**温州市政府分散采购**

**招 标 文 件**

项 目 编 号: ZJDO20221008001

项 目 名 称: 网络安全框架建设

采 购 方 式：公开招标

**采购人：温州市公安局交通管理局**

**采购代理机构：浙江东瓯工程造价咨询有限公司**

**二〇二二年十一月**

# 

# 目 录

[目 录 1](#_Toc14648)

[第一部分 投标供应商须知 3](#_Toc22010)

[一、 说 明 3](#_Toc26182)

[二、 招标文件 4](#_Toc29592)

[三、 投标文件的编制 5](#_Toc31539)

[四、 投标 8](#_Toc22301)

[五、 开标和评标 10](#_Toc9951)

[六、 授予合同 13](#_Toc6669)

[投标邀请函 2](#_Toc12885)

[第二部分 合同主要条款 15](#_Toc2167)

[第三部分 附件 21](#_Toc3030)

[附件一 投 标 函 21](#_Toc2135)

[附件二 投标一览表 22](#_Toc30499)

[附件三 投标分项报价表 23](#_Toc21827)

[附件四 证明文件 24](#_Toc29963)

[（1）法定代表人授权书 24](#_Toc31276)

[（2）供应商基本情况表 25](#_Toc17553)

[（3）资格条件承诺函 26](#_Toc633)

[（4）中小企业声明函 27](#_Toc12841)

[（5）残疾人福利性单位声明函 28](#_Toc25811)

[附件五 商务、技术条款偏离表 29](#_Toc19923)

[附件六 货物成套供货清单 31](#_Toc32077)

[附件七 供应商综合实力 32](#_Toc10017)

[附件八 项目需求理解 33](#_Toc22992)

[附件九 功能及服务 34](#_Toc26224)

[附件十 人员投入 35](#_Toc29432)

[附件十一 质量保证措施 36](#_Toc5335)

[附件十二 应急方案 37](#_Toc31939)

[附件十三 巡检计划 38](#_Toc12440)

[附件十四 培训计划 39](#_Toc5564)

[附件十五 售后服务 40](#_Toc23066)

[附件十六 项目业绩 41](#_Toc4238)

[附件十七 诚信投标承诺书 42](#_Toc1463)

[第四部分 采购内容及要求 43](#_Toc13090)

[一、 项目概况 43](#_Toc16602)

[二、 安全现状 44](#_Toc24502)

[三、 具体采购内容及技术要求 47](#_Toc19786)

[四、 其他要求 77](#_Toc32647)

[第五部分 评标原则及方法 79](#_Toc11157)

[政府采购活动现场确认声明书 81](#_Toc1036)

**▲备注：招标文件中带“▲”并加下划线的内容为实质性要求或者条款；带有下划线或深色底纹的内容，为招标文件的着重提醒内容，请投标供应商审慎阅读。**

# 投标邀请函

：

浙江东瓯工程造价咨询有限公司受温州市公安局交通管理局委托就网络安全框架建设项目进行公开招标，我们诚恳地邀请贵单位参加投标，并请按招标文件的要求认真准备，按时参加投标。

1．项目编号：ZJDO20221008001

2．项目名称：网络安全框架建设

3． 采购内容：详见招标文件第四部分。

采购预算: 126.2万元；

最高限价：126.2万元。

4． 招标文件获取时间：即日起至投标文件递交截止时间为止。（未按规定时间及方式获取招标文件的潜在供应商拒绝参加投标，且其提出的质疑不予受理）

招标文件获取地点：政府采购云平台（http://zfcg.czt.zj.gov.cn）

招标文件获取方式：实行“政府采购云平台”在线申请获取，不提供招标文件纸质版。供应商获取招标文件前应先完成“政府采购云平台”账号注册，后登陆政采云平台在线申请获取招标文件（进入“项目采购”应用，在获取招标文件菜单中选择项目，申请获取招标文件）

5. 投标文件递交截止时间：2022年11月24日09:30分整；

递交地点：通过“政府采购云平台（www.zcygov.cn）”在线投标。

6． 开标时间：2022年11月24日09:30分整；

开标地点：通过“政府采购云平台（www.zcygov.cn）”在线开标。

评标地点：浙江东瓯工程造价咨询有限公司会议室（温州市鹿城区隔岸路68号2楼）。

7． 采 购 人：温州市公安局交通管理局

联 系 人：章华栾

电 话：0577-56557283

1. 采购代理机构：浙江东瓯工程造价咨询有限公司

地 点：温州市鹿城区隔岸路68号2楼

联 系 人：金凯伦

手 机：15088555258

电 话 ：0577-88521066

同级政府采购监管部门：温州市财政局政府采购监管处

联 系 人：项先生、蔡女士

联系电话：0577-88532725、88521948

温州市公安局交通管理局

浙江东瓯工程造价咨询有限公司

2022年11月03日

# 第一部分 投标供应商须知

## 一、 说 明

1． 本次招标是根据《中华人民共和国政府采购法》、《采购法实施条例》、《政府采购货物和服务招标投标管理办法》、《浙江省政府采购项目电子交易管理暂行办法》等有关法律法规组织和实施。

**2． ▲合格投标供应商**

**2.1 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；**

**2.2 本项目谢绝联合体投标；**

**3. 投标供应商代表**

3.1 指全权代表投标供应商参加投标活动并签署投标文件的人。投标供应商代表可以是法定代表人（事业单位为法定负责人，下同）或其有效授权的本单位人员，▲**如果投标供应商代表不是法定代表人，须持有《法定代表人授权书》（见附件统一格式）、授权代表有效身份证件，否则授权代表身份不予认可，投标无效。**

**4. 投标费用**

4.1 投标供应商应承担所有与准备和参加投标有关费用，不论投标的结果如何，采购人和采购代理机构（以下统称为招标采购单位）均无义务和责任承担这些费用。

5． 投标供应商获取招标文件后，决定不参加本项目投标的，应在获取招标文件后5个工作日内以书面（加盖投标单位公章）电子邮件形式通知招标采购单位，如在规定期限内未收到投标供应商的书面函件，视为投标供应商同意参加投标。投标截止时无故（不可抗力事件影响除外）不参加投标的，将被采购单位列入非诚信供应商名单，影响其今后采购单位项目投标的诚信评价。

6. ▲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；公益一类事业单位不属于政府购买服务的承接主体，不得参与承接购买服务。

7. 如无特别说明，投标供应商参加本项目投标所使用的资格、信誉、荣誉、业绩与企业认证、人员必须为其单位所有。

8. ▲**参加本项目投标的供应商必须遵守“诚实信用”原则，并在投标文件中提供《诚信投标承诺书》（见附件统一格式），不提供该承诺书的投标文件将按无效标处理。**

**9.** ▲**投标供应商必须在《资格条件承诺函》（见附件统一格式）中对“2.合格投标供应商资格条件第2.1款”进行承诺，不按要求提供该承诺书的投标文件视为资格性审查不通过，投标无效，不得进入下一步评审。**

**10. 在线投标响应（电子投标）说明**

10.1 本项目通过“政府采购云平台（[www.zcygov.cn）”实行在线投标响应（电子投标），供应](http://www.zcygov.cn）\”实行在线投标响应（电子投标），供应)商应先安装“政采云电子交易客户端”，并按照本招标文件和“政府采购云平台”的要求，通过“政采云电子交易客户端”编制并加密投标文件。供应商未按规定加密的投标文件，“政府采购云平台”将予以拒收。

10.2 “政采云电子交易客户端”请自行前往“浙江政府采购网-下载专区-电子交易客户端”进行下载；电子投标具体操作流程详见本公告附件《供应商项目采购-电子招投标操作指南》；通过“政府采购云平台”参与在线投标时如遇平台技术问题详询400-881-7190。

10.3 为确保网上操作合法、有效和安全，供应商应当在投标截止时间前完成在“政府采购云平台”的身份认证，确保在电子投标过程中能够对相关数据电文进行加密和使用电子签章。使用“政采云电子交易客户端”需要提前申领CA数字证书，申领流程请自行前往“浙江政府采购网-下载专区-电子交易客户端-[CA驱动和申领流程](http://www.zjzfcg.gov.cn/bidClientTemplate/2019-05-27/12945.html" \o "CA驱动和申领流程" \t "_blank)”进行查阅。

**11.  根据《政府采购促进中小企业发展管理办法》（财库[2020]46号）规定，本项目专门面向中小企业进行采购，符合以下要求的供应商才能享受相关中小企业扶持政策，参加本项目磋商：**

**11.1 供应商按采购文件规定格式及要求在投标响应文件中出具了《中小企业声明函》（格式附件四-4），声明相关企业为中小企业的。如中标（成交），将在中标（成交）结果同时公告其《中小企业声明函》，接受社会监督。如提供的《中小企业声明函》内容不实的，属于提供虚假材料谋取中标，依照《政府采购法》等国家有关规定追究相应责任。**

**11.2 监狱企业视同小微企业，监狱企业参加投标应当提供由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，否则无效。**

**11.3 残疾人福利性单位视同小微企业。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供《残疾人福利性单位声明函》（见附件四-5），并对声明的真实性负责。如中标，将在中标结果同时公告其《残疾人福利性单位声明函》，接受社会监督。如提供的《残疾人福利性单位声明函》与事实不符的，依照《政府采购法》第七十七条第一款的规定追究法律责任。**

**11.4 对符合划分标准的个体工商户，视同中小企业。**

**12.** 为支持和促进中小企业发展，进一步发挥政府采购政策功能，温州市财政局出台了《温州市财政局关于温州市政府采购支持中小企业信用融资的通知》（温财采〔2020〕3号），供应商若有融资意向，可直接登录http://jinrong.zcygov.cn，查看信用融资政策文件及各相关银行服务方案，也可直接向各银行咨询相关业务。

## 二、 招标文件

1． 招标文件由招标文件目录所列内容及相关资料组成。

**2． 招标文件的澄清或修改**

2.1 招标采购单位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，招标采购单位应当在投标截止时间至少15日前，以书面形式（公告，下同）通知所有获取招标文件的潜在投标供应商；不足15日的，招标采购单位应当顺延提交投标文件的截止时间。该澄清或修改内容为招标文件的组成部分。

2.2 招标代理单位可以视采购的具体情况决定是否延长投标截止时间和开标时间，具体参照2.1条规定。

## 三、 投标文件的编制

1． 投标供应商应认真阅读招标文件中所有事项、格式、条款和技术规范等。投标供应商没有按照招标文件要求提交全部资料，或者没有仔细阅读招标文件，或者没有对招标文件各个方面做出实质性响应，是投标供应商的风险，由此造成的一切后果由投标供应商自行承担。

2．  **投标供应商应保证所提供文件资料的真实性，所有文件资料必须是针对本次投标的。如发现投标单位提供了虚假文件资料，其投标将被拒绝，并自行承担相应的法律责任。**

**3． 投标文件组成：**

3.1 投标文件由资格文件、商务技术文件和报价文件三个部分组成：

**（一）资格文件**

|  |  |  |
| --- | --- | --- |
| **序号** | **内容** | **备注** |
| 1 | 投标供应商营业执照（或事业单位法人证书）副本（复印件加盖公章） |  |
| 2 | 资格条件承诺函 | （附件四-3） |
| 3 | 中小企业证明文件 | （附件四-4、5） |
| 4 | 投标供应商认为需要提供的其他相关资格证明资料 |  |

**（二）商务技术文件**

|  |  |  |
| --- | --- | --- |
| **序号** | **内容** | **备注** |
| 1 | 投标函 | （附件一） |
| 2 | 法定代表人授权书 | （附件四-1） |
| 3 | 供应商基本情况表 | （附件四-2） |
| 4 | 诚信投标承诺书 | （附件十七） |
| 5 | 商务条款、技术规格偏离表 | （附件五1、2） |
| 6 | 货物成套供货清单 | （附件六） |
| 7 | 供应商综合实力 | （附件七） |
| 8 | 项目需求理解 | （附件八） |
| 9 | 功能及服务 | （附件九） |
| 10 | 人员投入 | （附件十） |
| 11 | 质量保证措施 | （附件十一） |
| 12 | 应急方案 | （附件十二） |
| 13 | 巡检计划 | （附件十三） |
| 14 | 培训计划 | （附件十四） |
| 15 | 售后服务 | （附件十五） |
| 16 | 同类项目业绩一览表 | （附件十六） |
| 17 | 投标供应商认为需要提供的其他相关资料 |  |

**（三）报价文件**

|  |  |  |
| --- | --- | --- |
| **序号** | **内容** | **备注** |
| 1 | 报价一览表 | （附件二） |
| 2 | 分项报价表 | （附件三） |

3.2 投标文件格式

投标供应商应根据招标文件中所提供的格式，内容按顺序填写并制作投标文件。**任何未按招标文件要求制作投标文件均可能会导致对其不利的评定，该风险由投标供应商自行承担。**

**4． 投标报价**

**4.1 投标报价是指本供应商为完成本次采购要求及完成技术标中所载明的设备费、软件费、系统集成、运输、安装、调试、人工费、利润、验收费、采购代理服务费、税金等完成合同所需的一切本身和不可或缺的所有工作开支、政策性文件规定及合同包含的所有风险、责任等各项全部费用，投标供应商应根据上述因素自行考虑含入投标报价。**

4.2 投标供应商必须按第三部分附件中的投标一览表、投标分项报价表（均统一格式）内容填写单价、合价和总价，并由法定代表人或授权代表签署。

4.3 本次投标均以人民币报价。

4.4 ▲招标采购单位不接受任何选择报价，对任何货物或服务只允许一个报价。

4.5 招标采购单位要求分类报价是为了方便评标，但在任何情况下不限制采购人以其认为最合适的条款、条件签订合同的权利。

**4.6 投标价报出后，投标供应商不得以任何理由予以变更。任何包含价格调整的要求，将被认为是非实质性响应投标而予以拒绝。**

**4.7 最低报价不能作为中标的保证。**

**5． 投标有效期**

**5.1 ▲自开标之日起90天内投标应保持有效。**

5.2 特殊情况下，在原投标有效期截止前，招标采购单位可与投标供应商协商延长投标有效期，这种要求和答复均以书面形式进行。投标供应商可拒绝接受延期要求。同意延长投标有效期的投标供应商不得修改投标文件。

5.3 在投标有效期内，投标供应商不能撤销投标文件，强行撤销投标文件的，应按预算（或最高限价）金额的2%赔偿对采购代理机构及采购人造成的损失。

**6. 投标文件的编制**

6.1 本项目通过“政府采购云平台（www.zcygov.cn）” 实行在线投标响应（即电子投标）。投标供应商应通过“政采云电子交易客户端”，并按照本招标文件和“政府采购云平台”的要求编制并加密投标文件。供应商未按规定加密的投标文件，“政府采购云平台”将予以拒收。

6.2 投标供应商应当按照本章节“投标文件组成”规定的内容及顺序在“政采云电子交易客户端”编制投标文件。其中资格文件和商务技术文件中不得出现本项目投标报价，如因投标供应商原因提前泄露投标报价，自行承担责任。

6.3 招标文件“第三部分 附件”中有提供格式的，投标供应商须参照格式进行编制（格式中要求提供相关证明材料的还需后附相关证明材料），并按格式要求在指定位置进行签章，否则视为未提供；招标文件“第三部分 附件”未提供格式的，请各投标单位自行拟定格式，并加盖单位公章（或CA电子公章）以及投标供应商代表签字，否则视为未提供。

6.4 在电子投标文件制作过程中投标文件编制内容不完整、编排混乱，未编有目录链接，或没有做好系统中每一评分项与投标文件对应内容关联的，导致投标文件被误读、漏读或者查找不到相关内容的，是投标供应商的责任，后果由投标供应商负责。

6.5 投标文件字迹模糊、潦草或表述不清所引起的后果由投标供应商负责。

6.6 投标文件中提供的各种证书、证件、证明资料，内容应该完整、清晰、易于辨识，如因为投标文件资料存有瑕疵，致使内容不全、模糊、难以辨认，或导致对材料真实性存疑等情形的，是供应商自己的风险，如因此导致评委作出对其不利的评定，一切后果由供应商自行承担。

6.7 本招标文件里“评分内容”中要求提供的各种证书、证件、证明资料须原件备查，即投标供应商在投标时不需要提供原件，如采购人、采购代理机构或评委会在后续环节中需要对相关资料原件进行真实性核查时，则投标供应商必须按要求提交相关原件及其他要求提供的辅助证明材料，如供应商不能按要求提供相关原件及其他要求提供的辅助证明材料以证明其资料真实性的，采购人及采购代理机构将做出对其不利的认定（包括取消其投标或中标资格），后果由投标供应商负责。

