项目名称：信息化运行维护费-1 2024 年大兴区教育网安全服务项目

政府采购

公开招标文件

招标编号:BJCD-ZB24085

采购人：北京市大兴区教师进修学校

采购代理机构：北京驰度项目管理咨询有限公司

2024 年 10 月

目　　录

第一章　投标邀请

项目概况

（信息化运行维护费-1 2024年大兴区教育网安全服务项目）项目的潜在投标人应在北京市政府采购电子交易平台获取招标文件，并于2024年11月12日09点00分（北京时间）前递交投标文件。

一、项目基本情况

1.项目编号：1101152421020002024 8-XM001

2.项目名称：信息化运行维护费-1 2024年大兴区教育网安全服务项目

3.项目预算金额：220.00万元、项目最高限价（如有）：/万元

4.采购需求：

包号	标的名称	采购包预算金额（万元）	数量	简要技术需求或服务要求
01	信息化运行维护费-1 2024年大兴区教育网安全服务项目	220.00	1	详见第五章服务要求

5.合同履行期限：2024年12月1日至2025年11月30日。

6.本项目是否接受联合体投标：□是　■否。

二、申请人的资格要求（须同时满足）

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：

2.1 中小企业政策

□本项目不专门面向中小企业预留采购份额。

■本项目专门面向　■中小 □小微企业　采购。即：提供的货物全部由符合政策要求的中小/小微企业制造、服务全部由符合政策要求的中小/小微企业承接。

□本项目预留部分采购项目预算专门面向中小企业采购。对于预留份额，提供的货物由符合政策要求的中小企业制造、服务由符合政策要求的中小企业承接。预留份额通过以下措施进行：/。

2.2 其它落实政府采购政策的资格要求：/。

3.本项目的特定资格要求：

3.1本项目是否接受分支机构参与投标：□是　■ 否；

3.2 本项目是否属于政府购买服务：

■否

□是，公益一类事业单位、使用事业编制且由财政拨款保障的群团组织，不得作为承接主体；

3.3 其他特定资格要求： 无 。

三、获取招标文件

1.时间：2024 年 10 月 22 日至 2024 年 10 月 28 日，每天上午 09:00 至 12:00，下午 12:00 至 17:00（北京时间，法定节假日除外）。

2.地点：北京市政府采购电子交易平台

3.方式：供应商使用 CA 数字证书或电子营业执照登录北京市政府采购电子交易平台（http://zbcg-bjzc.zhongcy.com/bjczj-portal-site/index.html#/home）获取电子版招标文件。

4.售价：0 元。

四、提交投标文件截止时间、开标时间和地点

投标截止时间、开标时间：2024 年 11 月 12 日 09 点 00 分（北京时间）。

地点：北京市大兴区北臧村镇经六路东 5 号 203 会议室。

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

1.本项目需要落实的政府采购政策：

（1）《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)；

（2）《中华人民共和国中小企业促进法》；

（3）《政府采购促进中小企业发展管理办法》（财库[2020]46 号）；

（4）《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)；

（5）《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68 号）；

（6）《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）；

（7）《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）；

（8）政府采购其他相关政策。

2. 本项目信息在北京市政府采购网（http://www.ccgp-beijing.gov.cn/）、中国政府采购网（http://www.ccgp.gov.cn/）同时发布。

3.本项目采用全流程电子化采购方式，请供应商认真学习北京市政府采购电子交易平台发布的相关操作手册（供应商可在交易平台下载相关手册），办理CA数字证书或电子营业执照、进行北京市政府采购电子交易平台注册绑定，并认真核实CA数字证书或电子营业执照情况确认是否符合本项目电子化采购流程要求。

CA数字证书服务热线 010-58511086

电子营业执照服务热线 400-699-7000

技术支持服务热线　　010-86483801

3.1 办理CA数字证书或电子营业执照

供应商登录北京市政府采购电子交易平台查阅 “用户指南”—“操作指南”—“市场主体CA办理操作流程指引”/“电子营业执照使用指南”，按照程序要求办理。

3.2 注册

供应商登录北京市政府采购电子交易平台“用户指南”—“操作指南”—“市场主体注册入库操作流程指引”进行自助注册绑定。

3.3 驱动、客户端下载

供应商登录北京市政府采购电子交易平台“用户指南”—“工具下载”—“招标采购系统文件驱动安装包”下载相关驱动。

供应商登录北京市政府采购电子交易平台“用户指南”—“工具下载”—“投标文件编制工具”下载相关客户端。

3.4 获取电子招标文件

供应商使用CA数字证书或电子营业执照登录北京市政府采购电子交易平台获取电子招标文件。

供应商如计划参与多个采购包的投标，应在登录北京市政府采购电子交易平台后，在【我的项目】栏目依次选择对应采购包，进入项目工作台招标/采购文件环节分别按采购包下载招标文件电子版。未在规定期限内按上述操作获取文件的采购包，供应商无法提交相应包的电子投标文件。

3.5 编制电子投标文件

供应商应使用电子投标客户端编制电子投标文件并进行线上投标，供应商电子投标

文件需要加密并加盖电子签章，如无法按照要求在电子投标文件中加盖电子签章和加密，请及时通过技术支持服务热线联系技术人员。

3.6 提交电子投标文件

供应商应于投标截止时间前在北京市政府采购电子交易平台提交电子投标文件，上传电子投标文件过程中请保持与互联网的连接畅通。

3.6.1 投标现场需提供的资料

投标人需在开标时，由投标单位法人或授权人参加开标会(地点:北京市大兴区北臧村镇经六路东 5 号 203 会议室)。届时应提供以下资料:①《投标文件》纸质版 正本 1 份，副本 2 份；②《投标一览表》纸质版 1 份（备用）③投标 U 盘 1 份，U 盘内容包括:加密《投标文件》TBJ 格式、未加密《投标文件》TBJ 格式文件、WORD 或 WPS 格式《投标文件》、PDF 格式《投标文件》。以上材料分别密封提交，并在信封上分别注明标明投标一览表、投标文件纸质版、投标 U 盘（所提交资料不退）。**④携带制作电子版《投标文件》的 CA 证书(钥匙)**。⑤拟派的开标代表为法定代表人时需提供法定代表人身份证明文件加盖公章及本人有效身份证原件及复印件加盖公章；拟派的开标代表为非法定代表人时需提供法定代表人（或分支机构负责人）委托授权书原件加盖公章及本人有效身份证原件及复印件加盖公章。以上资料需开标当日现场递交，采购人或采购代理机构不接受现场递交以外的投递形式，投标人采取其他投递形式致使投标无效，采购人或采购代理机构不承担任何责任。(现场递交系指投标人将投标文件相关资料直接递交给采购人或采购代理机构联系人，并签字确认)。

3.7 电子开标

供应商在开标地点使用 CA 数字证书或电子营业执照登录北京市政府采购电子交易平台进行电子开标。

七、对本次招标提出询问，请按以下方式联系。

1.采购人信息

名　　称：北京市大兴区教师进修学校

地　　址：北京市大兴区兴华大街三段四号

联系方式：任老师　69203830-1212

2.采购代理机构信息

名　　称：北京驰度项目管理咨询有限公司

地　　址：北京市大兴区北臧村镇经六路东 5 号

联系方式：胡伟、张迪、孟莉莉　010-61250550

3.项目联系方式

项目联系人：胡伟、张迪、孟莉莉

电　　话：010-61250550

第二章　投标人须知

投标人须知资料表

本表是对投标人须知的具体补充和修改，如有矛盾，均以本资料表为准。标记“■”的选项意为适用于本项目，标记“□”的选项意为不适用于本项目。

<table>
<tr><th>条款号</th><th>条目</th><th>内容</th></tr>
<tr><td>2.2</td><td>项目属性</td><td>项目属性：
■服务
□货物</td></tr>
<tr><td>2.3</td><td>科研仪器设备</td><td>是否属于科研仪器设备采购项目：
□是
■否</td></tr>
<tr><td>2.4</td><td>核心产品</td><td>■关于核心产品本项目_/_包不适用。
□本项目__包为单一产品采购项目。
□本项目__包为非单一产品采购项目，核心产品为：____。</td></tr>
<tr><td rowspan="2">3.1</td><td>现场考察</td><td>■不组织
□组织，考察时间：__年_月_日_点_分
考察地点：_____。</td></tr>
<tr><td>开标前答疑会</td><td>■不召开
□召开，召开时间：__年_月_日_点_分
召开地点：_____。</td></tr>
<tr><td>4.1</td><td>样品</td><td>投标样品递交：
■不需要
□需要，具体要求如下：
（1）样品制作的标准和要求：_____；
（2）是否需要随样品提交相关检测报告：
□不需要　□需要
（3）样品递交要求：_____；
（4）未中标人样品退还：_____；
（5）中标人样品保管、封存及退还：_____；
（6）其他要求（如有）：_____。</td></tr>
<tr><td>5.2.5</td><td>标的所属行业</td><td>本项目采购标的对应的中小企业划分标准所属行业：
<table>
<tr><th>标的名称</th><th>中小企业划分标准所属行业</th></tr>
<tr><td>信息化运行维护费-1 2024 年大兴区教育网安全服务项目</td><td>软件和信息技术服务业</td></tr>
</table>
</td></tr>
</table>

