采购编号：QPZFCG2026-045

青浦区政府采购中心

青浦区消防救援支队组网安全信创加固项目

招标文件

采购人：上海市青浦区消防救援支队

集中采购机构：青浦区政府采购中心

2026年04月30日

2026年04月30日

目　　录

第一章　　投标邀请

根据《中华人民共和国政府采购法》之规定，青浦区政府采购中心受采购人委托，对以下项目进行国内公开招标采购，特邀请合格的投标人前来投标。

一、合格的投标人必须具备以下条件：

1、符合《中华人民共和国政府采购法》第二十二条规定条件。

2、根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商。

3、其他资质要求：

3.1 本项目采购预算 3473700 元，超过采购预算的投标不予接受。

3.2 本项目非专门面向中小微企业采购。

3.3 联合投标:不允许。

3.4 未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn/cr/list)政府采购严重违法失信行为记录名单的供应商。

二、项目概况：

1、项目名称：青浦区消防救援支队组网安全信创加固项目

2、招标编号：详见招标公告（代理机构内部项目编号：QPZFCG2026-045）

3、预算编号：1826-000189087、1826-K00009550

4、 项目主要内容、数量及要求：详见招标需求。

5、交付地址：青浦区范围内

6、交付日期：本项目建设周期为 6 个月内完成项目建设并通过验收，其中从合同签订起 1 个月内完成所有设备交货，之后 1 个月内完成所有设备的安装部署及调试，之后 4 个月进行试运行及测试工作。

7、投标保证金：无

8、采购项目需要落实的政府采购政策情况：推行节能产品政府采购、环境标志产品政府采购。促进中小企业、监狱企业、残疾人福利性单位发展。规范进口产品采购政策。

9、本项目是否接受联合体投标：本次招标不接受联合投标。

三、招标文件的获取：

1、合格的供应商可于 2026-04-30 至 2026-05-12 上午 00:00:00~12:00:00；下午 12:00:00~23:59:59（节假日除外）。登录“上海政府采购网”在网上招标系统中上传如下材料：无。

2、凡愿参加投标的合格供应商应在上述规定的时间内按照规定获取招标文件，逾期不再办理。未按规定获取招标文件的投标将被拒绝。

3、获取招标文件其他说明：

注：投标人须保证获得招标文件需提交的资料和所填写内容真实、完整、有效、一致，如因投标人递交虚假材料或填写信息错误导致的与本项目有关的任何损失由投标人承担。

四、投标截止及开标时间：

1、投标截止及开标时间：2026 年 05 月 21 日 10:00，投标截止时间以后上传的投标文件恕不接受。

五、投标地点和开标地点：

1、投标地点： 上海政府采购网（www.zfcg.sh.gov.cn）。

2、开标地点：上海政府采购网（www.zfcg.sh.gov.cn）。

六、发布公告的媒介：

以上信息若有变更我们会通过“上海政府采购网”通知，请供应商关注。

七、其他事项

根据上海市财政局《**关于上海市政府采购云平台上线试运行的通知**》的规定，本项目采

购相关活动在由市财政局建设和维护的上海市政府采购云平台（简称：采购云平台，门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）进行。供应商应根据《上海市电子政府采购管理暂行办法》等有关规定和要求执行。供应商在采购云平台的有关操作方法可以参照采购云平台中的“操作须知”专栏的有关内容和操作要求办理。

投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在采购云平台上的签收情况，打印签收回执，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

八、联系方式

集中采购机构：青浦区政府采购中心

地址：青浦区城中西路 38 号南楼

邮编：201799

联系人：邓智 朱达君

电话：021-59732489

传真：021-59732489

采购人：上海市青浦区消防救援支队

地址：胜利路 1828 号

邮编：201799

联系人： 叶祎平

电话：22176363

传真：/

第二章　　投标人须知

前附表

一、项目情况

项目名称：青浦区消防救援支队组网安全信创加固项目

项目编号：QPZFCG2026-045

项目内容：详见需求

（采购标的对应的中小企业划分标准所属行业：软件和信息技术服务业）

二、联系方式

集中采购机构：青浦区政府采购中心

地址：青浦区城中西路 38 号南楼

邮编：201799

联系人：邓智 朱达君

电话：021-59732489

传真：021-59732489

采购人：上海市青浦区消防救援支队

地址：胜利路 1828 号

邮编：201799

联系人： 叶祎平

电话：22176363

传真：/

三、合格供应商条件

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：推行节能产品政府采购、环境标志产品政府采购。促进中小企业、监狱企业、残疾人福利性单位发展。规范进口产品采购政策。

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；

3.1、本项目预算为3473700元人民币，超过预算的投标不予接受。

3.2 本项目为非专门面向中小企业采购项目。

3.3、本项目不接受联合体投标。

四、招标有关事项

招标答疑会：不召开

踏勘现场：不组织

投标有效期：不少于90天

投标截止时间：详见投标邀请（招标公告）或延期公告（如果有的话）

递交投标文件方式和网址：

投标方式：由供应商在上海市政府采购云平台（门户网站：上海政府采购网）提交。

投标网址：http://www.zfcg.sh.gov.cn

开标时间和开标地点网址：

开标时间：同投标截止时间

开标地点网址：上海市政府采购云平台（门户网站：上海政府采购网，网址：http://www.zfcg.sh.gov.cn）

评标委员会的组建与评标方法：

评标方法：详见第五章《评标方法与程序》

中标人推荐办法：详见第五章《评标方法与程序》

五、其它事项

付款方法：详见合同

六、说明

根据上海市财政局《**关于上海市政府采购云平台上线试运行的通知**》的规定，本项目采

购相关活动在由市财政局建设和维护的上海市政府采购云平台（简称：采购云平台，门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）进行。供应商应根据《上海市电子政府采购管理暂行办法》等有关规定和要求执行。供应商在采购云平台的有关操作方法可以参照采购云平台中的“操作须知”专栏的有关内容和操作要求办理。

投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在采购云平台上的签收情况，打印签收回执，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

投标人须知

一、总则

1．概述

1.1 根据《中华人民共和国政府采购法》、《中华人民共和国招标投标法》等有关法律、法规和规章的规定，本采购项目已具备招标条件。

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

1.3 招标文件的解释权属于《投标邀请》和《投标人须知》前附表中所述的招标人。

1.4 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它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。

1.5 根据上海市财政局《关于上海市政府采购信息管理平台招投标系统正式运行的通知》(沪财采[2014]27号)规定，本项目招投标相关活动在上海市政府采购信息管理平台(简称：电子采购平台。网址：home.zfcg.sh.gov.cn）招投标系统进行。

2．定义

2.1 “采购项目”系指《投标人须知》前附表中所述的采购项目。

2.2 “货物和服务”系指招标文件规定的投标人为完成采购项目所需承担的全部义务。

2.3 “招标人”系指《投标人须知》前附表中所述的采购人和集中采购机构。

2.4 “投标人”系指从招标人处按规定获取招标文件，并按照招标文件向招标人提交投标文件的供应商。

2.5 “中标人”系指中标的投标人。

2.6 “甲方”系指采购人。

2.7 “乙方”系指中标的投标人。

2.8 招标文件中凡标有“★”的条款均系实质性要求条款。

2.9 “电子采购平台”系指上海市政府采购信息管理平台（上海政府采购网），网址：home.zfcg.sh.gov.cn。该平台由上海市财政局建设和维护。

3．合格的投标人

3.1 符合《投标邀请》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。

3.2 投标人投标所使用的资格、信誉、荣誉、业绩及企业认证必须为本人（或本法人、本组织）所拥有。

3.3 被省级及以上政府采购监督管理部门处分，禁止参加政府采购活动且尚在禁止期内的供应商不得参加本采购项目的投标。

3.4 联合体投标

3.4.1 两个以上的自然人、法人或者其他组织以联合体形式参加政府采购活动的，联合体各方均应具备《中华人民共和国政府采购法》第二十二条规定的条件，按招标文件规定向采购人提交“联合投标协议书”，应载明联合体主办方、各方承担的工作和义务，由主办方代表联合体参加政府采购活动；联合体各方应共同与采购人签订采购合同，就合同约定的事项对采购人承担连带责任。

3.4.2 联合体中有同类资质的供应商按照联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级。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。

3.4.3 招标人根据采购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采购规定的特定条件。

4．合格的货物和服务

4.1 投标人对所提供的货物和服务应享有合法的所有权，没有侵犯任何第三方的知识产权、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。

4.2 投标人提供的货物和服务应当符合招标文件的要求，其质量应当完全符合国家法律法规和相关政策规定，符合国家标准、行业标准或者地方标准；均有标准的以高（严格）者为准，没有国家标准、行业标准和企业标准的，按照通用标准或者符合采购目的的特定标准确定。

4.3 投标人提供的货物应当是全新的、未使用过的，应当说明投标货物的来源地，如投标货物非投标人生产或制造的，则应当按照招标文件的要求提供其从合法途径获得该货物的相关证明。

5．投标费用

不论投标的结果如何，投标人均应自行承担所有与投标有关的全部费用，招标人在任何情况下均无义务和责任承担这些费用。

6．信息发布

本采购项目需要公开的有关信息，包括招标公告、招标文件澄清或修改公告、中标公告以及延长投标截止时间等与招标活动有关的通知，招标人均将通过“上海政府采购网”（http://home.zfcg.sh.gov.cn）公开发布。投标人在参与本采购项目招投标活动期间，请及时关注以上媒体的相关信息，投标人因没有及时关注而未能如期获取相关信息，由此所产生的一切后果和责任由投标人自行承担，招标人在任何情况下均不对此承担任何责任。

7．询问与质疑

7.1 投标人对招标活动事项有疑问的，可以向招标人提出询问。询问可以采取电话、电子邮件、当面或者书面等形式。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7.2 投标人认为招标文件、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

知道或者应知其权益受到损害之日起七个工作日内，以书面形式向招标人提出质疑。其中，对招标文件的质疑，应当在其下载招标文件之日（以电子采购平台显示的报名时间为准）起七个工作日内提出；对招标过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果的质疑，应当在中标公告期限届满之日起七个工作日内提出。投标人应当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，超过次数的质疑将不予受理。以联合体形式参加政府采购活动的，其质疑应当由组成联合体的所有供应商共同提出。

7.3 投标人可以委托代理人进行质疑。委托代理人提出质疑的，应当提交投标人签署的授权委托书和代理人合法、有效的工作和身份证明。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。投标人为自然人的，应当由本人签字；投标人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。

7.4 投标人提出质疑应按照《政府采购质疑和投诉办法》（财政部令第 94 号）的有关规定提交质疑函和必要的证明材料。质疑函应当包括下列内容：（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；（2）质疑项目的名称、编号；（3）具体、明确的质疑事项和与质疑事项相关的请求；（4）事实依据；（5）必要的法律依据；（6）提出质疑的日期。质疑函应按照财政部制定的范本填写，范本格式可通过中国政府采购网（http://www.ccgp.gov.cn）右侧的“下载专区”下载。投标人为自然人的，应由本人签字；投标人为法人或者其他组织的，应由法定代表人、主要负责人或者其授权代表签字或者盖章，并加盖公章。

7.5 投标人提起询问和质疑，应当按照《政府采购质疑和投诉办法》（财政部令第 94 号）的有关规定办理。质疑函或者授权委托书的内容不符合《投标人须知》7.3 条和 7.4 条规定的，招标人将当场一次性告知投标人需要补正的事项，投标人超过法定质疑期未按要求补正并重新提交的，视为放弃质疑。

7.6 **投标人应当采取当面递交的形式向上海市青浦区政府采购中心（地址：青浦区城中西路 38 号南楼 307 室；联系电话：021-59732489）提交质疑书，不接受邮寄、传真等其它送达方式。**

7.7 招标人将在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知提出质疑的投标人及相关投标人，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7.8 如果对投标人询问或者质疑的答复将导致招标文件变更或者影响招标活动继续进行的，招标人将通知提出询问或者质疑的投标人，并在原招标公告发布媒体上发布变更公告。

8．公平竞争和诚实信用

8.1 投标人在本招标项目的竞争中应自觉遵循公平竞争和诚实信用原则，不得存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为。“腐败行为”是指提供、给予任何有价值的东西来影响采购人员在采购过程或合同实施过程中的行

为；“欺诈行为”是指为了影响采购过程或合同实施过程而提供虚假材料，谎报、隐瞒事实的行为，包括投标人之间串通投标等。

8.2 如果有证据表明投标人在本招标项目的竞争中存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为，招标人将拒绝其投标，并将报告政府采购监管部门查处；中标后发现的，中标人须参照《中华人民共和国消费者权益保护法》第55条之规定双倍赔偿采购人，且民事赔偿并不免除违法投标人的行政与刑事责任。

8.3 招标人将在**开标后、评标结束前**，通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关投标人信用记录，并对供应商信用记录进行甄别，对列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单、中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将拒绝其参与政府采购活动；两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商身份共同参加政府采购活动的，将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。

9．其他

本《投标人须知》的条款如与《投标邀请》、《招标需求》和《评标方法与程序》就同一内容的表述不一致的，以《投标邀请》、《招标需求》和《评标方法与程序》中规定的内容为准。

二、招标文件

10．招标文件构成

10.1 招标文件由以下部分组成：

（1）投标邀请（招标公告）

（2）投标人须知

（3）政府采购主要政策

（4）招标需求

（5）评标方法与程序

（6）投标文件有关格式

（7）合同书格式和合同条款

（8）本项目招标文件的澄清、答复、修改、补充内容（如有的话）

10.2 本招标文件阐明了投标人所需提供的货物和服务的范围和招标投标程序，是本次招标活动具有法律效力的文件。投标人应仔细阅读招标文件及补充文件的所有内容，并按照招标文件的要求提交投标文件。如果投标人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在各方面作出实质性响应，则投标有可能被认定为无效，其风险由投标人自行承担。

10.3 投标人应认真了解本次招标的具体工作要求、工作范围以及职责，了解一切可能影响投标报价的资料。一经中标，不得以不完全了解项目要求、项目情况等为借口而提出额外补偿等要求，否则，由此引起的一切后果由中标人负责。

10.4 投标人应按照招标文件规定的日程安排，准时参加项目招投标有关活动。

11．招标文件的澄清和修改

11.1 在投标截止时间 15 日前，招标人可以根据项目的需要对招标文件进行必要的澄清或者修改，通过“上海政府采购网”以澄清公告形式发布,并且通过电子邮件发送给已下载招标文件的所有供应商。如果澄清或者修改的内容可能影响投标文件编制的，且澄清公告发布时间距投标截止时间不足 15 天的，则应相应延长投标截止时间。延长后的具体投标截止时间以最后发布的澄清公告中的规定为准。

11.2 招标文件的澄清和修改内容为招标文件的组成部分，当招标文件与澄清公告就同一内容的表述不一致时，以最后发出的文件内容为准。澄清公告与招标文件具有同等的法律效力。

11.3 招标文件的澄清、答复、修改或者补充都由招标人以澄清公告的形式发布和通知，除此以外的其他任何澄清、修改的方式以及澄清、修改的内容均属无效，不得作为投标依据，否则，由此导致的风险由投标人自行承担，招标人不承担任何责任。

11.4 招标人召开开标前答疑会的，投标人应根据招标文件或者招标人通知的要求参加答疑会。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。

12．踏勘现场

12.1 招标人组织踏勘现场的，投标人应按《投标人须知》前附表规定的时间、地点前往参加踏勘现场活动。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。招标人不组织踏勘现场的，投标人可自行决定是否踏勘现场，投标人需要踏勘现场的，招标人应为投标人踏勘现场提供一定方便，投标人进行现场踏勘时应当服从招标人安排。

12.2 投标人踏勘现场发生的费用由其自理。

12.3 招标人在现场介绍情况时，应当公平、公正、客观，不带任何倾向性或误导性。

12.4 招标人在踏勘现场中口头介绍的情况，除招标人事后形成书面记录、并以澄清或修改公告的形式发布、构成招标文件的组成部分以外，其他内容仅供投标人在编制投标文件时参考，招标人不对投标人据此作出的判断和决策负责。

三、投标文件的编制

13．投标的语言及计量单位

13.1 投标人提交的投标文件以及投标人与招标人就有关投标事宜的所有来往书面文件均应使用中文。除签名、盖章、专用名称等特殊情形外，以中文以外的文字表述的投标文件视同未提供。

13.2 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，一律采用中华人民共和国法定计量单位（货币单位：人民币元）。

14．投标有效期

14.1 投标有效期从提交投标文件的截止之日起算，在《投标人须知》前附表规定的投标有效期内有效。投标有效期比招标文件规定短的属于非实质性响应，将被认定为无效投标。

14.2 在特殊情况下，在原投标有效期期满之前，招标人可书面征求投标人同意延长投标有效期。投标人可拒绝接受延期要求而不会导致投标保证金被没收。同意延长投标有效期的投标人需要相应延长投标保证金的有效期，但不能修改投标文件。