**7. 投标文件的签章**

7.1投标文件封面和内部有要求盖章或签字的地方应加盖投标供应商的单位公章（或CA电子公章，两者具有同等效力，下同）以及投标供应商代表签字。电子签章操作指南详见采购公告附件《供应商项目采购-电子招投标操作指南》。

7.2 投标文件不得涂改，若有修改错漏处，须加盖单位公章（或CA电子公章）或者投标供应商代表签字。

**8. 投标文件的形式**

8.1投标文件的形式：电子投标文件包括“电子加密投标文件”和“备份投标文件”，在投标文件编制完成后同时生成。其中备份投标文件不作为强制要求提供。

8.2 电子加密投标文件：电子加密投标文件是指通过“政采云电子交易客户端”完成投标文件编制后生成并加密的数据电文形式的投标文件。

8.3 备份投标文件：备份投标文件是指与电子加密投标文件同时生成的数据电文形式的电子文件（备份标书），其他方式编制的备份投标文件视为无效的备份投标文件。

**9. 投标文件的份数**

9.1 电子加密投标文件：一份，在线上传递交。

9.2 备份投标文件：一份，以介质（U盘）存储形式通过现场方式或邮寄（EMS、顺丰）方式递交采购代理机构。

**10. 投标文件的效力**

10.1投标文件的启用，按先后顺位分别为电子加密投标文件、备份投标文件。供应商不上传或提供电子加密投标文件的，投标无效。

10.2电子加密投标文件与备份投标文件的内容应完全一致。如因电子加密投标文件解密异常，才能启用备份投标文件，备份投标文件一旦启用，则电子加密投标文件即为失效。

## 四、 投标

**1. 电子加密投标文件的上传、递交**

1.1 投标供应商应在投标截止时间前将电子加密投标文件成功上传递交至“政府采购云平台”，在投标截止时间后上传提交投标文件的，将被政采云平台拒绝，投标无效。

1.2 电子加密投标文件成功上传递交后，供应商可自行打印投标文件接收回执。

**2. 备份投标文件的密封、递交**

2.1 **备份投标文件的密封及标记**

备份投标文件应当包装密封，封口处贴上封条，启封处加盖投标供应商法人公章并由法定代表人或授权代表签字，并在封皮上标注投标项目名称、编号、投标供应商名称、地址、联系人、联系电话、邮政编码，注明“备份投标文件”字样。如果未按上述要求密封及标记，招标采购单位对备份投标文件的误投和提前启封不负责任。

2.2 **备份投标文件的递交**

（1）投标供应商在“政府采购云平台”完成电子加密投标文件的上传递交同时，还可以在投标截止前一日以现场方式（评标地点）或邮寄（通过EMS、顺丰寄至邮寄地址）方式递交以介质（U盘）存储的备份投标文件。

（2）采购代理机构工作人员将做好备份投标文件的签收手续，明确备份投标文件的提交时间、份数、提交人等信息。没有密封包装或者逾期送达至指定地点的备份投标文件将不予接收。因密封不严、标记不明而造成过早启封、失密等情况，采购代理机构概不负责。

（3）采用EMS、顺丰邮寄递交备份投标文件的，应充分考虑邮寄时间，送达时间不迟于投标截止前一日17点整，具体以采购代理代理机构工作人员签收时间为准，并自行承担邮寄过程中可能发生的时间延误、密封破损等一切风险和责任。寄出前应对包装的密封情况进行拍照，寄出后将相关邮寄信息及照片发送至代理机构邮箱，告知代理机构邮件接收人并做好邮件密封核对工作。邮寄地址：温州市鹿城区隔岸路68号2楼；邮件接收人：金先生；联系电话：0577-88521066；邮箱：[358801740@qq.com；邮编：325000](mailto:155400207@qq.com；邮编：325000)。

2.3 通过“政府采购云平台”成功上传递交的电子加密投标文件已按时解密的，备份投标文件自动失效。

**3. 电子加密投标文件的解密和异常情况处理**

3.1开标后，采购组织机构将向各投标供应商发出电子加密投标文件的解密通知，各投标供应商代表应当在招标文件规定的时间内自行完成电子加密投标文件的在线解密。

3.2通过“政府采购云平台”成功上传递交的电子加密投标文件无法按时解密，投标供应商如按规定递交了备份投标文件的，以备份投标文件为依据（由采购组织机构按“政府采购云平台”操作规范将备份投标文件上传至“政府采购云平台”，上传成功后，电子加密投标文件自动失效），否则视为投标文件撤回。

3.3投标截止时间前，投标供应商仅递交了备份投标文件而未将电子加密投标文件上传至“政府采购云平台”的，投标无效。

**4. 投标文件的补充、修改或撤回**

4.1供应商应当在投标截止时间前完成投标文件的上传、递交，并可以补充、修改或者撤回投标文件。补充或者修改投标文件的，应当先行撤回原文件，补充、修改后重新上传、递交（撤回后需重新做好系统评分内容与投标文件对应内容的关联），如投标截止时间前未完成重新上传、递交的，视为撤回投标文件。投标截止时间后递交的投标文件，“政府采购云平台”将予以拒收。

4.2投标截止时间后，投标供应商不得撤回、修改投标文件。

## 五、 开标和评标

**1． 评标委员会**

1.1 本项目依法组建评标委员会。评标委员会由采购人或采购代理机构依法组建，成员包括采购人代表和评审专家，成员人数为五人或以上单数，其中评审专家不少于成员总数的三分之二。评标委员会成员名单在评审结果（采购结果）公告前保密。

1.2 评标委员会的成员在评标过程中必须严格遵守《政府采购法》等有关法律、法规的规定。

1.3 评标委员会负责具体评标事务，并独立履行下列职责：

　　（1）审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；

　　（2）要求投标供应商对投标文件有关事项作出澄清或者说明；

　　（3）对投标文件进行比较和评价；

　　（4）确定中标候选人名单，以及根据采购人委托直接确定中标人；

　　（5）向采购人、采购代理机构或者有关部门报告评标中发现的违法行为。

2． 评标过程的保密性

2.1 **开标后直至向中标供应商授予合同时止，凡与评审有关的资料均不得向投标供应商及与评标无关人员透露。如果投标供应商在评标过程中试图向招标采购单位施加影响，或扰乱开评标秩序，其投标将被拒绝。**

**3． 开标、评标**

3.1采购组织机构将按照招标文件规定的时间通过“政府采购云平台”组织开标、开启投标文件，所有供应商均应当准时在线参加。投标供应商如不在线参加开标大会的，视同认可开标结果，事后不得对开标过程和开标结果提出异议。如投标供应商因未在线参加开标而导致投标文件无法按时解密等一切后果由供应商自己承担。

3.2 向各投标供应商发出电子加密投标文件【开始解密】通知，由供应商在**采购代理机构发送解密指令后60分钟内**自行对已递交的电子加密投标文件进行解密。供应商在规定的时间内无法完成电子加密投标文件解密的，如已按规定递交了备份投标文件，将由采购组织机构按“政府采购云平台”操作规范将备份投标文件上传至“政府采购云平台”，上传成功后，电子加密投标文件自动失效。

3.3 投标文件解密结束后，采购代理机构将统一开启电子投标文件，各投标供应商需确认己方报价，并签署《政府采购活动现场确认声明书》（声明书已放在招标文件最后一页，由供应商打印填写签章），扫描回传邮箱（358801740@qq.com）。

3.4 开标结束后，采购人或采购代理机构将依据法律法规及招标文件的规定对投标供应商的资格文件进行审查，包括营业执照（或事业单位法人证书）、合格供应商资格证明文件，以确定是否具备投标资格。▲投标供应商未按要求提交上述资料或经审查所提交的资格证明材料无法证明其符合招标文件规定的“投标供应商资格要求”的，或具有其他违反法律法规规定应被取消投标资格情形的，资格审查将不予通过，其投标文件作无效标处理，并不再将其投标提交评标委员会进行后续评审。

采购人或采购代理机构对投标供应商所提交的资格证明材料仅负审核的责任。如发现投标供应商所提交的资格证明材料不合法或与事实不符，采购人可取消其中标资格并追究投标供应商的法律责任。

3.5评标委员会对符合资格的投标供应商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。▲没有满足招标文件实质性要求的投标作无效标处理。评标委员会决定投标的实质性要求只根据投标文件本身的内容，而不寻求外部的证据。投标供应商不得通过修正或撤销不合要求的偏离或保留从而使其投标成为实质上响应的投标。

3.6 评标委员会认为投标供应商的报价明显低于其他通过符合性审查投标供应商的报价，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；投标供应商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。

3.7招标文件中加“下划线”且加“▲”的条款，为实质性条款，不得负偏离，否则按无效标条款处理。对于标书中规定的实质性条款，判定是否构成实质性偏离，由评标委员会来判定。

投标响应微小负偏离或重大负偏离的认定，由评标委员会来判定，对属于微小负偏离的由评委在评分中予以酌情考量，对构成重大负偏离的，将被认定为是对招标文件实质上的不响应，按无效标条款处理。

3.8 评标委员按照招标文件中规定的评标方法和标准，对投标文件进行商务和技术评估，综合比较与评价。

**3.9** ▲**投标文件有下列情形之一的，经评标委员会认定后按无效标处理（无效标条款）：**

**（1）投标文件在招标文件规定的实质性响应内容中未按要求加盖单位公章（或CA电子公章）、无法定代表人签章（或CA电子签章）或其授权代表签字的；**

**（2）投标响应明显不满足招标文件中规定的采购需求及技术、服务要求的被认定构成重大偏离的，或不满足招标文件中规定的标注“▲”的实质性条款，或存在招标文件中明确规定的其他无效标情形的；**

**（3）投标文件内容不全或关键字迹模糊无法辨认的；**

**（4）投标文件的编制明显不符合招标文件规定的编制要求；**

**（5）在资格文件和商务技术文件中出现投标报价的；**

**（6）投标文件附有采购人不能接受的条件；**

**（7）未提供法定代表人授权委托书（法定代表人作为投标供应商代表的除外），或提供的法定代表人授权委托书信息填写不完整或没有加盖单位公章（或CA电子公章）或无法定代表人本人签章（或CA电子签章）或有涂改等情形导致无法确认其有效性的；**

**（8）同一投标供应商提交两个以上不同的投标文件（或投标方案）或者投标报价的；**

**（9）评标委员会认定投标供应商具有法律、法规规定的不良投标行为的；**

**（10）未按照采购文件标明币种进行报价的，或者投标报价涵盖的内容不符合采购文件要求的，或者投标报价超过采购预算（或最高限价）的；**

**（11）评标委员会认定供应商的报价明显低于其他通过符合性审查投标供应商的报价，有可能影响产品质量或者不能诚信履约的，但该供应商不能证明其报价合理性的；**

**（12）评标委员会认定不符合法律、法规和招标文件中规定的其他实质性要求的。**

3.10 投标文件商务报价出现前后不一致的，按照下列规定修正：

（1）投标文件中开标一览表内容与分项报价表内容不一致的，以开标一览表为准；

（2）大写金额和小写金额不一致的，以大写金额为准；

（3）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；

（4）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。▲如果投标供应商不接受对其价格错误进行修正，其投标无效。

4. 评标过程中遇到特殊情况，由评标委员会遵循公开、公正原则，采取投票方式按照少数服从多数原则决定。

5． 投标文件的澄清

5.1 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，评标委员会应当以书面形式（或通过“政府采购云平台”在线询标）要求投标供应商在30分钟内作出必要的澄清、说明或者补正。投标供应商的澄清、说明或者补正应当采用书面形式（或通过“政府采购云平台”在线答复），并由法定代表人或其授权的代表签字。投标供应商的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。拒不按要求对其投标文件进行澄清，说明或补正的投标供应商，评标委员会可以否决其投标。

5.2 ▲**经澄清后，若偏差仍存在，且不可接受，投标供应商则被认为是“没有实质性响应招标文件要求”，其投标不进入下一步评审。**

6． 确定中标候选供应商

6.1 本次招标由评标委员会确定2名中标候选供应商并向采购人推荐，采购人根据评标委员会的推荐结果按顺序确定中标供应商。

6.2 评标委员会依据法律、法规及招标文件有关规定按有效投标供应商的最终得分（即商务技术分与价格分之和）高低进行排序，得分前二名的投标供应商确定为第一和第二中标候选供应商（得分相同投标报价低的排序第一；得分且投标报价相同的，中标候选供应商并列，并确定技术部分得分高的为中标供应商）。

6.3 排名第一的中标候选供应商放弃中标；因不可抗力或自身原因提出不能履行合同；或未能在规定时间内与采购人签订合同的；或在规定时间内借故否认已经承诺的条件而拒签合同的；或已签合同却拒绝按合同约定履约的；或者因排名第一的候选供应商在本次采购活动中存在违法违规行为或其他原因被取消中标资格的，采购人可确定由排名第二的候选供应商为中标供应商，也可以重新开展政府采购活动。

**6.4 采购人根据招标文件、中标供应商的投标文件、合同等材料及时组织验收，并严把质量关。**

**6.5 采购人对决标结果不做任何解释，也不保证最低价中标。**

**7． 评标细则详见第五部分“评标原则及方法”。**

**8． 未详尽事宜，遵照有关法律法规执行。**

**9. 特别说明：如遇“政府采购云平台”电子化开标或评审程序调整的，按调整后程序执行。**

## 六、 授予合同

**1． 中标结果公告**

1.1 评标委员会推荐的中标候选人经采购人确认为中标供应商后，在浙江省政府采购网上发布中标结果公告，公告期1个工作日。

**2．**  **中标通知书**

2.1 中标供应商确定后，采购人将向中标供应商发出中标通知书。

2.2 中标通知书是合同的一个组成部分,对采购人和中标供应商均具有同等法律效力。

3． 授标时更改采购货物数量的权力

3.1 采购人在授予合同时有权对采购服务的数量在10%幅度范围内予以增加或减少,但不得对单价和其他的条款和条件作任何改变。

4． 签订合同

4.1 中标供应商应按中标通知书规定的时间、地点与采购人签订合同。

4.2 招标文件、中标供应商的投标文件、投标修改文件、评标过程中有关澄清文件及经投标供应商和评委双方签字的询标纪要和中标通知书均作为合同附件。

4.3 拒签合同的违约责任

**中标供应商接到中标通知书后，在规定的时间内因自身原因拒签合同的，或在规定时间内借故否认已经承诺的条件而拒签合同的，按自动弃标处理。如已签合同却拒绝按合同约定履行，以违约处理，采购人可单方终止合同，并上报采购监管部门。**

**4.4 合同一式五份，其中采购人二份，中标供应商二份，采购代理机构备案一份。中标供应商在采购合同签订后应及时将合同交采购代理机构备案。**

**5． 质疑与投诉**

5.1 投标供应商认为采购文件、采购过程、中标和成交结果使自己的合法权益受到损害的，可以在知道或应知道其权益受到损害之日起七个工作日内以书面形式向招标采购单位提出质疑。对采购文件提出质疑的，应当在获取采购文件（以云平台获取时间为准）或者采购文件公告期限届满之日起7个工作日内，否则将不予接受。对采购结果提出质疑的，质疑期限自采购结果公告（包括公示、预公告、结果变更公告等）期限届满之日起计算。供应商针对同一采购程序环节的质疑必须一次性提出，否则不予接受。

5.2 招标采购单位在收到投标供应商的书面质疑后七个工作日内作出答复，但答复的内容不得涉及商业秘密。质疑供应商对招标采购单位的答复不满意，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。联系方式：温州市财政局政府采购监管处项先生、蔡女士，联系号码：0577-88532725、88521948。

5.3 投诉人投诉时，应提交投诉书。投诉人对投诉书的真实性负责，恶意投诉将承当相应的法律和民事责任。

**6． 招标代理服务费**

6.1 ▲本项目采购代理服务费一次性收取人民币壹万柒仟元整（￥17000.00），由最终中标供应商在领取中标通知书时支付，采购代理费包含在投标总价中综合考虑。

6.2 采购代理服务费可以是现金、支票或汇票。

# 第二部分 合同主要条款

**政 府 采 购 合 同**

项 目 名 称： \_

项 目 地 点：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

合 同 编 号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

采 购 单 位：

中标供应商：

签 订 日 期：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

甲方（采购人）：

乙方（中标供应商）：

温州市公安局交通管理局的 （项目名称) (项目编号）在国内以公开招标方式进行采购，经评标委员会综合评定 （中标供应商名称）为中标供应商。为了明确甲、乙双方的权利和义务，履行各自的职责，高效优质地完成本项目的各项工作任务，按照《中华人民共和国采购法》、《中华人民共和民法典》等有关法律法规规定，经甲乙双方在平等、自愿的基础上共同协商一致，现签订合同如下。

