项目编号：310109000250228185680-09214750

信息安全加固建设项目

公开招标文件

2025年04月14日

采购单位：上海市中西医结合医院

地　　址：保定路 230 号

2025年04月15日

目　　录

第一章　公开招标采购公告

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》等规定，现就下列项目进行公开招标采购，欢迎提供本国货物、服务的单位或个人前来投标：

一、项目编号：310109000250228185680-09214750

二、公告期限：5 个工作日

三、采购项目内容、数量及预算

包号	包名称	数量	单位	预算金额（元）	简要规格描述或包基本概况介绍	最高限价（元）	备注
1	信息安全加固建设项目	1		1995600.00	中西医结合医院信息安全加固建设项目完善信息安全基	1995600.00	

					设系，止外因对保线损而成业的滞宕，保保路常使用。善有键全备软授件		

					和件保权硬维服务。足院建的产计存环的全满医新设国化算储境安需求，时须顾有境个用统国化造步同也兼原环各应系向产改逐过		

					渡。移动终端安全管理系统、病毒防治、主机监控与审计、日志分析、运维安全管理、WEB 应用防火墙、网络流控、终		

					接入控制等全硬设进加固。安软件备行		

四、合格投标人的资格要求

1、符合《中华人民共和国政府采购法》第二十二条的规定

2、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

本项目预算资金性质为仅面向中小微企业采购，投标单位为大型企业参与投标为无效投标。

信息安全加固建设项目资格审查要求包 1

序号	类型	审查要求	要求说明	项目级/包级
1	自定义	符合《中华人民共和国政府采购法》第二十二条规定及《中华人民共和国政府采购法实施条例》第十七条要求的	提供有效证明材料。	项目级

		供应商。		
2	自定义	根据《财库[2016]125号》之规定，企业信用报告合格的供应商。	提供有效证明材料。	项目级
3	自定义	有效提供企业自我声明——前三年内无违法记录及不诚信行为的供应商。	提供有效证明材料。	项目级
4	自定义	未列入失信被执行人、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、近三年不存在负面记录及其他不符合《中华人民共和国政府采购法》第二十二条规定条	根据响应人提供的材料及外部查询有效内容核对判定。	项目级

		件的供应商。		
5	自定义	投标有效期不足 90 天。	根据响应人的响应内容判定。	项目级
6	自定义	响应文件未按采购文件要求签署、盖章的	根据响应人的响应内容判定。	项目级
7	自定义	未满足带“*”号实质性指标的响应文件	根据响应人的响应内容判定。	项目级
8	自定义	以赠送方式响应的、对一个标项提供两个投标方案或两个报价的	根据响应人的响应内容判定。	项目级
9	自定义	响应文件含有采购人不能接受的附加条件的	根据响应人的响应内容判定。	项目级
10	自定义	供应商参加政府采购活动应当提交反映其财务状况、缴纳税收和社会保障资金情	根据响应人的响应内容判定。	项目级

		况的书面声明。		
11	自定义	不符合法律、法规和本采购文件规定的其他实质性要求的。	根据响应人的响应内容判定。	项目级
12	自定义	专门面向中小企业采购	请根据要求上传《中小企业声明函》。具体要求及格式以采购文件为准。	包 1

五、投标报名：

1、报名时间：2025-04-15 至 2025-04-23 上午 00:00:00~12:00:00；下午 12:00:00~23:59:59（节假日除外）。

2、报名方式：本项目实行网上报名，不接受现场报名。供应商登录上海政府采购网（http://www.zfcg.sh.gov.cn/）进行报名。

3、招标文件售价：0 元，招标文件请至公告附件处下载。

六、投标保证金：

[投标保证金收款账户（金额、开户行、户名、账号等）]

如需缴纳保证金，投标人应于 时前将投标保证金交至上海市虹口区政府采购中心，投标保证金若以网银、电汇方式交纳的，请将网银电脑打印凭证、电汇底单复印件写上所投项目名称、编号、投标联系人、联系电话，请在开标前一个工作日前到招标方服务台开收据。

七、投标截止时间和地点：

2025-05-06 10:30:00 上海政府采购网

八、开标时间及地点：

本次招标将于 2025-05-06 10:30:00 时整在上海政府采购网开标。

第二章　投标人须知

前附表

序号	内　容	要　　求
1	项目名称及数量	详见《公开招标采购公告》二
2	信用记录	根据财库[2016]125号文件，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn），以开标当日网页查询记录为准。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的供应商，**其投标将作无效标处理**。
3	政府采购节能环保产品	投标产品若属于节能环保产品的，请提供财政部、环境保护保部发布有效期内环境标志产品政府采购清单以及财政部、发改委联合发布有效期内节能产品政府采购清单。 招标需求中要求提供的产品属于节能清单中政府强制采购节能产品品目的，投标人须提供该清单内产品，**否则其投标将作为无效标处理。**
4	小微企业有关政策	1、根据财库〔2011〕181号的相关规定，在评审时对小型和微型企业的投标报价给予__%的扣除，取扣除后的价格作为最终投标报价（此最终投标报价仅作为价格分计算）。属于小型和微型企业的，投标文件中投标人必须提供的《中小企业声明函》以及本单位、制造商（如有）“国家企业信用信息公示系统——小微企业名录”页面查询结果（查询时间为投标前一周内，并加盖本单位公章），并在报价明细表中说明制造商情况。 2、根据财库[2017]141号的相关规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。属于享受政府采购支持政策的残疾人福利性单位，应满足财库[2017]141号文件第一条的规定，并在投标文件中提供残疾人福利性单位声明函（见附件）。 3.根据财库[2014]68号的相关规定，在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策，并在投标文件中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（格式自

		拟)。” **(注：未提供以上材料的，均不给予价格扣除)。**
5	答疑与澄清	投标人如对招标文件有异议，应当于公告发布之日起至公告期限满第 7 个工作日内，以书面形式向招标采购单位提出，逾期不予受理。
6	是否允许采购进口产品：	不允许进口产品具体要求详见第四章招标需求各标项的对应内容。
7	是否允许转包与分包	转包：否 分包：否
8	是否接受联合体投标	不允许 接受联合体投标的请提供联合体协议书。
9	是否现场踏勘	不组织现场踏勘 具体要求详见第四章招标需求各标项的对应内容。
10	是否提供演示	不进行演示 系统演示具体要求详见第四章招标需求各标项的对应内容。
11	是否提供样品	不要求提供样品 具体要求详见第四章招标需求各标项的对应内容。
12	投标文件组成	投标文件由资质文件、技术及商务文件、报价文件组成
13	中标结果公告	中标供应商确定之日起 2 个工作日内，将在上海市政府采购网(http://www.zfcg.sh.gov.cn/)发布中标公告，公告期限为 1 个工作日。
14	投标保证金	交纳：投标保证金应按《招标采购公告》六规定交纳。若一次投多个标项，只需交纳一个标项的投标保证金（按所需保证金最大额的标准交纳为准）。 退还：中标通知书发出之日起5个工作日内，未中标的投标人提供交入投标保证金时取得的第二联“供应商退款凭据”到招标方服务台办理，招标方以电汇或转账等方式退还投标保证金。
15	合同签订时间	中标通知书发出后 30 日内。规范政府采购合同签订行为，财政部制定了《政府采购货物买卖合同（试行）》，供采购人参考使用。
16	履约保证金	合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的10%。
17	付款方式	国库集中支付（采购人自行支付）详见各标项的商务要求表
18	投标文件有效期	90天
19	投标文件的	http://www.zfcg.sh.gov.cn接收

	接收	
20	招标方代理费用	无
21	解释权	本招标文件的解释权属于上海市虹口区政府采购中心。
22	新出台文件及要求	《关于简化政府采购供应商资格审查有关事项的通知》主要内容：不再要求供应商提供财务状况报告、依法缴纳税收和社会保障资金的证明材料。供应商参加政府采购活动应当提交反映其财务状况、缴纳税收和社会保障资金情况的书面声明。（如与本次采购过程中的内容有冲突，按照新文件执行）。超出招标文件要求的规定次数的质疑将不再受理。
23	备注	1，为方便告知投标单位后续政府采购相关事宜，投标单位需在投标文件中填写邮箱信息。2，电子投标文件在投标截止时间前上传至上海政府采购网，可不再打印纸质投标文件交至政府采购代理机构。3，虹口政府采购中心联系方式见采购公告，邮箱：hkqzfcgzx@163.com。

一、总　则

（一）适用范围

仅适用于本次招标文件中采购项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

（二）定义

1、“招标方”系指组织本项目采购的上海市虹口区政府采购中心。

2、“投标人”系指向招标方提交投标文件的单位或个人。

3、“采购人” 系指委托招标方采购本次货物、服务项目的国家机关、事业单位和团体组织。

4、“货物”系指招标文件规定投标人须向采购人提供的一切材料、设备、机械、仪器仪表、工具及其它有关技术资料和文字材料。

5、“服务”系指招标文件规定投标人须承担的劳务以及其他类似的义务。

6、“项目”系指投标人按招标文件规定向采购人提供的需求总称。

（三）投标人及委托有关说明

1、授权代表须携带有效身份证件。如授权代表不是法定代表人，须有法定代表人出具的授权委托书（格式见附件）。

2、投标人投标所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人所拥有。投标人投标所使用的采购项目实施人员必须为投标人员工（或投标人控股公司正式员工）。

3、以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

4、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。

5、投标人应仔细阅读招标文件的所有内容，按照招标文件的要求提交投标文件，并对所提供的全部资料的真实性承担法律责任。

（四）投标费用

不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用

（招标文件有其他相反规定除外）。

（五）质疑

1、投标人认为招标过程或中标结果使自己的合法权益受到损害的，可以在中标结果公告期限届满之日起七个工作日内，以书面形式向招标方提出质疑，须在法定质疑期内一次性提出针对同一采购程序环节的质疑。2、质疑应当以书面形式提出，格式见《政府采购质疑和投诉办法》（财政部令第94号）附件范本，下载网址：中国政府采购网(http://www.ccgp.gov.cn/)，位置：“首页-下载专区-政府采购供应商质疑函范本”。供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

a 供应商的姓名或者名称、地址、邮编、联系人及联系电话；

b 质疑项目的名称、编号；

c 具体、明确的质疑事项和与质疑事项相关的请求；

d 事实依据；

e 必要的法律依据；

f 提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。质疑应明确阐述招标过程或中标结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理，质疑函不符合《政府采购质疑和投诉办法》相关规定的，应在规定期限内补齐的，招标方自收到补齐材料之日起受理；逾期未补齐的，按自动撤回质疑处理。

（六）招标文件的澄清与修改

1、投标人应认真阅读本招标文件，发现其中有误或有不合理要求的，投标人应当于公告发布之日起至公告期限满第7个工作日内以书面形式向招标方提出。招标方将在规定的时间内，在财政部门指定的政府采购信息发布媒体上发布更正公告。**逾期提出招标方将不予受理。**

2、招标方主动进行的澄清、修改：招标方无论出于何种原因，均可主动对招标文件中的相关事项，用补充文件等方式进行澄清和修改。

3、招标文件澄清、答复、修改、补充的内容为招标文件的组成部分。

当招标文件与招标文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的书面文件为准。

二、投标文件的编制

（一）投标文件的组成

投标文件由资质文件、技术及商务文件、投标报价文件三部份组成。

1、资质文件

（1）投标声明书（格式见附件，含无重大违法记录及不诚信行为声明）；

（2）投标单位可自查自招标公告发布之日起至投标截止日内任意时间的“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）投标人信用情况。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的供应商，其投标将作无效标处理。（投标单位可不用截图于投标文件，采购人、采购代理机构或由采购人委托的评标委员会以开标当日的查询结果为准）。

（3）法定代表人授权委托书(格式见附件)；

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

（5）联合投标协议书（若需要）；

（6）联合投标授权委托书（若需要）；

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

2、技术及商务文件

（1）评分对应表（格式见附件，主要用于评委对应评分内容）

（2）投标项目明细清单（含货物、服务等）；

（3）技术响应表（格式见附件）；

（4）项目总体解决方案（可包含且不限于对项目总体要求的理解、项目总体架构及技术解决方案等）；

（5）项目实施计划（可包含且不限于保证工期的施工组织方案及人

力资源安排、项目组人员清单等）；

（6）列入政府采购节能环保清单的证明资料（若有）；

（7）商务响应表（格式见附件）；

（8）售后服务计划（可包含且不限于对用户故障的响应、处理、定期巡检、备品备件、常用耗材提供、驻点人员情况等）；

（9）技术培训计划（若有）；

（10）投标人履约能力（可包含且不限于技术力量情况、投标人各项能力证书）；

（11）案例的业绩证明（投标人业绩情况一览表、合同复印件等）；

（12）投标方认为需要的其他文件资料。

投标单位可根据采购需求内容和评审因素作技术文件响应。

3、报价文件：

（1）投标报价明细表（格式见附件）；

（2）投标人针对报价需要说明的其他文件和说明（格式自拟）；

（3）小微企业声明函、网页证明资料（若有，格式见附件）；

（4）残疾人福利企业声明函（若有，格式见附件）。

注：法定代表人授权委托书、投标声明书、投标报价明细表必须按招标文件格式要求正确签署并加盖投标人公章。

（二）投标文件的语言及计量

1、投标文件以及投标人与招标方就有关投标事宜的所有来往函电，均应以中文简体字书写。除签名、盖章、专用名称等特殊情形外，投标文件中以中文汉语以外的文字表述部分视同未提供。