条款号	条目	内容
11.2	投标报价	投标报价的特殊规定： ■无 □有，具体情形：_____。
12.1	投标保证金	□无 ■有，投标保证金金额：20000 元。（大写：贰万元整） 保证金形式：支票、汇票、本票、网上银行支付或者金融机构、担保机构出具的保函等非现金形式 投标保证金收受人信息： 开户行名称：北京驰度项目管理咨询有限公司 开　户　行：中国农业银行股份有限公司北京天富路支行 账　　号：1111 2301 0400 06543 (为方便采购代理机构及时准确的核实投标人的保证金是否到账，投标人电汇保证金时应在电汇汇款附言中注明：BJCD-ZB24085 投标保证金。保证金交纳后，需及时将保证金交纳证明（汇款凭证或保函等扫描件）上传至北京市政府采购电子交易平台） 退还投标保证金方式：招标文件规定期满后将按原帐号退还投标保证金。
12.7.2		投标保证金可以不予退还的其他情形： □无 ■有，具体情形： （1）在开标之日后到投标有效期满前，供应商擅自撤销投标的； （2）中标供应商不按规定与采购人签订合同的； （3）中标供应商不按规定提交履约保证金的（如需履约保证金）； （4）中标供应商擅自放弃中标的； （5）中标供应商未按招标文件规定按时足额缴纳中标服务费的。
13.1	投标有效期	自提交投标文件的截止之日起算 90 日历日。
22.1	确定中标人	中标候选人并列的，采购人是否委托评标委员会确定中标人： ■否 □是 中标候选人并列的，按照以下方式确定中标人： ■得分且投标报价均相同的，以 技术部分 得分高者为中标人 □随机抽取
25.5	分包	本项目的非主体、非关键性工作是否允许分包： ■不允许 □允许，具体要求： （1）可以分包履行的具体内容：_____； （2）允许分包的金额或者比例：_____； （3）其他要求：_____。
26.1.1	询问	询问送达形式： 书面形式

条款号	条目	内容
26.3	联系方式	接收询问和质疑的联系方式 联系部门：北京驰度项目管理咨询有限公司； 联系电话：010-61250550； 通讯地址：北京市大兴区北臧村镇经六路东 5 号。
27	代理费	收费对象： □采购人 ■中标人 收费标准：参照原国家计委印发的计价格[2002]1980 号关于《招标代理机构服务费管理暂行办法》的通知、发改办价格[2003]857 号令及发改价格[2011]534 号令，以中标金额为基数，按差额定律累积法计算； 缴纳时间：中标人在领取中标通知书时一次向采购代理机构交纳所有中标服务费。 开户行名称：北京驰度项目管理咨询有限公司 开　户　行：中国农业银行股份有限公司北京天富路支行 账　　号：1111 2301 0400 06543
28	履约保证金	□无 ■有，履约保证金金额：合同金额的 3% 。 提交履约保证金的时间：签订合同后 15 日内 履约保证金形式：支票、保函、电汇 履约保证金用于补偿买方因卖方不能履行其合同义务而蒙受的损失，履约保证金在法定的货物质量保证期期满前应完全有效。 如果卖方未能按合同规定履行其义务，买方有权从履约保证金中取得补偿。

投标人须知

一　说　明

1　采购人、采购代理机构、投标人、联合体

1.1　采购人、采购代理机构：指依法进行政府采购的国家机关、事业单位、团体组织，及其委托的采购代理机构。本项目采购人、采购代理机构见第一章《投标邀请》。

1.2　投标人（也称“供应商”、“申请人”）：指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。

1.3　联合体：指两个以上的自然人、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。

2　资金来源、项目属性、科研仪器设备采购、核心产品

2.1　资金来源为财政性资金和/或本项目采购中无法与财政性资金分割的非财政性资金。

2.2　项目属性见《投标人须知资料表》。

2.3　是否属于科研仪器设备采购见《投标人须知资料表》。

2.4　核心产品见《投标人须知资料表》。

3　现场考察、开标前答疑会

3.1　若《投标人须知资料表》中规定了组织现场考察、召开开标前答疑会，则投标人应按要求在规定的时间和地点参加。

3.2　由于未参加现场考察或开标前答疑会而导致对项目实际情况不了解，影响投标文件编制、投标报价准确性、综合因素响应不全面等问题的，由投标人自行承担不利评审后果。

4　样品

4.1　本项目是否要求投标人提供样品，以及样品制作的标准和要求、是否需要随样品提交相关检测报告、样品的递交与退还等要求见《投标人须知资料表》。

4.2　样品的评审方法以及评审标准等内容见第四章《评标方法和评标标准》。

5　政府采购政策（包括但不限于下列具体政策要求）

5.1　进口产品

5.1.1　指通过中国海关报关验放进入中国境内且产自关境外的产品，包括已

经进入中国境内的进口产品。关于进口产品的相关规定依据《政府采购进口产品管理办法》（财库〔2007〕119 号文）、《关于政府采购进口产品管理有关问题的通知》（财办库〔2008〕248 号文）。

5.1.2 本项目是否接受进口产品见第五章《采购需求》。

5.2 中小企业、监狱企业及残疾人福利性单位

5.2.1 中小企业定义：

5.2.1.1 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。关于中小企业的相关规定依据《中华人民共和国中小企业促进法》、《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）、《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300 号）、《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36 号）。

5.2.1.2 供应商提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（3）在服务采购项目中，服务由中小企业承接，即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。

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

5.2.1.4 以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

5.2.2 监狱企业定义：是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。

5.2.3 残疾人福利单位定义：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：

5.2.3.1 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）；

5.2.3.2 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；

5.2.3.3 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；

5.2.3.4 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；

5.2.3.5 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）；

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

5.2.4 本项目是否专门面向中小企业预留采购份额见第一章《投标邀请》。

5.2.5 采购标的对应的中小企业划分标准所属行业见《投标人须知资料表》。

5.2.6 小微企业价格评审优惠的政策调整：见第四章《评标方法和评标标准》。

5.3 政府采购节能产品、环境标志产品

5.3.1 政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门根据产品节能环保性能、技术水平和市场成熟程度等因素，确定实施政府优先采购和强制采购的产品类别及所依据的相关标准规范，以品目清单的形式发布并适时调整。依据品目清单和认证证书实施政府优先采购和强制采购。

5.3.2 采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。关于政府采购节能产品、环境标志产品的相关规定依据《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）。

5.3.3 如本项目采购产品属于实施政府强制采购品目清单范围的节能产品，则投标人所报产品必须获得国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则**投标无效**；

5.3.4 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。优先采购的具体规定见第四章《评标方法和评标标准》（如涉及）。

5.4 支持乡村产业振兴管理

5.4.1 为落实《关于运用政府采购政策支持乡村产业振兴的通知》（财库〔2021〕19号）有关要求，做好支持脱贫攻坚工作，本项目采购活动中对于支持乡村振兴管理的相关要求见第五章《采购需求》（如涉及）。

5.5 正版软件

5.5.1 依据《财政部 国家发展改革委 信息产业部关于印发无线局域网产品政府采购实施意见的通知》（财库〔2005〕366 号），采购无线局域网产品和含有无线局域网功能的计算机、通信设备、打印机、复印机、投影仪等产品的，优先采购符合国家无线局域网安全标准（GB 15629.11/1102）并通过国家产品认证的产品。其中，国家有特殊信息安全要求的项目必须采购认证产品，否则**投标无效**。财政部、国家

发展改革委、信息产业部根据政府采购改革进展和无线局域网产品技术及市场成熟等情况，从国家指定的认证机构认证的生产厂商和产品型号中确定优先采购的产品，并以“无线局域网认证产品政府采购清单”（以下简称清单）的形式公布。清单中新增认证产品厂商和型号，由财政部、国家发展改革委、信息产业部以文件形式确定、公布并适时调整。

5.5.2 各级政府部门在购置计算机办公设备时，必须采购预装正版操作系统软件的计算机产品，相关规定依据《国家版权局、信息产业部、财政部、国务院机关事务管理局关于政府部门购置计算机办公设备必须采购已预装正版操作系统软件产品的通知》（国权联〔2006〕1 号）、《国务院办公厅关于进一步做好政府机关使用正版软件工作的通知》（国办发〔2010〕47 号）、《财政部关于进一步做好政府机关使用正版软件工作的通知》（财预〔2010〕536 号）。

5.6 信息安全产品

5.6.1 所投产品属于《关于调整信息安全产品强制性认证实施要求的公告》（2009 年第 33 号）范围的，采购经国家认证的信息安全产品，否则**投标无效**。关于信息安全相关规定依据《关于信息安全产品实施政府采购的通知》（财库〔2010〕48 号）。

5.7 推广使用低挥发性有机化合物（VOCs）

5.7.1 为全面推进本市挥发性有机物（VOCs）治理，贯彻落实挥发性有机物污染治理专项行动有关要求，相关规定依据《北京市财政局北京市生态环境局关于政府采购推广使用低挥发性有机化合物（VOCs）有关事项的通知》（京财采购〔2020〕2381 号）。本项目中涉及涂料、胶黏剂、油墨、清洗剂等挥发性有机物产品的，属于强制性标准的，供应商应执行符合本市和国家的 VOCs 含量限制标准（具体标准见第五章《采购需求》），否则**投标无效**；属于推荐性标准的，优先采购，具体见第四章《评标方法和评标标准》。

6 投标费用

6.1 投标人应自行承担所有与准备和参加投标有关的费用，无论投标的结果如何，采购人或采购代理机构在任何情况下均无承担这些费用的义务和责任。

二　招标文件

7　招标文件构成

7.1　招标文件包括以下部分：

第一章　投标邀请

第二章　投标人须知

第三章　资格审查

第四章　评标程序、评标方法和评标标准

第五章　采购需求

第六章　拟签订的合同文本

第七章　投标文件格式

7.2　投标人应认真阅读招标文件的全部内容。投标人应按照招标文件要求提交投标文件并保证所提供的全部资料的真实性，并对招标文件做出实质性响应，否则**投标无效**。

8　对招标文件的澄清或修改

8.1　采购人或采购代理机构对已发出的招标文件进行必要澄清或者修改的，将以书面形式通知所有获取招标文件的潜在投标人，并在原公告发布媒体上发布更正公告。

8.2　上述书面通知，按照获取招标文件的潜在投标人提供的联系方式发出，因提供的信息有误导致通知延迟或无法通知的，采购人或采购代理机构不承担责任。

8.3　澄清或者修改的内容为招标文件的组成部分，并对所有获取招标文件的潜在投标人具有约束力。澄清或者修改的内容可能影响投标文件编制的，将在投标截止时间至少 15 日前，以书面形式通知所有获取招标文件的潜在投标人；不足 15 日的，将顺延提交投标文件的截止时间和开标时间。

三　投标文件的编制

9　投标范围、投标文件中计量单位的使用及投标语言

9.1　本项目如划分采购包，投标人可以对本项目的其中一个采购包进行投标，也

可同时对多个采购包进行投标。投标人应当对所投采购包对应第五章《采购需求》所列的全部内容进行投标，不得将一个采购包中的内容拆开投标，否则其对该采购包的投标将被认定为**无效投标**。