1. **合同项目名称**

1. **合同文件的组成**

下列文件构成本合同的组成部分：

1. 合同主要条款
2. 合同补充条款或说明（如有）

(2) 中标通知书

(3) 招标文件

(4) 投标文件

(5) 承诺书 （含询标时承诺）

1. **合同总价及付款方式**

1、合同总价（暂定）： 万元（大写 元），包括设备费、软件费、系统集成、运输、安装、调试、人工费、利润、验收费、采购代理服务费、税金等完成合同所需的一切本身和不可或缺的所有工作开支、政策性文件规定及合同包含的所有风险、责任等各项全部费用，投标供应商应根据上述因素自行考虑含入投标报价。

**▲2、付款方式：**

1. 预付款：签订合同后7个工作日内，甲方向乙方支付合同总价的50%预付款。
2. 履行期间付款：系统安装调试结束，乙方提交全部报告材料，经甲方组织确认，完成项目进入试运行后，甲方于7个工作日内，支付合同金额的20%款项。
3. 系统维护期满1年，运维任务合格，支付合同金额的10%款项。系统维护期满2年，运维任务合格，支付合同金额的10%款项。
4. 待三年系统维护期满后，由乙方提出验收申请，于20个工作日内组织项目验收，项目通过验收后7个工作日内支付剩余合同金额的10%款项。
5. **合同服务内容及要求**
6. 具体采购内容及技术要求：见招标文件第四部分“采购内容及要求”相关内容
7. 人员培训要求：见招标文件第四部分“采购内容及要求”相关内容
8. 售后服务要求：见招标文件第四部分“采购内容及要求”相关内容
9. 项目时间进度及交付地点要求：见招标文件第四部分“采购内容及要求”相关内容
10. **权利和义务**

（一）甲方权利与义务

1. 甲方有权要求乙方全面、高效、优质的履行合同规定的要求（包括招标文件的要求及履约过 程中甲方交待的事项）以及乙方承诺的义务（包括投标文件的承诺）。乙方未能如期达到本合同要求，甲方有权解除本合同，除扣除相应合同款外，乙方应赔偿甲方相应的损失。
2. 甲方有权对乙方的工作质量、进度及要求进行控制和管理，对发现的问题及时向乙方提出书面或口头改进意见，并限期予以整改完善。
3. 甲方有权对项目实施过程中的决策、控制、实施等环节实行全面管理，协调和监督工作开展，进行中间检查，组织成果评审。
4. 甲方有权对乙方不履行合同义务及其投标承诺的行为进行处罚。
5. 甲方有权检查乙方项目组的组成和人员到位情况、人员稳定情况，可要求乙方调整不合格项目组成员及员工，并在要求的时间内及时调整到位。
6. 甲方有权审查乙方编制的管理文件及技术文件。
7. 甲方有权根据政策的变动或项目实际需要，对合同项目内容进行修改和补充，乙方应积极配合。
8. 在合同有效期内，甲方应当履行合同约定的义务，如有违反，则应当承担违约责任。
9. 甲方需积极协助配合乙方开展相关工作，协助乙方解决问题、使之顺利开展工作。
10. 甲方需及时提供完整、充分的项目基础资料，若因资料提供不及时造成项目延期，甲方应与乙方协商解决。
11. 甲方应按时向乙方支付合同款项，如出现有合同款项扣罚或经济处罚的情况，将在扣罚相关金额后进行余额的支付。
12. 甲方负责组织评审和确认成果及重大技术方案，甲方接到乙方交付的各阶段性研究成果后，应及时组织评审，并将评审意见以书面方式通知乙方。
13. 在合同履行期间，如因甲方原因提出解除合同的，甲方应根据乙方已完成的实际工作量支付相应的费用。
14. 合同及招标文件规定的其他权利义务。

（二）乙方权利和义务

1. 乙方有权根据合同约定申请并获得项目合同款。
2. 乙方根据研究工作需要，在合同规定的由甲方提供的资料范围内，有权要求甲方提供相关资料。
3. 乙方应在承包范围内全面、高效、优质的履行合同规定的各项要求（包括招标文件的要求及履约过程中甲方交待的事项）以及己方承诺的义务（包括投标文件的承诺）。
4. 乙方应按甲方的要求开展工作，合同实施方案应事先征得甲方的同意在予以实施。如在合同履约过程中出现计划或方案变更情况时，应及时向甲方提出，并在征得甲方的同意后方可实施。
5. 乙方应接受甲方的管理、监督及检查，在项目实施过程中出现问题应及时的纠正并向甲方进行通报。
6. 乙方有义务配合甲方完成各项审批和各阶段成果审查工作。
7. 乙方应维护甲方的声誉和利益，服从甲方的统一安排。
8. 乙方应严格遵守国家有关法律、法规，若有违反，由此造成的一切后果由乙方承担。乙方如因上述原因使合同性质发生改变，甲方不负赔偿责任。
9. 甲方不承担乙方在合同履行过程中因其责任引起的一切事故、法律纠纷和经济责任，乙方须自行负责并处理合同履行过程中与第三方发生的所有事故、法律纠纷及一切费用。
10. 本项目不能擅自转让或分包。若需要分包，须经甲方认可，乙方对分包服务承担全部责任。如发现擅自转让或分包，甲方有权否决或终止合同，由此给甲方带来的一切损失，由乙方承担。
11. 乙方有技术保密的责任和义务，项目中所涉及的所有资料数据与成果文件乙方均应负责保密，未经甲方同意不得以任何形式透露给第三方。如发现乙方有泄密情况，可根据国家有关法律向对方追究法律责任。
12. 乙方负责项目履行过程中的安全责任问题，任何因人身安全伤害、财产损害问题导致的相关责任、赔偿等均由乙方全权负责和承担，乙方应切实做好安全防范工作，避免在工作中出现人身与财产的意外损害。
13. 承担本项目任务后，乙方在“项目实施周期”内向甲方提供与本项目相关的技术咨询服务。
14. 本合同执行中相关的一切税费均由乙方负担。
15. 合同及招标文件规定的其他权利义务。
16. **知识产权保证、归属**

1、本项目开发成果的知识产权和软件源代码在签订合同后为甲方所有，署名权为甲方、乙方双方所共有，乙方有权就本项目开发成果参与报奖评优等活动。

2、乙方保证最终提供给甲方的工作成果不会引起任何第三方基于该产品知识产权的指控，发生的任何侵权责任由乙方负责承担，与甲方无关。

3、本条款的规定不因本合同的到期而失效。

1. **违约责任**

1、甲方违约

1.1甲方未按约定及时提供基础资料，或受客观原因的制约未能履行合同约定职责的，有责任采取措施，消除影响。

1.2在合同履行期间，因甲方自身原因要求中止或解除合同，应向乙方偿付违约金，违约金按合同总价的20％计算；同时按实际己完成工作量向乙方支付合同款；不可抗力及政府政策调整原因除外。

2、乙方违约

2.1乙方未能履行合同义务，未遵守《招标文件》规定和《投标文件》中所承诺的服务内容及合同相关规定，均属违约行为。甲方根据合同规定条款，视乙方违约行为的情节轻重，做出警告、扣罚合同款项等处理，情节严重者，甲方有权单方终止本合同而不承担任何违约责任，由乙方承担一切经济损失和法律责任。因乙方违约造成甲方损失的，甲方从乙方的合同款中扣除。

2.2由于乙方原因，延误了各阶段任务完成时间，每延误一天（日历天），应减收该任务部分应收费用的千分之二，扣除最高限额为该任务部分合同费用的8%，一旦达到扣除服务费的最高限额，甲方有权单方面终止合同。

2.3由于乙方错误造成项目质量事故损失，乙方除负责采取补救措施外，应免收受损失部分的服务费用，并根据损失程度向甲方支付相应的赔偿金。

2.4合同生效后，乙方因自身原因要求终止或解除合同，应向甲方偿付违约金，违约金按合同总价的20％计算；甲方已付合同款需全部退还；不可抗力原因除外。

2.5乙方未认真履行合同义务和服务承诺，发现1次扣除合同总金额0.1%，即￥ (人民币 元整)。工作缺失造成不良后果的，确认一次扣除合同总金额0.5%，即￥ (人民币 元整)。

2.6因乙方责任发生违反公安网络和计算机使用规定的，发生一次扣除合同总金额0.5%，即￥ (人民币 元整)。被上级部门通报的，发生一起扣除合同总金额的0.75%，即￥ (人民币 元整)。被省级以上(含)部门的扣除合同总金额的1%，即￥ （人民币 元整)。

2.7合同执行期内，如因乙方责任造成甲方严重安全事件2起(含)以上，或被上级部门报3次(含)以上的甲方有权立即解除合同，可停止支付合同款，乙方将赔偿有关损失，乙方人员涉及违法犯罪的，依法追究其法律责任。

1. **不可抗力**

1、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。不可抗力事件延续30天以上，双方应通过友好协商，确定是否继续履行合同。

2、在合同有效期间发生不可抗力，导致合同不能或不能全部履行。双方可以按以下各项执行：

（1）因不可抗力导致合同终止，并不影响任何一方对不可抗力先前发生的违约行为合法追偿。

（2）甲方不承担因不可抗力造成合同不能正常履行的责任。

3、遇国家政策性调整，影响合同履行，双方协商解决。

1. **合同生效及终止**

（一）合同生效：本合同自甲乙双方法定代表人或委托代理人签字、盖章之日起生效。

（二）合同终止：本合同出现以下情况时终止。

1、提前终止

（1）乙方因自身过错未能履行合同和遵守有关规定，在甲方发出书面警告后仍无采取补救措施，甲方有权单方终止合同，乙方应无条件退还全额已支付合同款。

（2）根据招标文件第四部分要求及乙方在《投标文件》中做出的承诺性条款进行检查考评，不符合相关规定需终止合同的。

（3）乙方有以下行为之一的：

1）违反规定造成重大伤亡或重大损失。

2）因管理不善造成恶劣影响。

3）从事违法犯罪活动或其他损害甲方形象或声誉的活动。

4）未经甲方同意擅自将合同全部或部分转包、分包给第三者。

5）违反其他相关法律法规，造成恶劣影响。

6）《投标文件》承诺项目未落实到位的，弄虚作假及其他不正当行为。

（4）乙方破产清算、重组及兼并等事实发生，或被债权人接管经营，甲方无需通知乙方即可终止承包。

（5）合同规定的其他终止情况。

2、协议终止

经双方协商同意，可在任何时候终止合同。

3、自然终止

合同规定的义务履行完毕，合同自然终止。

（三）合同未尽事宜由双方协商解决，并以书面形式修改或补充本合同条款；合同的附件、修改（补充）件均与本主合同有同等的法律效力。

1. **争议的解决**

合同争议由双方友好协调解决。协商不一致，任何一方均可提起向甲方所在地人民法院提起诉讼。

1. **合同的份数**

本合同一式伍份，双方各执贰份，交采购代理机构备案壹份。

甲 方：（印章） 乙 方：（印章）

全权代表：（签字） 全权代表：（签字）

地 址： 地 址：

邮政编码： 邮政编码：

电 话： 电 话：

传 真： 传 真：

开户银行： 开户银行：

帐 号： 帐 号：

日 期： 日 期：

# 第三部分 附件

## 附件一 投 标 函

**投 标 函**

温州市公安局交通管理局

浙江东瓯工程造价咨询有限公司：

根据贵方为项目（编号：）的投标邀请，我方 （投标供应商名称） 作为投标供应商正式授权　 （授权代表全名，职务） 代表我方处理有关本投标的一切事宜，并参加本项目的投标。

在此提交的投标文件中，包括按“招标文件”要求编制的资格文件、商务技术文件、报价文件。

我方己完全明白招标文件的所有条款要求，并重申以下几点：

（一）本投标文件的有效期自投标截止日起**90**天内有效，如中标，有效期将延至合同终止日为止；

（二）我方已详细研究了招标文件的所有内容包括修改书（如有）和所有已提供的参考资料以及有关附件，我方完全理解并同意放弃在此方面提出含糊意见或误解的一切权力；

（三）我方明白并承诺在规定的开标时间之后，在投标有效期内不撤回投标；

（四）我方同意提供按照贵方可能要求的与投标有关的一切数据或资料；

（五）我方理解贵方不一定接受最低报价。

（六）我方如果中标，将保证履行招标文件以及招标文件修改书（如有）中的全部责任和义务，按质、按量、按期完成《合同书》中的全部任务。

（七）所有与本投标有关的函件请发往下列地址：

地址

电话

传真

电子邮件

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件二 投标一览表

**投标报价一览表**

**项目名称： 项目编号：**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名 称** | **投标报价（元）** | **备注** |
| 1 | 网络安全框架建设 |  |  |
| **投标报价 （大写）** | | 元 | |

**注：**

**1. 投标报价是指本供应商为完成本次采购要求及完成技术标中所载明的设备费、软件费、系统集成、运输、安装、调试、人工费、利润、验收费、采购代理服务费、税金等完成合同所需的一切本身和不可或缺的所有工作开支、政策性文件规定及合同包含的所有风险、责任等各项全部费用，投标供应商应根据上述因素自行考虑含入投标报价。**

2.此投标报价一览表中投标报价应与附件三“投标分项报价表”中“总计价”相一致,不一致的以投标一览表为准。

**3．▲此表不得自行增减内容，不按要求提供此表格将被视为没有实质性响应招标文件,其投标文件将被拒绝。**

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件三 投标分项报价表

**投标分项报价表**

**项目名称： 项目编号：**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项 目 内 容** | **报价（元）** | **备注** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | 总 计 价 |  |  |

注：1. 按投标报价费用构成逐项列出；表内总计价应与附件二“投标报价一览表”中的投标报价相一致。

2. **▲**不按要求提供投标分项报价表将视为没有实质性响应招标文件。

投标供应商名称（盖章）：

投标供应商代表（签字）:

日 期： 年 月 日

## 附件四 证明文件

## （1）法定代表人授权书

温州市公安局交通管理局

浙江东瓯工程造价咨询有限公司：

（投标供应商全称） 法定代表人 授权 （全权代表姓名） 为全权代表，参加贵办组织的 （项目名称、编号） 的招投标活动，全权代表我方处理招投标活动中的一切事宜。

本授权书于 年 月 日签章生效，本授权无转委托权，特此说明。

法定代表人 (签字或盖章)：

投标供应商名称（公章）：

日期： 年 月 日

附：

授权代表姓名：

职务：

|  |
| --- |
| 投标供应商授权代表身份证复印件  （粘贴处） |

详细通讯地址：

电话：

传真：

邮政编码:

## （2）供应商基本情况表

**项目名称： 项目编号：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 单位名称  （公章） |  | | | | |
| 单位地址 |  | | | | |
| 主管部门 |  | | | | |
| 成立时间 |  | 批准部门 |  | 批准文号 |  |
| 单位性质 |  | 开户银行及帐号 |  | 注册资金  （万元） |  |
| 资质等级 |  | 证号 |  | 发证单位 |  |
| …… |  |  |  |  |  |
| 相关认证证书 |  | | | | |
| 主要售后服务机构 |  | | | | |
| 联系人 |  | 电话 |  | | |
| 传真 |  | | |
| 职工概况 | 职工总人数 |  | 高级职称/资质（人数） | |  |
| 中级职称/资质（人数） | |  |
| 单位行政和主要技术人员 | | | | |
| 姓名 | 职务及职称 | 年龄 | 专业 | 从业年限 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| …… |  |  |  |  |

**注：附营业执照副本、资质证书等有关复印件。**

## （3）资格条件承诺函

温州市公安局交通管理局

浙江东瓯工程造价咨询有限公司：

我方参与 （采购项目名称、编号）投标，现郑重承诺：

1、我方符合《中华人民共和国政府采购法》第22条规定的资格条件，即

（1）我方具有独立承担民事责任的能力；

（2）我方具有良好的商业信誉和健全的财务会计制度；

（3）我方具有履行合同所必需的设备和专业技术能力；

（4）我方有依法缴纳税收和社会保障资金的良好记录；

（5）我方参加本次政府采购活动前3年内在经营活动中没有重大违法记录（没有因违法经营受到刑事处罚，没有被责令停产停业、被吊销许可证或者执照、被处以较大数额罚款等行政处罚，没有因违法经营被禁止参加政府采购活动的期限未满情形）。

