



项目编号：SHXM-15-20221025-1086

浦东新区网络安全监管 与保障服务

招标文件

(正式稿)

集中采购机构：上海市浦东新区政府采购中心

2022年11月

电子投标特别提醒

一、注册登记与安全认证

为确保电子采购平台数据的合法、有效和安全，各参与主体均应在上海市政府采购管理信息平台（以下简称“电子采购平台”）上注册登记并获得账号和密码。采购人、投标人、集中采购机构还应根据《上海市数字证书使用管理办法》等规定，向本市依法设立的电子认证服务机构申请用于身份认证和电子签名的数字证书（CA证书），并严格按照规定使用电子签名和电子印章。

二、招标文件下载

投标人使用数字证书（CA证书）登陆《上海政府采购网》（上海政府采购云平台），在电子政府采购平台下载并保存招标文件。如招标公告要求投标人在下载招标文件前进行报名登记，并查验资格证明文件的，投标人应当按照招标公告的要求先行登记后，再下载招标文件。

三、招标文件的澄清、补充与修改

采购人和集中采购机构可以依法对招标文件进行澄清、补充与修改。澄清、补充与修改的文件将在电子采购平台上予以公告，并通过电子采购平台发送至已下载招标文件的供应商工作区。

四、投标文件的编制、加密和上传

投标人下载招标文件后，应使用电子采购平台提供的投标工具客户端编制投标文件。

在投标截止前，投标人在“网上投标”栏目内选择要参与的投标项目，按照网上投标系统和招标文件要求填写网上投标内容。对于有多个包件的招标项目，投标人可以选择要参与的包件进行投标。只有投标状态显示为“标书提交”时，才是有效投标。

投标人和电子采购平台应分别对投标文件实施加密。投标人通过投标工具，使用数字证书（CA证书）对投标文件加密后，上传至电子采购平台，再经过电子采购平台加密保存。由于投标人的原因，造成其投标文件未能加密，导致投标文件在开标前泄密的，由投标人自行承担责任。

投标人在网上投标系统中，应提交投标文件彩色扫描件（PDF文件），投标文件组成内容详见招标文件要求。本项目恕不接受电子采购平台以外其他形式的投标。

投标人应根据招标文件的要求编制投标文件，投标文件内容应规范完整、简洁明了、编排合理有序，其中的扫描文件应清晰完整。考虑到电子采购平台运行现状，上传电子加密标书最大支持150M，详细技术问题可咨询电子采购平台运维单位。

投标人组成联合体形式投标，由联合体中的主体方进行网上投标操作，投标流程和要求参照以上条款。

投标文件内容不完整、格式不符合要求，导致投标文件被误读、漏读，由投标人自行负责，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

五、投标截止

投标截止后电子采购平台不再接受供应商上传投标文件。

投标截止与开标的的时间以电子采购平台显示的时间为准。

六、开标

开标程序在电子采购平台进行，投标人在完成网上投标后，按照招标文件规定的时间和地点，由其法定代表人，或经授权的代理人携带要求的材料及设备【笔记本电脑、无线网卡、数字证书（CA证书）】，登录《上海政府采购网》（上海政府采购云平台）（<http://www.zfcg.sh.gov.cn>）参加开标。

为确保您所参与的招投标工作的顺利进行，避免在此期间因数字证书办理更新、变更等而导致您

的投标文件解密失败，特提示您：在开标业务未完成期间，请勿进行数字证书的更新、变更等操作。您可以在投标前或开标业务完成后再进行数字证书更新、变更等操作，以避免因此给您的招投标工作带来不便。

七、投标文件解密

投标截止、电子采购平台显示开标后，投标人进行签到操作，操作时长以平台显示时间（目前为30分钟）为准。投标人签到完成后，由集中采购机构解除电子采购平台对投标文件的加密，投标人应在电子采购平台规定时间内使用数字证书（CA证书）对其投标文件解密，操作时长以平台显示时间（目前为30分钟）为准。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。

八、开标记录的确认

投标文件解密后，电子采购平台根据各投标人通过投标客户端填写并提交的《开标一览表》中的报价，自动汇总生成《开标记录表》。为此，投标人应正确填写，使投标客户端的《开标一览表》和投标文件中的《开标一览表》所填报价保持一致。

投标人应及时检查《开标记录表》的数据与其投标文件中的《开标一览表》是否一致，并作出确认。投标人因自身原因未作出确认的，视为其认可《开标记录表》内容。

九、其他

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）的规定，本项目招投标相关活动在电子采购平台（网址：www.zfcg.sh.gov.cn）电子招投标系统进行。投标人应根据《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。

本项目实施过程中因以下原因导致的不良后果，集中采购机构不承担责任，投标人参加本项目投标即被视作同意下述免责内容：

- 1、电子采购平台的程序设置对本项目产生的影响；
- 2、集中采购机构以外的单位或个人，在电子采购平台中的不当操作，对本项目产生的影响；
- 3、电子采购平台发生技术故障或遭受网络攻击对本项目所产生的影响；
- 4、其他无法预计或不可抗拒的因素。

十、电子采购平台技术咨询联系方式

联系电话：400-881-7190

投标邀请

根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》和《上海市电子政府采购管理暂行办法》之规定，受采购人的委托，集中采购机构对采购项目进行国内公开招标采购，特邀请合格的供应商前来投标。

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》第二十二条规定的供应商。
- 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、其他资格要求：

3.1 本项目面向大、中、小、微型企业，事业法人、其他组织或自然人采购。

3.2 本项目**不允许**联合体形式投标。

3.3 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。

二、项目概况：

- 1、项目名称：浦东新区网络安全监管与保障服务
- 2、招标编号：SHXM-15-20221025-1086
- 3、预算编号：151522-15503
- 4、项目主要内容、数量及简要规格描述或项目基本概况介绍：

本项目主要内容包含两部分，工作内容一为日常性网络安全技术服务，工作内容二为各类专项网络安全服务（包括主机安全防病毒服务、等级保护测评服务、网络安全综合监管平台服务），具体详见招标文件第二章项目招标需求。

本项目最高限价同预算金额，各工作内容最高限价分别为：工作内容一日常性网络安全技术服务最高限价6,828,000.00元、工作内容二各类专项网络安全服务最高限价6,380,000.00元。

按照《中小企业划分标准规定》（工信部联企业〔2011〕300号），本项目采购的**网络安全监管与保障服务**属于软件和信息技术服务业。

- 5、交付地址：上海市浦东新区范围内。
- 6、服务期限：自合同签订之日起2年。

7、采购预算金额：13,208,000.00元（国库资金：13,208,000.00元；自筹资金：0.00元）。本项目最高限价同预算金额，各工作内容最高限价分别为：工作内容一日常性网络安全技术服务最高限价6,828,000.00元、工作内容二各类专项网络安全服务最高限价6,380,000.00元。

8、采购项目需要落实的政府采购政策情况：节能产品政府采购、环境标志产品政府采购、促进中小企业发展、促进残疾人就业。

三、招标文件的获取

时间：2022-11-02 至 2022-11-09，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）。

合格的供应商可于招标公告发布之日起至公告截止时间内，登录《上海政府采购网》（<http://www.zfcg.sh.gov.cn>）在网上招标系统中上传如下材料：无。

合格供应商可在招标公告规定的时间内下载招标文件并按照招标文件要求参加投标。

凡愿参加投标的合格供应商应在招标公告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。

注：投标人须保证报名及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、投标截止时间及开标时间：

- 1、投标截止时间：**2022年11月23日09:30时**（电子采购平台显示时间）。
- 2、开标时间：**2022年11月23日09:30时**（电子采购平台显示时间）。

五、投标地点和开标地点

- 1、投标地点：上海政府采购网（<http://www.zfcg.sh.gov.cn>）。
- 2、开标地点：上海政府采购网（<http://www.zfcg.sh.gov.cn>）。届时请投标人代表持投标时所使用的数字证书（CA证书）参加开标。
- 3、开标所需携带其他材料：

自行携带无线上网的笔记本电脑、无线网卡、数字证书（CA证书）。

六、发布公告的媒介：

以上信息如果有变更我们会通过《上海政府采购网》通知，请供应商关注。

七、其他事项

1、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）的规定，本项目招投标相关活动在电子采购平台（网址：www.zfcg.sh.gov.cn）电子招投标系统进行。投标人应根据《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。

八、联系方式

采购人：	上海市浦东教育发展研究院	集中采购机构：	上海市浦东新区政府采购中心
地址：	上海市浦东新区枣庄路658弄10号	地址：	上海市浦东新区民生路1399号16楼
邮编：	200136	邮编：	200135
联系人：	周东红	联系人：	李月
电话：	50196038	电话：	58387055
传真：	50500088	传真：	68542614

第一章投标人须知及前附表

一、投标人须知前附表

本表关于项目的具体要求是对投标人须知的具体补充，两者如有矛盾，应以本表为准。

条款号	内容规定	备注
1.1	项目名称：浦东新区网络安全监管与保障服务	
5.1	关于现场踏勘 (1) 集合时间：****年**月**日**:**（北京时间） (2) 地点：***** (3) 联系人：***** (4) 联系电话：*****	（本项目不适用）
6.1	关于澄清答疑 (1) 提问递交截止时间： 2022年11月11日10:00时 （北京时间） (2) 提问递交方式：以书面形式（必须加盖投标人公章）递交至“《投标邀请》/八联系方式”集中采购机构地址。	
6.2	答疑会时间：****年**月**日**:**（北京时间） 地点：上海市浦东新区民生路1399号16楼16A11室	（本项目不适用）
10.1.1	投标人提交的投标文件商务部分应包括以下内容（不局限于以下内容）： (1) 投标承诺书 (2) 投标函 (3) 法定代表人身份证明及授权委托书 (4) 投标保证金（ 支票、汇票、本票、保函等非现金形式 ）（ 本项目不适用 ） (5) 投标人基本情况表 (6) 投标人应提交的资格证明材料 ①财务状况及税收、社会保障资金缴纳情况声明函； (7) 开标一览表 (8) 投标报价明细表 (9) 根据招标文件要求，投标人提供以下证明材料： ① 国家强制认证的产品承诺书 ； (10) 拟分包项目一览表（ 本项目不适用 ） (11) 投标人可提交的商务部分其他证明材料（不仅限于以下资料） ①中小企业声明函（注：仅中、小、微型企业须提供）； ②投标人综合实力介绍，包括投标人认为可以证明其履约能力和水平的《近三年类似项目承接及履约情况一览表》（详见“投标文件格式”），获得的有关荣誉证书，质量管理体系和质量保证体系等方面的认证证书 ③投标人认为可以证明其信誉和信用的其他材料； ④残疾人福利性单位声明函（注：仅残疾人福利单位提供）	投标文件内容不完整、格式不符合要求，导致投标文件被误读、漏读，由投标人自行负责，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

条款号	内容规定	备注
	⑤维保设备原厂授权书或售后服务承诺书（如有）。	
10.1.2	<p>投标人提交的投标文件技术部分应包括（不局限于以下内容）：</p> <p>（1）技术方案（包括：总体方案、分项实施方案）；</p> <p>（2）拟投入本项目的人员组成情况（包括《拟派人员汇总表》、《项目主要人员基本情况表》、《项目其他工作人员基本情况表》）；</p> <p>（3）项目服务质量保证措施（包括《项目实施进度计划表》、《风险管理表》）；</p> <p>（4）拟投所有产品清单、偏离表（包括《拟投所有产品清单》、《技术偏离表》等）；</p> <p>（5）拟投入本项目的设备材料情况（包括《主要设备、材料情况一览表》）；</p> <p>（6）其他需说明的问题或需采取的技术措施。</p>	投标文件内容不完整、格式不符合要求，导致投标文件被误读、漏读，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。
12.1	投标有效期：投标截止日期之后的90天（日历天）	
13.1	投标保证金：**元	（本项目不适用）
13.3	<p>投标保证金提交方式：支票、汇票、本票、保函等非现金形式</p> <p>投标保证金有效期：同“投标有效期”</p> <p>注：投标保证金（纸质原件）须在投标截止时间前提交集中采购机构 提交地址：上海市浦东新区民生路1399号**室</p> <p>联系人：*****</p>	<p>各包件的投标保证金应独立开具</p> <p>（本项目不适用）</p>
15.1	投标截止时间详见《投标邀请》	
★21.1	<p>开标结束后，采购人或采购代理机构对投标人的资格进行审查。投标人不满足下列情形之一的，其投标文件不予符合性审查。</p> <p>（1）投标人符合招标文件“投标人须知”第3条规定的资格条件的；</p> <p>（2）投标人按“投标人须知前附表”第10.1.1（6）条款规定提交资格证明材料。</p>	<p>1、本条款所提及内容均为实质性响应条件。</p> <p>2、投标人证明材料提供不完整，关键信息模糊、难以辨认或甄别的，视作未按要求提供资格证明材料。</p>
★21.3	<p>评标委员会如发现投标人及其投标文件不满足下列情形之一的，经评标委员会审定后，该投标文件作无效标处理。</p> <p>（1）投标文件中的下列内容按招标文件要求签署、盖章的（具体详见“投标文件格式”要求）：</p> <ul style="list-style-type: none"> ➢ 投标承诺书 ➢ 投标函 ➢ 授权委托书 ➢ 开标一览表 	本条款所提及内容均为实质性响应条件，若所列实质性检查内容判断标准与其他各处有矛盾之处，以此处所列要求为准。

条款号	内容规定	备注
	<p>(2) 投标人未提交两个以上不同的投标报价；（注：招标文件要求提交备选投标的除外）</p> <p>(3) 投标人接受招标文件规定的投标有效期的；</p> <p>(4) 接受招标文件规定的项目实施或服务期限；</p> <p>(5) 未出现投标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，且不能按评标委员会要求提供说明材料的；</p> <p>(6) 投标报价未超过招标文件中规定的预算金额；投标报价未超过招标文件中规定的各工作内容对应的单价上限（工作内容一日常性网络安全技术服务最高限价6,828,000.00元、工作内容二各类专项网络安全服务最高限价6,380,000.00元）；</p> <p>(7) 经评标委员会审定，投标报价未存在招标文件“第二章”第 17.4 条款所列情形之一的；</p> <p>(8) 按规定缴纳投标保证金；（本项目不适用）</p> <p>(9) 根据招标文件要求，投标人提供以下证明材料： ①国家强制认证的产品承诺书；</p> <p>(10) 按“投标人须知”第 21.4 条款规定，对投标报价算术性错误修正予以确认的；</p> <p>(11) 投标人接受“项目招标需求”中明确的结算原则和支付方式的；</p> <p>(12) 投标人未出现《政府采购货物和服务招标投标管理办法》第三十七条所列的串通投标情形之一的；</p> <p>(13) 投标人未出现提供虚假材料、行贿等违法行为；</p> <p>(14) 未因电子文档本身的计算机病毒、或电子文档损坏等原因造成投标文件无法打开或打开后无法完整读取的；</p> <p>(15) 满足招标文件规定的以下要求： ①接受并满足招标文件的实质性响应要求和条件；</p> <p>(16) 遵守《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》规定的。</p>	
23.3	本项目授权评标委员会依照评标办法确定中标人	
29.1	采购货物数量的更改：依据《中华人民共和国政府采购法》，需要从原供应商处添购的，添购资金总额不超过原合同采购金额的10%。	
31.1	<p>履约保证金金额：（单位：**元）</p> <p>履约保证金提交方式：支票、汇票、本票、保函等非现金形式</p> <p>履约保证金提交时间：签订合同协议书之前</p>	（本项目不适用）

二、投标人须知

（一）说明

1 总则

1.1 本项目（即“投标人须知前附表”写明的项目，以下简称“前附表”）已纳入本年度政府集中采购预算。本项目年度预算已经批准，招标范围、招标方式和招标组织形式已经核准。

1.2 本招标文件及今后的招标补充文件等是本项目招标过程中的规范文件，是采购人与中标人签订服务承包合同的依据，作为项目承包合同附件之一，具有同等法律效力。

1.3 各投标人应认真踏勘项目现场，熟悉项目现场及作业空间等情况，并在投标文件中考虑可能影响投标报价的一切因素。中标后，不得以不完全了解现场及周边等情况为理由要求提出经济补偿，否则，由此引起的一切后果由中标人负责。（本项目不适用）

1.4 各投标人必须认真阅读全部招标文件（包括招标补充文件），并不得擅自改变上述文件条款的规定，一旦作出投标决定，即视作投标人已完全理解和确认招标文件（含招标补充文件等）的一切内容与要求，已不需要作出任何其它解释和修改。凡投标人对上述文件条款的文字与数字的误读、漏读而引起投标文件的错误、遗漏、费用计算有误等，形成投标报价内容的差异，均属投标人失误，采购人和集中采购机构对此均不承担任何责任。开标后，除招标文件明确作相应调整外，一律不得作出其他任何调整。

1.5 投标人不得相互串通投标报价，不得排挤其他投标人的公平竞争，损害采购人或其他投标人的合法权益，投标人不得与采购人串通投标。评标委员会在评标阶段，对投标文件的审查、澄清、评议的过程中，一旦发现投标人有上述行为或对采购人、评标委员会以及其他有关人员施加影响的任何行为，其投标文件作无效标处理。

1.6 采购人不一定接受最低报价投标或收到的全部投标。

1.7 本次招标采购确定的是完成本项目的承包供应商，如果涉及到与本项目相关的部分设备产品或服务采购，国家、上海市或行业管理部门另有相关要求的，中标人在履约过程中的相关采购工作也应从其规定。

1.8根据《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库【2016】125号）的有关要求，采购人和集中采购机构将在开标后、评标开始前，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、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，以及上述网站查询中其他不符合《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。各供应商的信用信息查询记录作为采购文件一并归档。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。

1.9 本招标文件中的不可抗力是指不能预见、不能避免并不能克服的客观情况。应包括重大自然灾害（如台风、洪水、地震等）、政府行为（如征收、征用）、社会异常事件（如战争、罢工、骚乱）。

1.10 本招标文件中的政策性调价是指经政府授权的相关部门对职工最低工资标准、社保金和公积金缴存基数和比例的调整。

1.11 本招标文件未尽之处，或者与相关法律、法规、规范性文件要求不一致的，均按相关法律、法规、规范性文件要求执行。

1.12本招标文件中出现前后矛盾的，以在招标文件中出现顺序在后的解释为准（招标文件中有特别说明的除外）。

1.13 本招标文件中标有“★”的内容为实质性响应要求和条件。

1.14 本招标文件由采购人和集中采购机构负责解释。

2 招标范围和内容

2.1 本项目招标范围和内容详见招标文件“第二章”。

3 投标人的资格要求

3.1 合格的投标人应满足《投标邀请》中“合格的投标人必须具备以下条件”的要求。

3.2 投标人应当提供相应资格证明材料，具体详见“投标人须知前附表”第10.1.1（6）条款要求。

3.3 为该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，不得再参加该项目的其他采购活动。

3.4 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

4 投标费用

4.1 投标人在投标过程中的一切费用，不论中标与否，均由投标人承担。

5 现场踏勘（本项目不适用）

5.1 采购人或集中采购机构将在“前附表”中载明的地址和时间，统一组织投标人对现场及其周围环境进行现场踏勘，以便使投标人自行查明或核实有关编制投标文件和签订合同所必需的一切资料。

