

# 安全等级保护改造项目

项目编号：JSLT 竞磋[2021]-06-016

## 竞争性磋商文件

采 购 人 ： 溧阳市交通运输局

采购代理机构（章）：江苏溧投招标服务有限公司

法定代表人（章）：

日 期 ： 2021 年 10 月 21 日

# 目 录

供应商须知.....	3
第一章 竞争性磋商邀请函.....	4
第二章 竞争性磋商须知.....	7
一、总则.....	7
二、磋商响应文件的编制及保证金收取.....	8
三、响应文件的递交.....	10
四、磋商与评审.....	11
五、成交.....	14
六、合同签订相关事项.....	16
七、政策功能.....	16
第三章 合同格式.....	19
第四章 项目需求.....	22
第五章 评标方法与评标标准.....	45
第六章 常州市政府采购供应商信用管理暂行办法.....	48
第七章 响应文件格式.....	52

## 供应商须知

项号	内容规格
1	项目名称：安全等级保护改造项目 项目编号：JSLT 竞磋[2021]-06-016 预算金额：¥310.00 万元 最高限价：¥270.691 万元
2	响应文件份数：正本 1 份、副本 2 份
3	评审办法：综合评分法
4	磋商保证金：本项目不收取磋商保证金
5	磋商报价次数：2 次 注：1、报价：本项目报价总金额不得高于¥270.691 万元 2、供应商原则上进行两次报价，在磋商截止时间前提交的磋商响应文件首次报价书是第一次；商务技术磋商结束后的报价是第二次。如果符合磋商文件要求的供应商报价因高于项目预算导致合格供应商不足 3 家，磋商小组可视情况在给予所有符合要求的供应商均等机会条件下，进行第三次报价。
6	磋商有效期：自磋商之日起 45 个日历日
7	磋商文件提交截止后将进行供应商信用信息查询。信用中国网站（www.creditchina.gov.cn）
8	★本项目需要现场勘察，请各潜在供应商自行前往现场考察，对周边环境及基础数据自行采集和确认，由采购人签署回执单（附件六）并盖章，回执单原件须放入磋商响应文件，否则视为未实质性响应，作无效投标处理。

# 第一章 竞争性磋商公告

## 项目概况

“安全等级保护改造项目”的潜在供应商应在江苏省溧阳市溧城镇南环西路 108 号嘉源广场 2 幢 1 单元 5 楼获取磋商文件，并于 2021 年 11 月 02 日 09 点 30 分（北京时间）前递交响应文件。

### 一、项目基本情况

项目编号：JSLT 竞磋[2021]-06-016

项目名称：安全等级保护改造项目

采购方式：竞争性磋商

预算金额：¥310.00 万元

最高限价：¥270.691 万元

采购需求：溧阳市交通运输局安全等级保护改造以及服务等。

合同履行期限：合同签订后 30 天内完成项目建设（不含第三方相关检测及取证时间）

本项目不接受联合体投标

### 二、申请人的资格要求

1、满足《中华人民共和国政府采购法》第二十二条规定；

2、落实政府采购政策需满足的资格要求：本项目若符合节能环保产品、科技创新产品、经济薄弱地区、中小微企业等政策，将落实相关政策；

3、本项目的特定资格要求

(1) 未被“信用中国”网站（www.creditchina.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) 单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同下的政府采购活动。

### 三、获取采购文件

时间：2021 年 10 月 22 日至 2021 年 10 月 28 日，每天上午 9:00 至 12:00，下午 13:00 至 17:00（北京时间，法定节假日除外）

地点：溧阳市溧城镇南环西路 108 号嘉源广场 2 幢 1 单元 5 楼江苏溧投招标服务有限公司综合办

方式：现场报名 报名资料：①报名时需提供报名申请表一份（见附件 1），并按表格内要求递交报名材料（盖章并签字）；②《疫情期间参与政府采购活动开评标人员健康信息登记表》（见附件 2）。资料齐全、符合要求的由代理机构发放磋商文件（电子稿）

售价：¥1000 元/份（电汇或现金，电汇需备注项目编号及资金用途）

账户名称：江苏溧投招标服务有限公司；

账号：0131 8012 0100 0000 0868；

开户行：江南农村商业银行溧阳市盛世支行。

**磋商文件售后一概不退。供应商递交的磋商响应文件概不退还。一经报名，供应商不得更改单位名称。**

#### 四、响应文件提交

截止时间：2021 年 11 月 02 日 09 点 30 分（北京时间）

地点：溧阳市溧城镇南环西路 108 号嘉源广场 2 幢 1 单元 5 楼江苏溧投招标服务有限公司

#### 五、开启

时间：2021 年 11 月 02 日 09 点 30 分（北京时间）

地点：溧阳市溧城镇南环西路 108 号嘉源广场 2 幢 1 单元 5 楼江苏溧投招标服务有限公司

#### 六、公告期限

自本公告发布之日起 5 个工作日。

#### 七、其他补充事宜

##### 特别提醒：

1、原则上每家磋商供应商不得超过 1 名代表现场投标。磋商供应商代表进入开标室前须全程佩戴口罩，接受体温测量（经测量体温超过 37.2° C 不得入内）；出示当日苏康码，如出现发热、咳嗽等症状请勿参加。

2、进入开标区提交响应文件过程中应服从现场工作人员管理，有序排队，并保持社交距离。

3、对于参与开评标活动的供应商、采购人授权代表，应如实填报《疫情期间参与政府采购活动开评标人员健康信息登记表》并加盖单位公章。在进入采购代理机构时，请凭《疫情期间参与政府采购活动开评标人员健康信息登记表》和本人身份证原件方能到指定开评标场所。

4、采购活动进行中遇到疫情相关特殊情况，将立即报告同级新型冠状病毒感染的肺炎疫情防控应急指挥部和同级财政各部门。其余事项严格按照苏财购【2020】13 号文执行。

#### 八、凡对本次采购提出询问，请按以下方式联系。

##### 1、采购人信息

名称：溧阳市交通运输局

地址：溧阳市燕山中路 18 号交通大楼

联系方式：0519-87228118

##### 2、采购代理机构信息

名称：江苏溧投招标服务有限公司

江苏溧投招标服务有限公司

项目编号：JSLT 竞磋[2021]-06-016

地 址：江苏省溧阳市溧城镇南环西路 108 号嘉源广场 2 幢 1 单元 5 楼

联系方式：0519-87968552

3、项目联系方式

项目联系人：姜工

电话：0519-87968552

## 第二章 竞争性磋商须知

### 一、总则

#### 1、适用范围

1.1、本竞争性磋商文件（以下简称磋商文件）仅适用此项目。

1.2、本竞争性磋商按照《政府采购竞争性磋商采购方式管理暂行办法》（财库（2014）214号）执行。

#### 2、项目采购方式

本次采购采取竞争性磋商的方式。参加竞争性磋商的供应商以下简称“磋商供应商”。

#### 3、合格的磋商供应商

3.1、满足本磋商文件“磋商公告”中合格磋商供应商资格要求的规定。

3.2、满足本磋商文件实质性要求和条件的规定。

#### 4、参加磋商费用

4.1、磋商供应商应自行承担所有与参加磋商有关的费用，无论磋商过程中的做法和结果如何，江苏溧投招标服务有限公司（以下简称采购代理机构）在任何情况下均无义务和责任承担这些费用。

4.2、采购代理服务费：采用差额定率累进计费方式，在领取成交通知书前，成交人按照原国家发展计划委员会《招标代理服务费管理暂行办法》（计价格【2002】1980号）收费标准收取，但低于¥2000元时按最低¥2000元收取。

4.3、供应商报价应当包含上述费用，但无须单独列出。

名称：江苏溧投招标服务有限公司；

账号：0131 8012 0100 0000 0868；

开户行：江苏江南农村商业银行溧阳市盛世支行。

#### 5、磋商文件的约束力

供应商一旦购买了磋商文件并决定参加磋商，即被认为接受了本磋商文件的规定和约束，并且视为自收到竞争性磋商文件之日起已经知道或应当知道自身权益是否受到了损害。

#### 6、磋商文件的澄清及修改

6.1、任何要求对磋商文件进行澄清的供应商均应在提交首次响应文件截止时间5日前按磋商公告中的通讯地址，以书面形式通知采购代理机构。提交首次响应文件截止之日前，采购代理机构可以对已发出的磋商文件进行必要的澄清或者修改，澄清或者修改的内容作为磋商文件的组成部分。澄清或者修改的内容可能影响响应文件编制的，采购代理机构将在提交首次响应文件截止时间至少5日前，向所有获取磋商文件的供应商发布书面更正通知。不足5日的，采购代理机构应当顺延提交首次响应文件截止时间。

## 二、磋商响应文件的编制及保证金收取

### 7、磋商响应文件份数和签署

7.1、磋商供应商应严格按照磋商文件要求准备磋商响应文件（以下简称响应文件，“正本”1份和“副本”2份），每份响应文件须清楚地标明“正本”或“副本”字样。响应文件的正本应用打印机或不褪色墨水书写，且经法定代表人或授权代表签署，副本可以为正本的复印件。响应文件正本中，按磋商文件规定提交复印件或原件，文字材料需打印或用不褪色墨水书写，响应文件正本须经法定代表人或授权代表签字和加盖磋商供应商公章。本磋商文件所表述（指定）的公章是指刻有供应商法定名称的印章，不包括合同、财务、税务、发票等形式的业务专用章。

7.2、除对错处做必要修改外，响应文件不得行间插字、涂改或增删。如有修改错漏处，必须由响应文件签署人签字或盖章。因响应文件字迹潦草或表达不清所引起的不利后果由供应商承担。

7.3、供应商应按照磋商文件所规定的内容顺序，统一用 A4 规格幅面打印、装订成册并编制目录，逐页编码。由于编排混乱导致响应文件被误读或查找不到，责任由供应商承担。

### 8、响应文件的组成

供应商编写的响应文件应包括资信证明文件、技术条款响应及偏离表、商务条款响应及偏离表、服务承诺、人员配备的情况介绍、响应函等部分。

#### 8.1、证明供应商资格及符合磋商文件规定的文件

##### 8.1.1、一般资格要求：

- 1、具有独立承担民事责任的能力（提供法人或者其他组织的营业执照）；
- 2、具有良好的商业信誉和健全的财务会计制度；提供上一年度的财务状况报告（至少包括资产负债表和利润表），或其银行出具上一年度的资信证书复印件，或其上一年度经审计的财务报告复印件加盖公章；
- 3、具有履行合同所必需的设备和专业技术能力（根据项目需求提供履行合同所必需的设备和专业技术能力的证明材料）；
- 4、有依法缴纳税收和社会保障资金的良好记录（提供参加本次采购活动前半个月内依法缴纳税收和社会保障资金的相关材料）；
- 5、参加本次政府采购活动前三年内，在经营活动中没有重大违法记录（提供参加本次政府采购活动前三年内在经营活动中没有重大违法记录的书面声明，格式自拟）；

6、被“信用中国(www.creditchina.gov.cn)”网站和“中国政府采购网(www.ccgp.gov.cn)”网站列入失信被执行人、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的，不得参加本项目投标；



7. 法律、行政法规规定的其他条件（提供项目实施所必须的许可资质证明材料）。

8.1.2、磋商供应商不得存在下列情形之一：

- 1、为采购人不具有独立法人资格的附属机构（单位）；
- 2、与本采购项目的监理人、代建人、采购代理机构同为一个法定代表人的，或者相互控股、参股的；
- 3、与采购人存在利害关系可能影响采购公正性的；
- 4、单位负责人为同一人或者存在控股、管理关系的不同单位；
- 5、处于被责令停业、财产被接管、冻结和破产状态，以及投标资格被取消或者被暂停且在暂停期内；
- 6、因拖欠工人工资或者因发生质量安全事故被有关部门限制在采购项目所在地承接工程的；
- 7、投标人近3年内有行贿犯罪行为且被记录，或者法定代表人有行贿犯罪记录且自记录之日起未超过5年的。

8.2、技术条款响应及偏离表、商务条款响应及偏离表及投标说明

- 1、对磋商文件中的技术与商务条款要求逐项作出响应或偏离，并说明原因；
- 2、磋商供应商认为需要的其他技术文件或说明。

8.3、服务承诺、人员配备的情况介绍

- 1、磋商供应商的服务承诺应按不低于磋商文件中商务要求的标准；
- 2、提供磋商供应商有关服务的管理制度、服务人员的数量、素质、技术水平及服务的反应能力和相关证明材料。

8.4、响应函和响应报价表

- 1、磋商供应商应按照磋商文件中提供的格式完整、正确填写响应函、响应报价表；
- 2、响应报价表中的磋商报价应与响应文件中的磋商报价一致，如不一致，不作为无效投标处理，但评标时一律按响应报价表为准。