2、到本项目投标截止时间为止，我方未被“信用中国（[www.creditchina.gov.cn）、](http://www.creditchina.gov.cn）、) 中国政府采购网（www.ccgp.gov.cn）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。

以上承诺如有虚假，愿接受取消我方任何资格（投标/中标/签订合同）及其他任何形式的处理。

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

注：▲不按要求提交本承诺书按无效标处理。

## （4）中小企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展管理办法》（财库[2020]46号）的规定，本公司参加 温州市公安局交通管理局 的 网络安全框架建设 采购活动，服务全部由符合政策要求的中小企业承接。相关企业的具体情况如下：

1. 网络安全框架建设项目，属于 其他未列明行业 ，承接企业为 （填写企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元，属于 (填写中型企业、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： 年 月 日

相关说明及要求：

1. 从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。
2. 中小微企业标准：符合《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。
3. 请投标供应商按本表规定格式及要求填写并加盖单位公章。
4. 填写本表的投标供应商应为浙江政府采购网正式入库供应商。
5. 不属于中小微企业的无需出具该声明函。

## （5）残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加 单位的 项目（编号： ）采购活动提供本单位制造的货物，或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件五 商务、技术条款偏离表

**（1）商务条款偏离表**

**项目名称： 项目编号：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **招标文件**  **条目** | **招标文件**  **规格要求** | **投标文件**  **对应规格** | **说 明** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**注：** 如有偏离，必须在偏离表中进行详细对比说明并注明正偏离（负偏离），如所有条款均无偏离，则只需在“投标文件对应规格”第一栏中填写“无偏离”即可。如不说明偏离情况，视为完全响应招标文件要求无偏离。

投标供应商名称（盖章）：

投标供应商代表（签字）：

日期： 年 月 日

**（2）技术条款偏离表**

**项目名称： 项目编号：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **招标文件**  **条目** | **招标文件**  **规格要求** | **投标文件**  **对应规格** | **说 明** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**注：**如有偏离，必须在偏离表中进行详细对比说明并注明正偏离（负偏离），如所有条款均无偏离，则只需在“投标文件对应规格”第一栏中填写“无偏离”即可。如不说明偏离情况，视为完全响应招标文件要求无偏离。

投标供应商名称（盖章）：

投标供应商代表（签字）：

日期： 年 月 日

## 附件六 货物成套供货清单

1. **货物成套供货清单（或详细配置清单）**

**项目名称： 项目编号：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名 称** | **品牌、规格型号** | **单位** | **数量** | **原产地** | **制造商** | **质保期** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**（2）随机备品备件、易损易耗件和专用工具清单（如有）**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名 称** | **型号规格** | **数量** | **原产地/制造商** | **备注** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**注：投标供应商可按以上表格形式进行复制、附在技术标内。**

投标供应商名称（盖章）：

投标供应商代表（签字）：

日期： 年 月 日

## 附件七 供应商综合实力

**供应商综合实力**

|  |
| --- |
|  |

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件八 项目需求理解

**项目需求理解**

|  |
| --- |
|  |

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件九 功能及服务

**功能及服务**

|  |
| --- |
|  |

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件十 人员投入

**项目组人员一览表**

项目名称： 项目编号：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 | 性别 | 年龄 | 专业 | 职称/资质 | 证书号 | 拟任何职 | 是否为在温驻场人员 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

注：1、本表应附所列项目组成员相关证书、社保等证明复印件。

2、此表仅提供了表格形式，可按此表格复制。

3、请在本表中明确在温驻场人员。

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件十一 质量保证措施

**质量保证措施**

|  |
| --- |
|  |

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件十二 应急方案

**应急方案**

|  |
| --- |
|  |

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件十三 巡检计划

**巡检计划**

|  |
| --- |
|  |

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件十四 培训计划

**培训计划**

|  |
| --- |
|  |

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件十五 售后服务

**售后服务**

|  |
| --- |
|  |

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件十六 项目业绩

**项目业绩**

**项目名称： 项目编号：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目内容** | **委托单位** | **合同金额** | **业绩时间** | **联系方式** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：

1、本表可在不改变格式的情况下根据具体需要自行增减。

2、本表所列业绩作为专家评分的首要依据，未列入本表的业绩将不予认可。

投标供应商名称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

## 附件十七 诚信投标承诺书

**诚信投标承诺书**

温州市公安局交通管理局：

浙江东瓯工程造价咨询有限公司：

我公司参与 （采购项目名称、编号）投标，本公司郑重承诺：

1. 自觉遵守《中华人民共和国政府采购法》等法律法规的规定；
2. 投标文件中所提供的材料及技术参数真实有效，不存在虚假应标；
3. 保证绝不采取不正当手段诋毁排挤其他投标供应商；
4. 保证绝不向采购人、采购代理机构有关工作人员提供不正当利益,以影响采购结果的公正性。
5. 如中标，将全面忠实的履行投标文件所有响应与承诺，在规定的时间内与采购人签订采购合同。

我公司若违反上述承诺，愿接受取消投标（中标）资格及其他任何形式的处理。

投标供应商全称（盖章）：

投标供应商代表（签字）：

日 期： 年 月 日

注：▲不按要求提交本承诺书按无效标处理。

# 第四部分 采购内容及要求

## 一、 项目概况

1、项目背景

温州市公安局交通管理局（以下简称“交管局”）按照公安部、省厅关于加强公安信息中心建设的意见，全面贯彻落实国家信息安全等级保护制度，并紧密结合公安工作的现实需求，进一步明确了信息中心的业务规划、建设目标和职责任务，不断创新管理体制和用人机制，大力推进各类技术系统建设，逐步形成了高效、统一、权威的信息系统管理体系和规范有力的运行管理机制和制度。在应对未知和已知的网络信息安全风险和隐患，在基础合规前提下，并针对性地进行安全加固，从终端、服务器端、应用端、中间件、数据库层、信息制度管理层等各个方面，构建相对完善的安全保障体系，使得网络成为一个可信的计算环境进一步完善公安信息系统安全管理和技术防护体系,增强信息安全保护意识,明确信息安全保障重点,落实信息安全责任,切实提高公安系统信息安全防护能力，通过本项目实施，查找漏洞，整改隐患，为全面提高信息系统稳定运行提供安全保障。

纵观现有交管局的公安信息网、视频专网、政务外网，它承载了各级公安机关打击犯罪、维护稳定、服务群众、管理队伍等各项主要工作，汇集的业务数据和各类信息越来越重要和敏感。同时，网络安全问题也日益凸显，信息系统存在安全风险，系统被攻击破坏的隐患较大；病毒木马防御手段不多，网络边界遭到外部持续不断的渗透攻击；安全技术保障措施各自为政、缺乏联动，安全防护、安全监测和应急处置能力亟待提高。

1. 建设依据

本方案的设计过程中将按照国家的相关法律标准展开，在方案的设计过程中，既考虑满足合规要求，有符合单位的实际安全建设需求，主要依据的标准文件包含如下：

《中华人民共和国网络安全法》（2017年6月1日）

《网络安全等级保护管理条例》（征求意见稿）

《网络安全等级保护定级指南》（GB/T 22240-20XX）

《网络安全等级保护基本要求》（GB/T 22239-2019）

《网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《网络安全等级保护实施指南》（GB/T 25058-20XX）

《信息安全风险评估规范》（GB/T 20984-2007）

《电子信息系统机房设计规范》（GB/T 50174-2008）

《计算机场地安全要求》（GB/T 9361-2006）

## 安全现状

本次网络现状的分析涉及温州市公安局交通管理局（以下简称交管局）承载信息系统与业务系统的三张网络，分别为政务外网、公安网和视频专网。

政务外网主要为交管局提供互联网、电子政务网网络环境，政务外网主要分为有线网络和无线网络，无线网络涉及多种终端设备，有线网络包括传统PC、信创PC、MAC主机、网络设备、空调系统、门禁系统等，无线网络包括手机、自助终端、智能屏、移动PC、平板等设备；

视频专网与信号专网主要部署了视频网络系统与信号专网设备及与其相关的业务系统，交管局大部分视频类、信号类的调度管控工作依托于该网络进行开展。通过边界隔离交换系统，视频专网内部分业务系统数据会传输到公安网内对应应用中进行进一步的处理；

公安网主要承载着交管局大部分支撑日常工作的\*\*信息系统与数据业务系统，公安网除PC主机、服务器接入外，同时部署了虚拟化资源池，提供有效的信息资源支撑能力，辅助各类日常\*\*工作顺利进行。

## 具体采购内容及技术要求

**1、公安网服务能力要求**

**1.1 数据中心边界防护服务**

服务通过在业务系统前端部署冗余的数据中心防火墙，提供边界防御、访问控制、入侵防御、防病毒等安全能力，对数据中心进行边界保护，对所有流经数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，防范各类攻击行为，杜绝越权访问，防止非法攻击。通过合理布局，形成多级的纵深防御体系。

服务工具技术指标要求如下：

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 服务工具基础要求 | ★通过公安部检测获得销售许可证书，提供证书复印件。 |
| ★具备中国信息安全认证中心颁发的《中国国家信息安全产品认证证书》。 |
| ★具备中华人民共和国工业和信息化部颁发的《电信设备进网许可证》。 |
| 服务工具规格要求 | 标准2U专用千兆硬件平台，双交流电源；  硬盘≥1T；  接口≥12\*GE电口，≥12\*SFP光口，≥4\*SFP+光口；支持千兆接口总数≥24个，支持万兆接口总数≥4个  基本网络防火墙功能，IPSEC VPN功能，攻击防护，访问控制功能，用户认证功能，链路负载均衡功能、流量控制功能；  配置防病毒、入侵检测与防御模块； |
| 服务工具性能要求 | 设备最大吞吐量≥20 Gbps，HTTP吞吐量≥14 Gbps，IPS吞吐量≥10 Gbps，AV吞吐量≥10 Gbps，IPSec VPN性能≥3 Gbps，最大并发连接数≥500万，每秒新建连接数≥50万（默认SFP接口和SFP+接口都不带光模块），IPSec VPN隧道数≥1024，SSL VPN接入数≥3000 |
| 访问控制 | 支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、日志记录、会话老化时间、终端过滤等高级访问控制功能。 |
| 入侵防御 | 系统定义超过8000+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型。并支持在线升级和手动升级。 |
| 预置防护模板，可基于常见场景进行一键式的安全加固；支持基于常见协议进行异常检查，包括但不限于：HTTP、HTTPS、DNS、SMTP、POP3、FTP；检查内容支持自定义，包括但不限于：url长度、请求长度、目录长度、host字段、version字段、字符检测、文本长度、文件名长度、命令参数长度，支持针对每协议设置处置动作和事件等级。 |
| 支持自定义IPS特征，至少支持IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等协议自定义入侵攻击特征；可拓展协议字段，设置数据包中的匹配内容；支持选择包含、等于、不等于、大于、正则匹配等匹配方式；可选择多种匹配条件，支持设置“与”和“或”的匹配顺序；支持设置检测方向，包括双向、客户端方向和服务端方向；支持自定义选择重要等级。 |
| 病毒防护 | 支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀，支持查杀邮件正文/附件、网页及下载文件中包含的病毒，支持400万余种病毒的查杀，并支持在线升级和手动升级病毒库。 |
| ★支持对最多20级的压缩文件进行解压查杀。（须提供相关截图证明） |
| 基础防护 | 支持IPv4、IPv6双协议栈异常包攻击防御，攻击类型至少包含：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP选项、IP Spoof、Jolt2等。 |
| 至少支持telnet、ftp、imap、pop3、smtp、rlogin、http、oracle、mysql、postgres等常见协议的防暴力破解功能，针对每种协议可自定义检测时长、阈值和阻断时长。 |
| 支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习获得服务器合法的外联行为，检测流量中的异常访问流量，实现自动拦截；学习时长可选择1小时、12小时、一天、一周等。 |
| 资产安全分析 | 支持内网资产自动发现功能，开启后自动评估内网资产安全，无需人工干预。支持手动创建、导入导出资产信息。 |
| 支持展示内网资产的风险级别、IP、用户、部门、操作系统、重要程度、受攻击总数、来源等内容。 |
| 攻击链可视 | 支持安全事件攻击链分析，以资产和攻击者两种角度关联所有安全事件，将攻击过程阶段化，分析和统计每个攻击阶段的攻击内容和攻击次数，支持针对每个攻击阶段进行数据下钻，支持分析攻击时间、攻击源、攻击目的、攻击事件、检测模块、攻击级别等信息，帮助管理员清晰了解APT攻击的攻击进度，及时在数据泄露前加固网络，针对已经数据泄露的情况，进行事件回溯，为后续网络加固提供数据支撑。 |
| 应用识别 | ★应用特征不少于5000个，移动应用不少于450个。（须提供相关截图证明） |
| 支持根据标签选择应用，预置标签分类至少包含安全风险、高带宽消耗、降低工作效率等10大类；支持给每个应用自定义标签；支持根据标签选择一类应用做控制。 |
| 支持自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持DNS域名学习模式，可引用数据包特征中的目标域名或指定域名。 |
| 支持应用智能识别，有效识别P2P和迅雷行为，识别模式可选择严格、适中、宽松，支持排除扫描端口。 |
| 流量管理 | 支持基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套；支持基于地址、用户、服务、应用、时间等匹配条件进行流量控制；并支持配置保障带宽、最大带宽、每IP带宽、每用户带宽、带宽优先级等QoS动作。 |
| 支持带宽动态调整技术，带宽繁忙通道支持动态借用空闲通道的带宽，避免带宽浪费。 |
| 支持流量限额功能，可基于用户、源IP、目的IP、时间、应用等维度，进行日流量总额、月流量总额、当日使用时长、当月使用时长等限额类型进行流量管理；针对达到限额阀值的用户进行弹窗提醒，限额阀值和弹窗提醒频率支持自定义；针对超过限额的用户，管理员可选择禁止上网或者加入至惩罚流控通道。 |
| 防私接路由 | 支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断。 |
| 支持自定义配置终端数量、冻结时间和添加信任列表；支持例外排除功能，可针对终端类型分别设置阀值数量。 |
| 针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长。 |
| 认证 | 支持本地认证、Portal认证、Radius认证、LDAP认证、POP3认证、AD域单点登录、短信认证。 |
| 支持通过解析Radius、http流量，获取用户名、IP和MAC信息，实现无认证实名上线。 |
| 支持用户MAC感知，当用户MAC地址变更后，要求重新认证，避免冒名认证现象；支持伪Portal抑制技术，支持通过http302重定向或html-refresh方式抑制非正常的http或https的页面请求，从而保障系统稳定高效运行；支持基于https协议推送认证页面。 |
| 双机热备 | 支持双机热备，支持主主模式、主备模式，支持同步配置、会话、运行状态、VPN状态、特征库，支持配置抢占模式和抢占延时，支持配置HA监控接口。 |

**1.2 数据库防护服务**

数据库防护服务通过部署数据库安全网关系统。服务工具支持AIX,WINDOWS,LINUX,UNIX等主流操作系统环境中的oracle、MySQL、PostgreSQL、DB2、MSSqlserver等数据库，针对数据库攻击行为进行拦截和防护，同时提供数据库层面的虚拟补丁技术，技术人员能够提供防护策略配置，攻击行为分析及虚拟补丁修复等服务。