9.2 除招标文件有特殊要求外，本项目投标所使用的计量单位，应采用中华人民共和国法定计量单位。

9.3 除专用术语外，投标文件及来往函电均应使用中文书写。必要时专用术语应附有中文解释。投标人提交的支持资料和已印制的文献可以用外文，但相应内容应附有中文翻译本，在解释投标文件时以中文翻译本为准。未附中文翻译本或翻译本中文内容明显与外文内容不一致的，其不利后果由投标人自行承担。

10 投标文件构成

10.1 投标人应当按照招标文件的要求编制投标文件。投标文件的部分格式要求，见第七章《投标文件格式》。

10.2 对于招标文件中标记了“实质性格式”文件的，投标人不得改变格式中给定的文字所表达的含义，不得删减格式中的实质性内容，不得自行添加与格式中给定的文字内容相矛盾的内容，不得对应当填写的空格不填写或不实质性响应，否则**投标无效**。未标记“实质性格式”的文件和招标文件未提供格式的内容，可由投标人自行编写。

10.3 第四章《评标程序、评标方法和评标标准》中涉及的证明文件。

10.4 对照第五章《采购需求》，说明所提供货物和服务已对第五章《采购需求》做出了响应，或申明与第五章《采购需求》的偏差和例外。如第五章《采购需求》中要求提供证明文件的，投标人应当按具体要求提供证明文件。

10.5 投标人认为应附的其他材料。

11 投标报价

11.1 所有投标均以人民币报价。

11.2 投标人的报价应包括为完成本项目所发生的一切费用和税费，招标人将不再支付报价以外的任何费用。投标人的报价应包括但不限于下列内容，《投标人须知资料表》中有特殊规定的，从其规定。

11.2.1 投标货物及标准附件、备品备件、专用工具等的出厂价（包括已在中国国内的进口货物完税后的仓库交货价、展室交货价或货架交货价）

和运至最终目的地的运输费和保险费，安装调试、检验、技术服务、培训、质量保证、售后服务、税费等按照招标文件要求完成本项目的全部相关服务费用；

11.2.2 按照招标文件要求完成本项目的全部相关服务费用。

11.3 采购人不得向供应商索要或者接受其给予的赠品、回扣或者与采购无关的其他商品、服务。

11.4 投标人不能提供任何有选择性或可调整的报价，否则其**投标无效**。

12 投标保证金

12.1 投标人应按《投标人须知资料表》中规定的金额及要求交纳投标保证金，并作为其投标的一部分。

12.2 交纳投标保证金可采用的形式：政府采购法律法规接受的支票、汇票、本票、网上银行支付或者金融机构、担保机构出具的保函等非现金形式。

12.3 投标保证金到账（保函提交）截止时间同投标截止时间。以支票、汇票、本票、网上银行支付等形式提交投标保证金的，应在投标截止时间前到账；以金融机构、担保机构出具的保函等形式提交投标保证金的，应在投标截止时间前将原件提交至采购代理机构。由于到账时间晚于投标截止时间的，或者票据错误、印鉴不清等原因导致不能到账的，其**投标无效**。

12.4 投标保证金（保函）有效期同投标有效期。

12.5 联合体投标的，可以由联合体中的一方或者共同提交投标保证金，以一方名义提交投标保证金的，对联合体各方均具有约束力。

12.6 采购人、采购代理机构将及时退还投标人的投标保证金，采用银行保函、担保机构担保函等形式递交的投标保证金，经供应商同意后采购人、采购代理机构可以不再退还，但因投标人自身原因导致无法及时退还的除外：

12.6.1 投标人在投标截止时间前撤回已提交的投标文件的，自收到投标人书面撤回通知之日起 5 个工作日内退还已收取的投标保证金；

12.6.2 中标人的投标保证金，自采购合同签订之日起 5 个工作日内退还中标人；

12.6.3 未中标投标人的投标保证金，自中标通知书发出之日起 5 个工作日内退还未中标人；

12.6.4 终止招标项目已经收取投标保证金的，自终止采购活动后 5 个工作日

内退还已收取的投标保证金及其在银行产生的孳息。

12.7 有下列情形之一的，采购人或采购代理机构可以不予退还投标保证金：

12.7.1 投标有效期内投标人撤销投标文件的；

12.7.2 《投标人须知资料表》中规定的其他情形。

13 投标有效期

13.1 投标文件应在本招标文件《投标人须知资料表》中规定的投标有效期内保持有效，投标有效期少于招标文件规定期限的，其**投标无效**。

14 投标文件的签署、盖章

14.1 招标文件要求签字的内容（如授权委托书等），可以使用电子签章或使用原件的电子件（电子件指扫描件、照片等形式电子文件）；要求第三方出具的盖章件原件（如联合协议、分包意向协议、制造商授权书等），投标文件中应使用原件的电子件。

14.2 招标文件要求盖章的内容，一般通过投标文件编制工具加盖电子签章。

四 投标文件的提交

15 投标文件的提交

15.1 本项目使用北京市政府采购电子交易平台。投标人根据招标文件及电子交易平台供应商操作手册要求编制、生成并提交电子投标文件。并将投标现场需提供的资料提交至招标公告或投标邀请中指明的地址。

15.2 采购人及采购代理机构拒绝接受通过电子交易平台以外任何形式提交的投标文件，投标保证金除外。

16 投标截止时间

16.1 投标人应在招标文件要求提交投标文件截止时间前，将电子投标文件提交至电子交易平台并将投标现场需提供的资料提交至招标公告或投标邀请中指明的地址。逾期送达，不予受理。

17 投标文件的修改与撤回

17.1 投标截止时间前，投标人可以通过电子交易平台对所提交的投标文件进行补充、修改或者撤回。投标保证金的补充、修改或者撤回无需通过电子交易平台，但应就其补充、修改或者撤回通知采购人或采购代理机构。

17.2 投标人对投标文件的补充、修改的内容应当按照招标文件要求签署、盖章，

作为投标文件的组成部分。

五　开标、资格审查及评标

18 开标

18.1　采购人应当按招标公告或投标邀请的规定，在投标截止时间的同一时间和招标公告或投标邀请预先确定的地点组织公开开标。开标时邀请所有投标人代表、招标人和有关方面代表参加。参加开标的代表应签名报到以证明其出席。投标人法定代表人和授权代表均未出席开标大会的投标将被视为无效拒绝。

18.2　开标时，由监标人或投标人或其推选的代表检查投标文件的密封情况，经确认无误后，由招标采购人当众宣读投标人名称、投标价格、价格折扣、书面修改和撤回投标的通知、是否提交了投标保证金等。对于投标人在投标截止期前递交的投标声明，在开标时当众宣读，评标时有效。未宣读的投标价格、价格折扣等实质内容，评标时不予承认。

18.3　开标过程将对唱标内容做开标记录，由投标人代表签字确认。

18.4　投标人代表对开标过程和开标记录有疑义，以及认为采购人、采购代理机构相关工作人员有需要回避的情形的，应当场提出询问或者回避申请。采购人、采购代理机构对投标人代表提出的询问或者回避申请将及时处理。

18.5　投标人不足 3 家的，不予开标。

19 资格审查

19.1　见第三章《资格审查》。

20 评标委员会

20.1　评标委员会根据政府采购有关规定和本次招标采购项目的特点进行组建，并负责具体评标事务，独立履行职责。

20.2　评审专家须符合《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）的规定。依法自行选定评审专家的，采购人和采购代理机构将查询有关信用记录，对具有行贿、受贿、欺诈等不良信用记录的人员，拒绝其参与政府采购活动。

21 评标程序、评标方法和评标标准

21.1　见第四章《评标程序、评标方法和评标标准》。

六　确定中标

22 确定中标人

22.1　采购人将在评标报告确定的中标候选人名单中按顺序确定中标人，中标候选人并列的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定中标人；招标文件未规定的，采取随机抽取的方式确定。采购人是否委托评标委员会直接确定中标人，见《投标人须知资料表》。中标候选人并列的，按照《投标人须知资料表》要求确定成交供应商。

23 中标公告与中标通知书

23.1　采购人或采购代理机构自中标人确定之日起 2 个工作日内，在北京市政府采购网、中国政府采购网公告中标结果，同时向中标人发出中标通知书，中标公告期限为 1 个工作日。

23.2　中标通知书对采购人和中标供应商均具有法律效力。中标通知书发出后，采购人改变中标结果的，或者中标供应商放弃中标项目的，应当依法承担法律责任。

24 废标

24.1　在招标采购中，出现下列情形之一的，应予废标：

24.1.1　符合专业条件的供应商或者对招标文件作实质响应的供应商不足三家的；

24.1.2　出现影响采购公正的违法、违规行为的；

24.1.3　投标人的报价均超过了采购预算，采购人不能支付的；

24.1.4　因重大变故，采购任务取消的。

24.2　废标后，采购人将废标理由通知所有投标人。

25 签订合同

25.1　中标人、采购人应当自中标通知书发出之日起 30 日内，按照招标文件和中标人投标文件的规定签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

25.2　中标人拒绝与采购人签订合同的，采购人可以按照评标报告推荐的中标候选人名单排序，确定下一候选人为中标人，也可以重新开展政府采购活动。

25.3　联合体中标的，联合体各方应当共同与采购人签订合同，就中标项目向采购人承担连带责任。

25.4 政府采购合同不能转包。

25.5 采购人允许采用分包方式履行合同的，中标人可以依法在中标后将中标项目的非主体、非关键性工作采取分包方式履行合同。本项目的非主体、非关键性工作是否允许分包，见《投标人须知资料表》。政府采购合同分包履行的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包，否则**投标无效**。中标人就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

25.6 招标文件、中标单位的投标文件及其澄清文件等，均为签订合同的依据。

26 询问与质疑

26.1 询问

26.1.1 投标人对政府采购活动事项有疑问的，可依法提出询问，并按《投标人须知资料表》载明的形式送达采购人或采购代理机构。

26.1.2 采购人或采购代理机构对供应商依法提出的询问，在 3 个工作日内作出答复，但答复的内容不得涉及商业秘密。

26.2 质疑

26.2.1 投标人认为采购文件、采购过程、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 7 个工作日内，由投标人派授权代表以书面形式向采购人、采购代理机构提出质疑。采购人、采购代理机构在收到质疑函后 7 个工作日内作出答复。

