，各投标人在编制投标文件时请按照以下格式进行，并分别装订成册、密封包装。

注：报价文件不得与技术文件、商务文件包装在一起。

报价文件

目录

一、投标响应函

杭州市江干区数据资源管理局、浙江省成套工程有限公司：

_____(投标人全称)授权_____(全权代表姓名)(职务、职称)为全权代表，参加贵方组织的杭州市江干区数据资源管理局2019年江干区数据安全建设和政务服务保障项目(招标编号：　)招标的有关活动，并对此项目进行投标。为此：

1、我方同意在投标人编制和提交投标文件须知规定的开标日期起遵守本投标书中的承诺且在投标有效期满之前均具有约束力。

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

(1)具有独立承担民事责任的能力；

(2)遵守国家法律、行政法规，具有良好的信誉和商业道德；

(3)具有履行合同的能力和良好的履行合同记录；

(4)良好的资金、财务状况；

(5)提供的产品和服务符合中国政府规定的相应标准和环保标准；

(6)没有违反政府采购法规、政策的记录；

(7)没有发生重大经济纠纷和走私犯罪记录。

3、提供编制和提交投标文件须知规定的全部招标文件，包括招标文件正本1份，副本4份。具体内容为：

(1)报价文件；

(2)技术文件和商务文件；

(3)编制和提交投标文件须知要求投标人提交的全部文件；

(4)按招标文件要求提供和交付的货物和服务的投标报价详见开标一览表；

(5)保证忠实地执行双方所签订的合同，并承担合同规定的责任和义务；

(6)保证遵守招标文件中的其他有关规定。

4、我方完全理解贵方不一定要接受最低价的投标。

5、我方愿意向贵方提供任何与该项投标有关的数据、情况和服务资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

6、我方已详细审核全部招标文件，包括招标文件修改书（如有的话）、参考资料及有关附件，确认无误。我方完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

7、我方将严格遵守《中华人民共和国政府采购法》第七十七条规定，供应商有下列情

形之一的，处以采购金额5‰以上10‰以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动；有违法所得的，并处没收违法所得；情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

(1)提供虚假材料谋取中标、成交的；

(2)采取不正当手段诋毁、排挤其他供应商的；

(3)与采购人、其它供应商或者招标代理机构恶意串通的；

(4)向采购人、招标代理机构行贿或者提供其他不正当利益的；

(5)在招标采购过程中与采购人进行协商谈判的；

(6)拒绝有关部门监督检查或提供虚假情况的。

供应商有前款第(1)至(5)项情形之一的，中标、成交无效。

法定（授权）代表人（签字）：_____

投标人盖 章：

联系电话：_____传真：_____电子邮件：

联系地址：

邮政编码：_____传真号码：

日　　期：_____年____月____日

注：未按照本投标响应函要求填报的将被视为非实质性响应，从而可能导致该投标文件被拒绝。

二、开标一览表

杭州市江干区数据资源管理局、浙江省成套工程有限公司：

按你方招标文件要求，我们，本投标文件签字方，谨此向你方发出要约如下：如你方接受本投标文件，我方承诺按照如下开标一览表的价格完成编号为　的招标文件[项目名称：杭州市江干区数据资源管理局 2019 年江干区数据安全建设和政务服务保障项目]实施。

开标一览表

项目名称	投标报价
2019 年江干区数据安全建设和政务服务保障项目	（小写）
投标报价	（大写）
交货期	
质保期	

1、本投标文件及其所附文件涵盖了我方要约的全部内容。

(1)我方要约有效期为自投标截止日起 90 天；

(2)在投标有效标期内，我方受投标文件之价目表上我方要约金额的约束。

法定（或授权）代表人（签字）：

投标人名称（公章）:

日期：

三、报价明细清单

序号	项目名称	单位	采购数量	单价（元）	总价（元）
1	数据隔离网闸	3	台		
2	数据容灾系统扩容	1	批		
3	全区网络安全态势感知平台	1	套		
4	数据库脱敏系统	1	套		
5	数据安全监管平台	1	套		
6	云安全资源池建设	1	批		
7	网络回溯分析系统（虚拟化模块扩容）	1	批		
8	数据安全检查整改	1	套		
	漏洞扫描安全模块	1	套		
	WAF模块	1	套		
9	全国网站普查检查	1	年		
10	门户网站基础运维服务	1	年		
11	政务服务网江干分站检查	1	年		
12	信息系统等保测评	4	个		
13	政务网络漏洞检查与数据安全检查评估服务	1	年		
14	政务网络专网整合CE设备—大楼交换机（含模块）	2	台		
	政务网络专网整合CE设备—接入交换机（含模块）	5	台		
15	汇聚交换机（含模块）	2	台		
16	TAP交换机	1	台		
17	无线认证扩容	1	批		
18	UPS电池	32	节		
19	安全设备特征库升级及数据中心设备维保	1	年		
	……				