2、投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元），**否则将作无效标处理**。

（三）投标文件的有效期

1、自投标截止日起 90 天内投标文件应保持有效。**有效期不足的投标文件将作无效标处理。**

2、中标人的投标文件自开标之日起至合同履行完毕止均应保持有效。

（四）投标文件的签署和份数、包装

1、投标人应按本招标文件规定的格式和顺序编制、装订投标文件并标注页码，投标文件内容不完整、编排混乱导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任。

2、投标人在 http://www.zfcg.sh.gov.cn 上传投标文件。

3、投标文件须由投标人在规定位置盖章并由法定代表人或法定代表人的授权委托人签署，投标人应写全称。

4、投标文件不得涂改，若有修改错漏处，须加盖供应商公章或者法定代表人或授权委托人签名或盖章。投标文件因字迹潦草或表达不清所引起的后果由投标人负责。

（五）投标报价

1、投标文件只允许有一个报价，投标报价应按招标文件中相关附表格式填报，该投标报价应与明细报价汇总相等，且**不允许出现报价优惠等字样（明细出现“0”元，视同赠送）**。

2、投标报价**应包含项目所需全部货物、服务，不得缺漏**，是履行合同的最终价格（含货款、标准附件、备品备件、专用工具、包装、运输、装卸、保险、税金、货到就位以及安装、调试、培训、保修等一切税金和费用）。

3、投标报价总价金额到元为止，如投标报价总价出现角、分，将被抹除。

（六）投标保证金

1、投标人须按规定提交投标保证金。

2、保证金形式：网银、汇票、电汇、转帐支票。

3、招标方不接受以现金支票、现金及个人转账方式交纳的保证金。

投标保证金若以网银、电汇方式交纳的,请将网银电脑打印凭证、电汇底单复印件写上所投项目名称、编号、投标联系人、联系电话，请在开标前一个工作日前到招标方服务台开收据。

4、招标方在中标通知书发出后五个工作日内退还投标保证金，供应商办理投标保证金退还时需提供收据的第二联“供应商退款凭据”。**详见**

上海市政府采购网 http://www.zfcg.sh.gov.cn/ ，位置：“首页-在线服务”

保证金不计息。

5、投标人有下列情形之一的，投标保证金将不予退还：

（1）投标人在投标截止时间后撤回投标文件的；

（2）投标人在投标过程中弄虚作假，提供虚假材料的；

（3）中标人无正当理由不与采购人签订合同的；

（4）将中标项目转让给他人或者在投标文件中未说明且未经招标采购单位同意，将中标项目分包给他人的；

（5）其他严重扰乱招投标程序的；

（七）串通投标认定

有下列情形之一的，视为投标人串通投标，其投标无效：

1、不同投标人的投标文件由同一单位或者个人编制；

2、不同投标人委托同一单位或者个人办理投标事宜；

3、不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

4、不同投标人的投标文件异常一致或者投标报价呈规律性差异；

5、不同投标人的投标文件相互混装；

6、不同投标人的投标保证金从同一单位或者个人的账户转出。

（八）投标无效的情形

在评审时，如发现下列情形之一的，投标文件将被视为无效：

1、未按规定交纳投标保证金的；

2、投标方未能提供合格的资格文件、投标有效期不足的；

3、投标人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的；

4、投标文件未按招标文件要求签署、盖章的；

5、与招标文件有重大偏离、未满足带“*”号实质性指标的投标文件；

6、招标需求中要求提供的产品属于节能清单中政府强制采购节能产品品目的，投标人未提供该清单内产品的；

7、投标报价超出招标文件中规定的预算金额或者最高限价的；

8、标项以赠送方式投标的、对一个标项提供两个投标方案或两个报价的；

9、评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约，且不能证明其报价合理性的；

10、投标人不接受报价文件中修正后的报价的；

11、未按本章“二、投标文件的编制”第五点投标报价要求报价的；

12、投标文件含有采购人不能接受的附加条件的；

13、投标人被视为串通投标的；

14、不符合法律、法规和本招标文件规定的其他实质性要求的。

（九）错误修正

投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

（一）《开标记录表》报价与投标文件中报价不一致的，以《开标记录表》为准。

（二）大写金额和小写金额不一致的，以大写金额为准；

（三）单价金额小数点或者百分比有明显错位的，以《开标记录表》的总价为准，并修改单价；

（四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照经投标人加盖公章，或者由法定代表人或其授权的代表签字确认后产生约束力，投标人不确认的，其投标无效。

注：除评标委员会按相关法律法规要求的澄清、说明或者补正情形之外，《开标记录表》内容 与投标文件中相应内容不一致的，以《开标记录表》为准。

三、组织开、评标程序及评标委员会的评审程序

（一）组织开标程序

招标方将按照招标文件规定的时间、地点和程序组织开标（http://www.zfcg.sh.gov.cn/上开展）。

（二）组织评标程序

招标方将按照招标文件规定的时间、地点和程序组织评标，各评审专家及相关人员应参加评审活动并接受核验、签到，无关人员不得进入评审现场。

1、按规定统一收缴、保存评标现场相关人员通讯工具。

2、介绍评审现场的人员情况，宣布评审工作纪律，告知评审人员应当回避情形；组织推选评标委员会组长。

3、组织评标委员会各位成员签订《政府采购评审人员廉洁自律承诺书》。

4、采购人可以在评标前说明项目背景和采购需求，说明内容不得含有歧视性、倾向性意见，不得超出招标文件所述范围。说明应当提交书面材料，并随采购文件一并存档。

5、根据需要简要介绍招标文件（含补充文件）制定及质疑答复情况、按书面陈述项目基本情况及评审工作需注意事项等，让评审专家尽快知悉和了解所评审项目的采购需求、评审依据、评审标准、工作程序等；提醒评标委员会对客观评审项目应统一评审依据和评审标准，对主观评审项目应确定大致的评审要求和评审尺度；对评审人员提出的有关招标文件、投标文件的问题进行必要的说明、解释或讨论。

6、采购人代表或采购代理机构或由采购人委托的评标委员会对投标人资格文件进行审查并以开标当日为准对投标人“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）信用记录情况进行核实。

7、评标委员会组长组织评审人员独立评审。评标委员会对拟认定为投标文件无效，可组织相关投标人代表进行陈述、澄清或申辩；招标方可协助评标委员会组长对打分结果进行校对、核对并汇总统计；对明显畸高、畸低的评分，评标委员会组长应提醒相关评审人员进行复核或书面说明理

由，评审人员拒绝说明的，由现场监督员据实记录；评审人员的评审、修改记录应保留原件，随项目其他资料一并存档。

8、做好评审现场相关记录，协助评标委员会组长做好评审报告起草、有关内容电脑文字录入等工作，并要求评标委员会各成员签字确认。

9、评审结束后，招标方应对评标委员会各成员的专业水平、职业道德、遵纪守法等情况进行评价；同时按规定向评审专家发放评审费，并交还评审人员及其他现场相关人员的通讯工具。

（三）评审程序

1、在评审专家中推选评标委员会组长。

2、评标委员会组长召集成员认真阅读招标文件以及相关补充、质疑、答复文件、项目书面说明等材料，熟悉采购项目的基本概况，采购项目的质量要求、数量、主要技术标准或服务需求，采购合同主要条款，投标文件无效情形，评审方法、评审依据、评审标准等。

3、评审人员对各投标人投标文件的有效性、符合性、完整性和响应程度进行审查，确定是否对招标文件作出实质性响应。

4、评审人员按招标文件规定的评审方法和评审标准，依法独立对投标人投标文件进行评估、比较，并给予评价或打分，不受任何单位和个人的干预。

5、评审人员对各供应商投标文件非实质性内容有疑议或异议，或者审查发现明显的文字或计算错误等，及时向评标委员会组长提出。经评标委员会商议认为需要供应商作出必要澄清或说明的，应通知该投标人以书面形式作出澄清或说明。授权代表未到场或拒绝澄清说明或澄清说明的内容改变了投标文件的实质性内容的，评标委员会有权对该投标文件作出不利于投标人的评判。书面通知及澄清说明文件应作为政府采购项目档案归档留存。

6、评审人员需对招标方工作人员唱票或统计的评审结果进行确认，现场监督员应对评审结果签署监督意见。如发现分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致以及存在评分畸高、畸低情形的，

应由相关人员当场改正或作出说明；拒不改正又不作说明的，由现场监督员如实记载后存入项目档案资料。

7、评标委员会根据评审汇总情况和招标文件规定确定中标候选供应商排序名单。

8、起草评审报告，所有评审人员须在评审报告上签字确认。

四、评审原则

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

2、评审专家因回避、临时缺席或健康原因等特殊情况不能继续参加评审工作的，应按规定更换评审专家,被更换的评审人员之前所作出的评审意见不再予以采纳，由更换后的评审人员重新进行评审。无法及时更换专家的，要立即停止评审工作、封存评审资料，并告知投标人择期重新评审的时间和地点。

3、评审人员对有关招标文件、投标文件、样品或现场演示（如有）的说明、解释、要求、标准存在不同意见的，持不同意见的评审人员及其意见或理由应予以完整记录,并在评审过程中按照少数服从多数的原则表决执行。对招标文件本身不明确或存在歧义、矛盾的内容，应作对投标人而非采购人有利的解释;对因招标文件中有关产品技术参数需求表述不清导致投标人实质性响应不一致时，应终止评审，重新组织采购。评审人员拒绝在评审报告中签字又不说明其不同意见或理由的,由现场监督员记录在案后，可视为同意评审结果。

4、财政部令第87号《政府采购货物和服务招标投标管理办法》第三十一条规定：使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机

抽取方式确定，其他同品牌投标人不作为中标候选人。

非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前款规定处理。

五、确定中标供应商的原则

1、项目由评标委员会根据第三章《评标办法与评分标准》规定提出中标候选人排序。

2、采购人应当自收到评标报告之日起 5 个工作日内，在评标报告确定的中标候选人名单中按顺序确定中标人，或者采购人委托评标委员会在评标报告确定的中标候选人名单中按顺序确定中标人。采购人在收到评标报告 5 个工作日内未按评标报告推荐的中标候选人顺序确定中标人，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标人。

3、采购结果经采购人确认后，招标方将于 2 个工作日内在上海市政府采购网上发布中标公告，并向中标方签发《中标通知书》。

六、合同授予

（一）签订合同

1、采购人与中标人应当在《中标通知书》发出之日起 30 日内签订政府采购合同，招标方作为合同签订的鉴证方。

2、中标人拖延、拒签合同的，将被扣罚投标保证金并取消中标资格。

（二）履约保证金

1、合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的 10%。

2、按合同约定办理履约保证金退还手续。

七、货款的结算

货款由采购人按招标文件规定的付款方式自行支付。

第三章　评标办法及评分标准

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

一、总则

本次评标总分为 100 分。合格投标人的评标得分为各项目汇总得分，中标候选资格按评标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，按技术得分由高到低顺序排列。评分过程中采用四舍五入法，并保留小数 2 位。采购文件中未规定的评标标准不得作为评审依据。

二、分值的计算

技术、资信、商务及其他分按照评标委员会成员的独立评分结果汇总后的算术平均分计算，计算公式为：

技术、资信商务及其他分=评标委员会所有成员评分合计数/评标委员会组成人员数

投标人评标综合得分=价格分+(技术分+资信商务及其他分)

三、评标内容及标准

综合评分法

信息安全加固建设项目包 1 评分规则：

评分项目	分值区间	评分办法
报价分	0~10	报价得分＝价格分值×（有效最低投标价/有效投标报价）
方案设计	0~18	1. 功能概要说明（0-3 分）； 2. 总体拓扑图设计等的准确度（0-3 分）； 3. 供应商对本项目重点、难点分析的合理性（0-3 分）； 4. 本项目的方案设计科学性、可操作性（0-3 分）； 5. 设计前后拓扑对比（0-3 分）； 6. 验收标准和

		方案的科学性、可行性（0-3 分）。
实施方案	0~12	1. 系统、产品安装部署实施方案的可操作性（0-3 分）； 2. 项目实施的详细进度计划（0-3 分）； 3. 项目管理措施（0-3 分）； 4. 培训计划（0-3 分）。
实施人员	0~6	1.项目经理能力、经验、业绩情况，提供从业履历、相关证书和劳动合同，项目经理具备 PMP 或网络工程师中级证书或软件测试技能人才证书或 CISAW 证书，且有 5 年以上同类型项目管理经

		验，满足要求得3分，不满足得0分； 2.主要专业技术管理人员及项目组成员专业配备及数量满足项目需求，团队人员提供相关证书和劳动合同，满足上述全部要求的得3分，不满足得0分。
技术参数	0~32	根据该项技术参数的重要性、实用性、以及投标产品技术参数与招标文件要求的技术参数偏离程度等。“▲”号的技术指标每负偏离1项扣2分。一般技术指标每负偏离1项扣0.5分，扣完为止。 【提供产品功

		能截图及按要求的效果截图】
售后服务	0~9	1.售后服务方案，包括售后服务响应时间、服务计划与内容等（0-3 分）； 2.应急预案（0-3 分）； 3.质量保证和售后服务管理措施（0-3 分）。
投标人类似业绩	0~10	投标人近 3 年以来承接的有效的类似业绩。是否属于有效的类似业绩由评标委员会认定。有一个有效业绩得 2 分，每增加一个有效业绩加 2 分，最高得分为 10 分，没有有效的类似项目业绩的得 0 分。须有合同佐

		证（合同关键页复印件），需提供相关业绩的合同扫描件，扫描件中需体现合同的签约主体、项目名称及内容、交付日期等合同要素的相关内容，否则将不予认可。
投标单位综合实力	0~3	投标人具备信息安全管理体系（ISO27001）的符合性证书或证明文件。