26.2.2 质疑函须使用财政部制定的范本文件。

26.2.3 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。

26.2.4 投标人应在法定质疑期内一次性提出针对同一采购程序环节的质疑，法定质疑期内针对同一采购程序环节再次提出的质疑，采购人、采购代理机构有权不予答复。

26.3 接收询问和质疑的联系部门、联系电话和通讯地址见《投标人须知资料表》。

27 代理费

27.1 收费对象、收费标准及缴纳时间见《投标人须知资料表》。由中标人支付的，中标人须一次性向采购代理机构缴纳代理费，投标报价应包含代理费用。

28　其他

详见《投标人须知资料表》。

第三章　资格审查

一、资格审查程序

1　开标结束后，采购人或采购代理机构将根据《资格审查要求》中的规定，对投标人进行资格审查，并形成资格审查结果。

2　《资格审查要求》中对格式有要求的，除招标文件另有规定外，均为“实质性格式”文件。

3　投标人有任何一项不符合《资格审查要求》的，资格审查不合格，其**投标无效**。

4　资格审查合格的投标人不足 3 家的，不进行评标。

二、资格审查要求

序号	审查因素	审查内容	格式要求
1	营业执照等证明文件	投标人为企业（包括合伙企业）的，应提供有效的“营业执照”； 投标人为事业单位的，应提供有效的“事业单位法人证书”； 投标人是非企业机构的，应提供有效的“执业许可证”、“登记证书”等证明文件； 投标人是个体工商户的，应提供有效的“个体工商户营业执照”； 投标人是自然人的，应提供有效的自然人身份证明。 若本项目允许分支机构参加投标，则分支机构参加投标的，此处可提供该分支机构或其所属法人或其他组织的相应证明文件。	提供证明文件的电子件或电子证照
2	投标人资格声明书	提供了符合招标文件要求的《投标人资格声明书》。	格式见《投标文件格式》
3	投标人信用记录	查询渠道：信用中国网站和中国政府采购网（www.creditchina.gov.cn、www.ccgp.gov.cn）； 截止时点：投标截止时间以后、资格审查阶段采购人或采购代理机构的实际查询时间； 信用信息查询记录和证据留存具体方式：查询结果网页打印页作为查询记录和证据，与其他采购文件一并保存； 信用信息的使用原则：经认定的被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人，其**投标无效**。	无须投标人提供，由采购人或采购代理机构查询。

序号	审查因素	审查内容	格式要求
4	中小企业声明函	投标人提供中小企业声明函；如为监狱企业或残疾人福利性单位，不必提供中小企业声明函，但须按注 1 或注 2 要求提供证明材料。 注 1：监狱企业须提供由省级以上监狱管理局（北京市含教育矫治局）、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。 注 2：残疾人福利性单位须按招标文件要求提供《残疾人福利性单位声明函》。	格式见《投标文件格式》
5	投标保证金	按照招标文件的规定提交投标保证金。	

第四章　评标程序、评标方法和评标标准

一、评标方法

1　投标文件的符合性审查

1.1　评标委员会对资格审查合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。

1.2　评标委员会根据《符合性审查要求》中规定的审查因素和审查内容，对投标人的投标文件是否实质上响应招标文件进行符合性审查，并形成符合性审查评审结果。投标人《投标文件》有任何一项不符合《符合性审查要求》要求的，**投标无效**。

符合性审查要求

序号	审查因素	审查内容
1	授权委托书	按招标文件要求提供授权委托书；
2	投标完整性	未将一个采购包中的内容拆开投标；
3	投标报价	报价未超过招标文件中规定的预算金额；
4	报价唯一性	投标文件未出现可选择性或可调整的报价；
5	投标有效期	投标有效期满足招标文件要求；
6	签署、盖章	投标文件按招标文件要求签署、盖章；
7	实质性格式	标记为“实质性格式”的文件均按招标文件要求提供；
8	附加条件	投标文件未含有采购人不能接受的附加条件；
9	其他无效情形	不存在法律、法规和招标文件规定的其他无效情形；

2 投标文件有关事项的澄清或者说明

2.1 评标过程中，评标委员会将以书面形式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文字和计算错误的内容，作出必要的澄清、说明或者补正。投标人的澄清、说明或者补正应当采用书面形式，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。澄清文件将作为投标文件内容的一部分。

2.2 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，有权要求该投标人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；若投标人不能证明其报价合理性，评标委员会将其作为**无效投标处理**。

2.3 投标报价须包含招标文件全部内容，如分项报价表有缺漏视为已含在其他各项报价中，将不对投标总价进行调整。评标委员会有权要求投标人在评标现场合理的时间内对此进行书面确认，投标人不确认的，视为将一个采购包中的内容拆开投标，其**投标无效**。

2.4 投标文件报价出现前后不一致的，按照下列规定修正：

2.4.1 招标文件对于报价修正是否另有规定：

□有，具体规定为：_____

■无，按下述 2.4.2-2.4.7 项规定修正。

2.4.2 单独递交的开标一览表（报价表）与投标文件中开标一览表（报价表）内容不一致的，以单独递交的开标一览表（报价表）为准；

2.4.3 投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

2.4.4 大写金额和小写金额不一致的，以大写金额为准；

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

2.4.6 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。

2.4.7 同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人书面确认后产生约束力，投标人不确认的，其**投标无效**。

2.5 落实政府采购政策的价格调整：只有符合第二章《投标人须知》5.2 条规定情

形的，可以享受中小企业扶持政策，用扣除后的价格参加评审；否则，评标时价格不予扣除。

2.5.1 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对小微企业报价给予 10%的扣除，用扣除后的价格参加评审。

2.5.2 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，且接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的联合体或者大中型企业的报价给予 4 %的扣除，用扣除后的价格参加评审。

2.5.3 组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

2.5.4 价格扣除比例对小型企业和微型企业同等对待，不作区分。

2.5.5 中小企业参加政府采购活动，应当按照招标文件给定的格式出具《中小企业声明函》，否则不得享受相关中小企业扶持政策。

2.5.6 监狱企业提供了由省级以上监狱管理局（北京市含教育矫治局）、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的，视同小微企业。

2.5.7 残疾人福利性单位按招标文件要求提供了《残疾人福利性单位声明函》（见附件）的，视同小微企业。

2.5.8 若投标人同时属于小型或微型企业、监狱企业、残疾人福利性单位中的两种及以上，将不重复享受小微企业价格扣减的优惠政策。

3 投标文件的比较和评价

3.1 评标委员会将按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价；未通过符合性审查的投标文件不得进入比较与评价。

3.2 评标方法和评标标准

3.2.1 本项目采用的评标方法为：

■综合评分法，指投标文件满足招标文件全部实质性要求，且按照评

审因素的量化指标评审得分最高的投标人为中标候选人的评标方法，见《评标标准》，招标文件中没有规定的评标标准不得作为评审的依据。

□最低评标价法，指投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人的评标方法。

3.2.2 采用最低评标价法时，提供相同品牌产品（单一产品或核心产品品牌相同）的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照下述方法确定一个参加评标的投标人，其他**投标无效**。

□随机抽取

□其他方式，具体要求：_____

3.2.3 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。优先采购的具体规定（如涉及）__/__。

3.2.4 关于无线局域网认证产品政府采购清单中的产品，优先采购的具体规定（如涉及）__/__。

4 确定中标候选人名单

4.1 采用综合评分法时，提供相同品牌产品（单一产品或核心产品品牌相同）且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，评标委员会按照下述规定确定一个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。**（本项目不适用）**

□随机抽取

□其他方式，具体要求：_____

4.2 采用综合评分法时，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。评分分值计算保留小数点后两位，第三位四舍五入。

4.3 采用最低评标价法时，评标结果按本章 2.4、2.5 调整后的投标报价由低到高

顺序排列。投标报价相同的并列。投标文件满足招标文件全部实质性要求且投标报价最低的投标人为排名第一的中标候选人。

4.4 评标委员会要对评分汇总情况进行复核，特别是对排名第一的、报价最低的、投标或响应文件被认定为无效的情形进行重点复核。

4.5 评标委员会将根据各投标人的评标排序，依次推荐本项目（各采购包）的中标候选人，起草并签署评标报告。本项目（各采购包）评标委员会共（各）推荐 3 名中标候选人。

5 报告违法行为

5.1 评标委员会在评标过程中发现投标人有行贿、提供虚假材料或者串通等违法行为时，有向采购人、采购代理机构或者有关部门报告的职责。

二、评标标准

序号	评分因素		分值	评分说明
1	投标报价（10 分）		10 分	综合评分法中的价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分 10 分。其他投标人的价格分统一按照下列公式计算：投标报价得分=(评标基准价／投标报价)×10
2	商务部分（10 分）	业绩	8 分	类似项目业绩：供应商提供自 2021 年 10 月 1 日以来（以签订合同日期为准）具备类似项目业绩，一个得 2 分；本项最多得 8 分，未提供的不得分。须提供合同复印件（合同复印件中至少包括合同首页、合同主要内容页、双方签字盖章页）并加盖投标单位公章否则不得分。
		相关资质	2 分	1、具有 CCRC 信息安全风险评估服务资质证书得 1 分，不具备得 0 分。 2、具有 CCRC 信息安全安全集成服务资质证书得 1 分，不具备得 0 分。 注：提供证明材料复印件并加盖投标单位公章。
3	技术部分（80 分）	技术响应	30 分	根据投标文件所提供服务对招标技术需求的整体技术响应情况评审综合打分：技术指标完全满足或优于招标文件要求得 30 分。#号项