**3、响应报价表必须盖章，必须单独封装在信封中并且在磋商截止时间前与响应文件分别递交，否则视为无效投标。**

9、响应文件编制要求

9.1、磋商供应商提交的响应文件以及磋商供应商与采购代理机构及采购人就有关磋商的所有来往函电均应使用简体中文。磋商文件中既有文也有外文的，以中文文本为准。

9.2、除技术性能另有规定外，响应文件所使用的度量衡单位，均须采用国家法定计量单位。

9.3、除磋商供应商对错处做必要修改外，响应文件不得行间插字、涂改或增删。如有修改错漏处，必须由响应文件签署人签字或盖章。

10、有关费用处理

10.1、采购报价采用总承包方式，包括设备本身、安装调试费、人工费、服务费、税金以及交付使用过程中涉及到的其他一切费用（包括人员工资、《劳动合同法》规定的各种社会保险费、办公费等）。磋商供应商对合同内容的费用、质量、安全、文明服务等实行全面承包。磋商供应商的任何错漏、优惠、竞争性报价不得作为减轻责任、减少服务、增加收费、降低质量的理由。磋商文件中另有规定的除外。

#### 10.2、其他费用处理

磋商文件未列明，而磋商供应商认为必需的费用也须列入报价。

#### 11、报价采用的货币

磋商响应文件中的单价和总价，无特殊规定的采用人民币报价，以元为单位标注。磋商文件中另有规定的按规定执行。

#### 12、磋商保证金

本项目不收取磋商保证金。

### 三、响应文件的递交

#### 13、响应文件的密封和标记

13.1、磋商供应商应严格按照磋商文件要求的份数准备响应文件，每份响应文件须清楚标明“正本”或“副本”字样。一旦正本和副本不符，以正本为准。磋商供应商应将响应文件正本和所有副本密封。

#### 13.2、密封的响应文件应：

- (1) 按磋商公告中注明的地址送达规定地点；
- (2) 注明参加磋商项目名称、磋商文件编号；
- (3) 密封包装上应写明磋商供应商名称和地址。

13.3、如果密封包装未按要求密封和加写标记，采购代理机构对误投或过早启封概不负责。对由此造成提前开封的响应文件采购代理机构将予以拒绝，作无效响应处理。

#### 14、响应文件开启时间

14.1、采购代理机构收到响应文件的时间不得迟于本磋商文件规定的响应文件接收截止时间。

14.2、采购代理机构可通过修改磋商文件自行决定酌情推迟响应文件接收截止时间，在此情况下，磋商供应商的所有权利和义务以及受制的响应文件接收截止时间均应以延长后新的响应文件接收截止时间为准。

#### 15、迟交的响应文件

15.1 采购代理机构将拒绝在规定的响应文件接收截止时间后接收响应文件。

#### 16、响应文件的修改和撤回

16.1、磋商供应商在递交响应文件后，可以修改或撤回其谈判响应文件，但这种修改和撤回，必须在规定的响应文件接收截止时间前，以书面形式送达指定地点。

16.2、磋商供应商的修改或撤回通知书，应按本文件规定进行编制、密封、标记和发送，并应在封套上加注“修改”和“撤回”字样。

16.3、磋商供应商在提交最后报价之前，可以根据磋商情况退出磋商。

17、磋商响应有效期

17.1、磋商响应有效期为采购代理机构规定的响应文件接收截止时间后 45 天。磋商响应有效期比规定短的将被视为非实质性响应性而予以拒绝。

17.2、在特殊情况下，采购代理机构于原磋商响应有效期满之前，可向磋商供应商提出延长磋商响应有效期的要求。这种要求与答复均采用书面形式。磋商供应商可以拒绝采购代理机构的这一要求而放弃磋商响应。同意延长磋商响应有效期的磋商供应商既不能要求也不允许修改其响应文件。

#### 四、磋商与评审

18、磋商仪式

18.1、采购代理机构将在磋商公告中规定的时间和地点组织磋商开始仪式，仪式由采购代理机构主持，磋商供应商应委派携带有效证件的代表准时参加，参加仪式的代表需签名以证明其出席。

18.2、供应商到场要求及磋商现场需提供的材料：

供应商的法定代表人或委托代理人必须参加磋商评审会议，并在采购人按磋商程序进行点名身份核验时，各到场人员需提供以下材料：

(1) 如法定代表人参加时，须提交法定代表人身份证明文件原件及法定代表人第二代居民身份证原件；

(2) 如委托代理人参加时，须提交法定代表人授权委托书原件及委托代理人第二代居民身份证原件。

上述原件在投标截止时间前一次性递交，磋商截止时间后不再接受补充资料。

注意事项：以上参加人员在磋商截止时间时有下列情形之一的，视为自动放弃投标处理，采购人不予受理：

(1) 未到达磋商现场的；

(2) 未参加磋商签到的；

(3) 身份核验时未能提供相关材料的。

19、磋商小组

19.1、磋商开始仪式结束后，采购代理机构将组织磋商小组进行评审。

19.2、磋商小组由政府采购评审专家、采购人代表组成，且人员构成符合政府采购有关规定。

## 20、磋商评审过程的保密与公正

20.1、磋商小组、采购人和采购代理机构工作人员、相关监督人员等与评审工作有关的人员,对评审情况以及在评审过程中获悉的国家秘密、商业秘密负有保密责任。

20.2、在磋商评审过程中,磋商供应商不得以任何行为影响磋商评审过程,否则其响应文件将被作为无效响应文件。

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

## 21、评审过程的澄清、说明和更正

21.1、磋商小组在对响应文件的有效性、完整性和响应程度进行审查时,可以要求供应商对响应文件一含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等做出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。

21.2、接到磋商小组要求的供应商应派人按磋商小组通知的时间和地点做出书面澄清、说明或更正。供应商的澄清、说明或者更正应当由法定代表人或授权代表签字或者加盖公章。由授权代表签字的,应当附法人授权书。供应商为自然人的,应当由本人签字并附身份证明。

21.3、接到磋商小组澄清要求的供应商如未按规定做出澄清,其风险由供应商自行承担。

## 22、对响应文件的初审

### 22.1、响应文件初审分为资格性检查和符合性检查。

资格性检查:依据法律法规和磋商文件的规定,对响应文件中的资格证明文件等进行审查,以确定供应商是否具备参加磋商的资格。

磋商小组在进行资格性审查的同时,将在“信用中国”网站(www.creditchina.gov.cn)对供应商是否被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重失信行为记录名单情况进行查询,以确定供应商是否具备参加磋商的资格。

接受联合体的项目,两个以上的自然人、法人或者其他组织组成一个联合体,以一个供应商的身份共同参加政府采购活动的,联合体成员存在不良信用记录的,视同联合体存在不良应用记录。

符合性检查:依据磋商文件的规定,从响应文件的有效性、完整性和对磋商文件的响应程度进行审查,以确定是否对磋商文件的实质性要求作出响应。实质性要求是指本磋商文件中用带“★”的商务和技术要求,有一项不符合的,作无效投标处理,标注“△”的为重要参数。供应商必须在磋商响应文件内提供技术支持资料(包括产品彩页、资质证书、操作手册等),未提供技术支持资料的,评审时不予认可。

22.2、在正式磋商之前,磋商小组将首先审查每份响应文件是否实质性响应了磋商文件的要求。实质性响应的响应文件应该是与磋商文件要求的条款、条件和规格相符,没有重大负偏离或保留。

所谓重大负偏离或保留是指与磋商文件规定的实质性要求存在负偏离,或者在实质上与磋商文件不一致,而且限制了合同中甲方的权利或供应商的义务,纠正这些偏离或保留将会对其他实质性响应要求的供应商的竞争地位产生不公正的影响。重大偏离由磋商小组按照少数服从多数的原则认定。磋商小组决定响应文件的响应性只根据响应文件本身的内容,而不寻求外部的证据。

### 22.3、被认定为未实质性响应磋商文件的响应文件的情形

- (1) 未按照磋商文件规定要求密封、签署、盖章的;
- (2) 供应商在报价时采用选择性报价;
- (3) 供应商不符合磋商文件中规定的合格磋商供应商资格要求的;
- (4) 不符合法律、法规和磋商文件中规定的其他实质性要求和条件的;
- (5) 其他法律、法规及本磋商文件规定的属未实质性响应的响应文件的情形;
- (6) 供应商被“信用中国”网站(www.creditchina.gov.cn)列入失信被执行人或重大税收违法案件当事人名单或政府采购严重失信行为记录名单。

22.4、未实质性响应磋商文件的响应文件按无效响应处理,磋商小组将予以拒绝,供应商不得通过修改或撤销不合要求的偏离或保留而使其响应文件成为实质性响应的文件。

22.5、磋商小组将允许修正响应文件中不构成重大负偏离的、微小的、非正规的或不一致或不规则的地方,但这些修改不能影响任何供应商相应的名次排列。

## 23、磋商程序及评审方法和标准

### 23.1、磋商程序

23.1.1、对于通过资格性和符合性审查的供应商,磋商小组所有成员将集中与单一供应商分别进行磋商。

在磋商过程中,磋商小组可能根据磋商文件和磋商情况实质性变动的内容有:采购需求中的技术、服务要求以及合同草案条款。对磋商文件作出的实质性变动是磋商文件的有效组成部分,磋商小组将以书面形式同时通知所有参加磋商的供应商。

供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件,并由其法定代表人或授权代表签字或者加盖公章。

23.1.2、磋商文件能够详细列明采购标的的技术服务要求的,磋商结束后,磋商小组将要求所有实质性响应的供应商在规定时间内提交最后报价。第一轮报价(即响应文件中的报价)不公开唱标。

磋商文件不能详细列明采购标的的技术、服务要求,需经磋商由供应商提供最终设计方案或解决方案

的,磋商结束后,磋商小组将按照少数服从多数的原则投票推荐 3 家以上供应商的设计方案或者解决方案,并要求其在规定时间内提交最后报价。

最后报价是供应商响应文件的有效组成部分。根据“财政部关于政府采购竞争性磋商招标方式管理暂行办法有关问题的补充通知”,采用竞争性磋商方式招标的政府购买服务项目,在采购过程中符合要求的供应商(社会资本)只有 2 家的,竞争性磋商采购活动可以继续进行的。

23.1.3、磋商供应商未在磋商小组规定的时间内完成最后报价的视为放弃磋商,其磋商响应按无效响应处理。最后报价须由磋商供应商法定代表人或授权代表签字或者加盖公章。已提交响应文件的供应商,在提交最后报价之前,可以根据磋商情况退出磋商。

### 23.2、评审方法和标准

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

综合评分法,是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。评审时,磋商小组各成员独立对每个有效响应的文件进行评价、打分,然后汇总每个供应商每项评分因素的得分。

#### 23.2.2、评审标准

见本磋商文件第五章规定。

### 23.3、采购活动终止的情况

出现下列情形之一的,本次竞争性磋商采购活动将被终止:

- (1) 因情况变化,不再符合规定的竞争性磋商采购方式适用情形的;
- (2) 出现影响采购公正的违法、违规行为的;
- (3) 除本磋商文件第 23.1.2 条第三款规定的情形外,在采购过程中符合要求的供应商或者报价未超过采购预算的供应商不足 2 家的。

## 五、成交

### 24、确定成交供应商

24.1、磋商小组根据综合评分情况,按照评审得分由高到低顺序推荐 3 名以上成交候选供应商,并编写评审报告。符合本文件第 23.1.2 条情形的,可以推荐 2 家成交候选供应商。评审得分相同的,按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的,按照技术指标优劣顺序推荐。如合格磋商响应供应商数量等于拟确定成交的供应商数量,所有合格磋商响应供应商均为成交候选供应商。

24.2、采购人根据磋商小组推荐的成交候选人确定成交供应商。采购人确定成交供应商后,采购代理机构将在竞争性磋商公告发布媒体上发布成交结果公告,公告期限为 1 个工作日。

24.3、若有充分证据证明，成交供应商出现下列情况之一的，一经查实，将被取消成交资格：

- (1) 提供虚假材料谋取成交的；
- (2) 与评审专家、采购人、其他供应商或者采购代理机构工作人员恶意串通的；
- (3) 向评审专家、采购人或采购代理机构工作人员行贿或者提供其他不正当利益的；
- (4) 恶意竞争，最终总报价明显低于其自身合理成本且又无法提供证明的；
- (5) 不满足本磋商文件规定的实质性要求，但在评审过程中又未被磋商小组发现的；
- (6) 成交后无正当理由拒不与采购人签订政府采购合同或者未按照磋商文件确定的事项签订政府采购合同；
- (7) 将政府采购合同转包；
- (8) 法律、法规、规章规定的属于成交无效的其他情形。

#### 25、质疑处理

25.1、磋商供应商认为磋商文件、采购过程和采购结果使自己的权益受到损害的可以在知道或应知其权益受到损害之日起七个工作日内，以书面形式向采购代理机构一次性针对同一采购程序环节提出质疑，并将质疑材料原件送至采购代理机构。

上述应知其权益受到损害之日，是指：

- (1) 对可以质疑的磋商文件提出质疑的，为收到磋商文件之日；
- (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。

25.2、质疑必须按《政府采购法》、《政府采购法实施条例》的相关规定提交，未按上述要求提交的质疑函（含传真、电子邮件等）采购代理机构有权不予受理。

25.3、未参加磋商采购活动的供应商或在磋商采购活动中自身权益未受到损害的供应商所提出的质疑不予受理。

25.4、质疑函应当包括下列内容：

- (1) 质疑供应商的名称、地址、邮编、联系人、联系电话；
- (2) 具体的质疑事项及明确的请求；
- (3) 认为自己合法权益受到损害或可能受到损害的相关证据材料；
- (4) 提起质疑的日期；
- (5) 质疑函应当署名：质疑人为自然人的应当由本人签字并附有效身份证明。质疑人为法人或其他组织的，应当由法定代表人签字并加盖单位公章。质疑人委托代理质疑的，应当向采购代理机构提交授权委托书，并载明委托代理的具体权限和事项。