运输费、税收及其它费用	
合计：	大写：
	小写：

注：1、以上表格要求按服务项目报价，投标人报价应是完成本项目服务可能发生的全部费用及成交人的利润和应交纳的税金等一切费用。具体以甲方实际需求为准。

2、本表为应根据投标人拟投入本项目的人、材等成本，允许空白，投标人可以调整表格格式。

3、“投标总价”应与“商务报价一览表”中 “投标总价”一致。若不一致以商务报价一览表中的价格为准。

4、不提供此表格的可视为没有实质性响应采购文件。

5、报价应包括项目涉及的一切相关费用。

投标人名称(公章)：

法定代表人或其授权代表(签字)：

日期：　　年　月　　日

四、其他文件

中小企业声明函及其相关的充分的证明材料

中小企业声明函

【不属于中小企业的无需填写、递交】

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

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

2、本公司参加_____（采购人）的_____（项目名称）_____（标项名称）采购活动提供本企业提供服务，或者提供其他_____（请填写：中型、小型、微型）企业提供服务（制造商的中小企业声明函另附）。本条所称货物不包括使用大型企业注册商标的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人名称（盖章）：

日期：　　年　月　日

填写说明：

1）投标人为中型、小型、微型企业的提供此函；

2）中型企业不享受价格扣除，小型、微型企业的行业类别由评审专家结合投标人出具的证明材料认定；经认定不符合小型、微型企业标准的，不享受价格扣除；

3）所投标项内的产品如由多个企业制造的，在填写企业类型时，按产品生产企业中规模最大的企业类型填写；

4）投标产品制造商投标，提供投标人出具的《中小企业声明函》及其相关的充分的证明材料；代理商投标，提供投标人及产品制造商出具的《中小企业声明函》及其相关的充分的证明材料；

5）填写本表的投标人应为浙江政府采购网正式入库供应商，需提供浙江政府采购网正式入库供应商的证明材料；

6）证明材料为企业在职员工人数（提供社保缴纳凭证）、营业收入及资产总额（提供上一年度资产负债表、损益表、现金流量表或财务状况变动表）。也可提供浙江政府采购网中显示信息截图代替相关证明材料。

7)　投标人已通过浙江政府采购网申请注册并成为正式入库供应商【注：提供正式入库供应商的网站信息材料】

监狱企业声明函及其相关的充分的证明材料

监狱企业声明函

【不属于监狱企业的无需填写、递交】

本公司郑重声明，根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68 号）的规定，本公司为监狱企业。

根据上述标准，我公司属于监狱企业的理由为：_____。

本公司为参加（项目名称）（项目编号：_____）采购活动提供本企业提供服务。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（盖章）：

日期：　　年　月　日

技术文件

目 录

注：以上目录是编制投标技术文件的基本格式要求，各投标人可根据自身情况进一步细化。

一、技术解决方案

（由投标人根据采购需求及招标文件要求编制）

投标产品规格配置清单

序号	设备名称	投标品牌及型号	规格配置详细说明	数量	备注
1					
2					
3					
4					
5					

注：如果本项目涉及硬件设备采购，须在技术文件中提供此配置清单。

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　　年　月　　日

二、技术偏离说明表

名称	采购要求	投标响应	偏离	说明

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　　年　月　　日

三、组织实施方案

（由投标人根据采购需求及招标文件要求编制）

附表:项目实施进度计划表(以生效日算起)

工作日 / 内容	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	…

注：投标人可按上述时间表的格式自行编制切合实际的具体时间表。

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　　年　月　　日

四、售后服务方案

（由投标人根据采购需求及招标文件要求编制）

附表A:售后服务机构情况表（按此格式自制）

序号	机构名称	机构性质	注册地址	服务技术人员数量	联系电话

注：关于项目涉及的所有售后服务机构均在本表注明，包括投标人本单位和符合条件的第三方服务机构；

附表B：售后服务人员情况表（按此格式自制）

序号	类别	姓名	性别	年龄	学历	专业	职称	本项目中的职责	响应时间	到达现场时间
	总协调人									
	售后人员									

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　　年　月　　日

五、项目小组人员名单

（由投标人根据采购需求及招标文件要求编制）

附表A:本项目的项目经理情况表

姓名		页码	截止投标时间近3年业绩及承担的主要工作情况，曾担任项目经理的项目应列明细
性别			
年龄			
职称			
毕业时间			
所学专业			
学历			
资质证书编号			
其他资质情况			
联系电话			