14.3 中标人的投标文件作为项目合同的附件，其有效期至中标人全部合同义务履行完毕为止。

15．投标文件构成

15.1 投标文件由商务响应文件、技术响应文件和相关证明文件三部分构成。

15.2 商务响应文件、技术响应文件和相关证明文件所应包含的内容，以第四章《招标需求》规定为准。

15.3 电子采购平台对投标文件包含的内容和格式有相关规定的，应按照电子采购平台的规定办理并以其规定为准。

16．商务响应文件

16.1 商务响应文件包括但不限于以下部分：

（1）《投标函》；

（2）《开标一览表》（以电子采购平台设定为准）；

（3）《报价明细表》（详见第六章）；

（4）《资格条件响应表》、《实质性要求响应表》；

（5）《与评标有关的投标文件主要内容索引表》；

（6）法人代表授权委托书（详见第六章）；

（7）投标人基本情况简介（详见第六章）；

（8）中小企业声明函（中小企业提供）；

（9）《中华人民共和国政府采购法》第二十二条规定需要提交的材料；

（10）相关证明文件（投标人应按照招标文件所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同）；

（11）招标文件规定需要提供的其它材料。

17．投标函

17.1 投标人应按照招标文件中提供的格式完整地填写《投标函》。投标人不按照招标文件提供的格式填写《投标函》或者填写不完整的，投标人需承担其投标在评标时因此被扣分甚至被认定为无效标的风险。

17.2 投标文件中未提供《投标函》的，为无效投标。

18．开标一览表

18.1 投标人应按照招标文件和电子采购平台招投标系统提供的投标文件格式完整地填写《开标一览表》，说明其拟提供货物和相关服务的名称、规格型号、来源地、数量、价格、交付时间、质量保证期等。

18.2 《开标一览表》是为了便于招标人开标，《开标一览表》在开标时公布。投标人未按照招标文件和电子采购平台所提供的投标文件格式完整地填写《开标一览表》或者未提供《开标一览表》导致其开标不成功的，其责任和风险由投标人自行承担。

19．投标报价

19.1 投标人应当按照国家和上海市有关行业管理服务收费的相关规定，结合自身服务水平和承受能力进行报价。投标报价应是履行合同的最终价格，除《招标需求》中另有说明外，投标报价应是投标人为提供本项目所要求的全部服务所发生的一切成本、税费和利润，包括人工（含工资、社会统筹保险金、加班工资、工作餐、相关福利、关于人员聘用的费用等）、管理、税费及利润等。

19.2 报价依据：（1）本招标文件所要求的服务内容、服务期限、工作范围和要求。（2）本招标文件明确的服务标准及考核方式。（3）其他投标人认为应当考虑的因素。

19.3 投标人提供的货物和服务应当符合国家和上海市有关法律法规和标准规范，满足合同约定的服务内容和质量等要求。投标人不得违反标准规范规定或者合同约定，通过降低货物和服务质量、减少货物和服务内容等手段进行恶性竞争，扰乱市场秩序。

19.4 除《招标需求》中说明并允许外，投标的每一种货物或服务的单项报价以及采购项目的投标总价均只允许有一个报价，任何有选择的报价，招标人对于其投标均将予以拒绝。投标报价应是固定不变的，不得以任何理由予以变更。任何可变的或者附有条件的投标报价，招标人均将予以拒绝。

19.5 投标人应按照《招标需求》的要求和招标文件中关于报价的规定进行报价。投标人应按照招标文件提供的格式完整地填写报价明细表，说明其拟提供的货物和服务的内容、数量、价格、时间、价格构成等。

19.6 投标应以人民币报价。

20.《资格条件响应表》、《实质性要求响应表》

20.1 投标人应当按照招标文件所提供的格式逐项填写并提交《资格条件响应表》和《实质性要求响应表》，以证明其投标符合招标文件规定的合格投标人资格条件及实质性要求。

20.2 投标人未按照招标文件的要求对《资格条件响应表》和《实质性要求响应表》中规定的项目内容作出响应的为无效投标。

20.3 投标文件未提供《资格条件响应表》和《实质性要求响应表》的为无效投标。

21．与评标有关的投标文件主要内容索引表

21.1 投标人应按照招标文件提供的格式完整地填写《与评标有关的投标文件主要内容

索引表》。

21.2 《与评标有关的投标文件主要内容索引表》是为了便于评标。《与评标有关的投标文件主要内容索引表》与投标文件其他部分就同一内容的表述应当一致，不一致时将按照《投标人须知》第 32 条“投标文件错误的修正”的规定处理。

22．投标文件编制的响应性

22.1 技术响应文件

①投标人应按照《招标需求》的要求编制并提交技术响应文件，对招标人的技术需求应全面完整地做出响应并编制项目组织方案，以证明其投标的货物和服务符合招标文件规定。

②技术响应文件可以是文字资料、表格、图纸和数据等各项资料，其内容包括但不限于人力、物力等资源的投入以及服务内容、方式、手段、措施、质量保证及建议等。

22.2 相关证明文件

投标人应按照《招标需求》所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同。

23．投标文件的编制和签署

23.1 投标人应在上海政府采购网下载电子招标文件，使用上海政府采购网提供的客户端投标工具编制投标文件，并使用其数字证书进行电子签名。

23.2 投标人应按照招标文件和电子采购平台规定的内容、格式和顺序编制投标文件。凡招标文件提供有相应格式的，投标文件均应完整地按照招标文件提供的格式打印、填写并按要求在网上投标系统上传。投标文件内容不完整、格式不符合导致投标文件被误读、漏读或者查找不到相关内容的，由投标人自行负责，投标人需承担其投标在评标时因此被扣分甚至被认定为无效标的风险。

23.3 投标人应按照招标文件和电子采购平台的格式要求填写相关内容。投标文件中凡是招标文件要求签署、盖章之处，均应由投标人的法定代表人或法定代表人正式授权的代表签署和加盖公章。**（不包含合同专用章、投标专用章等企业专用章）**投标人应写明全称。如果是由法定代表人授权代表签署投标文件，则必须按照招标文件提供的格式出具《法定代表人授权委托书》（如果投标人自拟授权书格式，则其授权书内容应当实质性符合招标文件提供的《法定代表人授权委托书》格式之内容）并将其附在投标文件中。投标文件若有修改错漏之处，须加盖投标人公章或由法定代表人或法定代表人授权的代表签字（或盖章）。投标文件因字迹潦草或表述不清所引起的后果由投标人自负。

23.4 **其中对《投标函》、《开标一览表》、《法定代表人授权委托书》、《资格条件响应表》以及《实质性要求响应表》，投标人未按照上述要求加盖公章的，其投标无效。若《法定代表人授权委托书》中没有法定代表人签字或者盖章的，投标人投标无效。**

23.5 建设节约型社会是我国落实科学发展观的一项重大决策，也是政府采购应尽的义务和职责，需要政府采购各方当事人在采购活动中共同践行。目前，少数投标人制作的投标

文件存在编写繁琐、内容重复的问题，既增加了制作成本，浪费了宝贵的资源，也增加了评审成本，影响了评审效率。为进一步落实建设节约型社会的要求，提请投标人在制作投标文件时注意下列事项：

（1）评标委员会主要是依据投标文件中技术、质量以及售后服务等指标来进行评定。因此，投标文件应根据招标文件的要求进行制作，内容简洁明了，编排合理有序，与招标文件内容无关或不符合招标文件要求的资料不要编入投标文件。

（2）投标文件应规范，应按照规定格式要求规范填写，扫描文件应清晰简洁、上传文件应规范。

四、投标文件的递交

24．投标文件的递交

24.1 投标人应按照招标文件规定，在电子采购平台中按要求填写和上传所有投标内容。投标的有关事项应根据电子采购平台规定的要求办理。由于投标人的原因造成其投标文件未能加密而导致投标文件在开标前泄密的，由投标人自行承担责任。

24.2 投标文件中含有公章，防伪标志和彩色底纹类文件（如《投标函》、营业执照、身份证、认证证书等）应清晰显示。如因上传、扫描、格式等原因导致评审时受到影响的，由投标人承担相应责任。招标人可以要求投标人提供文件原件进行核对，投标人须按时提供，否则投标人须接受可能对其不利的评标结果，招标人将对该投标人进行调查，如发现有弄虚作假或者欺诈行为的，按有关规定处理。

24.3 投标文件中投标人营业执照（或事业单位、社会团体法人证书）、税务登记证等证明材料应清晰显示，如果因文件上传、扫描不清晰等原因导致《资格条件响应表》和《实质性要求响应表》所列项目内容不能进行审查的为无效投标。

24.4 投标人应充分考虑到网上投标可能发生的技术故障、操作失误和相应风险。对因网上投标的任何技术故障、操作失误造成投标人的投标内容缺漏、不一致或者投标失败的，招标人不承担任何责任。

24.5 **投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在电子采购平台上的签收情况，打印签收回执，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。**

25．投标截止时间

25.1 投标人必须在《投标邀请（招标公告）》规定的网上投标截止时间前将投标文件在电子采购平台上传并正式投标。

25.2 在招标人按《投标人须知》的规定酌情延长投标截止期的情况下，招标人和投标人受投标截止期制约的所有权利和义务均应延长至新的截止时间。

25.3 在投标截止时间后上传的任何投标文件，招标人均将拒绝接收。

25.4 投标截止与开标时间均以电子采购平台显示的时间为准。

26．投标文件的修改和撤回

（1）在投标截止时间之前，投标人可以对在电子采购平台电子招投标系统已提交的投标文件进行补充、修改或者撤回，并书面通知采购人或者采购代理机构。有关事项应根据电子采购平台规定的要求办理。

（2）投标截止后，投标人不得修改或者撤回其投标。

27．串通投标的有关规定

在投标过程中有以下情形之一的，视为投标人串通投标，其投标无效：

（一）不同投标人的投标文件由同一单位或者个人编制；

（二）不同投标人委托同一单位或者个人办理投标事宜；

（三）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；

（四）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；

（五）不同投标人的投标文件相互混装；

（六）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。

28．其他投标无效的规定

投标人存在下列情况之一的，投标无效：

（一）未按照招标文件的规定提交投标保证金的；

（二）投标文件未按招标文件要求签署、盖章的；

（三）不具备招标文件中规定的资格要求的；

（四）报价超过招标文件中规定的预算金额或者最高限价的；

（五）投标文件含有采购人不能接受的附加条件的；

（六）法律、法规和招标文件规定的其他无效情形。

五、开标

29．开标

29.1 招标人将按《投标邀请》或《延期公告》（如果有的话）中规定的时间在电子采购平台上组织公开开标。

29.2 开标程序在电子采购平台进行，所有上传投标文件的投标人应登录电子采购平台参加开标。开标主要流程为签到、解密、公布开标结果，每一步骤均应按照电子采购平台的有关规定操作。

29.3 投标截止，电子采购平台显示开标后，投标人应进行签到操作，在签到完成后由招标人解除电子采购平台对投标文件的加密。投标人应在规定时间内使用数字证书对其投标文件解密。**投标人签到和解密的操作时长分别为60分钟，投标人应在规定时间内完成签到和解密操作，逾期未完成的，视为放弃投标（但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者解密的除外）。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。**

29.4 投标文件解密后，电子采购平台根据投标文件中《开标一览表》的内容自动汇总生成《开标记录表》。投标人应及时使用数字证书对《开标记录表》的内容进行签名确认，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。投标人未参加开标的，视同其认可开标结果。

29.5 开标结束后，招标人根据《资格条件响应表》内容对投标文件进行资格性审查，审查每份投标文件是否满足投标人资格要求。若合格投标人不足 3 家的，不得评标。

六、评标

30. 评标委员会

30.1 招标人将依法组建评标委员会，评标委员会由采购人代表和上海市政府采购评审专家组成，其中专家的人数不少于评标委员会成员总数的三分之二。

30.2 评标委员会负责对投标文件进行评审和比较，并向招标人推荐中标候选人。

31. 投标文件符合性审查

31.1 在详细评标之前，评标委员会要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。实质性响应是指投标文件与招标文件要求的条款、投标人资格、条件和规格相符，没有招标文件所规定的无效投标情形。评标委员会只根据投标文件本身的内容来判定投标文件的响应性，而不寻求外部的证据。

31.2 没有实质性响应招标文件要求的投标文件不参加进一步的评审，投标人不得通过修正或者撤销不符合要求的偏离或保留从而使其投标成为实质上响应的投标。

31.3 开标后，招标人将拒绝投标人主动提交的任何澄清与补正。

31.4 招标人可以接受投标文件中不构成实质性偏差的小的不正规、不一致或不规范的内容。但是《评标方法与程序》中有规定的，在评标时则根据规定对其进行扣分。

★32. 异常低价投标审查

32.1 项目评审中出现下列情形之一的，评标委员会应当启动异常低价投标审查程序：

（1）投标报价低于全部通过符合性审查供应商投标报价平均值 50%的，即投标报价<全部通过符合性审查供应商投标报价平均值×50%；

（2）投标报价低于通过符合性审查的次低报价供应商投标报价 50%的，即投标报价<通过符合性审查的次低报价供应商投标报价×50%；

（3）投标报价低于采购项目最高限价 45%的，即投标报价<采购项目最高限价×45%；

（4）评审委员会基于专业判断，认为供应商报价过低，有可能影响产品质量或者不能诚信履约的其他情形。

32.2 评标委员会启动异常低价投标审查后，应当要求相关供应商在评审现场合理的时间内提供书面说明及必要的证明材料，对投标价格作出解释。书面说明、证明材料主

要是项目具体成本测算等与报价合理性相关的说明、材料。

32.3 如果投标人不能在评标委员会规定的时间内提供书面说明、证明材料，或者提的书面说明、证明材料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。

33．投标文件错误的修正

33.1 投标文件中若出现以下前后不一致和矛盾之处，按照下列规定进行修正：

（1）电子采购平台自动汇总生成的《开标记录表》内容与投标文件中的《开标一览表》内容不一致的，以《开标记录表》内容为准；

（2）投标文件中“开标一览表”内容与“报价明细表”及投标文件其它内容不一致的，以“开标一览表”内容为准；

（3）大写金额和小写金额不一致的，以大写金额为准；

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

（5）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；

（6）对投标文件中不同文字文本的解释发生异议的，以中文文本为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按规定经投标人确认后产生约束力，投标人不确认的，其投标无效。

33.2 投标文件中如果有其他错误或矛盾，将按不利于出错投标人的原则进行处理，即对于错误或者矛盾的内容，评标时按照对出错投标人不利的情形进行评分；如出错的投标人中标，签订合同时按照对出错投标人不利、对采购人有利的条件签约。

33.3 上述修正或处理结果对投标人具有约束作用。

34．投标文件的澄清

34.1 为了对投标文件审查、评价和比较，评标委员会可分别要求投标人对其投标文件中含义不明确、同类问题表述不一致或者有明显的文字和计算错误的内容等问题进行澄清。投标人应按照招标人通知的时间和地点派授权代表向评标委员会作出说明或者答复。

34.2 投标人的澄清、说明或者补正应采用书面形式（加盖公章），由法定代表人或者其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件范围或者改变投标文件的实质性内容。投标人的澄清文件是其投标文件的组成部分。

35．投标文件的评价与比较

35.1 评标委员会只对被确定为实质上响应招标文件要求的投标文件进行评价和比较。

35.2 评标委员会根据《评标方法与程序》中规定的方法进行评标，并向招标人提交书面评标报告和推荐中标候选人。

35.3 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；若评审得分相同的，由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，

招标文件未作规定的，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。

36．评标的有关要求

36.1 评标委员会应当公平、公正、客观，不带任何倾向性，评标委员会成员及参与评标的有关工作人员不得私下与投标人接触。

36.2 评标过程严格保密。凡是属于审查、澄清、评价和比较有关的资料以及授标建议等，所有知情人均不得向投标人或其他无关的人员透露。

36.3 任何单位和个人都不得干扰、影响评标活动的正常进行。投标人在评标过程中所进行的试图影响评标结果的一切不符合法律或招标规定的活动，都可能导致其投标被拒绝。

36.4 招标人和评标委员会均无义务向投标人做出有关评标的任何解释。

七、定标

37．确认中标人

除了《投标人须知》第 39 条规定的招标失败情况之外，采购人将根据评标委员会推荐的中标候选人及排序情况，依法确认本采购项目的中标人。

38．中标公告及中标、未中标通知

38.1 采购人确认中标人后，招标人将在两个工作日内通过“上海政府采购网”发布中标公告，公告期限为一个工作日。

38.2 中标公告发布后，招标人将及时向中标人发出《中标通知书》通知中标。向其他未中标人发出《中标结果通知书》，《中标通知书》对招标人和投标人均具有法律约束力。

38.3 **在公告中标（成交）结果的同时，未中标人的法定代表人携带本人身份证或法定代表人的授权代表携带《法定代表人授权委托书》、本人身份证可至上海市青浦区政府采购中心领取本投标人的未中标告知单（内容包括资格审查、符合性审查的情况及被认定为无效投标（响应）的原因、评审得分与排序，评标委员会的总体评价）。**

39．投标文件的处理

所有在开标会上被接受的投标文件都将作为档案保存,不论中标与否，招标人均不退回投标文件。

40．招标失败和终止招标活动

1、招标失败。在投标截止后，参加投标的投标人不足三家的；或者在评标时发现符合专业条件的投标人或者对招标文件做出实质响应的投标人不足三家的，由评标委员会确定为招标失败的，招标人将通过“上海政府采购网”发布招标失败公告。

