

五角场监狱网络安全等级保护 基础设施加固工程款

项目编号：**31000000250808127674-00264253**

招标代理机构内部项目编号：**H0701-2025-0610**

预算编号：**0025-00010276**

公 开 招 标 文 件

招 标 人：上海市五角场监狱

招标代理机构：上海同济工程咨询有限公司

2025 年 8 月

2025年08月14日

目录

第一部分	招标公告	8
第二部分	投标人须知	12
第三部分	采购需求	24
第四部分	合同条款	53
第五部分	评标办法	60
第六部分	格式附件	67

投标人须知前附表

序号	内容	说明与要求
1	项目名称	五角场监狱网络安全等级保护基础设施加固工程款
2	项目编号	项目编号： 310000000250808127674-00264253 招标代理机构内部项目编号： H0701-2025-0610 预算编号：0025-00010276
3	预算金额/最高限价	预算金额：人民币 139.08 万元，最高限价：人民币 139.08 万元。 注：投标人的投标报价超过预算金额、最高限价的将作无效投标处理。
4	采购资金的支付方式、时间、条件	1. 合同生效后 7 日内乙方向甲方提供合同价款 10%的履约担保，履约担保形式为银行保函； 2. 甲方收到乙方提供的有效的履约保函后 20 个工作日内，甲方向乙方支付合同总价的 30%预付款； 3. 甲方在标的物安装调试完毕并且验收合格后，根据乙方开具的相应金额增值税专用发票，向乙方支付货款总额的 70%货款，同时预付款转为货款。
5	招标概述	根据《中华人民共和国政府采购法》及有关法律、法规和规章规定，本项目已具备采购条件，依法进行招标采购。
6	招标方式	公开招标
7	招标人	单位名称：上海市五角场监狱 地 址：上海市嫩江路 199 号 联 系 人：李宇飞 电 话：021-65560609
8	招标代理机构	单位名称：上海同济工程咨询有限公司 地 址：上海市杨浦区四平路 1398 号 B 座 18 楼 邮 编：200092 联 系 人：陈敏铭 电 话：021-33627343 邮 箱：chenmm@tongji-ec.com.cn
9	包件	<input checked="" type="checkbox"/> 适用 <input type="checkbox"/> 不适用 有关包件的所有条款均不适用本项目
10	招标内容	五角场监狱目前具备互联网与政务外网两个网络，并且与第三方签订了相关网络运维合同，确保网络正常运行。目前因存在网络安全隐患，监狱制定了相应的整改方案，一方面通过加强日常巡检，强化基础的网络安全防范措施来确保网络安全，另一方面根据等级保护三级测评的要求编制预算，通过项目建设来消除安全隐患。 (具体内容详见招标文件第三部分一采购需求)

11	是否专门面向中小企业采购	<input type="checkbox"/> 是，本项目专门面向中小微企业采购，所有供应商不享受价格分优惠政策（详见第五部分评标办法） <input checked="" type="checkbox"/> 否， 本项目面向大、中、小、微型企业，事业法人等各类供应商采购 ，小微企业享受价格分优惠政策。（详见第五部分 评标办法）
12	采购标的对应的中小企业划分标准所属行业	工业

13	是否采购进口产品	<input checked="" type="checkbox"/> 不接受 <input type="checkbox"/> 接受，进口产品是指通过中国海关报关验放进入中国境内且产自境外的产品。
14	交付时间	项目合同正式签署后 1 个月内完成。
15	交付地点	上海市，招标人指定地点
16	报价货币	投标文件的报价采用人民币报价。
17	投标人资格要求	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：本次招标若符合政府强制采购节能产品、鼓励环保产品、扶持福利企业、促进残疾人就业、促进中小企业发展、支持监狱和戒毒企业等政策，将落实相关政策。 3.本项目的特定资格要求： 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； 3) 本项目面向大、中、小、微型企业，事业法人等各类供应商采购 ； 4) 本项目不接受联合体投标，本项目不得转让，不得分包。
18	是否接受联合投标	<input checked="" type="checkbox"/> 不接受 <input type="checkbox"/> 接受
19	公告发布媒体	上海政府采购网（ http://www.zfcg.sh.gov.cn/ ）
20	招标文件下载时间、下载地址及标书费支付地点	招标文件下载时间 2025-08-14 至 2025-08-21 ，每天上午 00:00:00~12:00:00 ，下午 12:00:00~23:59:59 （北京时间，法定节假日除外） 招标文件下载地址：上海政府采购网（ http://www.zfcg.sh.gov.cn ） 下载招标文件后，请与招标代理机构联系，获取图纸。
21	现场踏勘	<input checked="" type="checkbox"/> 不组织 <input type="checkbox"/> 组织
22	提问方式	书面提问（须加盖投标人公章）

23	招标答疑会 时间、地点	时间：如有，另行书面通知 地点：上海市杨浦区四平路 1398 号 B 座 1810B 会议室
24	领取补充招标文件时 间、地点	时间：另行安排（如有） 地点：上海市杨浦区四平路 1398 号 B 座 1810B 会议室（如有，将以书面形式统一发放所有投标人）
25	接收质疑的方式及联 系方式	投标人应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，质 疑函应以书面形式递交至招标代理公司（须由法定代表人、主要负责 人 或其授权代表签字或者盖章，并加盖投标人公章） 联系方式详见本表第 8 项
26	投标有效期	投标截止之日起 <u>90</u> 日历日
27	投标保证金	投标保证金金额： 人民币贰万柒仟元整 保证金递交截止时间：同投标截止时间，以保证金实际到账为准。 递交地点：上海市杨浦区四平路 1398 号 B 座 1810B 会议室 递交方式：转账、汇款、支票或代理单位接受的其他非现金方式。 为确保保证金在递交截止时间前到账，通过转账、汇款、支票方式递交 保证金的投标人，应在投标截止时间前完成保证金支付，保证金有效 期 应与投标有效期一致。 投标保证金汇款账号： 户名：“上海同济工程咨询有限公司 ” 开户银行：交通银行上海同济支行 帐号：310066344010141052919 注：银行转账时“备注栏”须注明项目名称及资金用途，例：“ 五角场监 狱网络安全等级保护基础设施加固工程款 ”，投标保证金”
28	投标截止时间	2025-09-05 10:00:00
29	投标文件提交截止 时间、地点	投标文件提交截止时间：同投标截止时间 投标文件提交地点：http://www.zfcg.sh.gov.cn
30	开标会 时间、地点	开标会时间：同投标截止时间 开标会地点：上海市杨浦区四平路 1398 号 B 座 1810B 会议室 届时请投标人代表持投标时所使用的数字证书（CA 证书）和可以无线 上网的笔记本电脑出席开标仪式。 注册地在上海的响应单位：投标人代表携带专用信用报告（加盖公章， 申请步骤：法人随申办--合同一码通--申请报告） 注册地非上海的响应单位：投标人代表携带：“信用中国”信用报告（加 盖公章）

31	投标文件的组成	<p>投标文件应包括下列部分：</p> <ol style="list-style-type: none"> 1) 投标书（附件 1）； 2) 法定代表人等资格证明书（附件 2）； 3) 授权委托书（附件 3）； 4) 开标一览表（附件 4）； 5) 投标报价明细表（附件 5）； 6) 货物报告（附件 6）； 7) 资格证明文件（附件 7）； 8) 中小企业声明函（附件 8）； 9) 残疾人福利性单位声明函(如有)（附件 9）； 10) 供应商书面声明； 11) 投标人认为需加以说明的其他内容。
32	投标文件格式	<p>投标人应按招标文件中提供的投标文件格式，填写投标书、法定代表人等资格证明书、授权委托书、开标一览表、投标报价明细表、偏离表、资格证明文件、中小企业声明函、残疾人福利性单位声明函（如有）等（详见第六部分 格式附件）。</p>
33	投标文件份数	<p>提供投标文件三份（纸质文件）并密封，须与上传的电子投标文件内容一致，如果上传的投标文件与纸质投标文件存在差异，以上传的电子投标文件为准，纸质文件仅作备查使用,不作为评审依据。</p>
34	评标方法	<p>综合评分法</p>
35	如发生此列情况之一，投标人的投标将被拒绝	<ol style="list-style-type: none"> 1) 未按规定获取招标文件的； 2) 投标人名称与报名时不一致的； 3) 未在投标截止时间前在电子平台上提交投标文件的。
36	中标服务费支付	<p>本项目中标单位在收到中标通知书时，按以下标准一次性向招标代理机构支付服务费：</p> <p>参照《招标代理服务收费管理暂行办法》（计价格[2002]1980号）、《关于降低部分建设项目收费标准规范收费行为等有关问题的通知》（发改价格[2011]534号）下浮 20%向招标代理机构支付招标代理服务费。</p>
37	政府采购政策落实	<p>本次招标若符合政府强制采购节能产品、鼓励环保产品、扶持福利企业、促进残疾人就业、促进中小微企业发展、支持监狱和戒毒企业等政策，将落实相关政策。</p>
38	其他	<ol style="list-style-type: none"> (1) 投标人必须在网上投标系统中录入缴纳保证金信息，并把必填项维护完成后，点击“提交”。 (2) 供应商在投标（响应）文件加密上传后，应及时查看签收情况。 (3) 开标（投标截止时间）后，招标代理机构将在信用中国（www.creditchina.gov.cn）、中国政府采购网中“政府采购严重违法失信行为信息记录”（www.ccgp.gov.cn/cr/list）对参与开标会的投标人进行信息查询、截图留存，确认投标人投标截止时间前三年，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等，若存在上述情况将拒绝其参与政府采购活动。

第一部分 招标公告

第一部分 招标公告

项目概况

五角场监狱网络安全等级保护基础设施加固工程款的潜在投标人应在上海市政府采购网获取招标文件，并于 **2025-09-05 10:00:00**（北京时间）前递交投标文件。

一、项目基本情况

项目编号：

项目名称：五角场监狱网络安全等级保护基础设施加固工程款

预算编号：0025-00010276

预算金额（元）：1390800.00 元（国库资金：1390800.00 元；自筹资金：0 元）

最高限价（元）：包 1-1390800.00 元

采购需求：

包名称：五角场监狱网络安全等级保护基础设施加固工程款

数量：1

预算金额：1390800.00 元

简要规格描述或项目基本概况介绍、用途：**五角场监狱目前具备互联网与政务外网两个网络，并且与第三方签订了相关网络运维合同，确保网络正常运行。目前因存在网络安全隐患，监狱制定了相应的整改方案，一方面通过加强日常巡检，强化基础的网络安全防范措施来确保网络安全，另一方面根据等级保护三级测评的要求编制预算，通过项目建设来消除安全隐患。**

（具体内容详见招标文件第三部分—采购需求）

合同履行期限：合同签订后1个月内完成。

本项目**不允许**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：本次招标若符合政府强制采购节能产品、鼓励环保产品、扶持福利企业、促进残疾人就业、促进中小企业发展、支持监狱和戒毒企业等政策，将落实相关政策。

3.本项目的特定资格要求：

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；

3) 本项目面向大、中、小、微型企业，事业法人等各类供应商采购；

4) 本项目不接受联合体投标，本项目不得转让，不得分包。

三、获取招标文件

时间：**2025-08-14至2025-08-21**，每天上午**00:00:00~12:00:00**，下午**12:00:00~23:59:59**

（北京时间，法定节假日除外） 地点：上海市政府采购网

方式：网上获取

售价（元）：0

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：**2025-09-05 10:00:00**（北京时间）

投标地点：本次投标采用网上投标，投标人应根据有关规定和方法，在“上海政府采购网”（<http://www.zfcg.sh.gov.cn>）电子招投标系统提交。

开标时间**2025-09-05 10:00:00**（北京时间）

开标地点：上海市杨浦区四平路1398号B座1810B会议室。

届时请投标人代表持投标时所使用的数字证书（CA 证书）和可以无线上网的笔记本电脑参加开标。

注册地在上海的响应单位：投标人代表携带专用信用报告（加盖公章，申请步骤：法人随申办--合同一码通--申请报告）

注册地非上海的响应单位：投标人代表携带“信用中国”信用报告（加盖公章）

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

《上海政府采购实施办法》（上海市人民政府令第 65 号）、《上海市电子政府采购管理暂行办法》（沪采[2012]22 号）及其他相关文件的规定，本项目通过上海政府采购网/采购云平台（<http://www.zfcg.sh.gov.cn>）实行全过程电子采购，投标人的报价应当符合有

关文件和上海政府采购云平台的要求。上海政府采购网/采购云平台（<http://www.zfcg.sh.gov.cn>）由上海市财政局建设和维护。潜在投标人的报价可以按照《上海市政府采购云平台供应商-项目采购操作手册》中的内容和操作要求实施。

七、对本次招标提出询问，请按以下方式联系。

1.采购人信息

名称：上海市五角场监狱

地址：上海市嫩江路199号

联系方式：李宇飞 021-65560609

2.采购代理机构信息

名称：上海同济工程咨询有限公司

地址：上海市杨浦区四平路1398号B座18楼

联系方式：陈敏铭 021-33627343

3.项目联系方式

项目联系人：陈敏铭

电话：021-33627343

第二部分 投标人须知

第二部分 投标人须知

1. 概述

1.1 本招标文件仅适用于《招标公告》和《投标人须知》前附表中所述采购项目的招标采购。

1.2 招标文件的解释权属于《招标公告》和《投标人须知》前附表中所述的招标人、招标代理机构。

1.3 参与招标投标活动的所有各方，对在参与招标投标过程中获悉的国家、商业和技术秘密以及其他依法应当保密的内容，均负有保密义务，违者应对由此造成的后果承担全部法律责任。

2. 定义

2.1“招标项目”系指招标人在招标文件里描述的所需采购的货物/服务。

2.2 包括一切设备、产品、机械、仪器仪表、备品备件、工具、手册等有关技术资料 and 原材料等，以及其所提供货物相关的运输、就位、安装、调试、技术协助、校准、培训、技术指导以及其他类似的义务。

2.3“服务”系指招标文件规定投标人承担的各类专业服务，包含但不限于产品设计开发、产品交付、安装调试、质量检测、技术指导、售后服务、专业劳务服务和其他类似的义务。

2.4“招标人”系指《投标人须知》前附表中所述的组织。

2.5“投标人”系指根据规定可以下载招标文件、并向招标人提交投标文件的供应商。但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。为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

2.6“中标人”系指中标的投标人。

2.7“买方”系指通过上海政府采购网采购货物或服务的本市各级国家机关、事业单位、团体组织。

2.8 “卖方”系指中标并向招标人提供货物/服务的投标人。

3. 合格的投标人

3.1 符合《招标公告》和《投标人须知》前附表中规定的合格投标人所必须具备的资质条件和特定条件。特定条件是指对投标人的财务要求、诚信要求以及其他要求等。

3.2 《招标公告》和《投标人须知》前附表规定接受联合体投标的，除应符合本章第 3.1 项要求外，还应遵守以下规定：

- (1) 联合体各方应提供已签订的联合协议书，明确主投标人和各方权利义务；
- (2) 由同一专业的投标人组成的联合体，按照资质等级较低的投标人确定联合体资质等级；
- (3) 招标人根据招标项目的特殊要求规定投标人特定条件的，联合体各方中至少应当有一方符合招标采购规定的特定条件。
- (4) 联合体各方不得再以自己名义单独或参加其他联合体在同一招标采购项目中投标。