注：须随表提交相应的证书复印件并注明所在投标技术文件页码。

附表B:本项目的项目小组人员情况表（按此格式自制）

序号	姓名	性别	年龄	学历（页码）	专业（页码）	职称（页码）	本项目中的职责	项目经历	参与本项目的到位情况

注：投标人可按上述的格式自行编制，须随表提交相应的证书复印件并注明所在投标技术文件页码。

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　　年　月　　日

六、优惠条件及特殊承诺

（由投标人根据采购需求自行编制）

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　年　月　日

七、备品备件及供选择的配套零部件清单

（由投标人根据采购需求自行编制）

八、培训计划

（由投标人根据采购需求自行编制）

附表：培训日程及费用

课程名称	提供的资料	持续时间	授课教师	培训对象	培训地点	课程费用
费用总计						

注解:A　课程清单按时间顺序排列，并提供以下详细资料：

●课程概要

●课程目的

●教学方式

●先决条件

●教材目录

B　按照附表A提供授课教师的简历

注：须随表提交相应的证书复印件并注明所在投标技术文件页码。

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　年　月　日

九、验收方案

（由投标人根据采购需求自行编制）

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　　年　月　　日

十、关于对招标文件中有关条款的拒绝声明

（由投标人根据采购需求自行编制）

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　　年　月　　日

十一、认为需要的其他技术文件或说明

（由投标人根据采购需求自行编制）

投标人名称（公章）：

法定代表人或其授权代表（签字）：

日期：　年　月　　日

商务文件

目录

一、法定代表人授权书

杭州市江干区数据资源管理局：

（投标人全称） 法定代表人 （法定代表人姓名） 授权本公司在职职工（授权代表姓名 、身份证号码）为合法委托代理人，参加贵单位组织的项目编号为 的 杭州市江干区数据资源管理局 2019 年江干区数据安全建设和政务服务保障项目的招标活动，全权处理采购活动中的一切事宜。

法定代表人签字（签名或印章）：

投标人全称（公章）：

日期：

附：

授权代表姓名：
职　务：
详细通讯地址：
传　真：
电　话：
邮政编码：
附身份证复印件

二、营业执照、资质证书复印件等

三、企业资质证书

四、投 标 人 单 位 情 况 表

投标人（公章）：　　填表日期：

<table>
<tr><td>单位名称</td><td colspan="2"></td><td>电 话</td><td colspan="2"></td><td>主管部门</td><td></td><td>企业负责人</td><td></td><td>职务</td></tr>
<tr><td>地　　址</td><td colspan="2"></td><td>传 真</td><td colspan="2"></td><td>企业性质</td><td></td><td>授权代表</td><td></td><td>职务</td></tr>
<tr><td>单位简历及机构</td><td colspan="5"></td><td>单位优势及特长</td><td colspan="4"></td></tr>
<tr><td rowspan="4">单位概况</td><td rowspan="2">职 工 总 数</td><td colspan="4">工程人员　　平均技术等级</td><td rowspan="4">上一年主要经济指标</td><td>指标名称</td><td></td><td>实际完成</td><td></td></tr>
<tr><td colspan="4">工程技术人员
其中：高级工程师</td><td>总产值</td><td>万元</td><td></td><td></td></tr>
<tr><td>流 动 资 金</td><td>万元</td><td rowspan="2">资金来源</td><td>自有资金</td><td>万元</td><td>实现利润</td><td>万元</td><td></td><td></td></tr>
<tr><td>固 定 资 产</td><td>原值　万元
净值　万元</td><td rowspan="2">资金性质</td><td>生产性</td><td>万元</td><td>银行贷款</td><td>万元</td><td colspan="2" rowspan="2">主要产品</td></tr>
<tr><td colspan="2"></td><td>非生产性</td><td>万元</td><td colspan="2"></td></tr>
</table>

五、声明书

致（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 XXXXXX）的响应，为此，我方就本次采购有关事项郑重声明如下：

1、我方已详细审查全部招标文件，同意招标文件的各项要求。

2、我方向贵方提交的所有投标文件、资料都是准确的和真实的。

3、若成交，我方将按投标文件规定履行合同责任和义务。

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

5、投标文件自开标日起有效期为 90 天。

6、我方参与本项目前 3 年内的经营活动中没有重大违法记录；

7、我方通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询，未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

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

法定代表人签名（或签名章）：_____ 日 期：

投标人全称（公章）：

六、供应商认为需要提供的其他文件和资料

七、代理服务费支付承诺书

代理服务费支付承诺书

致：浙江省成套工程有限公司：

我公司已认真阅读了招标文件（项目编号：ZJCT5-2019155）并在此承诺：

如中标，我公司将自中标公告发布之日起5个工作日内按招标文件规定的标准（金额）一次性向采购代理机构支付代理服务费。

承诺方（投标人）法定名称:_____（盖章）_____

法定代表人或授权委托人:_____（签字或盖章）_____

承诺方（投标人）法定地址:_____（盖章）_____

联系电话：_____　　联系传真：

承诺日期:_____年___月___日

投标文件封面

正（副）本

2019 年江干区数据安全建设和政务服务保障项目

项目编号：

（注明报价文件或商务文件或技术文件）

投

标

文

件

投标人全称：（加盖单位公章）

年　　月　　日