25.5、采购代理机构收到质疑函后,将对质疑的形式和内容进行审查,如质疑函内容、格式不符合规定,采购代理机构将告知质疑人进行补正。

25.6、质疑人应当在法定质疑期限内进行补正并重新提交质疑函,拒不补正或者在法定期限内未重新提交质疑函的,为无效质疑,采购代理机构有权不予受理。

25.7、对于内容、格式符合规定的质疑函,采购代理机构将在收到参加谈判供应商的书面质疑后七个工作日内作出答复,并以书面形式通知质疑供应商和其他相关供应商,答复的内容不涉及商业秘密。

25.8、供应商提出书面质疑必须有理、有据,不得恶意质疑或提交虚假质疑。否则,一经查实,采购代理机构有权依据政府采购的有关规定,报请政府采购监管部门对该供应商进行相应的行政处罚。

## 六、合同签订相关事项

### 26、签订合同

26.1、成交供应商确定后,采购代理机构以书面形式通知成交供应商领取成交通知书,成交供应商在收到书面通知之日起3个工作日内到江苏溧投招标服务有限公司领取成交通知书,逾期未领,则视为自动放弃成交资格。成交供应商应按成交通知书规定的时间、地点,按照磋商文件确定的事项与采购人签订政府采购合同,且不得迟于成交通知书发出之日起三十日内,由此给采购人造成损失的,成交供应商还应承担赔偿责任。

26.2、磋商文件、成交供应商的响应文件及磋商采购过程中有关澄清、承诺文件均应作为合同附件。

26.3、签订合同后,成交供应商不得将成交产品或服务进行转包。未经采购人同意,成交供应商也不得采用分包的形式履行合同,否则采购人有权终止合。转包或分包造成采购人损失的,成交供应商应承担相应赔偿责任。

### 27、履约保证金

本项目不交履约保证金。

## 七、政策功能

### 28、政策功能:

28.1、根据《常州市财政局关于新冠肺炎疫情防控期间加大政府采购支持中小微企业力度的通知》(常财购(2020)4号)的要求,落实相应措施。2020年度对小、微型企业产品的价格给予10%的扣除,用扣除后的价格参与评审。参加投标的中小企业,应当按照《政府采购促进中小企业发展暂行办法》(财库(2011)181号)的规定提供《中小企业声明函》(中小企业划型标准详见《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)。

28.2、参加投标的中小微企业,应当按照《政府采购促进中小企业发展暂行办法》(财库(2011)181号)的规定提供《中小企业声明函》(中小企业划型标准详见《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）；所投标产品的制造商为中小企业的，必须在“产地”栏内加填中小企业的完整名称，如未按要求填写和提供有效证明或相关内容表述不清的，不得享受价格扣除。

28.3、强制采购支持监狱和戒毒企业发展政策，监狱和戒毒企业提供的产品和服务在评标时获得优势，参加投标的监狱和戒毒企业，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，监狱和戒毒企业享受政府采购支持政策的要求详见财库【2014】68号。

28.4、政府采购促进残疾人就业政策，残疾人福利性单位提供的产品和服务在评标时将获得优势，参加投标的残疾人福利性单位，应当提供《残疾人福利性单位声明函》，残疾人福利性单位享受政府采购支持政策的要求详见财库【2017】141号。

28.5、强制采购节能产品、信息安全产品，优先采购环境标志产品节能产品、环境标志产品要求详见《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库209）9号）信息安全产品是指列入国家质检总局、国家认监委《信息安全产品强制性认证目录》并获得强制性产品认证证书的产品。

28.6、提供的产品属于信息安全产品的，供应商应当选择经国家认证的信息安全产品投标，并提供由中国信息安全认证中心按国家标准认证颁发的有效认证证书复印件。

28.7、提供的产品属于政府强制采购节能产品的，供应商应当选择《节能产品政府采购清单》中的产品招标，并提供参与实施政府采购节能产品认证机构出具的认证证书复印件。

28.8、提供的产品属于环境标志产品的，供应商应当选择环境标志产品政府采购清单中的，且经过认证的环境标志产品招标，并提供参与实施政府采购环境标志产品认证机构具有的认证证书复印件。

28.9、市级科技创新产品按《市政府办公室关于印发〈2020年常州市制造创新产品首购和推广推荐目录〉》（常政办发[2020]87号）执行。

28.10、根据财库（2011）59号文规定，如为信息系统项目，受托为整体采购项目或者其中分项目的前期工作提供设计、编制规范、进行管理等服务投标人不得再参加该分项目的采购活动。但属于《中华人民共和国政府采购法》第三十一条规定的单一来源方式采购情形的，不适用本条。

28.11、为推进社会诚信体系建设，根据财政部等政策要求，在政府采购活动中查询、使用信用记录，推进政府采购领域联合惩戒工作。

28.12、在政府采购活动中，通过“信用中国”、“中国政府采购网”、“诚信江苏”网站（江苏省项目）等渠道查询相关主体信用记录，对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的投标人，应当拒绝其参与政府采购活动。两个以上的自然人、法人或者其他组织组成一个联合体，以一个投标人的身

份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

## 第三章 合同格式

甲方: 溧阳市交通运输局

乙方:

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律法规的规定, 甲乙双方按照江苏溧投招标服务有限公司的中标结果签订本合同。

### 一、项目清单及合同金额(详见报价表, 附后)

1. 项目编号: \_\_\_\_\_。
2. 项目名称: \_\_\_\_\_。
3. 具体内容: \_\_\_\_\_ (详见乙方报价表)。
4. 合同金额: 人民币\_\_\_\_\_元(大写: \_\_\_\_\_)。

### 二、付款方式及期限

#### 1. 付款方式:

- (1) 本合同项下所有款项均以人民币支付。
- (2) 本合同项下的采购资金由甲方自行支付, 乙方向甲方开具发票。
- (3) 付款条件: 合同签订后支付合同金额的 30%的预付款, 施工进场材料全部到位后支付至合同金额的 60%, 验收合格后支付至合同金额的 95%, 验收合格满三年支付剩余 5%。

2. 项目验收合格后, 乙方须向招标代理机构出具《政府采购商品验收单》复印件。

### 三、交货时间、安装地点及交付方式

1. 交货时间: \_\_\_\_\_。
2. 交货地点: 采购人指定地点。
3. 交付方式: 免费送货上门, 并调试到能正常使用。

### 四、履约验收

采购人或者采购代理机构应当按照政府采购合同规定的技术、服务、安全标准组织对供应商履约情况进行验收, 并出具验收书。验收书应当包括每一项技术、服务、安全标准的履约情况。

### 五、保修条款、售后服务

严格遵守售后服务承诺, 产品在使用中出现任何问题, 甲方与乙方联系, 乙方在接到故障电话后\_\_\_\_小时(时间)内到达现场提供现场服务。有关内容如下:

1. 产品质保期为\_\_\_\_年。乙方承诺在保修期内, 若发生质量问题, 将免费负责更换或维修(同一产品, 同一质量问题连续两次维修仍无法正常使用的, 乙方必须更换相同型号产品)。在保修期外, 以最优惠的价格提供更换、维修。

2. 提供完整的培训计划, 为甲方培训多名系统维护、操作人员, 直至能独立操作设备。

3. 乙方在谈判文件中的其它服务承诺。

### 六、相关权利及义务

1. 甲方和见证方在验收时对不符合采购文件要求的产品有权拒绝接收和追究违约责任。

2. 见证方有权监督乙方的售后服务, 并对乙方的售后服务不符合谈判文件承诺内容时加以指出乃至追究合同责任。

3. 甲方、见证方在合同规定期限内协助履行付款责任。
4. 甲方、见证方对乙方的技术及商业机密予以保密。
5. 乙方有权按照合同要求及时支付相应合同款项。
6. 乙方有义务按谈判文件中的售后服务承诺提供良好的服务。

#### 七、违约责任

1. 甲乙双方均应遵守本合同, 如有违约, 将赔偿因违约给对方造成的经济损失, 并向对方支付本合同总额 5% 的违约金。若因乙方原因在合同规定期限内无法交货, 甲方有权终止合同, 并请示政府采购监管部门取消其中标资格, 经甲、乙双方协商同意继续履行合同, 甲方还将视情况在延迟交货期内每天按合同总额 3% 的标准收取违约金, 并提请政府采购监管部门将其列入不良行为记录。因不可抗力所导致的交货及付款延迟等按照《中华人民共和国合同法》有关条文及本合同第八条处理。

2. 乙方应严格遵守服务承诺, 如有违约, 将赔偿因服务违约给甲方造成的经济损失。若因乙方未按承诺的响应及到场维修时间进行排除故障, 甲方有权部分或全部扣除质量保证金; 若甲方电话通知乙方, 未按承诺时限到场维修, 超过 1 天未解决问题的, 甲方有权动用质量保证金进行故障处理, 并凭票扣除质量保证金, 追究服务违约的相关责任。

#### 八、不可抗力

甲方由于不可抗力的原因不能履行合同时, 应及时向乙方和见证方通报不能履行或不能完全履行的理由; 乙方由于不可抗力的原因不能履行合同时, 应在交货时间到期以前及时向甲方和见证方通报不能履行或不能完全履行的理由; 在取得有关主管机关证明以后, 可以签订延期履行、部分履行补充合同或者不履行合同, 并根据情况可部分或全部免于承担违约责任。

#### 九、争议

双方本着友好合作的态度, 对合同履行过程中发生的违约行为进行及时的协商解决, 如不能协商解决可向合同签约地法院通过法律诉讼解决。

#### 十、合同标的减少与追加处理

1. 如因在合同履行过程中有变更, 存在减少有关产品数量情况, 经甲乙双方现场确认, 报经审批后, 按乙方中标时的固定单价对总价进行调减, 并按有关规定签订补充合同。

2. 如因在合同履行过程中, 需追加与本合同标的相同的货物或者服务的, 在不改变合同条款的前提下, 经甲乙双方现场确认, 报溧阳市财政局审批后, 按乙方中标时的固定单价对总价进行调增, 并按有关规定签订补充合同, 但应注意追加增加的货物或者服务总价不得超过本合同金额的 10%。如追加的货物或者服务总价超过本合同金额的 10%, 按有关规定处理。

#### 十一、其它

1. 本合同一式五份, 甲方、乙方各执二份、招标代理机构执一份。
2. 本合同自签订之日起生效。
3. 本项目的采购文件、谈判文件等是本合同的附件, 与合同具有同等的法律效力。

4. 其它未尽事宜, 由双方友好协商解决, 并参照《中华人民共和国合同法》有关条款执行。

附件 1: 乙方报价表。

附件 2: 产品配置清单。

甲方(盖章):

乙方(盖章):

法定(授权)代表人:

法定(授权)代表人:

委托代理人:

委托代理人:

地址:

地址:

联系电话:

联系电话:

开户行:

账号:

## 第四章 项目需求

### 一、项目概况

信息时代的到来使得国家安全面临着前所未有的挑战。随着信息技术和网络技术的发展，以及互联网应用的广泛普及，信息安全已经成为国家安全的重要组成部分，特别是涉及国家安全和国计民生的基础信息网络和重要信息系统，因此为了适应新形势下的网络安全要求，进一步提高信息的保障能力，根据《信息安全等级保护管理办法》（公通字 2007【43】号）的精神，溧阳市交通运输局开展针对网络安全的整体规划，主要是安全等级保护改造以及安全服务；通过对智慧交通 IT 系统的安全等级划分，合理调配智慧交通 IT 系统的资源、信息科技资源、业务骨干资源等，重点确保智慧交通 IT 系统的核心信息资产的安全性，从而使重要信息系统的安全威胁最小化。切实改善信息安全治理和建设环境，加强风险控制，构建整体、严密、有效的信息安全等级保护体系。

### 二、建设需求

- (1) 针对溧阳市交通运输局的测评报告进行相应的网络安全整改，满足等级保护规范的相关要求；
- (2) 对溧阳市交通运输局的提供相关的安全服务，包括：风险评估、安全预警通告、应急响应、渗透测试、应急预案编写与演练等。

### 三、工程量清单

#### (1) 安全等级保护改造以及服务

序号	名称	数量	单位
1	抗拒绝服务系统	2	套
2	入侵防御系统	2	套
3	未知威胁检测	2	套
4	Web 应用防火墙	1	套
5	上网行为管理系统	1	套
6	漏洞扫描扩容	1	套
7	终端安全系统	200	点
8	日志审计系统	1	台
9	网闸	1	台
10	安全管理平台	1	套
11	安全管理平台-探针	1	套