5.2 现场踏勘期间的交通、食宿由投标人自行安排，费用自理。

5.3 如果投标人认为需要再次进入现场考察，应向采购人事先提出，采购人应予支持，费用由投标人自理。

5.4 除采购人的原因外，投标人自行负责在现场踏勘中所发生的人员伤亡和财产损失。

6 答疑会

6.1 在“前附表”规定的截止时间以前，投标人可以通过“前附表”明确的方式和途径向集中采购机构提出关于招标文件、提供资料及项目现场踏勘中存在的对本次投标的疑点问题。

6.2 采购人和集中采购机构在“前附表”规定的时间、地点召开答疑会，答疑会的目的是澄清、解答投标人就本项目提出的问题。

6.3 各投标人应在“前附表”规定的截止时间之前提出书面问题，采购人和集中采购机构将对收到的书面问题作统一解答，但不包括问题的来源。采购人和集中采购机构也可以主动对招标文件进行澄清、修改与补充。澄清、修改与补充的招标补充文件为招标文件的组成部分，对招标各方起约束作用，其将在电子采购平台上公告，并通过电子采购平台发送至已下载招标文件的投标人工作区，各投标人应主动获取，由于投标人自身原因未及时获取的，采购人和集中采购机构不承担责任。

7 合格的货物和服务

7.1 投标人所提供的货物和服务应当没有侵犯任何第三方的知识产权、技术秘密等合法权利，同时应当符合招标文件的招标需求，并且其质量完全符合国家标准、行业标准或地方标准。

（二）招标文件

8 招标文件的内容

8.1 本项目招标文件包括下列文件及所有按本须知第6.3和9.1条款发出的招标补充文件。

- 8.1.1 投标邀请
- 8.1.2 投标人须知及前附表
- 8.1.3 项目招标需求
- 8.1.4 投标报价须知
- 8.1.5 合同文本（草案）
- 8.1.6 投标文件格式
- 8.1.7 初步评审、详细评审
- 8.1.8 附件（如果有）

8.2 投标人应仔细阅读招标文件，按招标文件的规定与要求编写投标文件。如果投标文件与招标文件的规定与要求不符合，则投标人应自行承担投标风险。凡与招标文件的规定有重大不符合的投标文件，按本招标文件有关规定办理。

9 招标文件的修改

9.1 在投标截止时间之前，采购人和集中采购机构可能会因任何原因（包括本须知第6.1条款对在答疑期间提出的问题）对招标文件进行修改，该修改内容为招标文件的组成部分，对招投标各方起约束作用。当原招标文件与修改内容有差异的，以修改内容为准。

9.2 在投标截止时间15日前，采购人和集中采购机构可按本须知的规定，通过招标补充文件对招标文件进行修改，如果招标补充文件的发布时间距投标截止时间不足15天，将通知相应延长投标截止时间。

（三）投标文件的编制

10 投标文件的组成

10.1 投标文件由商务部分和技术部分组成。

10.1.1 投标人提交的投标文件商务部分，应包括内容详见“前附表”要求。

10.1.2 投标人提交的投标文件技术部分，应包括内容详见“前附表”要求。

10.2 投标文件编制的注意事项

10.2.1 投标人按上述内容及顺序排列编制投标文件，投标文件内容应规范完整、简洁明了，编排合理有序，其中的扫描文件应清晰完整。

10.2.2 技术部分标书应遵循以下要求

（1）投标人应针对本项目的具体情况和工作要求，通过对工作的重点和难点分析，从服务实施的方法和措施、服务流程、实施过程的质量控制管理、人员和设备配备（如果有）、售后服务（如果有）等方面编制技术标。

（2）技术部分标书内容要求表达精炼、准确、简要。

（3）技术部分标书文字部分统一采用宋体小四号字体，行距采用1.5倍行距。

10.2.3 投标人应按照电子采购平台要求的格式填写相关内容，凡招标文件要求签字、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字和加盖公章。

10.2.4 投标人应按招标文件要求的内容、格式和顺序编制投标文件，凡招标文件提供有相应格式（详见“投标文件格式”）的，投标文件均应完整的按照招标文件提供的格式填写，并按要求在电子采购平台进行有效上传。

10.2.5 投标文件内容不完整、格式不符合，而导致投标文件被误读、漏读或者查找不到相关内容的，

是投标人的责任，投标人应承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

11 投标报价

11.1 除招标需求另有说明外，投标报价应包括完成招标范围内全部工作内容；为达到招标要求所发生的一切辅助性、配合性的相关费用；按规定应计取的规费、保险、税金等；并且充分考虑合同包含的责任、义务和一般风险等各项全部费用。投标报价原则及计算方法见本招标文件“第二章”要求。

11.2 如项目中包含多个包件，且投标人同时响应两个（含两个）以上包件的，各包件应单独报价。

11.3 本项目的采购预算金额或最高限价详见《投标邀请》中“项目概况”，投标报价或各包件报价均不得超过公布的预算金额或最高限价。

11.4 投标人所报的投标报价（包括各子目单价及取费标准）在合同执行过程中是固定不变的（合同或招标文件中约定的变更除外），不得以任何理由予以变更。

11.5 本项目的报价按人民币计价，单位为元，报价精确到元。

12 投标有效期

12.1 投标文件在前附表中所述的投标有效期内保持有效，投标有效期不足的投标将被作为无效标。

12.2 在原定投标有效期满之前，如出现特殊情况，集中采购机构可以向投标人提出延长投标有效期的要求，对此投标人应立即向集中采购机构作出答复，这种要求和答复均应以书面形式进行。投标人可以拒绝集中采购机构的要求，且不会被作不良诚信记录和不予退还投标保证金的处理，但拒绝延长投标有效期的投标文件将不会列入评审范围。接受延长投标有效期的投标人不允许修改其投标文件，但评标委员会认为需对投标文件作出澄清的除外。

13 投标保证金（本项目不适用）

13.1 投标人应提交“前附表”规定金额的投标保证金，并作为其投标的一部分。

13.2 投标保证金是为了保护采购人和集中采购机构免遭因投标人的行为而蒙受损失。采购人和集中采购机构在因投标人的行为受到损害时可根据投标人须知第 13.5 条款的规定不予退还投标人的投标保证金，统一上缴国库。

13.3 投标保证金应按“前附表”中规定的其中一种方式提交，投标保证金有效期为投标有效期满后（“前附表”规定的天数）天。

13.4 凡没有根据本须知第 13.1 和 13.3 条款的规定提交投标保证金的投标，应按本须知第 21 条的规定视为无效标。

13.5 下列任何情况发生时，投标保证金将不予退还：

13.5.1 投标人在招标文件中规定的投标有效期内撤回其投标；

13.5.2 中标后不能按照投标文件的承诺签订合同的。

13.6 投标保证金的退还

13.6.1 未中标人的投标保证金在中标通知书发出后五个工作日内退还。

13.6.2 中标人的投标保证金在合同签订后五个工作日内退还。

14 投标文件的编制、加密和上传

具体详见《电子投标特别提醒》中相关要求。

15 投标截止时间

15.1 投标人应在规定的投标截止时间前，使用电子采购平台提供的客户端投标工具编制加密、上传投标文件，并打印“投标确认回执”。

15.2 在特殊情况下，采购人和集中采购机构如果决定延后投标截止时间，至少应在原定的投标截

止时间 3 日前将此决定书面通知所有的投标人。在此情况下，采购人、集中采购机构和投标人受投标截止时间制约的所有权利和义务，适用于延长后新的投标截止时间。

15.3 投标截止与开标的时间以电子采购平台显示的时间为准。

16 迟到的投标文件

16.1 投标截止后，不再接受投标人上传投标文件。

17 投标文件的修改与撤回

17.1 在投标截止时间之前，投标人可以使用电子采购平台提供的客户端招标工具，对投标文件进行修改。投标文件修改完成后，应在规定的时间内重新加密、上传投标文件，并确保投标状态显示为“正式投标”。

17.2 在投标截止时间之前，投标人可以使用电子采购平台提供的客户端招标工具，对投标文件进行撤回。

17.3 在投标有效期内，投标人不能修改或撤回投标文件，否则将按照本须知的规定作不良诚信记录。

（四）开标与评标

18 开标

18.1 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。

19 投标文件解密和开标记录的确认

19.1 投标截止、电子采购平台显示开标后，投标人进行签到操作，操作时长以平台显示时间（目前为 30 分钟）为准。投标人签到完成后，由集中采购机构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（CA 证书）对其投标文件解密，操作时长以平台显示时间（目前为 30 分钟）为准。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。

19.2 投标人因自身原因，未能在电子采购平台规定的解密时限内，将其投标文件解密的，视为放弃投标。

19.3 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》。

19.4 投标人应及时检查《开标记录表》的数据与其投标文件中的《开标一览表》是否一致，并作出确认。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。

20 评标委员会组成

20.1 评标委员会由 5 人以上（含 5 人）的单数组成，其中政府采购评审专家所占比例不少于成员总数的三分之二。采购人派代表参加评标委员会，集中采购机构不参与评标。

21 投标文件的初步评审

★21.1 开标结束后，采购人或采购代理机构对投标人的资格进行审查。投标人不满足“前附表”所列情形之一的，其投标文件不予符合性审查。

21.2 在详细评标之前，评标委员会将根据招标文件规定，对每份投标文件进行符合性审查，详细审查每份投标文件是否实质性响应了招标文件的要求。实质性响应的投标应该是与招标文件要求的全部条款、条件和规格相符，并没有重大偏离的投标；对关键条文的偏离、保留或者反对，将被认为是非实质性响应。实质性响应招标文件要求的供应商均不得少于 3 家。

★21.3 评标委员会如发现投标人不满足“前附表”所列情形之一的，经评标委员会审定后，将作无效标处理。

21.4 对于实质上响应招标文件要求，但在个别地方存在细微偏差的投标文件，经评标委员会审定确认后接受。对于投标报价有计算上和累计上的算术性错误的差错按下列方法进行修正。

21.4.1 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；

21.4.2 《开标记录表》内容与《投标报价分类明细表》及投标文件其它部分内容不一致的，以《开标记录表》内容为准；

21.4.3 单价金额小数点或者百分比有明显错位的，以《开标记录表》的总价为准，并修改单价；投标文件中如果同时出现上述两种或两种以上错误或矛盾的，则根据以上排序，按照序号在先的方法进行修正。

21.5 上述修正或处理结果对投标人具有约束作用，投标人不确认的，其投标文件无效。

22 投标文件的澄清

22.1 对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者修改。

22.2 投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。投标人的澄清、说明或者补正内容作为投标文件的组成部分，对投标人具有约束力。

23 详细评审

23.1 评标委员会对通过资格性及符合性检查的投标文件，根据招标文件规定的评标办法进行综合评审，未经评标委员会确认的价格和优惠条件在评标时不予考虑。

23.2 计算评标总价时，以满足采购人要求提供的全部服务内容为依据，评标价包括实施和完成全部内容所需的劳务、管理、利润、风险等相应费用，对所有列入评审范围的投标文件应适用相同计算口径，在同一基准上进行评定。

23.3 本项目中标人的确定方式详见“前附表”。

24 细微偏差

24.1 细微偏差是指投标文件在实质上响应招标文件的要求，但在个别地方存在漏项或者提供了不完整的技术信息和数据等情况，并且补正这些遗漏或者不完整不会对其他投标人造成不公平的结果。

（五）质疑与诚信记录

25 质疑

25.1 投标人认为招标文件、采购过程和中标结果使自己的权益受到损害的，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（具体格式可通过中国政府采购网 www.cccp.gov.cn 右侧的“下载专区”下载）向集中采购机构或采购人提出质疑。（采购人联系方式详见“投标邀请”）

集中采购机构地址：上海市浦东新区民生路 1399 号 16 楼 16A15 室

集中采购机构联系电话：（021）68542111；传真：（021）68542614

25.2 投标人应知其权益收到损害之日，是指：

25.2.1 对招标文件提出质疑的，为收到招标文件之日或者招标文件公告期限届满之日。

25.2.2 对采购过程提出质疑的，为各采购程序环节结束之日。

25.2.3 对中标结果提出质疑的，为中标结果公告期限届满之日。

25.3 质疑供应商不得以捏造事实、伪造材料或者以非法手段取得证明材料进行质疑。

26 诚信记录

26.1 投标人在本招标项目的竞争中应自觉遵循诚实信用原则，不得存在腐败、欺诈或其他严重违背诚信原则的行为。“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谎报、隐瞒事实，损害采购人的利益，包括投标人之间串通投标（递交投标书之前或之后），人为地使投标丧失竞争性，损害采购人从公开竞争中所能获得的权益。

26.2 如果采购人或集中采购机构有证据表明投标人在本招标项目的竞争中存在腐败、欺诈、报名截止之日前三年内在政府采购活动中有不良行为记录的或其他严重违背诚信原则的行为，则将拒绝其投标。

26.3 投标人有下列情形之一，采购人和集中采购机构将取消其评标资格，并将相关情况报浦东新区政府采购监督管理部门：

- 26.3.1 提供虚假材料谋取中标、成交的；
- 26.3.2 采取不正当手段诋毁、排挤其他投标人的；
- 26.3.3 与采购人、其他投标人或者集中采购机构恶意串通的；
- 26.3.4 向采购人、集中采购机构行贿或者提供其他不正当利益的；
- 26.3.5 在招标采购过程中与采购人进行协商谈判的；
- 26.3.6 拒绝有关部门监督检查或者提供虚假情况的；
- 26.3.7 开标后擅自撤销投标，影响招标继续进行的；
- 26.3.8 中标、成交后无正当理由拒绝签订政府采购合同的；
- 26.3.9 无正当理由拒绝履行合同的；
- 26.3.10 提供假冒伪劣产品或走私物品的；
- 26.3.11 拒绝提供售后服务，给采购人造成损害的；
- 26.3.12 政府采购管理部门认定的其他有违诚实信用的行为。

（六）授予合同

27 中标通知书

27.1 中标人确定后，采购人和集中采购机构将向中标人发出中标通知书。

27.2 中标通知书是合同文件的组成部分，对采购人和中标人均具有法律效力。中标通知书自发出后，如采购人自行改变中标结果或中标人自行放弃中标项目的，将依法承担法律责任。

28 合同授予的标准

28.1 除第 26 条的规定之外，采购人将把合同授予按第 23.3 条款确定的中标人。

29 授标合同时更改采购服务数量的权力

29.1 依据《中华人民共和国政府采购法》，需要继续从原供应商处添购的，添购资金总额不超过原合同采购金额的 10%。

30 合同协议书的签署

30.1 采购人与中标人应当在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同。

30.2 采购人和中标人应当按照政府采购相关法律法规的规定签订书面合同，合同的标的物、价款、质量、履行期限等主要条款应当与招标文件和中标人的投标文件的内容一致。

30.3 对于因采购人原因导致变更、中止或者终止政府采购合同的，采购人应当依照合同约定对供应商受到的损失予以赔偿或者补偿。

31 履约保证金

31.1 中标人在收到中标通知书后三十日内，并在签订合同协议书之前，应按“前附表”规定向采购人提交履约保证金，联合体的履约保证金由联合体主办人提交或联合体成员共同提交（招标文件另有规定的除外）。合同存续期间，履约保证金不得撤回。

31.2 如果中标人未按上述规定签订合同或提交履约保证金，采购人和集中采购机构将取消原中标决定。

第二章项目招标需求

一、说明

1 总则

1.1 投标人应具备国家或行业管理部门规定的，在本市实施本项目所需的资格（资质）和相关手续（如果有），由此引起的所有有关事宜及费用由投标人自行负责。

1.2 投标人对所提供的货物和服务应当享有合法的所有权，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。

1.3 投标人提供的货物和相关服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

★1.4 若本项目涉及国家强制认证产品（信息安全产品、3C 认证产品、强制节能产品、电信设备进网许可证等），则根据国家有关规定，投标人提供的产品必须满足强制认证要求。（详见第一章投标人须知及前附表 21.3（9））

★1.5 投标人提供的产品和服务必须符合国家强制性标准。

1.6 采购人在技术需求和图纸或图片（如果有）中指出的工艺、材料和货物的标准以及参照的技术参数或型号仅起说明作用，并没有任何限制性和排他性，投标人在投标中可以选用其他替代标准、技术参数或型号，但这些替代要在不影响功能实现的前提下，并在可接受范围内接受偏离。

1.7 投标人在投标前应认真了解采购人的维护需求、使用条件（使用空间、能源条件等）和其他相关条件，一旦中标，应按照招标文件和合同规定的要求提供货物及相关服务。

1.8 投标人应根据本章节中详细技术规格要求，采用市场主流产品或按照要求提供定制产品参加竞标。同时，**请投标人务必注意：无论是正偏离还是负偏离，都不得与招标要求相差太大，否则将可能影响投标人的得分。**一旦中标，投标人应按投标文件的承诺签订合同并提供相应的产品和服务。

1.9 投标人认为招标文件（包括招标补充文件）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。

二、项目概况

2 项目名称

浦东新区网络安全监管与保障服务

3 项目地点

上海市浦东新区范围内。

4 招标范围与内容

4.1 项目背景及现状

随着“互联网+智慧教育”的迅猛发展和教育行业信息化建设的持续推进，浦东教育需要通过专业的外包服务商开展持续的安全监管与保障服务。工作内容一日常性网络安全技术服务包括教育网信息系统（网站）应用安全监测服务、信息系统（网站）漏洞扫描服务、教育专网主机威胁监测服务、骨干网和数据中心网络系统安全服务、网络安全事件处置技术支撑服务、“40+1”网络安全现场检查技术服务等一系列服务；工作内容二各类专项网络安全服务包括教育网内主机安全防病毒服务、等级保护测评服务、网络安全综合监管平台服务等一系列服务；从制度、人员、技术、管理等方面，结合管理部门的监管措施，有效改善目前的安全状况，使得浦东教育全系统的网络安全服务保障能力得以综合提升，网络安全态势明显向好转变。

本项目总体目标是保障合同期内浦东教育行业网络信息系统的网络安全，通过招标专业服务的方式，做好全区教育信息系统的网络安全监管和保障服务工作。

4.2 项目招标范围及内容

本项目主要内容包含两部分，工作内容一为日常性网络安全技术服务，工作内容二为各类专项网络安全服务（包括主机安全防病毒服务、等级保护测评服务、网络安全综合监管平台服务），具体详见招标文件第二章项目招标需求三、技术质量要求。

本项目最高限价同预算金额，各工作内容最高限价分别为：工作内容一日常性网络安全技术服务最高限价 6,828,000.00 元、工作内容二各类专项网络安全服务最高限价 6,380,000.00 元。