				指标为重要指标，每有一项指标负偏离或未按要求提供证明材料的扣 1 分；其他技术指标，每有一项技术指标负偏离扣 0.5 分，扣完为止。
		项目实施方案	15 分	针对本项目服务内容和用户需求提供项目实施方案，包括但不限于：①项目实施计划；②设备实施方案；③服务质量保障方案；④技术服务方案；⑤项目实施与组织管理。 1.内容完整、无缺陷的得 15 分； 2.内容有 1 处不完整或有缺陷的得 12 分； 3.内容有 2 处不完整或有缺陷的得 9 分； 4.内容有 3 处不完整或有缺陷的得 6 分； 5.内容有 4 处不完整或有缺陷的得 3 分； 6.内容有 5 处不完整或有缺陷的得 1 分； 7.未提供得 0 分。
		项目理解	5 分	针对本项目服务内容和用户需求提供项目实施方案，包括但不限于：①对项目的理解；②项目重点难点分析；③项目优化方案。 1.内容完整、无缺陷的得 5 分； 2.内容有 1 处不完整或有缺陷的得 4 分； 3.内容有 2 处不完整或有缺陷的得 2 分； 4.内容有 3 处不完整或有缺陷的得 1 分； 5.未提供得0分。
		团队技术能力	10 分	项目负责人在本行业具有 5 年以上从业经验，且具备高级（含）以上技术职称或高级项目经理或硕士（含）以上学位等证书者得 5 分；项目负责人在本行业具有 5 年以上从业经验，且具备中级（含）以上技术职称或本科（含）以上学位等证书者得 2 分；不满足，得 0 分。（提供证书复印件并加盖公章）
				根据供应商提供的团队人员配备方案进行评分，包括但不限于：①团队构成、②人员配备、③岗位分工、④各岗位工作安排。 1.项目团队构成合理、人员配备充足、岗位分工明确、各岗位工作安排合理得5分；

				2.项目团队构成合理、人员配备基本充足、岗位分工基本明确、各岗位工作基本合理得3分； 3.项目团队构成不合理、人员配备不充足、岗位分工不明确、各岗位工作安排不合理得1分； 4.未提供得0分。
		安全培训方案	10 分	根据供应商提供的培训方案进行评分，包括但不限于：①培训方式、②培训时间、③培训目的、④培训内容。 1.内容完整、无缺陷的得10分； 2.内容有1处不完整或有缺陷的得8分； 3.内容有2处不完整或有缺陷的得5分； 4.内容有3处不完整或有缺陷的得3分； 5.内容有4处不完整或有缺陷的得1分； 6.未提供得0分。
		售后服务方案	10 分	针对本项目实际情况提供售后服务方案，包括但不限于：①售后服务方案；②售后服务承诺；③响应时间及处理周期；④出现问题有效的补救措施 1.内容完整、无缺陷的得10分； 2.内容有1处不完整或有缺陷的得8分； 3.内容有2处不完整或有缺陷的得5分； 4.内容有3处不完整或有缺陷的得3分； 5.内容有4处不完整或有缺陷的得1分； 6.未提供得0分。

注:不完整或有缺陷是指：涉及的规范及标准与本项目要求不一致或不相关，方案内容相互矛盾，方案内容与本项目无关，方案内容不清晰或交叉混乱，方案内容漏缺项。

第五章　服务要求

一、采购标的

1.1采购标的

序号	名称	数量	单位
1	大兴区教育网安全态势感知服务	1	年
2	数据中心防火墙安全防护服务	1	年
3	服务器安全防护服务	1	年
4	安全监控漏洞扫描服务	1	年
5	网站云防护服务	1	年
6	上网行为管理服务	1	年
7	日志审计服务	1	年
8	VPN 服务	1	年
9	数据安全服务	1	年
10	学校端安全处置服务	1	年
11	网站渗透测试服务	1	年
12	安全运营服务	1	年

1.2.项目概述

在当今数字化高速发展的时代，信息安全的重要性日益凸显，面对越发复杂多变的网络环境和日益严峻的安全挑战,加强信息安全防护能力是保证信息化运行的重点工作。本项目旨在为大兴教育网提供全面、可靠且具有前瞻性的信息安全保障。随着技术的不断演进和威胁的持续变化，我们将依据最新的行业标准和最佳实践，构建多层次的安全防护体系。通过先进的技术手段和严谨的管理流程，确保信息的安全性、完整性和可用性。大兴区教师进修学校信息中心肩负着全区教育信息化建设、管理和运维工作。目前全区教育网络、数据中心、信息安全等多项运维保障工作都由信息中心统一管理。信息中心数据中心缺乏足够完善的安全防护措施，页面遭篡改、信息被窃取的事件随时可能发生，不仅严重影响了学校正常工作的开展，还会造成较大范围的不良影响。在重大活动期间，为了避免教育网安全事件的发生，信息中心不得不采取禁止教育网各信息系统对外发布，确保重要时期的信息技术安全不会在教育网发生。

随着信息系统的校园网络规模和复杂性的不断增加，面对黑客攻击、未经授权入侵和其它威胁的风险也在逐渐增加。许多的系统管理人员常常忙于解决日常运维过程中出现的琐碎问题，以维持信息系统的持续可用，而没有更多精力定期检查信息系统中是否存在安全隐患、跟踪并获得相应的漏洞补丁、及时修复信息系统安全问题。为了降低信息系统中安全隐患被非法利用的可能性或在被利用后能及时加以响应，需要有专业的信息安全服务人员协助系统管理人员进行安全运维工作。

2014 年中央成立网络安全和信息化领导小组，习近平总书记亲自担任组长，并指出“没有网络安全，就没有国家安全；没有信息化，就没有现代化”，这标志着中国已把信息化和网络信息安全列入了国家发展的最高战略方向。此后，工信部、国资委、教育部等部委相继出台了《信息通信网络与信息安全规划（2016-2020）》、《关于进一步加强中央企业网络安全工作的通知》、《关于加强教育行业网络与信息安全工作的指导意见、《关于加强教育行业数据安全工作的通知》》等政策文件，全力推进我国信息安全产业发展，为推进新时代网络强国建设做出全面部署。同时，随着《国家安全法》、《网络安全法》《数据安全法》等法律法规的相继出台，标志着我国已全面开启建设网络强国之路。

随着大兴区教育网信息化深入建设，在给学校教学办公等提供全面信息化支持的同时，所面临的信息安全管理挑战也更加严峻，特别是《网络安全法》和《数据安全法》实施以来，教育行业面临的信息安全合规和监管压力极大增强。在国家新型网络空间安全形势和背景下，基于大兴区教育网现有信息安全管理现状及信息化建设情况，按照公安部、教育局等部门的要求,开展网络及信息安全整体保障服务项目，提高大兴区教育系统网络安全和数据安全管理水平，确保大兴区教育信息化业务的安全稳定运行。

二、商务要求

1、服务期限和地点

1.1 服务期限：2024 年 12 月 1 日至 2025 年 11 月 30 日

1.2 服务地点：采购人指定地点。

2、付款条件（进度和方式）

2.1 合同款计算方式，自签订合同之日起 1 年时间，年服务费人民币_____ 元整（大写：_____）

2.2 付款方式：合同款分 2 次支付，甲乙双方签订服务合同后 15 日内，乙方向甲方支付合同总金额的 3%作为履约保证金，甲方向乙方支付合同首付款人民币：1100000.00（大写：壹佰壹拾万元整）；项目结束通过验收后，剩余款项的结算以审计金额为准，审计结束后于 30 个工作日内付给乙方并同时无息退还履约保证金。

三、技术要求

1. 基本要求

1.1 采购标的需实现目标

通过本项目实施，能够有效发挥技术和设备的措施的效能，应对网络安全威胁的

动态变化，持续满足国家网络安全保障要求，加强风险控制措施的落实。大兴区教师进修学校通过协同专业的安全服务技术团队，采用规范化的运维管理，专业的安全数据分析和事件处置方法，通过可信、可控和可量化的高质量安全服务，建立北京市大兴区教育网网络安全运维体系，全面加强大兴区教育网网络安全、系统安全、信息安全、应用安全、数据安全、终端安全，保障终端、网络、系统和服务器安全，加强系统和应用软件安全管理和升级维护，从而更好的全面提高大兴区教育网网络和信息安全保障水平，保障大兴区教育网信息系统的各项业务应用以及业务数据的安全可靠。

1.2 国家相关标准、行业标准、地方标准或者其他标准、规范

（1）《信息安全技术网络安全等级保护实施指南》GB/T 25058-2019；

（2）《信息安全技术网络安全等级保护测评要求》GB/T 28448-2019

（3）《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

（4）《信息安全技术信息系统安全等级保护体系框架》GA/T 708-2007；

（5）《信息安全技术信息系统安全等级保护基本模型》GA/T 709-2007；

（6）《信息安全技术信息安全风险评估规方法》GB/T 20984-2022；

（7）《数据中心设计规范》GB 50174-2017

（8）《信息安全技术网络安全等级保护安全管理中心技术要求》GB/T 36958-2018

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

（10）《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019；

（11）《中华人民共和国数据安全法》

（12）《中国人民共和国个人信息保护法》

（13）《信息安全技术个人信息安全规范》（GB/T 35273-2020）

（14）信息安全技术 个人信息安全规范

（15）信息安全技术 网络安全等级保护基本要求

（16）信息安全技术 密码应用与安全性评估

（17）信息安全技术 网络安全事件应急处置规范

（18）信息安全技术 网络安全标准体系指南

（19）信息安全技术 网络安全标准体系基本要求

（20）信息安全技术 网络安全标准体系术语

（21）信息安全技术 网络安全标准体系框架

（22）信息安全技术 网络安全标准体系实施指南

（23）信息安全技术 网络安全标准体系评估方法

（24）信息安全技术 网络安全标准体系测试评估方法

（25）信息安全技术 网络安全标准体系符合性测试方法

（26）信息安全技术 网络安全标准体系实施效果评估方法

（27）信息安全技术 网络安全标准体系持续改进方法

（28）信息安全技术 网络安全标准体系监督与检查方法

（29）信息安全技术 网络安全标准体系培训与教育方法

2. 服务内容及要求

2.1采购标的需满足的技术规格要求

序号	名称	服务类别	服务内容	数量	单位	配置需求
1	大兴区教育网安全态势感知服务	安全组件	态势感知平台	1	套	存储容量：≥21T，在带宽性能≥1Gbps，存储时长≥1200 天，千兆电口≥4 个；千兆光口≥2 个； 具备威胁检测和攻防对抗功能、事前事中事后全时间检测、情报关联和智能分析、深度挖掘和辅助决策、检测响应和安全闭环、威胁分析与处置服务。 技术要求： #1、支持安全态势的可视化呈现，产品内置（非自定义）综合态势大屏、分支安全态势、安全事件态势、通报预警态势大屏、物联网安全态势大屏、全球网络攻击态势、资产态势、（需提供截图证明并加盖投标人公章） 2、支持基于 ATT&CK 能力图谱将网络安全现状映射到模型的各个阶段，支持命中攻击技术统计展示，支持基于规则检测引擎、情报检测引擎、文件分析引擎、攻击行为分析引擎以及异常行为引擎查看攻击技术分布，支持针对具体攻击技术展示检测能力图谱以及受影响的风险资产。 3、支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、服务与端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作。 4、支持跨三层取 MAC 地址，识别资产 MAC 地址，并能够解决不同资产 IP 冲突问题，以及 DHCP 场景 IP 变更的问题。 5、支持资产自动识别和资产扫描功能，支持自动入库、手动入库、设置扫描目标等功能，扫描类型可选择存活性（ARP/TCP/ICMP）、服务/端口（常用/全局）、操作系统、应用识别等。 6、支持责任人管理功能，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、自