2、终止招标。

（1）因重大变故导致采购任务取消的，招标人有权在发布招标公告、资格预审公告或者发出投标邀请书后终止招标活动。

（2）终止招标的，招标人将会在原公告发布媒体上发布终止公告，以书面形式通知已获取招标文件的所有潜在投标人。已经收取投标保证金的，招标人将在终止采购活动后 5

个工作日内，退还所收取的投标保证金及其在银行产生的孳息。

八、授予合同

41．合同授予

除了中标人无法履行合同义务之外，招标人将把合同授予根据《投标人须知》第 36 条规定所确定的中标人。

42．签订合同及付款

42.1 本项目中标人与采购人应在《中标通知书》发出之日起 30 日内签订政府采购合同。

42.2 按照合同有关条款支付价款。

43．其他

43.1 招标人将对开标、评标现场进行全程录音录像。

43.2 采购云平台有关操作方法可以参考采购云平台（网址：www.zfcg.sh.gov.cn）中的**“操作须知”**专栏。

第三章 政府采购政策功能

根据政府采购法，政府采购应当有助于实现国家的经济和社会发展政策目标，包括保护环境，扶持不发达地区和少数民族地区，促进中小企业发展等。

列入财政部、发展改革委发布的《节能产品政府采购品目清单》中强制采购类别的产品，按照规定实行强制采购；列入财政部、发展改革委、生态环境部发布的《节能产品政府采购品目清单》和《环境标志产品政府采购品目清单》中优先采购类别的产品，按规定实行优先采购。

中小企业按照《政府采购促进中小企业发展管理办法》享受中小企业扶持政策，对预留份额项目专门面向中小企业采购，对非预留份额采购项目按照规定享受价格扣除优惠政策。中小企业应提供《中小企业声明函》。享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

在政府采购活动中，监狱企业和残疾人福利性单位视同小微企业，监狱企业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，残疾人福利性单位应当提供《残疾人福利性单位声明函》。

政府采购活动中既有本国产品又有非本国产品参与竞争的，依法对本国产品给予价格评审优惠。

如果有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。

第四章 招标需求

一、项目概述、项目需求及目标要求

青浦区消防救援支队组网及安全加固项目
技术需求

2026 年 04 月

目 录

1. 项目背景

为大力推进上海市“十四五”时期消防救援信息化工作，进一步提升全总队互联网和电子政务外网的稳定性、安全性和可靠性，上海市消防救援总队提出较高的网络安全工作基本要求。

基础网络是总队各单位开展信息化工作的基础，管控是网络工作的关键性一环。总队各单位要着力加强网络安全制度建设、着力深化网络安全日常管理、着力强化网络安全监督检查，为网络工作提供制度保障，为网络基础设施提供支撑，为网络安全工作提供监督指导。

青浦消防救援支队积极响应总队指导意见，对支队机关及各基层队站的电子政务外网安全接入进行安全加固设计。满足分级接入、分级管理、分级负责的模式要求，另外针对现状进行差距分析，完善安全建设，保障业务安全运行。

2. 项目现状

青浦区消防救援支队现有两套网络系统，分别为消防指挥网和政务外网。两个网段物理隔离，其中消防指挥网用于访问市区两级的消防指挥调度系统的各类指挥作战应用，政务外网用于访问青浦消防信息网相关日常业务应用。

政务外网区域具体包括 3 部分：支队接入区、中队接入区、电子政务外网接入区。

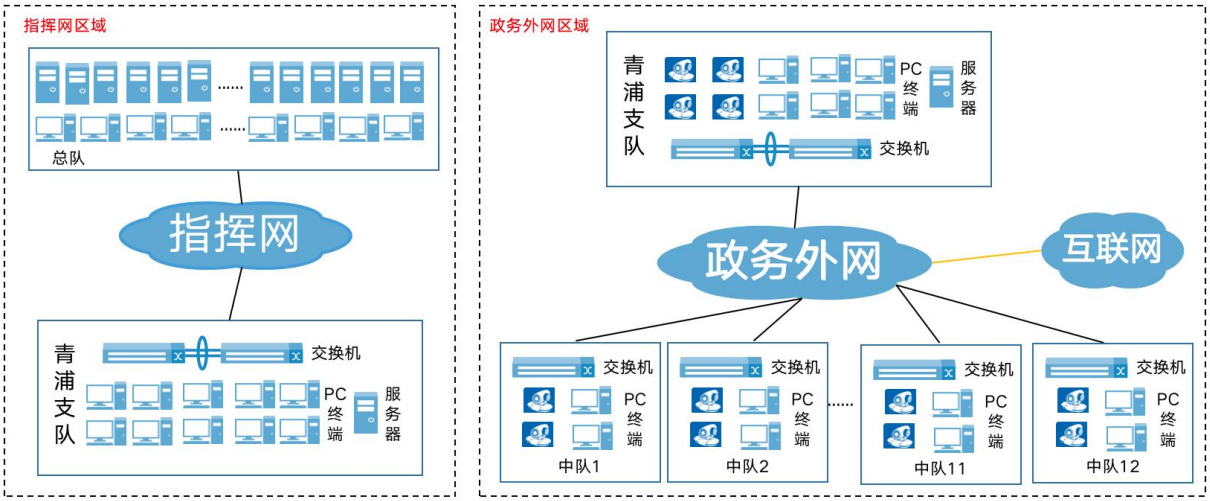
支队接入区：定位于为青浦消防救援支队终端服务器提供网络接入服务建立的区域。

中队接入区：定位于为消防救援支队下辖的各个基层消防中队终端提供网络接入服务建立的区域。

电子政务外网接入区：定位于为各级支队、中队用户提供对政务外网安全访问而设立的区域。

因支队和 12 个基层站的日常工作数据存在交互需求，所以青浦消防救援支队和 12 个基层站分别通过本地专线接入政务外网，通过政务外网来实现两者的网络通信及数据交互。

2.1. 现有网络拓扑



2.2. 本项目涉及的 12 个消防救援中队站点

徐泾站：徐泾镇华徐公路 423 号
华新站：华新镇华隆路 1599 号
赵巷站：赵巷镇镇中路 522 号
白鹤站：白鹤镇白石公路 519 号
城北站：香花桥街道胜利路 1828 号
青安站：夏阳街道青安路 345 号-349 号
盈浦站：盈浦街道青赵路 1190 号
朱家角站：朱家角镇珠湖路 910 号
练塘站：练塘镇泖甸路 119 号
金泽站：金泽镇沪青平公路 8555 号
重固小型站：重固镇赵重公路 2268 号
崧泽站：赵巷镇秀泉路 488 号

2.3. 现有机房现状

青浦区消防救援支队现有老机房位于大楼一层约 10m² 的弱电间，因建设年代较早，设计落伍未配置防盗窃、防破坏、防水防潮、温湿度控制、电力供应、防雷击、防静电等管控措施。本项目建设完成后，需完成现有机房内设备迁移至新机房。

2.4. 现有桌面终端及服务器

青浦区消防救援支队及下属的各中队现在使用的桌面终端和服务器包含约 200 台信创 ARM 架构电脑，

电脑操作系统采用了中标麒麟 V10；1 台信创 ARM 架构服务器，操作系统采用了银河麒麟 V10。

3. 建设目标

青浦区消防救援支队的互联网和电子政务外网作为市消防整体网络的有机组成部分，属于重要的信息化基础设施，需做到架构合理、传输高效、安全可靠、管理规范，为青浦消防救援支队各级人员开展消防救援业务工作提供有力支撑。 计划通过本项目的建设，提高网络安全防护能力，为互联网和电子政务外网及时配齐先进可靠的网络及安全设施设备，科学配置符合标准的网络安全策略，修订完善规范合理的网络规章制度，补充配备业务精湛的网络人员，从而确保整个网络的高效传输和韧性抗毁，最终通过网络安全等级保护第三级测评。

4. 建设内容

4.1. 支队网络安全加固

支队网络建设为此次网络安全加固项目中的核心部分，以《网络安全等级保护基本要求》为基本要求，从安全通信网络、安全区域边界、安全管理中心、安全计算环境等多个层面对支队网络进行安全建设，使青浦区消防救援支队网络具备安全可视、持续检测、协同防御等安全能力。

设计配置下一代防火墙、物联网应用安全控制系统、日志审计、数据库审计、运维审计、安全管理平台、未知威胁防御、终端检测与响应系统、web 应用防火墙、邮件数据泄露防护系统、漏洞扫描等完整的网络安全防护系统，保障青浦区消防救援支队网络、应用、数据安全，打造多位一体的立体防御体系。

需在支队网络出口处串联部署两台下一代防火墙，双机冗余部署，形成主备模式，可以有效避免单点故障引起的业务影响。下一代防火墙需利用自身的攻击防护能力保障网络安全，支持开启 IPSec 功能，建立 IPSec VPN 加密传输隧道，实现与中队网络的虚拟专网互连，保障网络通信过程中数据的完整性和保密性。

除了办公信息通信加密外，对于营区的视频监控也要进行安全防护。在支队部署一台物联网应用安全控制系统，对接入政务外网的摄像头进行识别对比，一旦出现合规登记外的非法接入终端，智能识别，快速阻断，保障政务外网接入终端的合法性。同时对于终端的业务类型也会进行识别比对，对于非视频类业务也会阻断，保障营区接入业务的合规性。

需部署专业的日志审计设备、数据库审计设备来对重要的用户行为和重要安全事件进行审计、溯源，结合专业的安全管理平台，对网络中各个位置的安全设备进行统一的管理，实现统一的配置下发，确保各个安全设备能够充分发挥各自的作用，满足等保建设的合规性。

运维审计系统需支持主从账号全生命周期的监控和管理，降低设备管理员管理大量用户帐号的难度和工作量，并针对帐号制定统一、标准的帐号安全策略；同时还可以提供统一界面，对用户、用户组、资源、资源组进行关联授权，结合精细的安全授权策略，实现运维权限的细粒度分配，最大限度保护 IT 资源的安全。

需部署未知威胁防御设备，利用自身的多种攻击检测引擎、病毒检测引擎结合威胁情报有效识别高危攻击、病毒木马等已知威胁；通过 AI 检测引擎、沙箱检测引擎发现恶意代码变种、APT 攻击、网络异常行为等未知威胁。能够关联分析攻击日志、网络流量变化、威胁情报、第三方安全日志等数据源进行安全事件有效判定，提升告警准确性；还需针对威胁事件进行原始数据全包追溯，实现精确溯源举证。

针对 PC 类终端，还需部署终端检测与响应系统，搭建主机层面的恶意代码防护机制，对蠕虫病毒、恶意软件、勒索软件、引导区病毒、木马等恶意文件进行有效查杀，保护终端安全。

针对现有的应用服务器，需部署 web 应用防火墙，对来自外部的 Web 攻击以及篡改行为进行检测和拦截，保护服务器承载的业务的稳定、可靠。

青浦区消防救援支队日常办公中数据安全面临的主要威胁在于收发邮件过程中，将重要的敏感信息误发，从而导致重要数据外泄，设计部署专业的邮件数据泄露防护系统，在邮件数据传输过程中，对邮件协议进行数据分析、识别敏感数据、将邮件数据脱敏处理，对相关行为进行审计，保障计算环境的数据安全。

4.2. 中队网络安全加固

中队与支队在日常工作中存在数据交互需求，两者都是通过接入政务外网进行通信，在通信过程中未采用校验技术或密码技术保证数据的完整性和保密性，网络存在遭受中间人攻击、进而出现传输数据被监听和窃取的风险。依据《网络安全等级保护基本要求》，在支队和 12 个基层站互联网边界部署下一代防火墙防火墙，并在下一代防火墙在支队和 12 个基层站间建立 IPSec VPN 加密传输隧道，实现广域网虚拟专网互连，保障网络通信过程中数据的完整性和保密性。

下一代防火墙除具备访问控制、NAT 功能外，还需集成病毒防护、URL 过滤、入侵防御、链路负载均衡等多种丰富功能，支持在互联网边界阻断各类恶意软件的非法入侵，也可以通过限制用户访问存在风险的网站，从而规避网站挂马和病毒文件被下载的威胁。

同时对于支队网络中的终端电脑，需部署专业的终端安全检测与响应系统，对主机层面进行安全加固，实现对主机层面恶意代码及其他威胁攻击的安全防护。

4.3. 安全物理环境加固

为了实现机房内部安全防护、防火、供电配电、空调降温、防水、防潮、防静电以及电磁防护。配备列间空调、微模块机柜、一体化 UPS、环控系统、门禁系统等设施，保障机房设备的安全运行的同时，保证网络及应用系统稳定运行。

5. 建设原则

（1）先进性、实用性

充分考虑设备选型的先进性和实用性，设备器材均为行业内知名品牌而且成熟的产品。

（2）通用性

所选设备需具有较高的通用性，易于熟悉掌握，便于消防队员及网络安全管理员操作。

（3）高可用性

关键节点采用主备或集群部署，避免因设备升级或单点故障导致全网瘫痪。

（4）兼容性、开放性

网络设备、安全设备应具备开放的 API 接口，确保能够被统一的运维平台或态势感知平台纳管，具备横向扩展能力，能够支撑业务的突发增长或未来的数字化转型需求。

（5）国际先进性

设备选型均为行业内知名品牌，系统具备先进水平，同时考虑以后升级换代的可能。

（6）分层防御

形成“边界-网络-主机-应用-数据”的多层防线，即使某一层失效，其他层仍能提供保护。

（7）合规性

遵循行业标准及国家等级保护（等保 2.0）及 ISO 27001 等合规要求。

6. 建设依据

《中华人民共和国网络安全法》

《信息安全技术网络安全等级保护基本要求》(GB/T 22239-2019)

《信息安全技术网络安全等级保护安全设计技术要求》(GB/T 25070-2019)

《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019)

《信息安全技术网络安全等级保护测评过程指南》(GB/T 28449-2018)

《信息安全技术 网络产品和服务安全通用要求》(GB/T 39276-2020)

《信息安全技术服务器安全技术要求和测评准则》(GB/T 39680-2020)

《上海市人民政府办公厅关于印发〈上海市电子政务外网管理办法〉的通知》(沪府办〔2020〕33 号)

上海市消防救援总队关于印发《总队互联网和电子政务外网组网指导意见（试行）》的通知（沪消[2022]106 号）

上海市消防救援总队关于印发《总队 2023 年度网络安全工作方案》的通知（沪消[2023]52 号）

上海市消防救援总队保密委员会办公室关于规范电子政务外网接入方式的通知（沪消保办[2022]5 号）

7. 详细建设清单

7.1. 设备清单

设备类型	设备名称	数量	单位
基础硬件	微模块化机柜	1	套
基础硬件	列间空调	2	台
基础硬件	一体化 UPS	1	套
基础硬件	环控系统	1	套
基础硬件	门禁系统	1	套
网络设备	48 口汇聚交换机	4	台
安全设备	政务外网出口防火墙	2	台
安全设备	指挥网出口防火墙	2	台
安全设备	基层站出口防火墙	12	台
安全设备	营区视频安全设备	1	台
安全设备	日志审计	2	台
安全设备	数据库审计	1	台
安全设备	运维审计	1	台
安全设备	安全管理平台	1	套
安全设备	未知威胁防御设备	1	台
安全设备	流量探针	1	台
安全设备	终端检测与响应系统	1	套
安全设备	WEB 应用防火墙	1	台
安全设备	邮件数据泄露防护系统	1	台
安全设备	漏洞扫描	1	台

7.2. 技术参数需求描述

7.2.1. 微模块化机柜

1. 机柜载荷：应具备静态载荷需≥2000Kg，动态载荷≥1100kg；
2. 机柜配重：机柜配重不低于 300kg 工况下，机柜需通过 8、9 烈度抗震测试；
3. 微模块：微模块需采用全密封系统；
4. 机柜尺寸：采用一体化框架设计结构；
5. 机柜门：微模块需用封闭冷通道形式，机柜应采用前门为单开玻璃门，后门为单开网孔门；
6. 机柜立柱：机柜立柱显示 U 位数标识，机柜后部两侧配置竖直理线板；
7. 机柜告警：机柜内有隐藏式弹门装置，并可高温告警联动，具备通道高温告警自动弹门功能；
8. 氛围灯：机柜内部具备氛围灯灯光颜色与状态联动功能,可通过系统告警状态（监控系统各类告警）、