3.3 投标人应遵守国家有关的法律、法规和管理办法。

4. 投标费用

4.1 无论投标过程中的做法和结果如何，投标人自行承担所有与参加投标有关的全部费用，招标人在任何情况下均无义务和责任承担这些费用。

招标文件

5. 招标文件的组成

5.1 招标文件用以阐明所需货物/服务、招标投标程序和合同条款。招标文件由下述部分组成：

- (1) 投标人须知前附表
- (2) 招标公告；
- (3) 投标人须知；
- (4) 采购需求；
- (5) 合同条款；
- (6) 评标办法；
- (7) 格式附件。

5.2 除非有特殊要求，招标文件不单独提供招标货物或提供服务所在地点的自然环境、气候条件、公用设施等情况，投标人被视为熟悉上述与履行合同有关的一切情况。

5.3 投标人应认真阅读招标文件中所有的事项、格式、条款和规范等要求。如果没有按照招标文件要求提交全部资料，或者投标文件没有对招标文件作出实质性响应，该投标有可能被拒绝或评定为无效投标，其风险应由投标人自行承担。

6.招标文件的澄清

6.1 投标人对招标文件如有疑点，可要求澄清，应按招标文件前附表规定通知招标代理机构或招标人。对在网上投标截止期以前收到的澄清要求，招标人或招标代理机构将以召开答疑会或者以网上下载的形式予以答复，答复中包括所问问题，但不包括问题的来源。招标人或招标代理机构将通知所有可以下载招标文件的投标人参加答疑会或者在网上下载。

7.招标文件的修改

7.1 在投标截止日期前的任何时候，无论出于何种原因，招标人可主动或在解答投标人提出的问题时对招标文件进行修改。

7.2 招标文件的修改、澄清将在电子平台上进行发布，投标人应主动在电子平台上及时获取相关信息并确认，否则由此产生的风险由投标人自行承担。

7.3 为使投标人编写投标书时有充分时间对招标文件的修改部分进行研究，招标人可以酌情延长网上投标截止日期。

投标文件的编写

8.编写要求

8.1 投标人应仔细阅读招标文件的所有内容及上海政府采购网网上投标操作指南，按招标文件的要求及上海政府采购网网上投标相关要求提供投标文件，以使其投标对招标文件的实质性要求作出完全响应。

8.2 投标人须在上海政府采购网下载、安装“上海市政府采购信息管理平台投标工具”，在该工具基础上完成投标文件录入、投标、投标文件加密等内容的操作。

9.投标的语言及计量单位

9.1 投标文件、投标交换的文件和来往信件，应以简体中文书写。

9.2 除在招标文件中另有规定外，计量单位应使用中华人民共和国法定计量单位。

10.投标文件的组成

10.1 投标文件应包括本文件前附表规定内容及网上投标系统中规定内容。

11.投标文件格式

11.1 投标人应按照招标文件或网上投标系统中提供的格式在网上完整地填写投标报价表以及相关投标内容。

12.投标报价

12.1 投标人应按招标文件中所附格式填写投标单价和投标总价。如果单价与总价不符，以单价为准。招标人不接受有任何选择的报价。

12.2 开标一览表是为了便于招标人开标，开标一览表内容在开标时将当众唱出。开标一览表的投标总价应与投标报价明细表的投标总价一致，不一致时以开标一览表内容为准。网上投标的投标内容均以网上投标系统开标时的开标记录内容为准。

12.3 最低投标报价不能作为中标的唯一保证。

12.4 投标人应在投标报价明细表上标明对本项目投标内容的单价和总价。

12.4.1 总价中不得包含招标文件要求以外的内容，否则评标时不予核减。

12.4.2 总价中不得缺漏招标文件所要求的内容，否则评标时将其他有效投标人中该项缺漏内容的最高投标报价计入其评标总价。

12.4.3 若缺漏招标文件内容的投标人最终成交，缺漏项仍然为投标人的合同范围，并且不得增加合同价。但缺漏招标文件所要求的内容达到一定比例或缺漏某些关键内容的，评标委员会有权认定为非实质性响应投标。

13.投标货币：投标文件的报价采用前附表所述货币进行报价。

14.投标人资格的证明文件

14.1 投标人必须按招标文件及网上投标系统的要求提交证明其有资格进行投标和有能力和履行合同的文件，作为投标文件的一部分。

14.1.1 投标人具有履行合同所需的财务、技术、开发等项目实施能力；

14.1.2 投标人应有能力履行招标文件文件中合同条款和货物/服务要求规定的由卖方履行的开发、供货、安装、调试、保修（应提供使用售后服务承诺）和其他专业技术服务的义务。

15.投标货物/服务符合招标文件规定的技术响应文件

15.1 投标人必须依据招标文件中招标项目要求及货物/服务要求，提交证明其拟供货物/服务符合招标文件规定的技术响应文件，作为投标文件的一部分。

15.2 上述文件可以是文字资料、图纸和数据。

16.投标保证金

16.1 本次投标保证金额：详见前附表

16.2 投标保证金用于保护本次招标免受因投标人的行为而引起的风险。

16.3 投标保证金应以转账、汇款、支票或招标代理机构同意接受的其他非现金方式递交，投标人应在招标文件规定的时间内递交投标保证金，并确保已如数到账。

16.4 保证金有效期应与投标有效期一致。

16.5 投标人必须在网上投标系统中录入缴纳保证金信息，并把必填项维护完成后，点击“提交”。

16.6 未中标人的投标保证金，将按投标人须知 28.4 款予以无息退还。

16.7 中标人的投标保证金，在合同签订之日起 5 个工作日内予以无息退还。

16.8 投标人在投标截止时间前撤回已提交的投标文件的，自收到投标人书面撤回通知之日起 5 个工作日内，退还已收取的投标保证金，但因投标人自身原因导致无法及时退还的除外。

16.9 发生以下情况投标保证金将被没收：

16.9.1 开标后投标人在投标有效期内撤回投标；

16.9.2 中标人未能按招标文件规定签订合同。

17.投标有效期

17.1 本项目投标有效期详见前附表。

17.2 特殊情况下，招标人可于投标有效期满之前要求投标人同意延长有效期，要求与答复均应为书面形式。投标人可以拒绝上述要求而其投标保证金不被没收。对于同意该要求的投标人，既不要求也不允许其修改投标文件，但将要求其相应延长投标保证金的有效期，有关退还和没收投标保证金的规定在投标有效期的延长期内继续有效。

18.投标文件的签署及规定

18.1 投标文件须按招标文件及电子招投标系统要求进行签章。

18.2 投标文件不得表达不清、未按要求填写或可能导致非唯一理解。

投标文件的递交

19.投标文件的录入、响应项制作及投标文件加密及纸质版投标文件密封

19.1 投标人在投标文件制作完成后须登录“上海市政府采购信息管理平台投标工具”客户端，将投标文件逐项录入。

19.2 投标文件上传完毕后须逐项完成响应项目内容的填写、资料上传等要求。

19.3 投标人完成投标文件录入、响应项制作后，可对投标文件进行加密，加密成功后即可对标书进行上传，上传成功后点击“回执确认”输入 CA 密码，投标人须自行对上传情况进行确认。

19.4 若供应商在响应截止时间前需要撤回已提交的响应文件，则须向招标人或采购代理机构提供书面撤回通知函（须加盖供应商单位公章及被授权人签字），招标人或采购代理机构在收到书面撤回通知函后在上海政府采购网电子平台进行撤回操作。

19.5 供应商在投标（响应）文件加密上传后，应及时查看签收情况，并打印签收回执。未签收的投标（响应）文件视为投标(响应)未完成。

20.提交投标文件的截止时间

20.1 所有投标文件须按电子平台规定时间上传、解密投标文件。

20.2 网上投标截止时间前，投标人应充分考虑到期间网上投标会发生的故障和风险。对发生的任何故障和风险造成投标人投标内容不一致或利益受损或投标失败的，招标人、招标代理机构不承担任何责任。

20.3 出现第 7.3 款因招标文件的修改推迟投标截止日期时，则按招标代理机构修改通知规定的时间提交。

21.迟交的投标文件

21.1 在网上投标截止时间后提交的任何投标，将被拒绝。

22.投标文件的修改和撤销

22.1 投标人在投标截止时间前，可以修改或撤回其投标。投标截止后，投标人不得修改或撤回其投标。

22.2 投标人不得在开标时间起至投标文件有效期期满前撤销投标文件。

开标和评标

23.开标

23.1 招标代理机构将在招标文件中规定的日期、时间和地点组织开标，届时请投标人代表持投标时所使用的数字证书（CA 证书）和可以无线上网的笔记本电脑出席开标仪式。对于价格折扣，只有在开标时公布的评标时才能考虑。

23.2 投标人须在电子平台规定的时间登陆上海政府采购网网上招投标系统，所有上传投标文件的供应商应登录电子平台参加开标程序，并均应按照电子平台的规定进行流程操作完成签到、唱标、结果确认签章等每一步骤，其中签到和解密的操作时长分别为半小时，投标人应在规定时间内完成上述签到或解密操作，逾期未完成签到或解密的投标人，其投标将作无效标处理。因系统原因导致投标人无法在上述要求时间内完成签到或解密的除外。如电子采购平台开标程序有变化的，以最新的操作程序为准。

23.4 投标文件解密后，电子采购平台根据各投标人填写的《开标一览表》内容自动汇总生成《开标记录表》。投标人应及时使用数字证书对《开标记录表》内容进行签名确认，投标人因自身原因未作出确认的视为其确认《开标记录表》内容。

24.评标委员会

24.1 招标人、招标代理机构将根据招标货物/服务的特点，依法组建评标委员会，其成员由技术、经济等方面的专家和招标人的代表组成，其中外聘专家人数不少于评标委员会总人数的 2/3。评标委员会对投标文件进行审查、质疑、评估和比较。

24.2 评标期间，如有需要投标人应派代表参加询标。

25.对投标文件的审查和响应性的确定

25.1 在对投标文件进行详细评估之前，评标委员会将依据投标人提供的证明文件审查投标人的技术、开发等项目实施能力。

25.2 评标委员会将确定投标是否对招标文件的实质性要求做出完全响应，而没有重大偏离。完全响应的投标是指投标符合招标文件的所有条款、条件和规定，且没有重大偏离或保留。重大偏离或保留系指影响到招标文件规定的采购范围、质量和进度，或限制了买方的权力和投标人的义务的规定，而纠正这些偏离将影响到其他提交实质性响应投标的投标人的公平竞争地位。

25.3 评标委员会判断投标文件的响应性仅基于投标文件本身而不靠外部证据。

25.4 评标委员会将确定非实质性响应的投标为无效投标，投标人不能通过修正或撤销不符之处而使其投标成为实质性响应的投标。

25.5 在得到评标委员会的认可后，投标人可以修改投标中不构成重大偏离的微小的、非正规的、不一致或不规则细微偏离，但这些补正不能对其他供应商造成不公平的结果。

25.6 评标委员会对确定为实质性响应的投标文件进行审核，如有计算错误或其它错误，须按如下原则进行调整：

(1) 开标一览表内容与报价明细表金额及投标文件其他部分内容不一致的，以开标一览表内容为准；

(2) 投标文件中数字表示的金额和文字表示的金额不一致时，应以文字表示的金额为准；

(3) 单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

(4) 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；

(5) 投标总价中不得包含招标文件要求以外的内容，否则，在评审时不予核减；

(6) 如有计算错误，评标委员会有权根据具体情况按对其最不利原则调整；

(7) 同时出现两种以上不一致的，按照前款规定的顺序修正。投标人修正后的报价应当采用书面形式，并加盖公章，或者由法定代表人或委派的授权代表签字确认后产生约束力，投标人不确认的，其投标无效。

25.7 如发生下列情况之一，投标人的投标将被拒绝：

1) 未按规定获取招标文件的；

2) 投标人名称与报名时不一致的；

3) 未在投标截止时间前在电子平台上提交投标文件的。

25.8 评标委员会在进行符合性审查时，对属于下列情况之一的投标文件（以上传的电子投标文件为准），将作无效投标处理：

(1) 投标文件未满足招标文件规定的签字、盖章要求的；

(2) 投标人对投标文件进行修改后，未在修改处由投标人法定代表人或法定代表人委托的投标代理人签字或盖章的；

(3) 明显不符合招标文件采购需求的；

(4) 同一投标人提交两个以上不同的投标文件或者投标报价，但招标文件要求提交备选投标的除外；

(5) 投标有效期少于招标文件规定有效期的投标文件；

- (6) 投标文件附有招标人不能接受的条件的；
- (7) 不接受本须知 25.6 规定调整投标文件中计算错误或其它错误的；
- (8) 未按前附表要求提交保证金的；
- (9) 不满足招标文件中“★”号条款的；
- (10) 不符合招标文件规定的其他实质性要求的；
- (11) 有下列情形之一的，视为投标人串通投标的：
 - a、不同投标人的投标文件由同一单位或者个人编制；
 - b、不同投标人委托同一单位或者个人办理投标事宜；
 - c、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；
 - d、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；
 - e、不同投标人的投标文件相互混装；
 - f、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。

25.9 澄清：评标委员会对投标文件中含义不明确、同类问题表述不一致或者有明显文字错误的内 容，可以书面形式（由评标委员会专家签字）要求投标人在规定的时间内作出必要的澄清、说明或者补正，投标人的澄清、说明或者补正应当采用书面形式，由其法定代表人或委派的授权代理人签字，并不得超出投标文件的范围或者改变投标文件的实质性内 容。投标人拒不进行澄清、说明、补正的，或者不能在规定时间内作出书面澄清、说明、补正的，评标委员会有权否决其投标。

25.10 根据相关法律法规的规定，出现下列情形之一的，评标委员会有权否决所有投标人的 投标或取 消采购活动：

- (1) 符合条件的投标人或对招标文件作实质性响应的投标人不足三家的（含网上招投标系统供应商解密阶段，解密成功的单位少于三家的）；
- (2) 出现影响采购公正的违法、违规行为的；
- (3) 因重大变故，招标采购任务取消的；
- (4) 投标人的报价均超过了预算金额，招标人不能支付的；
- (5) 评标委员会经评审认为所有投标文件都不符合招标文件要求的；
- (6) 多家投标人提供相同品牌产品投标，按一家投标人计算，计算后投标人少于三家的。

26. 评标原则及方法

26.1 对所有投标人的投标评估，都采用相同的程序和标准。

26.2 评标严格按照招标文件的要求和条件进行。

26.3 本次评标采用综合评分法，评标细则详见招标文件“第五部分评标办法”。

定标

27.定标准则

27.1 合同将授予其投标符合招标文件要求，并能圆满地履行合同的、对买方最为有利的投标人。

27.2 不能保证最低报价的投标最终中标。

28.中标通知

28.1 招标人将通过“上海市政府采购网”发布中标公告，中标结果公布后，招标代理机构将发出《中标通知书》、《评标结果通知》，投标人可至招标代理机构现场领取。《中标通知书》、《评标结果通知》一经发出即发生法律效力。

28.2 《中标通知书》将作为采购期限内签订合同的依据。

28.3 中标人与招标人签订合同之日起 5 个工作日内，招标代理机构无息退还中标人的投标保证金。

28.4 自中标通知书发出之日起 5 个工作日内，招标代理机构向未中标的投标人无息退还其投标保证金。

29.签订合同

29.1 中标人收到《中标通知书》后，按指定的时间、地点与招标人签订采购合同。

29.2 招标文件、中标人的投标文件及其澄清文件等，均为签订采购合同的依据。

29.3 中标或者成交供应商拒绝与招标人签订合同的，招标人可以按照评审报告推荐的中标或者成交候选人名单排序，确定下一候选人为中标或者成交供应商，也可以重新开展政府采购活动。