服务工具技术指标要求如下：

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 服务工具基础要求 | 通过公安部检测获得销售许可证书，提供证书复印件。 |
| 服务工具性能要求 | 支持对不少于16个数据库开展防护； |
| 支持数据库 | 支持oracle、MySQL、Mariadb、PostgreSQL、DB2、MSSqlserver、hive、hbase、kingbase、gbase8a、sybase、informix、MongoDB、达梦（DM）、人大金仓（KingBase）、ODPS、vertica等数据库 |
| 总览展示与告警 | 展示各个资产的访问控制情况、攻击防护情况、数据脱敏情况、设备运行情况  支持风险告警查询，且查询条件支持常见的账号、数据库名、客户端工具、操作系统用户名、客户端IP、操作类型、SQL关键字、执行结果、影响行数、执行时长等字段 |
| 敏感数据扫描 | 支持扫描发现14种敏感信息，包括身份证、银行卡、手机号、座机号、军官证、护照号、车牌号、MAC地址、日期、时间、港澳台通行证、台胞证、邮箱、中文姓名等，同时支持自定义敏感数据扫描规则。 |
| 审计功能 | 支持数据库操作类、表、视图、索引、存储过程等各种对象的所有SQL操作审计；  支持访问数据全审计，支持审计数据导出报表，审计日志支持syslog、kfaka外发。 |
| 访问控制 | 支持多种数据来源筛选管控，包括IP、客户端主机名、操作系统用户名、客户端工具名、数据库账号  ★对于越权的动作可以选择：阻断、脱敏、仅告警（提供相关截图证明）  支持与数据分级分类系统结合，实现基于身份认证和数据分级分类细粒度访问控制；  支持分组管理进行分组管控；实现资产和访问控制、身份认证直接的对应。 |
| 安全防护能力 | ★内置的特征策略包含缓冲区溢出、SQL注入、提权、数据库内核入侵探测等常见攻击特征，内置多种数据库安全规则（需提供相关截图证明）  自定义规则支持根据账号、数据库名、客户端工具、操作系统用户名、客户端IP、操作类型、SQL关键字等制定防护策略。  规则动作支持允许访问、命令阻断、会话阻断和动态脱敏；  支持数据库防护虚拟补丁技术，防护未升级数据库，并可以更新维护；  支持IP组、操作系统用户名组、客户端主机名组、客户端工具名组、数据库账号组、时间组和对象组的分组管理；  ★拦截阻断功能API化，可通过http请求供外部调用（需提供相关截图证明） |
| 系统管理 | 支持数据自动清理功能，支持根据保留天数和占用百分比自动清理最早的数据。  支持三权分立，除超级管理员外，内置系统管理员、安全管理员、审计员三种默认用户  支持SNMP获取设备信息，支持资源使用报表，支持调试工具：日志下载、连通性检测、tcpdump抓包  内置调试工具，支持连通性检测、支持TcpDump抓包工具，分析数据包情况。  支持系统安全配置如会话锁定、超时退出、IP访问控制、密码复杂性管理等安全措施。 |
| 操作日志 | 支持记录审计系统所有人员对设备的访问行为  自审计日志包含时间、用户、来源IP、操作名称、操作内容、操作结果等内容 |

**1.3 服务器虚拟补丁服务**

通过在公安网部署主机虚拟补丁系统，提供主机系统防护与加固、病毒查杀等能力。通过内核级东西向流量隔离技术，实现网络隔离与防护；拥有补丁修复、外设管控、文件审计等主机安全能力。

服务工具技术指标要求如下：

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基础要求 | | ★通过公安部检测获得销售许可证书，提供证书复印件。 |
| 服务工具规格要求 | | 包含终端管理中心软件一套，含不少于300个类服务器防护节点  实现对终端的统一管理和策略下发  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 |
| 防护功能 | 系统性能监控 | 支持对CPU使用率监控、内存占用率监控、磁盘读写监控、上下行流量监控。 |
| 支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端进行熔断。 |
| 高级威胁防护模块 | 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。 |
| 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。 |
| 对失陷后主机远控持久化行为进行检测（反弹shell、远程控制），可阻断远控。 |
| 对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为。 |
| ★可对渗透的收尾阶段的数据清除行为进行识别和阻断。（须提供相关截图证明） |
| 系统安全性模块 | 支持防端口扫描，锁定恶意的端口扫描，并记录告警。 |
| 支持系统/域控环境下的弱口令检测 |
| 支持扫描后对高危漏洞进行自动修复。 |
| 违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。 |
| 支持网站漏洞防护，防护内容包括SQL注入、XSS、应用程序漏洞及自定义规则。 |
| 支持智能检测防御CC攻击，并可进行高、中、低三档设置。 |
| 内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制。 |
| 支持流量画像，支持全网流量可视化。 |
| ★支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度（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。（须提供相关截图证明） |
| 支持显示隐藏的系统账户。 |
| 具有系统漏洞扫描和修复功能，提供真实漏洞补丁：  1.在补丁依赖关系上支持重启验证机制（保证补丁安装的稳定性）。  2.管理中心可作为补丁服务器，支持管理中心可上网和不可上网两种情况。提供离线补丁下载器，按需智能获取内网所需补丁。 |
| 具备为用户提供Windows漏洞修复的热补丁列表能力。 |
| 支持扫描的漏洞类型包括但不限于操作系统漏洞（Windows、Linux、AIX等）、数据库漏洞（MySQL等）、Web容器漏洞（Tomcat、Apache、Ngnix等）及其他组件漏洞。 |
| 云端威胁鉴定 | 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。 |
| 防病毒模块 | 支持文件实时监控，在文件执行、文件修改、存储介质连接时自动触发。 |
| 支持多种扫描模式包括极速模式、低资源占用模式设置，且低资源占用模式可自定义CPU使用率。 |
| 支持多引擎设置，包括默认引擎、深度扫描引擎。 |
| 支持对压缩包扫描及深度进行设置，默认9层深度。 |
| 支持对文件扫描进行跳过，默认50M以上文件进行跳过。 |
| 支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并将修复前的病毒文件进行备份。 |
| 支持对顽固流行病毒进行智能拦截。 |
| 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 |
| 提供专门的勒索风险评估功能。 |
| 提供专门的针对已知勒索病毒的防御引擎，并提供功能开关项。对于已知勒索病毒确保进程无法启动。 |
| 提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。同时支持白名单设置。 |
| 提供专门的挖矿风险评估工具。 |
| 提供专门的挖矿实时防御工具，并提供功能开关。 |
| 弹窗拦截 | 支持在客户端自定义设置需要拦截的弹窗 |

**1.4 大数据智能分析服务**

服务通过部署服务工具大数据分析平台，对全网的安全设备的安全数据进行收集，通过日志审计整合告警数据，通过网闸单向导入到公安网的大数据分析平台内，运用大数据分析建模及人工分析，为交管局用户发现潜在的入侵和高隐蔽性攻击，回溯攻击历史，对全网进行安全态势感知和展示，预测即将发生的安全事件，并通过该服务对公安网现网所有安全系统安全数据进行统一管理和感知，提升安全运维效率。

服务工具技术指标要求如下：

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基础要求 | | ★通过公安部检测获得销售许可证书，提供证书复印件。 |
| 服务工具规格要求 | | 规格：2U，2物理CPU ≥24核，内存≥256GB，配置企业级存储磁盘总容量≥24TB（或磁盘可用容量≥20TB），≥2GB RAID卡，冗余1+1电源模块，≥1G RJ45\*4，滑轨；  接口要求：千兆电口≥4个。 |
| 服务工具性能要求 | | 数据采集和处理性能≥1200EPS，每条数据大小>1KB；  可接收全流量吞吐量≥2Gbps；  接入日志源不少于200个；  10亿数据关键字查询结果响应时间<2秒；  支持≤ 2 GB的镜像流量。 |
| 数据接入 | | 1. 支持通过多种类型的安全、泛安全类数据接入采集，应包括但不限于设备日志数据、流量数据、弱点漏洞数据、系统性能数据、威胁情报数据、资产人员数据； 2. 支持通过流量采集设备采集接入全流量数据，包含流量中的请求包和返回包等信息，并可在数据检索中体现包信息； 3. 支持接入文本格式、CVS等格式的文件数据，可通过模板文件的填写导入实现资产数据的导入和管理； 4. 支持通过云端对接、本地导入或手动编辑的方式，接入威胁情报数据。 |
| 安全检测能力 | 行为审计与  可疑通信检测 | 1. 支持违规操作、违规访问、违规应用、违规外发等300种以上行为审计检测规则，可针对任意单条规则进行启用和禁用。 2. 支持隧道通信、可疑内容、恶意IP、恶意域名、恶意证书、远程控制等3000种以上可疑通信检测规则，可针对任意单条规则进行启用和禁用。 |
| 扫描探查检测 | 1. 支持端口扫描、服务扫描、Web扫描、扫描器指纹检测等300种以上的扫描探查检测规则，可针对任意单条规则进行启用和禁用。 |
| 漏洞利用检测 | 1. 支持SMB漏洞、RDP漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、shellcode等7000种以上漏洞利用检测规则，可针对任意单条规则进行启用和禁用。 |
| 恶意文件检测 | 1. 支持挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell等25000种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用。 |
| 配置风险检测 | 1. 支持弱口令风险、明文传输风险、HTTP配置风险、中间件配置风向、数据库配置风险、服务配置风险等100种以上配置风险检测规则。 |
| 主机和账号异常检测 | 1. 支持端口异常、主机对外扫描、主机对外攻击等主机异常检测能力，对任意单条检测规则支持启用和禁用。 2. 支持登录异常、暴力破解、行为异常等账号异常检测能力，对任意单条检测规则支持启用和禁用。 |
| Web攻击检测 | 1. 支持Webshell请求、XSS攻击、SQL注入、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、信息泄露、越权访问、XXE注入、网页篡改等13类、6000种以上web攻击检测规则，对任意单条检测规则支持启用和禁用。 |
| 安全分析能力 | 安全分析模型 | 1. 平台应内置包括规则模型、关联模型、统计模型、情报模型、离线模型等在内的≥5大类安全分析模型。 2. 安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容。 3. ★支持对安全日志里200个以上字段，包括但不限于应用协议、目的IP、目的主机名、目的端口、目的用户名、数据流方向、情报IOC等进行任意形式的逻辑与或非形式组合建模，运算方式包括但不限于AND、OR、等于、不等于、大于、小于、属于、不属于、存在、不存在等，并能根据组合方式自动生成运算表达式。（须提供相关截图证明） |
| 安管协作 | 1. ★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。（提供第三方机构证明材料） 2. 支持多级管理员间资产风险信息的隔离和共享，总部用户管理员可以分配下属组织架构的功能权限，支持按月和按周考核各组织架构的安管工作成果。 3. 分部安全管理员只可以使用所属组织架构具备的功能，只能管理与分析所属组织架构的资产和数据，分部具备单独的态势感知大屏； |
| 网络实体分析画像 | 1. 实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型过滤关联关系，支持通过一键溯源进行威胁关系的自动拓展。 2. 支持与终端检测类产品对接，查看主机进程、软件版本、漏洞病毒情况。 |
| 调查取证 | 场景化分析 | 1. 支持暴力破解、Web攻击、恶意程序、端口扫描等内置安全分析场景，基于场景特性进行默认条件的数据聚合分析，支持至少3个任意字段的快速聚合分析，聚合后的所有数据均支持快速统计分析，展示统计排序信息，支持分析结果导出。 2. 支持自定义场景安全分析，可对安全告警的任意字段进行聚合分析，支持的聚合的字段不少于300个，支持分析结果导出。 3. 支持智能检索语句分析，支持检索语句的中英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，历史检索语句快速导入；检索语句可直接发布成实时分析模型，对实时数据进行分析与告警。 |
| 取证分析 | 支持调查场景的四维自定义攻击流向图取证，攻击趋势取证、攻击链分布取证、和实体信息取证，展示攻击者和受害者的威胁情报与资产信息，可联动会话详情，点击查看不同溯源维度的会话详情，通过请求头，payload等详情字段定位攻击。 |
| 可视化安全分析 | 安全态势可视化 | 1. 支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示，提供不少于10块大屏展示界面 。 2. 支持立体、平面、球面等多种维度的网络实体关系透视，可在大屏上展示不同实体的标签属性，包括但不限于DNS服务器、监管单位、邮件服务器、黑客组织、WEB服务器等。 |
| 数据字典管理 | 1. 支持管理系统中原始日志、异常记录、安全告警的所有字段和取值，每个字段均有清晰的说明。 2. 支持数据标准管理，用户可以根据实际需求，对字典进行编辑，支持手动修改、增加或删除相应的字段。 3. 数据字典支持管理系统中原始日志和告警数据中所有字段的类型、取值范围、字段说明，支持数值、字符串、枚举、ip等≥9种字段类型。 |
| 威胁情报 | 1. 支持通过离线导入或手动编辑添加的方式，形成本地威胁情报，允许用户自建行业情报库，并实现情报库的增删改查、导入、导出功能。 2. 情报记录包含情报置信度、标签、组织名称、地理位置、运营商等信息。 3. 支持查看情报源中有效情报数量、最近更新时间、今日更新情报数量。 4. 情报查询支持通过IOC同时跨越多个情报源查询，结果汇总展示。 5. 碰撞情报IOC支持通过情报源、IOC类型、标签、置信度等多维度进行碰撞分析，内置威胁情报条数不少于400万条。 |
| 资产管理 | 1. 支持通过流量无侵入式自动发现资产，支持发现终端、Web服务器、DNS服务器、邮件服务器、FTP文件服务器等类型≥5种，其中web服务器支持自动识别服务域名和服务站点名称。 2. ★支持通过离线导入或手动编辑添加的方式，形成本地威胁情报，允许用户自建行业情报库，并实现情报库的增删改查、导入、导出功能，情报记录包含运营商、IOC类型、标签、置信度等，并支特统计情报源命中情报数量，针对单条无效情报可实现删除（提供第三方机构检测报告证明）。 3. 支持一键访问安全设备的管理界面、监控大屏、设备日志、处置联动记录。 4. 支持以单个IP地址、IP区间、子网掩码等3种模式录入安全域信息。 |
| 安全运营 | 1. 支持统一的安全运营工作台，在工作台可以集中查看当前用户的待办工单、最新通报预警状态。 2. 工单详情与备注支持多种内容格式，包括但不限于文字、图片、超链接、表格、代码片段、附件等类型。 3. 支持工单举证信息一键溯源，工单处置人员可以直接定位到工单关联的原始信息进行查看。 4. 支持通过安全告警自动派发工单到对应的安全管理员，支持自定义编辑预警信息内容。 5. 支持将预警信息直接转为内部通报，支持将通报内容作为工单定向指派。 |
| 系统管理 | 一站式运维 | 1. 支持大数据平台本身的计算、存储资源利用率监控。 2. 支持数据集与数据索引健康度监控。 3. 支持对平台各组件运行健康状态的集中监控。 4. 支持平台运行状态告警，运行监测引擎可独立于安全分析引擎工作，展示运维告警趋势、分布等。 5. ★支持大数据平台一键巡检，一键检查项包含但不限于数据健康、探针健康检查、大数据集群健康、Elasticsearch健康、实时流计算引擎健康、管理服务健康、服务器节点健康等多种维度检查，并能提供处置建议，一键导出各类服务的故障日志，包括但不限于Elasticsearch、Logstash、Ka\*\*a、实时计算引擎、操作系统等。（须提供相关截图证明） |
| 用户管理 | 1. 提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持根据对象属性自定义划分系统管理角色和一般用户角色，按照数据和功能分级灵活设置用户权限。 |
| 开放接口 | 平台开放API接口，第三方平台可通过OpenAPI获取平台的关闭规则、资产信息、联动策略等接口信息进行对接。 |
| 采集模块 | 日志采集解析 | 1. 日志采集方式应支持但不仅限于Syslog、ka\*\*a、ftp、部署代理等4种方式。 2. 支持采集异构设备的日志数据，实现包括但不限于安全类、网络类、应用服务器类、操作系统类等至少4大类、50种设备的日志接入采集。 3. 支持接入应用服务器的性能类数据，包括但不限于CPU、内存和磁盘的性能告警数据。 4. 内置解析规则支持厂商>100家，支持解析日志设备型号>2000种。 5. 无需配置解析规则与设备日志对应关系，自动完成解析。 6. 支持日志源≥200个。 7. 可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息，≥30个字段。 8. 具备同时保存事件原始日志数据和标准化后日志数据的能力。 |

**1.5 流量检测服务**

流量检测服务通过在公安网部署的检测探针，实时发现由外到内和由内到外的网络攻击行为。服务将实时发现网络中发生的各种已知威胁和未知威胁。技术人员将定期对入侵行为进行分析，发现公安网内威胁源头并输出报告。