第四章　招标需求

序号	事项	内容
1	采购单位（加盖公章）	上海市中西医结合医院
2	项目名称	信息安全加固建设项目
3	采购预算金额	19956000　元（国库资金：19956000元）
4	项目属性	货物口　　服务✓
5	采购意向是否已公开	2024 年 11 月 21 日于上海政府采购网

		发布采购意向公示
6	采购标的所属行业(按工信部联企业(2011)3006 号和财库〔2020〕46 号文，用于中小企业声明函)	软件和信息技术服务业
7	特定资格要求	无
8	是否专门面向中小企业	是✓ 否口
9	是否招一用三	是口 否✓
10	合同履行期限	180 日历天
11	质保或免费维护期	5 年
12	是否允许联合体投标	是口 否✓
13	是否允许采购进口产品	是口 否✓
14	是否现场踏勘	是口 否✓
15	是否要求提供样品	是口 否✓
16	付款方式	合同签订后 15 个工作日内支付 70%，验收完成 15 个工作日支付剩余 30%。
17	验收方式（履约验收后将材料交由政采中心电子归档保存）	数据局组织验收
18	本项目询问、质疑受理委托授权范围	虹口区政府采购中心
19	本项目评审办法	综合评分法✓ 最低评标价法口
20	按财政部 22 号令《政府采购需求管理办法》第十一条要求，是否已完成需求调查工作	是✓ 否口
21	本项目是否涉及信创产品（包括软、硬件）采购。（所有信创产品由采购单位按相关要求另行采购）	是口 否✓

1 项目简介

1.1 项目目标

近年来，针对医疗系统的入侵、攻击和破坏等行为越来越严重，如通过木马入侵、远程控制重要信息系统计算机，大量窃取敏感信息的事件不断发生，我国医疗行业基础信息网络和重要信息系统日益成为不法分子攻击窃密的重点目标，违法犯罪活动大幅度增加。

我院信息化发展迅速，为整个医院的业务以及患者提供了极大的方便与帮助，但是医疗信息的安全问题也伴随而来。同时上海市卫健委在历年上海市卫生工作要点，

明确指出医疗机构应重视网络安全工作，并将网络安全工作纳入每年绩效考核指标，并且每年对各个医疗单位展开“网络安全飞行检查”“网络安全周”“网络安全重保”等各项专项检查或抽查工作。同时，随着国际形势的风云变化，国家大力推进倡导国产化改造工作，对网络安全提出了更高的要求。

依据国家相关法律、法规及技术标准，按照三级等保安全建设要求、关键基础设施保护建设要求，建设一套完全符合国产化要求的网络安全基础设施。本架构既要满足医院新建设的国产化计算存储环境的安全需求，同时也须兼顾原有环境各个应用系统向国产化改造逐步过渡。

1.2 项目依据

- 《信息安全技术关键信息基础设施安全检查评估指南》;
- 《信息安全技术关键信息基础设施安全保障评价指标体系》;
- 《关键信息基础设施安全保护条例》(国务院令第 745 号);
- 《计算机信息系统安全保护等级划分准则》(GB17859-1999);
- 《信息安全等级保护定级指南》(GB/T22240-2020);
- 《信息安全等级保护基本要求》(GB/T22239-2019);
- 《信息系统通用安全技术要求》(GB/T20271-2006);
- 《信息系统等级保护安全设计技术要求》(GB/T25070-2019);

2 项目建设内容

2.1 项目清单

本次项目包含安全软硬件设备加固，所有软硬件均需提供五年授权和原厂服务，具体要求如下：

序号	产品名称	关键程度	单位	数量
1	移动终端安全管理系统	核心产品	套	1
2	病毒防治	核心产品	套	1
3	主机监控与审计	核心产品	套	1
4	日志分析	/	套	1
5	运维安全管理	/	台	1
6	WEB 应用防火墙	关键核心产	台	2

		品		
7	网络型流量控制	/	台	1
8	终端接入控制	核心产品	台	1

2.2 技术参数

本次项目包含安全软硬件设备加固，所有软硬件均需提供五年授权和原厂服务，具体要求如下：

2.2.1 移动终端安全管理系统【核心产品】

序号	指标项		指标描述
1	设备信息采集	设备列表	支持查看已经通过移动客户端注册到系统的移动设备列表，包括所有设备、在线设备、活跃设备、新接入设备、待审核设备、已审核设备、存在风险设备和已脱管设备
2		设备标签	可自定义设备标签规则，系统根据该标签规则自动归类设备，该标签下的策略自动对设备生效
3		搜索设备	可以通过当前用户、设备 ID、在线状态、设备状态、是否 root（越狱）、设备归属、设备类型、操作系统、操作系统版本、设备品牌、设备型号来搜索出相应的设备，支持组合搜索
4		设备基本信息	支持采集移动设备基本信息： 1）硬件信息，包括设备 ID、设备名称、设备型号、设备品牌、CPU 名称、操作系统名称、操作系统版本、内核版本、是否 ROOT 越狱、CPU 名称、蓝牙 MAC、WiFi MAC、移动运营商、IMEI、OAID 等 2）概要信息，包括当前用户、部门名称、设备归属、激活时间、最近登录时间客户端已获取权限等
5		设备实时状态	支持获取移动设备的实时状态： 1）性能：设备内存、ROM、CPU 负荷 2）电源：电池电量、电池电压、电池温度、电池状态、开机时长 3）网络：网络状态、信号强度、IPv4/IPv6 地址
6		设备应用安装信息	支持获取移动设备的应用安装列表，并支持应用远程卸载： 应用名称、设备归属、应用包名、版本号、文件大小
7		设备安全状态	支持感知移动设备的安全状态： 设备是否越狱/ROOT、设备密码合规性、设备是否锁定等
8		设备日志上传	管理员能控制台远程实时获取在线终端日志，错误日志支持手工反馈/自动上报
9		设备资产信息编辑和展示	支持对企业配发设备的资产信息进行自定义扩展，包括资产编号、设备厂商、供应商、采购价、购买日期、设备用途等，同时展示在设备管理界面，满足企业对设备的多维度信息统计要求，利于管理员对设备进行分类管理；

10	设备安全管理	设备黑名单	支持设备黑名单功能，黑名单设备客户端退出登录，无法再重新登录使用；取消黑名单后可正常使用；
11		设备实时控制	支持通过管理平台对移动设备下发实时控制指令，包括远程擦除企业数据、进入/取消特权、清除/解锁密码、启用/禁用摄像头、远程截屏、开/关蓝牙、推送消息、开/关安全隧道、远程定位设备、锁定设备、远程关机、远程注销等
12		设备定位	支持通过管理平台对移动设备进行实时定位，以及查看设备历史轨迹
13		DO 设备管理（Device Owner）	用户可通过客户端对其所属的全部设备进行管理 支持设备的实时控制，包括远程擦除企业数据、解除绑定、远程定位设备、锁定设备、远程关机、远程注销等；
14		策略生效（成功/失败）统计及详情	1）策略维度：支持统计不同策略的下发情况，可查看下发成功数和未下发成功数，统计下发成功率，支持查看下发/未下发的设备/用户详细信息；
15			2）用户维度：支持根据用户及部门查看策略下发详情，包括策略内容和下发状态，可对用户/部门批量授权/取消策略；
16			3）设备维度：支持选择设备查看策略下发情况，可对设备批量授权/取消策略；
17		策略分发方式	1）策略下发范围支持选择用户、部门和用户静态标签下发；
18			2）策略下发方式支持设备和设备静态标签下发；
19			3）策略下发方式支持用户动态标签和设备动态标签下发，支持配置多条动态计算规则，并可以选择“与”、“或”条件嵌套，可支持的条件变量包括但不限于：设备 ID、IMEI、IDFA、序列号、设备名称、设备型号、品牌、操作系统、操作系统版本、设备类型、设备归属、自动通过审批等；
20		屏幕水印(设备级)	提供水印技术（数字水印、图形水印）对配发设备进行安全防护，降低无意识泄密的概率，同时可以对数据泄密事件提供追溯手段： 1）支持数字水印内容完全自定义，包括设备信息（设备名、IP 地址等）用户信息（用户名、部门、手机号等）；
21			2）支持数字水印格式（内容展示顺序，例如设备名-用户名-日期）完全自定义；
22			3）支持数字水印位置（宽度、高度、角度）、水印密度（行间距、列间距）和字体样式（斜体、加粗、下划线）完全自定义；
23			4）支持明文水印、图形水印混合使用；**【功能及效果截图】**
24		锁定安全桌面	支持添加安全桌面，锁定前台无法退出，仅允许企业应用商店安装的应用和授权的应用使用，可限制给指定人员电话和短信功能。
25		时间同步	安全桌面时间与服务器时间同步

26		时间地理围栏	规定某时间/地理位置范围内，对限制设备部分功能使用： 1）围栏内只允许连接指定的上网接入点，管理员统一设定 WiFi 配置，SSID 名称、安全类型、WiFi 密码；
27			2）围栏内停用相机、蓝牙、截屏、蜂窝移动网络、WiFi 网络，围栏外解除;
28			3）围栏内 Android 启用安全桌面、自定义安全桌面应用，可控制电话和短信收发人员白名单；
29			4）支持自定义设置多个地理围栏；
30		应用限制	支持针对设备上应用安装、卸载或使用限制，防止设备安装使用企业不合规应用
31		违规事件	支持越狱 Root 事件、新设备接入事件、长时间未登录事件、违规安装应用、未安装指定应用、流量异常、硬件配置变更、用户变更、用户异常登录安全事件、设备丢失安全事件的管理，触发安全事件，被审计并触发事件处理预案
32		安全编排及风险处置自动化	安全事件自动化响应，无需人工干预，提高安全事件处置的效率：1）支持添加多个节点并自定义触发节点的执行动作，系统根据定义的触点执行阻止访问或强制修补等动作，包括是否允许用户访问门户、是否设置设备黑名单、是否开启响铃、是否开启设备隧道，是否开启用户隧道以及是否解锁设备等；
33			2）当用户恢复了违规行为自动执行恢复处理预案，保证时效性，减轻管理员维护工作量；
34	组织用户管理	身份认证	1）激活认证方式，支持多认证源接入认证并按顺序进行认证，如系统内置用户、LDAP 服务器用户、CAS 认证和 Radius 用户；
35			2）二次认证，支持统一用户管理，提供移动用户身份认证的集中管理，支持手势密码认证、指纹认证、人脸认证；
36		AD/LDAP 同步	能自动同步 AD/LDAP 及数据库中的组织架构信息和用户帐号信息
37		支持用户自定义属性	为便于管理和运维，支持对用户的扩展属性如办公地点、办公电话、年龄、学历等属性进行自定义控件，包括多行文本、数字、单选框、多选框等
38		特权账户管理	支持添加特权账号和权限组，可以赋予 APP 激活时的免审核、免短信认证、免扫码激活的权限
39	审计日志管理	设备控制日志	可以查看对移动终端设备下发的设备控制指令详情，包括用户、设备、指令状态、下发时间、生效时间等
40		设备违规信息	支持客户端违规审计，可以根据时间、部门、用户、用户组及违规类型进行统计，明细中可以详细记录违规信息
41		安全事件审计	1）事件下发信息：安全事件的下发审计（对有下发范围的事件）；
42			2）安全事件信息：审计发生的安全事件信息，可手动确认恢复事件；

43			3）安全事件汇总：安全事件汇总统计，图表显示统计结果。可以根据事件类别查看当天发生未恢复事件、当周发生未恢复事件、当月发生未恢复事件、所有未恢复事件。可以根据统计数据点击查看具体事件信息；
44		操作员日志	支持对管理员的操作行为进行记录，可以查看管理员针对管理平台的增、删、改操作记录的审计信息
45		客户端访问日志	审计 EMM 客户端的登录、退出、注销操作记录（包括访问时间、用户、部门、登录设备、是否成功、真实 IP 等），可以根据时间、部门、用户、用户组进行统计
46		客户端问题反馈日志	支持管理平台查看 EMM 客户端提交的移动端日志、影像（图片、视频等），可通过“客户端问题反馈日志”查看详细内容，支持文件导出，方便研发定位问题
47		日志导出	支持日志报表导出，包含客户端产生的日志及管理端产生的日志
48	平台支撑能力	统一管理	一套系统支持 COPE（配发设备）及 BYOD 设备（员工自有设备）的统一管理，无需切换系统，统一管理页面对所有设备进行管理
49		消息推送	1）支持给门户自身推送系统消息；
50			2）消息内容支持文本、富文本、超链接；
51			3）支持第三方应用消息推送，点击消息通知直接拉起业务应用，苹果、小米、华为、OPPO、vivo 等设备即使应用不打开或进程不在也能接收消息；
52	权限管理	三权分立	系统支持安全管理员、系统管理员、审计管理员三个角色，三者权限分离，互相制约。安全管理员负责创建管理员和赋权，系统管理员负责系统的操作，审计管理员负责系统的所有日志审计工作
53		分级管理	支持安全管理员、系统管理员以及审计管理员分级管理，可根据需要创建下级管理员，并分配下级管理员的管理权限和管理范围
54	授权数量		含 350 点授权，5 年软件质保
55	厂商授权		▲提供原厂授权函及 5 年售后服务承诺函。