变化显示不同颜色；

9. 传感器：需配置机柜门状态传感器；

10. LED 照明：机柜后部需配置 LED 照明系统，可根据对应门的开关状态来自动点亮或熄灭。

7.2.2. 列间空调

1. 空调设计：采用列间设计，安装简单、便于维护；

2. 空调性能：空调制冷量≥12.5KW，风量≥2500 m3/h，风冷型，恒温恒湿；

3. 压缩机：采用环保冷媒 R410A 制冷剂变频压缩机，并可根据实际负载散热需求在 4000W~12500W 柔性调节；

4. 加湿性能：加湿量≥1kg/h；

5. 风机系统：前后水平送回风；配置风机且风量可调；

6. 加热性能：电加热≥2kW；

7. 输入电压允许波动范围：380V±10%，在此范围内要求机组正常工作；

8. 输入频率允许波动范围：50HZ±2Hz，在此范围内要求机组正常工作；

9. 温湿度控制功能：应能按要求自动调节单排式微模块柜内温度，具有制冷、加热、加湿、除湿功能；

10. 送风温度调节范围：+18℃+32℃；回风温度调节范围：+18℃+38℃；相对湿度调节范围：40~70%RH。温度调节精度：1℃；相对湿度调节进度 5%。温度波动超限应能发出报警信号；

11. 控制系统：应具有微处理控制器，具有过压 、欠压等报警及故、障诊断，告警记录功能，自动保护，自动恢复，自动重启动等功能；应具备来电延时自启动功能，延时时间 1～240s 可设；应可通过布置在单排式微模块内发热量较高位置的传感器采集到的温湿度数据，联动关闭或开启压缩机、室内风机；

12. 排水方式：兼容上、下排水，支持强排水；

13. 漏水检测：空调机组配置漏水检测装置。

7.2.3. 一体化 UPS

1. 主机容量为 20kVA 的 UPS；

2. 输入电压 304-456 VAC；频率范围（50±4）Hz；

3. 输入功率因数（100％负载）≥0.9；

4. 输入谐波电流总含量（100％负载）＜5%；

5. 输出电压：220V/230V/240VAC 或 380/400/415VAC±1%；

6. 微模块设计：采用机架式配电组合形式，各配电单元均模块化设计，机架安装便于维护。配电包含市电配单单元、UPS 配电单元、PDU 配电单元放置于设备柜内；

7. 配电单元适配 UPS 容量：20kVA；

8. 市电配电单元：机架式安装，高度≤7U；总输入空开容量三相 380V/160A,应标配智能电量仪，应能监测市电主路电流、电压；含模块内空调配电 40A/3P*2；备用输出：32A/1P*1；标配 C 级防雷模块，带防雷空开；

9. UPS 配电单元：机架式安装，高度≤3U；UPS 输入开关：80A/3P*1；UPS 输出：63A/3P*1；维修旁路开关：63A/4P*1；

10. PDU 配电单元：机架式安装，高度≤6U；支路开关：32A/1P*18*；备用输出：32A/3P*1；含 UPS 配电连接线缆。

7.2.4. 环控系统

1. 硬件规格：监控主机配置触控一体屏，实现设备数据采集和界面展示功能，屏幕尺寸不小于 15.6 英寸，具备多种通讯串口，接口数量及类型不小于：2 路 RS232 接口、6 路 RS485 接口、6 路 DI 接口、4 路无源 DO、2 路有源 DO、6 路 DC12V 输出接口、 2 路 10/100M 以太网口；

2. 短信猫功能：监控主机具备短信猫功能，内置全网通 4G 模块；

3. 系统架构：采用 B/S 架构，无须安装客户端软件，通过浏览器即可访问，支持在 web 界面增删设备和修改名称；

4. 交互界面：系统应具有良好的人机界面，内置 3D 引擎，基于微模块实际设备进行可视化建模，3D 模型支持放大、缩小，自动旋转等操作；

5. 监控管理界面：系统针微模块 UPS、配电、空调、环境、能耗等具备独立的监控管理界面；根据设备类型，呈现相应的概览信息展示界面；具备曲线趋势分析功能，展现微模块供电电压、环境温湿度曲线等；

6. 告警功能：系统告警功能齐全，具备告警级别管理、告警确认、告警定位、告警时间、告警弹窗等功能；具备多种告警通知方式，支持声光、短信、邮件告警通知功能；支持自定义告警通知人员，方便管理；

7. 联动功能：系统具备联动功能，支持设置消防报警门禁常开、声光告警等联动规则；联动控制逻辑可自定义编辑，采用策略组态模式，支持用户自定义设置联动关系。

8. 报表功能：系统提供报表功能，支持查询导出告警报表、历史数据报表、操作日志等；告警报表内容包含告警级别、告警设备、告警名称、开始/结束时间等；历史数据报表支持设置时间段、筛选信号进行查询；

9. 权限管理和日志记录：系统需具备权限管理和日志记录功能，支持设置账号权限，包括查看、控制、设置参数等；支持系统操作日志和登录日志记录，可设置筛选条件生成报表导出。

10. 开放性接口：系统内置开放性接口，支持 MQTT、SNMP、运营商 B/C 接口等协议，能够对接管理平台。

7.2.5. 门禁系统

1.设备机柜内有隐藏式弹门装置，并可高温告警联动，具备通道高温告警自动弹门功能。

2.机房进户门需配置钢制防火门，安装多因子门禁控制器，支持人脸及密码认证，人脸数量不低于 10000 张；

3.配置自动闭门器。

7.2.6. 48 口汇聚交换机

1. 交换容量和转发性能：交换容量≥2.4Tbps，整机转发性能≥660Mpps；

2. 硬件规格：固化千兆电口≥48 个，万兆光口≥6 个；额外提供扩展槽位≥1 个，设备高度≤1U，支持可插拔冗余双电源；

3. 环境适应能力：为保障设备环境适应能力，设备支持 0-70℃宽温工作；

4. 功耗：为节能环保考虑，设备最大功耗不超过 70W；

5. ACL：支持基于 VLAN、MAC 地址、IP 地址、TCP/UDP 端口号等 ACL；

6. MAC：支持静态、动态、黑洞 MAC 表项；支持源 MAC 地址过滤；

7. VLAN：支持 4K 802.1Q VLAN；支持基于 MAC/ IP 子网/认证策略/端口的 VLAN；支持 Voice VLAN；支持 QinQ；

8. 端口功能：支持端口聚合、端口镜像、端口隔离；

9. VXLAN：支持 VXLAN 二层交换；支持 VXLAN 路由交换；支持 VXLAN 网关；支持 EVPN 分布式网关；支持 VxLAN 集中控制平面；

10. 虚拟化：支持多虚一虚拟化技术，将多台物理设备虚拟化为 1 台逻辑设备；

11. 路由表：OSPF 路由表容量≥12K；

12. 管理界面：支持中文管理界面、WEB 管理接口。

7.2.7. 政务外网出口防火墙

1. 性能要求：整机网络层吞吐量（双向）：IPv4≥40Gbps；整机应用层吞吐量（单向）：IPv4≥25Gbps；整机 TCP 新建：IPv4≥30 万/秒；整机 TCP 并发：IPv4≥1200 万；

2. 硬件规格：设备万兆光口≥12 个、千兆电口≥16 个，40G 接口≥2 个，扩展槽位≥2 个，设备高度≤1U，冗余电源；

3. 特征库：实配 3 年 IPS 特征库升级服务，以及 100 个 SSL VPN 授权；

4. ▲故障分析：支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查（需提供具备 CNAS 标识的第三方检测报告）；

5. 安全策略：支持基于不同安全策略设定会话长连接老化时间；

6. ▲虚拟化：支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备（需提供具备 CNAS 标识的第三方检测报告）；

7. 虚拟化：支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的 CPU 和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙；

8. 访问控制策略：访问控制策略支持基于源/目的 IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式；

9. 路由协议：支持静态路由、等价路由，支持 RIP、RIPng；OSPFv2/v3 动态路由协议；

10. 地址转换：支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源 IP 或者目的 IP 进行连接数控制；

11. 攻击防护：支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护；

12. 攻击防护：支持 SYN Flood、ICMP Flood、UDP Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；

13. 状态同步：双机支持 A/S，A/A 方式部署，支持配置同步，会话同步和用户状态同步；

14. 攻击防护：支持对信任区域主机外发的异常流量进行检测，如 ICMP，UDP，SYN，DNS Flood 等 DDoS 攻击行为；

15. 攻击防护：提供命令注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护。

7.2.8. 指挥网出口防火墙

1. 性能要求：整机网络层吞吐量（双向）：IPv4≥10Gbps；整机应用层吞吐量（单向）：IPv4≥6Gbps；整机 TCP 新建：IPv4≥23 万/秒；整机 TCP 并发：IPv4≥500 万；

2. 硬件规格：设备千兆光口≥2 个、千兆电口≥8 个，扩展槽位≥2 个，设备高度≤1U，支持双电源；

3. 特征库：实配 3 年 IPS 特征库升级服务，以及 10 个 SSL VPN 授权

4. ▲故障分析：支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查（需提供具备 CNAS 标识的第三方检测报告）；

5. 安全策略：支持基于不同安全策略设定会话长连接老化时间；

6. ▲虚拟化：支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备（需提供具备 CNAS 标识的第三方检测报告）；

7. 虚拟化：支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的 CPU 和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙；

8. 访问控制策略：访问控制策略支持基于源/目的 IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式；

9. 路由协议：支持静态路由、等价路由，支持 RIP、RIPng；OSPFv2/v3 动态路由协议；

10. 地址转换：支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源 IP 或者目的 IP 进行连接数控制；

11. 攻击防护：支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护；

12. 攻击防护：支持 SYN Flood、ICMP Flood、UDP Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测；

13. 状态同步：双机支持 A/S，A/A 方式部署，支持配置同步，会话同步和用户状态同步；

14. 攻击防护：支持对信任区域主机外发的异常流量进行检测，如 ICMP，UDP，SYN，DNS Flood 等 DDoS 攻击行为；

15. 攻击防护：提供命令注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护。

7.2.9. 基层站出口防火墙

1. 硬件要求：规格：1U，不少于 6 个千兆电口，内存 8GB，硬盘总容量不小于 128GB SSD；

2. 性能要求：网络层吞吐量≥10Gbps，IPS 吞吐量≥1 Gbps，防病毒吞吐量≥1Gbps，全威胁吞吐量≥800Mbps,并发连接数≥400 万，HTTP 新建连接数≥10 万；

3. 网络要求：支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于 3 种的调度算法，至少包括带宽比例、加权流量、线路优先等；支持 IPv4/IPv6 双栈工作模式，以适应 IPv6 发展趋势；支持基于应用、服务、时间、域名、IPv6 对象等维度的访问控制；

4. 应用控制：支持对不少于 8000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；

5. ▲防病毒：应具备独立的勒索防护模块，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略（需提供设备功能操作截图证明及关于“勒索病毒”的软件著作权证书）；

6. ▲入侵攻击防御：产品内置不低于 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则（需提供具备 CNAS 标识的第三方检测报告），实配 3 年入侵攻击防御特征库升级授权；

7. 账号安全：支持独立的账号安全防护模块，具备事前账号脆弱性、事中账号爆破、事后账号失陷的全生命周期安全防护，在设备界面可以详细展示账号安全相关信息，包括风险业务、风险等级、存在账号入口、存在弱口令、遭受口令爆破、异常登录账号登陆。

8. ▲安全策略管理：支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理（需提供具备 CNAS 标识的第三方检测报告）；

9. 日志存储与共享：支持多种安全日志存储方式，至少包括防火墙本机、日志服务器等不同方式。

支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间；支持用户自定义设置日志存储的天数或磁盘占用空间的比例；支持通过标准 SYSLOG 协议将日志传输给第三方日志平台进行集中存储与分析，日志类型包括但不局限在：应用控制日志、安全日志、流量审计日志、用户认证日志、系统操作日志、访问控制日志等。

10. 资质要求：需具备网络关键设备和网络安全专用产品安全认证证书，提供相关证书复印件；需具备 IT 产品信息安全认证证书 EAL4 增强级，提供相关证书复印件。

7.2.10. 营区视频安全设备

1. 硬件规格：设备高度≤1U，配置双电源，配置千兆电口≥8 个，万兆光口≥12 个；
2. 处理能力：处理能力：支持 300 路以上并发高清视频（4M 码流）的安全管控；
3. 传输时延：设备本身不能出现对视频业务产生如视频抖动、卡顿等现象，基于 SIP 的视/音频传输时延＜20 微秒；
4. GB 35114：支持与 GB 35114 C 级平台互联；
5. GA/T 1788.3：设备满足 GA/T 1788.3 要求，达到视频接入安全防护系统增强 II 级防护要求；
6. ▲GA/T 1788.3：设备满足 GA/T 1788.3 要求，达到设备准入控制系统防护要求（需提供具备 CNAS 标识的第三方检测报告）；
7. ▲GB35114：支持符合 GB35114 标准的终端接入检测功能，可对不符合 GB35114 的终端接入进行阻断并告警（需提供具备 CNAS 标识的第三方检测报告）；
8. GA/T 1400：支持 GA/T 1400 协议检测功能，可对不符合 GA/T 1400 协议的终端进行阻断并告警；
9. 认证：支持基于 Portal 认证的实名制违规外联检测机制，基于 portal 认证入网的设备，存在违规外联行为的终端，通讯会被阻断；支持无感知方式的违规外联检测机制，存在违规外联行为的终端，通讯会被阻断；
10. ▲历史数据重放：支持基于历史数据重放检测功能，可对存在历史数据重放攻击的终端进行阻断（需提供具备 CNAS 标识的第三方检测报告）；
11. 一机一档：支持一机一档信息双平台上报功能，可进行一机一档远程同步配置，上报成功后，可在其他平台查看一机一档信息；
12. 资产注册：支持资产注册及审批功能，资产注册用户可登录平台填写资产注册信息并提交申请，管理员用户可在申请记录中进行审批，同时支持资产注册流程可基于资产一机一档属性录入完整度下发阻断策略功能。

7.2.11. 日志审计

1. 硬件规格：设备高度≤2U，CPU≥8 核，内存≥16G，硬盘容量≥2T，千兆电口≥8 个，千兆光口≥4 个，扩展槽≥2 个；
2. 性能要求：处理性能：日志处理能力≥2000 条/秒、日志存储能力≥2.5 亿条/天；设备接入授权≥60 个；
3. 实时监控：支持实时监控功能，可实时展示接收的日志信息，并且可以根据日志名称、ip、类型等条件进行筛选展示；
4. 日志查询：支持日志查询，可根据时间、IP、安全级别等信息进行查询，可针对查询到的日志结果进行导出；

5. 审计分析策略：内置 62 种审计分析策略，包含：DDoS 攻击、Webshell 攻击、XSS 跨站脚本攻击、欺骗攻击、网络蠕虫、数据库高危操作、切换 root 用户、系统重启、硬件故障等

6. 采集对象：支持国内外主流厂商的安全设备；支持主流的路由器、交换机、负载均衡等网络设备；支持主流等操作系统；支持市场主流数据库及中间件软件；

7. 解析策略：内置 400+种标准化解析策略，包含 20000+条解析规则，支持自动将用户自定义告警、告警类型代码、内容代码、动作代码等映射至可读描述。

7.2.12. 数据库审计

1. 硬件要求：设备高度≤2U，千兆电口≥6 个，千兆光口≥4 个，扩展槽≥2 个；

2. 性能要求：网络吞吐≥2G，数据库吞吐量≥200Mb/秒，数据库处理能力≥10000 条/秒、入库量≥10000 条/秒；并发会话数≥500；

3. 数据库兼容性：支持市场主流具有知识产权的数据库；

4. 自动发现：支持自动发现网络中存在的数据库，并自动添加成审计对象进行审计，简化操作，避免配置故障；

5. 系统过滤：支持驱动及 IP 过滤，在流量进入网卡之前对网络流量进行扫描，对无用的信息从网络层进行过滤；

6. 系统过滤：支持添加系统语句规则来过滤系统语句，根据系统语句定义规则进行应用层过滤；

7. 审计策略：支持数据库操作命令、语句长度、语句执行回应、返回内容、返回行数、数据库名、应用账户、服务器端口、客户端 MAC、客户端 IP、客户端端口、会话 ID、关键字、时间等响应条件的审计策略；

8. 内置规则库：支持内置疑似命令注入、字段猜测、代码更改、等风险审计规则库，原厂提供 3 年规则库升级授权；

9. 审计规则：支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警；

10. 回溯事件：根据事件的时间范围、客户端 IP、关键字、进程名、应用账号、规则名、客户端端口号、返回内容等多种条件进行事件回放，回溯事件过程；

11. 资产智能发现：支持基于网络流量的资产发现功能，能够发现数据库表和资源账号，其中数据库表的自动发现支持表名、数据库名、发现次数和发现日期，资源账号自动发现支持在线天数、首次发现日期、末次发现日期。

7.2.13. 运维审计

1. 硬件要求：设备高度≤2U；CPU≥8 核，内存≥16G，硬盘容量≥2T，千兆电口≥6 个，千兆光口≥4，扩展槽≥2 个；

2. 性能要求：处理性能：最大字符连接≥50 个，最大图形连接≥25 个；设备管理授权≥60 个；

3. 部署方式：支持物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构；系统各模块支持以 B/S 方式管理，采用 https 加密方式访问；

4. 支持协议：支持 SSHv2、TELNET 等字符协议；支持 RDP、VNC 等图形协议；支持 FTP、SFTP、RDP 磁盘映射、RDP 剪切板等文件传输协议；支持通过协议前置机进行协议扩展，可支持扩展数据库、http/https、C/S 架构 应用等；