						动识别资产图库、手动导入资产退库、自定义资产名称等。针对自动识别资产退库功能，可设置全局退库时间，数据更新时间。支持主机资产分级管理，责任人管理。（需提供截图证明并加盖投标人公章，且所投产品必须提供第三方权威机构关于“资产全生命周期管理”功能项相关的产品检测报告） 7、支持自定义分支管理权限，分支管理员具备独立的管理页面，可设置分支管理员权限，如类型、责任人、管理范围、页面权限、设备权限等。 8、支持 DNS 服务器日志导入，可以接入 DNS 服务器的日志，安全分析引擎将结合 DNS 服务器的日志，定位出 DNS 服务器代理风险外连场景下真实源 IP，从而有效地进行风险处置闭环。支持对导入 DNS 服务器进行展示，展示内容至少包含日志源名称、日志源 IP、接入类型、今日日志传输量、传输日志总量、最近同步时间、运营状态等。（需提供截图证明并加盖投标人公章，为确保功能真实有效客户有权利要求供应商提供样机以备功能查验） 9、支持弱密码主动扫描，支持 SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL 等扫描协议，支持自定义扫描周期、发包频率、扫描时间段、扫描优先级、扫描对象等。弱密码检测规则支持高度自定义，包括规则名称、生效域名、规则配置、账号白名单、密码白名单、弱密码内容导入文件，其中规则配置至少支持密码长度、字符种类、字典序、密码与账号相同、web 空密码等。 10、支持 web 登录结果自定义，可根据登录行为检测是否登录成功，支持基于响应状态码、响应内容格式、URL、关键字、服务器 IP 地址、所属资产组等信息判定成功或失败的通用规则设置，支持机器学习引擎持续学习用户登录行为，生成登录成功规则模型。 #11、支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置。支持通过首页搜索框输入 IP/域名/URL/端口/通信对进行搜索，支持基于列表模式展示横向攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，建立全方位的持续性的检测能力。支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员快速找到攻击入口点。（需提供截图证明并加盖投标人公章，为确保功能真实有效客户有权利要求供应商提供样机以备功能查验） 12、支持 EBA 实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括 DGA 解析请求、外联 C&C 服务器、异常协议利用、下载可疑文件、异常横向访问等。 #13、支持勒索专项检测页面，帮助客户更好的应对日益严峻的勒索风险，支持对勒索主题的安全告警进行统一展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类，包括勒索常用端口、勒索常用漏洞、RDP 爆破、感染勒索病毒、黑客勒索攻击、勒索 C&C 通信等维度，

						支持展示受害资产以及受害资产攻击数 TOP5，支持以列表的形式展示勒索事件，包括最近发生时间、威胁描述、威胁定性、勒索风险、威胁等级、受害者 IP、攻击次数等信息（需提供截图证明并加盖投标人公章，为确保功能真实有效客户有权利要求供应商提供样机以备功能查验） #14、支持挖矿专项检测页面，帮助客户更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息（需提供截图证明并加盖投标人公章，且所投产品必须提供第三方权威检测机构关于“挖矿专项检测”功能项相关的产品检测报告，为确保功能真实有效客户有权利要求供应商提供样机以备功能查验） #15、支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它 4 个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置。（需提供截图证明并加盖投标人公章，为确保功能真实有效客户有权利要求供应商提供样机以备功能查验） 16、支持云端与本地威胁情报共享，实时收集同步攻击者 IP，并详细展示情报列表，包括 IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等，并可对本地威胁情报及云端威胁情报联动同品牌防火墙实现自动封锁。 17、支持综合安全风险、主机安全风险、脆弱性感知、外部威胁感知、工单报告、摘要报告、处置报告多种方式呈现，可快速生成月度、季度、年度报表，摘要报告支持至少三种导出方式，至少包含 ppt、pdf、doc，满足客户不同场景的汇报需求。 #18、支持 PPT 格式导出摘要报告，用户可直接通过导出的 PPT 报告进行工作汇报，高效体现工作价值。（需提供截图证明并加盖投标人公章）
2		安全组件	提供潜伏威胁探针 4 套	1	套	1、硬件指标：千兆电口≥4 个，万兆光口≥2 个，网络层吞吐量：≥10Gbps（核心交换区）；具备产识别与脆弱性评估、多维度威胁检测、事前事中事后全方位检测、情报关联和智能分析、检测响应和安全闭环、威胁分析与处置服务、平台级联与数据共享。 技术要求： #1、支持命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测等自定义配置启用，针对命令注入检测、SQL 注入检测等类型支持自定义高检出、低误报模式。（需

						提供截图证明并加盖投标人公章） 2、支持 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞、自定义 WAF 规则、WAF 云防护等网站攻击检测。 #3、支持敏感信息检测功能，内置身份证、MD5、手机号码、银行卡号、邮箱等敏感信息，可自定义敏感信息检测策略选择组合的敏感信息，可基于 IP 统计和连接统计 2 种方式进行命中次数统计（需提供截图证明并加盖投标人公章） #4、支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Media 漏洞攻击、Network Device、Shellcode 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击、IPS 云防护等服务漏洞攻击检测。（需提供截图证明并加盖投标人公章） 5、支持 FTP、IMAP、MS Sql、Mysql、Oracle、Discuz、Basic Authorization、Glassfish、POP3、RDP、Sip 、Jboss、Redis 、Ldap 、SMTP、SSH、Telnet、Tomcat、Sybase、Weblogic 、Wordpress 、VNC 等 73 种协议暴力破解检测。 6、支持检测出网络中的网络拓扑设备进行绘制，更直观可视化查看网络整体情况。 #7、支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。（需提供截图证明并加盖投标人公章） 8、支持 5 种场景的日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。（需提供截图证明并加盖投标人公章） 9、支持传输协议审计日志，包括 https、http、DNS、邮件协议审计日志、SMB、AD 域、WEB 登录、FTP、TELNET、ICMP 、SNMP 、SSL 、SSH、SIP 、ONVIF 、NFS 、SOCKS 、dhcp、netbios_nbns、全流量元数据审计、数据库审计协议等。 10、支持将流量还原的文件发送至沙盒分析；可支持安天追影高级鉴定系统第三方沙盒对接。 11、内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、白名单库。 #12、支持流量抓包分析，基于五元组灵活抓取数据包，可定义配置源 IP、源端口、目的 IP 和目的端口、传输层协议以及标签类型（vlan、vxlan、mpls）选择添加抓包任务，接口额外提供标签选项。（需提供截图证明并加盖投标人公章）
		安全组件		3	套	硬件指标：千兆电口≥4 个，千兆兆光口≥4 个；网络层吞吐量：≥4Gbps（其他分支节点）。具备产识别与脆弱性评估、多维度威胁检测、事前事中事后全方位检测、情报关联和智能分析、检测响应和安全闭环、威胁分析与处置服务、平台级联与数据共享。 技术要求：

						1、支持命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测等自定义配置启用，针对命令注入检测、SQL 注入检测等类型支持自定义高检出、低误报模式。 2、支持 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞、自定义 WAF 规则、WAF 云防护等网站攻击检测。 3、支持敏感信息检测功能，内置身份证、MD5、手机号码、银行卡号、邮箱等敏感信息，可自定义敏感信息检测策略选择组合的敏感信息，可基于 IP 统计和连接统计 2 种方式进行命中次数统计。 4、支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Media 漏洞攻击、Network Device、Shellcode 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击、IPS 云防护等服务漏洞攻击检测。 5、支持 FTP、IMAP、MS Sql、Mysql、Oracle、Discuz、Basic Authorization、Glassfish、POP3、RDP、Sip 、Jboss、Redis 、Ldap 、SMTP、SSH、Telnet、Tomcat、Sybase、Weblogic 、Wordpress 、VNC 等 73 种协议暴力破解检测。 6、支持检测出网络中的网络拓扑设备进行绘制，更直观可视化查看网络整体情况。 7、支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。 8、支持 5 种场景的日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。 9、支持传输协议审计日志，包括 https、http、DNS、邮件协议审计日志、SMB、AD 域、WEB 登录、FTP、TELNET、ICMP 、SNMP 、SSL 、SSH、SIP 、ONVIF 、NFS 、SOCKS 、dhcp、netbios_nbns、全流量元数据审计、数据库审计协议等。 10、支持将流量还原的文件发送至沙盒分析；可支持安天追影高级鉴定系统第三方沙盒对接。 11、内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、白名单库。 12、支持流量抓包分析，基于五元组灵活抓取数据包，可定义配置源 IP、源端口、目的 IP 和目的端口、传输层协议以及标签类型（vlan、vxlan、mpls）选择添加抓包任务，接口额外提供标签选项。
3		安全组件	联动模块	10	套	包含功能：设备联动处置授权 10 套。