质疑

30. 投标人质疑

30.1 投标人应根据《政府采购质疑和投诉办法》（中华人民共和国财政部令第 94 号）提出质疑。

30.2 投标人应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，质疑函应以书面形式递交至招标代理公司（须由法定代表人、主要负责人或委派的授权代表签字或者盖章，并加盖投标人公章）。

30.3 联系方式详见招标文件投标人须知前附表第 8 项。

其它

31.投标注意事项

31.1 招标人无义务向未中标人解释未中标理由。

31.2 本招标文件解释权属招标人和招标代理机构。

31.3 若发现供应商有不良行为的，将记录在案并上报有关部门。

31.4 投标人应自行办理网上招投标系统所需的相关手续、证书或设备等，并自行完成系统操作的学习（详见上海政府采购网“操作须知”），投标人须自行承担因系统操作、网络设备情况导致的任何问题或风险，包括造成的利益损失、投标失败等，招标人及招标代理机构不承担任何责任。

第三部分 采购需求

第三部分 采购需求

第1章 项目概述及总体要求

1.1 项目概述

五角场监狱目前的互联网、政务外网均未达到等级保护三级防护水平，并且经监狱管理局授权的某安全团队对我监进行了网络安全专项检查，发现存在：1、业务系统存在严重漏洞；2、主机安全防护措施失效；3、安全日志审计工作未落实；4、缺乏安全运维管理措施；5、未禁止无线网络的使用；6、电脑终端入网策略不完善等6个突出问题。以及网络安全管理制度存在缺失、缺乏安全基线标准及核查机制、未定期开展应用漏洞检测、缺乏网络安全专项培训及考核机制等4个一般问题。为确保监狱网络安全，急需对上述问题进行整改，并达到等级保护三级防护水平。

1.2 项目建设依据

《五角场监狱网络安全专项检查风险问题报告》

《上海市司法局网络安全和科技信息化领导小组办公室整改通知单》

《中华人民共和国计算机信息系统安全保护条例》（国务院令 147 号）第九条明确规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。

1.3 建设原则

本项目建设方案必须从监狱的结构和布局出发，结合监狱的实际管理、使用需要，以及国内外技术发展的现状和方向，参考兄弟省市监狱、拘留所、戒毒所技术建设的经验进行。本项目建设应遵循以下原则：

➤ 标准化和规范化原则

严格遵循国家有关法律法规和技术规范，从业务、技术、运行管理等方面整体建设，充分体现标准化和规范化。

➤ 安全性原则

充分考虑数据和网络的安全性，按照特殊场所保密要求，利用软、硬件手段进行安全防护。

➤ 可靠性原则

尽可能在有限的投资条件下，从系统结构、网络结构、技术措施、设备选型以及厂商的技术服务和维修响应能力等方面综合考虑，要求采用市面上成熟的成熟产品和配套方案，并提供详细的备品备件方案，最大限度的保障系统运行的稳定性。

➤ 经济性原则

本系统建设应当充分利用已有资源，避免重复工作，力求减少浪费。

➤ 开放性原则

基于业务未来发展的需要，充分考虑系统的兼容性以及可扩充、扩展能力，能够方便进行升级和更新。

➤ 易操作、维护原则

系统设备要具备多种控制方式，一旦出现故障，能够减轻对整个系统的影响，同时充分考虑减少系统维护时间和降低复杂程度。

1.4 建设内容

(1) 基础条件

五角场监狱目前具备互联网与政务外网两个网络，并且与第三方签订了相关网络运维合同，确保网络正常运行。目前因存在网络安全隐患，监狱制定了相应的整改方案，一方面通过加强日常巡检，强化基础的网络安全防范措施来确保网络安全，另一方面根据等级保护三级测评的要求编制预算，通过项目建设来消除安全隐患。

(2) 前期工作

按照上海市监狱管理局信息化建设项目管理工作规定、上海市五角场监狱信息化建设项目管理工作实施细则（试行）等制度要求，对项目进行绩效前评价，重点对项目的必要性、合理性、可行性以及预算进行审核。并且监狱成立项目管理小组对现场进行前期勘察，按照实际情况制定项目实施方案。确保项目规范、有序实施。

网络安全等级保护安全建设工作是网络安全等级保护制度的核心和落脚点。等级保护建设的目标是在网络定级工作基础上深入开展网络安全等级保护安全建设整改工作，使网络系统可以按照保护等级的要求进行设计、规划和实施，并且达到相应等级的基本保护水平和保护能力。

依据网络安全等级保护相关标准和指导意见，对上海市五角场监狱单位的网络安全等级保护基础设施加固项目互联网与政务外网系统按照“整体保护、综合防控”的原则进行安全建设案的设计，按照等级保护三级的要求进行安全建设规划，对安全建设进行统一规划和设备选型，实现案合理、组网简单、扩容灵活、标准统一、经济适用的建设目标。

依据网络安全等级保护三级标准，按照“统一规划、重点明确、合理建设”的基本原则，在安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等面进行安全规划与建设，确保“网络建设合规、安全防护到位”。

最终使互联网与政务外网系统达到安全等级保护第三级要求。经过建设后，使整个网络形成一套完善的安全防护体系，提升整体网络安全防护能力。

对于三级网络，经过安全建设整改，网络在统一的安全保护策略下要具有抵御大规模、较强恶意攻击的能力，抵抗较为重的自然灾害的能力，以及防计算机病毒和恶意代码危害的能力；具有检测、发现、报警及记录入侵行为的能力；具有对安全事件进行响应处置，并能够追踪安全责任的能力；遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保障性要求高的网络，应该能够快速恢复正常运行状态；具有对网络资源、用户、安全机制等进行集中控管的能力。

第2章 项目建设内容详述

2.1 互联网及政务外网等保三级

2.1.1 互联网及政务外网等保三级设备配置要求

2.1.1.1 系统概述

政务外网及互联网系统需满足等保三级的安全防护要求：

1. 系统定位

政务外网：面向政府部门内部业务协同的非涉密网络，承载跨部门、跨层级的数据交换和业务应用。

互联网区域：提供对外公共服务入口（如移动监控系统）。

2. 架构设计

分层分区：政务外网与互联网作为独立的网络区域，分别在系统内划分为外网接入区、核心交换区、业务应用区、安全管理区、安全办公区等，各区域间通过防火墙策略隔离。

冗余设计：核心网络设备、链路、服务器需冗余部署，保障高可用性。

安全边界：明确互联网与政务外网的边界，部署下一代防火墙、WAF 等安全设备，实现边界访问控制、入侵攻击防范、恶意代码防范、流量控制等安全边界防护与控制能力。

安全审计：部署上网行为管理、数据库审计、日志审计等安全设备，在关键节点对关键用户行为进行行为审计和数据分析，并对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。

安全管理：部署堡垒机设备，对系统管理员、审计管理员、安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；部署漏洞扫描设备，发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

终端安全：部署终端防病毒（EDR），采用免受恶意代码攻击的技术措施及时识别入侵和病毒行为，并将其有效阻断。

2.1.1.2 等保三级设备配置要求

1.网络设备

交换机/路由器：

- 关闭未使用端口，配置端口安全策略（如 MAC 地址绑定）。
- 启用 SNMPv3 加密协议进行设备管理，禁用默认账户。

2.安全设备

防火墙：

- 部署于网络或者区域边界，配置严格的访问控制策略，仅开放必要端口（如 HTTP/HTTPS）。
- 启用防 SYN Flood、IP 碎片攻击等 DDoS 防护功能。
- 实时监测网络流量，阻断 SQL 注入、XSS、暴力破解等攻击行为。

Web 应用防火墙（WAF）：

- 防护 OWASP Top 10 漏洞（如注入、跨站脚本）。
- 配置防爬虫、CC 攻击策略。

日志审计系统：

- 集中收集网络设备、服务器、安全设备的日志，留存时长≥6 个月。
- 配置异常行为告警（如多次登录失败、敏感操作）。

堡垒机系统：

- 对网络设备、安全设备、服务器等关键 IT 资产进行运维纳管，对运维人员的运维操作进行审计记录。

上网行为管理（网络审计）：

- 实现网络准入认证，流量控制、上网行为审计与控制；

数据库审计

- 对业务系统后端数据库流量进行全面审计，对数据库操作行为进行细颗粒度还原记录，对高危操作进行及时告警。

3.服务器与终端

操作系统：

- 最小化安装，关闭非必要服务（如 Telnet、FTP）。
- 定期更新补丁，配置强密码策略（长度≥8 位，含大小写、数字、特殊字符）。
- 数据库：
 - 启用访问控制（如 RBAC 角色权限模型），敏感数据加密存储（如 AES-256）。
 - 配置审计功能，记录数据增删改操作。

终端安全：

- 部署 EDR（终端检测与响应）软件，实现病毒查杀、U 盘管控、违规外联阻断。

2.1.1.3 数据安全

传输加密：业务系统强制使用 TLS 1.2+协议。

备份与容灾：

核心业务系统数据每日全量备份+增量备份，异地保存。
 关键系统部署双机热备或集群，RTO（恢复时间目标）≤4 小时。

2.1.1.4 合规关键点

等保测评：需通过第三方测评机构检测，覆盖安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理共 10 个层面。

持续运维：定期进行漏洞扫描、渗透测试、安全加固。

政务外网及互联网系统需按照等保三级要求，从网络架构、设备配置、数据安全、管理流程等方面构建纵深防御体系，确保系统抵御高强度攻击，保障业务连续性 & 数据隐私。实施时需结合《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》细化方案。

2.1.2 主要设备技术参数

项目需求清单如下：

序号	类型	名称	数量
1	安全设备	防火墙 A	1
2	安全设备	防火墙 B	2
3	安全设备	防火墙 C	1
4	安全设备	防火墙 D	2
5	安全设备	防火墙 E	1
6	安全设备	上网行为管理（网络审计）A	1
7	安全设备	上网行为管理（网络审计）B	1
8	安全设备	WAF A	1
9	安全设备	WAF B	1
10	安全设备	数据库审计 A	1
11	安全设备	数据库审计 B	1
12	安全设备	日志审计 A	1
13	安全设备	日志审计 B	1
14	安全设备	堡垒机 A	1
15	安全设备	堡垒机 B	1
16	安全设备	漏洞扫描 A	1
17	安全设备	漏洞扫描 B	1
18	安全软件	终端防病毒	1
19	机房整理	机房整理	1

注：本项目核心产品为：防火墙

★注：根据《强制性产品认证管理规定》“节能产品政府采购品目”，属于政府强制采购产品、节能产品，须提供有效期内的节能认证证书及 3C 认证证书。

2.1.2.1 政务外网

2.1.2.1.1 防火墙 A

指标项	参数要求
系统结构	产品符合国产化要求，由专用的国产化硬件平台、国产化安全操作系统及功能软件构成。
硬件规格	≤2U 标准机架式设备，配置不少于 8 个千兆电口、8 个千兆光口和 4 个万兆光口，配置不少于 8 个千兆多模光纤模块、4 个万兆多模光纤模块，不少于 1 个扩展槽位，冗余电源；
产品性能	网络层吞吐量(双向)：IPv4≥38.5Gbps，IPv6≥38.5Gbps。 应用层吞吐量（单向）：IPv4≥19.5Gbps，IPv6≥19.5Gbps。 TCP 新建连接速率：IPv4≥270 万/秒，IPv6≥270 万/秒。 TCP 并发连接数：IPv4≥6000 万，IPv6≥6000 万
授权及升级	3 年原厂商硬件维保服务，配置至少 3 年的入侵防御特征库、病毒防御特征库升级许可，提供设备原厂商授权及售后服务承诺；
工作模式	支持路由、交换、监听、混合等工作模式；
路由配置	支持动态路由（RIP、OSPF、BGP 等）、静态路由、策略路由配置；
地址转换	支持 SNAT、DNAT、双向 NAT、NoNAT 等多种转换方式；
DNS Doctoring	▲支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供产品功能截图证明）
安全策略	支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接等功能配置,简化用户管理；
策略分析	▲提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析等场景，可在 WEB 界面显示检测结果，支持策略变更信息管理，可查看变更策略、变更动作、变更时间、修改人等信息（提供产品功能截图证明）
双栈支持	支持 IPv4/IPv6 双栈工作模式，支持 IPv6 安全控制策略设置；支持对 IPv6 报文进行病毒防御、入侵防御、URL 过滤、抗 DDOS、流量控制、连接限制、文件过滤、数据过滤等；
入侵防御	▲支持独立的入侵防护规则特征库，特征总数在 5500 条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；（提供产品功能截图证明、产品资质等证明材料）
病毒过滤	▲支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御，病毒特征库规模超过 200 万；（提供产品功能截图证明）

安全防护	▲支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；（提供产品功能截图证明）
行为分析	▲内置行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；支持行为分析监控展示，可展示不同行为分析策略的实时数据和基线数据趋势；（提供产品功能截图证明）
日志审计	支持日志外发至多个 SYSLOG 服务器，可设置日志传输协议、外发时间类型、合并传输等参数；
系统备份	支持配置文件本地备份和回滚，支持软件版本本地备份；
高可用	▲支持与现有出口防火墙配置双机热备（HA）（提供承诺函等相关证明材料）
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有国家信息安全测评自主原创产品测评证书，提供资质复印件；
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.1.2 防火墙 B

指标项	参数要求
系统结构	产品符合国产化要求，由专用的国产化硬件平台、国产化安全操作系统及功能软件构成。
硬件规格	≤2U 标准机架式设备，配置不少于 10 个千兆电口、14 个千兆光口和 2 个万兆光口，不少于 1 个扩展槽位，冗余电源；；
产品性能	防火墙吞吐≥8G，并发连接≥300 万；
授权及升级	3 年原厂商硬件维保服务，配置至少 3 年的入侵防御特征库、病毒防御特征库升级许可，提供设备原厂商授权及售后服务承诺；
工作模式	支持路由、交换、监听、混合等工作模式；
路由配置	支持动态路由（RIP、OSPF、BGP 等）、静态路由、策略路由配置；
地址转换	支持 SNAT、DNAT、双向 NAT、NoNAT 等多种转换方式；
链路负载均衡	▲支持链路负载均衡功能，支持轮询、加权轮询、就近选路、优先级、带宽比率等多种链路负载均衡算法，支持备用选路算法，支持链路过载保护；（提供产品功能截图证明）

安全策略	支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接等功能配置,简化用户管理；
策略分析	▲提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析等场景，可在 WEB 界面显示检测结果，支持策略变更信息管理，可查看变更策略、变更动作、变更时间、修改人等信息（提供产品功能截图证明）
双栈支持	支持 IPv4/IPv6 双栈工作模式，支持 IPv6 安全控制策略设置；支持对 IPv6 报文进行病毒防御、入侵防御、URL 过滤、抗 DDOS、流量控制、连接限制、文件过滤、数据过滤等；
入侵防御	▲支持独立的入侵防护规则特征库，特征总数在 5500 条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；（提供产品功能截图证明、产品资质等证明材料）
病毒过滤	▲支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御，病毒特征库规模超过 200 万；（提供产品功能截图证明）
信息防泄漏	▲内置数据过滤功能，支持 HTTP、FTP、POP3、SMTP、TELNET 等协议，可对自定义关键字进行过滤；（提供产品功能截图证明）
网络诊断	▲支持在 WEB 界面进行网络诊断，支持 PING、TRACEROUTE、TCP、HTTP、DNS 等多种诊断方式（提供产品功能截图证明）
日志审计	支持日志外发至多个 SYSLOG 服务器，可设置日志传输协议、外发时间类型、合并传输等参数；
系统备份	支持配置文件本地备份和回滚，支持软件版本本地备份；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有国家信息安全测评自主原创产品测评证书，提供资质复印件；
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.1.3 防火墙 C