4.3 本项目服务期限为：自合同签订之日起 2 年。

5 承包方式

5.1 依据本项目的招标范围和内容，中标人以包质包量、包安全可靠的方式实施总承包。

5.2 本项目不允许分包。

6 合同的签订

6.1 本项目合同的标的、价格、质量及验收标准、考核管理、履约期限等主要条款应当与招标文件和中标人投标文件的内容一致，并互相补充和解释。

6.2 合同履行过程中，如遇不可抗力或服务内容变更（以招标文件和合同约定为准），经双方商定可以调整合同金额（调整原则以招标文件约定为准），并签订补充协议。

7 结算原则和支付方式

7.1 结算原则

7.1.1 本项目合同结算价以审计价为准，中标人的中标单价和结算下浮率（如果有）不变，实际工作量以采购人或第三方按照招标文件规定的验收标准核定为准。

7.2 支付方式

7.2.1 本项目合同金额采用**分期付款**方式，在采购人和中标人合同签订，且财政资金到位后，按下款要求支付相应的合同款项。

7.2.2 分期付款的时间进度要求和支付比例具体如下：

- （1）合同签订后 30 日内，支付合同金额的 20%；
- （2）服务期满一年且验收通过，财政第二年拨款到位后 30 日内，结合考核结果支付合同金额的 50%；
- （3）服务期满两年且验收通过后 30 日内，结合考核结果支付合同金额的 30%。

7.3 中标人因自身原因造成返工的工作量，采购人将不予计量和支付。

7.4 采购人不得以法定代表人或者主要负责人变更，履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审计等为由，拒绝或者延迟支付中小企业款项。如发生延迟支付情况，应当支付逾期利息，且利率不行低于合同订立时 1 年期贷款市场报价利率。

三、技术质量要求

8 适用技术规范和规范性文件

《中华人民共和国网络安全法》

《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》

《国家信息化领导小组关于加强信息安全保障工作的意见》

- 《网络安全等级保护实施指南》（GB/T25058-2019）
- 《网络安全等级保护定级指南》（GB/T22240-2008）
- 《网络安全等级保护基本要求》（GB/T22239-2019）
- 《网络安全等级保护设计技术要求》（GB/T25070-2019）
- 《网络安全等级保护测评要求》（GB/T28448-2019）
- 《网络安全等级保护测评过程指南》（GB/T28449-2018）
- 《国家网络安全事件应急预案》
- 《教育部关于加强教育行业网络与信息安全工作的指导意见》
- 《上海市教育信息化 2.0 行动计划（2018-2022）》
- 《上海市网络与信息安全事故专项应急预案》
- 《浦东新区教育网络信息安全规划方案》2020 版
- 《浦东新区网信工作“1+6”制度体系》

各投标人应充分注意，凡涉及国家或行业管理部门颁发的相关规范、规程和标准，无论其是否在本招标文件中列明，中标人应无条件执行。标准、规范等不一致的，以要求高者为准。

9 招标内容与质量要求

9.1 工作目标及工作量清单

9.1.1 工作目标

本项目规划，旨在依靠浦东教发院现有管理能力，依托网络安全技术，借助外部网络安全专业机构和安服务承建单位之力量，形成全行业的网络与信息安服务保障体系，实现“建设服务体系、管理技术贯通、依法合规监管、创新服务模式，引领全新局面”的总体目标。

9.1.2 工作量清单

工作量清单

序号	工作内容	分项内容	数量	运维维护要求	备注
1	日常性网络安全技术服务（工作内容一）	教育网信息系统（网站）应用安全监测服务	1	根据采购人需求覆盖全部 490 个教育网信息系统（网站），提供平台工具+平台值守+预警响应+人工验证。详见 9.2 日常性网络安全技术服务要求。	
		信息系统（网站）漏洞扫描服务	1	根据采购人需求覆盖全部信息系统（网站），含教育网内的学校和教育网外的民办学校、培训机构的信息系统（网站）不少于 578 个，漏洞扫描+人工验证+整改建议。详见 9.2 日常性网络安全技术服务要求。	
		教育专网主机威胁监测服务	1	针对教育网内日均在线 14 万台的主机安全威胁监测预警+分析验证服务。详见 9.2 日常性网络安全技术服务要求。	

		骨干网和数据中心网络系统安全服务	1	骨干网和数据中心网络与安全服务，重保值守+应急保障+应急演练+攻防演练（渗透测试）。详见 9.2 日常性网络安全技术服务要求。	
		网络安全事件处置技术支撑服务	1	所有的学校及纳管的培训机构的安全事件处置、事件通告、整改咨询指导。详见 9.2 日常性网络安全技术服务要求。	
		“40+1”网络安全现场检查技术服务	1	每年对数据中心和 40 家学校（教育网内抽取）进行检查，发现问题，指导整改建设。详见 9.2 日常性网络安全技术服务要求。	
2	各类专项网络安全服务（工作内容二）	教育网内主机防病毒安全服务	1	教育网内所有单位服务器和计算机终端，年均 4 万台主机进行病毒防护，提供中心端管理平台、分析报表和数据对接，病毒事件处置与主机安全在线技术支撑等。详见 9.3 各类专项网络安全服务。	
		等级保护测评服务	1	5 个系统三级等保测评及整改，4 个系统二级等保测评及整改。详见 9.3 各类专项网络安全服务。	
		网络安全综合监管平台服务	1	网络安全大数据平台软件、资产管理模块、安全编排自动化响应子系统、漏洞管理模块、业务流程模块、网络安全综合监管平台接入授权及系统定制开发等。详见 9.3 各类专项网络安全服务。	

说明：投标人不得对表内工作量进行缩减。

9.2 日常性网络安全技术服务要求

工作内容一日常性网络安全技术服务包含六项服务：

9.2.1 教育网信息系统应用安全监测服务

（1）服务概述

监测教育网内的网站与信息系统（B/S）的安全运行情况，对发现的威胁进行告警、分析处置与安全整改建议。

（2）服务内容

- 1) 选用企业级的 WEB 安全监测系统，对不少于 490 个信息系统（含网站）进行实时监测，包括可用性监测、DNS 解析监测、网页挂马监测、网页篡改监测和敏感关键字监测、暗链监测；
- 2) 值守分析：安排专人对监测平台进行值守，对监测发现的安全威胁或警告提交高级安全技术人员进行分析；
- 3) 对分析识别过的安全威胁和安全事件，向监管平台发出安全通告信息；
- 4) 汇总分析：对监测到的安全运行状况、通告情况进行统计分析，出具相关报告。

（3）监测系统的要求

使用企业级的 WEB 安全监测系统，第一时间发现信息系统遭受外部攻击或恶意使用的情况，及时告警避免遭受黑客入侵导致的网站内容篡改、数据泄露等恶性安全事件。在安全服务周期内，由服务提供商提供监测系统实现信息系统安全实时监测预警、定期汇总监测情况、分析应用安全整体状况，

并保障应用安全监测工具的日常运行和系统授权更新。

监测系统部署在教育数据中心，服务器和存储资源由数据中心提供。

（4）服务范围

浦东教育所有纳管信息系统（网站）。

（5）服务频次

教育专网内信息系统（网站）安全监测内容与服务频次

服务名称	服务内容	服务频次	服务方式
信息系统 （网站）安 全监测	可用性监测	每 30 分钟检测 1 次	实时监测
	DNS 解析监测	每 30 分钟检测 1 次（默认）	实时监测
	网页挂马监测	每 24 小时检测 1 次	实时监测
	网页篡改监测	首页每 15 分钟检测 1 次	实时监测
	敏感关键字监测	首页每 15 分钟检测 1 次	实时监测
	暗链监测	每 24 小时检测 1 次	实时监测
	安全通告	每工作日 1 次，重保期间 按需	文件发送到综合 监管平台
	安全监测汇总分析报告（定制）	每月 1 次	文件发送到综合 监管平台

（6）信息系统（网站）安全监测系统的功能要求

1) 可用性监测

服务工具采取各类方法有效监测应用系统、网络通信等原因导致的网站可用性问题。对网站的可用性获得更为全面详细的数据，如业务中断、访问延时等。对用户指定的信息系统域名或 IP 地址进行每周 7 天×24 小时互联网连通性监测，及时发现网络中断等问题，并向用户进行预警，协助用户排查、定位故障原因。

对 Web 信息系统开放的服务端口存活状况进行实时监控。该功能模块将试图与指定 Web 服务器的指定端口进行连接，查看 Web 系统是否接受此端口的连接。

通过 Http Head 方式探测 Web 服务器的连通情况。

网站平稳度检测通过记录首页加载时间、网络延时、丢包数据，自定义预警阈值，如网站响应事件超过阈值，平台将产生告警信息。

2) DNS 解析监测

DNS 解析监测服务通过远程探测的方式，对用户指定的信息系统域名或 IP 地址进行每周 7 天×24 小时 DNS 解析监测服务，及时发现 DNS 解析故障等问题，并向用户进行预警，协助用户排查、定位故障原因。

平台通过查询指定的服务器来解析特定的 Internet 地址来测试 Web 信息系统域名的可用性。如果 DNS 服务器无法解析地址，或者不可用，或者与平台记录的历史基准不一致，平台将产生告警信息。

通过部署多个监测节点，用以监控各地 ISP 的缓存服务器对目标站点的解析结果，确保各地用户都能正常访问用户站点。

服务方一旦发现解析出现异常或解析失败人工验证后在第一时间发出告警信息。DNS 扫描会详细检查目标站点授权域服务器的各项设置，指出设置不合理的地方，并给出合理的改进建议。

3) 网页挂马监测

网页挂马监测服务通过木马检测特征库，对用户指定的信息系统页面进行定时检测，判别用户信

息系统页面是否存在被植入的木马程序，并及时向用户进行预警，协助用户定位、隔离和删除木马程序，降低挂马事件对用户造成的影响。

采用特征分析和沙箱行为分析技术对网站进行木马监测，平台监测告警后通过安全专家确认，从而实现快速、准确的发现和定位网页木马，确保用户方在第一时间发现感染的木马并及时消除。

4) 网页篡改监测

对用户指定的信息系统页面进行定时检测，通过页面的大小、页面元素等技术比对，同时采用 html 标签域比对技术，对网站进行初始化采样并建立篡改监测基准，对基准内容进行泛格式化处理，解析出 html 的相关标签作为后续比对的基准。及时发现用户信息系统页面被恶意删除、篡改等事件，并向用户进行预警，提供页面恢复方案建议，使用户能够迅速恢复页面，降低页面篡改事件给用户带来的损失和影响。

篡改监测技术的基础是网页变更监测，系统采用标题更新审查、新增内容审查、特定关键词审查等多种方式来避免将所有的网页变更都认为是篡改事件。如果审查的内容触发了告警条件，平台立即捕捉网页快照，并启动告警程序。通过远程定时监测技术，可以有效的监测网页篡改行为，并针对篡改方式提供篡改截图取证功能，提升网站篡改类安全事件的处理效率。

5) 敏感关键字监测

敏感关键字监测服务通过智能算法精确检测用户的信息系统页面中是否包含敏感关键词，并采取人工核查的方式对敏感关键字的真实性进行判定，一旦发现敏感信息及时向用户预警，定位敏感信息的发布位置，提醒用户及时删除敏感信息或对敏感信息进行脱敏处理。

平台可通过定义敏感信息字典来管理敏感字，及时发现网页及评论中的不良信息发布事件。系统内置低俗内容检测模板，包含通用的暴力、色情等低俗信息的检测匹配策略，使用户可以快速准确的定位该信息的位置。

平台可实现通过辅助关键字技术来提高告警准确率，采用中文关键词以及语义分析技术对网站进行敏感关键字监测，实现精确的敏感字识别，确保网站内容符合互联网相关规定和个人信息保护要求。

6) 暗链监测

暗链监测服务通过对检测页面的深度、页面数量自定义的爬取，从而发现暗链，并支持对已检测出的 URL 进行白名单设置。

(7) 服务交付

1) 安全事件告警

安全事件告警服务将发现的网站异常经人工确认后，第一时间通过短信、邮件、电话、监管平台上传等方式向客户发布安全事件异常告警，协助用户做好防范措施。

网站监测服务提供每周 7 天×24 小时实时监测，发生安全事故后通过电话、短信、邮件、监管平台进行预警。

2) 安全监测报告

安全监测报告服务将发现的网站异常经人工确认后，针对异常安全事件信息通过邮件方式为客户提供解决方案，用户根据解决方案对异常事件进行处置，消除安全隐患、降低安全风险。

根据采购人要求每月定期提交相应的《xx 月教育网信息系统应用安全监测报告》。

安全监测的数据根据综合监管平台的接口要求和数据格式进行汇集和集中管理。

3) 安全通告服务

安全通告服务每周汇总最新的安全漏洞信息、病毒传播信息、重大安全事故、安全法律法规、业

界最新动态等，通过邮件发送给用户，使用户实时掌握最新的安全动态与安全资讯。

根据不定期发布的安全通告消息提供《安全通告报告》。

9.2.2 信息系统（网站）漏洞扫描服务

（1）服务概述

对教育网内的信息系统（网站）、教育网外民办学校和培训机构的信息系统(578 个)进行漏洞扫描、人工验证、威胁通告、复检验证、汇总分析。

（2）服务内容

扫描评估工具的选用：中标人既要使用用户方提供的扫描评估工具，又要使用中标人自有的扫描评估工具；若用户方提供的扫描评估工具超出服务有效期，则只使用中标人自有的扫描评估工具；扫描评估工具采用国内主流的产品，脆弱性和安全威胁发现能力、大规模应用扫描效率得到用户方项目管理部门的认可；

扫描通告：使用漏洞扫描或脆弱性评估工具识别主机和应用的安全漏洞或隐患，评估可能的影响，并将通告发送到综合监管平台，由平台管理人员通告相关单位；

人工验证：安排专业技术人员对扫描工具发现的安全漏洞进行人工验证，确认安全漏洞的真实性和可修补性，出具验证报告；

汇总分析：汇总扫描工具结果，分析安全漏洞或隐患，出具安全评估报告，提出安全整改的建议。

（3）服务范围

浦东教育网所有纳管信息系统（网站）；

（4）服务频次

区级信息系统（网站）每月扫描一次，重保期间按需增加扫描次数

校级信息系统（网站）每 2 个月扫描一次（全覆盖），并进行漏洞验证

报告推送：两个工作日内将扫描评估报告推送到综合监管平台

漏洞验证：同步开展，两个工作日内

汇总分析：每月一次

专题培训：每年一次

（5）服务交付

服务期间定期出具《区级信息系统（网站）漏洞扫描报告》、《校级信息系统（网站）漏洞扫描报告》、《信息系统（网站）漏洞汇总分析报告》。

整个服务期内出具扫描报告不少于 30000 份。

经确认的漏洞扫描数据根据综合监管平台的接口要求和数据格式进行汇集和集中管理。

扫描工具情况一览表

序号	设备类型	设备状态	要求	规格要求	用途
1	扫描工具 A (绿盟)	已使用	续保		远程安全 评估系统
2	扫描工具 B (安恒)	已使用	续保		远程安全 评估系统
3	扫描工具 C		中标人提	性能要求:	脆弱性扫

	（除 A 和 B 品牌以外）		供	2U 标准式机架设备、2 个千兆电口、1TB 硬盘、双电源；允许最大并发扫描 ≥ 90 个 IP 地址，允许最大并发任务 ≥ 15 个任务，满足无限 IP 授权扫描。 功能要求： 扫描器具备网络端口与服务扫描、主机安全扫描、应用安全扫描、数据库安全扫描和安全基线配置核查于一身的功能，结合信息安全风险评估理论分析的综合安全技术扫描和管理系统，提供日常安全监测使用。	描与管理 系统（WEB 扫描）
--	----------------	--	---	--	-----------------------

投标人提供服务所涉及的工具、软硬件产品在项目日常服务期间全部由中标人提供统一管理运维服务。

9.2.3 教育网内主机威胁监测服务

（1）服务概述

通过部署在数据中心的网络安全威胁感知系统，对教育网内的服务器和主机进行安全监测，包含承载业务的服务器、终端等，对发现的问题进行分析验证，向综合监管平台发出安全预警信息，并提出安全整改建议。

（2）服务内容

- a) 主机设备安全监测：通过网络安全探针对主机系统的安全威胁、安全攻击等安全状态进行探测预警，定期出具安全监测分析报告，将相关威胁信息纳入综合监管系统；
- b) 安全加固：根据安全漏洞、弱点等安全风险，进行对应的安全加固指导；
- c) 专题培训：针对主机威胁监测系统发现的漏洞和安全风险，对主机系统的安全使用与安全维护保障进行培训。

（3）威胁感知系统

威胁感知系统具有通过隐患主动探测、日志采集、流量分析、蜜罐诱捕等多种探针采集方式，通过主动威胁检测和被动流量分析相结合的方式对僵尸网络、数据泄露、远程控制、DDOS 攻击等各类安全威胁进行实时深度检测、智能分析，定位网络中存在的安全威胁，提供全面的检测能力。

系统部署在数据中心网络出口处。

（4）服务范围

针对教育网内在线的主机（日均 12 万到 14 万台）

（5）服务频次

- a) 主机的安全监测：实时
- b) 主机安全加固：培训与指导
- c) 安全通告与跟踪监管：按需
- d) 专题培训：每年一次

（6）主机威胁感知系统的功能要求

主机威胁感知系统通过主动威胁检测和被动流量分析相结合的方式对僵尸网络、数据泄露、远程

控制、DDOS 攻击等各类安全威胁进行实时深度检测、智能分析，提供以下检测能力：

1) 快速识别服务器被植入挖矿木马

可发现服务器被植入了各种挖矿木马，以及其频繁通信的矿池服务器。

2) 及时定位内网被感染肉机

可根据 NTA 流量分析发现内网可能遭受勒索病毒、蠕虫病毒感染的主机。

3) 实时发现遭受远控木马控制主机

威胁感知系统监测流量分析内网主机与来自境外主机存在异常受控流量，发现疑似远控程序与该主机存在的远控回连请求。

4) 精准检测网站被植入后门事件

监测分析发现某移动 IP 多次访问本地区网站服务器 web 后门的行为，定位网站被植入的后门路径。

a) 攻击检测服务

全流量检测：支持全流量检测，可根据需求打开或关闭全流量检测功能。

审计协议：支持解析 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、MSSQL、DB2、Oracle、HTTPS、SMTPS、POP3S、IMAPS 等协议报文（HTTPS、SMTPS、POP3S、IMAPS 加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号；支持 LDAP 登录行为识别；支持 VXLAN 镜像流量解析检测。

检测风险类别：支持检测 WEB 攻击、异常访问、恶意文件攻击、远程控制、WEB 后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼、邮件恶意链接、DGA 域名请求、SMB 远程溢出攻击、WEB 行为分析、隐蔽信道通信、暴力破解（包括 SSH、TELNET、RDP、FTP 暴力破解）、挖矿等风险。

告警黑白名单过滤：支持对文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑 IP 白名单、域名白名单、客户端 IP 白名单、服务端 IP 白名单、WEB 风险特征白名单进行设置。