5. 动作流：支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，

通过动作流配置即可实现单点登陆和审计接入；

6. 用户管理：支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期；

7. 口令策略：可以配置口令长度，是否包含字母及字母的长度，是否包含数字及数字的长度，是否包含符号及符号的长度，口令时效性，口令策略还可配置禁止包含的关键字；

8. 改密计划：支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度，口令变更方式支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式；

9. 访问控制：支持命令黑名单，对字符型设备的高危命令执行进行阻断，如 rm、shutdown、reboot 等；

10. 运维方式：支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用客户端工具实现单点登陆，不改变运维人员操作习惯；

11. 备份与维护：支持手动和自动定期备份配置信息，支持配置信息本地备份及异地 FTP 备份；支持系统配置还原，可以还原至任一备份点；

12. 智能管理：支持 NTP 系统时间同步配置，保证系统拥有可靠的时间戳；支持从 WEB 管理界面重启、关闭设备；支持通过 WEB 界面进行系统升级；支持 WEB 页面配置双机热备，保证系统可靠运行。

7.2.14. 安全管理平台

1. 基础功能：软件基础功能，包含威胁检测、分析中心、响应中心、资产中心、统计报表、仪表板、系统管理、态势感知等功能；

2. 安全场景：支持基于生成式人工智能大模型的方式，以自然语言聊天机器人的形式，统一协同人、系统、流程，对安全事件进行协同分析、协同调查、协同处置，从而提升整体网络安全运营能力；

3. 国密加密：平台系统账户密码存储支持使用国密 SM3 加密；流量传感器数据传输到平台支持使用国密 SM4 加密；日志采集器数据传输到平台支持使用国密 SM4 加密；支持使用国密浏览器访问平台，系统 HTTPS 支持国密 SM3_SM2 加密；

4. 关联规则：支持自定义关联规则，支持图形化连线拖拽的交互配置方式而非编辑逻辑语法树配置方式；提供 1100+条预置规则；支持日志关联规则建模，在指定的时间范围内，能够对来自不同数据源的日志进行关联分析，以发现可信度更高的威胁告警；

5. 工单处理：支持通过工单对安全事件进行跟踪处理，工单类型包括：通用、弱口令、告警、配置核查、漏洞、WEB 漏洞。工单流转中支持添加附件，支持 zip、rar、pdf、doc、docx、xls、、xlsx、ppt、pptx、txt、png、jpeg、、jpg 格式。工单状态包含待下发、待处置、处置中、已处置、已完成、已撤销；

6. 安全攻击预测：支持攻击技战术的预测能力，支持根据前序安全事件时间、前序攻击技术、攻击场景通过预测模型，预测下一小时和第二天发生的攻击技术和发生的整体概率。

7. 规则库：原厂提供 3 年规则库升级授权；

7.2.15. 未知威胁防御设备

1. 硬件配置：CPU ≥4 核，内存≥32GB,存储≥1T；
2. 硬件规格：千兆电口≥6 个，扩展槽≥2 个，高度≤1U，双电源；
3. 性能要求：应用层≥1.5Gbps，网络层≥3Gbps；

4. 规则库：原厂提供 3 年规则库升级授权；

5. 告警事件分析：支持告警事件分析，能够展示安全事件级别、攻击类型，源 IP、目的 IP、源端口、目的端口、源位置、目标位置情况；

6. 监测控制：支持监测控制展示，监测设备运行状态，包括但不限于设备版本、CPU 使用率、CPU 型号、内存占用率、磁盘占用率等；

7. 监测流量：支持监测流量状态，基于时间维度记录并展示流入、流出流量情况，并记录流量的总流入流出情况。支持流量监测的开关控制；

8. 沙箱分析：支持沙箱分析功能，分析结果包括但不限于文件名称、文件加密、受感染主机、威胁指数、传播次数、动态检测结果、静态检测结果、病毒检测结果。支持跳转展示沙箱分析详情，展示文件的静态检测、动态检测、病毒检测结果；

9. 上传分析：支持文件上传分析，分析维度包括但不限于文件名、文件类型、处理状态、检测结果、上传时间、检测完成时间、文件加密。支持跳转展示文件上传分析详情，展示文件的静态检测、动态检测、病毒检测结果。并支持文件下载；

10. 文件审计：支持文件审计功能，记录审计流量中流转文件的名称、类型、源 IP、目的 IP、时间、风险描述、协议类型，并支持审计文件下载、文件审计报表导出；

11. 威胁分析：支持邮件威胁分析，分析结果展示发件人、收件人邮箱地址、威胁指数、攻击类型、地址欺骗、恶意 URL 链接、敏感字。支持检测常见的邮件协议类型：SMTP、POP3、IMAP；

12. 解析还原：具备流量采集及协议解析还原能力，支持解析的协议包括但不限于 HTTP、FTP、TLS、SMB、DNS、POP3 等；

13. 病毒检测：支持多种病毒检测引擎，集成第三方专业防病毒厂商的专业病毒库，特征规则数量不少于 20000 条；

14. 边界完整性：支持边界完整性检测，可针对专网中的非法外联主机进行有效检测和定位，可检测出目标设备通过连接智能手机热点、通过智能手机 USB 共享网络、私接无线 AP、共享 Wi-Fi、以 NAT 方式接入的路由设备等方式的违规外联行为；

15. 监测大屏：设备内置 APT 监测大屏，无需配置外置日志接收及展示平台，支持展示安全告警级别分布、攻击流量 TOP、流量统计、攻击日志、威胁类型 TOP、恶意文件 TOP、源 IP、目的 IP 等；

16. 部署环境：支持 IPv4/IPv6 网络环境下的部署，支持对 IPv4/IPv6 网络的流量检测分析；

17. 综合分析：支持综合分析报告及独立的沙箱检测报告，报告分析内容包括但不限于反病毒检测分析、静态信息、网络行为分析、执行流程与截图、文件行为特征分析等。

7.2.16. 流量探针

1. 硬件要求：高度≤1U，内存 ≥16G，硬盘≥1T，千兆电口≥6 个，USB 口≥2 个；

2. 采集能力：流量采集能力≥1Gbps；

3. 规则库：原厂提供 3 年规则库升级授权；

4. 报文存储：支持全流量报文的存储，以及远程调取、查看和下载功能；

5. 镜像采集：通过旁路镜像采集网络全部流量，支持在线支持同时接入多个镜像口，每个口相互独立不影响，设备部署不影响原有网络结构；

6. 攻击检测：支持多种主机渗透攻击检测，至少包括：系统漏洞攻击、命令注入、应用程序漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、邮件漏洞攻击、文件漏洞攻击、网络设备漏洞攻击、浏览器漏洞攻击、Web 系统漏洞攻击等；

7. 攻击检测：支持多种 Web 渗透攻击检测，至少包括：命令注入、跨站脚本工具、代码注入、文件上传漏洞攻击、目录遍历攻击、文件包含漏洞攻击、服务器配置信息泄露、扫描探测、信息泄露探测等；

8. 攻击检测：支持多种类型挖矿病毒检测，至少支持 4 以上种挖矿病毒；支持多种协议的暴力破解，至少包括：SSH、FTP、POP3、SMB 等协议；支持多种数据库的漏洞攻击；

9. 协议解码：支持协议解码，至少包括： IPv4、ICMPv4、TCP、UDP、SCTP、Ethernet、PPP、PPPoE、Raw、SLL、QINQ、MPLS、GRE、ERSPAN、VLAN、VXLAN、Geneve 等；

10. 协议解析：支持应用层协议解析，能对网络通行行为识别，至少包括： HTTP、FTP、SMTP、DNS、DHCP、SSL、等行为；

11. 机器学习：支持基于机器学习的提取攻击者真实访问的 URL，全面掌握攻击者的攻击意图和访问记录，包括：攻击者 IP、攻击者 URL、访问行为的原始报文等。

7.2.17. 终端检测与响应系统

1. 系统架构：采用 B/S 架构的管理控制中心，支持跨平台统一管理，控制中心可统一接入管理网络中的具有知识产权的通用终端、以及专用终端防病毒；

2. 资产查看：支持查看全网资产的情况，包括计算机名、IP 地址、MAC 地址、操作系统、芯片类型等信息；

3. 微隔离：支持微隔离功能，能可视化的展示全网资产的网络访问关系，形成安全的安全访问控制，缩小网络暴露面；

4. 资产管理：支持资产运维和资产发现能力：可对终端资产进行关闭、重启、锁屏、结束进程、断开网络、远程协助等操作，同时可通过 ARP、PING、NMAP 三种方式对非法接入的终端资产进行探测，发现未安装客户端的终端资产；

5. 实时监测：支持对终端进行 CPU 和内存占用的资源实时监测，并可将占用和使用情况上报管控中心；

6. 查看全网：具备多维度的态势大屏，至少包括资产态势大屏、运维态势大屏、威胁态势大屏、数据安全态势大屏。展示内容至少包括威胁告警统计、攻击阶段统计、威胁等级统计、漏洞信息 Top5、终端威胁告警 Top5、敏感信息 Top5、敏感终端 Top5、最新告警事件、威胁态势评分等信息；

7. 智能分析：具备对全网终端资产进行统一管理和资产画像能力：可提供基于 AI 的智能分析，实现单个终端与全网终端的风险解读，直观展示终端资产的综合健康状态，并为用户提供合理的优化策略与处置建议；

8. 查杀引擎：本地查杀引擎:监控文件执行操作，发现有恶意进程启动时，及时告警并拦截阻止程序运行；

9. 策略任务：支持多定时任务，支持在策略中定义多个定时查杀任务；

10. 接口权限控制：支持对 USB、串口、并口等接口权限控制；

11. 敏感信息防护：支持基于关键字、正则表达式、文件指纹等方式检测终端敏感文件，并阻止敏感文件外发行为生效的能力；

12. 防止私自退出：支持支持客户端杀毒软件防非授权退出和软件自保护，可以做到防止用户私自退出安全防护，防止用户或第三方软件对安全防护软件的强退破坏。

13. 内置规则库：原厂提供 3 年规则库更新服务

7.2.18. WEB 应用防火墙

1. 性能要求：网络层吞吐量≥2.4Gbps；网络并发连接≥100 万；
2. 性能要求：HTTP 并发连接≥70 万，HTTP 新建连接数≥1.3 万；
3. 硬件规格：千兆电口≥4 个、千兆光口≥4 个，万兆光口≥2 个；
4. 规则库：实配 3 年 WAF 库；
5. 接入模式：支持透明模式、反向代理模式、单臂部署模式、插件引流模式等；
6. Web 攻击防护：支持 Web 攻击防护功能，支持 Web 业务控制防御功能；
7. 敏感信息检测：支持敏感信息检测防护，支持敏感词检测及过滤，自带敏感词库并进行可自定义,且敏感词支持导入导出；
8. 业务加固：支持 Web 业务加固防御功能，提供弱密码检测、网站语言安全、跨站请求伪造等防御功能；
9. 防暴力破解：支持防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值+动态令牌等方式
10. API 敏感数据泄漏安全防护：支持对 API 接口涉及到敏感数据进行检测与丢弃，避免 API 接口敏感数据被恶意获取，至少支持预定义 20 种以上的敏感数据识别，如身份证号、电话号码、邮箱等，支持自定义敏感数据格式识别；
11. 网页防篡改：支持网页防篡改功能，提供相应的客户端下载，支持对所有安装防篡改客户端的服务器进行集中管理，支持策略一键启用和一键关闭；
12. 智能封禁：支持智能封禁，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间；
13. 机器学习：支持机器学习功能，通过流量学习对进行业务建模，支持对 URL 的访问量和响应健康度进行图形化统计；
14. 网站安全访问控制：支持网站锁功能，在护网、节假日、国家重大会议、重保等时间节点，防护网站的安全；支持一键锁定功能，只允许访问网站禁止提交数据；同时，支持一键关停功能，网站禁止用户防护，并可返回界面提示。

7.2.19. 邮件数据泄露防护系统

1. 性能要求：处理能力≥20 万封邮件/天；
2. 硬件规格：千兆光口≥4 个，扩展口≥4 个；
3. 设计及部署模式：软硬件一体机模式，集业务平台和审计引擎于一体，支持物理旁路、逻辑串路部署，支持全邮件审计；
4. 攻击检测:系统支持邮件附件分析：使用多个检测引擎和定制化沙箱检测附件，包括多种 Windows 可执行文件、Microsoft Office、PDF、Zip、Web 内容和压缩文件类型等；
5. 威胁分析：支持沙箱分析可用于深入威胁研究和评估攻击的风险和起源；
6. 策略控制和执行：根据告警严重性级别，支持配置多种选项来处理恶意邮件，包括隔离、删除和带标记转发邮件等操作；
7. 黑白名单能力：系统在邮件安全管理方面需提供黑名单功能，用户不仅可以手动添加发件人黑名单，还能根据预设规则自动生成发件人黑名单，以有效阻断恶意邮件；
9. 附件分析和定制化沙箱：使用启发式技术和客户提供的关键词打开、解压缩和解锁附件；；
10. 密码保护附件分析：系统在处理压缩文件方面具备高度灵活性和智能性，支持用户自定义预设的解压密码集合，以适应不同场景下的解压需求；

11. 高级防护能力：系统具备多项高级功能，包括支持检测最多 20 层压缩格式的文件附件，并能识别到邮件正文、附件、图片中的二维码，进行相应处置，同时可提取嵌入在 MS office 以及 PDF 文档附件中的 URL 进行分析，也能分析邮件标题和正文中的 URL；

12. 邮件处置能力：系统提供了全面的邮件防护策略，允许用户对恶意邮件进行删除、阻止、隔离、转发等操作，以保障邮件安全；

13. 部署能力：支持分离式部署和集成部署。分离式部署下，管理端和业务端间采用安全协议进行通信；系统支持升级过程不影响业务；支持 MTA（阻止）、BCC（监控）及 SPAN/TAP（监控）部署模式可与任何现存邮件安全解决方案协同工作。

14. 内置特征库：实配 3 年特征库升级服务

7.2.20. 漏洞扫描

1. 硬件规格：设备 RJ45 串口≥1 个、USB 口≥2 个，10M/100M/1000M 自适应以太网电口≥6 个，千兆光口≥4 个，扩展槽位≥2 个；

2. 性能要求：最大并发扫描≥75 个 IP 地址，最大并发任务≥10 个任务，支持 IP 授权扫描数≥500 个；

3. 硬件规格：硬盘≥4T，设备高度≤1U；

4. 漏洞数：支持检测的漏洞数大于 400000 条，兼容 CNNVD、CNVD 等主流标准；

5. 漏洞库：支持系统漏洞库和 Web 漏洞库通过多种维度对漏洞进行检索，包括：漏洞名称、漏洞 ID、CNVD ID、CNNVD ID 编号、风险等级、是否使用危险插件、是否支持漏洞验证，漏洞发布日期、漏洞分类信息，原厂提供 3 年漏洞库升级授权；；

6. 扫描通知：支持扫描时通知被扫描主机，可自定义通知内容；

7. 弱口令检测：支持多种协议口令猜测，包括 SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM、REDIS、SMTP 等，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典；

8. Web 风险监测：支持网站风险监测，可以对网站可用性、网页变更、DNS 地址解析进行监测，实时发现网站风险；

9. 资产风险：支持资产的配置变更监测，可以根据实际情况设置任意检查结果作为变更基线，支持与自身或者其他设备的同类型变更项进行对比,周期性监测系统的文件、目录、启动项、进程等配置信息及变更状态。并支持生成配置变更监测报表；

10. 报告报表：支持对任务报表生成参数进行设置，包括自定义报表名称、报表单位、报表模板、是否生成单主机报表、安全结论、页眉、页脚和封面、并可根据漏洞风险级别、处置优先级、IP 地址进行过滤；

11. 高级数据分析：支持高级数据分析，可对同一 IP 的两次扫描结果进行风险对比分析，并可在线查看同一 IP 的多次历史扫描结果。

7.3. “▲”指标项汇总表

序号	设备名称	指标项	证明材料
1.	政务外网出口防火墙	4.▲故障分析：支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查；	需提供具备 CNAS 标识的第三方检测报告
2.	政务外网出口防火墙	6. ▲虚拟化：支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备；	需提供具备 CNAS 标识的第三方检测报告
3.	指挥网出口防火墙	4. ▲故障分析：支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查；	需提供具备 CNAS 标识的第三方检测报告
4.	指挥网出口防火墙	6. ▲虚拟化：支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备；	需提供具备 CNAS 标识的第三方检测报告
5.	基层站出口防火墙	5. ▲防病毒：应具备独立的勒索防护模块，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略；	需提供设备功能操作截图证明及关于“勒索病毒”的软件著作权证书
6.	基层站出口防火墙	6.▲入侵攻击防御：产品内置不低于 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则；	需提供具备 CNAS 标识的第三方检测报告
7.	基层站出口防火墙	8. ▲安全策略管理：支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；	需提供具备 CNAS 标识的第三方检测报告
8.	营区视频安全设备	6. ▲GA/T 1788.3：设备满足 GA/T 1788.3 要求，达到设备准入控制系统防护要求；	需提供具备 CNAS 标识的第三方检测报告
9.	营区视频安全设备	7. ▲ GB35114 ： 支 持 符 合 GB35114 标准的终端接入检测功能，可对不符合 GB35114 的终端接入进行阻断并告警；	需提供具备 CNAS 标识的第三方检测报告
10.	营区视频安全设备	10. ▲历史数据重放：支持基于历	需提供具备 CNAS 标识的