2.2.2 病毒防治【核心产品】

序号	指标项	指标描述
1	服务端基础功能	▲支持一个管理控制台同时管理 Linux、Windows 及国产操作系统，同时支持这些操作系统的服务器版和客户端版。如不兼容涉及重装，厂商需要负责完成全部点位重装并建议派驻两名工程师【须经甲方单位认可】，现场提供 1 年期技术保障。**【功能及效果截图】**
		服务控制端应能够管控医院存量杀毒客户端，确保医院后期终端杀毒运维一体化，包括但不限于病毒库更新等。
3		支持编辑资产管理信息，包括：资产等级，负责人，负责人邮箱，机房位置，固定资产编号，并支持填写其他备注信息
4		支持配置服务端备用 IP 地址，避免其中一个 IP 与客户端无法连接情况下，采用备用服务器进行通信。
5		支持配置服务端总下载带宽，避免大量客户端同一时间从服务端更新，造成带宽

		拥堵。
6	病毒检测能力	提供自主知识产权的防病毒引擎；
7		提供基于程序行为的独立恶意行为监控引擎，基于进程的操作行为和序列组合来应对未知威胁，包括：重复的系统文件，Hosets 文件修改，可疑行为，新 IE 插件，IE 设置修改，安全策略修改，动态链接库注入，Shell 修改，新服务，系统文件修改，防火墙策略修改，系统进程修改，新启动程序等
8		具备预测机器学习技术，可检测可疑进程中或来自可移动存储、Web 邮件等各渠道的文件中的新兴未知安全风险威胁。
9		产品能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁；
10		Linux ELF UPX 脱壳深度扫描能力
11	病毒防护能力	支持对压缩文件扫描，并可设定最大的压缩层数为 6
12		提供压缩文件扫描功能，可以对超过固定大小文件不予扫描，以减少扫描时间；
13		支持针对不同病毒类型针对性设置处置措施，可设定清除动作前，备份文件
14		为适应配置低的终端需求，不影响生产办公，终端在进行手动以及预设扫描时必须可以设置扫描时 CPU 占用比例，分高、中、低三个级别。低消耗下 CPU 高于 20%则暂停扫描以保证正常办公要求
15		具备爆发阻止功能，管理端可配置爆发阻止策略，封堵共享目录
16		具备机器学习能力
17		支持配置客户端的隔离恢复权限，避免客户端可以随意恢复隔离的病毒文件，造成病毒感染和传播。
18		具备 Web 信誉评估功能，包含 HTTPS 通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新
19		具备将可疑文件提交沙盒设备的联动能力，可自动提交可疑恶意文件，并可接收；
20		支持检测全局可疑站点（C&C)识别，监控可疑站点的连接，并提供记录或者阻止的处理措施；
21		支持 POC 高检出配置，可动态切换检测模式，可提升在打标环境下检测率
22	客户端基础功能	windows 客户端全功能支持英文版（包含软件商店、软件弹窗等）
23		支持以“普通模式”和“调试模式”收集客户端的故障信息，可以将收集的故障信息方便地反馈至安全厂商的服务人员进行故障排查分析。
24		可支持客户端在线实时迁移至指定的另一台服务器
25		支持客户端资源占用自动降级，当客户端 CPU 和内存使用率超过设定值时，将自动暂时关闭资源占用高的功能，待资源稳定时再开启。
26		支持设置客户端右下角托盘的展示与隐藏
27	产品更新及证书	支持管理员选择客户端立即更新或回退至上一版本
28		支持服务器端病毒码及引擎的还原功能；
29		支持 IOC，IOA 情报的单独更新和各自版本信息
30		所有产品必须是自主开发，拥有自主知识产权，提供软件著作权或专利证书
31	授权数量	含 350 点服务器+1300 点客户端授权，5 年软件质保及病毒库升级
32	厂商授权	提供原厂授权函及 5 年售后服务承诺函。

2.2.3 主机监控与审计【核心产品】

序号	指标项		指标描述
1	服务控制端	兼容性	▲为确保医院后期终端桌面管理一体化，减轻工作人员运维压力，新购服务控制端应能够统一管控医院现有存量客户端，如不兼容涉及重装或新购，厂商需要负责完成全部点位新购、重装费用，并至少派驻两名工程师【须经甲方单位认可】，现场提供 1 年期技术保障**【功能及效果截图】**

2		组织架构管理	支持手工维护组织架构部门和成员信息，批量导入导出操作；
3			支持 AD/LDAP、多 AD/LDAP 同步、钉钉、竹云 IAM、UOS 域、mysql 数据库同步组织架构
4			支持将组织架构中任意成员指定为系统管理员；支持配置管理员菜单和设备管理权限。
5		策略管理	支持指定设备、设备组、用户、用户组、部门、IP、MAC 下发策略； 支持策略离线生效; 支持策略下发例外管理（提供系统截图证明并加盖原厂商公章） 支持查看策略状态，策略未生效可能原因和生效时间，并可以根据时间段或文字输入未生效可能原因进行查询 支持策略变更审批、变更且下发策略时，可向审批员申请审批，审批同意后可进行策略变更及下发
6			支持策略场景定义，客户端在线、客户端离线等状态，可从以下维度（互联网状态、本地 IP 范围、终端在线情况、VPN 状态、网卡使用状态、TCP 连接状态、ICMP 连接状态、检测脚本、安全模式状态）定义。
7		平台扩展性	支持准入控制、桌面管理、数据防泄露、文档加密、终端检测响应、防病毒、移动终端管理功能模块一体化，一个管控平台，一个客户端。
8		定时任务	支持通过定期任务配置，自动将用户密码到期提醒和数据指标汇总信息以邮件方式通知管理员，将后台相关数据报表定期汇总和通知
9	客户端	客户端防护	支持客户端自我防护机制，客户端文件、进程、注册表、服务等都无法停止、修改、删除；客户端正常运行情况下安装目录隐藏；
10		安全模式	支持客户端安全模式下运行，客户端策略依然生效；
11		离线策略	客户端支持策略导入和导出功能，策略导出后可用于其他终端的导入，用于终端离线管控场景。支持离线终端审计信息导出、支持将终端产生的离线审计信息在后台设备概要信息中一键导入。 支持在客户端升级过程中断后支持回退操作；支持助手离线状态下回退；
12		功能在线调整	支持客户端功能在线调整，在功能调整、问题验证等场景下支持客户端文件（配置文件、DLL 等）实时替换，无需覆盖安装、重启终端；
13		多操作系统支持	支持 Windows、macOS、Linux 客户端、国产化统信 UOS/麒麟操作系统、移动终端；
14	设备概要信息	设备基本属性	支持以设备为维度，展示设备名称、IP、MAC 地址、所属用户、所属部门等详细信息，所展示的设备字段可进行自定义选择是否进行展示；可根据设备资产编号状态进行查询
15		软硬件资产管理	支持自动采集终端设备信息，包括：硬件信息、操作系统信息、软件信息、用户信息、已应用的策略信息、历史 IP 地址信息等。

16			支持显示完整的终端信息，包含但不限于：计算机名、用户名、操作系统版本及主机进程信息、主机端口信息、主机服务信息。
17		设备查询	支持根据硬件信息检索设备，并设置任意组合进行查询其 IP 地址、MAC 地址、设备名称、设备类型、网段、网段组、用户、部门、设备组、设备位置、连接交换机、设备状态、客户端运行状态、主板型号、主板序列号、BIOS 制造商、PCI 设备描述、CPU 型号、设备历史 IP、软件名称、CPU 频率、内存大小、硬盘大小、操作系统、设备最近启动时间、设备最近离线时间、设备发现时间、客户端最近离线时间、逻辑磁盘、显卡、声卡、网卡、显示器；
18			支持将上述查询条件进行标签保存，后续只需要点击标签接口快速查询，无需再次输入查询条件；
19		自定义设备组	支持配置设置组，在入网安全规则、入网安全检查的策略中调用手工分组；其中，支持手工分组、自动分组两种方式；手工分组支持 excel 方式导入设备列表；自动分组支持通过 IP 地址段及部门进行自动分组；
20		配置变更事件	支持对设备的 CPU、内存条、显卡、光驱、硬盘、主板、网卡进行监控； 支持对设备所有的软件变化、除 windows 补丁包外的软件配置变化、指定软件、指定软件外配置的变化； 支持审计拆卸硬盘及更换硬盘行为并上传至设备配置变更信息展示（提供系统截图证明并加盖原厂商公章）
21	单点运维	单点运维	1、进程：支持查看实时进程详细信息、实时进程历史行为、进程文件、对进程进行内存转储；支持根据进程反查数据，支持启动/停止终端进程 2、启动项：支持查看启动项文件路径/注册表路径、禁用/删除启动项、支持可选显示系统启动项 3、驱动：查看驱动及驱动文件路径 4、服务：查看服务信息、启动/停止/重启服务、修改服务启动类型 5、注册表：查看注册表、支持新增、删除、编辑、重命名注册表 6、本地文件：查看、下载/删除本地文件、新建文件夹、上传文件 7、远程调查：支持各种 cmd、powershell 命令调查终端系统
22			支持设置终端定时开机
23	非授权外联控制	非法外联控制	支持 Windows 终端设备的外联接口进行安全管控，包括但不限于红外、蓝牙、软盘、光盘、串口、并口、网络接口、USB 接口以及其他外联设备；
24			支持禁用终端电脑共享 WiFi 热点（含 windows 和 macOS)
25			支持对无线以太网卡进行禁用、审计、仅在有线网卡工作时禁用、WiFi 白名单、WiFi 黑名单控制；
26			支持无线 SSID 仿冒检测；（提供系统截图证明并加盖原厂商公章）
27			支持根据设备的 PID、HWID 等信息进行禁用和例外；从而达到一次允许或禁止某个厂家的设备或某一批次的设备；（提供系统截图证明并加盖原厂商公章）

28			支持 Linux 下 U 盘禁用，macOS 支持禁用 U 盘并审计、未注册 U 盘只读并审计、禁止和审计自建 WiFi、禁用和审计无线网卡、WiFi 白名单、蓝牙控制
29		硬件管理策略	支持基于设备 GUID、设备实例路径、显示名称、设备服务名等进行某一类设备进行管控，包括审计与禁止；
30		网络连接审计与控制	支持通过 PING/TCP/HTTP 等方式检测终端是否与互联网连通、检测终端是否与其他网络连通（含电脑直连方式）、检测终端是否与特定网络连通；
31			非法外联处置：禁用网卡；阻断网络直到事件恢复或必须由管理员恢复；锁屏，必须管理员恢复；
32	补丁管理	补丁检查与更新	无需额外搭建补丁服务器，能够对终端的补丁安装情况进行检查和强制修复；也支持与微软 WSUS 补丁服务器联动；
33		补丁服务器离线自动更新方案	在补丁服务器不直接开放互联网、不采用代理服务器代理上互联网，确保网络隔离的情况下，有能够将补丁文件、补丁库文件从互联网自动下载并更新到内网服务器的解决方案
34		补丁智能中继	手工指定或自动学习选举出智能分配中继点，中继点只需安装客户端 无需安装其他组件；并支持中继点到服务器的下载流量限速，PC 到中继点的限速带宽控制（提供系统截图证明并加盖原厂商公章）
35		补丁闲时安装	支持补丁闲时安装，超过预设时间鼠标键盘无操作才进行补丁安装。
36		补丁安装情况	支持统计补丁安装情况，如未安装、已安装并生效、已安装未重启、补丁总计，补丁安装率等状态；
37		补丁卸载	支持补丁批量远程卸载；按照安装时间、安全更新级别、安全更新类型等条件进行多个补丁同时卸载。
38	终端安全	防火墙	支持终端主机防火墙控制，对指定进程、协议、IP、域名、服务端口访问进行审计、入站和出站阻断控制，
39			支持已安装客户端的主机与未安装客户端或客户端离线的主机进行隔离控制；支持 DNS 黑白名单控制。
40		主机进程管理	支持以进程名称、进程文件属性、进程文件 CRC 值、进程文件 MD5 值、软件名称、目录名称、进程签名等方式进行黑白名单进程管控；能对重要进程运行状态进行监视；
41		注册表访问控制	支持指定进程创建、修改、删除、重命名注册表行为的阻止与审计；
42		终端用户操作系统账户管理策略	支持管理员对终端操作系统账户/账户组配置变更、账户登录、注销的行为进行审计。对合规账户进行监控审计，及时发现终端上存在的违规账户。