私网 IP 地理位置定义：支持对私网地址 IP 地理位置信息添加，在产生告警时，定义 IP 可正常显示所属地理位置信息。

弱口令风险检测：支持对 Telnet、FTP、POP3、SMTP、IMAP 等协议进行弱口令检测。

告警详细展现：可支持详细展现告警级别、时间、威胁名称、状态、客户端 IP、客户端 IP 所在地理位置、服务端 IP、服务端 IP 所在地理位置、报文、操作等信息，包含请求 URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度等信息。

主机威胁分析：可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等。

b) 失陷主机检测服务

远程控制检测：支持根据威胁情报、DGA 域名请求、IDS 规则、用户配置数据，发现被远程控制的内部主机。

DGA 域名请求检测：具备 DNS 协议解析功能，发现发起 DGA 域名请求的失陷主机。

挖矿行为检测：可发现利用失陷主机挖矿的行为。

c) 抓包检测服务

抓包任务：同时支持至少 16 个抓包任务抓包，每个抓包任务可配置抓包规则，按照 IP、端口、协议等信息进行抓包，将抓取的原始流量包保存于本地以供后续分析和取证使用，每个抓包任务最大包件为 20MB。

d) 管理功能

三权分立用户管理：提供三权分立的用户管理能力：系统配置管理员、用户管理员、审计员相互独立，支持自定义管理用户权限和角色。

风险处理：支持根据需要对风险状态进行选择处理中、处理完成、延迟处理、拒绝处理等。

一键登录排错：支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能。

设备状态监控：支持对设备的 CPU、内存等状态进行监控，并在设备界面中进行展示。

知识库：根据不同的风险信息，提供风险分析和处置建议知识库。

e) 日志报表

告警与报表：告警可详细展示风险级别、发生时间、告警名称、客户端 IP、服务器 IP、报文内容（URL、请求头、请求参数、请求内容）。

可根据需要针对单个告警添加白名单。

支持短信、邮件、syslog、snmp、ftp、综合监管平台等告警方式。

支持对 syslog、监管平台发送的风险信息进行加密传输。

支持同时发送多人、单条发送、发送统计等高级告警功能。

报表能够支持 WORD、PDF 等格式导出。

日志数据管理：审计数据保留策略满足天数和百分比两个控制参数，支持 web 界面可配置，且恢复数据不影响正常的审计功能。对审计日志可自动备份并加密，导入设备才能进行恢复查看，并可自动释放磁盘空间。

（7）服务交付

服务期内每月出具《学校主机系统与网络安全威胁监测报告》、《学校主机系统与网络安全威胁通告情况报告》。

网络安全威胁监测数据根据综合监管平台的接口要求和数据格式进行汇集和集中管理。

9.2.4 骨干网和数据中心网络系统安全服务

（1）服务概述

对数据中心和教育网所有接入点（骨干网）的网络设备和安全设备进行信息化资产管理、维护管理、安全管理和应急响应处置、应急演练服务、攻防演练等，确保教育网接入系统的安全可靠运行。

重保期间，提供 1 名网络安全服务专家、1 名高级网络安全工程师参与重保。

（2）服务内容

- 1) 管理体系制定：根据最新的法律法规和新的网络安全规范要求，对教育网网络系统的安全管理制度进行完善或修订；
- 2) 教育网接入点网络资产管理：资产分类明细、责任部门、重要程度、所处位置、安全状态等信息；
- 3) 网络与安全设备的维护管理，对网络系统与安全设备进行巡查、警告、维修、监控等管理；
- 4) 网络系统的安全管理，重要账户的管理、安全配置管理、维护操作管理、变更管理、远程维护管理；
- 5) 维护服务包括系统巡检服务、故障处置服务、安全配置核查服务；
- 6) 网络系统的安全事件处置服务和应急响应服务；

- 7) 针对应急预案开展应急演练；
- 8) 针对目标的信息资产进行网络安全攻防演练，以达到验证系统安全性，发现问题，解决问题；
- 9) 重保期间的安全保障、安全策略强化、安全事件研判分析、强化应急响应支撑；由专业安全团队在重要保障时期提供安全值守、应急响应服务，范围周期包括:春节假期、两会期间、五一假期、国庆假期、及年度重大社会活动期间（以两个月计）；
- 10) 网络系统的安全使用与维护保障培训。

(3) 服务范围

教育网接入点 700 到 900 个（学校网络出口）网络与安全设备。

(4) 服务频次

网络系统安全管理制度修订：一次或年度修订一次

- a) 网络系统资产登记及更新：每季度一次
- b) 网络系统的设备维护：每工作日
- c) 网络安全设备的维护管理：每工作日
- d) 网络和安全设备安全检查：两月一次
- e) 网络和安全设备安全加固：两月一次
- f) 网络故障、网络安全事件处置:按需
- g) 网络安全应急演练：每年一次
- h) 网络安全攻防演练：每年一次
- i) 网络系统安全使用与安全保障培训：每年一次

(5) 服务交付

服务期内根据服务频次定期出具《教育网网络系统安全管理制度修订稿》、《教育网网络系统资产登记表》、《教育网网络系统设备维护管理记录》、《教育网网络系统网络与设备安全维护保障记录》、《教育网网络系统维护保障总结报告》、《教育网网络系统安全事件应急响应报告》、《教育网网络系统应急演练报告》、《教育网网络系统攻防演练计划》、《教育网网络系统攻防演练总结报告》、《教育网网络系统安全培训报告》。

骨干网与数据中心网络系统安全维护与应急保障的数据根据综合监管平台的接口要求和数据格式进行汇集和集中管理。

(6) 所需工具

骨干网和数据中心网络系统安全服务提供的工具与证书：

科目名	系统安全服务所需工具		
工具名称	用途	要求	数量
资产发现工具	主动扫描，发现主机、应用等资产	1、对数据中心或骨干网范围内的主机或应用系统的指纹（对操作系统版本、开放端口、提供的服务、服务版本等）进行识别； 2、该工具可以为独立的软件或相关运维系统的功能组件； 3、具备自动探测发现未知信息资产功能，并对资产进行全生命周期管理的功能，资产类型包括主机、	1

		网络设备、安全设备、数据库、中间件、应用组件(含数据文件)等； 4、可识别数据中心的资产和骨干网范围内的资产。	
基线检查	主机安全基线检查	1、检查服务器、中间件和应用系统基础平台是否满足安全规范要求，通过检查各安全配置参数是否符合标准来度量； 2、包括账号配置安全、口令配置安全、授权配置、日志配置、IP 通信配置等方面内容； 3、要求支持等保/CIS 等多重标准、覆盖各类操作系统/应用； 4、结合资产清单，自动识别服务器需检查的基线。	1
VPN	提供安全的网络连接，支持远程安全访问	1、一体化的 IPSec/SSL 的 VPN 安全网关，设备集成企业级的状态包过滤防火墙功能、流缓存功能； 2、适合于数据中心和运维单位网络之间的或远程移动用户与数据中心网络之间的远程安全互连，支持流缓存功能； 3、支持基于 TCP、UDP、ICMP 的应用；支持主流操作系统（Windows、Linux、Mac）； 4、支持主流商业加密算法与国密算法，要求 IPSecVPN 加密速度 $\geq 100\text{Mbps}$ 。	2
堡垒机	重要系统、设备维护审计	1、具有身份认证、账号管理、授权管理、事中控制、事后审计等功能； 2、所有系统运维人员通过堡垒机对服务器、安全管理系统进行管理和运维； 3、堡垒机具有拦截非法访问和恶意攻击，对不合法命令进行命令阻断，过滤掉所有对目标设备的非法访问行为，并对内部人员误操作和非法操作进行审计监控，以便事后责任追踪； 4、堡垒机运维管理的对象不少于 200 个。	2
IDS+蜜罐	网络安全防护检测与诱捕系统	1、IDS 依照一定的安全策略，对网络、系统的运行状况进行监视，发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统的安全； 2、IDS 监测并分析用户和系统的活动，核查系统配置和漏洞，对操作系统进行日志管理，并识别违反安全策略的用户活动，针对已发现的攻击行为作出适当的反应，如告警、中止进程等； 3、与 IDS 协同的蜜罐将攻击者从关键系统引诱到专门的诱骗系统，以发现新的复杂的网络攻击。	1
Pdedu 证书	域名证书	此证书为通配符证书，支持一个域名以及该域名所有下一级域名，不限制下一级域名数量，以便业务拓展的需要。	1(2022 年)
Pudong-edu 证书	域名证书	此证书为通配符证书，支持一个域名以及该域名所有下一级域名，不限制下一级域名数量，以便业务拓展的需要。	1(2022 年)

投标人提供服务所涉及的工具、软硬件产品在项目日常服务期间全部由中标人提供统一管理运维服务。

(7) 网络安全应急响应服务的具体要求

应急响应服务主要是为了达到及时发现和解决浦东教育数据中心和骨干网日常运营过程中出现的紧急事件和重大事故，降低紧急及重大事件对信息系统的影响，以确保信息系统的稳定、可持续运营。

1) 应急预案

a) 应急预案的设计

应急预案的设计确定应急活动所需的浦东教育信息中心资源，包括人员、设备、资金和其他物资，尤其是人员的保障和对其他资源的统一调度等。应急资源的保障也包含浦东教育信息系统供应商、开发商、系统集成商，以及其它外协和相关单位的支持。

b) 应急预案的启动条件

应急预案的启动严格规定应急措施的实施流程，并确定调用应急资源的程序、决策者和相关责任人等。

c) 应急预案的演练

浦东教育信息中心的应急演练可以在仿真条件下进行，但参加演练的人员与实际执行应急预案的人员的组成相近。应急预案演练包括应急预案演练的计划安排、演练过程和效果的详细记录，演练活动的评估报告和应急预案改进建议等。

d) 评估报告和改进建议

应急预案演练的效果进行评估，评估报告对应急预案是否可操作、应急程序是否科学合理、应急资源是否迅速到位做出明确的结论，评估报告有明确的责任人。对应急预案演练中存在的问题，提出改进意见，如果问题突出，建议改进后重新进行演练。

2) 应急响应组织

e) 领导协调小组

由浦东教育信息中心分管信息化的领导和网络安全服务商、信息系统维护服务商的分管领导（组员）组成，对信息系统的安全事件和应急响应的进行决策管理。

f) 分析小组

由应急响应服务商、系统维护服务商、应用集成商技术负责人、技术专家共同组成，对安全事件分析、应急预案选择、应急处置方案制定负有直接的技术责任。

g) 数据恢复小组

数据恢复小组成员由数据库管理员、备份管理员、网络安全管理人员共同组成，负责日常数据维护与备份工作，应急事件发生时负责数据恢复工作的实施。

h) 系统恢复小组

系统恢复小组成员由系统管理员、系统维护服务商、软件开发商、硬件供应商共同组成，负责日常网络、主机、信息系统故障的排除工作，应急事件发生时负责相关系统恢复工作的实施。

i) 基础设施保障小组

基础保障小组由动力管理员、机房设施管理员共同组成，负责基础设施的日常保障工作，应急时负责基础设施的保障与恢复工作。

j) 安全保密管理小组

安全保密管理小组由用户保密管理人员、安全服务商、安全保密产品供应商、安全保密软件开发商共同组成，负责系统的日常安全保密工作，以及应急时安全保密分析调查与故障恢复工作。

k) 外围支持小组

针对不可控因素，备选各专业的信息化专家和外围服务人员，当浦东教育信息网数据

中心出现 I 级（最严重级别）网络安全事件时，可以随时邀请对应的专家和外围支持小组参与应急响应处置，确保在最短时间解决问题。

3) 事件分析

事件发生后，首先是对事件进行判断，评估系统损失，继而选择相应的应急预案或指定新的应急方案。此阶段的参与人员是应急分析小组的成员。在经过事件的定位后，选择相应的应急响应工作成员，执行应急响应预案。

4) 通知和启动

一旦确认系统遭到破坏、紧急状况发生或即将发生，通知是最初采取的应急活动，包括通知应急恢复人员、评估系统损失和执行应急计划。在启动阶段完成后，恢复人员将执行应急措施，恢复系统功能，恢复丢失或被破坏的数据。

5) 响应流程

应急服务一般由服务商的一线服务人员、二线服务人员、后备专家、原厂商及专家团队、咨询公司共同负责，领导协调小组提供决策支持。响应时间为 1 小时。具体的应急响应流程为：

- a) 出现安全事件，首先通知值班人员。
- b) 当出现骨干网络问题，值班人员对故障进行处理与初步判断，当怀疑为网络设备故障时，立即通知系统分析小组网络负责人，并填写值班记录。
- c) 分析小组网络负责人首先在电话中指导值班员进行进一步的分析指导工作，初步判断为网络安全事件时立即赶赴现场，并通知领导协调小组负责人，当分析判定在现场确认安全事件满足应急启动条件，立即通知领导小组负责人，并填写应急预案启动申请。
- d) 领导协调小组负责人批准应急预案启动申请，并组织系统恢复小组、设备保管人员以及供应商启动应急预案。

6) 恢复流程

- e) 系统恢复小组根据安全事件的类型，重新恢复系统或调换发生故障的设备，采取相应应急措施；
- f) 设备厂商对发生故障的设备进行故障分析，进行调试与检修直至设备恢复正常状态；
- g) 在下班或休息时间，系统恢复小组对已修复或更换的系统进行性能和功能测试，测试通过后恢复系统。

7) 总结阶段

安全服务商通过参与应急响应各阶段的记录信息，回顾安全事件处理的全过程，整理与事件相关的各种信息，对事件处理过程进行总结和分析：

- h) 向用户方提供经审核过的网络安全事件处理报告；
- i) 向用户方提供网络安全方面的措施和建议；
- j) 根据安全状态分析和影响分析的结果，明确安全事件等级、影响程度以及优先级等，形成安全分析报告，按照安全事件等级以及安全事件报告程序上报。

9.2.5 网络安全事件处置技术支撑服务

(1) 服务概述

由采购人网络安全管理部门负责，以安全服务提供商的服务人员为主成立网络安全通报中心，开

展网络安全威胁预警、网络安全事件处置、网络安全活动通知、网络安全情报分享为主要内容的安全通报服务，面向所有的学校及纳管的培训机构进行安全预警、预告、通告、通知和处置通报。

直接参与采购人指定的网络安全事件处置支持服务。

围绕网络安全事件进行通知、协调、管理和报告。

（2）服务内容

a) 成立网络安全通报中心，通报中心接受安全管理部门的日常管理，通报中心的主要工作人员由安全服务提供商派出；

b) 通报中心及时响应并分析安全威胁预警、安全可疑事件；

c) 根据网络安全事件处置管理制度，落实不同安全事件的报告、指挥、处置和汇报流程，组织现场处理、参与系统恢复、分析事件原因、撰写事件报告等；

d) 收集汇总事件证据、配合鉴定事件产生的原因，提交初步分析报告；

e) 对教育网外的学校或民办机构的安全事件进行通告，并指导其开展应急处置；

f) 应急处置完成后，协调专家进行安全管理和安全技术方面的分析，针对问题进行制度修订或安全技术整改，修订应急预案；

g) 直接参与采购人指定的网络安全事件处置支持服务。

（3）服务范围

所有的学校及纳管的培训机构的安全事件应急处置、事件通告。

（4）服务频次

a) 安全通告：现场值守，每周 5 天×8 小时

b) 应急响应管理：按需

c) 应急预案修订：每年不少于 1 次

（5）服务交付

服务期内按服务频次出具《网络安全通报通告日常工作记录》、《网络安全应急响应处置报告》、《网络安全管理或安全技术整改建议》。

网络安全事件处置支持服务的数据根据综合监管平台的接口要求和数据格式进行汇集和集中管理。

9.2.6 “40+1”网络安全现场检查技术服务

（1）服务概述

选择 40 所浦东教育单位和数据中心（含教育云和骨干网），每年进行一次安全检查（抽查），出具安全检查报告，并根据自查结果进行安全状态分析评估，调整安全服务策略，强化安全管理，修订安全规划。

（2）服务内容

a) 安全检查计划：制定安全检查计划，包含检查范围、计划执行、人员调配、检查表单编订。

b) 安全检查执行：每年开展一次安全抽查，检查内容包括安全管理制度的执行情况、安全技术措施的有效性、安全配置与安全策略的一致性、密码产品的使用合规情况、数据安全与个人信息保护的情况。

c) 安全汇总分析：汇总安全检查数据，形成安全检查报告，对检查中发现的问题和隐患，根据网络安全法规和规范要求选择调整安全措施，依据风险分析和业务需求调整安全策略和安全配

置。

d) 安全工作优化：根据保护对象的安全保护要求及其他相关系统、使用群体，进行新一周期的安全规划和安全方案设计。

（3）服务范围

抽样 40 所浦东教育单位+数据中心（含教育云和骨干网），抽取按照采购人制定的规则进行。

（4）服务频次

每年一次、检查周期约一个月。

（5）服务交付

服务完成后 7 日内交付《XX 学校网络安全检查报告》、《XX 学校安全问题汇总报告》、《学校网络安全规划调整建议》。

网络安全现场检查服务数据根据综合监管平台的接口要求和数据格式进行汇集和集中管理。

9.3 各类专项网络安全服务

工作内容二各类专项网络安全服务包含三项服务：

9.3.1 教育网内主机防病毒安全服务

（1）服务概述

针对教育网内的服务器、终端（主机）、数据中心所有服务器提供恶意代码与病毒防护、补丁管理等终端安全防护功能，对主机防病毒系统提供安装、使用、维护服务，对恶意代码和病毒事件进行分析、紧急处置，开展终端安全专题培训。

（2）服务内容

- 1) 防病毒服务体系：选择大型企业级的病毒防护系统，兼顾补丁管理等终端安全功能，防病毒体系支持分区分级管理，支持虚拟化、移动终端、哑终端、信创平台等新的计算形态，多中心管理能力，管理策略与相应的服务规模适合浦东教育要求。
- 2) 威胁发现：防病毒系统收集终端上的各种安全状态信息，包括：漏洞修复情况、病毒木马情况、危险项情况、安全配置以及终端各种软硬件信息等。这些状态信息会汇集到控制中心，安全服务值守人员可全面了解网内所有终端的安全情况、硬件状态以及软件安装情况。
- 3) 立体防护：系统具有漏洞修复、病毒木马查杀、黑白名单、硬件准入、软件准入等多样化的防护手段，从准入、防黑加固、病毒查杀、软件和上网行为控制等多个层次，保障终端安全。
- 4) 安全管控：对防病毒和防恶意代码系统进行三级四区一中心管理，病毒管理中心为安全管理人员提供统一修复漏洞、统一杀毒、统一升级、流量管理、软件统一分发卸载等管理功能，具有分析报表和数据对接能力。
- 5) 及时升级病毒库，对病毒传播事件进行识别、报警和病毒事件紧急处置。
- 6) 汇总分析：对病毒防护的安全运行状况进行分析，并出具相关报告。
- 7) 专题培训：对学校网管员开展防范恶意代码与病毒的培训。

（3）服务范围

- 1) 针对教育网内主机 4 万台进行部署；
- 2) 学校、分中心、中心三级管理中心。

（4）服务频次

- 1) 管理中心值守：每周 5 天×8 小时
- 2) 监测告警服务：按需
- 3) 恶意代码与病毒事件处置服务：按需
- 4) 汇总分析：每月一次，重保期间按需
- 5) 专题培训：每年一次