指标项	参数要求
系统结构	产品符合国产化要求，由专用的国产化硬件平台、国产化安全操作系统及功能软件构成。
硬件规格	≤2U 标准机架式设备，配置不少于 10 个千兆电口、8 个千兆光口，不少于 2 个扩展槽位，冗余电源。
产品性能	防火墙吞吐量≥1Gbps，并发连接数≥100 万，每秒新建连接数≥1.2 万，全威胁吞吐量≥350Mbps；

授权及升级	3 年原厂商硬件维保服务，配置至少 3 年的入侵防御特征库、病毒防御特征库升级许可，提供设备原厂商授权及售后服务承诺；
工作模式	支持路由、交换、混合等工作模式；
路由配置	支持动态路由（RIP、OSPF、BGP 等）、静态路由、策略路由配置；
地址转换	支持 SNAT、DNAT、双向 NAT、NoNAT 等多种转换方式；
安全策略	▲支持多元组的访问控制规则，至少支持基于源 MAC、源端口、服务、时间、域名、URL 等多个元素进行访问控制,支持对单条访问控制策略进行最大并发连接数和长连接的限制；（提供产品功能截图证明）
应用控制	▲支持对通过设备的 DNS 查询请求进行域名过滤；支持 FTP 行为过滤，包括但不限于 FTP 上传、文件下载、文件删除、目录删除、创建目录、重命名、列表等（提供产品功能截图证明）
双栈支持	支持 IPv4/IPv6 双栈工作模式，支持 IPv6 安全控制策略设置；能针对 IPv6 的目的/源地址、源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；
入侵防御	▲支持独立的入侵防护规则特征库，特征总数在 5000 条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；（提供产品功能截图证明、产品资质等证明材料）
恶意代码防护	▲支持恶意代码防护（病毒过滤）功能，可针对 HTTP、SMTP、POP3、FTP 协议进行动态阻断；恶意代码特征库总数大于 200 万；（提供产品功能截图证明）
高级威胁防护	▲支持高级威胁防护，可对 DGA、隐蔽信道、恶意加密流量进行检测，并实时记录日志（提供产品功能截图证明）
黑名单	▲内置静态黑名单功能，可设置多个对象条件，如：源目 IP 地址、源目端口、源目 MAC、协议等，实现对特定报文进行快速过滤（提供产品功能截图证明）
日志审计	支持日志外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.1.4 上网行为管理（网络审计）A

指标项	指标要求
硬件配置	标准机架式设备，高度≤2U，配置不少于 4 个千兆电口，硬盘存储≥1T；
产品性能	适配带宽≥200M，网络吞吐量≥800M；
授权及升级	包含三年特征库升级许可和硬件维保服务，提供设备原厂商授权及售后服务承诺；
部署模式	支持路由模式，旁路模式、网桥模式、混合模式部署；切换部署模式无需重启，不影响设备正常使用；

网络适配性	▲支持接口链路聚合，支持基于轮循、主备、哈希、广播、802.3ad、发送自适应、双向自适应等多种负载方式；（提供产品功能截图证明）
实时监控	能够提供流量适用排名，提供前 50 名用户流量适用情况，并支持趋势图、黑名单、显示活跃服务等操作。通过黑名单可以直接强制某个流量异常用户下线或者快速修改带宽；
安全防护	支持 ARP 欺骗防护，支持 ARP 保护对象以及 ARP 广播间隔设置； 支持 DOS/DDOS 防护功能，支持 ARP 洪水攻击防护，基于数据包攻击、异常报文侦测和扫描防护等功能； ▲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；（提供产品功能截图证明）
用户管理	▲可通过 NetBIOS 协议扫描内网的主机信息，扫描结果将列出每个主机的 IP 地址、MAC 地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理；（提供产品功能截图证明） 支持本地认证、第三方服务器认证、微信认证、企业微信认证等多种认证方式。
行为管控	支持应用标签分类，包含但不限于安全风险、外发文件泄密风险、高带宽消耗、降低工作效率、论坛和微博发帖、发送电子邮件等分类，支持用户自定义应用标签、自定义标签描述； ▲支持 HTTPS 网站识别，支持加密网站搜索，支持 SSL 论坛加密发帖内容识别，支持基于关键字的控制；（提供产品功能截图证明） 关键字组支持通配符配置，支持论坛、微博发帖关键字过滤，支持搜索引擎关键字过滤，支持邮件内容、正文标题、附件内容的关键字过滤，支持包含制定关键字的页面过滤；
流量管理	▲支持每个用户的源，服务等，进行最大上下行会话数控制，避免网络滥用；（提供产品功能截图证明） 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；
上网日志分析	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； 从内网整体网络的宏观角度展现网络使用概况、上网目的地分布、热门应用流量分布、网站类型分析、终端类型分析、在线人群趋势、高风险人群排名、违规行为统计等多维度全方位展现网络的使用综合态势，给网络管理提供依据；
系统管理	▲一键下载设备健康信息，当设备发生故障时如丢包、宕机、异常重启等问题时可以通过设备健康信息获取有效数据，能够快速定位问题。（提供产品功能截图证明）
产品资质	具备中华人民共和国工业和信息化部颁发的《电信设备进网许可证》，提供资质复印件等证明材料； 具备 IT 产品信息安全认证证书，提供资质复印件等证明材料

2.1.2.1.5 WAF A

指标项	参数要求
系统结构	产品符合国产化要求，由专用的国产化硬件平台、国产化安全操作系统及功能软件构成；产品必须为专业性 WEB 应用防火墙硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能。

硬件规格	标准机架式设备，高度≤2U，配置不少于4个千兆电口、4个千兆光口和2个万兆光口，配置不少于4个千兆多模光纤模块、2个万兆多模光纤模块，不少于2个扩展槽，冗余电源；
产品性能	HTTP吞吐量≥3500Mbps，HTTP请求速率≥5万/秒 HTTP并发连接数≥350万；
授权及升级	3年原厂硬件维保服务，配置3年特征库升级许可，提供设备原厂授权及售后服务承诺；
部署方式	支持串联部署、负载均衡模式部署、反向代理模式部署、旁路监测模式部署等多种部署模式；
路由配置	支持静态路由，策略路由，ISP路由配置
网络适应性	▲支持提取客户端真实IP头；自动尝试匹配X-Forwarded-For, X-Real-IP, Cdn-Src-Ip用以获取真实客户端IP。（提供产品功能截图证明）
访问控制	支持网络层访问控制，支持基于源IP地址、目的IP地址、协议类型及接口区域等条件的访问控制。
WEB攻击防护	支持识别和阻断SQL注入攻击、Cookie注入攻击、命令注入攻击、跨站脚本(XSS)攻击、跨站请求伪造(CSRF)攻击等Web安全攻击，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。
多重编码检查	▲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。（提供产品功能截图证明）
网页防篡改	▲支持网关型网页防篡改，无需在服务器中安装任何插件，即可对网站文件内容进行篡改防护，当检测到篡改后可以实时恢复篡改内容。（提供产品功能截图证明）
协议合规检查	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。
DDoS攻击防护	▲支持DDoS攻击防护基线学习，可以自动学习用户http正常流量阈值模型，并给出推荐阈值配置项，支持DDoS攻击动态黑名单功能，检测到DDoS攻击将其攻击源自动加入黑名单。（提供产品功能截图证明）
日志报表	支持记录系统日志、管理日志、流量日志、攻击日志等多种日志类型，支持多条件与查询，支持以syslog格式向远端日志服务器发送日志。
业务数据分析	▲支持对防护的WEB服务器进行健康检查，支持ICMP、TCP、HTTP、HTTPS类型的健康检查。（提供产品功能截图证明）
设备管理	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。
高可用性	支持双机热备，包括主备、主主负载均衡、连接保护等模式。
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有国家信息安全漏洞库兼容性产品资质，提供资质复印件；

产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.1.6 数据库审计 A

指标项	参数要求
系统结构	产品符合国产化要求，由专用的国产化硬件平台、国产化安全操作系统及功能软件构成；
硬件规格	标准机架式设备，高度≤2U，配置不少于 6 个千兆电口、4 个千兆光口和 2 个万兆光口，配置不少于 4 个千兆多模光纤模块、2 个万兆多模光纤模块，硬盘容量≥4TB，不少于 2 个扩展槽位，冗余电源。
产品性能	记录事件能力≥5 万条/秒，抓包速率≥5.4Gbps
授权及升级	三年原厂商硬件维保服务，提供设备原厂商授权及售后服务承诺；
数据库类型	支持细粒度解析 40+种数据库协议，包括但不限于 Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata、Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis、KingBase、DaMeng、Oscar、GBase、Inspur_KDB、Highgo、GaussDB 等国内外主流数据库系统。
数据库自动发现	支持从数据库流量中自动识别数据库，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息；
SQL 操作审计	具备数据库操作类、表、视图、索引、触发器、游标、事务各种对象的 SQL 操作审计，支持详细的审计日志； ▲支持以图形化展示正常 SQL 与慢 SQL 分布占比情况以及 TOP10 慢 SQL 的详细分析，分析包含数据库用户名、源 ip、SQL 语句、SQL 操作类型、SQL 语句响应时间等关键要素；（提供产品功能截图证明）
双向审计	支持数据库请求和返回的双向审计，特别是 SQL 返回结果集、SQL 语句响应时间、连接时长、表影响的字段、影响行数等内容；
敏感防护	▲支持对审计日志中敏感数据（身份证号、手机号、银行卡号等）进行掩码处理，进行隐私保护，敏感保护规则可自定义；（提供产品功能截图证明）
复杂 SQL 审计能力	▲支持超长 SQL 语句审计，至少不低于 2M，支持多层嵌套 SQL 语句的审计，有效分割、准确审计主流数据库协议的多 SQL 语句；（提供产品功能截图证明）
SQL 错误统计分析	▲支持多个维度展示错误占比及趋势，系统内置超过 20000 条以上数据库协议的 SQL 错误码，且支持给出出错原因、出错信息以及解决办法；（提供产品功能截图证明）
日志管理	支持审计日志、系统日志等日志本地存储，也支持通过 Syslog 等方式外发至日志服务器；

IPv6 支持	支持 IPv6 网络环境下的数据库审计，可识别 IPv6 的相关主体与客体资源；
报表模板	支持等保、萨班斯法案报表模板以及自定义报表，可以按日、周、月等周期自动生成报表，支持 DOCX、HTML、PDF、XLSX 等格式导出报表；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件
	产品应具中国国家信息安全产品认证证书，提供资质复印件
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.1.7 日志审计 A

指标项	指标要求
系统结构	产品符合国产化要求，由专用的国产化硬件平台、国产化安全操作系统及功能软件构成；
硬件规格	标准机架式设备，高度≤2U，配置不少于 6 个千兆电口、4 个千兆光口和 2 个万兆光口，硬盘容量≥4TB，冗余电源；
产品性能	日志采集处理均值≥3000EPS；
授权及升级	实配 50 个日志源授权，包含三年原厂商硬件维保服务，提供设备原厂商授权及售后服务承诺；
日志源管理	▲支持手动添加日志源，支持对重点日志源的关注设置，支持通过关注列表快速查看重点日志源的状态，至少包括当日日志量、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）
数据采集	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 300 种日志对象的日志数据采集；
	支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据；
	▲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；（提供产品功能截图证明）
	支持对文本类型日志源进行限速采集，匀速采集日志，防止对系统资源产生突发冲击；
数据存储	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；
	▲支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月、永久保存等多种周期参数；（提供产品功能截图证明）
	▲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；（提供产品功能截图证明）
数据查询	支持实时日志查询，支持历史备份文件导入查询；
	支持等于、不等于、大于、小于、正则表达式等查询条件；支持多条件组合查询；
	支持为不同类型日志设置不同的查询条件和显示条件；
	支持在日志查询结果上针对源 IP、目的 IP、操作、源端口、目的端口等字段一键快速统计；

	支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析；
安全审计	系统内置安全审计规则，以及对应的上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应；
告警管理	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；
	支持告警抑制规则设定，防止报警信息短时间内大量发送； 支持邮件、Snmp Trap、声音、声光、短信等多种告警方式，支持报警内容引用字段变量参数；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.1.8 堡垒机 A

指标项	参数要求
系统结构	产品符合国产化要求，由专用的国产化硬件平台、国产化安全操作系统及功能软件构成；
硬件规格	≤2U 标准机架式设备，配置不少于 6 个千兆电口，4 个千兆光口，配置不少于 4 个千兆多模光纤模块，内存不少于 16G，硬盘容量不小于 4TB，不少于 2 个扩展槽位，冗余电源；
产品性能	图形并发数≥100，字符并发数≥500；
授权及升级	配置不少于 50 个主机/设备许可，用户数不限制，三年原厂硬件维保服务，配置三年的软件升级许可，提供设备原厂授权及售后服务承诺；
部署方式	设备采用物理旁路部署，不改变现有网络结构；
用户管理	支持用户的增删改查、锁定、解锁、清空等操作，对用户进行全生命周期管理；支持用户有效期定义，针对临时用户或者短期用户可以建立有效期用户，过期后自动注销；支持以部门方式对用户进行分组管理；
认证管理	支持本地认证和三方认证服务器接入认证，如 AD、LDAP、Radius 服务器，支持通过 AD 域服务器和 LDAP 服务器进行用户同步；支持双因子认证，认证方式支持动态口令认证、短信认证、数字证书认证、USB-KEY 认证等多因素认证方式；
视频回放	支持常见运维标准协议：SSH、TELNET、RDP、VNC、FTP、SFTP、SCP； 可通过应用发布的方式进行协议扩展，如浏览器（http、HTTPS）、数据库（Oracle、MySQL、SQL Server、DB2、Informix、Sybase、PostgreSQL 等）、C/S 客户端工具（VMware 等）。
应用编排	▲支持各种自定义客户端工具，支持通过动作流配置提供广泛的应用接入支持，在不作二次开发的情况下，可灵活扩展且实现帐号口令的代填。（提供产品功能截图证明）

Html5	支持最新的 html5 技术，在同一 WEB 窗口页签中，无需 JAVA 应用插件或调用本地应用客户端，即可实现对目标设备的快速运维；
会话分享	▲支持会话请求远程协助，且协同会话保持实时同步。（提供产品功能截图证明）
视频回放	▲支持在线或者离线方式回放操作过程，支持操作记录视频回放时水印显示运维用户；（提供产品功能截图证明）
自动化任务	支持手动或自动执行运维脚本，内置常用运维脚本，支持自定义上传脚本；
虚拟化	▲支持对堡垒机虚拟为多台逻辑堡垒机，虚拟堡垒机之间实现独立配置、独立数据。实现 IT 资源的动态分配、灵活调度、跨域共享，提高 IT 资源利用率。（提供产品功能截图证明）
IPv4/IPv6 支持	支持在 IPV4/IPV6 网络环境下部署，支持管理 IPV4/IPV6 资产。
安全管理	▲支持 HTTPS 方式和 Console 方式进行管理,支持管理口与业务口分离，启用管理隔离后，实现管理和运维操作的分离。（提供产品功能截图证明）
监控与日志	支持实时监控 CPU、内存、磁盘等硬件性能，支持将本机日志、告警日志通过 SYSLOG 外发至日志服务器。
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件
	产品应具有 IT 产品信息安全认证证书，提供资质复印件
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.1.9 漏洞扫描 A