服务工具技术指标要求如下：

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务工具规格要求 | 软硬一体化2U标准机架式设备；  1+1冗余电源 ；  内存≥16G ；  硬盘容量≥2T；  接口数量不少于 6个；  接口类型：千兆RJ45网口不少于2个(管理口不少于2个)、千兆RJ45网口不少于4个； |
| 服务工具性能要求 | MTBF 大于65000小时；  吞吐率≥1Gbps； |
| 高可用性 | 部署方式：旁路镜像模式部署，不影响服务器处理性能和网络架构。  运行监控： 可监控系统CPU、内存、磁盘使用情况、网口状态、网口流量、网口丢包情况及数据外送量大小情况。 |
| 数据同步 | 支持通过KA\*\*A接口向态势感知平台报送流量审计数据与风险告警信息。  自定义配置：可在前端页面自定义配置探针与大数据平台之间的数据传输类型、各类型数据均支持任意字段的发送配置。 |
| 行为审计与  可疑通信检测 | 支持违规操作、违规访问、违规应用、违规外发等300种以上行为审计检测规则，可针对任意单条规则进行启用和禁用。  支持隧道通信、可疑内容、恶意IP、恶意域名、恶意证书、远程控制等3000种以上可疑通信检测规则，可针对任意单条规则进行启用和禁用。 |
| 扫描探查检测 | 支持端口扫描、服务扫描、Web扫描、扫描器指纹检测等300种以上的扫描探查检测规则，可针对任意单条规则进行启用和禁用。 |
| 漏洞利用检测 | 支持SMB漏洞、RDP漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、shellcode等7000种以上漏洞利用检测规则，可针对任意单条规则进行启用和禁用。 |
| 恶意文件检测 | ★具备挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell、恶意邮件等17000种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用。（须提供相关截图证明） |
| 配置风险检测 | 支持弱口令风险、明文传输风险、HTTP配置风险、中间件配置风向、数据库配置风险、服务配置风险等100种以上配置风险检测规则。 |
| 主机和账号异常检测 | 支持端口异常、主机对外扫描、主机对外攻击等主机异常检测能力，对任意单条检测规则支持启用和禁用。  支持登录异常、暴力破解、行为异常等账号异常检测能力，对任意单条检测规则支持启用和禁用。 |
| Web攻击检测 | ★支持Webshell请求、XSS攻击、SQL注入、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、信息泄露、越权访问、XXE注入、网页篡改、SSRF攻击等16类Web攻击检测，具备9000种以上Web攻击检测规则，对任意单条检测规则支持启用和禁用。支持基于语义分析的SQL注入精准检测。（须提供相关截图证明） |
| 规则库管理 | 威胁检测规则支持页面查看，具备中文相关介绍，包括但不限于漏洞名称，危险等级，影响系统，对应CVE编号。  支持基于规则ID、规则名称、CVE编号、规则等级、规则类型、规则状态、应用协议等不同条件进行规则快速检索。 |
| 策略管理 | 支持IP与地理信息映射，用户可新增指定IP或IP段的地理信息，支持IP或IP段地理信息导入导出，确保输出数据地理信息准确。  支持IP NAT配置管理、flow数据清洗管理。 |
| 系统管理 | 支持与态势感知平台进行数据同步，同步信息包括安全域、内IP等。  支持前端可视化配置管理接口、监听接口，包括修改IP地址、启用禁用监听接口等。  支持前端可视化进行设备运维操作，包括重启设备、关机重启服务、开关SSH服务等，可一键下载探针运行日志，方便运维人员日常运维工作。 |

**1.6 日志分析服务**

日志分析服务通过在公安网部署的日志审计系统和复用大数据分析平台的日志审计能力进行日志的存储和分析，服务通过归集网络中各类设备及应用日志信息，进行日志记录的统一收集、存储、分析、查询、审计和报表输出，并将归集后的日志和告警信息同步给安全运营中心做进一步的通报和展示。

服务工具技术指标要求如下：

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务工具基础要求 | ★通过公安部检测获得销售许可证书，提供证书复印件。 |
| 服务工具规格要求 | 标准1U硬件，不少于1个console口；  内存≥8GB，硬盘≥2TB（2T\*1）；  网口类别：不少于6个千兆工作管理口(1管理口+1HA口+4审计口)  网络端口：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。 |
| 服务工具性能要求 | 审计性能：支持审计不少于25个日志源；  日志处理能力EPS≥4000/秒，峰值处理能力≥5000/秒。 |
| 日志收集 | 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集。 |
| 可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。 |
| 支持使用代理(Agent)方式提取日志并收集；安装包支持界面下载，且安装支持可视化向导。 |
| 支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。 |
| 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等； |
| 支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。 |
| 日志分析 | 可以基于日志等级进行过滤。 |
| 可以通过自定义配置过滤掉用户不关心的日志。 |
| 支持对收集到的重复日志进行自动聚合归并，减少日志量。 |
| 支持可由用户定义和修改的日志聚合归并逻辑规则。 |
| 支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备。 |
| 日志支持文本方式输出给第三方平台，进行数据共享。 |
| 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展。 |
| 支持基于跨设备的多事件关联分析。 |
| 具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。 |
| 内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景。 |
| 进行关联分析的规则可定制。 |
| ★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。（须提供相关截图和第三方检测机构检测报告证明） |
| 日志备份 | 可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比等策略。 |
| 支持日志本地备份及恢复。 |
| 支持日志备份自动传送到远程服务器。 |
| 支持从远程仓库恢复数据。 |
| 支持FTP、SAMBA、NFS和FILE，4种方式的远程服务器。 |
| 应用性能监控  （APM） | 支持监控设备自身CPU、内存、磁盘等工作运行状况。 |
| ★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。（须提供相关截图和第三方检测机构检测报告证明） |
| 支持以下对象的性能监控：  操作系统 - Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris  数据库 - MySQL、Oracle  应用服务器 - Weblogic、Tomcat  Web服务器 - Apache |
| 支持应用性能历史详情回溯查看。 |
| 告警功能 | 可预设置安全告警策略。 |
| 支持数据阀值设置，超过阀值将产生告警。 |
| 可以通过邮件、短信和屏幕显示进行告警。 |
| 自动防止在短时间内大量发送报警信息(告警抑制)。 |
| 具备报警合并和在一个时间段内抑制报警次数的能力。 |
| ★支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警。（须提供相关截图证明） |
| 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 |
| 系统自带自身管理日志。 |
| 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。 |
| 提供一键式故障排除功能。 |
| 提供自助式的升级接口，支持升级、规则升级。 |
| 资产管理 | 注册用户资产时，提供自动发现识别能力。 |
| ★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。（须提供相关截图和第三方检测机构检测报告证明） |

**2、视频专网服务能力要求**

**2.1 日志分析服务**

日志分析服务通过在视频专网部署日志采集探针，归集网络中各类设备及应用日志信息，进行日志记录的统一收集、存储、分析、查询、审计和报表输出，并将归集后的日志和告警信息同步给安全运营中心做进一步的通报和展示。

服务工具技术指标要求如下

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务工具基础要求 | ★通过公安部检测获得销售许可证书，提供证书复印件。 |
| 服务工具规格要求 | 标准2U硬件；  内存≥8GB，硬盘≥2TB（2T\*1）；  网口：不少于6个千兆工作管理口（1管理口+1HA口+4审计口)，不少于1个console口  网络端口：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。 |
| 服务工具性能要求 | 审计性能：支持审计不少于100个日志源；  日志处理能力EPS≥4000/秒，峰值处理能力≥5000/秒。 |
| 日志收集 | 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集。 |
| 可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。 |
| 支持使用代理(Agent)方式提取日志并收集；安装包支持界面下载，且安装支持可视化向导。 |
| 支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。 |
| 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等； |
| 支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。 |
| 日志分析 | 可以基于日志等级进行过滤。 |
| 可以通过自定义配置过滤掉用户不关心的日志。 |
| 支持对收集到的重复日志进行自动聚合归并，减少日志量。 |
| 支持可由用户定义和修改的日志聚合归并逻辑规则。 |
| 支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备。 |
| 日志支持文本方式输出给第三方平台，进行数据共享。 |
| 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展。 |
| 内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景。 |
| 进行关联分析的规则可定制。 |
| ★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。（须提供相关截图和第三方检测机构检测报告证明） |
| 日志备份 | 可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比等策略。 |
| 支持日志本地备份及恢复。 |
| 支持日志备份自动传送到远程服务器。 |
| 支持从远程仓库恢复数据。 |
| 支持FTP、SAMBA、NFS和FILE，4种方式的远程服务器。 |
| 应用性能监控  （APM） | 支持监控设备自身CPU、内存、磁盘等工作运行状况。 |
| ★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。（须提供相关截图和第三方检测机构检测报告证明） |
| 支持以下对象的性能监控：  操作系统 - Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris  数据库 - MySQL、Oracle  应用服务器 - Weblogic、Tomcat  Web服务器 - Apache |
| 支持应用性能历史详情回溯查看。 |
| 告警功能 | 可预设置安全告警策略。 |
| 自动防止在短时间内大量发送报警信息(告警抑制)。 |
| 具备报警合并和在一个时间段内抑制报警次数的能力。 |
| ★支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警。（须提供相关截图证明） |
| 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 |
| 系统自带自身管理日志。 |
| 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。 |
| 提供一键式故障排除功能。 |
| 提供自助式的升级接口，支持升级、规则升级。 |
| 资产管理 | 注册用户资产时，提供自动发现识别能力。 |
| ★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。（须提供相关截图和第三方检测机构检测报告证明） |

**2.2 流量检测服务**

流量检测服务通过在视频专网部署的流量分析探针，实时发现由外到内和由内到外的网络攻击行为。服务基于丰富的特征库实时发现网络中发生的各种已知威胁和未知威胁。技术人员将定期对入侵行为进行分析，发现公安网内威胁源头并输出报告。

服务工具技术指标要求如下：

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基础要求 | | ★通过公安部检测获得销售许可证书，提供证书复印件。 |
| 服务工具规格要求 | | 软硬一体化1U标准机架式设备  电源：单电源  CPU≥2核4线程  硬盘容量≥1T  内存≥8G  接口数量：不少于6个  管理口：千兆RJ45网口≥2个  业务口：千兆RJ45网口≥4个  MTBF大于65000小时 |
| 服务工具性能要求 | | 吞吐率：网络层≥500Mbps、应用层≥100Mbps  WEB检测：HTTP最大并发数1万/秒  邮件检测：邮件处理数: ≥50万封/24小时  支持管理节点≥5个  文件检测≥1万个/24小时 |
| 综合功能 | 全流量检测 | 支持全流量检测，可根据需求打开或关闭全流量检测功能 |
| 风险数据包保存 | 支持风险数据包保存功能，可存留会话的请求和相应数据包，帮助用户还原攻击过程，进行取证和关联分析；并支持系统内置wireshark组件在线预览风险数据包 |
| 数据包去重 | 支持数据包去重功能，在原始流量存在重复包的情况下能够自动剔除重复的数据包，确保分析结果的准确性，数据包去重功能不影响设备的处理性能 |
| 审计协议 | 支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW V9等协议报文（HTTPS、SMTPS、POP3S、IMAPS加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号；  支持识别QQ、WEB、LDAP、FTP、TELNET、邮件、SMB、RADMIN、ORACLE、MSSQL、SYBASE、MYSQL、DB2、postgreSQL、REDIS等登录行为；  支持多层 VLAN、VXLAN、MPLS、GRE、VN-Tag等网络流量的解析检测 |
| 检测风险类别 | 支持检测WEB攻击、恶意文件攻击、远程控制、WEB后门访问、行为分析、DGA域名请求、SMB远程溢出攻击、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为、漏洞利用、邮件社工攻击、ARP欺骗、密码明文形式传输等行为 |
| 告警黑白名单过滤 | 支持文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑IP白名单、域名白名单、客户端IP白名单、服务端IP白名单、WEB特征风险白名单、IDS规则白名单的配置 |
| 弱口令风险检测 | 支持对HTTP、IMAP、SMTP、POP3、Redis、Telnet、FTP等协议的弱口令检测 |
| WEB登录 | 支持自定义HTTP登录行为的用户名获取来源，包括但不限于请求头、URL、Cookie、POST-body；支持自定义配置状态码、返回内容与登陆成功/失败状态的绑定关系。 |
| 暴力破解检测 | 支持自定义启用/禁用暴力破解模型；并支持自定义配置模型统计周期、登录次数、聚合维度、检测机制等参数 |
| 拒绝服务攻击检测 | ★支持自定义启用/禁用拒绝服务攻击模型；并支持自定义配置模型统计周期、单包长度阈值、统计周期内包数量阈值等参数（须提供相关截图证明） |
| ARP欺骗检测 | 支持根据MAC与IP地址的绑定关系，分析网络中的ARP流量，判断ARP应答包中的IP和MAC地址是否匹配 |
| 文件攻击检测 | 解析协议 | 支持 HTTP、FTP、SMB、SMTP、POP3、IMAP、NFS、TFTP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输文件检测 |
| 动态沙箱检测 | 对存在恶意行为的文件输出完整的二进制动态分析报告  动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险  可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量、返回结果、返回值等信息  可显示文件运行过程中企图访问的IP、域名，以及域名及对应的IP  ★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（须提供相关截图和第三方机构证明）  采用多并发沙箱检测技术，集成主流的操作系统winXP、win7、win10、linux等多种检测环境，拥有多项自主研发技术和专利。结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析 |
| 自定义YARA规则设置 | 支持导入自定义YARA规则，可从静态文件和运行内存中检测文件威胁。  支持单个规则或多个规则累加告警  支持从规则状态、类型、等级、描述等方面进行自定义配置 |
| 失陷主机检测 | 远程控制检测 | 支持根据威胁情报、DGA域名请求、IDS规则、用户配置数据，发现被远程控制的内部主机 |
| DGA域名请求检测 | 具备DNS协议解析功能，发现发起DGA域名请求的失陷主机 |
| 挖矿行为检测 | 可发现利用失陷主机挖矿的行为 |
| 失陷主机分析 | 支持以失陷主机维度进行分析，分析内容包括失陷主机IP、MAC地址、攻击类型、访问次数、攻击开始时间、攻击结束时间 |
| 管理功能 | 资产识别和管理 | 支持对流量中的IP地址、端口等进行统计，快速识别未登记资产。可基于特定应用或服务对内部资产进行梳理（系统类型、IP、域名、端口等），查看资产端口暴露情况，特别是以非标端口提供的服务情况；可深入识别运行在资产上的设备类型、应用、服务信息详细情况（类型、版本、服务名称等） |
| NAT地址解析 | 支持自定义NAT转换前的IP字段名和字段位置，最多支持5个，并支持对字段名进行优先级排序；可配置不会被NAT转换的代理服务器资产IP |
| 一键登录排错 | ★支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、信息收集等功能。（须提供相关截图证明）  支持在页面实时查看物理内存、共享内存、硬盘分区、硬盘I/O、监听端口、内存占用TOP10进程、CPU占用TOP10进程，无需登录后台，提高设备安全性  支持自定义时间查询和导出设备内存、CPU、磁盘空间的使用状态日志 |
| 可视化展示 | 导航：支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP流量、DNS流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示  失陷主机：支持大屏展示失陷主机风险态势，包括失陷主机视角/横向攻击视角、失陷主机/黑客组织TOP5、风险类别排名、回连区域排名、失陷主机事件统计柱状图、最新事件、失陷主机数，支持实时数据自动刷新  攻击溯源：支持大屏展示风险较为严重的事件，并进行攻击溯源，包括攻击主机个数最多的情报事件TOP10、威胁情报告警类型分布、3D攻击关系图、威胁活动（弱点探测、渗透入侵、获取权限、命令与控制、数据盗取）；支持按IP搜索关联的攻击事件，包括攻击拓扑图、攻击者基本信息、被攻击者信息、攻击过程（攻击过程列表内容包括时间、攻击者、被攻击者、攻击链阶段、风险标签、攻击次数） |

**2.3 运维审计服务**

运维审计服务通过部署堡垒机在视频专网，对运维人员的运维操作进行统一审计和权限控制。在运维人员访问设备进行安全运维前，需通过访问控制使操作人员统一先访问堡垒机，再通过堡垒机登录目标主机，起到运维审计的效果。