		史数据重放检测功能，可对存在历史数据重放攻击的终端进行阻断；	第三方检测报告

注：投标人提供的证明材料需加盖制造商公章。

7.4. 系统集成

投标人需独立完成本项目的设备供货、设备上架、安装、调试、软件部署、集成等工作，对本项目的建设内容和目标进行深化设计，出具项目实施所需的网络安全拓扑图、机柜布置图、路由协议图等。图纸由采购人审核通过后方可进行施工，施工期间需保护已有的建设成果，如有破坏，需按照不低于原建设标准进行修复。

1）网络安全系统集成

完成新建机房内的网络及安全设备上架、安装、调试、安全规划、配置与策略、日志采集与监控、统一平台管理；及旧机房内现有的网络及设备搬迁、上架、安装、调试、纳管。改变单点防护思维，构建分层、立体的防护体系。要求在网络边界、关键区域边界、核心资产前端均部署相应的防护设备，确保单一设备失效不会导致整体防线失守。打破设备孤岛。所有安全设备必须纳入统一的运维管理体系，实现策略的统一分发、日志的统一采集、状态的统一监控，避免出现管理盲区。

集成后的系统整体可用性通常要求达到 99.99%以上，关键链路切换时间需满足业务容忍度。集成方案应覆盖边界防护（防火墙）、入侵检测与防御（入侵防御系统/下一代防火墙）、终端接入控制、运维审计（堡垒机）、日志审计、数据库安全等。

集成方案必须满足《网络安全等级保护基本要求》中对于“安全区域边界”、“安全通信网络”和“安全计算环境”的相关技术指标。

需采用标准化部署，统一设备命名规范、接口地址规划、管理账号权限体系、日志格式标准。确保“一设备一档案，一策略一审批”。

集成过程中，若涉及现网设备替换或链路调整，必须制定详尽的割接方案与回退方案，确保对现网业务的影响降至最低。

2）机房环境集成

机房环境集成方案必须满足《网络安全等级保护基本要求》，完成新建机房配套的电子门禁、环控、精密空调、UPS 等物理运行环境的安全、调试、统一管理，出入记录必须保存 6 个月以上。机柜、服务器等主要设备必须进行物理固定（如上架固定），并设置明显且不易除去的标识。配置精密空调及温湿度传感器，支持接入环境监控系统并与精密空调实现自动化联动。

3）终端检测与响应系统集成

完成终端检测与响应系统在客户端和服务器的安装及部署，升级病毒特征库为最新版，支持对终端进程、网络连接、文件操作、注册表变更、用户登录等行为的 7×24 小时持续监测。在自主可信环境下，需深度适配国产 CPU 和操作系统内核，利用操作系统底层安全能力实现行为监测和主动防御。

8. 实施要求

中标方应充分考虑投标项目的建设要求，提出完整的项目管理、范围管理、进度管理、质量管理、信息系统安全管理、变更管理等方案。

本项目建设周期为6个月内完成项目建设并通过验收，其中从合同签订起1个月内完成所有设备交货，之后1个月内完成所有设备的安装部署及调试，之后4个月进行试运行及测试工作。投标人须在建设周期内完成所有施工内容，包含且不限于设备供货、设备上架安装、加固、模块安装、加电、调试、策略配置、验收、培训等工作。同时，投标人负责提供安装调试时所需使用的各类仪器、工具、设备和安装材料，安装材料应包括电力电缆、通信电缆、光纤及相关的接头等。

投标人应根据对项目的理解做出项目及人员配置管理计划，包括组织结构、项目负责人、 组成人员及分工职责。中标方公司应具备后备支持力量，提供支持，并能满足项目资源调配要求。

为确保本项目顺利进行，要求项目调研、项目实施、系统对接、测试期间人员不少于 1 位项目经理及 2 位信息安全工程师，2 位项目实施人员；培训、试运行期间驻场人员不少于 1 位工程师，1 位项目实施人员。

本项目建设主体为网络安全系统集成，需常态化运行，支持7*24小时无故障运行，投标人需针对本项目投入专业的工程技术人员不少于5名。具体需求如下：

1. 投标人拟投入本项目的项目经理需具备信息系统项目管理师高级职称；
2. 项目实施团队中至少应包含2名中级及以上信息安全师、2名注册信息安全工程师。

上述持证人员不可重复，单人持有多证的情况只认定为持有一张证书。

以上所有人员需提供在投标单位自2025年12月01日至今任意一个月的社保证明材料并加盖公章。

以上专业技术人员职称，需具有省级以上国家机构颁发的证书。

投标人需具有CCRC信息安全服务资质(信息安全应急处理）（二级及以上）、CCRC信息安全服务资质(信息系统安全集成）（二级及以上）等相关资质认证。

投标人需重视本项目中的数据安全，消防应急救援工作过程中的数据具有极高的价值，是数据挖掘的基础。投标人需制定多种数据备份方案或机制，保障系统运行过程中产生的数据不丢失、损坏、泄露，具有相应的数据拯救、恢复的能力。

系统建设完成后，针对重大活动（招标人提前3日通知），投标人需承诺提供不少于2人的专业技术团队进行驻场保障服务。

9. 质量要求

中标人应负责系统及系统设备在实施现场就位安装和调试、操作培训等的全部工作，按照合同文件工作与管理要求负责对项目进度的安排、现场的安全文明施工统一管理和协调，严格遵守国家、本市安全生产有关管理规定，严格按安全标准组织项目实施，采取必要的安全防护措施，消除安全事故隐患。由于中标人管理与安全措施不力造成事故的责任和因此发生的费用，由中标人承担。

投标人提供的产品和相关服务应符合国家和上海市与本项目有关的各项质量和安全标准、规范和验收要求以及相关政府管理部门和行业有关规定和规程，标准、规范等不一致的，以要求严的为准。

投标人提供设备的各种性能参数应满足招标文件和合同技术附件规定的要求。投标人提供的软件的各项功能参数应该满足招标文件和合同技术附件规定的要求。

在保修期内，系统发生故障或被发现存在安全漏洞，中标人要调查故障原因并修复直至满足最终验收指标和性能的要求。保修期内的技术服务内容包括平台功能相关的 BUG 修正、系统调优等基础服务，新增的需求开发除外。

10. 售后服务

（一）项目质保期

项目验收后，投标人须提供不少于 3 年的免费质保，免费质保期自项目验收通过之日起。质保期内软件系统需提供免费升级、迭代服务。

（二）售后服务要求

1、投标人需提供不少于 4 人的售后维护团队，其中 3 人负责系统中所有的硬件维护，1 人负责软件日常维护、系统异常修复、数据安全及技术咨询服务。投标人拟投入本项目的售后服务及运维保障服务团队，需能提供快速修复的能力，紧急故障从报修到解决问题，不超过 2 小时；或具有完善的紧急备用措施，保障网络及安全防护系统不间断运行。

2、投标人须提供 7*24 的全天候售后响应，投标人接到报修后需 10 分钟内响应，1 小时内达到现场处置、4 小时排除一级故障，8 小时内排除二级故障，对于不影响业务的三、四级故障，16 小时内排除。

3.提供相应设备的备品备件，当设备出现故障时，能及时更换坏掉的设备，保证整个系统的可用性。

4、投标人负责在整个合同期内的各项系统正常、无间断运行，当遇有重大活动、突发事件等需要应急保障时，投标人接到报修后需 1 小时内达到现场，2 小时修复故障。

5、投标人在质保期内需每季度对系统进行一次例行巡检，并提供巡检报告。

11. 项目验收

1.设备运抵安装现场后，采购人将与中标人共同开箱签收。签收时发现短缺、破损, 采购人有权要求中标人立即补发和负责更换。

2.项目验收时中标人应提供必备的技术资料：

（1）相关的技术资料（测试报告、产品合格证书、保修卡等）；

（2）提供设备保养、维修操作规程；

（3）提供系统特殊件及配套件的清单、技术参数；

（4）进口设备应提供由独立的商检机构开具的所有设备的原产地证明。

3.设备安装、调试达到技术规范书规定的指标并正常运行 5 个工作日后，可进行系统验收测试。验收规范(包括项目、指标、方式和测试仪器等)应由中标人提交给采购人。采购人可根据合同及技术规范书进行修改和补充, 经双方确认后形成验收文件作为验收依据。验收测试合格后, 双方签署验收协议。

4、如果属于采购人原因导致使系统未能通过验收，采购人应在合理时间内排除故障，再次进行验收。

如因中标人原因导致验收未通过，则相应停止支付合同款，直至验收通过后支付。采购人根据网络安全系统的技术规格要求和质量标准，对网络安全验收合格，签署验收意见。

5、项目资料验收主要包括：所有的合同协议、竣工图纸资料、用户使用说明书、培训资料及随附产品的各类说明书等，具体参照青浦区数字化项目验收文档规范要求。

6、项目质量验收主要包括：

1)项目完成合同所规定的任务，达到系统所规定的功能要求；

2)系统运行稳定可靠，试运行时系统所有软硬件性能满足合同要求及试运行期间出现的问题已被解决；

3）等保测评费由采购人承担，另行采购；

4）如因中标人提供的软硬件产品或系统集成不符合招标文件要求，整改费用由中标人承担；如因缺少相关设备或软件造成测评不通过或无法达到验收要求的，由中标人自行出资购买相关硬件及软件，并与现有的软硬件进行匹配，直至符合项目验收要求及通过测评，且增补软硬件的产权在验收后完全归属招标人。

12. 技术培训要求

培训范围和对象为系统的使用人员、技术人员（系统管理员、网络管理人员、安全管理人员、系统维护人员等）。

预期培训目标：

1)使技术人员掌握相关的专业技术，了解应用系统的设计思路，在运行、使用和维护过程中发挥作用；

2)使系统使用人员了解网络安全系统基础知识、工作原理，掌握网络安全系统的操作方法；

3)使业务人员能够在短时间内掌握网络及安全防护系统的操作使用；

4）培训的方式、时间、期限由采购人确定，投标人须予以配合，培训时间不设限制，直至采购人完全掌握系统常用操作。

说明：

（1）为保证招标的合法性、公平性，投标人认为上述项目技术需求存在排他性或歧视性条款，可在收到或下载招标文件之日起七个工作日内提出并附相关证据，招标人将及时进行调查或组织论证，如情况属实，招标人将对上述相关技术需求做相应修改。

（2）项目附件所列采购需求，投标人可以对其中不合理处进行修改调整，并说明详细理由，招标人如在附件中指出的工艺、材料和设备标准以及参照的规格、品牌、型号仅起说明作用，并没有任何限制性，投标人在投标中可以选用其他替代标准、规格、品牌或型号，但这些修改和替代要实质上优于招标人在附件中要求及指出的工艺、材料和设备的标准以及参照的规格、品牌、型号的要求。

二、项目工作范围与工作要求

1.项目单位要求：

1.1 中标人应具有常设的基地(包括人员、办公场所、备品备件库等)和良好的技术支持保障能力；

1.2 在项目服务实施期间，中标人应严格执行国家、地方、行业各项有关本项目业务管

理和安全作业的法律、法规和制度，积极主动加强和服务业务及安全等有关的管理工作，并按规定承担相应的费用。中标人因违反规定等原因造成的一切损失和责任由中标人承担。

1.3 各投标人在投标文件中要结合本项目的特点和采购人上述的具体要求制定相应的服务管理措施，同时应适当考虑购买自己员工和第三方责任保险，并在报价中列支相应的费用清单。

2.项目人员要求：

2.1 中标人在投标书中承诺并经招标人认定的项目负责人必须是本单位在职职工（以提供的社保缴纳证明为依据）和该项目的实际负责人，项目负责人应具有本专业技术职称和相关专业工作经验。项目负责人的其他项目兼职情况必须列明，项目负责人如有不尽其职或虚名挂靠，采购人有权要求撤换，直至要求解除合同，由此造成的责任由中标人负责。

2.2 项目组主要技术管理人员也应是本单位在职职工（以提供社保为依据），项目组成员的数量和专业分工应足够满足本项目需要，专业应配置合理并具有类似的项目运行维护经验。

2.3 项目人员应具有良好的职业道德和严谨的工作作风并应能够按照委托计划的要求按期到位开展工作。

2.4 未经采购人同意，中标人不得调换或撤离上述人员，若自行更换或撤离，应扣除相应维护服务费用。如采购人认为有必要，可要求中标人对上述人员中的部分人员作出更好的调整。

2.5 维护单位必须按照国家和上海市有关用工法规和政策要求为项目组成员办理各类法定保险。

3.投标人在投标阶段应根据本项目具体情况、采购人需求和国家、本市有关规定与标准制定运行维护方案，在中标后据此进行细化，经招标人确认后按照确认的运行维护方案和运行维护计划组织运行维护，接受招标人代表对运行维护质量的检查、监督和考核。未经采购人事前书面许可，中标人不得自行调整运行维护方案或更改运行维护措施。

4.根据实际需要或其他原因，采购人认为确有必要调整运维方案并以书面形式要求中标人运行维护人员调整运行维护时间或更改运行维护措施时，中标人应遵从采购人要求。

5.投标人应考虑在运行维护期间确保不得影响采购人日常正常活动的进行，中标人必须按采购人需求结合本项目具体情况在投标书中明确本项目运行维护措施、应急措施、安全、文明工作措施并按此实施。

三、项目运维质量标准和考核要求

1.运行维护质量标准

1.1 中标人提供的服务应符合国家、地方及相关政府管理部门和行业与本项目有关的各项服务标准、规范、规章要求，并满足采购人实际需求，标准、规范等不一致的，以要求高

的为准。

1.2 中标人应根据实际应用情况和招标人规定的要求制定运维方案（运维手册）实施运行维护服务，并应达到规定的服务质量标准。因中标人原因导致运维质量达不到约定的目标标准，中标人承担违约责任，并承担由此造成的一切经济损失。

1.3 中标人的系统运行维护还应符合下列要求：

（1）中标人应根据采购人提供的资料，通过调查建立运行维护工作台册，格式应按采购人要求制定、执行，并必须在规定时间内上报各类由采购人规定的报表；

（2）中标人应及时搜集、整理、归纳、掌握系统有关应用故障信息及时掌握设备和系统应用情况，分析原因，作出运行维护情况预测，制定对策预案和应急维保预案，采取必要的预防性措施；

（3）中标人对已定运维计划、方案、时间等工作因各种原因需调整，应事先征得采购人的同意，未经批准不得随意调整；

（4）若因采购人业务需要或突发事件，中标人必须服从采购人的指挥和安排，协助调查解决有关突发问题，并有义务及时配合、提供技术服务或协助应急抢修，按照采购人的要求及时认真处理；

（5）完成采购人交办的相关任务。

1.4 双方对项目服务质量有争议，由双方同意的质量检测机构鉴定，所需费用及因此造成的损失，由责任方承担。双方均有责任，由双方根据其责任分别承担。

2.运维考核要求

2.1 中标人应认真按照行业的标准、规范、本合同的要求以及本项目需求（见附件）和投标承诺进行运行维护，随时接受采购人的检查和考核，为检查、考核提供便利条件。

2.2 采购人可按照合同约定的时间、标准进行日常随机检查和定期考核，发现运维质量达不到约定标准的部分，采购人可要求中标人采取一切补救措施，直到符合约定标准。

2.3 检查和考核标准、奖惩措施，按本项目采购需求（见附件）约定。

2.4 本项目连续 2 次月度考核未达标准，将按照违约处理，情况严重者，甲方有权解除合同。

2.5 若中标人认为运维质量不达标的责任不在中标人，由中标人承担举证责任。

四、投标报价依据与要求

1.报价依据：本招标文件明确的服务范围、服务内容和管理要求、服务等级、质量标准与考核要求等及行业和物价管理部门有关收费标准。

2.报价要求：

2.1 为准确投标报价，各投标人应结合招标需求仔细踏勘运维项目现场(若需要)，详细了解项目运行情况、目标要求及与所需进行运维保障的系统基础设施（设备）数量、种类、

现状，对应系统软件、应用软件、系统安全等各因素。各投标人在报价时要充分考虑所需服务在服务期限内各项工作所必须发生的各类费用及应承担的相关责任后进行报价。

2.2 本招标文件明确的中标服务方式及其他投标人认为应考虑的各类影响报价因素也请在报价中统一考虑，并结合项目保障情况报出本单位能够承受的报价（不设底线），但报价低于成本价的将被判为废标。

2.3 除非招标文件另有规定，招标文件中运维费用是指招标文件中说明的全部运维工作内容的报酬，其中必须包括前期收集资料、建档、服务期间提供技术支撑与技术咨询服务、按照规定的频次进行运行维护、出具报告、人员开支、材料使用、设施与设备使用、相关各类保险费、交通费及其他与运行维护相关的措施费、管理费用、利润及税金等全部费用以及合同明示或暗示的所有责任、义务和一切风险费用。投标报价必须是唯一的。