12	风险评估服务	1	套
13	安全预警通告服务	1	套
14	应急响应服务	1	套
15	渗透测试服务	1	系统
16	应急预案编写及演练服务	1	套

#### 四、相关要求

##### 1、安全等级保护改造及服务

###### (1)、抗拒绝服务系统

指标项	规格要求
△基本要求	要求具备自主研发的安全操作系统, 且非 OEM 产品。
使用环境	采用专用的网络安全硬件架构, 采用自主知识产权的专用安全操作系统。
△硬件平台情况	电源规格: 冗余电源; 机箱规格: 1U; 接口配置: “6 个千兆电口” 含 HA 口、管理口; 扩展槽位: 1; 小包防御能力 (64 字节/pps): 88.8 万 pps, 最大保护服务器数量: 32 台, 最大 flow 数据处理能力: 100,000Flow/秒
△最大清洗能力	600Mbps
基本功能	支持在线串接、旁路检测和旁路清洗三种模式。
	支持 IPv4/IPv6 双栈方式;
	攻击日志一键了解攻击信息, 攻击类型、防护手段、攻击源分部、攻击大小等信息; 信誉日志的信誉 IP、时间等信息, 支持 CSV、XML、Html 等;
	系统支持统一平台管理, 在集群部署时支持对多台设备的集中管理, 日志收集, 运行状态监控, 策略下发等;
★防护自学习	支持针对防护对象的自学习功能; 学习结果图表展示, 展示了推荐阈值、最大阈值、最小阈值等; 支持针对学习周期, 自定义支持学习结果自动/手动方式配置防护规则 (提供产品功能截图证明并加盖厂商公章)
网络层清洗	包括但不限于: IP Fragment Flood、ICMP FLOOD、and attack、tcp misuse、udp misuse、tcpsscan attack、targa3 attack、smurf ack、fraggle attack、rr attack、sr attack、ip option attack、tracert attack、ping of death attack、redirect attack、

	unreach attack、icmp large attack、protocol null attack 等网络层 DoS 或 DDoS 攻击的清洗;
△传输层清洗	支持对 TCP flood、TCP FRAG flood、syn flood、ack flood、synack flood、fin flood、rst flood、TCP ABNORMAL FLAG FLOOD、新建 SESSION FLOOD 、SESSION FLOOD、UDP Flood、UDP FRAG flood、UDP 反射 flood 等传输层协议的清洗。支持对 cldap 反射端口攻击、memcached 反射端口攻击、ssdp 反射端口攻击; (提供产品功能截图证明并加盖厂商公章)
应用层清洗	支持在 IPv6/IPv4 双栈协议下的 HTTPS/HTTP、SIP、DNS、NTP 等协议的 DDOS 的防护;
★过滤器	支持基于 IP、TCP、UDP、ICMP、ICMPv6、HTTP、HTTPS、DNS、SIP、NTP、OTHER 等协议的自定义报文特征过滤; 支持基于应用协议的关键字段的过滤, 可过滤字段包括但不限于: 域名、源地理、源/目的 IP、IP 总长度、TTL、TOS、分片、分片偏移、源/目的端口、tcp 标记、tcp 窗口大小、udp 长度、icmp 类型/编码、icmpv6 类型/编码、起始偏移、深度、字符串、正则表达式、URL、host、请求方法、cookie、accept、x-forwarded-for、true-client-ip、location、refere、rcontent-encoding、body、content-length、version、questions、answers、authorities、additional、DNS 标记、查询类、查询类型等。支持基于源地理 IP 流量的过滤, 并且要求国内精准到省级、直辖市, 国外精准到具体国家; 支持多种处理方式, 如: 丢弃、跳过防御、白名单、黑名单、免认证名单、全局限速、IP 限速、debug 调试等动作。(提供产品功能截图证明并加盖厂商公章)
△抓包方式	自动抓包: 支持攻击时、流量异常时自动抓包留存电子凭证、并支持自定义抓包数量。(提供产品功能截图证明并加盖厂商公章)
△产品资质	中国信息安全测评中心颁发的《信息技术产品安全测评证书》(EAL3+级别)
	中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》(抗拒绝服务攻击(增强级))
★厂商资质	所投产品厂商提供 TL9000 电讯业质量管理体系认证证书
	所投产品厂商提供 CMMI 5 级证书
	所投产品厂商提供网络安全应急服务支撑单位证书(国家级)
	所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级



	所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级
--	---

## (2)、入侵防御系统

指标项	规格要求
△基本要求	要求具备自主研发的安全操作系统, 且非 OEM 产品。
△硬件配置要求	2U 机架式结构, 最大配置为 26 个接口, 默认 1 个管理口, 5 个 10/100/1000BASE-T 接口(支持 1 组 Bypass), 4 个 SFP 插槽; 2 个扩展槽位; 1TB 硬盘; 标配冗余电源。
△性能要求	整机吞吐量: 6Gbps 最大并发连接数: 120 万。
★系统要求	支持多操作系统引导, 出于安全性考虑, 多系统需在设备启动过程中进行选择, 不得在 WEB 维护界面中设置系统切换选项。(提供产品功能截图证明并加盖厂商公章)
入侵防御引擎	要求支持丢弃报文、记录日志、禁止连接、TCP reset 结束 TCP 会话等多种响应动作。
	要求支持自定义攻击检测规则。
	要求支持黑名单, 将攻击源加入黑名单, 一段时间内禁止访问
攻击特征库	应涵盖广泛的攻击特征库、能够针对 5900+ 种以上攻击的攻击行为、异常事件, 以及网络资源滥用流量, 进行检测和防御。
病毒特征库	支持 440 万以上病毒检测规则。
URL 过滤引擎	系统应具备独立的 URL 检测过滤引擎。
DDOS 防御	系统应支持独立的 DDOS 检测、阻断及防御基线自学习的能力。
	系统支持防御包括 land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_option、teardrop、targa3、ipspooof、Synflood、Icmpflood、Udpflood、Portscan、Ipsweep 等在内的 DOS/DDOS 攻击。
	★系统支持主机并发连接数和半连接数的限制。(提供产品功能截图证明并加盖厂商公章)
应用管理	系统应支持灵活的应用管理策略配置功能, 实现基于主机地址、区域、时间、应用等多维度的全面、细致监控。
	支持对应用协议的阻断和流量管控以及记录应用日志。
日志管理	系统应提供基于告警级别、时间、IP 地址、事件类型、等条件的日志检索功能, 具备日志导出备份、清除功能
	△系统应支持多种形式的日志存储, 本地存储、发送至日志服务器、本地日志服务器双存储、自动方式判断日志服务器状态自动决定日志的记录方式。(提供产品功能截

	图证明并加盖厂商公章)
系统展示	系统应支持按照时间、源 IP、源端口、目的 IP、目的端口、网络接口、风险级别等条件生成统计分析报表, 报表内容包括攻击防护、病毒过滤、应用管控、URL 过滤四大类。
	报表系统应支持报表以 word、html 格式导出。
	支持查看任意接口接受和发送报文字节大小分布图
	系统支持 web、命令行等多形式灵活安全策略配置。
	系统应提供邮件、声音、snmp 多形式的告警方式。
	△应支持设备机箱温度监视以及报警, 可以自定义温度阈值。(提供产品功能截图证明并加盖厂商公章)
	应支持实时查看网络流量/攻击状况
△产品资质	产品必须具备中华人民共和国公安部颁发的《计算机信息系统安全产品销售许可证》
	产品具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品检测证书》(EAL3+级)
★厂商资质	所投产品厂商提供 TL9000 电讯业质量管理体系认证证书
	所投产品厂商提供 CMMI 5 级证书
	所投产品厂商提供网络安全应急服务支撑单位证书(国家级)
	所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级
	所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级

## (3)、未知威胁检测

指标项	规格要求
△基本要求	要求具备自主研发的安全操作系统, 且非 OEM 产品。
△硬件配置要求	1U 标准机架式, 单电源, 标配 4 个 10/100/1000BASE-T 端口和 4 个 SFP 插槽, 其中 2 个 10/100/1000BASE-T 接口(作为 HA 口和管理口); 不支持接口扩展。默认带 1 年特征库升级授权
△性能要求	日志存储空间: 2T; 系统存储空间: 250G SSD
基本功能	软硬一体化标准机架式设备, 单台设备即可完成对 APT 攻击全生命周期的监测及数据分析与风险预警功能。

	<p>系统应具备流量采集、文件还原、文件静态和动态沙箱检测、web 攻击检测、异常行为分析、数据分析与风险预警等功能，能够检测已知/未知恶意文件，0Day/nday 漏洞利用，Web 攻击，恶意扫描攻击等；还支持对失陷主机、DGA 域名、动态域名、隐蔽信道、异常协议等异常通信行为进行分析告警。</p> <p>支持在 IPv4、IPv6、IPv6 和 IPv4 混合网络环境下提供 APT 攻击全生命周期的监测及数据分析与风险预警功能。</p>
文件还原	支持检测文件格式自定义，如：新增 .do 后缀类型的文件，系统对此类型文件进行实时检测。
△检测引擎	具备动态行为检测引擎、机器学习检测引擎、威胁情报检测引擎、AV 检测引擎、CVE 检测引擎、YARA 规则检测引擎等文件检测引擎，且每种检测引擎均可输出各自检测结果。（提供产品功能截图证明并加盖厂商公章）
文件 hash 检测	支持对所有已检测过的文件 HASH 进行统一存储，并提供搜索、查看、重新检测功能。
★机器学习	支持 3 种以上机器学习算法模型（静态检测模型、动态检测模型、静态和动态混合检测模型）对文件进行威胁判定，且每种机器学习模型会对所支持的样本文件进行检测，输出不同的机器学习算法对样本恶意与非恶意的判定结果。（提供产品功能截图证明并加盖厂商公章）
攻击检测	支持攻击事件会话 PCAP 文件记录、存储和 PCAP 文件在线查看功能。
★隐蔽信道检测	支持 DNS、HTTP、ICMP 至少三种协议的隐蔽信道通信检测。（提供产品功能截图证明并加盖厂商公章）
KILLCHAIN 关联分析	△支持交互式的 KILLCHAIN 可视化分析功能，对攻击过程智能化关联分析，方便还原攻击过程，对攻击进行溯源追踪。（提供产品功能截图证明并加盖厂商公章）
	支持在单一界面内对系统检测到的各类攻击行为按照网络杀伤链不同阶段进行展示，以全局的视图呈现网络中指定资产遭受到的攻击情况并支持按照攻击阶段、威胁类别、时间周期进行过滤筛选。
网络安全知识库	提供网络安全知识库，能够为系统检测的威胁信息并提供知识说明。知识库内容包括威胁类型、威胁标签、描述信息、受影响范围、处置建议、参考信息、代码示例、流量示例、安全普及知识、时间线等信息。
△产品资质	中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》
	中国信息安全认证中心颁发的《IT 产品信息安全认证证书》，测试标准为：ISCCC-TR-083-2018《APT 安全监测产品安全技术要求》

★厂商资质	所投产品厂商提供 TL9000 电讯业质量管理体系认证证书
	所投产品厂商提供 CMMI 5 级证书
	所投产品厂商提供网络安全应急服务支撑单位证书（国家级）
	所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级
	所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级

## (4)、WEB 应用防火墙

指标项	规格要求
△基本要求	要求具备自主研发的安全操作系统，且非 OEM 产品。
△硬件配置要求	1U 机架式结构；最大配置为 24 个接口；默认包括 2 个可插拨的扩展槽和 6 个 10/100/1000BASE-T 接口和 2 个 SFP 插槽；（默认 ETH2 口和 ETH3 口具有 Bypass 功能）单电源；含 1 年特征库升级服务。内含 SQL 注入、XSS、CSRF 等 WEB 攻击防护功能、URL 访问控制功能、防盗链功能、WEB 漏洞扫描功能、DDOS 攻击防护功能、网页防篡改功能、服务器负载均衡功能、报表分析及告警功能
△性能要求	网络层吞吐>3.5G，应用层吞吐 500Mbps，
网络部署	支持基于域名和 IP 多种方式提供网站防护。
	支持静态路由，策略路由，ISP 路由配置。
安全防护	△支持 HTTP/HTTPS 站点防护，在代理模式下支持 HTTPS 流量解析，支持 SSL 卸载功能。（提供产品配置截图证明并加盖厂商公章）
	支持网络层访问控制，支持基于源 IP、目的 IP 及源目的区域、服务类型、地理位置区域等条件的访问控制。
	支持 IP 黑白名单配置。
	支持 2600+ 的应用层安全防护规则
	应能识别和阻断 SQL 注入攻击, Cookie 注入攻击, 命令注入攻击;
	★支持恶意扫描防护：通过人机识别方式，进行恶意扫描智能检测；支持扫描防护阈值设置和扫描 IP 的阻断周期设置。（提供产品配置截图证明并加盖厂商公章）
应能识别和阻断跨站脚本 (XSS) 攻击	