服务工具技术指标要求如下：

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基础要求 | | ★通过公安部检测获得销售许可证书，提供证书复印件。 |
| 服务工具规格要求 | | 授权资产不少于100个  硬件性能：并发字符连接最大100个  并发图形连接最大20个  软件功能：功能无限制 |
| 服务工具性能要求 | | 机箱高度：1U  标配网口：≥2\*GE电管理口，≥4\*GE电业务口  单硬盘，硬盘容量≥2T  ≥1个RJ45串口，单电源 |
| 用户管理要求 | 用户角色 | 支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。支持自定义用户权限。 |
| 身份认证方式 | 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 |
| 单点登录认证 | 支持标准化对接CAS、JWT单点登录认证，且支持配置是否自动创建堡垒机中不存在用户。 |
| 多用户双因子认证 | 基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证 |
| 多种认证组合使用 | 支持域认证与双因子认证结合使用，如同时使用AD/LDAP用户名+AD/LDAP密码+手机APP动态口令登录堡垒机、同时使用AD/LDAP用户名+AD/LDAP密码+短信口令登录堡垒机 |
| 用户密码及登录策略设置 | 可以设置用户密码的长度、复杂度、相关度，其中相关度可以设置密码与用户名的关系，可以选择是否检查历史密码。并可支持密码过期前告警；可设置用户密码错误达到一定次数后的锁定时长及登录失败次数的重置时间 |
| 设备管理要求 | 支持的协议和应用 | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具 |
| IE/谷歌浏览器代填 | ★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（须提供第三方机构证明） |
| URL访问管控 | 支持对http/https类资产进行URL黑白名单限制，禁止在未授权情况下，通过手动输入URL跳转至其它web网站 |
| 自动收集和自动授权 | ★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（须提供第三方机构证明） |
| 数据库管理 | 数据库兼容性 | 标准支持DB2、oracle、mysql、sqlserver、PG、人大金仓、达梦数据库的协议运维代理，可实现自动登录，自动登录可直接调用本地windows系统的数据库客户端工具（包括ssms、sqlwb、workbench、mysql、DbVisualizer、plsql、sqlplus、toad、dbcmd、Quest Central、pgadmin3、psql、ksql、Isql、DIsql、DMmanger等），无需应用发布前置机 |
| 数据库命令管控 | 数据库支持命令阻断功能，精确到数据库，表、字段级别 |
| 数据库双重审计 | 支持同时对数据库会话记录图形审计及命令提取 |
| 数据库双向审计 | 支持对数据库运维会话的上行和下行命令进行审计 |
| 自动改密要求 | 主机自动改密 | 支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能，且自动改密不借助于Agent，无需开放445、135、139等高危端口 |
| 完善的改密机制 | 支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、密码恢复、手工验证密码、调试改密等;支持邮件、FTP、SFTP等发送方式，改密后的密码可支持加密分段发送；支持对进行中任务实时停止。 |
| 运维方式要求 | 运维管理 | 支持B/S架构进行堡垒机运维管理，至少支持使用IE、谷歌、火狐、Microsoft Edge等浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等本地运维客户端工具 |
| 专用客户端运维 | 支持Windows/Mac操作系统下C/S架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作。 |
| 运维客户端自带运维工具，可不依赖 xshell/Securecrt/mstsc等工具进行运维操作 |
| 客户端还至少需支持资产分组、资产连通性检测，批量运维、资产运维审批、命令审批、二次运维审批等能力。其中资产分组操作支持个性化设置，即每个运维人员可单独设置分组，相互之间独立。 |
| 客户端支持VPN登录功能 |
| H5运维 | H5运维方式：支持ssh、telnet、rlogin、rdp、vnc协议的H5运维，无需本地运维客户端工具 |
| H5运维方式支持在线会话协同，即运维人员可自行邀请堡垒机用户共同运维同一会话，邀请人数不限，但单个邀请链接仅能邀请一人 |
| H5运维方式下，可支持RDP/SSH在线文件传输，无需借助第三方客户端工具，通过web页面即可 |
| 客户端工具登录 | 客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty/winscp/Xftp等客户端工具登录堡垒机访问图形、字符或SFTP、FTP设备 |
| SSH网关代理直连 | 支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备 |
| 审计日志要求 | 运维审计日志 | 支持对运维操作会话的在线监控、实时阻断；支持录像回放、支持记录起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志 |
| 禁审功能 | 支持提供禁止审计功能，可对部分设定策略的会话不审计录像，防止机密信息二次泄漏 |
| RDP文字记录 | 支持对RDP屏幕文字内容、标题窗口、键盘输入的记录和搜索定位 |
| SQL记录 | 支持审计主流数据库（如DB2、oracle、mysql、sql server、PG、人大金仓、达梦）运维中的SQL语句，可进行关键信息定位查询，并可过滤数据库客户端自动发起的语句，方便查询真实人为的数据库操作 |
| 安全策略要求 | 运维规则策略 | 支持通过基于时间、IP/IP段、用户/用户组、主机组、主机账号、命令控制策略等组合访问控制策略，授权用户可访问的目标设备。 |
| 运维二次审批 | 对重要设备启用登录审核功能，运维人员须向管理员申请登录，管理员允许之后才可登录；并且管理员在审批时可以设置审批有效期，及在有效期内是否不限制登录次数。 |
| 命令审批 | ★支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。（须提供第三方机构证明） |
| 水印功能 | H5运维及查看录像全程支持水印功能 |

**2.4 服务器虚拟补丁服务**

通过在公安网部署主机虚拟补丁系统，提供主机系统防护与加固、病毒查杀等能力。通过内核级东西向流量隔离技术，实现网络隔离与防护；拥有补丁修复、外设管控、文件审计等主机安全能力。

服务工具技术指标要求如下：

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **技术要求** |
| 服务工具基础要求 | | ★通过公安部检测获得销售许可证书，提供证书复印件。 |
| 服务工具规格要求 | | 包含终端管理中心软件一套，含124个类服务器防护节点  实现对终端的统一管理和策略下发  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 |
| 防护功能 | 系统性能监控 | 支持对CPU使用率监控、内存占用率监控、磁盘读写监控、上下行流量监控。 |
| 支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端进行熔断。 |
| 高级威胁防护模块 | ★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。（须提供相关截图证明） |
| 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。 |
| 对失陷后主机远控持久化行为进行检测（反弹shell、远程控制），可阻断远控。 |
| 对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为。 |
| ★可对渗透的收尾阶段的数据清除行为进行识别和阻断。（须提供相关截图证明） |
| 系统安全性模块 | 支持防端口扫描，锁定恶意的端口扫描，并记录告警。 |
| 支持系统/域控环境下的弱口令检测 |
| 支持扫描后对高危漏洞进行自动修复。 |
| 支持网站漏洞防护，防护内容包括SQL注入、XSS、应用程序漏洞及自定义规则。 |
| 支持智能检测防御CC攻击，并可进行高、中、低三档设置。 |
| 内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制。 |
| 支持流量画像，支持全网流量可视化。 |
| 支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度（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。 |
| 支持显示隐藏的系统账户。 |
| 具有系统漏洞扫描和修复功能，提供真实漏洞补丁：  1.在补丁依赖关系上支持重启验证机制（保证补丁安装的稳定性）。  2.管理中心可作为补丁服务器，支持管理中心可上网和不可上网两种情况。提供离线补丁下载器，按需智能获取内网所需补丁。 |
| 具备为用户提供Windows漏洞修复的热补丁列表能力。 |
| 支持扫描的漏洞类型包括但不限于操作系统漏洞（Windows、Linux等）、数据库漏洞（MySQL等）、Web容器漏洞（Tomcat、Apache、Ngnix等）及其他组件漏洞。 |
| 云端威胁鉴定 | ★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。（须提供相关截图证明） |
| 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。 |
| 防病毒模块 | 支持文件实时监控，在文件执行、文件修改、存储介质连接时自动触发。 |
| 支持多种扫描模式包括极速模式、低资源占用模式设置，且低资源占用模式可自定义CPU使用率。 |
| 支持多引擎设置，包括默认引擎、深度扫描引擎。 |
| 支持对压缩包扫描及深度进行设置，默认9层深度。 |
| 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 |
| 提供专门的勒索风险评估功能。 |
| 提供专门的针对已知勒索病毒的防御引擎，并提供功能开关项。对于已知勒索病毒确保进程无法启动。 |
| 提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。同时支持白名单设置。 |
| 提供专门的挖矿风险评估工具。 |
| 提供专门的挖矿实时防御工具，并提供功能开关。 |
| 弹窗拦截 | 支持在客户端自定义设置需要拦截的弹窗 |

**3 政务外网安全服务能力要求**

**3.1** **日志审计服务**

通过在政务外网部署日志审计系统，提供政务外网内网络设备的日志收集、审计能力，提供日志的保留、分析及相关安全服务。

服务工具技术指标要求如下：

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 性能要求 | 性能参数：默认包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，可用存储量≥2TB（RAID1 模式），平均每秒处理日志数（eps）最大性能≥1200。  硬件参数：规格：2U，内存大小≥16G，硬盘容量≥64G minisata+2T SATA\*2，电源：单电源，接口：支持不低于6千兆电口+2万兆光口SFP+。  含：日志审计分析管理系统软件V3.0(\*1套);  万兆多模-850-300m-双纤(\*2个); |
| 日志采集 | 支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Ka\*\*a等多种方式完成日志收集； |
| 支持接入TLS加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。 |
| 日志标准化 | 支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。 |
| 日志过滤 | ★支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。（需提供产品功能截图证明） |
| 日志转发 | 支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和ka\*\*a方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志 |
| 全文检索 | ★支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；（需提供产品功能截图证明） |
| 支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等。 |
| 支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析。 |
| 日志分析 | 支持自定义审计规则与关联规则，支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上。 |
| 资产管理 | 支持对IPv4/ipv6对象的自动发现功能，对自动发现的设备可以修改、删除或转为资产。 |
| 日志告警 | 支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件。 |
| 日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量。 |
| 系统管理 | 提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持IP免登录，指定IP免认证直接进入平台；支持只允许某些IP登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持usb-key认证。 |
| 支持个性化定制，支持全系统更换logo与系统名称，支持一键恢复默认。 |

**3.2 政务外网流量采集服务**

通过在政务外网部署流量采集工具，采集网络流量，支持已有态势感知分析平台，提供相关安全服务。

服务工具技术指标要求如下：

|  |  |
| --- | --- |
| 功能项 | 功能要求说明 |
| 性能指标 | 性能参数：吞吐性能≤500Mbps。  硬件参数：规格：1U，内存大小≥16G，硬盘容量≥128G MSATA+4T SATA，电源：单电源，接口：支持不低于6千兆电口+2万兆光口SFP+。  功能描述：安全感知管理平台SIP一体机以网络流量监测为核心，结合威胁情报、机器学习、失陷主机检测、NTA流量分析、可视化等技术，对全网安全进行可视，帮助用户看清业务、看到威胁、看懂风险，并辅助用户进行决策，让更多中小客户实现业务风险全局可视化，满足等保合规。  含：安全感知管理平台软件V3.0(\*1套);  安全感知系统平台特征库软件 V2.0(\*2套);  万兆多模-850-300m-双纤(\*2个); |
| 大屏可视 | 支持不同安全视角展示16个独立的大屏展示功能，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏等，同时能满足多种场景的监控，比如日常运维、护网场景。 |
| 支持大屏轮播，支持不同视角展示全网安全态势，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、资产态势等态势。 |
| 脆弱性感知 | ★密码检测技术基于UEBA学习技术（无监督自我学习）提取登陆成功的特征，通过UEBA技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，包括响应体内容Json、响应体关键字Keyword、响应体MD5值、响应体长度Length、登录跳转路径Location，可实时自动生成学习到的登陆成功规则。（需提供产品功能截图证明） |
| 支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH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。 |
| 处置中心 | 支持安全域维度展示安全风险，包含安全域列表、安全域评分、事件类型TOP5、IP地址、IP类型、风险等级、关键风险、状态等信息 |
| 挖矿检测 | ★平台内置挖矿安全知识库，对常见的挖矿如：Bluehero挖矿蠕虫变种、虚拟货币挖矿、EnMiner挖矿病毒、PowerGhost挖矿病毒、DDG挖矿病毒、Docker挖矿、DDG挖矿变种、GroksterMiner挖矿病毒、Linux 挖矿木马、ZombieBoy挖矿木马等提供详细的背景介绍、感染现象、详细分析、相关IOC（MD5、C2、URL）、解决方案。（需提供产品功能截图证明） |
| 分析中心 | 支持DNS服务器日志导入，可以接入DNS服务器的日志，安全分析引擎将结合DNS服务器的日志，定位出DNS服务器代理风险外连场景下真实源IP，从而有效地进行风险处置闭环。 |
| 支持安全检测日志、审计日志、第三方日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS、HTTP、用户、数据库、文件审计、POP3、SMTP、IMAP、LDAP、FTP、Telnet等。 |
| ★备基于AI的webshell通信流量检测，可检出加密（如冰蝎）的通信流量。，具备650+webshell规则检测，且覆盖webshell整个攻击阶段检测，包括webshell上传点探测、webshell上传下载、webshell通信。（需提供产品功能截图证明） |
| 文件威胁分析支持平台内置的静态文件检测引擎、AI智能引擎、SAVE查杀引擎、webshellkiller引擎，利用LSA, AutoEncoder, LogicRegression, SVM, 随机森林，XGBoost等多种机器学习算法组合进行综合研判。支持采用AI技术针对无文件落地的恶意脚本进行检测。 |
| 支持SIEM日志关联分析结果的可视化展示。并且内置关联规则对日志进行二次分析，分析结果可视化展示。包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等。 |
| 支持针对政企邮件混淆宏病毒威胁检测，可通过不断下钻的特征向量提取和聚类算法有效检出邮件威胁。支持对smtp、imap、pop3、webmail等邮件协议审计，提取邮件正文和附件中的流量，并对邮件附件、正文链接、邮件行为、发件人等多维度进行规则和机器学习检测，从而识别出钓鱼邮件、病毒邮件、垃圾邮件、鱼叉式钓鱼等恶意邮件。 |
| 报告中心 | 支持综合安全风险、主机安全风险、脆弱性感知、外部感知、工单、摘要、处置报告多种方式呈现，也支持自定义时间导出PPT报告。  可快速生成月度、季度、年度PPT报表，摘要报告支持PPT格式导出；包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等，帮助用户高效汇报，体现安全工作价值。 |
| 支持短信/邮件/微信/实时告警推送。告警条件、推送频率、推送时间等可自定义；  短信邮件告警支持策略部编辑，可将不同告警内容发送至不同的责任人；  邮件告警支持报表通知事件举证清晰，支持邮件标记已处置，简化处置运维。 |
| 重保中心 | 具备实战化攻防中心，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面梳理暴。实战阶段的实时攻击分析，实时展受害者IP、攻击者IP、XFF、攻击结果、攻击次数、事件类型、威胁等级、联动响应、状态码、确定性等级等20个以上类型。实战阶段的全过程可视溯源分析、总结阶段的值守报告等全过程流程。 |
| ★支持云端与本地威胁情报共享，实时收集同步攻击者IP，并详细展示情报列表，包括IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等，并可对本地威胁情报及云端威胁情报联动同品牌防火墙实现自动封锁。（需提供产品功能截图证明） |
| 设备管理 | 具备安全日志分析引擎、DnsFlow行为分析引擎、HttpFLow分析引擎、NetFLow分析引擎、MailFLow分析引擎、SmbFLow分析引擎、威胁情报分析关联引擎、第三方安全检测引擎、文件威胁检测引擎等、异常账号行为分析引擎、恶意脚本行为分析引擎、文件智能分析引擎等；支持自动升级或离线手动升级。 |

**4、安全保障服务**

**4.1 风险评估服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 温州市公安局交通管理局。 |
| 服务期限及频率 | 测试系统数量：10个  服务频率：一年2次 |
| 服务内容 | 参照风险评估标准和管理规范，针对温州市公安局交通管理局信息系统的威胁性和脆弱性进行风险评估，从系统及其处理、传输和存储的数据信息的保密性、完整性和可用性等安全属性进行科学评估识别信息系统中关键资产及对信息系统中的风险与威胁进行分析汇总，梳理现有安全建设各方面的不足之处，提出安全整改建议。 |
| 交付物 | 每次风险评估服务实施完成后48小时内，提交服务交付成果，《系统风险评估报告》 |

**4.2渗透测试服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 温州市公安局交通管理局。 |
| 服务期限及频率 | 测试系统数量：10个  服务频率：一年2次 |
| 服务内容 | 针对温州市公安局交通管理局各公安业务网业务系统，通过真实模拟黑客使用的工具、分析方法来对业务系统进行模拟攻击，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，识别工具扫描无法发现的问题，按需提供渗透测试，提供3年服务。有效解决温州市公安局交通管理局公安网对内暴露且可能被利用的安全风险，进一步提升公安网内网数据中心的安全防护能力。并根据渗透结果输出相应报告，同时配合进行整改。 |
| 交付物 | 测试完成后出具《渗透测试报告》，报告需包含测试安全漏洞情况及整改加固建议，根据报告进行网络安全漏洞整改加固工作，并待加固完成后进行复测，检查安全漏洞整改落实情况，出具《渗透测试复测报告》 |

**4.3制度体系建设服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 温州市公安局交通管理局。 |
| 服务期限及频率 | 4套 |
| 服务内容 | 根据交管局网络安全管理的现状、差距以及风险评估和安全测试结果为依据，按照最新等级保护标准要求，协助交管局制定网络安全管理制度体系，明确管理方针、策略，以及相应的规定、操作规程、业务流程和记录表单，从贴合实际用户业务流程的原则出发，按照交管局管理标准，编写管理制度文件，并进行沟通和修订。 |
| 交付物 | 4套网络安全制度 |