4		配套安全服务	资产脆弱性管理	12	次/年	对新增资产增量评估、资产变更持续检测、高危风险持续复查、指定漏洞定向检测、持续对 0Day 漏洞进行检测/监控并预警。 2、针对漏洞的特征进行安全防护组件的策略调整和配置。 3、提供对应的漏洞修复方案，持续跟踪漏洞复测情况。 交付内容：《资产台账》12 份。 不少于 120 工时。
5		配套安全服务	未知威胁发现	12	次/年	及时对未公开威胁进行评估、针对高危威胁风险进行通告。 交付内容：《安全态势感知报告》12 份。 不少于 48 工时。
6		配套安全服务	安全事件处置	50	次/年	针对态势感知平台分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助学校快速恢复业务，消除或减轻影响。 不少于 100 工时
7		配套安全服务	应急响应（针对下属 268 所学校）	120	次	提供日常的应急技术和应急响应服务，包括帮助用户提供完整的应急技术保障框架和解决方案、为用户定制预警监测解决方案和应急响应服务等。 应急响应流程： 入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。 入侵威胁清除：排查攻击路径，恶意文件清除。 入侵原因分析：还原攻击路径，分析入侵事件原因。 加固建议指导：结合现有安全防御体系，协助进行安全加固、提供整改建议、防止再次入侵。 提供全年 7*24 小时的电话支持安全服务，确认需要信息安全专家或安全服务队伍现场支持后，根据安全事件级别进行应急响应。服务频次：按需 交付内容：交付《应急响应报告》不少于 120 次。 不少于 240 工时。
8	数据中心防火墙安全防护服务	安全组件	提供数据中心防火墙 1 套	1	套	网络层吞吐量≥99G；应用层吞吐量≥39G；WAF 吞吐量≥13G；并发连接数≥2000 万；HTTP 新建连接数≥65 万；接口:千兆电口≥4 个；千兆光口 SFP≥4 个；万兆光口≥8 个；包含 Web 安全防护、Web 扫描、实时漏洞分析、敏感信息防泄漏等针对业务安全保障的功能，适用于数据中心、对外发布区域的服务器保护场景。具备 OWASP web 攻击防护、系统/应用漏洞攻击防护、威胁情报预警与处置、专业的网页防篡改、高效精准的黑链检测、多维敏感信息防泄漏、智能化 CC 攻击防护、可视化网站风险展示、自助化快速安全运维、网站安全扫描等功能。 技术要求： 1、产品内置超过 4580 种 WEB 应用攻击特征，支持对跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。 2、产品支持 X-Forworded-For 字段检测，并对非法源 IP 进行日志记录和联动封锁。 #3、产品支持服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和联动封锁。（需提供产品功能截图证明和具备 CMA/CNAS 标识的第三方检测报告并加盖投标人公章）

						#4、产品支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。（需提供产品功能截图证明和具备 CMA/CNAS 标识的第三方检测报告并加盖投标人公章） 5、产品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。 #6、产品支持云威胁情报网关技术，通过全球超过 30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。（需提供产品功能截图证明并提供 POP 节点在线查询链接和具备 CMA/CNAS 标识的第三方检测报告并加盖投标人公章） #7、产品支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发。（需提供产品功能截图证明和具备 CMA/CNAS 标识的第三方检测报告并加盖投标人公章） 8、产品支持与态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。 9、产品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。（需提供产品功能截图证明和具备 CMA/CNAS 标识的第三方检测报告并加盖投标人公章） #10、当主机故障时，双机切换时不丢包，并可实现双机部署下升级不断网。（需提供产品功能截图证明和具备 CMA/CNAS 标识的第三方检测报告并加盖投标人公章） #11、产品支持联动云平台，支持流量日志分析、事件聚合、云端专家研判，安全事件微信端就可接受预警和处置。（需提供产品功能截图证明并提供官方机构针对该功能的检测证明并加盖投标人公章）
9		配套安全服务	安全策略管理	12	次/年	策略信息收集后，结合实际业务安全需求，对现有安全策略进行差距分析，发现策略缺失、策略冗余、策略未废止等问题，并制定相应工作方案开展策略优化工作； 服务频次：12 次/年；交付内容：交付《安全策略调优》12 份。 不少于 48 工时
10		配套安全服务	安全加固	12	次/年	根据事件发生的根因、影响范围，针对性给出安全加固方案； 交付内容：交付《安全加固报告》12 份。 不少于 96 工时
11	服务器安全防护服务	安全组件	服务器安全防护软件	500	个	需求说明： 500 个服务器端授权；具备虚拟流量可视化、持续检测 Web 后门、暴力破解检测与响应、性能实时查看、僵尸网络检测 技术要求： #1、提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数 （需提供截图证明并加盖投标人公章）

						2、支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。 3、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户 4、支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴 5、具备自研的基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种 6、支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz 的自启动，可以防止黑客攻击 7、支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件 Hash 值，文件大小，文件创建时间；可配置 WebShell 实时扫描，一旦发现 WebShell 文件，可自动隔离或仅上报不隔离 8、提供基于可信鉴定方式的进程防护方式，通过人工智能自学习机制，自动建立信任进程名单，阻断非可信进程的运行并提供配置指引，同时支持通过模板和手动的方式添加信任进程 #9、支持 windows 服务器 RDP 远程登录保护，可开启 RDP 远程登录二次认证，以防止黑客对服务器的入侵（需提供截图证明并加盖投标人公章） 10、支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具 11、支持对勒索入侵的主流方式 RDP 暴破做全方位保护，包括 RDP 登录校验、RDP 文件加白二次校验等功能。 #12、支持流行 Windows 高危漏洞的轻补丁免疫防御，支持 Windows 补丁批量一键修复（需提供截图证明并加盖投标人公章）
12		安全组件	虚拟补丁更新服务	1	年	针对 WINDOWS 服务器进行补丁更新
13		配套安全服务	病毒处置服务	100	次/年	针对中毒终端进行病毒查杀和微隔离，服务频次：不少于 100 次。不少于 100 工时。
14	安全监控漏洞扫描服务	安全组件	提供 WEB 安全监控漏洞设备 1 套	1	套	需求说明： 默认包含资产数≥50；最大可扩展授权数≥150 漏扫和 WEB 漏扫不限 IP 数：不限制；接口：千兆电口≥4 个；千兆光口≥2 个； 具备资产发现、系统漏洞扫描、WEB 漏洞扫描、弱口令扫描、基线配置核查、合规自检平台 技术要求：

						#1、支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。（需提供截图证明并加盖投标人公章） 2、支持从漏洞视角分类型呈现风险概览和详情信息，支持在线查看展示“系统漏洞”、“WEB 漏洞”、“弱口令”和“基线风险”的名称、风险等级、漏洞数、最近发现时间，并可关联漏洞详情。漏洞详情可支持展示漏洞名称、漏洞类型、发现时间、影响资产、漏洞描述、漏洞影响、修复建议、CVE 编号、CNNVD 编号和举证信息。 #3、支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。（需提供截图证明并加盖投标人公章） 4、支持操作系统、网络设备、数据库、中间件等漏洞扫描。支持国产数据库的漏洞扫描，包括达梦、人大金仓、南大通用等。 5、系统漏洞扫描支持高级配置功能，可支持存活性探测配置、端口扫描策略配置、UDP 扫描启用、低可信度漏洞扫描、web 应用扫描启用等配置功能。 6、系统漏洞扫描支持任务立即执行、指定时间执行和周期执行三种执行方式，且指定时间可以精确到分钟，周期执行可精确到每日、每周、每月和自定义周期等。 7、内置不同的 WEB 漏洞模板，包括高可利用 WEB 漏洞、通用应用漏洞、SQL 注入漏洞、XSS 注入漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览，支持报表形式展示漏洞模板详情，包括漏洞总数、漏洞名称、漏洞类型、风险等级等信息。 8、WEB 漏洞扫描支持高级配置功能，可支持 fuzz 测试启用、WEB 访问策略、WEB 爬行策略等配置功能。支持并发线程数、超时限制、目录深度、链接总数自定义配置。 9、Web 漏洞扫描支持任务立即执行、指定时间执行、周期执行三种执行方式，且指定时间可以精确到分钟，周期执行可精确到每日、每周、每月和自定义周期等。 10、支持对 Windows、Linux 等操作系统、Oracel、MySQL、DB2、SQL Server、MySQL 等数据库按照等保二级、等保三级要求实施基线配置核查。 11、基线配置核查支持任务立即执行、指定时间执行和周期执行三种执行方式，且指定时间可以精确到分钟，周期执行可精确到每日、每周、每月和自定义周期等。 12、支持离线基线配置核查功能，支持通过基线配置模板导出离线脚本、通过任务列表导入基线扫描结果等功能。 13、提供检测结果综述分析，按照等保 2.0 的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。 #14、按“一个中心、三重防护”的架构展示检测结果，每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和

						人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认。 （需提供截图证明并加盖投标人公章） #15、产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表。 （需提供截图证明并加盖投标人公章）
15		配套安全服务	系统漏洞扫描服务	12	次/年	对部署在信息中心的信息系统进行系统漏洞扫描后的服务，服务频次：12 次/年，每次 28 系统（总服务器不少于 300 个），交付内容：交付《主机系统漏洞检测分析报告》12 份。 不少于 672 工时。
16		配套安全服务	WEB 漏洞扫描服务	4	次/年	对部署在信息中心的信息系统进行 WEB 漏洞扫描后的服务。服务频次：4 次/年，交付内容：交付《Web 漏洞检测分析报告》4 份。 不少于 464 工时。
17		配套安全服务	配置核查服务	12	次/年	对部署在信息中心的信息系统进行安全评估，配置核查，出具整改报告。服务频次：每季度对重点服务器进行配置核查。交付内容：交付《配置核查分析报告》12 份。 不少于 96 工时。
18	网站云防护服务	安全组件	网站云防监控	30	个	需求说明： 30 个域名云防护服务，单个域名带宽≥50M，并支持根据实际使用情况动态调整。具备整体风险评估、可用性实时监控、篡改实时监控、0DAY 漏洞实时监控 技术要求： 1.网站防火墙：支持常见攻击的发现与拦截，并记录攻击日志。支持 WEB 应用扫描/爬虫防护、异常 HTTP 请求防护、文件包含防护、远程恶意代码执行防护、XSS 跨站脚本攻击防护、SQL 注入防护等多种防护 2.网站管控： a.区域访问管控：对某些地区的访问进行限制，可根据需求自定义限制的国家或地区。 b.时段访问管控：对某些时段的访问进行限制，可根据需求自定义限制访问的时段。 c.访客 IP 类型管控：通过大数据分析，形成一系列 IP 行为库用于区分不同访客类型，可根据需求屏蔽某类 IP 访问。类型包括：IDC、代理、教育机构、广告网络、搜索引擎等 d.网站关停：紧急情况时，可一键关停网站，阻止任何人访问。 3.精准访问控制：实现对特定访问行为的精准的访问控制。支持拦截、放行、加黑、加白、人机验证等多种处置动作 4.自定义告警规则：针对多项指标及站点个性化需求，自定义告警条件及告警次数、沉默周期、告警时段、通知方式（邮件、短信）等 5.自定义拦截页面：通过编辑 HTML 代码自定义拦截页面，提升用户体验。 6.协同防御：共享云防御全网安全大数据情报以及可信第三方提供的恶意攻击 IP 地址等信息，快速阻断来自各