	<p>具备 WebShell 攻击, 文件包含漏洞利用、目录遍历等攻击的防护功能</p> <p>△支持多重编码检查功能, 可对多重的编码均进行安全防御检查, 有效防止攻击绕过 WAF。(提供产品配置截图证明并加盖厂商公章)</p> <p>支持防护动作自定义, 包括告警、拒绝、重定向, 错误页面等多种防护动作, 同时支持返回错误页面自定义。</p> <p>支持对 HTTP 协议合规性进行验证, 提供 HTTP 协议规范化功能, 可自定义最大请求头长度、最大 body 长度、最大请求行长度、最多 cookies 个数、最多 header 头个数等。</p> <p>对 DDoS 流量支持检测清洗和强制防御两种模式, 检测清洗根据是否到达阈值对流量进行清洗, 强制清洗对所有流量直接进行流量清洗判断。</p> <p>★支持虚拟补丁功能, 支持导入 WAF 内置扫描器及 appscan、w3af 等第三方扫描器的扫描结果生成 WAF 的防护规则, 对此类网站漏洞直接防护。(提供产品配置截图证明并加盖厂商公章)</p>
数据分析	<p>支持对防护的 WEB 服务器进行健康检查, 可以实时监测服务器的活跃状态, 并且可定期备份健康记录。</p> <p>可以查看通过 WAF 的所有 IPV4 及 IPV6 客户端和服务器 IP 地址及端口连接数及状态。</p> <p>可以实时查看设备并发连接数、每秒事务数及 HTTP 应用层吞吐率等数据并以可视化的方式展示。</p> <p>支持对攻击事件类型, 攻击源, URL 攻击次数统计, 动作统计等 WEB 安全信息进行可视化展示。</p> <p>可以实时查看设备 CPU、内存、硬盘等自身使用率情况</p>
系统管理	<p>支持 WEB 界面、SSH、Console 等多种方式进行设备配置管理, 支持通过 WEB 界面直接跳转到控制台 Console 界面。</p> <p>支持 ping、TRACEROUTE、TCP、HTTP、DNS、抓包工具等多种故障诊断方式。</p> <p>支持规则库的在线升级和离线升级。</p>
△产品资质	<p>计算机信息系统安全专用产品销售许可证, 提供证书复印件并加盖原厂公章</p> <p>国家信息安全测评信息技术产品安全测评证书 EAL3+级证书, 提供证书复印件并加盖原厂公章</p>

★厂商资质	所投产品厂商提供 TL9000 电讯业质量管理体系认证证书
	所投产品厂商提供 CMMI 5 级证书
	所投产品厂商提供网络安全应急服务支撑单位证书（国家级）
	所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级
	所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级

## (5)、上网行为管理系统

指标项	规格要求
△基本要求	要求具备自主研发的安全操作系统，且非 OEM 产品。
△硬件配置要求	标准机架尺寸，2U 高度；1 个串口 (RJ45)，2 个 USB2.0 接口，6 个千兆电口，2 个 SFP 插槽和 2 个可插拨的扩展槽；支持 1 对 Bypass；标配双电源；默认含一年系统版本升级、URL 库及应用特征库升级许可
△性能要求	16G 内存；设备至少支持 ≥1TB 硬盘。
网络功能	支持路由模式，旁路模式、网桥模式、混合模式部署。
	△支持基于应用层服务和 SAAS 的策略路由，可基于 IP、国家列表、ISP 自动地址表和域名来控制目的地址；（提供产品配置截图证明并加盖厂商公章）
	支持 PPPoE 拨号以及负载均衡。
	支持基于链路上行、下行、总流量自动均衡的多链路负载均衡算法，基于固定指派链路的自动均衡算法，基于最佳路径的多链路负载均衡算法；
安全防护	支持基于策略方向、源地址、目的地址、服务、生效时间的安全策略。
	支持移动终端发现后拒绝移动终端接入并支持启用事件告警。支持移动终端列表添加信任列表。
	支持对 TCP、UDP、ICMP、TCP SYN 超时时间，无回应 UDP 超时时间设置，并能支持按照新建会话与总会话比例设置老化开始或者结束。
用户管理	支持按照公司架构创建用户组、用户、支持多层组和用户，分组能继承父组策略，用户能继承组的策略。
	支持隐藏设备源地址，替换成可自定义的伪装地址。

	★支持通过磁卡识别用户身份, 并对用户做控制。(提供产品配置截图证明并加盖厂商公章)
行为管控	支持 6000 种以上的应用, 至少支持 2400 种以上的移动应用
	支持 L2TP 协议剥离、GRE 协议剥离、LWAPP 协议剥离、CAPWAP 协议剥离, 并支持自定义协议剥离。 ★支持基于授权签名的方式实现 https 审计免除告警的行为。(提供产品配置截图证明并加盖厂商公章)
流量管理	支持基于源 ip、地址簿、用户及用户组的流控策略。支持基于每个人的限速以及整体限速。
	支持每个用户的源, 目的活跃连接数控制, 避免网络滥用
	支持基于用户、协议、应用、url、文件类型的带宽保障行为, 可以通过队列实现重要业务优先转发。
日志分析	支持无线环境下, 移动终端接入识别, 对未添加信任的黑名单支持拒绝加入网络。发现移动终端后, 可支持拒绝该移动终端, 或者告警。
	为了日志安全性, 设备必须支持独立硬盘存放审计日志, 不能与审计系统共用硬盘。
	设备必须支持内置报表中心, 默认自带数据库无需再安装数据库。
	支持通过集中管理平台或者 ftp 方式备份日志。
行为分析	能够进行层层深入的递进式查询, 获取某应用对应的用户, 或某用户使用网络应用的情况, 便于对网络使用现状进行深入分析。
	通过对网络线路实时流量趋势、以及应用流量、用户流量进行展示, 统计分析出每条专线的负载情况, 从而实时地掌握校园网络线路的使用情况。
	支持对内网用户的主机进行分析, 判断是否具有挖矿、勒索病毒、垃圾邮件行为等, 分为高位和潜在区分。
△产品资质	支持用户上网过程中的告警分析, 以折线图和饼状图等多角度, 罗列违规用户和行为记录, 展示给管理员。
	公安部网络安全保卫局《计算机信息系统安全专用产品销售许可证》
★厂商资质	中国信息安全认证中心颁发《IT 产品信息安全认证证书》 所投产品厂商提供 TL9000 电讯业质量管理体系认证证书

所投产品厂商提供 CMMI 5 级证书
所投产品厂商提供网络安全应急服务支撑单位证书（国家级）
所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级
所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级

**(6)、漏洞扫描扩容**

序号	产品要求	功能与技术描述
1	WEB 应用漏洞扫描能力	<p>产品提供 Web 应用扫描能力, 提供多种 Web 应用漏洞的安全检测, 如 SQL 注入、跨站脚本、网站挂马、网页木马、CGI 漏洞等。</p> <p>可在界面中列出被检测网站的目录结构</p> <p>Javascript 解析引擎的支持, 能从 Javascript 代码中分析出 url。</p> <p>支持基于 basic、NTLM、Cookie 等认证方式的 Web 应用系统安全扫描。</p> <p>支持登录预录制功能, 能够根据用户操作, 录制并指定 Web 扫描 url, 使产品能够扫描和分析一些常规页面爬取程序检测不到的 url。</p>

**(7)、终端防御系统**

指标项	规格要求
△基本要求	要求具备自主研发的安全操作系统, 且非 OEM 产品。
基本要求	系统支持中/英文界面, 系统部署采用 C/S 架构, 管理采用 B/S 架构, 管理员只需通过浏览器登录控制中心, 即可对系统进行管理。
系统部署	<p>客户端安装支持本地安装、WEB 安装</p> <p>支持级联部署及管理, 可实时查看下级终端威胁及在线情况, 上级可对下级灵活分配授权, 同时可实现分级管理中心能够通过一级管理中心升级病毒库和客户端版本。</p>
终端环境	<p>客户端至少支持 WindowsXP、Windows 7、Windows 8、Windows 10 等 32 位/64 位终端操作系统, 支持 Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、Windows server 2019 等 32 位/64 位服务器操作系统。</p> <p>支持 Linux 操作系统以及中标麒麟、银河麒麟、中科方德、深度、UOS 等国产操作系统和人大金仓、达梦数据库等</p> <p>支持虚拟机、主流虚拟化终端环境 (VMware、华为、华三、阿里、腾讯等)</p>



	客户端安装后至多占用 50M 硬盘资源, 日常内存占用不到 20M, 有效节省 PC/Server 资源
系统管理	管理中心支持实时显示客户端的状态及终端基本信息, 包括客户端连接状态、服务状态; 终端机器名称、客户端版本、病毒库版本、IP 地址、MAC 地址、操作系统版本、高危及功能漏洞、主板信息、显卡信息、内存大小和物理位置等信息, 并支持终端信息导出
	支持即时/定时实现客户端病毒查杀, 支持下发关机、重启、升级、病毒查杀、重新连接、漏洞扫描、漏洞修复、显示消息、后门检测 (linux)、分发设置等操作, 并对以上操作配置详情, 客户端执行情况跟踪, 实现管理中心对客户端的任务状况监控
	支持终端防卸载、防退出功能, 管理员能够统一设置防卸载密码, 防止终端用户随意脱离保护。
	△支持远程控制, 通过管理中心实现对客户端的远程运维。(提供产品功能截图证明并加盖厂商公章)
	可设置不同的管理员角色, 每个角色分配不同的操作权限和终端权限
	支持控制中心访问控制, 包含 WEB 访问控制定制超时时间、登录重试次数、IP 锁定时长及解锁, IP 访问控制指定具体 IP 可访问控制中心。
	支持定制磁盘管理规则, 对审计日志、系统日志、终端日志、告警日志等即时或定期清理, 实现磁盘瘦身
终端防御	支持对终端内部文件进行全盘扫描、快速扫描, 自定义扫描三种扫描能力, 同时支持错峰扫描。
	支持基于虚拟沙盒的高效的本地反病毒引擎, 实现极高的本地查杀能力。
	★设置诱饵文件并实时监控, 当勒索病毒对该文件进行加密操作时进行拦截。(提供产品功能截图证明并加盖厂商公章)
	主动对 U 盘中的文件进行扫描, 对 U 盘传播类恶意软件常见恶意修改操作进行修复
	支持黑客入侵拦截功能, 针对网络数据流的深层分析, 检测入站流量, 提供虚拟补丁保护应用程序免受攻击, 有效阻止勒索病毒等高危威胁的入侵。
★对系统关键位置进行防护, 阻止无文本攻击、流氓、广告程序对系统的恶意篡改等行为。从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护 (提供产品功能截图证明并加盖厂商公章)	
系统管理	对流氓软件、弹窗广告能够实现智能拦截, 同时也可以自定义添加截图拦截弹出。

	支持启动项管理,对相关启动项进行一键优化,阻止终端不必要的程序启动。
	支持统计分析客户端上报的威胁日志,包含病毒排行统计、趋势统计等多维度,并进行图表显示。
	支持对客户端上报的安全日志进行审计、可通过预置字段及自定义字段结合自定义历史时间过滤详细日志,能够快速定位终端安全状况。
	客户端上报的告警日志,可预置字段及自定义字段过滤详细日志,快速定位终端安全状况;定制符合企业敏感程度的告警规则,达到告警阈值,产生告警日志并通过邮件推送给管理员,保证告警及时性。
△产品资质	中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》 中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》(EAL3+级)
★厂商资质	所投产品厂商提供 TL9000 电讯业质量管理体系认证证书
	所投产品厂商提供 CMMI 5 级证书
	所投产品厂商提供网络安全应急服务支撑单位证书(国家级)
	所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级
	所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级

## (8)、日志审计系统

指标项	规格要求
△硬件配置要求	1U 机架式设备; 16G 内存; 250G SSD 系统盘; 数据存储容量 4T, Raid5, 自带 7 千兆电口 (2 管理口+4 数据口+1 BMC 口), 6 USB 接口 (含 2 个 3.0); 单电源; 含 50 日志源授权
△性能要求	日志综合采集处理峰值: 5000EPS。
部署方式	支持单级部署; 支持代理分布式部署采集日志。
基本要求	支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于 26 类 300 种日志对象的日志数据采集;
	对所管理设备的日志原始数据完整存储, 支持数据本地集中存储;
	内置系统运行相关告警规则, 包括检测到新日志源、节点掉线、主动日志源长期不外

	发日志、存储上限告警、主机认证失败等, 可启用/禁用规则;
功能要求	△数据存储能力: 压缩加密存储, 压缩比不低 10:1; 日志存储不低于 10000 条/M ; (提供产品功能截图证明并加盖厂商公章)
	支持百亿级数据交互式多条件查询, 百亿级数据查询响应时间小于 10s;
	★支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率, 降低对系统资源的占用, 保障重要日志的收集; (提供产品功能截图证明并加盖厂商公章)
	支持日志转发给第三方系统平台, 支持设置多个日志转发 IP 地址, 支持转发格式化日志或仅转发原始日志;
	支持对所管理设备的日志原始数据完整存储, 支持数据本地集中存储、网络存储;
	支持日志备份功能, 支持本地备份和 FTP 备份方式, 支持自动备份和手动备份;
	△支持为不同类型日志设置不同的查询条件和显示条件; (提供产品功能截图证明并加盖厂商公章)
	支持安全告警概况、安全告警趋势的统一展示, 实时告警可根据级别、规则类型等进行分类;
	★支持基于时间轴展示告警数据分布, 能够通过时间轴进行查询分析; (提供产品功能截图证明并加盖厂商公章)
	支持邮件、Snmp Trap、声音、声光、短信、一信通响应、数据库响应等多种告警方式, 支持报警内容引用字段变量参数。
	支持手动添加日志源, 管理员可以对日志源进行查看、批量修改、添加、编辑、删除以及启\禁用的操作;
	△支持对重点日志源的关注设置, 并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息; (提供产品功能截图证明并加盖厂商公章)
	支持基于策略的多日志源海量日志实时关联分析, 发现安全事件实时告警。
支持将日志源管理权限分配给不同的操作管理员, 不同用户管理不同日志源的日志, 互不干扰;	
△产品资质	具备公安部颁发的《《计算机信息系统安全专用产品销售许可证》, 提供证书复印件并加盖原厂公章