43		终端系统自检	持对终端配置和环境进行检查，包括设备注册情况，软件（Office、IE、WPS）版本检查、磁盘剩余空间检查，是否启用 IE 代理、DNS 检查、DHCP 检查、加域信息检查、网络连接检查、系统账户密码长时间未修改检查；支持自定义检查项，对终端的注册表、文件、操作系统版本、进程、服务进行检查，同时，可对以上检查条件进行任务组合检查；
44		windows 本地安全策略	支持禁止修改注册表、禁止修改网络属性、禁止设置 TCP/IP 属性、禁止设置固定 IP 等；支持对系统服务的启动类型进行设置
45	消息通知	消息通知	1、可给指定的 IP 范围、网段、部门、设备分组或所有代理发送广播信息; 2、提供管理员消息发布渠道，包含通知频率、通知时间段、通知框属性（窗体大小、窗体显示位置、置顶、关闭、窗体超时自动关闭）控制； 3、支持纯文本、富文本、HTML 文件通知、HTML-zip 文件通知、URL 通知；
46	节能管理	节能措施	支持闲时（鼠标/键盘长时间未操作）终端关机、注销、锁定、重启、睡眠、休眠、关闭显示器等操作；
47	远程协助	远程模式	支持管理员强制远程和管理员发起申请由终端确定后建立远程协助；支持终端用户主动发起远程申请协助；支持多对一模式，多个管理员可同时对一个终端进行远程协助；支持一对多模式，一个管理员可同时对多个终端进行远程协助；支持在锁屏、注销、系统未登录状态下发起远程协助； 支持 NAT 环境远程；
48		远程审计与交互	支持对管理员的远程会话过程详细审计功能、支持远程协助过程录像；支持带宽自动优化功能；支持远程传送文件和文件夹功能、支持远程即时通讯；
49		多平台支持	支持远程协助 Windows、macOS 终端；
50	助手首页运营管理	助手首页个性化定制	支持在客户端首页进行个性化定制发布企业相关文化/政策/公告相关的图片，进行公告通知，并支持将常用网址、业务系统在助手首页定制，支持在助手首页进行常用工具发布，简化故障运维；同时也支持将终端技术信息显示在首页的运维风格显示；
51	数据管控	屏幕录像	1、基于远程、邮件、插入 USB、即时聊天等行为进行自动录屏 2、屏幕录像播放支持“普通模式”和“极速模式”，播放支持暂停；支持在底部显示用户、设备信息，不遮挡录屏播放；录像分屏审计，多屏切换查看；
52		文件操作管控	支持管控终端上的文件操作，文件源或目的为本地硬盘、移动存储介质（U 盘、移动硬盘、SD 卡）、安卓智能设备通过 ADB 方式、网络共享、mstsc 远程桌面或其他存储设备，可以进行禁止、审计、备份等管控操作；
53			支持对文件的读、写、复制、剪切、创建、删除、另存为、新建、重命名等动作进行监控；支持记录文件路径、文件名、文件大小；文件操作过程中进行敏感检查；对行为进行阻断；对拷贝进行加密、解密、透明加解密、审批、审计、上传拷贝文件副本；

54	终端水印	屏幕水印方案	支持将水印信息加载到屏幕上方，支持宏参数替换（用户名、用户全名、计算机名、计算机全名、IP 地址、MAC 地址、日期、时间）。支持自定义显示位置、字体、字号、水印密度、水印颜色、透明度；支持水印单行模式、对齐方式、水印位置；支持明文水印、二维码水印、图片水印、矢量水印（点阵矢量图形方式，浮现在屏幕上方；支持设置颜色、透明度、形状大小、形状间距）； 支持始终加载在屏幕最上方与仅加载在屏幕桌面上方,不遮挡应用窗口；
55			当屏幕水印颜色与背景色相近时，水印颜色自动增强反色，并可自定义调整屏幕反色检测间隔的时间
56			支持屏幕截图控制、附加盲水印（QQ、微信、企业微信、TIM、企业 QQ、钉钉、键盘按键截屏）；
57			支持对接**高维数据**的盲水印技术，实现在用户无感知的情况下的屏幕盲水印以及泄漏后的追溯；
58			支持明文水印：在文档打印时，将水印信息一起打印到文档上，支持宏替换。支持自定义显示位置、字体、字号、水印密度、水印颜色、透明度；支持水印单行模式、对齐方式、水印位置；支持明文水印、二维码水印、图片水印、矢量水印（点阵矢量图形方式，浮现在屏幕上方；支持设置颜色、透明度、形状大小、形状间距）；
59	授权数量		含 1300 点授权，5 年软件质保
60	厂商授权		提供原厂授权函及 5 年售后服务承诺函。

2.2.4 日志分析

序号	指标项	指标描述
1	性能要求	平均每秒处理日志数（eps）性能不低于 2000 条/秒，含 500 个日志审计授权。5 年软件质保。
2	丰富脚本解析方法	根据用户日志的格式，增加脚本解析日志的方法，满足新增品牌的日志解析
3	优化原有脚本解析方法	优化日志解析脚本逻辑，提高脚本解析速度及准确度
4	支持的网络及安全设备日志接入	支持网络设备及安全设备的日志接入，包括天融信 ,迪普,锐捷等设备日志接入
5	应用业务日志接入	增加应用日志的接入，包括 java,nginx,redis 等等应用日志的接入
6	网络智能扫描	1.系统应能够在无需其它条件参数的情况下，发现指定网络当中在线的 IP 资源。
7		2.系统应能够识别 IP 所对应的设备为网络设备还是服务器，并标示出该服务器上正在运行的各种服务。
8	自动发现扩展	1.系统需支持自动发现能力的扩展，可以通过编写脚本的方式实现对新类型配置项属性的自动发现。
9		2.系统需提供可视化界面用于将脚本所发现的属性与系统中配置项模型的属性进行匹配。
10	分组维护管理	1.系统应支持用户根据其组织机构、或数据维护职责等纬度创建相应的维护组，并设定系统中那些角色用户有权限访问所创建的维护组。

11		2.系统需支持创建配置项的自动认领规则，对于属性满足规则的配置项可自动被纳入到维护组中。
12	系统扩展性要求	1.投标单位需提供承诺书，承诺系统需提供方便灵活的二次开发工具，当采购人业务需求发生变化时时，可以快速根据实际新需求进行定制开发新功能，以插件的方式无缝接入原有系统，平台系统本身无需任何改动，实现采购人业务监控的持续发展及完善。
13		2.投标人须提供系统软件二次开发工具及该工具的使用手册，供招标人保证管理软件系统的扩展性及持续性。
14	系统性能要求	1.Agent 最少的资源占用：在受控设备上安装 Agent 来采集数据并且和服务器进行通讯，应保证在受控设备上安装的客户端程序无论是硬盘占用空间、内存占用空间、网络占用带宽，还是 CPU 使用率都保持最小，最大不超过 3%。
15		2.Agent 跨平台：在受控设备上安装 Agent 应支持 windows、linux、hp unix、Sco unix、Aix Unix 等目前主流操作系统。
16		3.松耦合：数据采集不能对其他系统的稳定运行造成影响；
17		4.及时性：保证告警、性能、配置信息能及时采集，采集的周期用户可以通过界面配置；
18		5.采集方式多样性：支持 Agent、主动探测、接收上报等多种采集方式。
19	统计报表要求	报表平台支持把基础医院、软件资源、应用系统等资产情况进行统计及分析，并且以每日、每周、每月以报表形式导出成为 Excel、PDF、Word 等多种格式。
20		报表视图需涵盖以下信息：
21		1、实时显示当前业务系统内 CI 项信息。
22		2、实时显示选中 CI 项的关联关系。
23	厂商授权	提供原厂授权函及 5 年售后服务承诺函。

2.2.5 运维安全管理

序号	指标项	指标描述
1	授权数量	500 个 icense(管理资源数)，可扩展至 1000:最大支持 500 个图形并发会话或最大支持 1000 个字符并发会话。
2	硬件配置	≤2U 机架结构，≥6 个千兆电口，≥4 个千兆光口，≥16G 内存，配置≥4T 硬盘，CPU：国产化自主可控 8 核或以上
3	首页展示	系统应具备首页展示功能，首页展示系统相关业务数据，至少应包括工单、用户、资产、会话统计；实时运维会话数；今日用户与资产运维统计；月运维趋势统计；今日运维 TOP10；行为告警分布；运维指令 TOP10
4	图表展示	系统首页展示数据应采用图表方式进行呈现，图表展示方式包括但不限于饼状图、折线图、仪表盘、柱状图，展示效果清晰，数据呈现无错行混乱等现象
5	运维趋势	系统应能够按照月为周期统计多协议运维频率，统计协议包括但不限于 SSH、WEB、RDP、SFTP、Telnet 等，可选择多协议与单协议不同展示方式

6	免客户端	资产运维登录应采用免客户端设计，运维人员在使用过程中无需安装任何登录组件
7	资产类型/组选择	系统在运维页面应提供资产类型与资产组选择，系统自动展示选择类型/资产组下当前用户具备登录权限的资产
8	资产搜索	运维登录页面应支持资产搜索功能，并支持资产全量数据的模糊搜索
9	离线登录	系统应具备针对 SSH、SFTP、Telnet 等字符协议的离线登录方式，具备针对相关资产的 Session 导出，支持多款字符型管理工具，包括但不限于 CRT 中文版、CRT 英文版、Xshell 等
10	批量运维	系统应支持多资产多协议的批量运维管理，运维人员可通过策略创建的方式勾选对应资产与协议生成批量运维策略，一键批量快捷登录。
11	用户创建	系统应具备自身账号管理能力，通过页面配置的方式进行系统账号的创建添加操作，创建用户应支持对于各项数据管理，包括但不限于用户名、用户描述、密码、角色、用户组、邮箱、手机、身份证号码、到期时间、认证方式等，用户创建过程中可随机生成符合策略的密码，避免初始密码重复造成账号盗用风险
12	用户认证	系统应具备多种强认证方式，实现二级认证，认证方式包括但不限于 Google 令牌认证、短信认证、Radius 认证、AD 域认证、LADP 认证、证书认证、动态口令认证等
13	用户锁定	系统应能够创建临时用户，可对创建的用户进行到期时间设定，用户到期后自动锁定，被锁定用户可通过管理员手动解锁并延长使用周期
14	用户组管理	系统应具备针对用户的组织管理，可按照部门、权限、责任等相关信息创建用户组，支持多级列表展示
15	用户导入导出	系统应具备用户信息的导入导出功能，可选择部分用户或全量用户导出，系统具备导入模块下载，模板中应具备对导入字段的解释说明注释，通过编辑模块或修改历史导出数据，页面导入系统，实现用户快捷创建与批量修改
16	用户统计	系统应具备用户统计功能，能够按照用户组与用户角色饼状图展示用户分布比例
17	多权分离	系统应能够对用户进行权限划分，系统内置多种操作权限，其中包括但不限于超级管理员、安全保密员、安全审计员、系统管理员、运维管理员、运维操作员，并提供权限角色新建功能，用户可根据自身管理需要创建特色的管理角色
18	用户授权	系统应支持创建用户时授权资产功能，可按照单资产或资产组授权，简化系统授权配置操作
19	协议支持	系统应支持 SSH、RDP、SFTP、FTP、Telnet、VNC、X11 等标准协议管理
20		系统应支持 Orcale、Sqlserver、Mysql 等数据库管理
21		系统应支持 B/S、C/S 应用程序管理
22	资产管理	系统应具备资产创建管理功能，提供统一的资产管理界面，用户通过资产管理界面可配置资产名称、资产类型、资产型号、资产地址（域名）、计算机名、资产组、资产账号、资产协议等信息
23	资产导入导出	系统应具备资产信息的导入导出功能，可选择部分资产或全量资产导出，具备导入模板下载，模板内应具备字段说明注释，通过编辑模块或历史导出信息，页面导入系统，实现资产快捷创建与批量修改
24	资产组配置	系统应具备针对资产的分组管理，支持多级列表展示

25	应用发布服务器配置	系统应具备应用发布服务器配置与管理功能，支持对各类应用程序的地址配置，支持内置应用发布服务器模式
26	资产类型	系统应具备资产类型添加编辑页面，用户可按照自身资产情况添加资产类型，资产类型可独立挂载改密脚本，避免因资产类型问题出现改密任务失败等业务问题
27	资产授权	系统资产管理应支持授权管理功能，可将资产按照资产账号、资产协议等信息授权于用户/用户组实现资产授权，系统自动同步资产授权信息与用户授权信息
28	运维策略	系统应具备针对运维行为的策略配置管理功能，策略配置采用统一界面设计，无需在其他功能页面另行挂载，运维策略应支持针对访问地址、访问时间、对象行为等运维行为的控制，控制方式应支持审批、阻断、告警等多种模式
29	上下行控制	系统应支持运维过程中文字的上下行控制，上下行控制应支持单向配置
30	本机访问策略	系统应具备针对本系统的访问控制策略，策略配置采用统一页面设计，无需在其他功能页面另行挂载，本机访问策略应支持针对时间、IP 地址等访问行为的控制，控制方式应支持阻止、放行等多种模式
31		针对于访问时间的设定应支持按照年、月、日、时、分的周期性控制方式
32	改密策略	系统应具备自动批量改密功能，用户可选择资产采用手动指定密码或密码策略随机生成的方式进行改密，改密策略应支持周期性执行，执行周期应能支持每天、每周、每月的频率
33	改密记录查询	系统应支持改密策略运行后的改密信息查询，改密记录至少应包含运行结果、执行过程等信息
34	密码规则策略	系统应具备密码策略管理功能，通过配置密码策略实现登录用户口令复杂度设定，设定内容应包括但不限于密码长度、大写字母个数、小写字母个数、特殊字符个数、数字个数、改密周期等，应支持下次登录强制修改密码设定
35	防暴力破解	系统应支持设定多次密码错误锁定用户功能，应具备计数重置时间、密码错误次数、锁定时长等相关信息的设定
36	审批策略	系统应能够对审批模式及审批负责人进行配置，审批模式应支持并行审批、串行审批等多种模式，审批流程可设置三级负责人审批，每级可为多个负责人
37	策略优先级	系统应具备类似于防火墙策略优先级控制的管理模式，用户可自由调整策略执行控制的优先级，并可通过页面查询策略命中次数
38	用户追溯	系统应具备按照用户与时间范围展示用户运维行为，展示方式应为树形图表展示，展示内容应不少于时间、资产、运维次数等信息
39	资产追溯	系统应支持按照资产与时间范围展示资产被运维情况，展示方式应为树形图表展示，展示内容应不少于运维人员、运维时间、运维次数等信息
40	授权图谱	系统应支持按照用户组\用户与资产组\资产生成运维授权图谱，图谱具备多种布局展示，展示布局包括但不限于平铺布局、广度布局、圆形布局、网格布局、同心圆布局、休闲布局等