**4.4基线检查**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 温州市公安局交通管理局。 |
| 服务期限及频率 | 每年提供2次基线检查服务。 |
| 服务内容 | 针对温州市公安局交通管理局各公安业务网业务系统，结合各行业安全规范和标准，参照安全配置基线和规范对配置进行优化。包括网络设备（包含但不限于交换机、路由器、防火墙等）、操作系统（包含但不限于各windows、Linux、Unix版本）和数据库系统（包含但不限于Oracal、SQL Server、DB2、Mysql等主流数据库）的安全配置基线。 |
| 交付物 | 每次基线检查服务实施完成后48小时内，提交服务交付成果，《基线检查报告》 |

**4.5安全培训**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 温州市公安局交通管理局。 |
| 服务期限及频率 | 每年提供1次安全培训服务。 |
| 服务内容 | 结合温州市公安局交通管理局各公安业务网业务系统现状，根据不同的用户类型安排有针对性的培训内容。  管理人员主要包括：高层管理、业务专家等。  对管理人员的培训，目的是使他们了解国家相关部门对系统信息安全管理和建设的相关标准，同时建立起一套具有针对性和适用性的安全管理办法。  对技术人员的培训，目的是使他们了解信息系统所面临的严峻安全威胁和挑战，以及如何进行全面有效的安全防护措施。  全员培训主要包括：安全意识培训等。  全体成员的培训，目的是让大家对信息安全的有初步的认识和逐步提高安全意识，让安全事故可以得到有效的避免。 |
| 交付物 | 每次安全培训完成后48小时内，提供本次培训使用的课件。 |

**4.6安全运营服务**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 服务范围 | 温州市公安局交通管理局。 |
| 服务期限及频率 | 3年 |
| 服务内容 | 1. 安全加固服务   根据实际需求，针对风险评估以及信息系统日常运维过程中发现的安全漏洞和隐患，按需提供安全加固服务。   1. 安全运维   针对交管局整体信息系统开展日常安全运维服务工作，服务内容包括但不限于：设备运行安全监测、安全事件告警监控、配置及备份更新，并提供安全设备系统升级、协助安全设备故障处理、安全设备防护告警监测、负责日常网络安全事件以及协助进行重大网络安全事故的应急响应工作。   1. 重保安全值守   按需提供重保值守服务，次数由重大活动为基准。在重点时期（包括：国庆、亚运、二十大等）前对现有网络运行的服务器、终端、网络设备、安全设备、网站及应用系统等开展安全检查，从而发现硬件、软件、协议的实现或系统安全策略上的缺陷问题，对发现的问题提供对应安全整改建议，在重点时期做好安全加固及防护，并提供1名安全技术人员重要时段安全保障值守服务，保障安全稳定运行。   1. 安全应急响应处置   根据交管局安全事件情况，按需提供应急响应处置服务，基于温州市公安局交通管理局公安具体的安全事件开展应急响应，安全事件检测、安全事件抑制、安全事件根除、安全事件恢复、安全事件总结，最终形成协调联动机制，增强应急技术能力，健全应急响应机制。安全事件处置完成，系统得到恢复。找到安全事件发生原因并提供安全解决方案。提供交付物安全事件应急响应报告。 |
| 交付物 | 《网络安全运维月报》、《安全加固报告》、《应急响应报告》、《重大活动保障方案》、《重大活动保障报告》 |

## 四、 其他要求

**1. 交付或者实施的时间和地点要求：**

**1.1 交付或者实施的时间：**

**合同签订后2个月内完成所有软硬件安装并上线试运行，试运行时间为不少于1个月。**

**1.2 交付地点：**采购人指定地点。

**2. 售后服务：**

**2.1 技术支持：**

免费运维服务期内，须提供每周7天，每天8小时的售后服务，在接到用户故障报告后响应时间不超过30分钟；如不影响网络和信息系统正常运行的，应在60分钟处置完成；如对网络和信息系统正常运行造成影响的，应在30分钟处置完成，期间如不能修复，必须提供应急措施，保证系统的正常运行。

免费运维服务期内，供应商需免费为采购人进行版本升级、软件维护、数据维护、使用培训、数据迁移（如有）、安全漏洞和隐患的消除等上门服务。

**2.2 维保期限：**

**▲须提供不少于三年（36个月）服务，服务期满服务工具的所有权转移给采购人。**

**3. 系统培训：**

实际操作培训：根据采购人要求，对使用人员集中进行设备操作应用培训，场次、人数不限。

现场培训：根据采购人要求，对相关技术人员集中进行设备安装集成培训，场次不少于3场，人数不限。

系统培训：进行基础操作培训，包括最新技术、设备使用、维护以及运行管理等内容，场次不少于3场，人数不少于10人。

系统管理培训：中标人应向采购人免费提供系统管理维护的技术培训，包括必要的有关系统软件、应用软件和后台管理软件的操作培训课程。系统培训场地、教学资料、环境等由建设方提供。培训课程及时间安排由中标人提供并经采购人认可，培训讲师不少于2人，且培训时间不少于5个工作日。

系统应用培训：面向采购人的操作使用培训、以及常见软硬件系统故障恢复。系统培训方式和场地由采购人决定，培训材料、课程安排由中标人提供并经采购人认可，培训讲师不少于2人，且培训场次不少于3轮。

1. **付款方式见第二部分“合同主要条款”。**
2. **▲本项目采购预算为126.2万元，最高限价为126.2万元，投标供应商的投标报价不得超过采购预算（或最高限价），否则其投标文件作无效标处理。投标报价是指本供应商为完成本次采购要求及完成技术标中所载明的设备费、软件费、系统集成、运输、安装、调试、人工费、利润、验收费、采购代理服务费、税金等完成合同所需的一切本身和不可或缺的所有工作开支、政策性文件规定及合同包含的所有风险、责任等各项全部费用，投标供应商应根据上述因素自行考虑含入投标报价。**

**6.项目实施和运维要求**

**6.1 中标方在项目实施及运维过程中，保证所投入的硬件、软件，固件升级、代码库更新，规则变更等所有人员操作和维护动作，不会对交管局现有网络与安全带来故障和风险。任何软硬件和动作实施，如果会带来网络和安全扰动的，必须事先提出，与交管局负责人员做好沟通、制定细致操作策略，双方确认后再实施。如有违反本条描述之要求，造成交管局网络、服务、安全、系统等异常，影响正常工作的，每发生一起扣款千分之一的合同金额，扣款金额上限为合同金额的百分之十，计算扣款，扣款金额上限为合同金额的百分之十，扣款超过百分之十的，甲方有权可解除合同。**

**6.2 中标方对本次项目投入的软硬件设备性能指标，固件代码库更新频度，监测规则等，都应符合信息系统等保三级要求，如不符，中标方必须无条件更换符合要求软硬件设备，如未落实，每一项，按照合同金额的百分之一实施扣款，扣款金额上限为合同金额的百分之十，超过百分之十的，甲方有权可解除合同。**

**6.3 本次项目的实施，是为确保交管局网络信息整体安全可控，建立安全防护屏障，随时发现潜在安全威胁风险，及时处置消除隐患。如在运维期间，交管局如发生因网络安全、病毒攻击、漏洞攻陷等网络安全事件，被上级机关通报整改扣分，造成影响的，每发生一起，按照合同金额的百分之二实施扣款，如在重大安保期间，交管局发生被上级通报扣分的网络安全事件，每发生一起，按照合同金额的百分之五实施扣款，扣款金额上限为合同金额的百分之十，超过百分之十的，甲方有权可解除合同。**

**6.4 本项目运维期间，如发生本项目的任何产品的运行、设置、维护等故障，中标方有30分钟故障处置时间，超过5分钟，如对网络和信息系统正常运行造成影响的，每30分钟按照合同金额的千分之一实时扣款，扣款金额上限为合同金额的百分之十，超过百分之十的，甲方有权可解除合同。如不影响网络和信息系统正常运行的，应在60分钟处置完成，超过60分钟的，每次按照合同金额的万分之一实施扣款。是否影响网络和信息系统正常运行，由甲方判定。**

**6.5 在运维期，甲方会组织实施项目运维工作是否到边到位的随机抽检。如发现中标方未按照标书和合同要求，实施各项规定的运维工作，如没有及时处置安全设备的威胁告警，没有按照要求设定最小必要安全访问策略等等行为的，每发现一起，按照合同金额的百分之一实施扣款，扣款金额上限为合同金额的百分之十，超过百分之十的，甲方有权可解除合同。**

# 第五部分 评标原则及方法

**根据《中华人民共和国政府采购法》等相关法律、法规特制定以下评标办法。**

**一、 总 则**

评标工作应遵循公开、公平、公正、科学、择优原则，科学、严谨的态度，认真进行评标，推进技术进步，确保项目质量，最大限度的保护当事人权益。严格按照招标文件的商务、技术要求，对投标文件进行综合评定，编写评标报告。对落标单位，评委会不作任何落标解释。投标供应商不得以任何方式干扰招投标工作的正常秩序，一经发现其投标文件将被拒绝。

**二、 评标组织**

评标工作由招标采购单位依法组建的评标委员会负责。

**三、 评标程序**

开标后，采购人对各投标供应商的资格进行审查；然后评标委员会对合格投标供应商进行符合性审查，并按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

**四、 评标办法**

1、 **本项目评标办法采取百分制综合评分法**，**其中商务技术分70分，价格分30分。**即最大限度地满足招标文件实质性要求前提下，按照招标文件中规定的各项评分内容进行综合评审。以最终得分（即商务技术分与价格分之和）高低进行排序，得分前二名的投标供应商依次确定为第一和第二中标候选供应商（得分相同投标报价低的排序第一；得分且投标报价相同的，中标候选供应商并列，并确定技术部分得分高的为中标供应商）。

2、 评标过程中遇到特殊情况，由评标委员会遵循公平、公正原则，采取记名投票方式按照少数服从多数原则决定。

3、 投标截止时间止及评审期间，如出现有效供应商＜3家时，该项目废标，并重新组织采购。

**五、 评分细则**

**1、商务技术分的评定（70分）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评审项目** | **分值** | **评分标准** |
| 1 | 供应商综合实力 | 6 | 1、具有ISO9001质量管理体系认证证书，有得2分，没有不得分。  2、具有ISO20000信息技术服务管理体系认证证书，有得2分，没有不得分。  3、具有ISO27001信息安全管理体系认证证书，有得2分，没有不得分。  （提供有效期内的证书复印件，否则不得分） |
| 2 | 产品技术响应情况 | 25 | 投标供应商对服务支撑工具的技术参数响应指标负偏离每一项扣减1分，星号★参数每负偏离一项扣2分，扣完为止。 |
| 3 | 项目需求理解 | 4 | 基于对项目背景、总体情况、建设思路、系统需求、建设内容的理解和熟悉程度，投标文件内容的完整、合理及原有安全产品基本功能、现状的了解程度、提供详细描述。评审专家综合评分。  （1）了解程度全面，针对性强的，得3-4分；  （2）了解程度较全面，针对性较强的，得2分；  （3）了解程度、针对性一般的，得1分；  （4）不提供不得分。 |
| 4 | 功能及服务 | 4 | 方案整体架构与功能点的可行性、合理性、规范性，与用户现有系统的兼容性，包括总体设计及服务涉及，由评审专家综合评分。  （1）方案能贴合采购人需求，合理可行的得3-4分；  （2）方案能比较贴合采购人需求，较合理可行的得2分；  （3）方案能基本贴合采购人需求，合理性、可行性一般的得1分；  （4）不提供不得分。 |
| 5 | 投标供应商人员投入 | 15 | 1、项目负责人同时具有网络工程师、信息安全工程师、CISP、CCRC（网络安全应急响应工程师）及VCP认证证书的得5分，少一项扣1分，扣完为止，本项最高得5分。  2、项目团队拥有1名CISP-CSE安全工程师(云安全工程师）的得2分 ，否则不得分。  3、项目团队拥有1名CISP-BDSA安全工程师（大数据安全分析师）的得2分，否则不得分。  4、项目团队拥有1名ITSS IT服务项目经理的得2分，否则不得分。  5、项目团队拥有1名操作系统专业认证工程师的得2分，否则不得分。  6、项目团队拥有1名数据库专业认证工程师的得2分，否则不得分。  证明材料：提供相关人员相应证书的复印件和社保证明资料，否则不得分。 |
| 6 | 质量保证措施 | 3 | 维保服务质量保证计划措施，投标供应商是否有明确的质量保证目标，质量保证措施和体系合理先进及详细的实施内容等，由评审专家综合评分。   1. 质量保证体系内容完整、描述清晰，质量保障措施完备周全、科学合理、可行，能充分保障项目质量及有效满足采购需求的得3分； 2. 保障体系及保障措施基本完整、可行的得2分； 3. 保障体系及保障措施简单，明显欠缺不足的得1分； 4. 未提供不得分。 |
| 7 | 应急方案 | 3 | 提供详细应急服务方案，在突发事件与特殊时段，如节假日或深夜，如何提供应急服务，应急服务方案考虑周到性，切实可行性，针对性，由评审专家综合评分。   1. 方案内容完整具体、条理清晰、合理可行，针对性强，满足采购要求，有利于项目实施的得3分； 2. 方案基本完整、可行，内容稍有欠缺的得2分； 3. 方案简单，可行性较差，内容明显欠缺不足的得1分， 4. 未提供不得分。 |
| 8 | 巡检计划 | 3 | 根据投标供应商拟定的项目维护计划（驻点人员安排，定期巡检等情况）的有效性等，由评审专家综合评分。  (1)计划合理、可行性强、完全满足采购需求的得3分；  (2)计划较合理可行、针对性较强的得2分；  (3)计划基本贴合采购人需求，合理性、可行性、针对性一般的得1分；  (4)不提供不得分。 |
| 9 | 培训计划 | 2 | 根据投标供应商拟定的培训方案、计划的可行性及合理性，由评审专家综合评分。  （1）方案内容完整具体、条理清晰、合理可行，针对性强的，得2分；  （2）方案简单，可行性较差的得1分，  （3）未提供不得分。 |
| 10 | 售后服务 | 3 | 根据投标供应商拟定的售后服务的响应情况（对用户故障响应、处理等），由评审专家综合评分。   1. 能提供快速便捷、及时安全的服务响应能力的，得3分； 2. 服务响应能力一般的，得2分， 3. 服务响应能力的，得1分。 4. 未提供不得分。 |
| 11 | 同类项目业绩 | 2 | 投标供应商2019年1月1日（以合同签署时间为准）以来承接的类似项目案例。有一个得1分，最高2分，否则不得分。  证明材料：提供合同（包括首页、合同内容描述页、合同盖章页）复印件并加盖投标供应商公章，否则此项业绩不得分。 |

**注 ：每个评委根据上述评分内容和分值独立打分，然后将各评委汇总分的算术平均值作为该投标供应商的商务技术最后有效得分。（计算分值四舍五入，精确到小数点后二位）**

**2、价格评分（30分）**：

（1）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。

（2）投标供应商的投标报价等于评标基准价时其价格分为满分；

（3）其他投标供应商的价格分按以下公式计算：

价格分=（评标基准价/投标供应商投标价）×30（四舍五入，保留小数点后2位）

**（4）▲投标供应商的投标报价超过采购预算（或最高限价）的，作无效标处理。**

3． 有效投标供应商的综合得分为技术资信分和商务（价格）分的总和。

4、 评标委员会按各有效投标供应商综合得分高低顺序排列，综合得分前两名的投标供应商依次作为第一中标候选供应商和第二中标候选供应商向采购人推荐，并提交评标报告。

**六、 定标办法**

本次招标由评标委员会确定2名中标候选供应商并向采购人推荐，采购人根据评标委员会的推荐结果按排名顺序确定中标供应商。

**七、 中标结果公告**

中标供应商确定后，中标公告在浙江政府采购网上发布，在发布中标公告的同时，采购人将向中标供应商发出中标通知书。中标通知书对采购人和中标供应商具有同等法律效力。

**八、 投标供应商义务**

投标供应商应随时接受评标委员会的询标，解答包括有关的商务、技术等问题。评标结束，所有评标资料归档备查。

**政府采购活动现场确认声明书**

浙江东瓯工程造价咨询有限公司：

本人经由 （供应商名称）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）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。

（二）现已清楚知道并严格遵守政府采购法律法规和现场纪律

（三）我发现 与 （供应商名称）之间存在或可能存在上述第二条第 项利害关系。

投标供应商代表签名：

日期: 年 月 日