	具备中国信息安全认证中心颁发的《IT 产品信息安全认证证书》，提供证书复印件并加盖原厂公章
△厂商资质	所投产品厂商提供 TL9000 电讯业质量管理体系认证证书
	所投产品厂商提供 CMMI 5 级证书
	所投产品厂商提供网络安全应急服务支撑单位证书（国家级）
	所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级
	所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级

## (9)、网闸

指标项	规格要求
△基本要求	要求具备自主研发的安全操作系统，且非 OEM 产品。
△硬件配置要求	电源规格:单电源;机箱规格:2U;接口配置:内外端机双侧液晶屏; 内端机 6 个 10/100/1000Base-T 接口, 2 个 SFP 插槽, 1 个扩展槽位; 外端机 6 个 10/100/1000Base-T 接口, 2 个 SFP 插槽, 1 个扩展槽位; 内外端机各 1TB 硬盘。
△性能要求	网络吞吐量: 1G; 并发连接数: 20 万;
硬件架构	硬件架构由内端机、外端机、专有隔离硬件三部分组成。内端机和外端机各自具有独立主板、独立总线, 独立的存储和运算单元; 内端机和外端机之间非网线、USB 线、SCSI 线等线缆直连, 基于光隔离技术专有硬件进行隔离和数据交换。
安全浏览功能	支持 IP 地址、端口、时间以及基于源用户身份的访问控制策略。 ★内置 HTTP 安全模块, 支持 URL 过滤引擎、内容过滤引擎、文件过滤引擎、病毒过滤引擎、网页过滤引擎安全防护及单独启停控制。(提供产品功能截图证明并加盖厂商公章)
文件传输功能	提供基于 FTP 协议和 TFTP 协议的文件传输功能。
	支持代理、透明、路由三种接入方式 △支持 FTP 协议内部命令及数据层内容过滤, 支持允许、阻断、告警三种处理方式 (提供产品功能截图证明并加盖厂商公章)
数据库访问功能	提供对多种主流数据库, 如: MYSQL、SQLSERVER、ORACLE、DB2、SYBASE 等系统的安全访问。

	△内置数据库安全模块, 支持内容过滤引擎, 能够对数据库用户名、命令、关键字等内容进行管控, 支持允许、阻断、告警三种处理方式。(提供产品功能截图证明并加盖厂商公章)
文件同步功能	提供有客户端和无客户端两种文件同步方式。
	支持 NFS、FTP 等多种文件服务器类型, 支持实时同步和周期性同步。
	支持基于文件大小和文件修改时间的同步策略, 可手动指定上下限阈值
	支持首次同步策略处理, 可选合并和完全一致两种处理方式
数据库同步功能	提供有客户端和无客户端两种数据库同步方式。
	提供多种主流数据库系统如: ORACLE、SQLSERVER、MYSQL、达梦数据库的同步。
	支持一对一、一对多、多对一方式的数据库同步; 支持同构、异构数据库之间的同步, 同步可具体设置到字段级别。
	★支持网闸同侧数据库之间的数据同步, 网闸可旁路部署实现数据库同步(提供产品功能截图证明并加盖厂商公章)
安全防护	支持企业版和专业版双病毒防御引擎, 采用国内外知名厂商病毒库, 支持病毒库升级, 并提供后续升级服务。
	△支持基于 URL 分类知识库的 web 网站过滤功能, 支持 URL 知识库的升级, 并提供后续升级服务。(提供产品功能截图证明并加盖厂商公章)
	支持 DOS 攻击防御, 支持端口扫描防御、IP 扫描防御、支持 IP\TCP\UDP 源限速和目的限速, 可手动设置相关阈值。
系统管理	管理端通过独立的管理口与网闸内端机相连, 策略统一从内端机下发, 不允许采用外端机上的任何网络接口进行管理。
	提供统一的 https 管理界面, 支持 ssh 和 telnet 远程管理, 支持配置文件的加密导入导出。
	提供固件维护和 license 升级功能, 支持本地、FTP、TFTP 三种导入方式。
日志审计	支持日志审计功能, 包括管理日志、系统日志、策略日志、同步日志和应用行为日志。支持日志记录查询、删除、导出, 日志记录可导出文本文件和数据库文件两种格式。
	支持日志记录本地数据库存储, 也可以将日志传输到独立的日志服务器上, 传输日志格式支持 syslog 和 welf, 支持日志加密传输。
△产品资质	公安部计算机信息系统安全专用产品销售许可证书(增强级)

	信息安全认证中心中国国家信息安全产品认证证书（二级）
△厂商资质	所投产品厂商提供 TL9000 电讯业质量管理体系认证证书
	所投产品厂商提供 CMMI 5 级证书
	所投产品厂商提供网络安全应急服务支撑单位证书（国家级）
	所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级
	所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级

## (10)、安全管理平台

指标项	规格要求
△硬件配置要求	软硬件一体形态, 2U, 双 CPU, 128G 内存, 256GB SSD 硬盘+24TB SATA 硬盘, 支持 RAID, 板载 2 千兆电口+2 万兆光口, 4 千兆电口卡+2 万兆光口卡, 双电源。
态势展示	支持态势大屏展示, 包括全网态势、资产态势、漏洞态势、攻击态势, 支持大屏展示时间设置, 支持态势大屏中相关信息下钻跳转到对应的详细页面。
	支持全网资产概述、高危资产、漏洞、告警趋势、安全日志趋势、告警统计、最新告警名称和影响范围、热点威胁等内容的相关展示
	支持通过轮播进行资产总量、漏洞总数、日志总数相关信息的展示, 支持按资产类型及失陷状态进行展示, 支持按漏洞级别进行展示, 支持按日志级别进行展示
	★支持主动发现内网漏洞功能并关联资产, 漏洞分析类型包含 Web 安全、windows 安全、通用等漏洞; (提供产品功能截图证明并加盖厂商公章)
功能要求安全监测	支持日志实时监视, 支持按照设备 IP、设备类型、事件级别、过滤器等条件进行事件分类监视, 支持清空日志显示列表、停止和启动刷新、刷新闻隔设置
	△支持资产性能监测概览, 支持监测设备总数、异常数、主机异常数、网络设备异常数、安全设备异常数展示, 支持监控资产性能状态占比、性能告警 TOP10、规则类型事件分布、CPU 使用率 TOP10、内存使用率 TOP10、磁盘使用率 TOP10, 支持性能监控详细列表, 包括 IP、资产名称、归属安全域、资产类型、性能状态、连通状态、CPU 使用率、内存使用率、磁盘使用率、操作等 (提供产品功能截图证明并加盖厂商公章)
	支持对安全处置情况进行概览分析, 包括待处置告警数、待处置漏洞数、待处置风险资产数、待处置威胁源数、待处置漏洞 TOP5、风险资产 TOP5、威胁源 TOP5

	△支持在我的工单分组中进行工单分派、取消、查看详情、查看流程图等操作, 支持新建工单, 包括工单名称、级别、派单人、业务流程、描述等信息, 支持工单统计报表导出 (提供产品功能截图证明并加盖厂商公章)
安全分析	支持至少 50 种日志展示字段, 支持列集分组自定义、保存及快速切换, 支持 pcap 导出、预览, 支持检索日志的导出, 包括但不限于 txt、csv、excel, 支持按时间序列统计日志
	支持对日志的详情展示, 支持日志的详情、溯源、附件、一键封堵、加入白名单、加入关注名单、封堵申请等操作
	★支持对全部资产进行画像分析, 支持以列表形式展示资产相关信息, 展示信息包括不限于资产名称、IP、风险等级、失陷状态、漏洞、告警、遭受攻击阶段等, 支持按照日期、IP 地址、风险等级、失陷状态、告警、遭受攻击阶段、资产类型、是否有暴露面等条件进行过滤查询, 支持至少 10 种展示列自定义, 支持按照 TXT、CSV、EXCEL 等格式进行资产信息导出 (提供产品功能截图证明并加盖厂商公章)
资产管理	支持资产管理, 支持资产新增、修改、删除, 支持自定义资产信息, 包括资产三性等基本信息、资产类型、所属业务系统、所属物理位置、责任人、漏洞、补丁及软硬件信息等, 支持资产批量删除、资产导出、资产导入, 支持资产模板下载, 支持资产详情查看, 详情包括资产属性基本信息、资产相关漏洞信息, 可视化呈现资产的多维度信息;
	支持综合查询, 支持资产基本信息查询、用户基本信息查询、资产漏洞信息查询、资产补丁信息查询。
集中管控	支持管控拓扑图展示, 支持拓扑动态提示管理设备产生的告警, 支持拓扑图右击直接查看选中设备的设备概览、设备详情、告警列表等信息
	△支持策略管理, 支持策略新建、删除、查看、编辑、下发、下发记录等, 支持策略标签管理, 策略内容包括名称、标签、设备类型、执行设备、策略分类、配置项类型、状态、源地址、源端口、目的地址、目的端口、终端地址 (提供产品功能截图证明并加盖厂商公章)
知识情报	支持系统使用云端情报和离线情报, 支持对云端威胁情报来源配置包括接口地址、用户名、密码, 支持对离线威胁情报进行导入
	支持内生情报管理, 包括恶意 IP 地址、恶意 URL、恶意样本、恶意域名、垃圾邮件等, 支持情报进行分类自定义查询, 支持自定义威胁情报信息, 支持威胁情报的导

	入
系统设置	支持 WEB 页面升级补丁, 包括补丁导入、应用、还原、下载、删除、查看等操作, 支持 WEB 页面重启系统
△产品资质	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》, 提供证书复印件并加盖原厂公章
	具备网络关键设备和网络安全专用产品安全认证证书(中国网络安全审查技术与认证中心), 提供证书复印件并加盖原厂公章
△厂商资质	所投产品厂商提供 TL9000 电讯业质量管理体系认证证书
	所投产品厂商提供 CMMI 5 级证书
	所投产品厂商提供网络安全应急服务支撑单位证书(国家级)
	所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级
	所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级

## (11)、安全管理平台-探针

指标项	规格要求
△硬件配置要求	2U 机架式机构; 冗余电源; 默认接口 6 个电口、4 个千兆光口; 5 个扩展槽位; 50 个最大接口配置; 支持液晶屏;
△性能要求	最大并发连接数: 150 万; 综合检测性能: 3G
基本要求	支持对设备 WEB 页面、命令行方式配置管理, 可直接从 web 中实现命令行方式管理。
	支持设置 CPU 利用率、内存利用率、硬盘利用率、CPU 温度、系统温度、并发连接数、新建连接数的监控阈值。
	★支持攻击检测规则库、应用识别规则库、URL 分类规则库、僵尸主机规则库、威胁情报库、地理信息库, 各规则库相互独立。(提供产品功能截图证明并加盖厂商公章)
攻击检测	支持独立的攻击检测引擎, 支持 8500 种以上的攻击规则库。



	支持扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问攻击、注入攻击、URL 跳转、跨站攻击、Webshell、浏览器劫持、文件漏洞攻击等多种常见攻击行为。
	支持对 SMTP、POP3、IMAP、FTP、TELNET、LDAP、RDP 等服务的弱口令登录行为检测，采用弱口令字典和口令强度两种方式检测，可自定义口令度规则，如密码长度、密码字符类型等。
僵木蠕检测	△采用僵尸主机与控制主机异常通信行为检测的方式，具有独立的僵尸主机特征库，能够对 10000 种以上僵尸主机行为进行监测，包括僵尸网络行为、木马控制行为、蠕虫活动行为、挖矿行为、勒索软件行为、移动端木马控制行为、APT 行为等多类型的僵尸主机行为。（提供产品功能截图证明并加盖厂商公章）
	支持对检测到的控制主机数量、僵尸主机数量实时统计，记录控制主机的活跃次数，控制了多少僵尸主机、地理位置监控，且支持以地图的形式展现控制主机的地理分布。
DDoS 检测	支持独立的 DDoS 检测引擎，支持对 IP 扫描攻击、TCP 扫描攻击、端口扫描攻击等多种扫描攻击行为检测；支持对 ICMP FLOOD 攻击行为、SYN FLOOD 攻击行为、ACK FLOOD 攻击行为、SYN ACK FLOOD 攻击行为、RST FLOOD 攻击行为、UDP FLOOD 攻击行为、DNS REQUEST FLOOD 攻击行为、DNS REPLY FLOOD 攻击行为、HTTP URI CC 攻击检测、HTTP FLOOD 攻击行为、HTTPS FLOOD 攻击行为等多种 FLOOD 攻击行为检测。
	支持 DDOS 自学习模式检测，可设定学习时长，根据周期内流量状态自动学习，设置流量阈值。流量状态异常触发阈值，系统自动进行告警。
恶意程序检测	★支持对恶意程序实现特征检测、机器学习检测、内置虚拟沙箱检测等多种检测方式，并且多种检测方式相互独立、互不影响；支持专业沙箱设备联动检测。（提供产品功能截图证明并加盖厂商公章）
	机器学习检测能够对目标文件实时检测实时还原效果，不依赖规则库检测实现对未知恶意程序检测。
	支持对恶意文件还原捕获，可自定义捕获文件大小，支持对恶意文件、疑似恶意文件、无风险文件还原。支持对还原捕获的恶意文件使用 FTP 服务、SFTP 服务外发第三方平台。
APT 检测	支持通过威胁情报检测已知 APT 事件，通过恶意程序检测未知 APT 事件，通过僵尸行为规则库检测已知的 APT 组织。