指标项	参数要求
系统结构	产品符合国产化要求，由专用的国产化硬件平台、国产化安全操作系统及功能软件构成。
硬件规格	≤2U 标准机架式设备，配置不少于 6 个千兆电口、4 个千兆光口，≥2 个扩展槽位；硬盘容量≥4T；配置 4 个千兆多模光模块；冗余电源
产品性能	Web 并发扫描任务≥3 个；系统并发扫描任务≥5 个，IP 地址并发扫描≥80 个；基线核查并发扫描任务≥4 个；
授权及升级	支持 50 个 Web 域名扫描授权，支持无限制 IP 扫描授权，基线核查支持 100 个资产，配置 3 年原厂硬件维保服务和特征库升级服务，提供设备原厂授权及售后服务承诺；
工作模式	支持 web 扫描、系统扫描、基线核查等扫描模式，支持对扫描任务进行克隆、查询、导出、删除、查看等操作，支持断点续扫功能；
被动扫描	▲支持被动扫描功能，支持 http 代理和镜像流量两种被动扫描方式；（提供产品功能截图证明）

漏洞扫描能力	支持扫描主流操作系统、Web 服务器、数据库、网络主机、移动设备、应用及软件的安全漏洞；
	▲支持扫描大数据组件的安全漏洞，如 Spark、Splunk、Kafka、Storm、Cassandra、Ambari、Impala、Solr、Oozie、Hbase、Hadoop 等，可扫描漏洞数量不少于 400 条；（提供产品功能截图证明）
	▲支持扫描系统漏洞数量大于 240000 种，web 漏洞数量大于 5000 种，数据库大于 3000 种，CVE 漏洞数大于 60000。（提供产品功能截图证明）
	产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少 CVE、CNCVE、CNVD、BUGTRAQ、CNNVD 编号；
主机存活探测	主机存活探测支持 ARP ping、ICMP ping、TCP ping、UDP ping、TCP SYN、TCP ACK 等多种方式；
弱口令探测	▲支持 ActiveMQ、FTP、Highgo、HTTP、IMAP、Kingbase、MongoDB、MS SQL、Mysql、Oracle、POP3、Postgres、RDP、RTSP、SMB、SMTP、SNMP、SSH、Sybase、Telnet、Tomcat、UXDB、Weblogic 等弱口令探测；（提供产品功能截图证明）
	支持密码字典模板管理，能够按照用户名、密码以及用户名&密码组合等不同类别的字典；
专项漏洞验证	▲支持 POC 脚本库，通过构造真实可控的请求报文，对目标进行无害化漏洞验证；（提供产品功能截图证明）
漏洞管理	支持漏洞生命周期管理，可标注未修复、确定、忽略、修复、已验证等多种漏洞状态；
报表管理	支持在线报表，可详细展示任务综述信息、主机列表、漏洞列表、对比分析、参考标准等信息，漏洞分布支持风险等级过滤查看，支持扫描任务中自动生成报表，包含 html、pdf、word、excel、wps、xml 等多种格式类型，可通过设置邮箱、FTP 自动发送；
资产管理	支持资产自动发现，快速发现组织节点范围内的资产信息；支持从资产节点和资产创建扫描任务，支持导出扫描任务报告；
漏洞预警	▲漏洞库升级完成后，列举出受新漏洞影响的资产，进行资产漏洞预警；（提供产品功能截图证明）
系统管理	支持限制 webui、ssh、telnet 方式登陆最大并发管理数，超出限额时，可选择提示不能登陆、踢掉最不活跃的用户等方式处理；
	支持日志外发至日志服务器，支持自定义传输协议、编码格式、时间设置、日志语言等参数；
	在 WEB 界面提供资源监控开关，可对 CPU 占用率、内存占用率、磁盘占用率设置阈值；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；
	产品应具有中国国家信息安全产品认证证书，提供资质复印件；

2.1.2.2 互联网

2.1.2.2.1 防火墙 D

指标项	参数要求
硬件规格	≤2U 标准机架式设备，配置不少于 6 个千兆电口，硬盘容量≥1T；
产品性能	防火墙吞吐量≥5G，并发连接数≥150 万，每秒新建连接数≥5 万
授权及升级	3 年原厂商硬件维保服务，配置至少 3 年的入侵防御特征库、病毒防御特征库升级许可，提供设备原厂商授权及售后服务承诺；
工作模式	支持路由、交换、监听、混合等工作模式；
路由配置	支持动态路由（RIP、OSPF、BGP 等）、静态路由、策略路由配置；
地址转换	支持 SNAT、DNAT、双向 NAT、NoNAT 等多种转换方式；
DNS 双向智能转换	▲防火墙作为 DNS 服务器可依据访问地址来源将服务器域名解析为内部地址或外部地址，同时支持通过配置多条转换策略，实现内网资源服务器的负载均衡；（提供产品功能截图证明）
安全策略	支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接等功能配置,简化用户管理；
策略分析	▲提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析等场景，可在 WEB 界面显示检测结果；（提供产品功能截图证明）
双栈支持	支持 IPv4/IPv6 双栈工作模式，支持 IPv6 安全控制策略设置；支持对 IPv6 报文进行病毒防御、入侵防御、URL 过滤、抗 DDOS、流量控制、连接限制、文件过滤、数据过滤等；
入侵防御	▲支持独立的入侵防护规则特征库，特征总数在 5500 条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；（提供产品功能截图证明、产品资质等证明材料）
病毒过滤	▲支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御，病毒特征库规模超过 200 万；（提供产品功能截图证明）
安全防护	▲支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板；（提供产品功能截图证明）
行为分析	▲内置行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；支持行为分析监控展示，可展示不同行为分析策略的实时数据和基线数据趋势；（提供产品功能截图证明）

日志审计	支持日志外发至多个 SYSLOG 服务器，可设置日志传输协议、外发时间类型、合并传输等参数；
系统备份	支持配置文件本地备份和回滚，支持软件版本本地备份；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有中国国家信息安全产品认证证书，提供资质复印件；
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.2.2 防火墙 E

指标项	参数要求
硬件规格	≤2U 标准机架式设备，配置不少于 5 个千兆电口、2 个千兆光口；
产品性能	防火墙吞吐量≥1.5Gbps，并发连接数≥50 万，每秒新建连接数≥1.5 万，全威胁吞吐量≥350Mbps；
授权及升级	3 年原厂硬件维保服务，配置至少 3 年的入侵防御特征库、病毒防御特征库升级许可，提供设备原厂授权及售后服务承诺；
工作模式	支持路由、交换、混合等工作模式；
路由配置	支持动态路由（RIP、OSPF、BGP 等）、静态路由、策略路由配置；
地址转换	支持 SNAT、DNAT、双向 NAT、NoNAT 等多种转换方式；
安全策略	▲支持多元组的访问控制规则，至少支持基于源 MAC、源端口、服务、时间、域名、URL 等多个元素进行访问控制,支持对单条访问控制策略进行最大并发连接数和长连接的限制；（提供产品功能截图证明）
应用控制	▲支持对通过设备的 DNS 查询请求进行域名过滤；支持 FTP 行为过滤，包括但不限于 FTP 上传、文件下载、文件删除、目录删除、创建目录、重命名、列表等（提供产品功能截图证明）
双栈支持	支持 IPv4/IPv6 双栈工作模式，支持 IPv6 安全控制策略设置；能针对 IPv6 的目的/源地址、源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；
入侵防御	▲支持独立的入侵防护规则特征库，特征总数在 5000 条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；（提供产品功能截图证明、产品资质等证明材料）
恶意代码防护	▲支持恶意代码防护（病毒过滤）功能，可针对 HTTP、SMTP、POP3、FTP 协议进行动态阻断；恶意代码特征库总数大于 200 万；（提供产品功能截图证明）
高级威胁防护	▲支持高级威胁防护，可对 DGA、隐蔽信道、恶意加密流量进行检测，并实时记录日志（提供产品功能截图证明）

黑名单	▲内置静态黑名单功能，可设置多个对象条件，如：源目 IP 地址、源目端口、源目 MAC、协议等，实现对特定报文进行快速过滤（提供产品功能截图证明）
日志审计	支持日志外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.2.3 上网行为管理（网络审计）B

指标项	指标要求
硬件配置	标准机架式设备，高度≤2U，配置不少于 4 个千兆电口，硬盘存储≥1T；
产品性能	适配带宽≥200M，网络吞吐量≥800M；
授权及升级	包含三年特征库升级许可和硬件维保服务，提供设备原厂商授权及售后服务承诺；
部署模式	支持路由模式，旁路模式、网桥模式、混合模式部署；切换部署模式无需重启，不影响设备正常使用；
网络适配性	▲支持接口链路聚合，支持基于轮循、主备、哈希、广播、802.3ad、发送自适应、双向自适应等多种负载方式；（提供产品功能截图证明）
实时监控	能够提供流量适用排名，提供前 50 名用户流量适用情况，并支持趋势图、黑名单、显示活跃服务等操作。通过黑名单可以直接强制某个流量异常用户下线或者快速修改带宽；
安全防护	支持 ARP 欺骗防护，支持 ARP 保护对象以及 ARP 广播间隔设置；
	支持 DOS/DDOS 防护功能，支持 ARP 洪水攻击防护，基于数据包攻击、异常报文侦测和扫描防护等功能； ▲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；（提供产品功能截图证明）
用户管理	▲可通过 NetBIOS 协议扫描内网的主机信息，扫描结果将列出每个主机的 IP 地址、MAC 地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理；（提供产品功能截图证明）
	支持本地认证、第三方服务器认证、微信认证、企业微信认证等多种认证方式。
行为管控	支持应用标签分类，包含但不限于安全风险、外发文件泄密风险、高带宽消耗、降低工作效率、论坛和微博发帖、发送电子邮件等分类，支持用户自定义应用标签、自定义标签描述；
	▲支持 HTTPS 网站识别，支持加密网站搜索，支持 SSL 论坛加密发帖内容识别，支持基于关键字的控制；（提供产品功能截图证明）
	关键字组支持通配符配置，支持论坛、微博发帖关键字过滤，支持搜索引擎关键字过滤，支持邮件内容、正文标题、附件内容的关键字过滤，支持包含制定关键字的页面过滤；
流量管理	▲支持每个用户的源，服务等，进行最大上下行会话数控制，避免网络滥用；（提供产品功能截图证明）
	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；

上网日志分析	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； 从内网整体网络的宏观角度展现网络使用概况、上网目的地分布、热门应用流量分布、网站类型分析、终端类型分析、在线人群趋势、高风险任人群排名、违规行为统计等多维度全方位展现网络的使用综合态势，给网络管理提供依据；
系统管理	▲一键下载设备健康信息，当设备发生故障时如丢包、宕机、异常重启等问题时可以通过设备健康信息获取有效数据，能够快速定位问题。（提供产品功能截图证明）
▲产品资质	具备电信设备进网许可证，提供资质复印件； 具备 IT 产品信息安全认证证书，提供资质复印件；

2.1.2.2.4 WAF B

指标项	参数要求
系统结构	产品必须为专业性 WEB 应用防火墙硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能；
硬件规格	标准机架式设备，高度≤2U，实配不少于 8 个千兆电口、2 个千兆光口和 2 个万兆光口，≥2 个扩展槽；
产品性能	应用层吞吐≥500M，网络层吞吐≥3.5G，并发连接≥90 万，新建连接≥4400
授权及升级	3 年原厂硬件维保服务，配置 3 年特征库升级许可，提供设备原厂授权及售后服务承诺；
部署方式	支持串联部署、负载均衡模式部署、反向代理模式部署、旁路监测模式部署等多种部署模式；
访问控制	支持应用层访问控制功能；
WEB 攻击防护	支持识别和阻断 SQL 注入攻击、Cookie 注入攻击、命令注入攻击、跨站脚本(XSS)攻击、跨站请求伪造(CSRF)攻击，支持扫描防护，支持 WebShell、文件包含漏洞利用、目录遍历等攻击的防护，支持对网站登录暴力破解防护，支持盗链防护，支持爬虫攻击防护； 支持自定义对身份证、信用卡、手机号码、座机电话号码、邮箱地址等敏感信息做检查，当检查到此类数据后支持通过配置特殊字符*予以替换隐藏； 支持对多重的编码均进行安全防御检查； 支持对文件的上传下载进行控制；
DDoS 攻击防护	▲支持基线学习，可以自动学习用户 http 正常流量阈值模型，并给出推荐阈值配置项。（提供产品功能截图证明）
防护动作	支持自定义防护动作，至少包括告警、拒绝、重定向、错误页面等；
协议检查	支持对 HTTP 协议合规性进行验证，支持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；
自学习	支持自学习建模功能，可以通过学习正常 URL 参数的长度、参数类型、请求方法等数据特点创建白名单模型，如果参数违反白名单模型则认为是非法流量直接阻断，开启自学习建模功能后可生成自学习网站参数的自学习结果报告；
网页防篡改	▲支持无需在服务器中安装任何插件对网站文件内容进行篡改防护，当检测到篡改后支持实时恢复篡改内容（提供产品功能截图证明）
安全分析	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；

日志外发	支持以 syslog、welf 等格式向远端日志服务器发送日志，日志传输支持加密；
设备管理	支持 SNMP 的 V1、V2、V3 管理，支持 SNMP 陷阱主机功能；
WEB 漏洞扫描	▲WAF 内置 WEB 漏扫功能，支持对 WEB 应用漏洞进行扫描检测，支持自定义每日、每周、每月等扫描周期设置，并能够以 pdf、html、txt、xml 等格式导出 web 漏洞扫描报告（提供产品功能截图证明）
双机热备	支持主备、主主负载均衡、连接保护等模式； 支持两台 WAF 配置同步，至少支持全局同步和策略同步；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件； 产品应具有国家信息安全漏洞库兼容性产品资质，提供资质复印件； 产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.2.5 数据库审计 B

指标项	参数要求
硬件规格	≤2U，实配不少于 6 个千兆电口，硬盘≥1T；
产品性能	网络吞吐≥100Mbps，峰值 SQL 处理能力≥1000 条/s
售后服务	3 年原厂硬件维保服务，提供设备原厂授权及售后服务承诺；
数据库类型	支持 Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata 等数据库系统 支持 Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis 等国际主流数据库系统 支持 KingBase、DaMeng、Oscar、GBase、浪潮_KDB、Highgo、Gauss DB 等国内主流数据库系统
数据库发现	支持从数据库流量中自动识别数据库，自动添加到待监控审计列表；
SQL 操作审计	支持数据库操作类、表、视图、索引、触发器、游标、事务各种对象的 SQL 操作审计； ▲以饼图展示正常 SQL 与慢 SQL 分布占比情况、TOP10 慢 SQL 的详细分析：数据库用户名、源 ip、SQL 语句、SQL 操作类型、SQL 语句响应时间等要素（提供产品功能截图证明） 支持多个维度展示错误占比及趋势，以列表形式给出出错原因、出错信息以及解决办法，支持 20000 条以上数据库协议的 SQL 错误码；
双向审计	支持数据库请求和返回的双向审计，至少包括 SQL 返回结果集、SQL 语句响应时间、连接时长、表影响的字段、影响行数等内容
数据库监控	支持依据数据库实例监控数据库的连接池、缓冲区、表空间、死锁、CPU、内存、硬盘等信息，支持自定义告警阈值进行健康评估；
弱口令扫描	▲支持数据库服务器弱口令扫描，扫描出的弱密码支持脱敏显示（提供产品功能截图证明）
实名审计	支持以用户名、源 IP、部门、域名、主机名、邮箱、联系电话为条件的实名审计；
会话回放	▲支持会话回放功能,并至少支持 0.5 倍速、1 倍速、1.5 倍速、2 倍速、4 倍速等多级播放速度调节（提供产品功能截图证明）
敏感防护	支持对审计日志中敏感数据（身份证号、手机号、银行卡号等）进行掩码处理，敏感保护规则支持自定义；
数据查询	支持以访问数据库时间、源目 IP、源目端口、数据库名、客户端程序、SQL 语句、返回码、SQL 错误信息、影响行数、业务用户名、SQL 操作