41	会话统计	系统应支持对于运维行为的统计图表展示，展示图表包括但不限于资产运维趋势点线图、用户运维次数（TOP10）柱状图、协议运维排名柱状图、协议运维趋势点线图
42	指令统计	系统应支持对于运维指令的统计图表展示，展示图表包括但不限于指令分布（TOP10）柱状图、TOP10 指令用户分布柱状图、指令资产账号分布饼状图、指令排行（TOP10）柱状图
43	统计周期	系统应支持对于统计图表展示数据按照时间周期设定，统计范围可按照系统内置周期或自由设定，应支持数据图表自动刷新设定
44	图表编辑	系统应支持对于统计图表的编辑功能，可自由调整图表的大小、位置等图表布局展示
45	实时会话	系统应具备实时会话监控功能，当运维人员进行运维操作时审计员可通过实时会话监控操作过程，出现危险行为时可实时阻断，监控过程对于运维人员应为无感设定
46	历史会话	系统应提供运维操作的历史在线查询页面，用户通过此页面查询历史操作行为，操作记录采用行为仿真的方式呈现操作过程，操作回放支持暂停、播放、多倍速播放等，倍速播放包括但不限于 0.5 倍速、2 倍速、4 倍速、8 倍速、16 倍速等，回放过程应支持指令定位功能，点击指令自动跳转至对应视频位置
47	数据索引	系统应具备数据索引功能，数据索引按照天进行压缩存储，用户可自由开启关闭数据索引
48	网络设置	系统应提供针对自身的网络设置功能
49	状态外发	系统支持被动将自身性能通过 SNMP 协议采集至上层平台
50	日志外发	系统应支持通过 syslog 协议将审计信息、告警信息外发至对应的上层平台
51	云注册管理	系统应支持云中心授权模式，支持独立授权服务器部署，用户可根据自身需求分配授权
52	厂商授权	提供原厂授权函及 5 年售后服务承诺函。

2.2.6 WEB 应用防火墙【关键核心产品】

序号	指标项	指标要求
1	处理能力	对外支持 IPV4/6 双协议栈；应用吞吐≥2G；网络吞吐≥4G；并发量≥50 万。
2	硬件配置	≤2U,USB 口≥2，管理口≥1，≥6 个千兆电口，≥2 个千兆光口，≥2 个万兆光口，≥32G 内存，3.5 寸热插拔硬盘位≥1，配置≥1T 硬盘，双电源。
3	售后服务	5 年软件、特征库升级，5 年硬件质保，提供 7×24 小时在线技术支持，1 小时内响应服务。
4	系统能力	支持直通模式，流量经过系统，不做任何检测及拦截处理。
5		所投产品的防护配置和查询功能须支持 IPv6。
6		所投产品须支持针对中文域名的防护。
7		平台具备 HA 部署能力。能够进行在线状态检测，并根据检测结果自动切换，并保持配置同步、session 同步。

8		本项目中所投产品不应含有使用 Flash 技术用于访问重要策略控制的内容。
9		系统管理员具备账户管理功能，支持对口令复杂度和口令生存期的设置。
10		具备自检信息功能，可显示设备自身系统运行状态信息及异常告警。
11		报警功能支持界面及邮件报警。
12		支持反向代理部署模式，逻辑串联。支持 IP 地址收敛效果，支持互联网端对非标端口收敛效果。
13	安全防护	支持对源站非 80/443 端口但为 HTTP 协议的防护，支持对 HTTP 协议的异常元素、异常参数、非法编码和解码的灵活控制与处理。
14		支持域名或 IP 地址及多端口形式访问防护。
15		能基于多种 HTTP 方法执行访问控制，包括：GET、POST、HEAD、PUT 等。
16		支持针对主流 Web 服务器及插件的已知漏洞防护。Web 服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS 等；插件应覆盖：dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress 等。
17		支持 SQL 注入、XSS、SSI 指令、Webshell 防护，路径穿越及远程文件包含的攻击防护。支持使 HTTP 头域中的 Cookie、Referer、User-Agent，Except 字段过防护策略。
18		支持 CSRF（跨站请求伪造）防护。
19		支持爬虫防护，实现对爬虫特征进行识别和阻断，防止页面因爬虫而引起信息泄露等问题。
20		支持工具类软件对站点高频扫描的防护，并提供应用层人机识别的拦截手段。
21		支持识别非法上传/下载行为，阻断敏感信息泄露、恶意代码攻击、错误配置攻击、隐藏字段攻击、会话劫持攻击、参数篡改攻击、弱口令攻击、Webshell 行为拦截。
22		支持识别并阻断自动化攻击及第三方引擎的访问。
23		防应用层 HTTP DDoS（CC）攻击。
24		支持白名单功能，可添加单个或一个段落的地址开放于白名单内，不受策略限制。
25		支持攻击黑名单限制，可将识别到的黑 IP 加入黑名单内，并可设定黑名单时长，时间到后可自动解禁。
26	安全加固	支持 Web 站点隐藏和伪装的安全策略，包括操作系统类型、WEB 服务器类型、HTTP 响应报文头。
27		支持自定义错误页面的拦截，防止 404、403、502 等报错页面泄露敏感信息。
28		支持 TLS 加固策略，至少能够提供 TLS1.2 以上的安全加固措施。
29		支持 HTTPS 强制跳转。
30		支持站点锁定，可以将站点页面缓存到防护平台。
31		支持对请求（POST）数据和响应（GET）数据进行脱敏。
32	web 组件加密	支持 Cookie 内容加密。
33		▲支持针对 WEB 站点中的代码文件名称进行加密。【提供产品功能截图，以及效果截图：通过 Burpsuite 工具抓包，截图加密后的效果】
34		支持 HTML 内容整体动态加密，可防站点目录爬取、防爬虫解析等。通过浏览器查看网络传输到应用层的页面代码应为密文。

35		▲支持 JS 文件源码实时动态加密，可防关键代码分析调试、可防 JS 开源框架漏洞。支持反馈给浏览器的源代码加密，阻止源代码浏览器端的代码分析调试。【提供产品功能截图，以及效果截图：通过 Burpsuite 工具抓包，截图加密后的效果】
36	数据安全	支持 WebAPI 动态发现、威胁监测及名称加密等功能。【提供功能截图及效果截图】
37		支持针对请求数据进行安全检查，支持对 SQL 注入、XSS 注入、CMD 注入、自动化攻击、Webshell 等场景进行安全防护。
38		▲支持对 API 接口名称进行动态加密，加密算法采用国密算法 SM2/SM3/SM4 标准。【提供产品功能截图，以及效果截图：通过 Burpsuite 工具抓包，截图加密后的效果】
39		▲支持对 API 上行（POST）数据进行动态加密，加密算法采用国密算法 SM2/SM3/SM4 标准。【提供产品功能截图，以及效果截图：通过 Burpsuite 工具抓包，截图加密后的效果】
40		▲支持对 API 下行数据进行动态加密，加密算法采用国密算法 SM2/SM3/SM4 标准。【提供产品功能截图，以及效果截图：通过 Burpsuite 工具抓包，截图加密后的效果】
41		支持针对浏览器端 WebAPI 加密环境安全检查，针对拟爬虫浏览器检查。
42	重保模式	支持重点时期开启重保模式，业务系统对互联网显示重保模式页面。
43		重保模式页面支持对每个不同站点进行个性化自定义设置。
44		重保模式的页面内容支持用户自定义，上传自定义内容后实时生效。
45		重保模式支持用户对日期范围、时间段范围进行自定义，自定义后实时生效，其中日期支持周一至周日的复合选择自定义。
46		重保模式支持用户自定义 IP 白名单，如白名单内的 IP 不显示重保模式。
47		重保模式效果支持用户提前设置各种参数，时间到了后会自动生效。
48		支持提供站点和策略的多对多的绑定关系，单个站点可以绑定多个重保策略，单个策略可以匹配多个站点.
49	后台管理系统安全性	后台 Web 管理界面须为中文界面显示。
50		后台支持对保护的域名或 IP 资产进行管理及监测(包括状态及流量) 。
51		后台管理系统需要 B/S 架构，支持 PC 端机器访问时 HTTPS 双向身份认证，即只对安装了证书的系统才支持业务访问。
52		后台管理系统需要 B/S 架构，敏感数据或业务数据需要加密保护。
53		支持后台管理系统三权分立，包括系统管理员、策略管理员、审计管理员。
54	日志功能	支持基于时间、域名、动作、事件类型、URL、返回码等条件的日志查询。
55		支持在安全日志中带有客户端真实 IP 地址，便于 IP 溯源。
56		支持日志分时段导出、全部导出。
57		支持以 Syslog 格式向指定统一 Syslog 日志中心推送本地日志信息。
58		支持日志存放周期管理，须支持 6 个月及以上天数的存放，过期日志可配置自动清理。
59	厂商授	▲提供原厂授权函及售后服务承诺函。

	权	

2.2.7 网络型流量控制

序号	指标项	指标描述
1	硬件配置	≤2U 机架结构，≥4 个千兆电口，≥2 个千兆光口，≥16G 内存，配置≥1T 硬盘，CPU：国产化自主可控 8 核或以上，5 年软硬件质保。
2	挖矿检测	1. 提供多样性的挖矿检测手段，能够检测挖矿木马投递、挖矿木马横向移动行为、挖矿软件、矿池域名解析、矿池连接、矿池协议等。
3		2. 矿池协议告警须提供虚拟币种类别。
4		3. 挖矿告警须提供专项告警页面，独立于其它告警。
5		4. 能够自动解析 DNS 响应的矿池及 IP 地址。
6	支持协议	1. 支持 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW、TFTP、NNTP 等 176 种协议报文识别，支持 1000+种应用识别；
7		2. 支持识别 ORACLE、HTTP、RDP、TELNET、SSH、FTP、SMB、MYSQL、PGSQL、REDIS、IMAP、POP3、SMTP 等登录行为；
8		3. 支持多层 VLAN、VxLAN、MPLS、GRE 等网络流量的解析检测；
9	沙箱分析	1. 提供内置沙箱系统，内置沙箱允许用户导入自定义镜像，并支持平台沙箱镜像。
10		2. 能够对样本进行过滤去重减少分析数量
11		3. 具有安全风险评估技术分析：包含针对注册表、内存、程序、网络活动、文件系统等操作系统环境的变化进行记录与分析
12		5. 沙箱能够对未知漏洞利用代码和恶意程序的以下行为进行动态分析：
13		1). 进程操作行为
14		2). 文件操作行为，文件删除、下载、共享或者复制
15		3). 系统配置操作行为，自运行或其他系统配置
16		4). 网络通信行为，控制与命令 (C&C)违规外联
17		5). 恶意未知威胁逃逸行为
18		6). 内存镜像分析，畸形，有瑕疵，或者带有已知威胁特征，劫持、重定向，或数据窃取，进程、服务，或者内存对象被篡改
19		6. 支持未知威胁事件证据留存
20		7. 广泛的文档分析支持：Acrobat Reader 7, 8, 9, X, 微软 Office 常用版本（Word, Excel, Powerpoint）、Flash 常用版本、LNK、执行文件，微软 HTML Application（HTA）, JS, JSE, VBS, VBE, Java, Java Applet, PowerShell Script 等。
21		8. 对提交的可疑 URL 利用沙箱执行页面扫描、动态链接分析、动态脚本及控件分析，并针对 URL 指向的可疑文件进行沙箱分析
22		9. 提供分析结果的自动入库：侦测设备自我学习功能
23		10. 提供样本分析报告，报告内容包括：样本基本信息、执行后行为记录、重点标注恶意行为。
24		11. 提供灵活的沙箱投递策略，支持按照数据网络协议、文件类型等条件灵活配置投递策略。
25	威胁分类告警	支持按照网络攻击、挖矿、扫描、暴力破解、恶意文件、威胁情报等告警进行分类，提高运维效率。须截图证明
26	WebShell	1. 支持主流 Webshell 工具检测：冰蝎、哥斯拉、菜刀、蚁剑、weevely、

	工具检测	开山斧等。
27		2. 支持 WEBSHELL 检测,可检测访问 webshell 的行为,包含具体对应的 URL、返回码、返回数据包内容等，可显示 Webshell 后门是否植入成功
28	暴力破解行为检测研判	1. 支持 HTTP、TELNET、FTP、MYSQL、PGSQL、REDIS、IMAP、POP3、SMTP、RDP、SSH、SMB、DB2、MongoDB、MSSQL 等协议的暴力破解，能识别出登录次数、账户信息、爆破成功与否的攻击状态；
29		2. 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；
30		3. 支持分布式爆破、慢速爆破检测，且界面可配。
31	威胁情报	1. 失陷主机检测功能具备威胁情报 IOC 检测能力，支持的威胁类型包括但不限于：远控、钓鱼、僵尸网络、矿池地址、挖矿木马、勒索软件、窃密木马、远控木马、网络蠕虫、黑客工具、APT 攻击事件、流氓推广、其他恶意软件，IOC 情报总量达 800 万以上。
32		2. 支持提供域名、URL、IP 类型的威胁情报检测，对 IP 情报可以精确到端口级别。支持和威胁情报云端联动，有效检测新威胁。
33	威胁检测特征自定义	支持网络威胁自定义与威胁情报自定义，网络威胁能自主添加规则名称，规则等级与规则类型，语法兼容业界最常用的 snort 规则的写法。威胁情报自定义包括 IP、URL、DOMAIN、文件 HASH 四种类型，可以根据具体的使用场景进行选择。威胁情报自定义的规则可以支持多个同类对象的集合，比如对多个 IP 同时进行监控。
34	恶意文件流转溯源	能够以某个恶意文件为中心，溯源整个文件的流转记录，并以图形化方式展示出来，直观展示在不同时间点上该恶意文件在不同主机服务器上的传播路径，支持文件下载。需截图证明
35	威胁流量数据下载	支持威胁流量的自动存储，及威胁流量 PCAP 文件格式下载。
36	网络流量威胁验伤	支持对网络 Http 攻击流量的应答码及攻击状态展示
37	流量抓包与回放	1. 能够配置灵活的抓包策略，支持设定抓包的 P 地址范围、协议等条件，可设定抓包文件大小。
38		2. 支持 pcap 回放功能，对导入的 pcap 进行回放并进行威胁检测，回放产生的告警必须和生产网络流量的告警分页面展示，避免干扰正常安全运营。
39	厂商资质	设备制造厂商商具备《信息安全服务资质-软件开发服务资质》，需提供有效证书的复印件；
40		具有国家信息安全漏洞库兼容性资质证书，需提供有效证书的复印件
41	厂商授权	提供原厂授权函及 5 年售后服务承诺函。