WEB 安全检测	支持对 SQL 注入攻击、跨站攻击、浏览器劫持攻击、URL 跳转攻击、WEB 远程代码执行攻击、WEB 缓冲区溢出攻击、WEB 漏洞攻击、Webshell 上传攻击、WEB 越权攻击、WEB 扫描攻击、目录遍历攻击、WEB 口令暴力破解攻击等多种类型的 WEB 攻击检测。
虚拟沙箱	支持模拟仿真沙箱环境, 对文件进行扫描分析、脱壳分析、动态行为分析等深度检测, 脱壳分析支持多层壳、虚拟 机保护壳、自定义壳、高级包裹器。
威胁情报	本地嵌入独立的威胁情报库, 不依赖其他设备或情报平台, 即可独立的实现威胁情报检测能力。 威胁情报库数量超过 790 万, 可通过手动添加、批量导入的方式自定义威胁, 并且满足威胁白名单能力。
加密流量检测	支持卸载 SSL, 实现对 HTTPS、SMTPS 等加密流量的分析检测。
溯源取证	支持攻击取证、僵尸主机取证、恶意程序取证、威胁情报取证, 取证类型支持报文取证和样本文件取证两种形式。
URL 检测	支持数量超过 1000 万的 URL 地址库, URL 类型涉及包括搜索引擎、购物、社交、招聘求职、财经、下载、政策法规、成人内容、非法及不良等。
威胁处置	支持对入侵攻击、僵尸蠕行为、恶意程序传播、APT 攻击、WEB 攻击、访问非法 URL/ 域名、恶意 IP 访问等安全事件阻断处置。 支持通过发送 RSET 包阻断。 支持防火墙联动, 实现联动阻断恶意事件的通信。防火墙阻塞时间可自定义。
△产品资质	计算机信息系统安全专用产品销售许可证 国家信息安全漏洞库兼容性资质证书
△厂商资质	所投产品厂商提供 TL9000 电讯业质量管理体系认证证书 所投产品厂商提供 CMMI 5 级证书 所投产品厂商提供网络安全应急服务支撑单位证书 (国家级) 所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级 所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级

## (12)、风险评估服务

序号	服务名称	服务描述
----	------	------

1	风险评估服务	对现有网络中的网络架构、网络协议、系统、数据库等资产安全现状进行了解, 确定在系统的具体环境下到底存在什么安全漏洞和安全隐患, 一旦这些脆弱性被黑客利用会造成什么样的资产风险和影响。建议在部署基本的安全系统并运营一段时间后, 定期通过完善的风险评估服务检查整个系统面临的危险并根据评估结果对网络加以调整和优化。
2	安全预警通告服务	供最新的安全动态、技术和定制的安全信息, 包括实时安全漏洞通知、定期安全通告汇总、临时安全解决方案和安全知识库更新等。
3	应急响应服务	网络安全的发展日新月异, 无法实现一劳永逸的安全, 所以当紧急安全问题发生, 一般技术人员又无法迅速解决的时候, 及时发现问题、解决问题就必须依靠专业的应急响应服务来实现。 在第一时间对客户信息系统面临的紧急安全事件进行应急响应。紧急安全事故包括: 大规模病毒爆发、网络入侵事件、拒绝服务攻击、主机或网络异常事件等。
4	渗透测试服务	针对新上线的业务系统进行人工黑盒测试, 发现可能存在的恶意代码或安全风险
5	应急预案编写及演练服务	指定单位内部应急预案, 编写应急预案方案, 并针对预案中的部分内容进行演练
6	厂商资质	服务厂商具备中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级, 提供有效证书的复印件。 服务厂商具备中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级, 提供有效证书的复印件。

### ★五、付款方式

- 1、本合同项下所有款项均以人民币支付。
- 2、本合同项下的采购资金由甲方自行支付,乙方向甲方开具发票。
- 3、付款条件:合同签订后支付合同金额的30%的预付款,施工进场材料全部到位后支付至合同金额的60%,验收合格后支付至合同金额的95%,验收合格满三年支付剩余的5%。

### ★六、交货期

合同签订后30天内完成项目建设(不含第三方相关检测及取证时间)

### 七、售后服务

**★1、质保期:**质保期3年,在此期间内投标人对所有设备的维修与保养负责,其一切费用由投标人承担。无论在质保期内或外,由于设备本身质量问题或工艺缺陷,投标人则免费负责维修及更换。在质保期外,投标人负责设备的维修,对修理、更换的零部件收取工本费。

2、设备发生故障投标人在3小时内响应,12小时到达现场处理并在24小时内解决故障;设备若出现重大故障,投标人应在收到招标人通知后48小时内解决故障或者提供备用设备,直至整体系统正常运行。

#### 3、相关服务

- (1)编写专用用户手册,并制定维修服务准则,按照招标人要求和准则的内容为招标人提供优质、高效、有序的服务。
- (2)设备运行后,每两个月一次进行现场检查及监督操作人员的操作规范。
- (3)设备运行后,投标人负责提供系统软件的升级服务,免费建立常年固定服务进行定期和不定期回访。

## 第五章 评标方法与评标标准

### 一、评标方法与定标原则

评委会将对确定为实质性响应磋商文件要求的响应文件进行评价和比较, 评标采用综合评分法, 总分为100分, 按评审后得分由高到低顺序排列, 得分相同的, 按投标报价由低到高顺序排列, 得分且投标报价相同的, 按技术指标优劣顺序排列, 由评标委员会推荐3名及以上成交候选人。具体打分办法如下:

### 二、评标标准

评分标准		分值
价格 (30 分)	采用低价优先法计算: 即所有满足招标文件要求且最后报价最低的投标人的价格为投标基准价, 其价格分为满分。其他投标人的价格分按照下列公式计算(小数点后保留二位): 投标报价得分=(投标基准价/最后投标报价)×30%×100。	30 分
技术部分 (50 分)	技术参数 (25 分) <p>1、各项技术指标完全满足招标文件要求得满分;</p> <p>2、每一项加★的指标项负偏离, 视为未实质性响应招标文件, 作无效投标处理;</p> <p>3、每一项加△的指标项负偏离扣 2 分, 每项不加△的指标项负偏离扣 1 分, 扣完为止。</p> <p>(各项技术指标的响应情况均须提供有效证明材料(中文), 包括产品彩页、资质证书、操作手册等; 其他类型证明材料是否被认定为有效证明材料, 以评委会的意见为准, 未提供证明材料者视为该项响应负偏离。)</p>	25 分
	技术方案 (15 分) <p>提供技术服务方案, 包括但不限于实施方案、验收方案、培训方案等;</p> <p>计划详细、全面, 总体安排科学, 考虑周全, 有合理化建议的得 11-15 分;</p> <p>概述较为详细, 总体安排可行, 方案考虑比较细致, 能满足项目实施需要的得 6-10 分;</p> <p>计划简单, 基本能满足项目实施需要的得 0-5 分;</p> <p>未提供方案的不得分。</p>	15 分
	现场陈述 (10 分) <p>现场陈述包括但不限于目前用户整体网络架构、业务运行现状以及相应的安全风险, 方案整体规划设计, 实现目标和价值等。</p> <p>1、现场陈述流畅、表述清晰、对项目理解深刻到位、针对性很强, 充分体现项目的需求 7-10 分;</p> <p>2、现场陈述基本流畅、表述基本清晰、对项目有一定深度、针对性较强, 基本体现项目需求, 得 4-6 分;</p>	10 分

	<p>3、现场陈述不流畅、表述不够清晰、对项目理解存在一定偏差、针对性不强,不能全面体现项目的需求,得 0-3 分。</p> <p>注:只允许投标供应商项目负责人进入,陈述人员需携带第二代居民身份证以便核实,要求与投标文件中项目负责人为同一人;陈述人员自行准备陈述内容,内容及格式不限,展示方式自拟,现场有电脑可用(自行携带 U 盘);项目负责人未能参加陈述的,本项不得分;现场陈述时间应当控制在 10 分钟之内。</p>	
商务部分 (18分)	<p>所投产品厂商提供 TL9000 电讯业质量管理体系认证证书的,得 2 分;</p> <p>所投产品厂商提供 CMMI 5 级证书的,得 2 分;</p> <p>所投产品厂商提供网络安全应急服务支撑单位证书(国家级)的,得 2 分;</p> <p>所投产品厂商提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质证书-风险评估类二级的,得 1 分;</p> <p>所投产品厂商提供中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质认证证书-安全运维一级的,得 1 分。</p>	8 分
	<p>项目经理同时具有 CISA 证书、IT 服务项目经理证书、CISP 证书的,得 3 分;</p> <p>(缺一不得分)</p> <p>实施人员具备 CISP-DSG 的得 1 分,最多得 3 分;</p> <p>实施人员具备 CISP 的得 0.5 分,最多得 1 分。</p>	7 分
	<p>售后服务</p> <p>(3 分)</p> <p>供应商针对本项目提供原厂的维保方案及服务 7*24 小时的,得 3 分。</p>	3 分
投标文件完整性、规范性 (2 分)	<p>根据供应商响应文件编制情况进行评分:</p> <p>1、响应文件编制条理清晰,页码完整,整洁美观得 2 分;</p> <p>2、响应文件编制条理一般,页码部分缺漏,基本整洁美观得 1 分;</p> <p>3、响应文件编制条理混乱,无页码,目录标注不一致、不清晰得 0 分。</p>	2 分

注:以上要求的相关资料均需提供复印件,不提供的不得分。

说明:

- 1、评审标准中涉及的证明材料均需附入投标文件内(复印件加盖红章)。需要原件备查的资料,原件或者公证件带至招标现场备查,过期不补。
- 2、评标时,未能按以上要求提供相应证明(复印件和原件、公证件)的,不作为评标依据,不得分。
- 3、为便于评分,请磋商供应商按评分表样式,逐条列出证明材料所在页码,格式自定。
- 4、根据《常州市财政局关于新冠肺炎疫情防控期间加大政府采购支持中小微企业力度的通知》(常财购

(2020) 4号) 的要求, 2020年度对小、微型企业产品的价格给予10%的扣除, 用扣除后的价格参与评审。参加投标的中小微企业, 应当按照《政府采购促进中小企业发展暂行办法》(财库(2011) 181号) 的规定提供《中小企业声明函》(中小企业划型标准详见《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); 所投标产品的制造商为中小企业的, 必须在“产地”栏内加填中小企业的完整名称, 如未按要求填写和提供有效证明或相关内容表述不清的, 不得享受价格扣除。

5、对国家认定的节能产品和环保产品分别给予投标价的5%价格扣除, 用扣除后的价格参与评审(特别说明: 节能、环保产品必须纳入“中国政府采购网<http://www.ccgp.gov.cn>”等官方网站“节能、环保产品查询系统”, 且以提供的证书复印件为准)。

6、市级科技创新产品按《市政府办公室关于印发<2020年常州市制造创新产品首购和推广推荐目录>》(常政办发[2020]87号) 执行。

7、多项政策不得重叠计算, 多项政策都符合时以价格“扣除百分比高”的计算。

## 第六章 常州市政府采购供应商信用管理暂行办法

常州市财政局关于印发《常州市政府采购供应商信用管理暂行办法》的通知

常财规〔2017〕6号

各辖市（区）财政局、政府采购代理机构、市级有关单位：

为更好维护我市政府采购市场秩序，进一步规范供应商的政府采购行为，促进供应商诚信经营和公平竞争，根据《中华人民共和国政府采购法》等其他有关法律法规的规定，我局研究制定了《常州市政府采购供应商信用管理暂行办法》，现印发给你们，请遵照执行。

附件：《常州市政府采购供应商信用管理暂行办法》

常州市政府采购供应商信用管理暂行办法

### 第一章 总则

**第一条** 为了维护政府采购市场秩序，规范供应商的政府采购行为，促进供应商诚信经营和公平竞争，根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》（财政部令第87号）、《江苏省政府采购供应商监督管理暂行办法》等其他有关法律法规的规定，结合我市实际情况，制定本办法。

**第二条** 本办法适用于在常州市范围内进行的政府采购活动。

市级单位实施的政府采购项目，涉及供应商失信行为的，由市财政部门进行管理；**辖市（区）单位实施的政府采购项目，涉及供应商失信行为的，由辖市（区）财政部门进行管理。**