	类型、数据库表名、表影响字段等数据库字段作为查询和统计条件；
复杂 SQL 审计能力	支持超长 SQL 语句审计，至少不低于 5M； 支持多层嵌套 SQL 语句的审计；
端口重定向	支持端口重定向审计，在服务器端口变化动态协商为其他端口时同样能精确审计；
基线管理	支持根据某时间范围内用户或业务系统对数据库的操作行为构建 SQL 基线模板； 智能基线防护功能，可开启基线学习模式，自定义学习时长，掌握学习进度和基线详情，学习结束后可自动切换到防护状态，对学习的安全基线以外的行为智能识别自动告警；
业务关联审计	支持插件方式和非插件方式的业务关联审计；
一键巡检	支持系统本身主要运行功能服务模块的运行状态巡检，保证系统安全稳定运行；
安全管理	支持红莲花、密信等支持国密 SM2/SM3/SM4 算法的安全浏览器登录管理；
日志外发	支持 Syslog、SNMP、kafka 等方式外发日志；
磁盘管理	支持磁盘清理，支持根据磁盘利用率、保存时限配置磁盘清理条件，支持存储外发；
告警通知	支持通过声光、邮件、短信等方式对审计日志、系统日志进行告警通知；
报表管理	支持等保、萨班斯法案报表模板以及自定义报表，支持按日、周、月等周期自动生成报表； 支持 DOCX、HTML、OFD、PDF、XLSX 格式导出报表；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件； 产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.2.6 日志审计 B

指标项	详细要求
授权及升级	三年原厂商维保服务，配置不少于 20 个日志源授权；提供原厂商授权及售后服务承诺；
数据采集	支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集； 支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集，支持通过 Agent 采集日志数据； 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；
数据存储	支持日志原始数据完整存储，支持本地存储和网络存储； ▲支持独立设置日志和报表数据存储时间为 1 个月、3 个月、6 个月、永久保存等周期参数（提供产品功能截图证明） 支持多盘并行存储，支持自动切换存储位置，支持磁盘阵列、SAN、DAS 等外部高性能存储； 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；
数据查询	支持实时日志查询，支持历史备份文件导入查询；

	支持等于、不等于、大于、小于、正则表达式等查询条件，支持多条件组合查询；
	支持查询结果快速统计，支持自定义统计规则，支持以分、时、周、月、年定时执行自动统计，支持将统计结果报表发送到指定邮箱；
	支持基于时间轴展示日志数据分布，支持通过时间轴进行查询分析；
告警管理	支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备 IP、源 IP、目的 IP 等方式快速检索安全事件告警，检索结果支持 Excel 等格式导出；
	▲支持基于时间轴展示告警数据分布，支持通过时间轴进行查询分析(提供产品功能截图证明)
	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；
报表管理	支持不少于上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建
	支持统计分析报表以 PDF、word、execl、html 等方式导出，支持实时报表、计划报表；
日志源管理	支持手动添加日志源，支持对日志源进行查看、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，支持通过关注列表快速查看重点日志源的状态，至少包括当日日志量、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）
系统管理	支持用户按角色管理，支持三权分立；
	支持将日志源管理权限分配给不同的操作管理员；
	支持设置非法用户访问控制策略；
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.2.7 堡垒机 B

指标项	参数要求
硬件规格	≤2U 标准机架式设备，配置不少于 4 个千兆电口，2 个千兆口，硬盘容量不小于 1TB；
产品性能	图形并发数≥25，字符并发数≥50；
授权及升级	配置不少于 50 个主机/设备许可，用户数不限制，三年原厂商硬件维保服务，配置三年的软件升级许可，提供设备原厂商授权及售后服务承诺；
部署方式	设备采用物理旁路部署，不改变现有网络结构；
用户管理	支持用户的增删改查、锁定、解锁、清空等操作，对用户进行全生命周期管理；支持用户有效期定义，针对临时用户或者短期用户可以建立有效期用户，过期后自动注销；支持以部门方式对用户进行分组管理；

认证管理	支持本地认证和三方认证服务器接入认证，如 AD、LDAP、Radius 服务器，支持通过 AD 域服务器和 LDAP 服务器进行用户同步；支持双因子认证，认证方式支持动态口令认证、短信认证、数字证书认证、USB-KEY 认证等多因素认证方式；
视频回放	支持常见运维标准协议：SSH、TELNET、RDP、VNC、FTP、SFTP、SCP； 可通过应用发布的方式进行协议扩展，如浏览器（http、HTTPS）、数据库（Oracle、MySQL、SQL Server、DB2、Informix、Sybase、PostgreSQL 等）、C/S 客户端工具（VMware 等）。
应用编排	▲支持各种自定义客户端工具，支持通过动作流配置提供广泛的应用接入支持，在不作二次开发的情况下，可灵活扩展且实现帐号口令的代填。（提供产品功能截图证明）
Html5	支持最新的 html5 技术，在同一 WEB 窗口页签中，无需 JAVA 应用插件或调用本地应用客户端，即可实现对目标设备的快速运维；
会话分享	▲支持会话请求远程协助，且协同会话保持实时同步。（提供产品功能截图证明）
视频回放	▲支持在线或者离线方式回放操作过程，支持操作记录视频回放时水印显示运维用户；（提供产品功能截图证明）
自动化任务	支持手动或自动执行运维脚本，内置常用运维脚本，支持自定义上传脚本；
自动发现	▲通过 IP 网段扫描，快速发现指定 IP 地址范围内的资产，并自动识别 IP 和端口，方便管理员快速添加资产。（提供产品功能截图证明）
IPv4/IPv6 支持	支持在 IPV4/IPV6 网络环境下部署，支持管理 IPV4/IPV6 资产。
安全管理	▲支持 HTTPS 方式和 Console 方式进行管理，支持管理口与业务口分离，启用管理隔离后，实现管理和运维操作的分离。（提供产品功能截图证明）
监控与日志	支持实时监控 CPU、内存、磁盘等硬件性能，支持将本机日志、告警日志通过 SYSLOG 外发至日志服务器。
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件
	产品应具有 IT 产品信息安全认证证书，提供资质复印件
	产品应具有 IPv6 Ready Logo 认证，提供资质复印件
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；

2.1.2.2.8 漏洞扫描 B

指标项	指标要求
硬件规格	配置不少于 4 个千兆电口
系统性能	支持无限制 IP 扫描授权，并发扫描 IP 地址 ≥ 10 ，并发系统扫描任务 ≥ 3 ；

	配置 3 个域名扫描授权，并发 web 扫描任务≥1
升级授权	配置 3 年原厂商硬件维保服务和特征库升级服务，提供设备原厂商授权及售后服务承诺；
漏洞扫描	▲支持扫描系统漏洞数量大于 400000 种，数据库大于 3300 种，国产化漏洞大于 55000 种，云计算平台漏洞大于 5700 种，大数据组件漏洞大于 430 种，Web 漏洞数量大于 7400 种（提供产品功能截图证明）
	漏洞库至少包括 CVE、CNCVE、CNVD、BUGTRAQ、CNNVD、CVSS 等信息
	支持扫描主流操作系统、Web 服务器、数据库、网络主机、移动设备、应用及软件的安全漏洞；
	▲支持 API 扫描，通过 API 扫描补充扫描链接，支持上传 csv、wsdl 等格式的文件进行扫描（提供产品功能截图证明）
	支持网络打印机、摄像头、移动终端等设备的漏洞发现；
	支持对 DB2、MSSQL、MySQL、Oracle、GBASE、DMDB 等主流数据库进行登陆认证扫描；
	扫描目标支持 ip、域名、网段、子网的组合配置；
口令猜解	支持自定义口令猜测时间、猜测频率、猜测次数、最大并发线程数；
	支持 DB2、FTP、IMAP、MSSQL、MYSQL、Oracle、POP3、POSTGRES、RDP、Redis、RTSP、SMB、SMTP、SNMP、SSH、TELNET、TOMAT 等的弱口令探测
漏洞管理	支持漏洞管理，支持跟踪漏洞修复状态
	▲内置丰富的 POC 脚本库，通过构造真实可控的请求报文，对目标进行无害化漏洞验证（提供产品功能截图证明）
漏洞预警	▲漏洞库升级完成后，列举出受新漏洞影响的资产，进行资产漏洞预警（提供产品功能截图证明）
系统报表	支持在线报表，支持详细展示任务综述信息、站点列表、漏洞列表、对比分析及参考标准
▲产品资质	产品应具有中华人民共和国国家版权局计算机软件著作权登记证书，提供资质复印件；
	产品应具有网络关键设备和网络安全专用产品安全认证证书或者网络安全专用产品安全检测证书，提供资质复印件；
	产品应具有中国国家信息安全产品认证证书，提供资质复印件；

2.1.2.2.9 终端防病毒

指标项	参数要求
产品架构	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管理中心，即可对系统进行管理。
终端环境支持	客户端至少支持 Windows（WindowsXP、Windows 7、Windows 8、Windows 10、Windows 11 等 32 位/64 位终端操作系统，支持 Windows server 2003、Windows server2008、Windows server 2012、Windows server 2016、Windows server 2019 等 32 位/64 位服务器操作系统）、Linux（Red Hat Linux、Ubuntu Linux、SuSE Linux、CentOS、Debian 等）以及国产化操作系统（如中标麒麟、银河麒麟、中科方德、深度、UOS 等国产操作系统）
授权及升级	至少包含 60 个终端授权，配置 3 年原厂商软件维保服务和特征库升级服务，提供产品原厂商授权及售后服务承诺；

客户端资源占用	▲客户端资源占用：客户端安装后至多占用 50M 硬盘资源，日常内存占用不到 30M，有效节省 PC/Server 资源（提供产品功能截图证明）
终端升级	支持在线升级、离线升级，平台立即、定时推送升级；
任务下发	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、文件分发设置等操作，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；
终端发现	▲支持通过 PING、ARP、NMAP 方式扫描，发现尚未纳入管控的终端，支持展示终端的终端在线、离线、安装情况（提供产品功能截图证明）
安全防护策略	▲支持定制安全防护策略：包括病毒防御（包括不限于病毒查杀、文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（包括不限于黑客入侵拦截、IP 协议控制、恶意网站拦截、IP 黑名单）；合规管控（包括不限于文档检测、文档跟踪、USB 存储、设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）等功能（提供产品功能截图证明）
终端防卸载	支持终端防卸载、防脱离功能，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。
微隔离	▲支持不同终端组、不同 IP、不同服务之间的安全隔离和访问控制，规范内部网络不同对象的访问行为。支持协议包括但不限于 TCP、UDP、TCP/UDP、ICMP、IGMP、GGP、PUP、IDP、ND、ESP、AH、RDP、GRE、SKIP、RAW。（提供产品功能截图证明）
病毒扫描	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，支持对压缩文件内的恶意文件扫描；
Webshell 检测	▲支持对 webshell 后门进行扫描检测，webshell 后门规则数量大于 100000。（提供产品功能截图证明）
勒索病毒诱捕	▲支持开启勒索诱捕功能，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）
下载保护	在下载过程中对文件进行检测，发现恶意程序立即弹窗阻止，并记录安全日志。
系统管理	支持远程控制，通过管理中心实现对客户端的远程运维，可设置例外终端。
	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。
	支持对安全策略备份、恢复。
▲产品资质	产品应具有计算机软件著作权登记证书，提供资质复印件；
	产品应具有网络安全专用产品安全认证或者安全检测证书，提供资质复印件；

2.1.2.3 系统工程量清单

序号	类型	设备名称	数量	用途
1	安全设备	防火墙（含 A、B、C、D、E）	7	开启入侵防御、防病毒功能模块，防火墙实现访问控制、入侵攻击防范、恶意代码防范等功能
2	安全设备	上网行为管理（网络审计）（含 A、B）	2	实现网络准入认证，流量控制、上网行为审计与控制；
3	安全设备	WAF（含 A、B）	2	实现对业务应用系统的安全防护，识别并阻断 SQL 注入、XSS 攻击等常见 WEB 攻击行为。
4	安全设备	数据库审计（含 A、B）	2	对业务系统后端数据库流量进行全面审计，对数据库操作行为进行细颗粒度还原记录，对高危操作进行及时告警。
5	安全设备	日志审计（含 A、B）	2	采集网络设备、安全设备、业务系统、服务器等各资产的日志数据集中存储、分析，并保证审计记录的留存时间满足 180 天以上。
6	安全设备	堡垒机（含 A、B）	2	通过集中化账号管理、多权限认证、细粒度授权控制和多形式审计记录，使运维操作处于可管、可控、可见、可审的状态下，规范运维的操作步骤，避免误操作和非授权操作带来的隐患。
7	安全设备	漏洞扫描（含 A、B）	2	对信息资产进行漏洞扫描，并形成漏洞扫描报告和修复建议。
8	安全软件	终端防病毒	1	实现病毒查杀、漏洞修复、系统加固等功能。

2.2 项目其他要求

2.2.1 建设周期

项目建设期为项目合同正式签署后 1 个月，自相关合同签署起进入建设期，建设期结束时间以最终系统验收时间为准。

2.2.2 调试运行

对系统的功能、性能、安全等进行详细分析，制定系统的整体架构及技术实现方案；

确定系统的架构模式，确实系统的技术架构，制定系统的技术解决方案；

分析系统的需求，确定系统的模块划分，完成系统模块设计；

系统经过总体功能测试，并提交测试报告；

系统经过约定时间期限的试运行，并提交试运行报告；

2.2.3 人员要求

本项目实施人员不少于五人，项目经理，技术负责人，技术人员等，需提供本人近3个月连续社保证明。

2.2.4 售后服务要求

本项目要求提供自竣工验收之日起不少于3年的质保期；

质保期内提供软硬件保修服务，对故障报修无条件及时响应；在接到故障报修通知后，在15分钟内响应，2小时内到达故障现场进行抢修，在4小时内修复故障；若属于硬件故障，应在24小时内修复，不能立即修复的应提供备品备件应急使用。

各投标单位在方案中应针对项目的特点制定的质保期承诺和售后服务承诺及措施、突发情况下的应急措施和承诺、人员培训计划、备品备件的供应计划等。

2.2.5 项目团队要求

项目实施期间需委派1名具有一级建造师资格项目经理进行现场管理，并配置本项目相关的技术人员，相关人员需持有相关技术证书。

4.6 项目验收

中标单位必须完成招标要求及合同规定的全部建设内容；

项目的所有技术文档、图纸已整理完成并经过审核，符合规范要求；

项目具备以下条件的，投标人可以申请竣工验收：

(1) 除发包人同意的甩项工作和缺陷修补工作外，合同范围内的全部以及有关工作，包括合同要求的试验、试运行以及检验均已完成，并符合合同要求；

(2) 已按合同约定编制了甩项工作和缺陷修补工作清单以及相应的施工计划；

(3) 已按合同约定的内容和份数备齐竣工资料。

对于竣工验收不合格的项目，承包人完成整改后，应当重新进行竣工验收，经重新组织验收仍不合格的且无法采取措施补救的，则发包人可以拒绝接收不合格项目，因不合格项目导致其他项目不能正常使用的，承包人应采取措施确保相关项目的正常使用，由此增加的费用和（或）延误的工期由承包人承担。