（5）服务交付

根据服务要求定期交付《教育网恶意软件与病毒防护监测报告》、《教育网恶意软件与病毒防护情况报告》、《病毒防护汇总分析报告》与《安全培训相关文档》。

恶意软件与病毒防护数据根据综合监管平台的接口要求和数据格式进行汇集和集中管理。

（6）防病毒系统要求

1) 终端病毒与恶意代码防范

终端安全防护系统，支持对蠕虫病毒、恶意软件、广告软件、勒索软件、引导区病毒、BIOS 病毒的查杀，提供多引擎的协同联动处置工作。

可提供云查杀功能，提高病毒检出率，降低系统资源占用。通过使用云端的黑白名单验证的方法，可以最大限度的保护数据安全。

提供主动防御功能，防御未知病毒、未知威胁和 0-Day 攻击。

2) 双病毒特征库与双病毒检测引擎

提供双引擎的查杀技术，采用两套独立的病毒库、病毒检测引擎对已知病毒进行检测，以提高检测的准确率。

3) 样本黑白名单管理

为了避免内网出现误杀、漏杀文件，系统需要具备自定义文件黑白名单功能，可以针对全网批量添加或导入文件名、文件 MD5+SHA1 名单的方式，解决误杀问题，以及克服突发应急安全事件时病毒库未及时更新仍可有效查杀特种木马等问题。

4) 全网终端漏洞统一维护管理

要求终端安全系统可以对全网计算机进行漏洞扫描把计算机与漏洞进行多维关联，可以根据终端或漏洞进行分组管理，并且能够根据不同的计算机分组与操作系统类型将补丁错峰下发，在保障网络带宽的前提下可以有效提升全网整体漏洞防护等级。

5) 补丁管理

提供国内的补丁高速下载渠道，补丁事先进行兼容性验证。

系统具有补丁安装回退机制，在装了相关补丁导致系统出现蓝屏或其他异常状况后，可以回退到打补丁之前的上一个系统状态。

可以进行补丁下载与安装的统一调度，保证终端用户的系统资源在打补丁时被大量占用，影响用户正在进行的作业。同时对于正在编辑文档的用户进行提示，保护用户正在编写的文档。

6) 弹窗拦截

终端安全管理系统提供软件弹窗拦截功能，管理员可通过策略通道，当开启此功能后，可拦截教学电子白板、一体机第三方软件中含有不利于青少年健康成长信息的弹窗。全屏模式拦截和全天开启拦截两种模式，支持教职工在课堂全屏放映 PPT 或全屏播放视频时拦截，同时终端用户可在终端的设置中心按需调整开启或关闭弹窗防护功能并选择相应模式。

终端会在第三方软件弹窗时自动拦截，并自动上报给控制中心。管理员可以通过查询功能，分别查看不同时间不同分组的终端拦截日志。可以记录每次拦截的时间、次数、位置，教学的管理者可以通过弹窗事件作为考核学校教育质量的一个技术指标。

7) 流量监控

通过使用终端安全管理系统维护管控模块中的单点管理功能，管理员可以了解指定终端的网络流量情况，包括终端的实时网络速度、一段时间内的下载上传流量等，帮助管理员查证及定位网络中消耗大量带宽的终端，避免非法应用占用大量带宽。

8) 非法外联

非法外联管理模块可以针对浦东教育经常遇到的通过 4G 网卡、随身 WiFi 等方式使内网电脑可以通过非法途径连接外网导致核心数据泄漏等问题的出现，非法外联管理模块无论终端使用何种方式连接外网都可以在第一时间对管理员发送告警并隔离非法终端，在最大程度上保障数据中心及学校核心数据安全。

9) 应用程序安全

应用程序安全支持三种策略：针对终端在线作用、针对终端离线作用和针对在线和离线终端作用。应用程序安全支持进程黑白名单，添加进白名单的进程为信任进程，而黑名单中的进程为恶意进程，系统将直接阻断该类进程。另外，还有进程红名单，添加进程红名单的进程为必须运行进程，可以防止恶意程序对该必备类型进行破坏。

10) 网络安全

网络安全防护一个支持多种策略，管理员可以添加某些网络连接的协议类型，IP 地址和端口号或者添加 URL 地址来使它成为黑名单或者白名单，从而保证用户网络安全。

11) 外设管理

采用策略化的外设管理模式，针对不同类别外设设置多个策略，一个策略可以包括多种类型设备的控制，使管理策略更有针对性，并支持分配到不同的分组上面。管理员可通过终端安全管理系统对 PC 终端外设进行强有力的全面管控，杜绝数据外泄和感染病毒的风险。

12) 桌面安全加固

浦东教育下辖学校的终端数量不断增加，PC 统一配置逐渐成为管理中的突出问题。如果没有集中管控手段，逐台操作工作量非常大，且 PC 用户也会擅自变更配置，会造成内网 PC 的基本配置无法统一管理，出现诸如账户密码太简单被恶意软件渗透，私设代理上网引入外界风险等一系列问题。桌面安全加固能帮助信息中心及校园的 IT 管理员对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件检查等功能进行细粒度的统一强管控，并支持不同的分组设置不同的策略功能。协助 IT 管理员做到全网终端统一配置的管控目标，提高 IT 管理员的维护水平。

13) 硬件信息资产管理

系统具备跟踪硬件信息资产变更功能，可帮助管理员及时获取硬件信息资产的变更记录，硬件新增、丢失情况，对硬件变更准确监控，及时预警，方便财务审计，轻松构建专业的硬件信息资产监控与审计平台。

14) 系统自动升级

在无须维护管理人员参与的情况下，对客户端软件、管理控制台软件、客户端病毒特征库、系统/应用的漏洞补丁进行自动下载、升级与安装。

为了避免升级过程中导致网络拥塞，终端的升级将从内网的升级服务器统一拉取升级文件，即终

端不会从位于 Internet 的升级服务器下载升级文件。

15) 远程协助功能

提供远程协助功能可对浦东区各个校园需要帮助的计算机终端进行远程维护操作，帮助远程计算机终端进行异地操作和检查系统问题。

16) 终端 Agent 强制安装与运行

终端 Agent 一旦安装之后，便强制运行，不允许终止 Agent 进程的运行，并且默认情况下不允许卸载，即不能手工卸载 Agent 程序，也不允许第三方工具对 Agent 程序进行删除，如必须卸载 Agent 软件，必须提供卸载密码。

(7) 服务工具与产品的技术要求

分类指标	指标要求	
1、基础功能	控制中心管理	管理中心采用 B/S 架构，当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受，支持双因子认证登录方式； 为防病毒系统相关的关键功能，请提供产品截图予以证明。
	客户端管理	支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护，支持设置自我保护功能；
2、防病毒	病毒查杀日志	病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间；
	病毒防护报表	病毒报表支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒发现触、方式统计、趋势图表、按分组、按终端、按病毒名称；
	病毒扫描	支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，层数可达 10 层； 为防病毒系统相关的关键功能，请提供产品截图予以证明。
	主动防御	支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护； 为防病毒系统相关的关键功能，请提供产品截图予以证明。
	网络防护	支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁；
	杀毒引擎	支持不少于三个杀毒引擎混合使用，提高病毒检出率；
3、补丁管理	自动编排修复漏洞	支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。 为防病毒系统相关的关键功能，请提供产品截图予以证明。
	漏洞修复设置	支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段；
	补丁日志	支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞 CVE 编号、漏洞 CNVD 编号、未安装、已安装、已安装未生效、已排除、未更新

		补丁库。并支持导出统计报表； 为防病毒系统相关的关键功能，请提供产品截图予以证明。
4、终端管控	外 设 管理	支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径， 通过添加实现例外或加黑； 为防病毒系统相关的关键功能，请提供产品截图予以证明。
	进 程 管理	支持终端进程红名单、黑名单、白名单功能。可设置核心进程必须运行， 也可保护核心进程不被结束，违规并告警；
	知 识 库	支持统计终端的出口地址列表，搜集终端连接的无线信号信息统一展示， 标识出 ssid 可连通互联网，可连通服务器的情况，汇总展示内网终端上报的 进程信息，支持设置进程匹配规则；
	违 规 外联	支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、 终端锁屏、断网+锁屏处理；支持例外白名单添加；
	能 耗 管理	支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外 开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、 锁定+关闭显示器、休眠和睡眠处理； 为防病毒系统相关的关键功能，请提供产品截图予以证明。
	网 络 防护	支持对网卡进行防护，支持阻止终端修改 IP 地址、使用动态 IP 地址、热点 创建和 IPV6 地址使用等，可自定义提示内容和生效时间；
5、主机防火墙	支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任 意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自 定义端口范围、支持自定义目标 IP，支持输入 IP 范围；	
6、认证信 创	同类产品具有信创版，支持本项目特定终端的需求； 为防病毒系统相关的关键功能，请提供产品截图予以证明。	

9.3.2 等级保护测评服务

(1) 服务概述

针对数据中心的重要信息系统（网站）提供等级保护测评及协助整改服务。

(2) 服务内容

- 1) 等级保护测评：针对数据中心的应用信息系统进行安全等级保护测评，测评方式是委托具有专业资质的第三方测评机构进行安全测评，测评满足信息中心对时效性的要求；
- 2) 根据安全级别定期进行等级测评，发现不符合项按要求进行整改，现有安全手段或设施不能满足的立项建设或整改；
- 3) 等级保护测评协助服务：协助进行等级保护备案、测评准备、安全整改以及安全加固方案编订等工作；
- 4) 将通过测评的报告信息和整改的相关信息纳入综合监管平台。

(3) 服务范围

纳入等保测评的信息系统（网站）9 个。

第一轮 三级等保测评 信息系统（网站）5 个；

第二轮 三级等保测评 信息系统（网站）5 个；

二级等保测评 信息系统（网站）4个。

（4）服务频次

项目第一年和第二年每年一批

（5）服务交付

服务完成后定期出具《XX 信息系统等级保护测评报告》、《XX 信息系统等级保护加固方案》。

重要信息系统等保测评服务的数据根据综合监管平台的接口要求和数据格式进行汇集和集中管理。

9.3.3 网络安全综合监管平台服务

（1）服务概述

网络安全综合监管平台是一种采集全网流量及日志数据，结合机器学习、数据建模、行为识别、关联分析、人工智能等方法，对海量异构的安全数据进行分析，以资产、威胁、脆弱性等维度进行安全分析及监管的模式，从浦东教育系统的实际业务发展目标和安全监管与运营需求的角度出发，打造特定的网络安全能力，贯穿安全体系的建设、使用、管理、运维等全周期，高效整合技术、工具、服务、流程、人员等全要素，打通网络安全预防、保障、监控、应急等全流程，构建面向浦东新区教育的体系化安全运营能力，并生成全方位的安全全景视图，实现数据的长时间窗口存储、全文检索分析、异常行为检测和安全合规要求，支撑安全决策和应急响应，帮助用户建立安全预警机制，增强整体安全防护能力，使得浦东新区教育的网络综合安全可知、可见、可控。

浦东教育网络安全综合监管平台的服务范围包括：数据中心服务器区、核心交换区、办公区、教育云区等重要网络区域，以及各学校的互联网业务区、办公区以及服务器区等。

平台符合信创相关要求。

（2）服务内容

- 1) 平台租赁及运营服务。平台的租赁及运营服务包含两部分内容，一是为网络安全综合监管平台租赁服务，平台包含数据采集子系统、数据分析子系统、监管工作子系统等基础功能模块；二是平台的运营支撑服务，运营支撑服务通过人工现场值守及安全专家二线支撑的方式，实现整个平台的技术咨询、关联分析规则制定、安全威胁信息流转处置以及平台故障处理等运营服务工作。
- 2) 场景化定制服务。通过对浦东教育安全管理工作沉淀的数据分析，深度结合浦东教育的安全监管工作的现状需求，分析总结出符合安全监管工作实际需要的场景模型，并对场景模型进行流程分析、数据对接分析、功能设计分析与数据可视化展现的定制化设计服务。

包括以下功能模块：

- 数据采集与系统对接服务
- 数据分析与大数据处理服务
- 信息资产发现与管理
- 网络安全感知与威胁分析服务

- 安全服务与保障业务监管服务
- 安全通报与督导服务
- 网络安全运营与监控服务
- 安全事件协同响应与处置
- 数据报表管理与数据可视化服务
- 安全管理绩效考核服务

（3）服务目标

- 1) 实现信息资产管理全面化。通过分析现有安全管理数据，对接信息资产发现类设备工具，实现信息资产的探测、统计、管理，包括网络设备、安全设备、服务器、IP、域名及安全相关人员等信息等，对信息安全资产的监管是实现信息系统安全监管的必要工作，有针对性的进行安全监管。
- 2) 实现安全监管自动化。建立跨部门的监管业务协同机制，实现责任告知、安全状态告知、日常监管、联合惩戒、联合处置、监管预警、报表统计等功能，构建监管处置协同应用体系。
- 3) 实现安全业务流程化。对于安全业务工作进行流程化，对安全业务处置过程进行全程监督，实现安全事件处置事前、事中、事后“协同联动、全程监管”，提高安全维护效率和规范化，提升安全事件处置效果。
- 4) 实现数据报表立体化。以信息化方式归集统计安全问题数据，对网络安全事件全流程跟踪，全方位展示，实现网络安全工作线上监管，宏观把握教育网络安全态势。
- 5) 实现威胁处置联动化。集中汇聚各类安全设备、上级通告、外部威胁等数据，通过关联性数据分析，联动安全设备，实现安全威胁联动处置，自动流程流转，提高安全处置效率，降低安全维护压力。
- 6) 实现安全工作量考核。围绕网络安全管理工作的开展、监管、评价，及时收集和监控管辖单位的安全事件与信息反馈，针对考核单位进行安全绩效评分，衡量其在网络安全管理工作中的各类要素，勾绘出网络安全概况，规范日常网络安全管理工作。
- 7) 实现资源管理规范。拓宽数据获取渠道，整合网络安全信息系统数据、学校教育单位数据和第三方安全通告数据，构建汇聚式一体化数据库，为平台打下坚实稳固的数据基础。
- 8) 助力信息安全决策。在大数据分析监测基础上，加强对浦东教育安全工作的事中事后监管，侧重公办学校、培训机构的落实安全工作监管、维护团队处置过程监管，提升监管效能，为浦东教育预见信息安全问题、辅助决策提供基础支撑。

（4）服务范围

所有纳管的信息资产、系统、威胁、警告、事件等。

对各服务科目的数据进行集中采集、统计、分析和展示，并根据用户方的格式要求进行报告定制，形成周报、月报和年报。

(5) 服务交付

根据服务要求定期交付《网络安全综合监管服务报告》、《网络安全综合监管平台的日常任务完成情况统计报表》、《网络安全预警、威胁、事件通告汇总》、《网络安全管理考核记录与汇总》。

(6) 其他要求

平台软件通过第三方软件测试和安全测评。

(7) 服务工具与产品的技术要求

分类指标	指标要求	
1、安全综合监管	威胁攻击监管	展示系统攻击、脆弱性等资产安全监管，告警处置、资产管控、告警调查量等安全运营态势和各种网络安全风险的状况
	平台运营监管	安全运营态势展示平台总体安全运营情况，包括新增告警量、调查中告警量、处置完成告警量、已审批流程量
	整体安全监管	展示网络威胁攻击源地理分布、网络威胁实时告警列表、网络攻击类型占比、系统攻击类型占比、脆弱性分类占比、用户异常行为类型占比、系统攻击分布等
	综合安全大屏	展示内网安全、外部威胁、威胁源 IP TOP10、被攻击目标 IP TOP5、威胁攻击趋势、威胁级别分布、安全事件确认列表、预警安全事件列表、管控资产量等
	互联网安全大屏	展示全球被攻击源 IP TOP5、攻击趋势、攻击类型、被攻击域名 TOP5、被攻击最多 URL TOP5、域名攻击源区域 TOP10、威胁级别分布、实时事件
	内网安全大屏	展示内容：资产安全评级、内部受攻击主机、攻击趋势、系统威胁情况、实时事件、攻击杀伤链、威胁级别； 为综合监管平台相关的关键功能，请提供产品截图予以证明。
2、仪表盘	自定义仪表盘	自定义仪表盘可根据使用者对于图形化、数字化展示的要求，进行自定义配置，支持定义展示时间段、刷新时间间隔、添加组件、过滤数据、设置背景等
3、事件管理	安全事件	对平台内的安全事件进行列表展示，提供事件搜索功能，可以通过事件等级、责任人、事件名称、处置状态进行快速搜索；支持通过时间查询安全事件；支持安全事件的批量导出和批量处置功能
	事件策略	支持自定义配置归并策略，将彼此存在关联性的告警，自动化归并整合；支持策略的新建和导入；支持通过关键字快速搜索策略
4、告警管理	告警列表	用于对告警策略的输出的安全告警的综合展示，包含条件搜索、告警跟踪趋势、告警列表
5、资产管理	资产管理	支持对业务系统、IP、域名、设备、服务等分别进行管理，支持对资产详情进行编辑和查看

6、漏洞管理	资产视角	可以从宏观角度，观察当前维护的资产当中，总体的脆弱性风险评分、资产总数、资产风险比例、高危资产、资产清单，并定位具体的资产，对漏洞进行排查
	漏洞视角	支持以漏洞本身为切入点，展示系统漏洞发展趋势、漏洞处置状态、漏洞清单等
	漏洞清单	漏洞清单从系统漏洞和网站漏洞两个维度对发现的漏洞进行展示，并支持多种类型的查询条件
	扫描任务	扫描任务支持对监管平台对接的扫描器设备的管理和对扫描任务的创建与跟踪； 为综合监管平台相关的关键功能，需提供产品截图予以证明。
7、策略管理	实时策略	支持展示不同分类的实时策略，支持实时策略的新建、查看、编辑、复制、启用、关闭，也支持导入、导出。需支持内置模板，实现不同的字段过滤功能
	离线/基线配置	支持展示不同分类的离线/基线策略，支持离线/基线策略的新建、查看、编辑、复制、启用、关闭，也支持导入、导出，支持以清单模式展示策略/模型的详细信息
8、报表中心	报表列表	报表列表是对报表任务执行结果的管理，可以进行报表导出和删除操作；列表详情展示报表的名称、报表任务、报表选用模板和生成时间
	报表任务	报表任务分类两大类：单次报表任务和周期报表任务，可以对报表任务进行新增、删除、编辑和执行
	报表模板	报表模板分两种类型：内置默认综合报表模板和自定义模板。内置模板主要包括平台运行状况、安全概览、告警分析、威胁分析、漏洞监管；自定义模板可以根据自身需要自定义报告内容，支持图表和文字结合； 为综合监管平台相关的关键功能，需提供产品截图予以证明。
9、情报管理	威胁情报	威胁情报支持把情报数据导入到监管平台，可以手动添加或批量导入
	在线查询	在线查询支持本地和微步在线情报查询，输入关键信息比如 IP、URL、手机号、文件哈希值等进行情报在线查询。
10、系统管理	用户管理	支持管理系统操作用户，展示用户列表，支持新建、编辑、删除，并支持通过账号、姓名、工号、部门等条件进行搜索
	部门管理	包括用户账号、用户姓名、用户工号、用户状态、部门、角色等的管理
	权限管理	可编辑角色的应用操作权限，最低细化到二级目录
	安全设置	系统登录安全相关的设置，包括密码复杂度、登录失败次数、登录失败处理、密码修改周期、web 访问方式、SSL 证书、web 访问限制