本办法所称供应商，是指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。

本办法所称招标文件是指公开招标的招标文件及非公开招标的招标文件。

本办法所称响应文件是指公开招标的投标文件及非公开招标的响应文件。

**第三条** 财政部门对参加政府采购活动的供应商实行诚信管理制度。诚信管理以公开、公平、公正为基础，遵循统一标准、分级管理、信息共享原则。

### 第二章 供应商诚信义务

**第四条** 供应商参与政府采购活动，应当履行以下诚信义务：

（一）自觉遵守政府采购法律法规，维护政府采购市场秩序和公平竞争环境，接受财政部门的监督检查；

（二）诚信参与政府采购活动，依法履行政府采购合同和政府采购活动中的各项承诺，为采购人提供符合招标文件规定的货物、工程和服务；

（三）**保守在政府采购活动中获悉的国家秘密和他人商业秘密；**



(四) 法律法规规定的其他诚信义务。

### 第三章 供应商失信行为

第五条 供应商在参与政府采购活动中有下列情形之一的，属于**失信行为**：

(一) 响应文件中故意不按招标文件要求提供有关技术、财务状况、信誉、业绩、服务、资质及其他证明材料，或未携带上述原件或者公证件的；

(二) 响应文件中提供虚假材料或虚假承诺的；

(三) 采取不正当手段诋毁、排挤其他供应商的；

(四) 已响应参加政府采购活动而无故不参加的；

(五) 与采购人、其他供应商或者采购代理机构恶意串通的；

本办法所列的恶意串通，包括以下情形：

1. 不同供应商的投标文件由同一单位或者个人编制；

2. 不同供应商委托同一单位或者个人办理投标事宜；

3. 不同供应商的投标文件载明的项目管理成员或者联系人员为同一人；

4. 不同供应商的投标文件异常一致或者投标报价呈规律性差异；

5. 不同供应商的投标文件相互混装；

(六) 向采购人、采购代理机构及评审小组成员行贿或提供其他不正当利益的；

(七) 在招标过程中与采购人进行协商谈判的；

(八) 不遵守开标现场纪律，扰乱评审现场的；

(九) 在有效期内擅自撤销投标（响应文件），影响招标活动继续进行的；

(十) 被确定为中标或成交候选供应商后无正当理由放弃中标或成交资格；中标、成交后无正当理由不签订政府采购合同的；

(十一) 不按照招标文件规定签订合同，或者与采购人另行签订背离合同实质性内容协议的；

(十二) 将中标、成交项目转让给他人，或者违反招标文件规定，将中标、成交项目分包给他人的；

(十三) 拒绝履行合同义务的；

(十四) 未按合同规定履行合同义务，造成不良后果的；

(十五) 擅自变更、解除合同的；

(十六) 实物配发和定点招标供应商所提供产品或服务价格高于成交价格或承诺的；

(十七) 拒绝有关部门监督检查或者提供虚假情况的；

(十八) 各级政府采购监管部门认定的其他失信行为。

第六条 供应商在政府采购质疑、投诉和信访举报活动中，有下列情形之一的，属于失信行为：

- (一) 在常州市域内**一年内两次**以上质疑、投诉和信访举报均查无实据的；
- (二) 捏造事实或提供虚假质疑、投诉和信访举报材料的。
- (三) 不配合相关部门调查取证的。

#### 第四章 失信行为记录

第七条 一般情况下，政府采购代理机构、采购人、供应商等政府采购各方当事人应在发现供应商存在上述失信行为后的**7个工作日内**，**及时将具体情况以书面形式向财政部门报告**。报告内容包括：

- (一) 失信供应商名称、联系人及联系方式；
- (二) 报告人的姓名或名称、联系人及联系方式；
- (三) 供应商失信行为的具体表现及事实依据。

供应商失信情况报告实行实名制。报告人为自然人的，应当由本人签字；为法人或者其他组织的，由法定代表人签字并加盖单位公章，同时提供相关身份证明。

第八条 各级财政部门收到供应商失信行为报告后，应积极调查核实，属于应予行政处罚的违法行为，应依法进行行政处罚，并予以失信记录，不属于行政处罚的失信行为，应依照本办法规定予以失信记录。

第九条 失信行为等级记录包括**一级失信行为记录**，记录期为一年；**二级失信行为记录**，记录期为二年；**三级失信行为记录**，记录期为三年；共三个等级。

第十条 供应商在政府采购活动中有**本办法规定的一项失信行为**，作为一级失信行为予以记录。

第十一条 供应商在政府采购活动中有**下列情形之一的**，作为二级失信行为予以记录：

- (一) 存在本办法规定的两项失信行为的；
- (二) 在一级失信行为记录有效期内，又出现本办法规定的一项失信行为的；
- (三) 失信行为造成不良后果或影响的。

第十二条 供应商在政府采购活动中有**下列情形之一的**，作为三级失信行为予以记录：

- (一) 存在本办法规定的三项以上失信行为的；
- (二) 一级失信行为记录有效期内，又出现本办法规定的两项失信行为的；
- (三) 二级失信行为记录有效期内，又出现本办法规定的一项失信行为的；
- (四) 失信行为情节严重、性质恶劣，造成重大危害或影响的；

第十三条 失信行为等级记录内容包括：

- (一) 供应商姓名或名称；
- (二) 失信行为具体表现；
- (三) 失信行为等级；

(四) 记录有效期;

(五) 记录日期及记录机关。

第十四条 失信行为等级记录均以书面形式通知供应商, 辖市(区)财政部门做出记录后应报市财政部门备案。

第十五条 各级财政部门对供应商做出失信行为等级记录后, 应将记录情况纳入常州市公共信息基础数据库并在 2 个工作日内, 在常州市政府采购网、信用常州上公示。

## 第五章 失信行为惩戒

第十六条 采购人和采购代理机构在制定招标文件或招标文件时, 应就供应商的诚信情况做出相关规定。对于被行政处罚尚在禁止参加政府采购活动期内的供应商, 不得参加政府采购活动, 否则中标、成交结果无效。对于被做出失信行为等级记录且该记录尚处于有效期内的供应商, 应明确在其参与政府采购活动时给予一定的分数扣减或价格增加。具体标准为: 采用综合评分法的, 对于一级失信行为供应商给予其总分值 2% 的减分, 二级失信行为供应商给予其总分值 4% 的减分, 三级失信行为供应商给予其总分值 6% 的减分。采用最低评标价法的, 对于一级失信行为供应商给予其报价 2% 的加价, 二级失信行为供应商给予其报价 4% 的加价, 三级失信行为供应商给予其报价 6% 的加价。

## 第六章 失信行为记录与诚信奖励

第十七条 供应商被做出失信行为等级记录, 如能主动消除影响或损害, 积极制定并落实整改措施, 并在记录有效期内的政府采购活动中无失信行为发生的, 经供应商申请并报做出记录的财政部门同意, 经调查核实后, 可以在记录有效期截止后, 撤销网上公示信息。

第十八条 供应商应诚信经营, 在企业经营活动及政府采购活动中未有失信记录的, 可以在招标文件中明确在同等条件下优先招标其货物、工程与服务。

## 第七章 附则

第十九条 本办法自公布之日起 30 日后施行。

第二十条 本办法由市财政局负责解释。

## 第七章 响应文件格式

### 格式一: 磋商响应函

致: 江苏溧投招标服务有限公司

我单位收到贵单位“\_\_\_\_\_”磋商文件后, 经详细研究, 我们决定参加该项目磋商活动。为此, 我方郑重声明以下诸点, 并负法律责任。

1、按磋商文件规定的各项要求提供采购人所需产品及服务, 包括但不限于以下部分: 准备(包括现场踏勘、技术核对等)、设备(包括备品备件、专用工具)、技术资料、设计、制造、检验、包装、技术资料、发货、运输、装卸至现场指定地点、安装调试、技术指导培训、质保期及维保服务和磋商文件所要求的相关服务等全部内容。

2、我方承诺财务状况良好, 依法缴纳税金和社会保障资金, 具备履行合同所必需的设备和专业技术能力, 参加政府采购活动前3年内在经营活动中没有重大违法记录。

3、我方承诺该响应文件在该项目的全过程中保持有效, 不作任何更改和变动。

4、我们愿按《中华人民共和国合同法》履行自己的全部责任。

5、我方同意遵守贵机构有关磋商活动的各项规定。

6、愿意提供磋商文件中要求所有资料, 并保证完全真实准确, 若有虚假和违背, 我公司愿意承担由此而产生的一切后果。

7、提交投标文件后, 视为供应商完全理解、认可磋商文件的所有内容, 并不再对磋商文件提出任何质疑。

8、遵守磋商文件中要求的收费项目和标准。

9、与本次磋商活动有关的正式通讯地址为:

供应商全称(公章):

地址:

邮编:

电话:

传真:

供应商开户行:

账户:

法定代表人或授权代表姓名(签字):

联系电话:

日期: 年 月 日

**格式二：响应报价表**

项目名称：安全等级保护改造项目

项目编号：JSLT竞磋[2021]-06-016

项目名称	磋商报价 (万元)	合同履行期限	备注

供应商全称（公章）：

法定代表人（授权代表）（签字或盖章）：

日期： 年 月 日

### 格式三: 法人委托授权书

江苏溧投招标服务有限公司:

本授权书声明: 注册于                                  (磋商供应商住址) 的                                  (磋商供应商名称) 法定代表人                                  (法定代表人姓名、职务) 代表本公司授权在下面签字的                                  (磋商供应商代表姓名、职务) 为本公司的合法代理人, 就贵方组织的项目名称                                 , 项目编号:                                 , 以本公司名义全权处理一切与之有关的事务 (包括参加磋商报名、参与磋商活动、处理询问、质疑、投诉等), 其行为代表公司行为, 我公司愿意承担由此而产生的一切后果!

本授权书于     年    月    日 签字生效, 特此声明。

供应商盖章:

法定代表人签字:

被授权人签字:

日期:     年    月    日

附: 法定代表人及被授权人有效身份证件复印件

**格式四: 法定代表人资格证明书**

单位名称:

地址:

姓名:

性别:

年龄:

职务:

系\_\_\_\_\_的法定代表人。为实施(项目名称) (项目编号)的工作, 签署上

述项目的响应文件、进行磋商、签署合同和处理与之有关的一切事务。

特此证明。

供应商盖章:

法定代表人签字:

日期: 年 月 日

法定代表人身份证

(复印件) 粘贴处

备注:

- 1、法定代表人参加磋商时, 需携带法人资格证明和本人身份证原件。
- 2、委托代理人参加磋商时, 需携带授权委托书和本人身份证原件。

附件一、偏离表

商务条款/技术条款偏离表

序号	磋商文件要求的商务条款/技术条款	磋商文件商务/技术响应描述	偏离情况
	自行填写	...	

供应商全称（公章）：

法定代表人（授权代表）（签字或盖章）：

日期： 年 月 日

注：

- 1、此表为表样，行数可自行添加，但表式不变。
- 2、“偏离情况”栏请注明“响应/正偏离/负偏离”。。



## 附件二、资格证明文件

备注：对本章所有的响应文件格式，供应商可根据自身情况进行补充和修改，但补充和修改不得造成与本格式内容有实质性的违背。

## 附件三、其他证明文件

备注：供应商可增加认为需要的其他证明文件，但提供的证明材料不得造成与本格式内容有实质性的违背。

## 附件四、中小企业声明函格式

### 《中小企业声明函》

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

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

2. 本公司参加\_\_\_\_\_单位的\_\_\_\_\_项目采购活动提供本企业制造的产品，由本企业承担工程、提供服务，或者提供其他\_\_\_\_\_（请填写：中型、小型、微型）企业制造的产品。本条所称产品不包括使用大型企业注册商标的产品。

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。

企业名称（盖章）：

日期：

注：供应商如属于以上情形的请提供。如不提供此声明函的，价格将不做相应扣除。

## 附件五、 政府采购供应商信用承诺书

为维护公开、公平、公正的政府采购市场秩序，树立诚实守信的供应商形象，本单位在参与政府采购活动中，自愿作出以下承诺：

一、严格遵守国家法律、法规和规章，全面履行应尽的责任和义务，全面做到履约守信，具备《政府采购法》第二十二条第一款规定的条件。

二、本单位已经阅读并充分理解《常州市政府采购供应商信用管理暂行办法》，自愿按照《常州市政府采购供应商信用管理暂行办法》规定，发生失信行为将记录并公开到“信用常州”、常州市政府采购网。

三、本单位提供给注册登记部门、行业管理部门、司法部门、行业组织以及在政府采购活动中提交的所有资料均合法、真实、有效，无任何伪造、修改、虚假成份，并对所提供资料的真实性负责。

四、严格依法开展生产经营活动，主动接受行业监管，自愿接受依法开展的日常检查；违法失信经营后将自愿接受约束和惩戒，并依法承担相应责任。

五、承诺本单位自觉接受行政管理部门、行业组织、社会公众、新闻舆论的监督。

六、承诺本单位自我约束、自我管理，重合同、守信用，不制假售假、商标侵权、虚假宣传、违约毁约、恶意逃债、偷税漏税、价格欺诈、垄断和不正当竞争，维护经营者、消费者的合法权益。

七、承诺本单位在信用中国（江苏）网站中无违法违规、较重或严重失信记录。

八、承诺本单位提出政府采购质疑和投诉坚持依法依规、诚实信用原则。

九、根据政府采购相关法律法规的规定需要作出的其他承诺。

十、承诺本单位若违背承诺约定，经查实，愿意接受行业主管部门和信用管理部门相应的规定处罚，承担违约责任，并依法承担相应的法律责任。

十一、承诺本单位同意将以上承诺事项上网公示，违背承诺约定行为将作为失信信息，记录到常州市公共信用信息系统，并予以公开。

承诺单位（盖章）：

法定代表人（负责人）：

附件六：现场踏勘回执单

## 现场勘察回执单

溧阳市交通运输局、江苏溧投招标服务有限公司：

\_\_\_\_\_公司于\_\_\_\_\_年\_\_\_\_月\_\_\_\_日至本项目实施地点进行现场勘察，对周边环境及基础数据已进行自行采集和确认，并向采购人详细了解本项目要求及获取编制响应文件的所有资料。

采购人（盖章）：

采购人代表（签字）：

日期： 年 月 日

供应商（盖章）：

供应商授权代表（签字）：

日期： 年 月 日