项目需要试运行的，除专用合同条款另有约定外，试运行的内容应与投标人承包范围相一致，试运行费用由投标人承担。

由投标人组织试运行，并在试运行前 48 小时书面通知监理人，通知中应载明试运行内容、时间、地点。投标人准备试运行记录，发包人根据投标人要求为试运行提供必要条件。试运行合格的，监理人在试运行记录上签字。

对于包含复杂设备的建设项目，应对验收后使用和维护保养设备的人员进行培训考核，确保由培训考核合格人员进行使用和维护保养，费用由投标人承担。

第四部分 合同条款

(参考)

注：本合同仅为合同的参考文本，若与项目需求书内容有冲突，以项目需求书为准，合同签订双方可根据项目的具体要求进行修订。

第四部分 合同条款

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]

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-供应商联系人电话]

根据《中华人民共和国民法典》等有关法律法规的规定，现依照五角场监狱网络安全等级保护基础设施加固采购项目的采购结果，经双方协商现就有关事项达成如下条款/补充协议：

一、乙方应严格按照报价文件内容提供中选的货物（列表）：（单位：人民币元）

1. 1 货物详细信息详见乙方投标文件。

本合同的合同价为[合同中心-合同总价]元（[合同中心-合同总价大写]）。与交货有关的所有费用应包含在合同价中，买方不再另行支付任何费。

二、供货时间：乙方必须于[合同中心-合同有效期]将招标文件及投标文件响应的货物送至甲方指定地点，免费安装完毕，并承担运输过程中发生的一切费用。

三、安装及调试：乙方必须在甲方指定的地点免费进行货物的安装，安装所需的相应配套设施及安装费用（如有）由乙方自行负责解决，用户提供必须的现场安装条件。如甲方因为基建施工等原因影响乙方进场安装，甲方应及时通知乙方，完工期可适当顺延。如乙方不按本合同约定提交设备所产生的任何费用由乙方负责，甲方对由此所引起的变动不予确认。另外，乙方在甲方安装设备或施工过程中的安全责任由乙方全部责任。

四、质量标准：乙方所提供的货物必须是原厂生产的、全新的、未使用过的（包括零部件），并符合原厂质量检测标准（以说明书为准）和国家质量检测标准以及合同规定的质量规格和性能要求，如货物不符合本合同约定的要求，甲方有权拒绝接受。如采购耗材，乙方所提供的配合物资耗材应按照甲方所给定的物资耗材配方生产所得，且质量参数满足甲方要求。如货物不符合本合同约定的要求，甲方有权拒绝接收。

五、权利保证：乙方应保证甲方在使用乙方提供的货物或货物的任何部份不受第三方关于侵犯其所有权、专利权、商标权、工业设计权等等指控。甲方如果因第三方侵权索赔而遭受损失的，有权向乙方追偿。

六、验收及货物所有权、风险转移：甲方负责货物清点和验收。乙方所提供的货物安装调试完成后，甲方必须按本合同所约定的货物清单及要求对货物的品牌、外观、规格、数量、配件及安装调试后的使用性能、运行状况、技术资料及其他质量指标进行检测、验收，乙方必须在验收现场提供必要的技术支持，甲方

应在乙方所提供的货物安装调试完成后尽快组织验收。若其质量参数与合同规定不符，或验收不合格的，甲方有权拒收货物。如货物在保证期内被证明存在缺陷，包括潜在的缺陷或使用不合适的材料，甲方有权凭有关证明文件向乙方提出索赔。

除双方另有约定外，乙方就货物安装调试完毕并经甲方验收合格接受后，货物的所有权及货物灭失、损害风险由乙方转移至甲方。

七、异议期：甲方若对与货物有关的事项提出异议，应在货物验收后的七个工作日内书面通知乙方，乙方应在三个工作日内负责解决。

八、付款方式：按下列方式，转账支付：

1.合同生效后7日内乙方向甲方提供合同价款10%的履约担保，履约担保形式为银行保函；

2.甲方收到乙方提供的有效的履约保函后20个工作日内，甲方向乙方支付合同总价的30%预付款；

3.甲方在标的物安装调试完毕并且验收合格后，根据乙方开具的相应金额增值税专用发票，向乙方支付货款总额的70%货款，同时预付款转为货款。

九、售后服务：

在质保服务，乙方应按照本次招标文件中有关质量保证和售后服务的承诺执行，国家有规定的按国家规定执行。

十、索赔：

1、乙方对货物与合同要求不符负有责任，并且甲方已于规定的检验、安装、调试和验收测试期限内和质量保证期内提出索赔，乙方应按甲方要求的下述一种或多种方法解决索赔事宜。

(1) 乙方同意甲方拒收货物并按被拒收货物的合同价格的金额付给甲方，乙方负担发生的一切损失费用，包括利息、银行费用、运输和保险费、检验费、仓储和装卸费以及为保管和保护被拒绝货物所需要的其它必要费用。

(2) 根据货物的疵劣和受损程度以及甲方遭受损失的金额，经乙方和甲方同意降低货物价格。

(3) 更换有缺陷的零件、部件和设备，或修理缺陷部分，以达到合同规定的规格、质量和性能，乙方承担一切费用和 risk 并负担甲方遭受的一切直接费用。同时乙方应相应延长被更换货物的质量保证期。

(4) 如出现乙方所交付的货物在质保期内出现货物本身的质量问题而乙方不予修理或更换，及乙方不响应甲方报修等服务问题，乙方向甲方支付合同总额 5% 的赔偿金。

2、如果甲方提出索赔通知后 30 天内乙方未能予以答复，该索赔应视为已被乙方接受。若乙方未能在甲方提出索赔通知的 30 天内或甲方同意的更长一些的时间内，按甲方同意的上述任何一种方式处理索赔事宜，甲方将从未付的合同价款中扣回索赔金额，同时按本合同第十三条规定追究乙方的违约责任或解除合同。

十一、双方责任和义务：

1、乙方按合同清单上的货物运达指定地点并安装调试完成后，甲方应在 7 个工作日内验收完毕，若甲方无正当理由拖延时间，不能及时付款，按国家政府采购法有关规定由甲方赔偿乙方损失。

2、乙方所交货物不符合本合同要求的，甲方有权拒收；同时，乙方向甲方偿付设备款30%违约金。

3、乙方不能交付货物的，乙方向甲方支付设备款 30%违约金。

4、乙方逾期交付货物，乙方向甲方每日偿付设备款 5%的违约金。

十二、终止合同

1、在补救违约而采取的任何其他措施未能实现的情况下，即在甲方发出的违约通知后30天内（或经甲方书面确认的更长时间内）仍未纠正其下述任何一种违约行为，甲方可向乙方发出书面违约通知，终止全部或部分合同：

（1）如果乙方未能在合同规定的期限内或甲方准许的任何延期内合格交付部分或全部货物。

（2）乙方未能履行合同项下的任何其它义务。

2、任何一方由于下列原因而导致不能或暂时不能履行全部或部分合同义务的，不负责任：水灾、火灾、地震、干旱、战争或其他任何在签约时不能预料、无法控制且不能避免和克服的事件。但受不可抗力影响的一方，应尽快地将所发生的事件通知对方，并应在事件发生后 15 天内将有关机构出具的不可抗力事件的证明寄交对方，如果不可抗力事件之影响超过 120 天，双方应协商合同继续履行或终止履行的事宜。

3、本合同于约定全部义务履行完毕后而终止；

4、双方协商一致可以终止履行本协议。

十三、合同纠纷的处理方式：若发生争议，由双方友好协商解决。协商不成可到合同签订所在地人民法院诉讼解决。

十四、本采购项目的招标文件、乙方的投标文件均为本合同不可分割的一部分。

十五、本合同未尽事宜，双方另行补充。

十六、本合同壹式肆份，经双方签章后即时生效。甲方叁份，乙方壹份，具有同 等效力。

十七、本合同未尽事宜，双方可以另行协商，商定内容经双方代表签字并盖章后与本合同具有同等效力。设备供货清单、技术参数、售后服务承诺及本合同未尽事宜详见补充合同，若补充合同与本合同有不同之处以补充合同为准。

[合同中心-补充条款列表]

签约各方：

甲方（盖章）：

乙方（盖章）：

法定代表人或授权委托人：[合同中心
2025年08月14日]

法定代表人或授权委托人：[合同

-采购单位联系人_1]

中心-供应商联系人_1]

日期：[合同中心-签订时间]

日期：[合同中心-签订时间_1]

合同签订点:网上签约

第五部分 评标办法

第五部分 评标办法

综合本项目的特点，根据相关法律法规的规定，本着保护竞争，维护招标工作公开、公平、公正原则，特制定本评标办法，作为选定本次招标中标人的依据。

1、资格性审查

开标后，采购代理机构和招标人依法对投标人的资格性进行审查，若下述项缺漏或无效的或存在重大不良记录的投标人，将不通过资格性审查，且不进入后续符合性审查及详细评审。具体内容如下：

- (1) 营业执照或法人登记证书等；
- (2) 财务状况及税收、社会保障资金缴纳情况声明函；
- (3) 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的书面声明；

(4) 在信用中国（www.creditchina.gov.cn）、中国政府采购网中“政府采购严重违法失信行为信息记录”（www.ccgp.gov.cn/cr/list）对参与开标会的投标人进行信息查询、截图留存，确认投标人截至投标截止时间前三年内，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等。

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，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。

- (5) 具备法律、行政法规规定的其他条件的证明材料；
- (6) 具备履行合同所必需的设备和专业技术能力的证明材料；
- (7) 本项目投标人必须满足的其他资格条件；

通过资格性审查的投标人满足 3 家的，进入详细评审，若通过不足 3 家则不得进行评标。

2、评标委员会

2.1 招标人、招标代理机构将根据招标货物/服务的特点，依法组建评标委员会，其成员由技术、经济等方面的专家和招标人的代表组成，其中外聘专家人数不少于评标委员会总人数的 2/3。评标委员会对投标文件进行审查、质疑、评估和比较。

2.2 评标委员会履行下列职责：

(1) 对通过资格性审查的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求；

(2) 要求投标人对投标文件有关事项作出澄清或者说明；

(3) 对投标文件进行比较和评价；

(4) 评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求；

(5) 确定中标候选人名单，以及根据招标人委托直接确定中标人；

(6) 向招标人、采购代理机构或者有关部门报告评标中发现的违法行为；

(7) 评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

3、详细评审

3.1 本项目的评标采用综合评分法，总分 100 分，其中价格标权数为 30%，技术商务标权数为 70%。

3.2 政府采购主要政策：

(1) 中小企业划型标准按照《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）》文的相关规定认定。

(2) 根据《财库〔2014〕68 号》监狱企业视同小型、微型企业，享受中小企业发展的政府采购政策（监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件）。

(3) 根据《财库〔2017〕141 号》符合条件的残疾人福利性单位视同小型、微型企业，享受中小企业发展的政府采购政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

(4) 参加政府采购活动的中小企业应当按“关于印发《政府采购促进中小企业发展管理办法》的通知[财库〔2020〕46 号]”和《财库〔2017〕141 号》规定提供《中小企业声明函》和《残疾人福利性单位声明函》。未提供上述资料的报价，其价格不予扣除。

(5) 对于列入政府采购节能产品、环境标志产品实施品目清单的产品，应根据财政部、发展改革委、生态环境部等部门确定的实施政府优先采购和强制采购相关标准规范执行；采购的产品属于品目清单范围的，采购人及采购代理机构将依据国家确定的认证机构出具

的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。

上述品目清单以最新公布内容为准，投标人须在投标文件中提供相应的证明材料。

若国家或者上海市规定政府采购应当强制采购或优先采购的其他产品和服务，按照其规定实行强制采购或优先采购。

若属于规定必须强制采购的节能产品，投标人须提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，评标委员会须推荐符合强制节能要求产品的投标人为中标人，若投标人未提供相关节能产品认证证书，则作无效标处理。

3.3 若本项目面向大、中、小、微型企业，事业单位及社会组织等各类供应商采购，且供应商提供了完整、真实的“中小企业声明函”，属于小型或微型企业的供应商按下述规定享受价格分优惠政策，中标单位应切实落实面向中小企业预留采购份额的政策要求：

(1) 根据《政府采购促进中小企业发展管理办法》的相关规定，对小型或微型企业产品的价格给予 10 的扣除，以扣除后的价格作为评审价格；专门面向中小企业采购时，则不再给予价格 10% 的扣除。

(2) 若投标人为联合体，组成联合体或者接受分包合同的中小企业与联合体内其他企业、分包企业之间不得存在直接控股、管理关系。接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30% 以上的，采购人、采购代理机构应当对联合体或者大中型企业的报价给予 4% 的扣除，用扣除后的价格参加评审。

(3) 供应商提供的货物或服务符合下列情形的，享受中小企业扶持政策：

1) 货物采购项目：货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标，享受中小企业扶持政策。

注：货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。

2) 服务采购项目：服务由中小企业承接，即提供服务的人员为中小企业按照《中华人民共和国劳动合同法》订立劳动合同的从业人员，享受中小企业扶持政策。

3.4 采用综合评分法的，评标结果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并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的排名第一的中标候选人为中标人。若出现排名第一的中标候选人放弃中标或不能按招标文件规定签订合同等原因取消中标资格，则按排名顺序依次确定其后中标候选人为中标人或重新招标。

3.5 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，由评标委员会参照上述

3.4 相关规定确定中标人推荐资格，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，将以本招标文件第三部分采购需求中核心产品判定。多家投标人提供的核心产品品牌相同的，按前述规定处理。

3.6 评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

具体评分细则如下：

评分细则

序号	评审因素	分值	评分说明	备注
一、价格得分（30分）				
1	投标总价	30	1、根据财政部 87 号令文件规定，综合评分法中的价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为基准价，其价格分为满分 30 分。 2、其他投标人的投标报价得分计算公式如下： 投标报价得分=(评标基准价 / 投标报价)×30%×100。	客观分
二、商务部分（18分）				

1	类似业绩	6	<p>类似业绩指：投标人近3年以来承接的有效的类似项目业绩。</p> <p>是否属于有效类似业绩由评委根据投标人业绩项目的服务内容、技术特点等与本项目的类似程度进行认定。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6分，没有有效的类似项目业绩的得0分。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、合同金额、交付日期等合同要素的相关内容，否则将不予认可。</p>	客观分
2	人员要求	12	<p>1、项目负责人具有一级建造师（机电或通信与广电专业）证书得3分；</p> <p>2、技术负责人具有注册信息安全专业人员 CISP 证书得3分；</p> <p>3、相关技术人员中具有高级网络工程师或网络安全专家的得2分，具有信创集成项目管理师的得2分，具有系统集成中级职称得2分；</p>	客观分
三、技术部分（52分）				
1	需求理解	10	<p>对系统现状、应用环境、体系结构需求、功能需求、性能要求和实施要求等需求内容的理解程度；重难点分析、合理化建议、风险分析及控制方案的优劣进行评审；</p> <p>上述几方面的内容详细全面且全都与项目履约相关，完整合理，可行性很强，可得10分；</p> <p>上述几方面的内容全面但不够详细，内容与项目履约相关，可行性较强，可得5分；</p> <p>上述几方面的内容不全面不详细，虽与项目履约相关但可行性一般，可得3分；</p> <p>上述几方面的内容不全面不详细，与项目履约无关，可行性差，不得分。</p>	主观分
2	技术参数	15	<p>根据各投标单位所报产品技术参数与招标文件“第三部分采购需求”中“三、具体技术参数”响应情况进行综合评审：</p> <p>（1）评审内容：重要技术参数：“▲”条款。 “▲”条款技术参数每有1项指标负偏离扣2分，扣完为止。</p> <p>（2）评审内容：一般技术参数：非“▲”条款。 投标人所投产品未标注“▲”的产品技术参数每有1项指标负偏离扣1分，扣完为止。</p> <p>（设备参数条款需在《技术条款偏离表》中体现响应情况及偏离情况，要求提供证明材料的需按照参数要求提供相应的证明材料复印件并按要求盖章，如不提</p>	客观分