2.4 除非本招标文件另有规定，本项目一旦中标，中标人在服务期内按照合同规定的服务标准与服务范围、内提供项目运维服务的（合同）总价不做任何调整。

2.5 投标人报价中相应的各类安全文明运维措施费，人工工资、社会保障、福利、社会管理等各类费用应符合国家、地方相关管理部门的规定进行计费，并包括在总价中。

2.6 运行维护投标报价应有细目、单价和总价。

2.7 投标人提供的项目工作及相关服务，应当符合国家有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。投标人不得违反标准规范规定或合同约定，通过降低服务质量、减少服务内容等手段进行恶性低价竞争，扰乱正常市场秩序。

3.其他要求：对于符合要求的投标书，在签订合同协议前，如发现中标价中有缺漏项，其他计算和汇总方面的算术差错，将按对中标人不利原则修正。

五、投标文件的编制要求

投标人应按照第二章《投标人须知》“三、投标文件”中的相关要求编制投标文件，投标文件的商务响应文件（包括相关证明文件）和技术响应文件应当包括（但不限于）下列内容：

1、投标人提交的商务响应文件应由以下部分组成：

（1）《投标函》

（2）《开标一览表》（在采购云平台填写）

（3）《投标报价分类明细表》

（4）《资格条件响应表》

（5）《实质性要求响应表》

（6）《与评标有关的投标文件主要内容索引表》

（7）《法定代表人授权委托书》（含被授权人身份证复印件）

（8）投标人营业执照（或事业单位、社会团体法人证书）、税务登记证（若为多证合一的仅需提供营业执照）

（9）参加本次政府采购活动前三年内，在经营活动中没有重大违法记录的声明函，截止至开标日成立不足 3 年的供应商可提供自成立以来无重大违法记录的声明

（10）关于财务状况及税收、社会保障资金缴纳情况声明函

（11）享受政府采购优惠政策的相关证明材料，包括：中小企业声明函、监狱企业证明文件、残疾人福利性单位声明函、关于符合本国产品标准的声明函等**（中标人享受中小企业扶持政策、残疾人福利性单位支持政策或提供符合本国产品标准声明的，其声明函将随中标结果同时公告）；**

（12）联合投标时，提供《联合投标协议书》

（13）无关联关系承诺函

（14）投标人基本情况简介

（15）投标人质量管理和质量保证体系等方面的认证证书

（16）投标人认为与本项目相关的其他材料。

2、技术响应文件由以下部分组成：

（1） 投标人对本项目需求的理解、对本项目重点难点的分析

（2） 投标人对本项目的合理化建议

（3） 项目网络图

（4） 技术方案

（5） 实施方案

（6） 售后服务

（7） 企业实力

（8） 项目团队成员资质

（9） 项目案例

（10） 按照本招标文件要求提供的其他技术性资料以及投标人需要说明的其他事项。

以上各类响应文件格式详见招标文件第六章《投标文件有关格式》（格式自拟除外）。

第五章　评标方法与程序

一、资格审查

招标人将依据法律法规和招标文件的《投标人须知》、《资格条件响应表》，对投标人进行资格审查。确定符合资格的投标人不少于3家的，将组织评标委员会进行评标。

二、投标无效情形

1、投标文件不符合《资格条件响应表》以及《实质性要求响应表》所列任何情形之一的，将被认定为无效投标。

2、单位负责人或法定代表人为同一人，或者存在直接控股、管理关系的不同供应商，参加同一包件或者未划分包件的同一项目投标的，相关投标均无效。

3、除上述以及政府采购法律法规、规章、《投标人须知》所规定的投标无效情形外，投标文件有其他不符合招标文件要求的均作为评标时的考虑因素，而不导致投标无效。

三、评标方法与程序

（一）评标方法

根据《中华人民共和国政府采购法》及政府采购相关规定，结合项目特点，本项目采用“综合评分法”评标，总分为100分。

（二）评标委员会

1、本项目具体评标事务由评标委员会负责，评标委员由采购人代表及政府采购评审专家组成。招标人将按照相关规定，从上海市政府采购评审专家库中随机抽取评审专家。

2、评标委员会成员应坚持客观、公正、审慎的原则，依据投标文件对招标文件响应情况、投标文件编制情况等，按照《投标评分细则》逐项进行综合、科学、客观评分。

（三）评标程序

本项目评标工作程序如下：

1、符合性审查。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。

2、澄清有关问题。对投标文件中含义不明确或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者纠正。投标人的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，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，也不得通过澄清而使进行澄清的投标人在评标中更加有利。

3、比较与评分。评标委员会按招标文件规定的《投标评分细则》，对符合性审查合格的投标文件进行评分。

4、推荐中标候选供应商名单。各评委按照评标办法对每个投标人进行独立评分，再计算平均分值，评标委员会按照每个投标人最终平均得分的高低依次排名，推荐得分最高者为第一中标候选人，依此类推。其中提供相同品牌产品且通过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，报价最低的投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。如果供应商最终得分相同，则按报价由低到高确定排名顺序，如果报价仍相同，则由评标委员会按照少数服从多数原则投票表决。

（四）评分细则

本项目具体评分细则如下：

1、投标价格分按照以下方式进行计算：

（1）价格评分：报价分＝价格分值×（评标基准价/评审价）

（2）评标基准价：是经符合性审查合格（技术、商务基本符合要求，无重大缺、漏项）满足招标文件要求且投标价格最低的投标报价。

（3）评审价：投标报价无缺漏项的，投标报价即评审价；投标报价有缺漏项的，按照其他投标人相同项的最高报价计算其缺漏项价格，经过计算的缺漏项价格不超过其投标报价10%的，其投标报价也即评审价，缺漏项的费用视为已包括在其投标报价中，经过计算的缺漏项价格超过其投标报价 10%的，其投标无效。

（4）如果本项目非专门面向中小企业采购，对小型和微型企业投标人的投标价格给予 10%的扣除，用扣除后的价格参与评审。如果本项目非专门面向中小企业采购且接受联合体投标（或参加谈判、报价），联合协议中约定小型或微型企业的协议合同金额占到联合体协议合同总金额 30%以上的，给予联合体 4%的价格扣除，用扣除后的价格参与评审。联合体各方均为小型或微型企业的，联合体视同为小型、微型企业。组成联合体的大中型企业或者其他自然人、法人或其他组织，与小型、微型企业之间不得存在投资关系。中小企业投标应提供《中小企业声明函》，如为联合投标的，联合体各方需分别填写《中小企业声明函》。

（5）政府采购活动中既有本国产品又有非本国产品参与竞争的，依法对本国产品给予

价格评审优惠，对本国产品的报价给予20%的价格扣除，用扣除后的价格参与评审。当采购项目或者采购包中含有多种产品，投标人为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该投标人提供的全部产品成本之和的比例达到80%以上时，依法对该投标人提供的全部产品给予价格评审优惠，即对该投标人提供的全部产品的总报价（投标报价）给予20%的价格扣除，用扣除后的价格参与评审。提供符合本国产品标准的产品，投标人应出具《关于符合本国产品标准的声明函》。当采购项目或者采购包中含有多种产品的，投标人还应当提供《关于本国产品比例的声明函》。

（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。

4.2 投标文件其他评分因素及分值设置等详见《投标评分细则》。

投标评分细则（100 分）

评审因素	分值	类型	评分标准
报价得分	30	客观分	投标报价得分=(评标基准价/投标报价)×价格权值。
需求理解及分析	6	主观分	1.投标人对本项目需求和现状理解是否准确到位；（0-2 分）。 2.投标人对本项目重点难点分析是否准确到位；（0-2 分）。 3.投标人对本项目的合理化建议是否有效可行；（0-2 分）。
设备选型及配置情况	10	客观分	技术参数中标注“▲”的为重要参数，共 10 个“▲”，其中“▲”条款技术参数如未按要求提供相关证明材料的（详见技术要求），视为参数不满足，满分 10 分，每一条不满足则扣 1 分，扣完为止。
项目网络图	3	主观分	根据投标人提供的网络安全拓扑图进行评分，图纸设计是否合理、针对性是否强、完整度是否高（0-3 分）。
技术方案	16	主观分	1.根据投标人提供的网络安全技术方案，是否构建了“边界-网络-主机-应用-数据”的多层防御体系；是否具备较高的网络安全防护、便捷的集中管控和对未知威胁进行识别、预警、隔离的能力进行评分（0-6 分）； 2.根据投标人提供的邮件防泄漏技术方案，是否具备较高的处理能力，简单易用的部署架构，对多层级压缩文件的防护能力，对恶意邮件处理方式的多样进行评分（0-5 分）； 3.根据投标人提供的整体技术方案，是否完全响应等保 2.0 第三级的“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”等要求进行评分（0-5 分）。
实施方案	15	主观分	1.投标人根据项目要求是否提供进度计划，包括但不限于项目进度管理、过程管理节点计划、保障措施组织方案等是否满足招标要求。（0-5 分） 2.投标人能否根据项目特性提供集成方案，包括设备部署规划、网络拓扑、综合布线及实施保障措施，是否满足招标要求。（0-5 分） 3.投标人能否提供针对本项目的项目质量、应急管理方案，包括但不限于项目质量保证体系、项目质量控制方法、项目质量保障措施、应急预案，提供的方案是否满足项目各阶段的实施需求。（0-5 分）
项目团队	5	客观分	1、项目经理具有信息系统项目管理师高级职称证书的得 1 分，不提供不得分。； 2、本项目的实施团队中至少包含 2 名中级及以上信息安全师、2 名注册信息安全工程师；需提供相关证明材料并加盖公章，每提供一名人员得 1 分，共 4 分。 注： （1）上述持证人员不可重复，单人持有多证的情况只认定为持有一张证书，其他证书不得分。无证或者证书不在有效期的不得分。

			（2）以上所有人员需提供在投标单位自 2025 年 12 月 01 日至今任意一个月的社保证明材料并加盖公章，否则不予认可。
企业实力	2	主观分	根据投标人的综合服务能力，合同履约能力进行评审；
项目授权	2	客观分	投标人提供政务外网出口防火墙、指挥网出口防火墙、基层站出口防火墙、营区视频安全设备产品制造厂商针对本项目的投标授权书和售后服务承诺函的，并加盖原厂授权公章，每提供一款设备的投标授权书和售后服务承诺函的得 0.5 分，最高 2 分，不提供的不得分。
类似项目业绩	3	客观分	投标人近三年以来承接的有效的类似业绩，是否属于有效的类似项目业绩由评审委员认定。每提供一个有效的业绩得 1 分，最高得分为 3 分，没有有效的类似业绩不得分。需提供项目中标通知书、合同复印件（需体现签约主体、建设内容、金额、双方盖章、合同时间），否则不予认可。
售后服务	8	主观分	根据对售后服务（包括拟投入本项目的维修人员（0-1 分）、售后服务体系（0-1 分）、报修方式（0-1 分）、响应时间（0-1 分）、维护力量（0-1 分），设备及系统提供免费年检（0-1 分）、设备故障修复时间（0-1 分）、原厂巡检服务（0-1 分））进行评审。

第六章　　投标文件有关格式

一、商务响应文件有关格式

1、投标函格式

致：_____（招标人名称）

根据贵方_____（项目名称、招标编号）采购的招标公告及投标邀请，_____（姓名和职务）被正式授权代表投标人_____（投标人名称、地址），按照网上投标系统规定向贵方提交投标文件 1 份。

据此函，投标人兹宣布同意如下：

1.按招标文件规定，我方的投标总价为_____（大写）元人民币。

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.投标有效期为自开标之日起 _____日。

4.如我方中标，投标文件将作为本项目合同的组成部分，直至合同履行完毕止均保持有效，我方将按招标文件及政府采购法律、法规的规定，承担完成合同的全部责任和义务。

5.如果我方有招标文件规定的不予退还投标保证金的任何行为，我方的投标保证金可被贵方没收。

6.我方同意向贵方提供贵方可能进一步要求的与本投标有关的一切证据或资料。

7.我方完全理解贵方不一定要接受最低报价的投标或其他任何投标。

8.我方已充分考虑到投标期间网上投标可能会发生的技术故障、操作失误和相应的风险，并对因网上投标的任何技术故障、操作失误造成投标内容缺漏、不一致或投标失败的，承担全部责任。

9. 我方同意开标内容以采购云平台开标时的《开标记录表》内容为准。我方授权代表将及时使用数字证书对《开标记录表》中与我方有关的内容进行签名确认，授权代表未进行确认的，视为我方对开标记录内容无异议。

10.为便于贵方公正、择优地确定中标人及其投标货物和相关服务，我方就本次投标有关事项郑重声明如下：

（1）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。

（2）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。

地址：

电话、传真：

邮政编码：

开户银行：

银行账号：

投标人授权代表签名：

投标人名称（公章）：

日期：　　年　　月　　日

2、开标一览表格式

青浦区消防救援支队组网安全信创加固项目包 1

包号	项目名称	最终报价(总价、元)

填写说明：

（1）“最终报价（元）”指每一包件报价，所有价格均系用人民币表示，单位为元，精确到个位数。

（2）投标人应按照《招标需求》和《投标人须知》的要求报价。

3. 报价分类明细表格式

系统设备名称	型号、规格、品牌	产地	设备、材料单价（含运输、服务保险等）	数量	合价(人民币元)
产品软件					
				小计：	
软硬件集成费					
安装调试费					
措施费用及其他					
				小计：	
培训					
				小计：	
设计					
管理费					
利润					
税金					
				小计：	
总价					

说明：总报价=各应用系统开发报价+产品软件供货、安装报价

4、资格条件响应表

项目名称：

招标编号：

包号：

序号	项目内容	具备的条件说明（要求）	投标检查项（响应内容说明(是/否)）	详细内容所对应电子投标文件名称	备注
1	法定基本条件	1、符合《中华人民共和国政府采购法》第二十二条规定的条件：营业执照（或事业单位、社会团体法人证书）、税务登记证（若为多证合一的，仅需提供营业执照）符合要求，**提供财务状况及税收、社会保障资金缴纳情况声明函。**2、未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单的供应商。			
2	联合投标	本项目不接受联合投标。			
3	法定代表人授权	1、在投标文件由法定代表人授权代表签字（或盖章）的情况下，应按招标文件规定格式提供法定代表人授权委托书；2、按招标文件要求提供被授权人身份证。			
4	三年经营中没有重大违法记录声明	提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明。			

投标人授权代表签字：_____

投标人（公章）：_____

日期：　　年　　月

5、实质性要求响应表

项目名称：

招标编号：

包号：

项目内容	具备的条件说明（要求）	投标检查项（响应内容说明(是/否)）	详细内容所对应电子投标文件名称	备注
投标文件内容、密封、签署等要求	1、投标文件按招标文件要求提供《投标函》、《开标一览表》、《资格条件响应表》以及《实质性要求响应表》；2、投标文件按招标文件要求密封（适用于纸质投标项目），电子投标文件须经电子加密（投标文件上传成功后，系统即自动加密）。			
投标有效期	不少于 90 天。			
投标报价	1、不得进行选择性报价（投标报价应是唯一的，招标文件要求提供备选方案的除外）；2、不得进行可变的或者附有条件的投标报价；3、投标报价不得超出招标文件标明的采购预算金额或项目最高限价； 4、投标报价有缺漏项的，缺漏项部分的报价按照其他投标人相同项的最高报价计算，计算出的缺漏项部分报价不得超过投标报价的 10%。			
交付日期	按照项目招标要求及合同有关条款执行。			
质量保质期	按照项目招标要求及合同有关条款执行。			
3C 认证	若投标产品属于“中国强制性产品认证”（3C 认证）范围（包括电线电缆、家用和类似用途设备、音视频设备、信息技术设备、照明电器、电信终端设备、防盗报警产品、安防实体防护产品等类别，详见 http://www.cnca.gov.cn），则须提供投标产品 3C 认证证书。			
节能产品	根据《财政部 发展改革委 生态环境部 市场监管总局 关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9 号）以及财政部、发展改革委发布的《节能产品政府采购品目清单》，投标人应当在其投标文件中提供其投标产品的节能产品认证证书，该认证证书应当由国家确定的认证机构出具并处于有效期内，否则视为非实质性响应，其投标无效。			
网络关键	若投标产品属于《网络关键设备和网络安全专用产品目			

设备和网络安全专用产品	录》范围（包括路由器、交换机、 服务器（机架式）、 可编程逻辑控制器（PLC 设备）、数据备份一体机、 防火墙（硬件）、WEB 应用防火墙（WAF）、 入侵检测系统（IDS）、入侵防御系统（IPS）、安全隔离与信息交换产品（网闸）、反垃圾邮件产品、网络综合审计系统、网络脆弱性扫描产品、安全数据库系统、网站恢复产品（硬件）等，详见 http://www.miit.gov.cn），则必须承诺投标产品已按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**(承诺书见格式）**			
实行进网许可制度的电信设备	若投标产品属于工业和信息化部要求的实行进网许可制度的电信设备，则必须承诺投标产品获得工业和信息化部颁发的进网许可证（含进网试用批文）。**(承诺书见格式）**			
“★”要求	符合招标文件中标有“★”的要求			
采购进口产品政策	本次采购不接受整体由进口产品所组成的系统			
付款方法	按照项目招标要求及合同有关条款执行。			
合同转让与分包	合同不得转让、不得分包。			
公平竞争和诚实信用	公平竞争和诚实信用：不得存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为。			
无关联关系承诺	1：本公司不是为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商； 2：与本公司单位负责人或法定代表人为同一人，或者存在直接控股、管理关系的不同供应商，没有参与本项目的投标；			