2.2.8 终端接入控制【核心产品】

序号	指标项	指标描述

1	基本要求	系统要求	投标产品需符合公安部终端接入控制标准（GA/T 1105-2013）（提供相关证明材料）
2			具有独立自主知识产权，须为标准机架式硬件产品。具有独立自主知识产权的准入控制技术。
3			支持与现有准入系统联动，获取网络及终端信息。**【功能及效果截图】**
4		硬件及性能要求	支持 1500 个终端接入；5 年软硬件质保
5			≤2U 机架结构，≥6 个千兆电口，≥4 个千兆光口，≥16G 内存，配置≥4T 硬盘，CPU：国产化自主可控 8 核或以上
6		IPv6 支持	支持在 IPv4 和 IPv6 双栈环境下的终端准入控制、重定向、认证、安检、修复等。
7		高可用性	1. 准入设备必须具备 HA 模式；
8			2. 提供专属第三方检查平台，在系统故障时提供秒级的逃生功能；
9			3. 支持智能逃生，当异常指定时间段内异常入网终端达到指定阀值时开启自动逃生。
10		语言支持	1.支持终端入网时客户端和 WEB 页面语言显示跟随系统或自行中英文双语切换）；
11			2.管理员平台支持中文界面，英文界面。
12		准入技术	1.准入设备支持基于多厂商 Virtual Gateway 的 VLAN 隔离技术，实现无客户端下端口级准入控制。
13			2.准入设备支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面；
14			3.支持交换机接口动态 VLAN 下发、端口隔离模式的网络边界管理。
15			4.支持通过 MAC 旁路认证进行 ACL 下发的准入控制。
16		802.1x 特性支持	1.支持根据账户指配下发的 VLAN/ACL。
17			2.通过 802.1x 认证进行 VLAN 切换后，可以在 30 秒内重新进行 IP 地址获取，避免切换 VLAN 后需要等待较长时间才能够访问网络。
18			3.终端（PC 和哑终端）认证通过后，当需要对终端进行下线、切换 VLAN/ACL 等动作时，准入系统可以通过动态授权（CoA）的方式立即执行，而不需要等待重认证周期。
19			4.支持系统自带客户端。
20			5.支持域计算机单点登录，在 802.1x 环境下，管理员将终端加入了域管理，终端用户第一次使用时准入客户端可以帮助用户进行 802.1x 认证，以便终端可以和 AD 域服务器进行账号验证，避免第一次无法登录的问题。
21			6.支持 Linux GUI 认证，提供常见主流 Linux（包括：ubuntu、Readhat 等）802.1x 客户端，可以通过客户端进行 802.1x 认证。

22			7.支持自定义 Radius 属性下发。支持针对指定特征的终端（MAC），ASM 在其接入时给交换机下发特定的 Radius 属性，使得支持 Radius 属性的交换机对该终端做出特定动作。
23		多路支持	1.单台准入设备可支持至少 2 路策略路由准入控制。
24			2.单台准入设备可支持至少 2 个镜像口进行准入控制。
25			3.单台准入控制设备支持至少 2 种准入技术组合使用，以增强环境的兼容性。
26		定向引导	1.支持终端入网 IE 浏览器重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持 http 代理及多重重定向引导。
27			2.可根据用户的实际环境自定义非 80 端口的 Web 服务端口号及用户重定向引导。
28			3.支持使用域名进行终端入网重定向，可以实现准入服务器 IP 地址变动的环境下。
29			4.能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。
30			5.具有 Linux、Android 等系统专属客户端，支持认证引导和准入管理。
31	认证管理	证书认证	1.在进行 Ukey 认证时，支持多个合法的根证书。终端用户认证时，自动进行根证书的匹配。
32			2.支持采用软证书认证。
33			3.支持 802.1x 客户端认证时使用 Ukey 进行认证。
34		接入审核	能够针对不同的角色或设备状态有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。
35		认证控制	支持某类（角色）账户只能在指定的时间段、IP 段认证入网。
36		自助账号申请	1.支持用户在认证页面自行进行账号的申请。
37			2.用户可自行提交用户名、密码、姓名、电话、部门、E-Mail 等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分发的困难。
38	来宾管理	来宾角色	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长。
39		二维码认证	已入网员工可以通过扫描来宾终端上二维码，放行来宾用户入网。
40	Linux 操作系统		1. 支持 Kylin，UOS 系统终端，支持 X86，ARM 架构。
41			2.支持杀毒软件（含是否安装、版本和病毒库）的检查和自动修复。
42			3.支持针对系统开启的端口进行检查（支持例外进程调用特定端口）。
43			4.支持必须安装软件、禁止安装软件、必须运行进程、禁止运行进程的检查和修复。

44		5.支持针对电脑未设置开启密码、密码弱口令进行检查，支持自动修改成管理员指定的口令。
45		6.支持域用户检查。
46		7.支持自主签名 Kylin 系统客户端。
47	自定义安全检查	通过检测终端文件、指定文件版本、大小、MD5，注册表的项、注册表值，进程、服务状态进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的对终端进行安全检查和修复。
48	产品证书要求	1.《网络安全专用产品安全监测证书》
49		2.中国国家信息安全产品认证证书
50	厂商授权	▲提供原厂授权函及 5 年售后服务承诺函。

2.3 付款方式说明

1) 合同签订后，支付合同总额的 70%。

2）数据局完成项目终验，支付合同总额的 30%。

3 项目要求

3.1 人员要求

投标人应充分理解本项目的技术及实施复杂度，组建技术服务团队，参与本项目的各类人员应具备相应的技术能力。在服务期内，投标人不得随意更换项目组技术人员，若因特殊情况需要更换服务人员时，需经招标人同意后，方可更换技术能力、资格条件相同或更高的技术人员。

1.项目经理具备 PMP 或网络工程师中级证书或软件测试技能人才证书或 CISAW 证书，且有 5 年以上同类型项目管理经验。

2.建议配备 3 人团队，人员的专业能力应具备信息系统项目管理师证书或信息安全中级工程师证书或 CISP 或 CISAW 等证书。

3.2 实施方案要求

项目实施前须向招标人提交详细技术服务方案，方案应包含但不限于技术人员安排、使用工具和应急响应措施等内容，且方案应完善并符合招标人现场实际情况、针对性及操作性强，经招标人确认后方可实施。

3.3 施工要求

供应商应承担所供产品的安装、调试和配置工作，同时应提供完整的安装调试文档及系统配置文件。响应供应商应全力与用户及其他相关产品供应商配合，保证系统按时、正常地投入运行。响应供应商需保证项目实施的过程不能影响招标人各项业务的正常进行，对危险操作提出风险规避方案和相应的应急预案，并指明可能产生的后果，在征得招标人批准后方可实施。响应供应商需保证所配置的产品有合法的使用权。

提供 7*24 小时应急服务，1 小时响应，2 小时到现场。

3.4 其他要求

供应商具有 ISO 27001 信息安全管理体系认证。

4 对投标单位要求

1.投标单位需提供详细专业的方案设计，包括但不限于功能概要说明；总体拓扑图设计准确；对本项目重点、难点的合理分析；方案设计具有科学性、可操作性；提供设计前后拓扑对比；验收标准和方案科学、可行。

2.投标单位需提供完善科学的实施方案：系统、产品安装部署实施方案具有可操作性；具有详细的项目实施的进度计划；项目管理措施科学合理；培训计划完善科学。

3.投标单位需有专业且富有经验的团队支持。项目经理具有开展项目对应的能力、经验和业绩情况，项目经理具备 PMP 或网络工程师中级证书或软件测试技能人才证书或 CISAW 证书，且有 5 年以上同类型项目管理经验，需提供从业履历、相关证书和劳动合同；主要专业技术管理人员及项目组成员专业配备及数量满足项目需求，团队人员提供相关证书和劳动合同。

4.为确保投标单位产品满足实际使用要求，投标产品技术参数需符合满足招标文件技术参数要求（并更具需要提供产品功能截图及按要求的效果截图）。

5.投标单位需提供优质完善的质量保证和售后服务方案，包括售后服务响应时间、服务计划与内容；应急预案；质量保证和售后服务管理措施。

5 其他

1.投标单位必须在报名时正确填写单位邮箱，在投标文件的投标单位相关资料中也应有单位邮箱。

2.本项目评审要素的所有内容是采购需求的组成部分，各投标单位要对照其内容进行投标响应。

3.本项目预算资金性质为仅面向中小微企业采购，投标单位为大型企业参与投标为无效投标。

4.本项目为服务类项目，所属行业为 软件和信息技术服务业 （用于中小企业声明函），中小微的投标单位须在投标文件中提供中小企业声明函，具体格式如下：

中小企业声明函（服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法（财库〔2020〕46 号）的规定，本公司参加（上海市中西医结合医院）的（信息安全加固建设项目）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（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

（信息安全加固建设项目），属于软件和信息技术服务业； 承建（承接）企业为_____（企业名称），从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于_____（中型企业、小型企业、微型企业）。

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

企业名称（盖章）：

日 期：

注：各行业划型标准

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

第五章　政府采购合同主要条款指引

包 1 合同模板：

[合同中心-合同名称]

合同统一编号： [合同中心-合同编码]

合同内部编号：

合同各方：

甲方：[合同中心-采购单位名称]	乙方：[合同中心-供应商名称]
地址：[合同中心-采购单位所在地]	地址：[合同中心-供应商所在地]
邮政编码：[合同中心-采购人单位邮编]	邮政编码：[合同中心-供应商单位邮编]
电话：[合同中心-采购单位联系人电话]	电话：[合同中心-供应商联系人电话]
传真：[合同中心-采购人单位传真]	传真：[合同中心-供应商单位传真]
联系人：[合同中心-采购单位联系人]	联系人：[合同中心-供应商联系人]

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1．乙方根据本合同的规定向甲方提供以下服务：

1．1 乙方所提供的服务其来源应符合国家的有关规定，服务的内容、要求、服务质量等详见合同附件。

2．合同价格、服务地点和服务期限

2．1 合同价格

本合同价格为[合同中心-合同总价]元整（[合同中心-合同总价大写]）。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2．2 服务地点： 甲方指定。

2．3 服务期限 ：按照采购文件等相关要求。

本服务的服务期限：[合同中心-合同有效期]。

3．质量标准和要求

3．1 乙方所提供的服务的质量标准按照国家标准、行业标准或制造厂家企业标准确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合合同目的的特定标准确定。

3．2 乙方所交付的服务还应符合国家和上海市有关安全、环保、卫生之规定。

4．权利瑕疵担保

4．1 乙方保证对其交付的服务享有合法的权利。

4．2 乙方保证在服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。

4．3 乙方保证其所交付的服务没有侵犯任何第三人的知识产权和商业秘密等权利。

4．4 如甲方使用该服务构成上述侵权的，则由乙方承担全部责任。

5．验收

5．1 服务根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 10 个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

5．2 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。

5．3 如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由乙方单方面进行验收，并将验收报告提交甲方，即

视为验收通过。

5．4 甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

6．保密

6．1 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

7．付款

7．1 本合同以人民币付款（单位：元）。

7．2 本合同款项按照以下方式支付。

7．2．1 付款内容：（分期付款）

7．2．2 付款条件：

[合同中心-支付方式名称]

（1）本合同付款按照上述付款内容和付款次序分期付款或一次性付款。

8．甲方（甲方）的权利义务

8．1、甲方有权在合同规定的范围内享受，对没有达到合同规定的服务质量或标准的服务事项，甲方有权要求乙方在规定的时间内加急提供服务，直至符合要求为止。

8．2 如果乙方无法完成合同规定的服务内容、或者服务无法达到合同规定的服务质量或标准的，造成的无法正常运行，甲方有权邀请第三方提供服务，其支付的服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。

8．3 由于乙方服务质量或延误服务的原因，使甲方有关或设备损坏造成经济损失的，甲方有权要求乙方进行经济赔偿。

8．4 甲方在合同规定的服务期限内有义务为乙方创造服务工作便利，并提供适合的工作环境，协助乙方完成服务工作。

8．5 当或设备发生故障时，甲方应及时告知乙方有关发生故障的相关信息，以便乙方及时分析故障原因，及时采取有效措施排除故障，恢复正常运行。

8． 6 如果甲方因工作需要对原有进行调整，应有义务并通过有效的方式及时通知乙方涉及合同服务范围调整的，应与乙方协商解决。

9．乙方的权利与义务

9．1 乙方根据合同的服务内容和要求及时提供相应的服务，如果甲方在合同服务范围外增加或扩大服务内容的，乙方有权要求甲方支付其相应的费用。

9．2 乙方为了更好地进行服务，满足甲方对服务质量的要求，有权利要求甲方提供合适的工作环境和便利。在进行故障处理紧急服务时，可以要求甲方进行合作配合。

9．3 如果由于甲方的责任而造成服务延误或不能达到服务质量的，乙方不承担违约责任。

9.4 由于因甲方工作人员人为操作失误、或供电等环境不符合合同设备正常工作要求、或其他不可抗力因素造成的设备损毁，乙方不承担赔偿责任。

9．5 乙方保证在服务中，未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任。

9． 6 乙方在履行服务时，发现存在潜在缺陷或故障时，有义务及时与甲方联系，共同落实防范措施，保证正常运行。

9．7 如果乙方确实需要第三方合作才能完成合同规定的服务内容和服务质量的，应事先征得甲方的同意，并由乙方承担第三方提供服务的费用。

9．8 乙方保证在服务中提供更换的部件是全新的、未使用过的。如果或证实服务是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