11、数据采集功能要求	网络安全设备采集	支持主流安全设备、网络设备、主机、数据库、中间件、应用系统和虚拟化系统的日志采集功能，包括但不限于：防火墙、IPS/IDS、WAF、漏扫设备、DLP、基线核查设备等
	采集代理控制	采集代理支持资源消耗的限制配置：CPU 核数、CPU 占用比例、文件句柄数、内存占用、EPS 速度
	采集代理类型	支持 Linux、Windows 主流版本环境下代理方式采集实时应用日志数据
	数据采集类型	支持多种数据采集方式，包括 Syslog、FTP、文件、JDBC/ODBC、Kafka、接口、主机终端(win/linux)Agent、RabbitMQ、SNMP、Pulsar、HDFS、oracle、mysql 等，支持进行水平扩展分布式数据采集
	数据解密	支持对 base64 加密的数据进行解密操作，支持 avro 反序列化数组、集合等对象； 为综合监管平台相关的关键功能，请提供产品截图予以证明。
	敏感数据脱敏	支持对隐私数据的保护，对采集数据中的敏感数据进行脱敏处理，支持常用身份证、电话号码、电子邮件等，同时支持自定义设置脱敏规则； 为综合监管平台相关的关键功能，请提供产品截图予以证明。
	流量数据采集	支持高速大流量采集，支持 af-packet 与 dpdk 模式下，网络流量旁路镜像多网口采集，采集方式支持单采集器采集、分布式采集
12、数据存储功能	基础数据存储	支持原始日志、范式化日志事件、告警等数据全量集群存储，根据不同的数据集特点，可以分别设置不同的存储策略，包括：数据副本的设置，数据分片个数的设置
	数据备份存储策略	界面支持备份的数据直接转储到 NFS 或 HDFS 外部存储组件上； 为综合监管平台相关的关键功能，请提供产品截图予以证明。
	网络流量数据存储策略	存储可根据源目的 IP、端口四元组条件对 PCAP 存储数据进行过滤，并支持协议解析数据的条件过滤
13、高级分析	机器学习算法分析	结合历史事件对进行离线长周期分析，支持机器学习算法，发现未知威胁事件，支持任务模式，结果可展现相关联的原始事件详细内容
	威胁场景自动聚合溯源分析	可持续进行威胁评估，随时间变化持续加入相关告警等，并可根 据威胁的严重程度与影响面，动态给出威胁等级和分数进行优先级排序，便于快速响应处置
	历史数据回溯检测	新增分析规则或更新威胁情报后，可对已有历史数据进行规则验证或利用规则和更新后的情报针对历史数据进行威胁追踪发现
	异常行为挖掘技术	支持基于 CUBE 的“多维度行为基线引擎”和“行为会话重组引擎”，实现基于行为分析的特征提取和风险指标计算，使用机器学习算法和预定义规则找出严重偏离基线的异常行为；为综合监管平台相关的关键功能，请提供产品截图予以证明。

		支持上下文感知技术，组合用户和实体维度信息管理模块、自动用户及实体发现模块和 ETL 动态补全三个功能模块，实现针对分析对象的上下文感知，自动发现未知的账号、设备、应用等； 为综合监管平台相关的关键功能，请提供产品截图予以证明。
	两级数据分析	构建在机器学习算法之上的异常和威胁两级分析架构，大幅减少告警量，减低误报率，并且两者关联展现； 为综合监管平台相关的关键功能，请提供产品截图予以证明。
	可编排算法调度模块	支持分布式调度引擎，支持实时数据和历史数据的分析，为综合监管平台相关的关键功能，请提供产品截图予以证明。 支持多种聚合和分析算子,可以实现对数据的清洗、转换、聚合、分析等功能。
		内置多种有监督和无监督学习算法，支持在流处理中引入神经网络算法
		支持基于管道符方式进行分析算子编排，支持界面返回结果； 为综合监管平台相关的关键功能，请提供产品截图予以证明。
14、网络安全管理绩效考核	设置考评机制和评分标准	参照市级主管部门网络安全绩效考评系统设置考评机制和评分标准，规范考核学校、直属机构的网络安全管理活动，并可根据用户实际考核情况进行定制，由采购人方审定； 为综合监管平台相关的关键功能，请提供产品截图予以证明。
	对网络安全管理全流程进行跟踪考评	设置网络安全管理考评点，收集并审核过程资料、报告和留痕信息，对网络安全管理全流程进行跟踪考评，有效反映各单位网络安全管理的实际工作和成效
	网络安全管理评分与对比分析	支持对考评项的评分对比、各阶段的评分对比，及时提醒安全管理任务未完成的情况，反映加分项和扣分项，对各单位考核结果进行对比排序，体现网络安全综合治理的成效； 为综合监管平台相关的关键功能，请提供产品截图予以证明。
15、用户实体行为展示	风险评估	以用户维度，对相关高风险用户进行行为分析评估，包括：用户风险评分，用户行为溯源、用户评分周期变化、异常行为挖掘、组内其他用户风险状况
	风险总体展示	风险展示：通过异常、威胁、用户、设备、应用、数据等维度进行整体的风险状况的展示； 为综合监管平台相关的关键功能，请提供产品截图予以证明。

9.4 其他要求

投标人根据服务需要提供相关工具和软件，费用列入投标报价，服务期内不再产生另外费用。

投标人提供的系统平台、工具、软件产品拥有知识产权，非 OEM 产品。属于网络安全类的产品或工具如具有国家网络安全专用产品安全认证或安全检测通过的证书，请在投标文件中提供，并提供具体技术要求的相对应的产品截图予以证明。

投标人提供的服务工具、产品确保及时更新到最新版本，相关的引擎、特征库、知识库、安全机制等为最新。

9.5 服务范围

9.5.1 点位分布

数据中心（电信临港机房）、浦东各公办教育单位（含未来新开办）、民办教育单位（含未来新开办）、浦东教育纳管的培训机构（含未来新开办）。

9.5.2 服务范围

（1）信息系统（网站）

序号	部署位置	数量	服务内容	备注
1	部署在教育云内	490	应用监测， 漏洞扫描	如有新增，同时纳入
2	部署在教育网外	88	漏洞扫描	如有新增，同时纳入

（2）纳管单位

序号	类别	数量	服务内容	备注
1	公办教育单位	497	应用监测， 漏洞扫描、 事件处置、 安全检查、 防病毒	如有新增，同时纳入
2	民办教育单位	155	应用监测、 漏洞扫描、 事件处置、 安全检查	如有新增，同时纳入
3	培训机构	28	漏洞扫描、 事件处置	如有新增，同时纳入

（3）监管平台需对接系统（包括但不限于）

序号	类别	数量	备注
1	运维平台	1	
2	统一云管平台	1	
3	网络威胁态势感知平台	1	
4	WAF 管理平台	1	
5	防火墙管理平台	1	
6	上网行为管理平台	1	
7	服务器端防病毒系统	1	

8	终端防病毒系统	1	
9	防篡改管理平台	1	
10	应用监测平台	1	
11	漏洞扫描系统	3	
12	日志系统	1	

10 人员及设备要求

10.1 人员要求

投标人为本项目提供的项目组所有人员为本单位职工（在投标文件中提供运维服务团队人员近 3 个月内的在职证明材料），且为该项目施工现场的实际操作者。

本项目服务团队人员要求 36 人，其中项总负责人 1 人，项目经理 2 人（工作内容一日常性网络安全技术服务项目经理 1 人，工作内容二各类专项网络安全服务 1 人），高级技术服务人员 12 人，中级技术服务人员 12 人，等保服务人员 3 人，驻场服务人员 6 人；未经采购人同意，中标人不得调换或撤离上述人员，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。

本项目中人员岗位要求（但不仅限于）详见下表。

人员配备一览表

序号	岗位名称	建议配置岗位人数	基本要求	备注
1	项目总负责人	1	具有类似的网络安全项目管理经验不低于 5 个，网络安全技术工作十年以上（含）的经验，项目总负责人参与项目的管理决策工作，具备协调服务供应商内部资源的权限，具备国内项目管理类职称和专业领域高级职称，在投标文件中提供近 3 个月的内在职证明材料及相关资格证书扫描件	
2	项目经理	2	项目经理为本项目专门设置，分别支撑保障对应的工作内容；参与指定工作内容的项目日常管理活动，网络安全技术工作五年以上（含）的经验，具备国内项目管理类职称和专业领域高级职称，在投标文件中提供近 3 个月的内在职证明材料及相关资格证书扫描件	
3	高级服务人员	12	具有网络安全技术工作五年以上（含）的经验，高级工程师职称（或相当于高级）并提供资质证明材料，在投标文件中提供近 3 个月的内在职证明材料及相关资格证书扫描件。 包括但不限于以下负责人：监测服务负责人、漏洞扫描负责人、主机威胁监测负责人、应急演练负责人、重保负责人、网络安全现场检查负责人、主机防病毒负责人、等级保护测评负责人、综合监管平台负责人，各 1 名。	
4	中级服务人员	12	具有网络安全技术工作三年以上（含）的经验，中级工程师（或相当于中级）并提供资质证明材料，在投标文件中提供近 3 个月的内在职证明材料及相关资格证书扫描件	
5	等保服务人员	3	具有等保服务工作经验，等级保护类职称并提供资质证明材料，在投标文件中提供近 3 个月的内在职证明材料及相关资格证书扫描件	

序号	岗位名称	建议配置 岗位人数	基本要求	备注
6	驻场服务人员	6	要求最少 3 个专业领域相关职称服务人员,其余人员具有网络安全技术工作两年以上(含)的经验,具备独立开展网络安全服务工作的能力,在投标文件中提供近 3 个月的在职证明材料及相关资格证书扫描件	
	合计	36		

10.2 设备要求

投标人在实施本项目时,配备能完成本项目的相关材料、制品、设备、车辆等。

(1) 本项目所有材料、设备,由中标人自行解决,相关费用包含在报价中。

(2) 本项目所用的材料、制品、设备等,供货单位送达施工现场后,由中标人负责办理验收交割手续,并负责日常保管工作。

10.3 运维办公场所要求

投标人在中标通知书发出之日起 15 日内到达用户方指定的运维办公场所。

11 安全生产、文明施工（安装）与环境保护要求

11.1 投标人应具备上海市或有关行业管理部门规定的在本市进行相关安装、调试服务所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由投标人自行负责。

11.2 在项目实施期间为确保安装作业区域及周围环境的整洁和不影响其他活动正常进行，中标人应严格执行国家与上海市有关安全文明施工（安装）管理的法律、法规和政策，积极主动加强和落实安全文明施工（安装）及环境保护等有关管理工作，并按规定承担相应的费用。中标人若违反规定野蛮施工、违章作业等原因造成的一切损失和责任由中标人承担。

11.3 中标人在项目实施期间，必须遵守国家与上海市各项有关安全作业规章、规范与制度，建立动用明火申请批准制度，安全用电等制度，确保杜绝各类事故的发生。

11.4 中标人现场设备安装负责人应具有专业证书，安装人员必须持证上岗。中标人应对设备安装、调试期间自身和第三方安全与财产负责。

11.5 中标人在组织项目实施时必须按安装施工计划协调好现场施工（安装）工作，在项目验收合格移交前对到场货物承担保管责任。中标人在项目实施期间必须保护好施工区域内的环境和原有建筑、装饰与设施，保证环境和原有建筑、装饰与设施完好。

11.6 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安全文明施工（安装）和安全生产管理措施，同时应适当考虑购买自己员工和第三方责任保险，并在报价措施费中列支必须的费用清单。

12 运维质量和考核管理要求

12.1 运维质量要求

本项目计划通过两年时间，建立并完善浦东教育全行业的网络安全监管与服务保障系统，业务范围覆盖数据中心、公办学校、民办学校、社会培训机构。具体的运维质量要求如下表：

工作内	类别	指标项	指标值
-----	----	-----	-----

容一日 常性网 络安全 技术服 务考核 指标	服务指标	服务期间信息系统（网站）漏洞扫描报告	不少于 3 万份
		威胁监测的主机数	不少于 12 万台
		应急响应时间（服务人员到达事件现场）	不超过 1 小时
	效益指标	网络安全事件	无重大安全事件
	满意度指标	服务对象满意度	良好率 90%以上
工作内 容二各 类专项 网络安全 服务考 核指标	类别	指标项	指标值
	服务指标	服务期内教育网内主机部署防病毒产品的主机数量	不少于 4 万台
		通过等保测评的信息系统数量	第一年 5 个 第二年 9 个
		综合监管平台的测评	通过第三方的软件测试和安全测试
	效益指标	网络安全事件	无重大安全事件
满意度指标	服务对象满意度	良好率 90%以上	

备注：所谓重大安全事件，（1）造成特别重要信息系统遭受特别严重的系统损失；由于网络攻击造成的业务中断超过 3 个小时及以上的；（2）产生特别重大的社会影响。核心业务数据或重要数据被泄露导致大范围社会传播事件，造成严重社会影响。

12.2 考核管理要求

若因中标人服务不及时或服务质量问题造成网络安全事件，每发生一次处以合同总额 0.1% 的罚金，超过 2 次采购人有权解除合同。未完成服务质量要求的每项处以合同总额 0.2% 的罚金。

13 现场组织协调

13.1 投标人须自行负责与新区相关单位的沟通协调，解决、落实施工过程中所需办理的各类施工证件和许可证明；

13.2 投标人须自行负责与政府相关委办局和各街镇相关单位的沟通协调；

13.3 投标人须自行负责采购人各部门的沟通协调，解决涉及项目建设的其他问题。

14 项目的保密和产权

14.1 投标人保证对其提供的服务及出售的标的物享有合法的权利，应保证在其出售的标的物上不存在任何未曾向采购人透露的担保物权，如抵押权、质押权、留置权等，并承诺本项目所使用的产品、系统、软件等内容，不会有涉及侵权或其他违法情况的发生。若存在上述问题，一律由投标人承担相

关法律责任；

14.2 在本合同项下的任何权利和义务不因中标人发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则中标人的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对采购人承担连带责任。

14.3 中标人应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。

四、投标报价须知

15 投标报价依据

15.1 投标报价计算依据包括本项目的招标文件（包括提供的附件）、招标文件答疑或修改的补充文书、运维工作量清单、备品备件清单、项目现场条件等。

15.2 招标文件明确的项目范围、运维内容、运维期限、运维质量要求、设备管理要求及考核要求等。

15.3 工作量清单（包含运维工作量清单和备品备件清单，以下简称工作量清单）说明

15.3.1 工作量清单应与投标人须知、合同条件、项目质量标准和要求等文件结合起来理解或解释。

15.3.2 采购人提供的工作量清单是依照采购需求测算出的本次招标的标的物清单。投标人如发现工作量清单和实际工作内容不一致时，应立即以书面形式通知采购人核查，除非采购人以答疑文件或补充文件予以更正，否则，应以此清单内容为准。

16 投标报价内容

16.1 本项目报价为全费用报价，是履行合同的最终价格，除投标需求中另有说明外，投标报价（即投标总价）应包括为实施本项目所需的全部运维服务所产生的人工（含工资、加班工资、工作餐、社会统筹保险金、关于人员聘用的费用等）、设备和材料采购、运输、装卸、仓储、保管、机械使用、培训、验收、配合、保险、劳务、管理、利润、税费、伴随服务等费用。

16.2 投标报价中投标人应考虑本项目可能存在的风险因素。投标报价应将所有工作内容考虑在内，如有漏项或缺项，均属于投标人的风险，其费用视作已分配在报价明细表内单价或总价之中。投标人应逐项计算并填写单价、合计价和总价。

16.3 在项目实施期内，对于除不可抗力因素之外，人工价格上涨以及可能存在的其它任何风险因素，投标人应自行考虑，在合同履约期内中标价不作调整。

16.4 投标人按照投标文件格式中所附的表式完整地填写《开标一览表》及各类投标报价明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

17 投标报价控制性条款

17.1 投标报价不得超过公布的预算金额或最高限价，其中各分项报价均不得超过对应的预算金额或最高限价。

17.2 本项目只允许有一个报价，任何有选择的报价将不予接受。

17.3 投标人提供的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。不得违反法规标准规定或合同约定，不得通过降低服务质量、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。

★17.4 经评标委员会审定，投标报价存在下列情形之一的，该投标文件作无效标处理：

17.4.1 对工作量清单中的工作量进行缩减的；

17.4.2 投标报价和技术方案明显不相符的。

五、政府采购政策

18 节能产品政府采购

18.1 按照财政部、发改委发布的《关于印发〈节能产品政府采购实施意见〉的通知》（财库[2004]185号）要求，政府采购属于“节能产品政府采购清单”（以下简称‘节能清单’）中产品时，在技术、服务等指标同等条件下，应当优先采购节能清单所列的产品。采购人需购买的材料产品属于政府强制采购节能产品品目的，投标人必须选用节能清单中相应的材料产品（清单中无对应细化分类或节能清单中的产品无法满足工作需要的除外）。

18.2 节能清单的公告媒体为中国政府采购网(<http://www.ccgp.gov.cn/>)、中国环境资源信息网(<http://www.cern.gov.cn/>)、中国节能节水认证网(<http://www.cecp.org.cn/>)。

18.3 在采购公告发布前已经过期的以及尚在公示期的节能清单均不得作为评标时的依据。

19 环境标志产品政府采购

19.1 按照财政部、环保总局联合印发的《关于环境标志产品政府采购实施的意见》（财库[2006]90号）要求，采购人采购的产品属于“环境标志产品政府采购清单”中品目的，在性能、技术、服务等指标同等条件下，应当优先采购清单中的产品。

19.2 “环境标志产品政府采购清单”的公告媒体为中国政府采购网（<http://www.ccgp.gov.cn/>）、国家环境保护总局网（<http://www.sepa.gov.cn/>）、中国绿色采购网（<http://www.cgpn.cn/>）。

19.3 在采购公告发布前已经过期的以及尚在公示期的“环境标志产品清单”均不得作为评标时的依据。

20 促进中小企业发展

20.1 中小企业（含中型、小型、微型企业，下同）的划定按照《中小企业划型标准规定》（工信部联企业【2011】300号）执行，参加投标的中小企业应当提供《中小企业声明函》（具体格式见“投标文件格式”），反之，视作非中小企业，不享受相应的扶持政策。如项目允许联合体参与竞争的，则联合体中的中小企业均应按本款要求提供《中小企业声明函》。

20.2 依据市财政局 2015 年 9 月发布的《关于执行促进中小企业发展政策相关事宜的通知》，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》。