投标人授权代表签字或盖章：_____

投标人（公章）：_____

日期：　　年　　月

6、与评标有关的投标文件主要内容索引表

项目名称：

招标编号：

包号：

项目内容	具备的条件说明	响应内容说明 （是/否）	详细内容所对应 电子投标文件名称	备注

说明：上述“具备的条件说明”可以参照本项目评标方法与程序及评分细则进行自定义。

7、客观分评审因素情况表

序号	名称	是否响应	响应情况	响应材料对应在响应文件中的页码 **（标注商务标、技术标）**

8、法定代表人授权委托书格式

致：青浦区政府采购中心

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，职务）以我方的名义参加贵中心_____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、投标文件澄清、签约等一切具体事务和签署相关文件。

我方对被授权人的签名事项负全部责任。

在贵中心收到我方撤销授权的书面通知以前，本授权书一直有效。被授权人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。除我方书面撤销授权外，本授权书自投标截止之日起直至我方的投标有效期结束前始终有效。

被授权人无转委托权，特此委托。

在此粘贴被授权人身份证复印件 （有照片一面）

委托人（法定代表人）签字或盖章：

投标人公章：

日期：

受托人（签字或盖章）：

住所：

身份证号码：

邮政编码：

电话：

传真：

日期：

9、投标人基本情况简介格式

（一）基本情况：

1、单位名称：

2、地址：

3：邮编：

4、电话/传真：

5、成立日期或注册日期：

6、行业类型：

（二）基本经济指标（到上年度 12 月 31 日止）：

1、实收资本：

2、资产总额：

3、负债总额：

4、营业收入：

5、净利润：

6、上交税收：

7、从业人数：

（三）其他情况：

1、专业人员分类及人数：

2、企业资质证书情况：

3、其他需要说明的情况：

我方承诺上述情况是真实、准确的，我方同意根据招标人进一步要求出示有关资料予以证实。

投标人授权代表签字或盖章：_____

投标人（公章）：_____

日期：　　年　　月

10.中小企业声明函

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，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、青浦区消防救援支队组网及安全加固项目，属于 软件和信息技术服务业 行业；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：

说明：（1）本声明函所称中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

（2）本声明函所称服务由中小企业承接，是指提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员，否则不享受中小企业扶持政策。

（3）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。

（4）采购标的对应的中小企业划分标准所属行业，以招标文件文件第二章《供应商须知》规定为准。

（5）中标人享受中小企业扶持政策的，其在投标客户端中“中小企业声明函”一栏上传的文件将自动随中标结果同时公告。供应商请勿在投标客户端“中小企业声明函”一栏上传投标文件其他内容，否则因自动公告该栏文件导致中标人商业秘密等信息泄露的，招标人不承担任何责任。（实际以采购云平台最新的操作程序为准）

（6）供应商在投标客户端“中小企业声明函”一栏与投标文件中，多处上传本声明函

的，以投标客户端“中小企业声明函”一栏上传的作为认定依据。

（7）供应商应当按照采购文件中明确的采购标的对应行业出具中小企业声明函，而非按照供应商的经营范围出具中小企业声明函。

注：行业划型标准：

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。

11、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，本单位安置残疾人___人，占本单位在职职工人数比例___%，符合残疾人福利性单位条件，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：

说明：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》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）。

中标人为残疾人福利性单位的，本声明函将随中标结果同时公告。

如投标人不符合残疾人福利性单位条件，无需填写本声明。

12.关于符合本国产品标准的声明函

本公司（单位）郑重声明，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）的规定，本公司（单位）提供的以下产品属于本国产品。具体情况如下：

1.（产品名称 1）[1]，生产厂为（厂名）[2]，厂址为（生产厂址）。（产品名称 1）的中国境内生产的组件成本占比≥（规定比例）[3]。（产品名称 1）的（关键组件）[4] 在中国境内生产。（产品名称 1）的（关键工序）[5] 在中国境内完成。

2.（产品名称 2），生产厂为（厂名），厂址为（生产厂址）。（产品名称 2）的中国境内生产的组件成本占比≥（规定比例）。（产品名称 2）的（关键组件）在中国境内生产。（产品名称 2）的（关键工序）在中国境内完成。

……

本公司（单位）对上述声明内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）：

日期：　　年　　月　　日

1.产品如有型号，请在“产品名称”栏一并填写。

2.生产厂名与厂址应与生产厂营业执照载明的相关信息保持一致。

3.该产品的中国境内生产的组件成本占比相关要求实施前，“规定比例”栏可不填，下同。

4.该产品的关键组件要求实施前，“关键组件”栏可不填，下同。

5.该产品的关键工序要求实施前，“关键工序”栏可不填，下同。

说明：（1）本国产品标准适用于货物，包括政府采购货物项目和服务项目中涉及的货物。适用本国产品标准的货物具体是指《政府采购品目分类目录》中的货物类产品，但不包括其中的房屋和构筑物，文物和陈列品，图书和档案，特种动植物，农林牧渔业产品，矿与矿物，电力、城市燃气、蒸汽和热水、水，食品、饮料和烟草原料，无形资产。

（2）根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》规定，在分产品确定在中国境内生产的组件成本占比要求、以及特定产品的关键组件、关键工序相关要求实施前，本国产品应当符合以下条件：产品应当在中国境内生产，即在中华人民共和国关境内实现从原材料、组件到产品的属性改变。属性改变是指经过制造、加工或者组

装等工序，产生完全不同于原材料、组件的新产品，并具有新的名称和特征（用途）。属性改变不包括以下细微操作：

1.为确保产品在运输或者储存期间保持某种状态而进行的操作；

2.为产品运输或者销售进行的包装或者展示；

3.在产品或者其包装上粘贴或者印刷品牌、标志、标识以及其他用于区别的标记；

4.简单的上漆、磨光和分装；

5.其他不属于属性改变的情形。

（3）当采购项目或者采购包中含有多种产品的，投标人还应当提供《关于本国产品比例的声明函》，承诺提供的符合本国产品标准的产品成本之和占提供的全部产品成本之和的比例达到80%，如投标人未按照前述要求提供相关内容的，不享受本国产品的支持政策。

（4）中标人提供的本声明函将随中标结果同时公告。

13.关于本国产品比例的声明函

本公司（单位）郑重声明，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）的规定，本公司（单位）提供的符合本国产品标准的产品成本之和占提供的全部产品成本之和的比例达到 80%。

本公司（单位）对上述声明内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）：

日期：　　年　　月　　日

14、参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明

我方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。

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。

投标人（公章）：

日期：

15、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：

16、无关联关系承诺函

本公司（联合体）参加（项目名称）采购活动，本公司承诺：

1：本公司不是为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商；

2：与本公司单位负责人或法定代表人为同一人，或者存在直接控股、管理关系的不同供应商，没有参与本项目的投标；

特此承诺

本公司对上述承诺的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（盖章）：

日期：

17、关于网络关键设备和网络安全专用产品以及实行进网许可制度的电信设备的声明

本公司承诺，本公司所投产品属于《网络关键设备和网络安全专用产品目录》范围的，所投产品均已按照相关国家标准的强制性要求，具有具备资格的机构安全认证合格或者安全检测符合要求。

本公司承诺，本公司所投产品属于软件和信息化部要求的实行进网许可制度的电信设备，所投产品均已获得软件和信息化部颁发的进网许可证（含进网试用批文）。

特此声明

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

18、制造厂家项目授权书格式（根据项目需要）

致：青浦区政府采购中心

作为设在_____（制造厂家地址）的制造/生产_____（货物名称或描述）的_____（制造厂家名称），在此以制造厂的名义授权（代理公司名称和地址）用我厂制造的上述货物就贵中心_____项目（项目名称、招标编号）递交投标文件并进行后续的合同谈判和签署合同。

1.我方此次向贵方提供的货物名称为：_____；规格型号：_____；我方保证：该货物既非试验产品也非积压产品，而是于_____年达产的成熟产品，且生产（完工）日期不早于_____年___月；在可以预见的_____（天）内，我方没有对该型号产品进行升级、停产、淘汰的计划。我方郑重承诺，为上述代理公司提供的货物符合采购招标文件的各项要求。上述代理公司在其投标文件中提供的有关我方的各项证明文件和资料经我方审查属实，有关我方的声明是真实的。

2.作为原厂商，我方保证以投标合作者来约束自己，并对该投标共同和分别承担招标文件中所规定的义务。我方保证为本项目的组织实施、售后服务提供纯正的、专业化的技术支持，并对我厂制造的上述货物承担合同规定的全部质量保证责任。

3.我方该型号产品的市场销售情况良好，最近实施（完工）的同类项目有：

采购单位名称	采购数量	单价	合同金额（万元）	合同签订日期	验收日期	联系人及联系电话

4.我方诚意提请贵方关注：有关该型号产品的生产、供货、售后服务以及性能等方面的重大决策和事项有：

_____

5.我方同意按照贵方要求提供与投标有关的一切数据或资料。

制造厂家（公章）：_____

日期：_____年_____月_____日

二、技术响应文件有关表格格式

1、项目负责人情况表

项目名称：
招标编号：
包号：

姓名		出生年月		文化程度		毕业时间	
毕业院校和专业			从事本类项目工作年限			联系方式	
职业资格			技术职称			聘任时间	
主要工作经历： 主要管理服务项目： 主要工作特点： 主要工作业绩： 胜任本项目负责人的理由：							

需附项目负责人毕业证书、职称及职业资格证书及项目负责人依法缴纳社保费的证明。

2、主要管理、技术人员配备及相关工作经历、职业资格汇总表

项目名称：

招标编号：

包号：

项目组成员姓名	年龄	在项目组中的岗位	学历和毕业时间	职称及职业资格	进入本单位时间	相关工作经历	联系方式
……							

需附上述人员毕业证书、职称及职业资格证书及上述人员依法缴纳社保费的证明。

3、投标人类似项目一览表

序号	年份	项目名称	项目内容	服务时间	合同金额（万元）	用户情况		
						单位名称	经办人	联系方式
1								
2								
3								
4								

4、安装实施方案格式

项目名称：

招标编号：

包号：

方案内容：

投标人授权代表签字或盖章：_____

投标人（公章）：_____

日期：_____年_____月_____日

5、售后维修服务承诺

项目名称：

售后服务体系及制度	（包括专业维修服务机构的名称、地址、售后服务体系及相关制度）
售后服务内容及保障措施	（包括售后服务范围、内容，服务计划，维修响应时间、保修责任等）
售后服务联系方式	（包括联系人、地址、联系电话等）

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

6、“▲”指标项汇总表

序号	设备名称	指标项	证明材料
11.	政务外网出口防火墙	4.▲故障分析：支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查；	需提供具备 CNAS 标识的第三方检测报告
12.	政务外网出口防火墙	6. ▲虚拟化：支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备；	需提供具备 CNAS 标识的第三方检测报告
13.	指挥网出口防火墙	4. ▲故障分析：支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查；	需提供具备 CNAS 标识的第三方检测报告
14.	指挥网出口防火墙	6. ▲虚拟化：支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备；	需提供具备 CNAS 标识的第三方检测报告
15.	基层站出口防火墙	5. ▲防病毒：应具备独立的勒索防护模块，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略；	需提供设备功能操作截图证明及关于“勒索病毒”的软件著作权证书
16.	基层站出口防火墙	6.▲入侵攻击防御：产品内置不低于 16000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则；	需提供具备 CNAS 标识的第三方检测报告
17.	基层站出口防火墙	8. ▲安全策略管理：支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；	需提供具备 CNAS 标识的第三方检测报告
18.	营区视频安全设备	6. ▲GA/T 1788.3：设备满足 GA/T 1788.3 要求，达到设备准入控制系统防护要求；	需提供具备 CNAS 标识的第三方检测报告
19.	营区视频安全设备	7. ▲GB35114：支持符合 GB35114 标准的终端接入检测功能，可对不符合 GB35114 的终端接入进行阻断并告警；	需提供具备 CNAS 标识的第三方检测报告
20.	营区视频安全设备	10. ▲历史数据重放：支持基于历史数据重放检测功能，可对存在历史数据重放攻击的终端进行阻断；	需提供具备 CNAS 标识的第三方检测报告

三、各类银行保函格式

1、预付款银行保函格式

致：（采购人名称）

鉴于_____（卖方名称）（以下简称“卖方”）根据年月日与贵方签订的_号合同（以下简称“合同”）向贵方提供（货物和相关服务描述）。

根据贵方在合同中规定，卖方要得到预付款，应向贵方提交由一家信誉良好的银行出具的、金额为（以大写和数字表示的保证金金额）的银行保函，以保证其正确和忠实地履行所述的合同条款。

我行（银行名称）根据卖方的要求，无条件地和不可撤消地同意作为主要责任人而且不仅仅作为保证人，保证在收到贵方第一次要求就支付给贵方不超过（以大写和数字表示的保证金金额），我行无权反对和不需要先向卖方索赔。

我行进而同意，要履行的合同条件或买卖双方签署的其他合同文件的改变、增加或修改，无论如何均不能免除我行在本保函下的任何责任。我行在此表示不要求接到上述改变、增加或修改的通知。

本保函自收到合同预付款起直至　　年　　月　　日前一直有效。

出证行名称：_____

出证行地址：_____

经正式授权代表本行的代表的姓名和职务（打印和签字）：_____

银行公章：_____

出证日期：_____

说明：1、本保函应由商业银行的总行或者分行出具，分行以下机构出具的保函恕不接受。

2、本保函由中标人在合同生效前提交。

2、履约保证金（银行保函）格式

致：（买方名称）

鉴于（卖方名称）（以下简称“卖方”）根据年月日与贵方签订的号合同向贵方提供（货物和服务描述）（以下简称“合同”）。

根据贵方在合同中规定，卖方应向贵方提交由一家信誉良好的银行出具的、合同规定金额的银行保函，作为卖方履行合同义务和按照合同规定提供给贵方的服务的履约保证金。

我行同意为卖方出具此保函。

我行特此承诺，我行作为保证人并以卖方的名义不可撤销地向贵方出具总额为（以大写和数字表示的保证金金额）元人民币的保函。我行及其继承人和受让人在收到贵方第一次书面宣布卖方违反了合同规定后，就立即无条件、无追索权地向贵方支付保函限额之内的一笔或数笔款项，而贵方无须证明或说明要求的原因和理由。

本保函自出具之日起至全部合同服务按合同规定验收合格后三十天内完全有效。

出证行名称：_____

出证行地址：_____

经正式授权代表本行的代表的姓名和职务（打印和签字）：_____

银行公章：_____

出证日期：_____

说明：本保函由中标人在中标后提交。

第七章　　合同书格式和合同条款

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]**

地址： **[合同中心-采购单位所在地]**

邮政编码： **[合同中心-采购人单位邮编]**

电话： **[合同中心-采购单位联系人电话]**

传真： **[合同中心-采购人单位传真]**

联系人： **[合同中心-采购单位联系人]**

[供应商信息-联合体]

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、服务质量等详见招标文件和投标文件。

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：甲方指定地点。

2．3 服务期限

本服务的服务期限：本项目建设周期为 6 个月内完成项目建设并通过验收，其中从合同签订起 1 个月内完成所有设备交货，之后 1 个月内完成所有设备的安装部署及调试，之后 4 个月进行试运行及测试工作并最终完成验收。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。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。

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：

(1) 合同签订后，所有硬件设备到货后，采购人在财政资金到位后 20 个工作日内支付合同金额的 20%；

(2) 所有硬件设备安装调试部署及测评完成后，采购人在财政资金到位后 20 个工作日内支付合同金额的 60%；

(3) 项目通过竣工验收并完成项目审计后，按照审计结果支付尾款。

8．甲方的权利义务

8．1 甲方有权在合同规定的范围内享受本项目服务，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，造成服务无法正常运行，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，使甲方有关本项目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 当服务或设备发生故障时，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服务范围进行调整，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，发现本项目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，保证本项目正常运行。

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。

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合同金额 3%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，并可向乙方主张合同总金额 20%的违约金，违约金不足以弥补损失的，还应补足损失。

（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 本合同一式三份，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： 本合同书、本项目成交通知书、乙方的本项目响应文件、本项目采购文件中的合同条款、本项目采购文件中的采购需求、其他合同文件（需列明）。

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。

20.4 上述文件互相补充和解释，如有不明确或不一致之处，按照上述文件次序在先者为准。同一层次合同文件有矛盾的，以时间较后的为准。

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）：

法定代表人或授权委托人（签章）：

[供应商法定代表人-联合体]

合同签订点:网上签约