10．补救措施和索赔

10．1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10．2 在服务期限内，如果乙方对提供服务的缺陷负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）根据服务的质量状况以及甲方所遭受的损失，经过买卖双方商定降低服务的价格。

（2）乙方应在接到甲方通知后七天内，根据合同的规定负责采用符合规定的规格、质量和性能要求的新零件、部件和设备来更换在服务中有缺陷的部分或修补缺陷部分，其费用由乙方负担。

（3）如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述

规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11．履约延误

11．1 乙方应按照合同规定的时间、地点提供服务。

11．2 如乙方无正当理由而拖延服务，甲方有权没收乙方提供的履约保证金，或解除合同并追究乙方的违约责任。

11．3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

12．误期赔偿

12．1 除合同第 13 条规定外，如果乙方没有按照合同规定的时间提供服务，甲方可以应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（天）赔偿延期服务的服务费用的百分之零点五（0.5%）计收，直至提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

13．不可抗力

13．1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13．2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13．3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行合同的协议。

14．履约保证金

14．1 在本合同签署之前，乙方应向甲方提交一笔金额为元人民币的履约保证金。履约保证金应自出具之日起至全部服务按本合同规定验收合格后三十天内有效。在全部

服务按本合同规定验收合格后 15 日内，甲方应一次性将履约保证金无息退还乙方。

14．2 履约保证金可以采用支票或者甲方认可的银行出具的保函。乙方提交履约保证金所需的有关费用均由其自行负担。

14．3 如乙方未能履行本合同规定的任何义务，则甲方有权从履约保证金中得到补偿。履约保证金不足弥补甲方损失的，乙方仍需承担赔偿责任。

15．争端的解决

15.1 合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一切争端。如从协商开始十天内仍不能解决，可以向同级政府采购监管部门提请调解。

15．2 调解不成则提交上海仲裁委员会根据其仲裁规则和程序进行仲裁。

15．3 如仲裁事项不影响合同其它部分的履行，则在仲裁期间，除正在进行仲裁的部分外，本合同的其它部分应继续执行。

16．违约终止合同

16．1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

（1）如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部服务。

（2）如果乙方未能履行合同规定的其它义务。

16．2 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

17．破产终止合同

17．1 如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

18．合同转让和分包

18.1 除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

19．合同生效

19．1 本合同在合同各方签字盖章并且甲方收到乙方提供的履约保证金后生效。

19．2 本合同一式份，甲乙双方各执一份。一份送同级政府采购监管部门备案。

20．合同附件

20．1 本合同附件包括： 招标(采购)文件、投标（响应）文件

20．2 本合同附件与合同具有同等效力。

20．3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

21．合同修改

21．1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

签约各方：

甲方（盖章）： 乙方（盖章）：

法定代表人或授权委托人（签章）： 法定代表人或授权委托人（签章）：

日期：**[合同中心-签订时间]** 日期：[合同中心-签订时间]

合同签订点:网上签约

第六章 投标文件格式附件

附件 1：

信息安全加固建设项目

项目编号：310109000250228185680-09214750（标项　）

资

质

文

件

投标人全称：

地　　址：

时　　间：

1、资质文件目录

（1）投标声明书（格式见附件，含无重大违法记录及不诚信行为声明)；

（2）“信用中国”网站（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）投标人信用查询情况。（以开标当日采购人或采购代理机构或由采购人委托的评标委员会核实的查询结果为准）

（3）法定代表人授权委托书(格式见附件)；

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

（5）联合投标协议书（若需要）；

（6）联合投标授权委托书（若需要）；

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

（8）财务状况，税收及社保缴纳声明函。

（9）前三内经营活动中无重大违法记录和无不诚信行为的声明。

附件 2：

声 明 书

致上海市虹口区政府采购中心：

（投标人名称）系中华人民共和国合法企业，经营地址_____。

我（姓名）系（投标人名称）的法定代表人，我方愿意参加贵方组织的（信息安全加固建设项目）（编号为3101090002502281856 80-09214750）的投标，为此，我方就本次投标有关事项郑重声明如下：

1、我方已详细审查全部招标文件，同意招标文件的各项要求。

2、我方向贵方提交的所有投标文件、资料都是准确的和真实的。

3、若中标，我方将按招标文件规定履行合同责任和义务。

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

5、投标文件自开标日起有效期为 90 天。

6、我方参与本项目前 3 年内的经营活动中没有重大违法记录及不诚信行为；

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

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

法定代表人签名（或签名章）：_____ 日 期：

投标人全称（公章）：

附件 3：

法定代表人授权委托书

上海市虹口区政府采购中心：

我____（姓名）系____（投标人名称）的法定代表人，现授权委托本单位在职职工 _____（姓名）为授权代表，以我方的名义参加项目编号：_____项目名称：_____项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。我方对授权代表的签名事项负全部责任。

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

授权代表无转委托权，特此委托。

授权代表签名：_____ 职务：

授权代表身份证号码：_____电话：

邮箱（方便告知投标单位后续相关事宜）：

法定代表人签名（或签名章）：_____ 职务：

法定代表人身份证号码：_____电话：

投标人全称（公章）：_____ 日 期：_____

附件 4：

联 合 投 标 协 议 书

甲方：

乙方：

（如果有的话，可按甲、乙、丙、丁…序列增加）

各方经协商，就响应 _____组织实施的编号为 号的招标活动联合进行投标之事宜，达成如下协议：

一、各方一致决定，以 _____ 为主办人进行投标，并按照招标文件的规定分别提交资格文件。

二、在本次投标过程中，主办人的法定代表人或授权代理人根据招标文件规定及投标内容而对招标方和采购人所作的任何合法承诺，包括书面澄清及响应等均对联合投标各方产生约束力。如果中标并签订合同，则联合投标各方将共同履行对招标方和采购人所负有的全部义务并就采购合同约定的事项对采购人承担连带责任。

三、联合投标其余各方保证对主办人为响应本次招标而提供的产品和服务提供全部质量保证及售后服务支持。

四、本次联合投标中，甲方承担的工作和义务为:

乙方承担的工作和义务为：

五、有关本次联合投标的其他事宜：

六、本协议提交招标方后，联合投标各方不得以任何形式对上述实质内容进行修改或撤销。

七、本协议签约各方各持一份，并作为投标文件的一部分。

甲方单位：　　（公章）　　乙方单位：　　（公章）

法定代表人：　　（签章）　　法定代表人：　　（签章）

日　期：　　年　　月　　日　　日　期：　　年　　月　　日

附件 5：

联合投标授权委托书

本授权委托书声明：根据 _____与_____签订的《联合投标协议书》的内容，主办人_____的法定代表人_____现授权 _____为联合投标代理人，代理人在投标、开标、评标、合同谈判过程中所签署的一切文件和处理与这有关的一切事务， 联合投标各方均予以认可并遵守。

特此委托。

授权人（签名）：

日期：　　年　月　日

授权代表（签名）：

日期：　　年　月　日

联合体甲方单位：　　（公章）　联合体乙方单位：　　（公章）

法定代表人：　　（签章）　法定代表人：　　（签章）

日　期：　年　月　日　　日　期：　年　月　日

附件 6：

信息安全加固建设项目

项目编号：310109000250228185680-09214750（标项　）

技术及商务文件

投标人全称：

地　　址：

时　　间：

2、技术及商务文件目录

（1）评分对应表（格式见附件，主要用于评委对应评分内容）

（2）投标项目明细清单（含货物、服务等）；

（3）技术响应表（格式见附件）；

（4）项目总体解决方案（可包含且不限于对项目总体要求的理解、项目总体架构及技术解决方案等）；

（5）项目实施计划（可包含且不限于保证工期的施工组织方案及人力资源安排、项目组人员清单等）；

（6）列入政府采购节能环保清单的证明资料（若有）；

（7）商务响应表（格式见附件）；

（8）售后服务计划（可包含且不限于对用户故障的响应、处理、定期巡检、备品备件、常用耗材提供、驻点人员情况等）；

（9）技术培训计划（若有）；

（10）投标人履约能力（可包含且不限于技术力量情况、投标人各项能力证书）；

（11）案例的业绩证明（投标人业绩情况一览表、合同复印件等）；

（12）投标方认为需要的其他文件资料。

附件 7：

评分对应表

投标人全称（公章）：_____ 标项：

评分项目	投标文件对应资料	投标文件页码
对应第三章评分办法及评分标准（报价除外）		
……		

授权代表签名：_____ 日期：

附件 8：

投 标 项 目 明 细 清 单

投标人全称（公章）：_____ 标项：

货物类

序号	货物名称	品牌	规格型号	单位及数量	性能及指标	产地

服务类

序号	服务内容	服务人员数量	工作量

注：在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。

授权代表签名：_____ 日期：

附件 9：

技 术 响 应 表

投标人全称（公章）：_____ 标项：

招标文件要求	投标文件响应	偏离情况

注：投标人应根据投标设备的性能指标、对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

授权代表签名：_____ 日 期：

附件 10：

项目组人员清单

投标人全称（公章）：_____ 标项：

姓名	职务	专业技术资格	证书编号	参加本单位工作时间	劳动合同编号

注：在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行划表填写。

授权代表签名：_____ 日　　期：

附件 11：

商务响应表

投标人全称（公章）：_____ 标项：

项目	招标文件要求	是否响应	投标人的承诺或说明
供货时间(项目工期)及地点			
付款条件			
违约责任及争议解决方式			
项目维护计划			
响应情况			
本地化服务要求			
技术培训			
公司技术力量情况			
经验或业绩要求			
……			

授权代表签名：_____ 日期：

附件 12：

投标人业绩情况一览表

投标人全称（公章）：

采购单位名称	设备或项目名称	采购数量	单价	合同金额（万元）	附件页码		采购单位联系人及联系电话
					合同	验收报告	
备注	提供投标人同类项目合同复印件、用户验收报告（如有）。						

授权代表签名：_____　　时　间：_____

附件 13：

信息安全加固建设项目

项目编号：310109000250228185680-09214750（标项　）

报价文件

投标人全称：

地　　址：

时　　间：

3、报价文件目录

（1）投标报价明细表（见附件 14）；

（2）投标人针对报价需要说明的其他文件和说明（格式自拟）；

（3）中小微企业声明函（见附件 15）；

（4）残疾人福利企业声明函（见附件 16）。

附件 14：

投 标 报 价 明 细 表

投标人全称（公章）：

招标编号及标项：

信息安全加固建设项目包 1

备注	投标人专用邮箱	最终报价(总价、元)

授权代表签名：　　日期：

附件 15：

中小企业声明函（货物）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司（联合体）参加*（单位名称）*的*（项目名称）*采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

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

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

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。

备注：请认真填写中小企业声明函，中小企业声明函填写不全或者填写错误，在审查认定时对投标单位不利，均有可能导致投标废标风险。

中小企业声明函（工程、服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法（财库〔2020〕46 号）的规定，本公司（联合体）参加*（单位名称）*的*（项目名称）*采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

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

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

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。

备注： 请认真填写中小企业声明函，中小企业声明函填写不全或者填写错误，在审查认定时对投标单位不利，均有可能导致投标废标风险。

附件 16：

残疾人福利性单位声明函

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

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日　期：

附件 18：

政府采购活动现场确认声明书

上海市虹口区政府采购中心：

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

一、本单位与采购人之间 □不存在利害关系 □存在下列利害关系_____：

A.投资关系　　B.行政隶属关系　　C.业务指导关系

D.其他可能影响采购公正的利害关系(如有,请如实说明)_____。

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

A.法定代表人或负责人或实际控制人是同一人

B.法定代表人或负责人或实际控制人是夫妻关系

C.法定代表人或负责人或实际控制人是直系血亲关系

D.法定代表人或负责人或实际控制人存在三代以内旁系血亲关系

E.法定代表人或负责人或实际控制人存在近姻亲关系

F.法定代表人或负责人或实际控制人存在股份控制或实际控制关系

G.存在共同直接或间接投资设立子公司、联营企业和合营企业情况

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

I.其他利害关系情况_____。

三、现已清楚知道并严格遵守政府采购法律法规和现场纪律。

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

（供应商代表签名）

年　月　日

财务状况及税收、社会保障资金缴纳情况声明函

我方（供应商名称）符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括：

1. 具有健全的财务会计制度；

2. 有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：

前三年内无重大违法记录及无不诚信行为声明函

我方（供应商名称）承诺在参加本项目政府采购活动前三年内，在经营活动中无重大违法记录及无不诚信行为，我方遵守相关国家法律法规，符合《中华人民共和国政府采购法》及相关法规规章规定的有关政府采购供应商应当具备的条件，符合拟申请项目的供应商相关要求。

我方（供应商名称）已通过（包括但不限于“信用中国”、“中国政府采购网”、“国家企业信用公示系统”等）法定途径，全面自查确认：我方在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。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：