20.3 如项目允许联合体参与竞争的，组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

20.4 对于小型、微型企业，按照《政府采购促进中小企业发展管理办法》（财库【2020】46号）和《关于进一步加大政府采购支持中小企业力度的通知》（财库【2022】19号）规定，其报价给予 **10%** 的扣除，用扣除后的价格参与评审。

20.5 如项目允许联合体参与竞争的，且联合体各方均为小型、微型企业的，联合体视同为小型、微型企业，其报价给予 **10%** 的扣除，用扣除后的价格参与评审。反之，依照联合体协议约定，小型、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。

20.6 供应商如提供虚假材料以谋取成交的，按照《政府采购法》有关条款处理，并记入供应商诚信档案。

21 促进残疾人就业（注：仅残疾人福利单位适用）

21.1 符合财库【2017】141号文中所示条件的残疾人福利性单位视同小型、微型企业，享受促进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。

21.2 残疾人福利性单位在参加政府采购活动时，应当按财库【2017】141号规定的《残疾人福利性单位声明函》（具体格式详见“投标文件格式”），并对声明的真实性负责。

第三章 采购合同

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-采购单位邮编]

邮政编码： [合同中心-供应商单位邮编]

电话： [合同中心-采购单位联系人电话]

电话： [合同中心-供应商联系人电话]

传真： [合同中心-采购单位传真]

传真： [合同中心-供应商单位传真]

联系人： [合同中心-采购单位联系人]

联系人： [合同中心-供应商联系人]

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

1 乙方根据本合同的规定向甲方提供以下信息系统运维服务：

1.1 信息系统运维服务

乙方所提供的信息系统运维服务其来源应符合国家的有关规定，信息系统运维服务的内容、要求、服务质量等详见合同附件。

2 合同金额、服务期限和服务地点：

2.1 合同金额：本合同金额为人民币[合同中心-合同总价]元整，大写：[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 服务期限

本信息系统运维服务的服务期限： [合同中心-合同有效期]

2.3 服务地点

本信息系统运维服务地点：上海市浦东新区范围内。

3 质量标准和要求

3.1 乙方所提供的信息系统运维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 乙方所交付的信息系统运维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信息系统运维服务享有合法的权利。

4.2 乙方保证在信息系统运维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信息系统运维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 如甲方使用该信息系统运维服务构成上述侵权的，则由乙方承担全部责任。

5 验收

5.1 维护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维护服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的(10)个工作日内，确定具体日期，由双方按照本合同的规定完成维护服务验收。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，直至维护服务完全符合验收标准。

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

5.4 甲方根据合同的规定对维护服务验收合格后，签署验收意见。

6 保密

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

7 付款

7.1 本合同以人民币付款（单位：元）。

7.2 本合同款项按照以下方式支付。

7.2.1 本项目合同金额采用**分期付款**方式，在采购人和中标人合同签订，且财政资金到位后，按下款要求支付相应的合同款项。

7.2.2 分期付款的时间进度要求和支付比例具体如下：

（1）合同签订后 30 日内，支付合同金额的 20%；

（2）服务期满一年且验收通过，财政第二年拨款到位后 30 日内，结合考核结果支付合同金额的 50%；

（3）服务期满两年且验收通过后 30 日内，结合考核结果支付合同金额的 30%。

7.3 中标人因自身原因造成返工的工作量，采购人将不予计量和支付。

7.4 采购人不得以法定代表人或者主要负责人变更，履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审计等为由，拒绝或者延迟支付中小企业款项。如发生延迟支付情况，应当支付逾期利息，且利率不行低于合同订立时 1 年期贷款市场报价利率。

8 甲方（甲方）的权利义务

8.1 甲方有权在合同规定的范围内享受信息系统运维服务，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，造成信息系统的无法正常运行，甲方有权邀请第三方提供服务，其支付的服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。

8.3 由于乙方维护服务质量或延误服务的原因，使甲方有关信息系统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，协助乙方进行系统维护和故障解决。

8.5 当信息系统或设备发生故障时，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调整原有信息系统，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维护服务，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维护服务，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 乙方保证在信息系统运维服务中，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 乙方在履行维护服务时，发现信息系统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，保证信息系统正常运行。

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 乙方保证在维护服务中提供更换的部件是全新的、未使用过的。如果或证实信息系统运维服务是有缺陷的，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 在维护服务期限内，如果乙方对提供维护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：

10.2.1 根据信息系统运维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信息系统

运维服务的价格。

10.2.2 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维护服务中有缺陷的部分或修补缺陷部分，其费用由乙方负担。

10.2.3 如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11 履约延误

11.1 乙方应按照合同规定的时间、地点提供服务。

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

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

12 误期赔偿

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

13 不可抗力

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

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

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

14 履约保证金

14.1 在本合同签署之前，乙方应向甲方提交一笔金额为（/）元人民币的履约保证金。履约保证金应自出具之日起至全部货物按本合同规定验收合格后三十天内有效。在全部货物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。**采购人逾期退还履约保证金 / /**。

14.2 履约保证金可以采用**支票、汇票、本票、保函等非现金形式**。卖方提交履约保证金所需的有关费用均由其自行承担。

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。

16.1.1 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信息系统运维服务。

16.1.2 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 3 份，以中文书写，签字各方各执 1 份，另有一份报财政部门备案。

20 合同附件

20.1 本合同附件包括：招标文件、投标文件等。

20.2 本合同附件与合同具有同等效力。

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

21 合同修改

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

[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（签章）：

法定代表人或授权委托人（签章）：

日期：**[合同中心-签订时间]**

日期：[合同中心-签订时间_1]

合同签订点：网上签约

第四章投标文件格式

说明：1、投标人未按本投标文件格式填写的，或相关证书与证明材料提供不完整的，投标人需承担其投标文件在评标时被扣分甚至被评标委员会否决的风险。2、相关表式不够，可另附页填写。

与评审相关的投标文件内容索引表

（此表置于投标文件首页）

项目名称或包件号:_____

序号	招标文件内容说明	是否提供/ 满足	对应 投标 文件 起始 页码	备注
一、商务部分				
1	投标承诺书			<u>经投标人盖章、法定代表人或授权代理人签字或盖章</u>
2	投标函			<u>经投标人盖章、法定代表人或授权代理人签字或盖章</u>
3	法定代表人身份证明及授权委托书			<u>经投标人盖章和法定代表人签字或盖章</u>
4	投标保证金（本项目不适用）			投标保证金（支票、汇票、本票、保函等非现金形式） 投标文件中提供原件扫描件加盖公章（注：原件在投标截止时间之前提交集中采购机构）
5	投标人基本情况表			
6	投标人应提交的资格证明材料			财务状况及税收、社会保障资金缴纳情况声明函；资格（资质）证书
7	开标一览表			<u>经投标人盖章、法定代表人或授权代理人签字或盖章</u>
8	投标报价明细表			此表的价格总计须与“开标一览表”总报价保持一致
9	根据招标文件要求，投标人提供以下证明材料： ①国家强制认证的产品承诺书。			
10	拟分包项目一览表（本项目不适用）			
11	投标人可提交的商务部分			中小企业声明函；近三年承揽的类似项目情况表；残疾人福利性单位声明函（仅残疾人福利

序号	招标文件内容说明	是否提供/满足	对应投标文件起始页码	备注
	其他证明材料			单位提供)；维保设备原厂授权书或售后服务承诺书(如果有)；供应商认为可以证明其能力、信誉和信用的其他材料等
二、技术部分				
1	技术方案			总体方案、分项实施方案、《项目实施进度计划表》等
2	拟投入本项目的人员组成情况			《拟派人员汇总表》、《项目主要人员基本情况表》、《项目其他工作人员基本情况表》
3	项目服务质量保证措施			《项目实施进度计划表》、《风险管理表》
4	拟投所有产品清单、偏离表(如需)			《拟投所有产品清单》、《技术偏离表》等
5	拟投入本项目的设备材料情况			《主要设备、材料情况一览表》
6	其他需说明的问题或需采取的技术措施。			

一、投标人提交的商务部分相关内容格式

1 投标承诺书格式

投标承诺书

本公司郑重承诺：

将遵循公开、公平、公正和诚实守信的原则，参加项目的投标。

一、不提供有违真实的材料。

二、不与采购人或其他投标人串通投标，损害国家利益、社会利益或他人的合法权益。

三、不向采购人或评标委员会成员行贿，以谋取中标。

四、不以他人名义投标或者其他方式弄虚作假，骗取中标。

五、不进行缺乏事实根据或者法律依据的质疑或投诉。

六、不在投标中哄抬价格或恶意压价。

七、保证所提供的所有货物、服务均无专利权、商标权、著作权或其他知识产权等有侵害他方的行为。

八、已对照“投标人须知”第 3 条要求进行了自查，承诺满足招标文件对投标人的资格要求，且在参加此次采购活动前 3 年内，在经营活动中无重大违法记录。

九、我方承诺投标文件中提供的相关资料均真实有效。

十、保证中标之后，按照投标文件承诺履约、实施项目。

十一、接受招标文件规定的结算原则和支付方式。

十二、按照招标文件和相关规范性管理文件要求，按时足额发放员工的工资，且职工工资标准不低于全市最低工资标准，同时按规定缴纳相应的社会保险费等，我方将积极配合采购人和第三方履约过程中的员工工资支付情况的监督。

十三、已按《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》相关法律法规的规定，充分行使了对招标文件（含补充文件）提出质疑的权利，已完全理解和接受招标文件（含补充文件）的所有内容及要求，无需做进一步解释和修正。

十四、我方承诺严格按照《上海市电子政府采购管理暂行办法》、《上海市数字证书使用管理办法》等有关规定和要求参加本次投标。

十五、本公司若违反本投标承诺，愿承担相应的法律责任。

投标人（盖章）：

法定代表人或授权代理人（签字或盖章）：

年月日

提示：投标人未按要求提供本承诺书的，经评标委员会审定后，作为非实质性响应投标而不纳入详细评审。

2 投标函格式

投标函

项目名称：

致：（采购人全称）

上海市浦东新区政府采购中心

1、我方已详细审查全部招标文件（包括答疑文件）以及全部参考资料和附件，我方已完全理解和确认招标文件对本项目的一切内容与要求，已不需要作出任何其它解释，我方同意放弃对这方面有不明及误解的权利。

2、我方同意所递交的投标文件在招标文件规定的投标有效期内有效，并遵守在此期限内，本投标文件对我方一直具有约束力，随时可接受中标。

3、如果我方的投标文件被接受，我方将提供履约担保（如果有）。我方保证在投标文件承诺的服务期限内完成合同范围内的全部内容，保证本项目服务质量全部达到投标文件承诺的标准和要求。

4、除非并直到制定并实施正式协议书，本投标文件及你方书面中标通知，应构成你我双方间有约束力的合同文件。

5、我方提供人民币***元整的投标保证金（**支票、汇票、本票、保函等非现金形式**）（**本项目不适用**），若我方在投标有效期内撤回我方的投标，或在收到贵方的书面中标通知书后不在规定的期限内签订承包合同，则我方同意贵方没收我方的投标保证金，并对我方参与政府采购项目予以不良诚信记录。

6、我方已按照本项目招标文件中所附的《资格性及符合性检查表》进行了自查，对评标委员会根据《资格性及符合性检查表》判定的非实质性响应投标无任何异议。

7、我方同意按照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》及相关法律法规的规定提出询问或质疑。我方已经充分行使了对招标要求提出质疑和澄清的权利，因此我方承诺不再对招标要求提出质疑。

8、投标人同意提供按照贵方可能要求的与其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。

投标人（盖章）：

法定代表人或授权代理人（签字或盖章）：

3 法定代表人身份证明及授权委托书格式

3.1 法定代表人身份证明

投标人：

单位性质：

请选择以下一项：1) 国家行政企业、公私合作企业、中外合资企业、社会组织机构、国际组织机构、外资企业、私营企业、集体企业、国防军事企业、其他（请填写）

地址：

成立时间：年月日

营业期限：

姓名：性别：

年龄：职务：

系（投标人名称）的法定代表人。

特此证明。

投标人（盖章）：

法定代表人（签字或盖章）：

时间：年月日

法定代表人身份证扫描件粘贴处

3.2 授权委托书

本授权书声明：注册于（公司注册地点）的（公司名称）法定代表人（姓名）代表本公司授权：
（公司名称）（职务）（姓名）为正式的合法代理人，参加（项目名称、包件）的投标工作，以投
标人的名义签署投标书、进行投标、签署合同并处理与此有关的一切事务，本授权书不得转委托。

投标人（盖章）：

法定代表人（签字或盖章）：

时间：年月日

授权代理人身份证扫描件粘贴处

4 投标保证金（银行保函）格式（本项目不适用）**投标保证金（银行保函）**

致：_____（采购人全称）

上海市浦东新区政府采购中心

本保函作为（投标人名称、地址）（以下简称投标人）参加贵方（项目名称和招标编号）项目投标的投标保证金。

（银行名称）不可撤销地保证并约束本行及其继承人和受让人，一旦收到贵方提出下列**任何一种情况**（如以联合体形式投标的，则联合体各方均适用）的书面通知后，不管投标人如何反对，立即无条件、无追索权地向贵方支付总额为********元人民币。

（1）投标人在开标后至投标有效期期满前撤回投标；

（2）投标人不接受贵方按照招标文件规定对其投标文件错误所作的修正；

（3）投标人在收到中标通知书后三十天（30）内，未能和贵方签订合同或提交可接受的履约保证金；

（4）投标人有招标文件规定的腐败、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行为。

除贵方提前终止或解除本保函外，本保函自开标之日起到投标有效期期满后三十（30）天（即至**年**月**日）有效，以及贵方和投标人同意延长的并通知本行的有效期内继续有效。

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、如以联合体形式投标的，银行保函可由联合体中任意一方提供。
- 3、投标人如同时参加同一项目多个包件投标的，各包件的投标保函应独立开具。

5 投标人基本情况表格式

投标人基本情况表

项目		内容及说明	
一、营业基本情况			
单位名称		经营场所地址	
注册编号		注册日期/有效期限	
企业类型及单位性质		经营范围	
法定代表人		电话/传真	
二、基本经济指标（截止到上一年度12月31日止）			
实收资本		资产总额	
负债总额		营业收入	
净利润		上缴税收	
上一年度资产负债率		上一年度主营业务利润率	
三、人员情况（以报名的时间为时点统计并填写）			
技术负责人		联系电话	
在册人数			
其中职称等级		其中执业资格	
职称名称	级别 (如：高级、中级、 初级、技工、其 他)	人数	执业资格名称 人数
四、其他			
开户银行名称 (供应商是法人的，填 写基本存款账户信息)		开户银行地址 (供应商是法人的，填 写基本存款账户信息)	
开户银行账号 (供应商是法人的，填 写基本存款账户信息)		所属集团公司（如有）	
企业资格（资质） (如有，需提供彩色扫 描件加盖公章)		质量体系认证 (如有，需提供彩色扫 描件加盖公章)	
近三年内因违法违规受 到行业及相关机构通报 批评以上处理的情况			

项目	内容及说明
其他需要说明的情况	

我方承诺上述情况是真实、准确的，同意根据采购人（进一步）要求出示有关资料予以证实。

6 投标人应提交的资格证明材料

说明：以下扫描件均应为 A4 纸大小

6.1 财务状况及税收、社会保障资金缴纳情况声明函

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：

6.2 法人或其他组织的资格（资质）证书

资质（资格）证书

法人或其他组织的资格（资质）证书扫描件粘贴处



7 开标一览表格式

开标一览表

浦东新区网络安全监管与保障服务包 1

项目名称	服务期限	备注	投标总价(总价、元)

说明：

- 1、所有价格均系用人民币表示，单位为元，报价精确到元。
- 2、投标人应按照《项目招标需求》和《投标人须知》的要求报价。
- 3、服务期限填写自合同签订之日起 2 年。
- 4、投标总价应为 2 年度报价的总计。投标总价不得超过公布的预算金额（本项目预算金额为 13,208,000.00 元），不得超过招标文件中规定的各工作内容对应的单价上限（工作内容一日常性网络安全技术服务最高限价 6,828,000.00 元、工作内容二各类专项网络安全服务最高限价 6,380,000.00 元）！
- 5、如此表中的内容与投标文件其它部分内容不一致的，以此表内容为准。
- 6、此表必须与上海市政府采购信息管理平台投标工具投标客户端《开标一览表》中的内容保持一致。

投标人（盖章）：

法定代表人或授权代理人（签字或盖章）：

日期：****年**月**日

8 投标报价明细表格式

8.1 投标报价明细表

序号	工作内容	数量	服务期限	投标报价（元）	备注
一	日常性网络安全技术服务	1	自合同签订之日起 2 年		工作内容一日常性网络安全技术服务最高限价 6,828,000.00 元
二	各类专项网络安全服务	1	自合同签订之日起 2 年		工作内容二各类专项网络安全服务最高限价 6,380,000.00 元
投标总价（元）					预算金额为 13,208,000.00 元

说明：

- 1、所有价格均系用人民币表示，投标总价精确到元。
- 2、投标总价不得超过公布的预算金额（本项目预算金额为 13,208,000.00 元），不得超过招标文件中规定的各工作内容对应的单价上限（工作内容一日常性网络安全技术服务最高限价 6,828,000.00 元、工作内容二各类专项网络安全服务最高限价 6,380,000.00 元）！
- 3、此表中的投标总价应与《开标一览表》中的投标总价保持一致。

8.2 投标报价分类明细表格式

(1) 投标报价分类明细表（按工作内容）

项目名称或包件号：

单位：元(人民币)

序号	具体内容	数量	服务期限	投标报价	备注
一	日常性网络安全技术服务	1			工作内容一日常性网络安全技术服务最高限价 6,828,000.00 元
1	教育网信息系统（网站）应用安全监测服务	1			
2	信息系统（网站）漏洞扫描服务	1			
3	教育专网主机威胁监测服务	1			
4	骨干网和数据中心网络系统安全服务	1			

5	网络安全事件处置技术支撑服务	1			
6	“40+1”网络安全现场检查技术服务	1			
二	各类专项网络安全服务	1			工作内容二各类专项网络安全服务最高限价 6,380,000.00 元
1	教育网内主机防病毒安全服务	1			
2	等级保护测评服务	1			
3	网络安全综合监管平台服务	1			
投标总价（元）					

说明：

- 1、所有价格均系用人民币表示，投标总价精确到元。
- 2、投标人可根据本项目实际情况对以上内容进行扩充或缩减（不仅限于以上类别）。
- 3、此表中的投标总价应与《开标一览表》中的投标总价保持一致。
- 4、投标总价不得超过公布的预算金额（本项目预算金额为 13,208,000.00 元），不得超过招标文件中规定的各工作内容对应的单价上限（工作内容一日常性网络安全技术服务最高限价 6,828,000.00 元、工作内容二各类专项网络安全服务最高限价 6,380,000.00 元）！

(2) 投标报价分类明细表

项目名称或包件号:

单位: 元(人民币)