			供或不按要求提供则视为无效响应，扣除相应分值)	
3	实施方案	10	系统集成与产品安装部署实施方案（组织结构及分工、详细进度安排、产品采购管理、质量控制方法、安全管理、试运行及验收方案等）是否详细完整；培训内容、培训方法、培训师资等培训方案是否合理 上述几方面的内容详细全面且全都与项目履约相关，完整合理，可行性很强，可得 10 分； 上述几方面的内容全面但不够详细，内容与项目履约相关，可行性较强，可得 5 分； 上述几方面的内容不全面不详细，虽与项目履约相关但可行性一般，可得 3 分； 上述几方面的内容不全面不详细，与项目履约无关，可行性差，不得分。	主观分
4	项目实施进度计划	6	进度计划符合项目实际需求、科学合理，包括但不限于：明确了各阶段的时间安排和任务分配且与招标文件需求一致；进度保障措施完善，提供了详细的进度保障措施，包括人员、设备、资金等方面的安排； 上述几方面的内容详细全面且全都与项目履约相关，完全合理，可行性很强，可得 6 分； 上述几方面的内容全面但不够详细，内容与项目履约相关，可行性较强，可得 3 分； 上述几方面的内容不全面不详细，虽与项目履约相关但可行性一般，可得 1 分；	主观分
5	售后服务	6	售后服务方案、管理措施、应急预案等是否完整合理。内容详细全面且全都与项目履约相关，完整合理，可行性很强，可得 6 分； 上述几方面的内容全面但不够详细，内容与项目履约相关，可行性较强，可得 3 分； 上述几方面的内容不全面不详细，虽与项目履约相关但可行性一般，可得 1 分； 上述几方面的内容不全面不详细，与项目履约无关，可行性差，不得分。	主观分
6	企业综合能力	5	投标人具有有效的质量管理体系认证得 1 分；环境管理体系认证得 1 分；职业健康安全管理体系认证得 1 分；信息安全管理体系认证得 1 分；具有高新技术企业认证证书或专精特新证书的得 1 分， 注：需提供相关证书原件扫描件，否则不得分。	客观分
合计			100 分	

注：以上各项评分内容，如投标人未提供相对应内容，评标委员会不受最低评分标准限制，可予以零分计算。

三、总分计算

由评审小组成员对每一份响应文件进行独立评分，然后取算术平均值（保留小数点两位）。计算每个投标人的实际得分（价格标得分+技术商务标得分），并按得分高低排出名次。

第六部分 格式附件

第六部分 格式附件

附件 1

投标书（格式）

致_____（招标人）_____：

根据贵方为 _____项目（编号：_____）的投标邀请，签字代表_____（全名职务）经正式授权并代表投标人_____（投标人名称、地址）提交投标文件。

全权代表宣布如下：

- （1）我方将按招标文件的规定履行合同责任和义务。
- （2）我方已详细研究了全部招标文件，包括招标文件的澄清和修改文件（如果有的话）、参考资料及有关附件，我们已完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。
- （3）我方承诺在投标有效期内（提交投标文件截止之日起 90 日历日）不修改、撤销投标文件。
- （4）我方按照招标文件要求递交投标保证金人民币_____元整。
- （5）如果在规定的开标时间后，我方在投标有效期内撤回投标，投标保证金将被贵方没收。
- （6）我方同意提供按照贵方可能要求的与投标有关的一切数据或资料，完全理解贵方不一定要接受最低价的投标或收到的任何投标。
- （7）与本投标有关的一切正式往来通讯请寄：

地址：_____ 邮编：_____

电话：_____ 传真：_____

投标人名称（公章）：_____

被授权人（签字或盖章）：_____

日期：____年____月____日

附件 2

法定代表人等资格证明书（格式）

致____（招标人）_____：

兹证明____（姓名）现任我单位 ____ 职务。

附：法定代表人性别：

身份证号码：

统一社会信用代码：

单位类型：

经营范围：

投标人名称：（盖章）

日期： 年 月 日

粘贴法定代表人身份证复印件（正反面）

附件 3

授权委托书（格式）

致_____（招标人）_____：

兹委托_____（姓名），身份证号码：_____，
_____，全权代表我公司参与_____（项目名称、编号）的投标
活动，受委托人由 此所出具并签订的一切有关文件，我公司均予承认。

本授权书有效期：_____年_____月_____日至_____年_____月_____日

授权公司：_____（盖
章）

法定代表人：_____（签字
或盖章）

被授权人：_____（签字
或盖章）

粘贴被授权人身份证复印件（正反面）

附件 4

开标一览表（格式）

投标人名称：

项目编号：

预算编号：

货币单位：元（人民币）

网络安全等级保护基础设施加固工程款包 1

交付时间	质保期	投标总价（包括所有采购内容）(总价、元)

注：1、以上报价包含本项目产生的所有费用（含税），若报价非整数，报价精确到小数点后两位。中标后，招标人不再另外支付其他费用。

2、此表投标总价须与附件 5 投标报价明细表合计总价一致。

投标人名称（盖章）：

法定代表人或授权委托人（签字或盖章）：

日期： 年 月 日

附件 5

投标报价明细表（参考格式）

项目名称：

项目编号：

预算编号：

货币单位：元（人民币）

序号	设备名称	品牌 / 型号	制造商	产地	...	数量	单位	单价 (元)	合计 (元)	备注
					...					
					...					
合计 总价	小写： 大写：									

说明：

- 1、所有价格均系用人民币表示，单位为元，精确到小数点后两位。
- 2、该表中包含投标人认为完成本项目所需的所有费用,各项费用须列出明细清单。上表合计报价之和应等于“开标一览表”中的投标总价。如果不提供详细单项报价将视为没有实质性响招标文件。

投标人名称（盖章）：

法定代表人或授权委托人（签字或盖章）：

日期： 年 月 日

附件 5-1 备品备件费用等清单（如有，参考格式）

（招标人）：

若中标，我司承诺质保期后 3 年内，以不高于报价表中的单价向招标人供应 备品备件。

序号	装备名称	备品备件名称	单价（元）	品牌	型号	制造商名称	产地	维修期人工工时费单价（元）	...
									...
									...
									...
									...
									...

注：

1.所投产品如有备品备件，投标人应提供货物质保期内及质保期结束后一年的备品备件、易损件和易耗件一览表，按要求列出详细清单，标出制造商、型号、数量、单价、总价，其费用分项报价，不计入投标总价，并承诺在质保期后 3 年内以不高于上述清单价格，且按招标人不时要求的数量及合理时间向招标人提供该易损件和备品备件。

2.维修期人工工时费单价。

投标人名称（公章）：_____

法定代表人或授权委托人（签字或盖章）：_____

日期：____ 年____ 月 ____ 日

附件 6 货物报告

包括但不限于以下内容：

- 1、合同履行能力
- 2、产品质量保证
- 3、功能指标
- 4、项目实施方案
- 5、对接方案
- 6、故障及应急处理
- 7、培训方案
- 8、售后服务方案
- 9、验收保障
- 10、售后服务承诺及保障措施
- 11、演示评审
- 12、按照招标文件要求提供的其他技术性资料以及投标人认为需要说明的其他事项。

注：以上内容，投标人应结合本招标文件第五部分评标办法的要求详细描述并提供相关证明文件。

附件 6-1 投标货物标“★”条款技术偏离表（如有）

项目名称：_____

_____ 项目编号：

投标产品	招标文件要求	投标文件的 响应参数	详细内容所对 应投标文件名 称	详细内容所对 应投标所在页 码	偏离说明

1、“★”号条款为实质性要求，不满足或未按要求响应招标文件中“★”号条款的，将作为废标 处理。

2、如果投标文件的响应对招标文件有偏离，请在此表中清楚地列明，并加以说明。

投标人名称（盖章）

法定代表人或授权委托人（签字或盖章）：

日期： 年 月 日

附件 6-2 投标货物重要技术参数(▲条款) 技术偏离表 (如有)

项目名称: _____

_____ 项目编号: _____

投标产品	招标文件要求	投标文件的响应	偏离说明	详细内容所对应 投标文件页码

注:

1. 投标人应针对招标文件的采购需求中“▲条款”内容逐条响应。
2. “▲”号条款为重要技术参数，不满足或未按要求响应招标文件中“▲”号条款的，则视为该项指标负偏离。
3. “▲”号技术参数必须在投标文件中如实提供技术支持资料，如果应标参数与技术支持资料不一致时，以技术支持资料为准，不能提供技术支持资料，视为该指标不满足技术要求。
4. 如果投标文件的响应对招标文件有偏离，请在此表中清楚地列明，并加以说明。
5. 如果表格叙述不下，可另附页说明，但要便于招标人查阅。

投标人名称 (盖章)

法定代表人或授权委托人 (签字或盖章):

日期: 年 月 日

附件 6-4 拟派项目负责人情况表（格式）

1.一般情况					
姓名		年龄		技术职务	
职务		本合同中拟任职务		为投标人服务时间	
学历/专业					
所获证书					
2.经历					
年份	负责过的主要项目 (类型金额)		该项目中任职		备注

注：

- 1.须提供相关证明材料（如相关证书复印件）。
- 2.项目负责人一旦确定，中标后原则上不再变更，若变更，须征得招标人同意。

附件 6-5 项目对接服务承诺函（参考格式）

致_____（采购人）_____：

（需根据招标文件要求进行相关承诺，并需承诺能于交付时间内完成对接。）

投标人名称：（盖章）

法定代表人或授权委托人：（签字或盖章）

日期： 年 月 日

附件 6-6 拟派本项目技术人员情况表（格式）

序号	姓名	年龄	相关证书 持证情况	本项目中担 任职务	类似项目 经验	备注
1						
2						
3						
4						
...						

注：

- 1.须提供相关证明材料（如相关证书复印件）；
- 2.项目组技术人员一旦确定，中标后原则上不再变更，若变更，须征得招标人同意；

附件 6-7 投标人（2022 年 1 月 1 日起至今）承担的类似项目业绩一览表（格式）

序号	项目名称	委托单位	委托时间	项目完成时间	合同金额	备注
1						
2						
3						
4						
...						
...						

注：1.供应商需提供上述类似项目的合同扫描件，合同扫描件中需体现合同的 签约主体、项目名称及内容、合同金额、交付日期等合同要素的相关内容。

2.业绩时间以合同签订时间为准。

附件 7

资格证明文件

目录

- 1、营业执照或法人登记证书等；
- 2、财务状况及税收、社会保障资金缴纳情况声明函；
- 3、具备履行合同所必需的设备和专业技术能力的证明材料；
- 4、具备法律、行政法规规定的其他条件的证明材料；
- 5、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的书面声明；
- 6、如以分支机构（分公司/分所等）名义报价的，须提供总公司（总部/总所等）授权函；
- 7、中小企业声明函（如有）；
- 8、根据本招标文件采购需求还需提供的其他证明文件。

须知

- 1、投标人应提交相关证明文件，以及提供其他有关资料。
- 2、投标人提交的文件将给予保密，但不退还。

附件 7-1

投标人资格声明函

致____（招标人）_____：

关于贵方____年__月__日_____项目（项目编号：_____）的
投标邀请，本签字人愿意参加投标，并证明提交的下列文件和说 明是准确和真
实的。

- 1、营业执照或法人登记证书等；
- 2、财务状况及税收、社会保障资金缴纳情况声明函；
- 3、具备履行合同所必需的设备和专业技术能力的证明材料；
- 4、具备法律、行政法规规定的其他条件的证明材料；
- 5、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的书面声明；
- 6、如以分支机构（分公司/分所等）名义报价的，须提供总公司（总部/总所等）
授权函；
- 7、根据本招标文件采购需求还需提供的其他证明文件。

本签字人确认投标文件中关于资格的一切说明都是真实的、准确的。

投标人名称（盖章）：

本资格声明函授权代表（签字或盖章）：

附件 7-2

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的书面声明

致：_____（招标人）

我公司承诺在参加本项目政府采购活动前三年内，在经营活动中没有重大违法记录，遵守国家其他有关的法律、法规和管理办法。

特此声明。

（注：重大违法记录是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

供应商在参加政府采购活动前 3 年内因违法经营被禁止在一定期限内参加政府采购活动，期限届满的，可以参加政府采购活动）

投标人名称（盖章）：

法定代表人或授权委托人（签字或盖章）：

日期： 年 月 日

附件 7-3 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。

名称（公章）

供应商

日期：

注：①本声明函未提供或未盖章的，视为不符合《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，作无效投标处理。

②如发现供应商提供虚假声明，不符合《政府采购法》第二十二条规定条件的，由财政部门依法进行处理处罚。

附件 8

中小企业声明函（格式）

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¹，属于（中 型企业、小型企业、微型企业）；

2. （标的名称），属于（采购文件中明确的所属行业）行业；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结构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

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

说明：（1）本声明函适用于所有在中国境内依法设立各类所有制和各种组织形式的企业、个体工商户。

（3）若中标，本声明函作为中标公告的一部分进行公示，接受社会监督，请如实填写。若提供虚假信息，则取消中标资格，并依法承担相应责任。

（4）特别说明：本项目为货物采购，投标人必须将本次投标的所有货物明细在中小企业声明中列出，并列出相应的货物对应的制造商信息及制造商所属企业性质，未按要求提供或填写中小企业声明函，将不认定为中小企业，无法享受中小企业扶持政策。

附：《中小企业划型标准规定》各行业划型标准

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 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 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上

的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 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 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。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 2000 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 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。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 2000 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 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 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 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（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。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 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 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元

及以上的为 小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

(十六)其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

附件 9 残疾人福利性单位声明函（格式）（如有请提供）

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。

投标人名称（盖章）：

日期： 年 月 日

说明：若中标，本声明函作为中标公告的一部分进行公示，接受社会监督，请如实填写。如投标人不符合残疾人福利性单位条件，无需填写本声明。

附：《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》

享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：

（1）安置的残疾人占本单位在职职工人数的比例不低于 25%（含 25%），并且安置的残疾人人数不少于 10 人（含 10 人）；

（2）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

（3）为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；

（4）通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；

（5）提供本单位制造的货物、承担的工程或者服务（以下简称产品），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）。

残疾人是指法定劳动年龄内，持有《中华人民共和国残疾人证》或者《中华人民共和国残疾军人证（1至8级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或者服务协议的雇员人数。

供应商书面声明

致：_____（招标人）

我公司承诺已自查，在参加本项目政府采购活动中未违反《中华人民共和国政府采购法实施条例》第十八条“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。

为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。”

特此声明。

投标人名称（盖章）：

法定代表人或授权委托人（签字或盖章）：

日期： 年 月 日

保证金退还信息表（格式）

投标人全称：	
保证金的递交	
已递交的保证金形式：	
已递交的保证金金额：	
保证金的退还	
开户行：	
户名：	
帐号：	
保证金退还联系人：	
联系电话：	

注：

- 1、投标人可将递交保证金的银行汇款凭证作为本页附件。
- 2、投标人应准确填写保证金的退还账号、联系人等相关信息，以便招标代理机构及时退还保证金。