序号	工作内容	投标价	小计	备注
一	人工费			
			
			
二	材料及器具（设备）使用费（如有）			
			
			
三	管理费及税金			
四			
投标总价（元）:				

说明:

- 1、所有价格均系用人民币表示，投标总价精确到元。
- 2、人工费即实施该项目所涉及的有关人员的基本工资、社会保险费、福利费、培训费等一切费用。可按招标需求中罗列的工作内容作分类描述和详细报价。
- 3、材料及器具（设备）使用费即实施该项目使用的材料及器具（设备）所产生的一系列费用，包括材料，器具设备，定期检测所发生的材料，按规范要求需维修更换的设备等的使用费。可按招标需求中罗列的工作内容作分类描述和详细报价。
- 4、投标人可根据本项目实际情况对以上内容进行扩充或缩减（不仅限于以上类别）。
- 5、此表中的投标总价应与《开标一览表》中的投标总价保持一致。
- 6、投标总价不得超过公布的预算金额（本项目预算金额为 13,208,000.00 元），不得超过招标文件中规定的各工作内容对应的单价上限（工作内容一日常性网络安全技术服务最高限价 6,828,000.00 元、工作内容二各类专项网络安全服务最高限价 6,380,000.00 元）！

8.2.1 人工费报价明细表格式

人工费报价明细表

项目名称或包件号:

单位: 元(人民币)

序号	岗位名称	人员数量 (人)	工时 (人/月)	工时单价 (元)	费用小计	执业资格或职称	备注
1							
2							
3							
4							
5							
6							
7							
8							
合计							

说明:

- 1、工时单价中应包含基本工资、社会保险费、福利费及其他费用。
- 2、基本工资: 根据劳动合同约定或国家及企业规章制度规定的工资标准计算的工资。人员的基本工资不得低于本市职工最新的最低工资标准。
- 3、社会保险费: 按国家及上海市规定计取。
- 4、福利费: 包括福利基金、工会基金、教育基金、加班费、服装费、午餐费、高温费等。
- 5、其他费用: 除了以上各项费用之外的费用, 如税金、员工的日常培训费等。
- 6、此表中的合计数应与《投标报价分类明细表》中“人工费”的合计数保持一致。

9 投标人提供的其他证明材料

① 国家强制认证的产品承诺书；

提示：投标人应按招标文件“前附表”第10.1.1（9）要求提供相应证明材料

国家强制认证的产品承诺书

致：招标人、招标代理机构

我方参加（项目名称）（包件号及包件名称）投标所投入的产品皆符合国家强制性标准。本项目中若涉及国家强制认证产品，我方承诺提供的产品皆满足相关强制认证要求。

投标人（盖章）：

法定代表人或授权代理人（签字或盖章）：

日期：****年**月**日

10 拟分包项目一览表格式（本项目不适用）

拟分包项目一览表

项目名称或包件号: _____

分包内容	价格	分包人名称	分包人资格（资质）	以往做过的类似项目的经历

说明：

- 1、附分包人相关证书复印件。

11 投标人可提交的商务部分其他证明材料格式

11.1 中小企业声明函的格式（仅中型/小型/微型企业需提供）

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）参加的（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. （标的名称），属于软件和信息技术服务业（采购文件中明确的所属行业）；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）；

2. （标的名称），属于（采购文件中明确的所属行业）；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）本声明函适用于所有在中国境内依法设立的各类所有制和各种组织形式的企业。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）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。

注：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。

11.3 投标人认为可以证明其能力、信誉和信用的其他材料

说明：扫描件应为 A4 纸大小

投标人需提交的可以证明其能力、信誉和信用的其他材料扫描件粘贴处

11.4 残疾人福利性单位声明函格式（仅残疾人福利性单位提供）

残疾人福利性单位声明函

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

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日期：

11.5 维保设备原厂授权书或售后服务承诺书（如果有）

说明：扫描件应为 A4 纸大小

维保设备原厂授权书或售后服务承诺书
扫描件粘贴处

二、投标人提交的技术部分相关内容格式

1 技术方案

【包括：总体方案、分项实施方案等】；

说明：[具体组成内容和编写要求详见“前附表”](#)

2拟投入本项目的人员组成情况

2.1 拟派人员汇总表格式

拟派人员汇总表

项目名称或包件号：_____

序号	岗位类别及职务	姓名	性别	年龄	学历	职称（或从业资格或执业资格）	相关工作年限	备注
1								
2								
3								
4								
5								
6								
7								
8								
9								

说明：

- 1、请按岗位类别及职务详细罗列参与本项目的人员名单及其基本情况。
- 2、除招标文件另有规定外，上述人员必须为本单位在职人员，不得是兼职人员和退休人员。
- 3、上表如若行数不够，可自行扩充。

2.2 项目主要人员基本情况表格式

项目主要人员基本情况表

姓名		性别		年龄		从事本专业 工作年限	
毕业院校和专业	**年**月毕业于*****学校*****系（科），学制**年						
职称（或执业资格）			拟在本项目中担任的职务				
主要工作经历							
年~ 年	参加过的项目			担任何职		备注	

说明：

1、主要人员需每人填写一份此表。“主要人员”是指实际参与本项目的项目总负责人、项目经理（工作内容一）、项目经理（工作内容二）、监测服务负责人、漏洞扫描负责人、主机威胁监测负责人、应急演练负责人、重保负责人、网络安全现场检查负责人、主机防病毒负责人、等级保护测评负责人、综合监管平台负责人等。

2、表后需附相关证书（包括职称/职业资格、执业资格、学历等）和在职证明材料等，所附证书和证明材料均为原件扫描件。

在职证明材料是指：投标人单位提供相关人员在任承诺书（格式自拟）。

3、如果表格填写不准确，或证书（证明材料）提供不完整的，投标人需承担其投标文件在评标时被扣分甚至被认定为无效标。

4、表式不够，可另附页填写。

2.3 项目其他工作人员表基本情况表格式

拟派项目其他工作人员表基本情况表

项目名称或包件号: _____

序号	姓名	性别	年龄	学历	主要分工	资格水平证书	相关工作年限	其他

3项目服务质量保证措施**3.1 项目实施进度计划表格式****项目实施进度计划表**

项目名称或包件号:_____

序号	时间	工作内容	阶段成果/完成进度

3.2 风险管理表格式**风险管理表**

项目名称或包件号:_____

序号	预期风险	应对方案
1		
2		
3		

4 拟投备品备件清单、偏离表（如需）

4.1 拟投备品备件清单（如需）

拟投备品备件清单（如需）

项目名称或包件号: _____

序号	备品 备件 名称	数量	品 牌、 型号	规 格 参 数	制造 商 名 称	产 地	质 保 期	是否 为 优 先 采 购 品 目	是否 为 国 家 强 制 认 证 产 品	备 注
1										
2										
3										
4										
5										

说明:

- 1、此表中“规格参数”这一项请详细描述，如遇篇幅过长，另制表描述；
- 2、投标人应如实填写备品备件信息。
- 3、如本项目所采购的备品备件属于优先采购品目【包括属于节能产品品目、环境标志产品品目、向我国企业转让技术、与我国企业签订消化吸收再创新方案的供应商的进口产品（以下简称优先采购进口产品）】、或其他国家强制认证产品的，须填写以下分项表。

4.1.1 节能产品格式（如需）

节能产品一览表

项目名称或包件号: _____

序号	节能产品名称	型号	制造商名称	是否属于强制节能	备注
1					
2					
3					

说明: 若本项目涉及节能产品采购, 投标人应选用节能产品品目清单中的产品, 并如实填写上表, 同时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的认证证书。

节能产品认证证书的扫描件粘贴处
(证书须在有效期之内)

4.1.2 环境标志产品格式（如需）

环境标志产品一览表

项目名称或包件号: _____

序号	环境标志产品名称	型号	制造商名称	备注
1				
2				
3				

说明：若本项目涉及环境标志产品采购，投标人应选用环境标志品目清单中的产品，并如实填写上表，同时提供国家确定的认证机构出具的、处于有效期之内的环境标志产品的认证证书。

环境标志产品认证证书的扫描件粘贴处
(证书须在有效期之内)

4.1.3 优先采购进口产品格式（如需）

优先采购进口产品一览表

项目名称或包件号: _____

序号	优先采购进口产品名称	型号	制造商名称	备注
1				
2				
3				

说明：若本项目涉及进口产品采购，如投标人所提供的产品为向我国企业转让技术、与我国企业签订消化吸收再创新方案的，供应商应如实填写上表，并同时提供相关材料。

优先采购进口产品的证明材料扫描件粘贴处

4.1.4 强制认证产品证书（如需）

说明：若本项目涉及国家强制认证产品（信息安全产品、3C 认证产品、电信设备进网许可证等），投标人应提供该产品按国家标准认证颁发的有效认证证书复印件。

投标人需提交的本项目涉及国家强制认证产品，如信息安全产品、3C 认证产品、电信设备进网许可证等材料的扫描件粘贴处

4.2 拟投备品备件技术规格偏离表（如需）

项目名称或包件号：_____

序号	子项名称	备品备件名称	招标要求	投标参数	偏离情况 (正/无/负)	对应 投标文件页码	说明

说明：

- 1、上表中所列参数为该项目核心指标，投标人应根据实际投标备品备件的参数指标对照填写；
- 2、除上述所列指标以外，如投标人另有偏离（包括正偏离和负偏离）的指标，请一并如实填写；
- 3、如投标备品备件实际技术规格与技术需求无偏差，在“是否有偏差”一列填写“无”；
- 4、投标备品备件的规格、技术参数和性能与招标文件的要求如不完全一致，请注明是“正偏离”还是“负偏离”。

5拟投入本项目的设备材料情况

拟配设备、材料情况一览表

项目名称或包件号:_____

序号	设备、材料名称	数量	单价	品牌	产地	规格型号	额定功率或容量	备注（如使用区域等）

6 其他需说明的问题或需采取的技术措施

2023年5月

第五章初步评审和详细评审

一、初步评审

资格性及符合性检查表

序号	检查内容	检查结果
	一、资格性检查	
1	投标人满足招标文件“投标人须知”第 3 条规定的投标人应具备资格条件的	
2	投标人按“投标人须知前附表”第 10.1.1（6）条款提交资格证明材料	
	二、符合性检查	
1	投标文件中的下列内容按招标文件要求签署、盖章的（具体详见“投标文件格式”要求）： ▲投标承诺书▲投标函▲授权委托书▲开标一览表	
2	未发现投标人递交两份或多份内容不同的投标文件，或在一份投标文件中对同一招标项目报有两个或多个报价，且未声明哪一个有效；（注：招标文件另有规定除外）	
3	接受招标文件规定的投标有效期	
4	接受招标文件规定的项目实施和服务期限	
5	未出现投标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，且不能按评标委员会要求提供说明材料的；	
6	投标报价未超过招标文件中规定的预算金额；投标报价未超过招标文件中规定的各工作内容对应的单价上限（工作内容一日常性网络安全技术服务最高限价 6,828,000.00 元、工作内容二各类专项网络安全服务最高限价 6,380,000.00 元）；	
7	未发现投标报价存在“第二章”第 17.4 条款所列情形之一的	
8	按规定交纳投标保证金（本项目不适用）	

9	根据招标文件要求，投标人提供以下证明材料的： ① <u>国家强制认证的产品承诺书</u> 。	
10	按“投标人须知”第 21.4 条款规定，对投标报价算术性错误修正予以确认的	
11	接受招标文件规定的结算原则和支付方式	
12	未出现《政府采购货物和服务招标投标管理办法》第三十七条所列的串通投标情形之一的	
13	未出现提供虚假材料、行贿等违法行为	
14	未发现因电子文档本身的计算机病毒、或电子文档损坏等原因造成投标文件无法打开或打开后无法完整读取的	
15	满足招标文件规定的以下要求： ① <u>接受并满足招标文件的实质性响应要求和条件</u> 。	
16	未发现投标人违反《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》规定的	

注意：

1、以上符合性检查内容由评标委员会负责最终审定，未通过资格性及符合性检查的投标将被作为非实质性响应投标而不纳入详细评审范围。

2、集中采购机构详细列出资格性及符合性检查的目的在于方便投标人进行自查，请投标人对照招标文件（包括答疑和补充文件）的内容进行自查，以避免投标文件出现非实质性响应的情况。本表中所列实质性检查内容判断标准与“前附表”中所列要求有矛盾之处，以“前附表”中所列要求为准。

二、详细评审

【浦东新区网络安全监管与保障服务】评标办法

（一）评标原则

1、本评标办法作为本项目择优选定中标人的依据，在评标全过程中应遵照执行，违反本评标办法的打分无效。

2、评标委员会负责对符合资格的投标人的投标文件进行符合性审查。对通过符合性审查的投标文件按此评标办法进行详细评审，未通过符合性审查的投标文件将被作为无效标而不纳入详细评审范围。

3、本次评标采用“综合评分法”，分值保留小数点后两位，第三位四舍五入。

4、评标委员会根据招标文件（包括答疑和补充文件）的规定，对各投标人商务标的完整性、合理性、准确性进行评审，确认商务标的有效性和评标价，以此为基础计算各投标人的商务标得分。

5、评标基准价为通过符合性审查的所有投标中的最低投标报价。如果评标委员认定投标人的报价明显低于其他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；投标人不能在评标委员会规定的时间内证明其报价合理性的，评标委员会应将其作为无效标处理。

6、对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人做出必要的澄清、说明或者补正。

7、按照《政府采购促进中小企业发展管理办法》（财库【2020】46号）《关于进一步加大政府采购支持中小企业力度的通知》（财库【2022】19号），对于非专门面向中小企业采购的项目，小型和微型企业参加投标的，享受以下扶持政策，用扣除后的价格参与评审：

（1）小型、微型企业的最终报价给予 **10%** 的扣除；

（2）如项目允许联合体参与竞争的，且联合体各方均为小型、微型企业的，联合体视同为小型、微型企业，其报价给予 **10%** 的扣除。反之，依照联合体协议约定，小型、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。

8、残疾人福利性单位视同小型、微型企业，其投标价格享受小型和微型企业同等的价格扣除政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

9、评标委员会成员对投标人的投标文件进行仔细审阅、评定后各自独立打分，评委应并提出技术标的详细评审意见（方案的优缺点均加以评述），打分可在规定幅度内允许打小数。

10、本项目技术标评审项中标有“*”内容属于客观评审因素，根据《政府采购货物和服务招标投标管理办法》要求，评标委员会成员对客观评审因素评分应一致。

11、技术标、商务标两者之和为投标人的最终得分，评标委员会按照各有效投标人最终得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列，得分且投标报价相同的，按技术标得分由高到低顺序排列。依照上述排序方法后仍出现得分相同时，

由评委记名投票表决，得票多者排名靠前。评标委员会推荐得分排名前二名的投标人作为中标候选人，其中第一中标候选人为中标人。

(二) 评审内容及打分原则

类别	分值	项目		权重	评分办法	评定分
商务	20	价格	报价得分	20	投标报价得分=（评标基准价 / 投标报价）×20 注：评标基准价为通过资格性及符合性检查的所有投标中的最低投标报价。	
技术	80	技 术 服 务 水 平	服务方案设计	12	一、评审内容： 1、对采购需求的理解及合理化建议； 2、服务定位和目标； 3、服务方案设计； 4、重点难点分析和应对措施。 二、评审标准： 1、方案合理，具有较强的针对性、具体性、操作性，得 11~12 分； 2、方案合理，但针对性、具体性、操作性有欠缺的，得 9~11（不含 11）分； 3、方案欠合理，且针对性、具体性、操作性欠缺的：得 7~9（不含 9）分。	
			项目具体实施安排	14	一、评审内容： 1、服务实施安排（日、周、月、年计划）；	

类别	分值	项目	权重	评分办法	评定分
				2、服务目标实施方案，原厂服务方案等； 3、服务机构设置、人员驻场安排情况等； 4、培训方案；（如需） 5、安全文明措施（如果有）。 二、评审标准： 1、安排合理，进度详细，具有较强的针对性、具体性、操作性，得 12~14 分； 2、安排合理，进度合理，但针对性、具体性、操作性有欠缺的，得 10~12（不含 12）分 3、安排欠合理，进度欠合理，且针对性、具体性、操作性欠缺的：得 9~10（不含 10）分。	
		故障应急处理方案	10	一、评审内容： 1、应急响应方案（包括详细的应急响应过程，响应方式，响应时间，故障修复时间等）； 2、针对典型安全事件或风险、重大节假日或任务的应急预案以及应急演练等。 二、评审标准： 1、安排合理、详细，具有较强的针对性、	

类别	分值	项目		权重	评分办法	评定分
					<p>具体性、操作性，得 9~10 分；</p> <p>2、安排合理、详细，但针对性、具体性、操作性有欠缺的，得 8~9（不含 9）分；</p> <p>3、安排欠合理、不够详细，且针对性、具体性、操作性欠缺的：得 6~8（不含 8）分。</p>	
			服务机构设置及管理制度	10	<p>一、评审内容：</p> <p>1、项目服务机构及其运作方法与流程；</p> <p>2、各项管理制度；</p> <p>3、服务档案等资料记录、移交计划等。</p> <p>二、评审标准：</p> <p>1、方案合理，具有较强的针对性、具体性、操作性，得 9~10 分；</p> <p>2、方案合理，但针对性、具体性、操作性有欠缺的，得 7~9（不含 9）分；</p> <p>3、方案欠合理，且针对性、具体性、操作性欠缺的：得 6~7（不含 7）分。</p>	
			拟投入的资源（人力、材料、设备）配置	28	<p>一、评审内容：</p> <p>1、拟投入资源（包括人力、设备、材料、人员职称学历和在职证明材料等）综合评价。</p> <p>2、负责人经历、能力、实际参与度等。</p> <p>二、评审标准：</p> <p>主要人员在职证明材料、职称学历证书完整提供，按以下内容进行评审；未完整提供，得 17 分；</p> <p>1、拟投入资源充分，负责人能力、经历与项目相符，实际参与度高，得 25~28 分；</p> <p>2、拟投入资源较合理，负责人能力、经历与项目基本相符，实际参与度一般，得 21~25（不含 25）分；</p> <p>3、拟投入资源缺乏，负责人能力、经历与项目基本无关，实际参与度欠缺：得 17~21（不含 21）分。</p>	
		投标人履约能力	投标人综合实力	6	<p>一、评审内容：</p> <p>1、近三年有效类似项目的承接情况；</p> <p>2、投标人的综合履约能力。</p> <p>二、评审标准：</p> <p>1、是否属于近三年有效类似项目由评标委员会根据投标人提供的项目承接情况在业务内容、技术特点等方面与本项目类似程度进行认定。有一个得 2 分，在此基础上每增加一个加 1 分，最高得分为 4 分，没有得 0 分；</p>	

类别	分值	项目	权重	评分办法	评定分
				2、近三年承接的有效类似项目获得的用户或第三方评价情况、与本项目相关的第三方技术认可情况，得 0~2 分。	
合计			100		

采购人：上海市浦东教育发展研究院
集中采购机构：上海市浦东新区政府采购中心
2022 年 11 月