						行各业的高危攻击源、精准拦截各类恶意 IP 攻击，大幅度提升黑客攻击防御效果。 7.防篡改 a.防黑锁：锁定重要资源，如 logo、首页，进行快照缓存，防止被黑客篡改。 b.篡改检测：监测重要资源，如 logo、首页，在发生改变时进行通知告警。 c.篡改日志：记录每一次篡改事件，便于定位篡改发生时间、位置，为快速处置提供依据。
19		配套安全服务	流量分析	12	次/年	针对网站访问情况进行流量总结统计； 服务频次：12 次/年 交付内容：交付《月度安全报告》12 份。 不少于 48 工时。
20		安全组件	网站监测预警服务	不限次	年	针对云防护网站提供实时监测，提供预警报告； 服务频次：按需不限次，包含 30 个域名
21		安全组件	应急处置服务	不限次	年	针对暗链、挂码等问题网站进行应急响应处置； 服务频次：按需不限次 交付《应急处置报告》
22	上网行为管理服务	安全组件	提供上网行为审计设备 1 套	1	套	需求说明： 网络层吞吐量（大包）≥59G；带宽性能≥29Gb；支持用户数≥200000；每秒新建连接数≥280000；最大并发连接数≥18000000；接口：千兆电口≥4 个、千兆光口≥4 个、万兆光口≥8 个； 具备身份认证、上网行为控制、流量控制、安全防护、行为审计； 技术要求： 1、支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证； #2、支持提供二维码和会议号，用户扫码或输入会议号认证上网；支持通过验证手机号码实名认证（需提供截图证明并加盖投标人公章） 3、支持 Windows 终端调用管理员上传脚本/程序以满足个性化检查要求，可设置周期性运行或者运行一次，可设置以当前用户或 SYSTEM 用户权限执行，执行结果检查是否生效； 4、支持 Windows 桌面水印，支持设置水印的内容、透明度、密度，水印效果预览，离线时继续生效； #5、支持放通或封堵 TCP\UDP 端口、ICMP 协议，可设置对所有 IP 或者指定 IP 执行，离线时继续生效（需提供截图证明并加盖投标人公章） 6、支持对终端应用联网管控，可设置禁止或允许访问互联网，禁止或允许访问指定 IP 地址，离线时继续生效 7、支持 Windows 终端外联行为检查，包括：连接外网检查、PPPoE 拨号检查、双网卡行为检查、无线网卡检查、链接非法 WIFI 检查（可设置合法 WIFI 白名单）、4G 网卡检查、否使用非法网关（可设置合法网关白名单），对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户； 8、支持自定义测试地址，检查终端是否能 PING 通，对

						不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户； #9、告警事件中支持违规外联告警选项，用于对违规外联行为使用进行预警（需提供截图证明并加盖投标人公章） 10、支持设置终端访问地址白名单或黑名单，写入终端防火墙 ACL 策略，管控规则可离线生效 #11、支持 U 盘和移动硬盘拷贝的文件内容以及插入和拔出行为的审计；（需提供截图证明并加盖投标人公章） 12、支持允许用户登录 Webmail 收邮件，而禁止发送 Webmail 邮件的功能 #13、基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中；用户指定应用上网流速超过预设阈值后，网关自动提醒该用户（需提供截图证明并加盖投标人公章） 14、支持文件传输应用的外发附件审计，包括 WinSCP、XFftp，FileZilla、SecureFX、OneDrive； 15、支持远程应用的外发附件审计,包括 Teamviewer、向日葵、Anydesk、RDP。 #16、支持与同品牌下一代防火墙系统实现认证联动，可以转发用户认证信息到下一代防火墙，实现单点登录（需提供截图证明并加盖投标人公章）
23	日志审计服务	安全组件	提供日志审计设备 1 套	1	套	需求说明： 默认包含主机审计许可证书数量≥500 个；最大可扩展审计主机许可数≥1500；可用存储量≥8TB（RAID1 模式）；平均每秒处理日志数（eps）最大性能≥6000；接口：千兆电口≥6 个；万兆光口≥2 个。具备数据审计、数据范式化、数据过滤、数据转发、数据分析、事件分析、审计管理、告警监控。资产：400+服务器日志记录，180 天 技术要求： #1、支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射，以满足除内置解析规则之外未被覆盖的日志类型的解析。（需提供截图证明并加盖投标人公章） 2、支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。 3、支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，同时支持转发已解析日志和原始日志的两种日志 4、支持 TLS 加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。 #5、支持 SM3 国密算法，保障日志完整性，可以有效防止日志篡改等攻击行为（需提供截图证明并加盖投标人公章） 6、支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所

						属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件； 7、支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括 base64、Unicode、GBK、HEX、UTF-8 等。 8、支持网站攻击、漏洞利用、C&C 通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到 350 条以上，支持自定义关联分析规则。 9、支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN 账号异常场景分析、Windows 服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析。 10、支持个性化定制，支持全系统更换 logo 与系统名称，支持一键恢复默认。 #11、支持 POC 测试工具一键生成数据,验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险。（需提供截图证明并加盖投标人公章） #12、支持等保合规自检，用户可自查设备是否满足等保要求。（需提供截图证明并加盖投标人公章）
24	VPN 服务	安全组件	提供 VPN 设备 1 套	1	套	需求说明： 提供接入授权≥500 个；设备整机理论最大并发会话数≥60w；接口：千兆电口≥6 个；千兆光口 SFP≥2 个； 具备多种身份认证方式，支持灵活组合，保障接入用户身份安全、多重端点安全机制，支持客户端安全检查、SSL 专线、移动端数据保护、支持多种国际标准算法和国家商密算法，保障传输安全、支持 URL 级权限控制、支持独立日志中心等功能。 技术要求： #1、支持终端使用包括 IE6、7、8、10、11 或其他 IE 内核的浏览器，以及最新版本的非 IE 内核浏览器，如 Windows EDGE，Google Chrome，Firefox，Safari，Opera 最新版登录 SSLVPN 系统，登录后可完整支持各种 IP 层以上的 B/S 和 C/S 应用。（需提供截图证明并加盖投标人公章） 2、支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访；支持 Web 参数修正，可针对 Flash、Java、Applet、或视频播放器对象所引用资源路径进行修正，避免无法播放的问题。 3、产品应提供环境检测、自动修复工具，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响 SSL VPN 的使用，减轻运维工作。 4、产品必须支持防中间人攻击，产品可在用户登录 SSLVPN 时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。 5、支持设备自身的抗攻击防护，支持防 Host 头部攻击

						设置，用于防止 Host 头部攻击，设备只允许通过符合设置规则的地址进行访问；支持防 SWEET32 攻击设置，用于防止 SWEET32 攻击。（需提供截图证明并加盖投标人公章） 6、支持与阿里钉钉、企业微信 APP 认证对接，移动端访问企业自建应用时可自动拉起 VPN，实现其内置应用的 VPN 安全接入 7、单台 VPN 设备可扩展同时支持 5 套以上 CA 根证书； #8、必须支持至少 4 条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠 SSLVPN 设备同样可实现 SSLVPN 接入用户的多线路自动优选功能（提供证明材料，并加盖投标人公章） 9、支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式。 #10、支持利用网页进行动态寻址的方法，客户端无需安装插件、不依靠 IP 地址库、不依赖于第三方动态 IP 寻址、直接根据速度探测实现用户端接入线路的自动优选，用户通过访问寻址代理页面（简称 Webagent 页面），通过 Webagent 页面自动寻找 VPN 设备 IP(非 DDNS）,该方法不必单独注册域名或占用 IP 地址，大大降低了系统部署难度。（提供证明材料，并加盖投标人公章） 11、支持针对不同的 web 页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。 #12、针对 B/S 资源支持 WebCache 技术，动态缓存页面元素，提高 Web 页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果（提供界面配置截图，并加盖投标人公章）
25	数据安全服务	安全组件	提供数据安全检查工具系统 1 套	1	套	峰值性能：≥500Mbps 针对行业客户的监管检查和被监管单位或有业务需要单位的敏感数据安全检查和自查自处理的工具型产品。数据安全检查工具主要是针对主机电脑中存放的涉敏文件进行主动检查并具备处理能力、网络中传输敏感数据的监测以及云 / 存储 (数据库) 敏感数据检查，为满足合规检查或常态化自查处理及后续的防泄露建设提供基础输入。 技术要求： 1、为方便运维管理，系统须支持基于用户的标签管理，可对用户标签下发策略进行管控 2、需支持非结构化数据内容识别规则，包含关键词组、正则匹配、关键词对的方式 3、需支持基于样本文件的敏感数据机器学习，支持对机器学习的结果展示，展示形式包含词云和以表格形式展示敏感词权重两种形式 4、需支持配置数据来源，包括文件下载的 Web 应用、客户端应用、代码仓库

						5、需支持压缩包穿透检测，不少于 15 层 6、需支持基于 MD5 值的数据流转溯源分析，分析包含文件的重命名、拷贝、外传、下载，外传途径分析 7、需支持配置一次性和周期性执行资产扫描任务，可全盘扫描、特定目录扫描，也可过滤数据分类、文件大小、文件格式、文件修改时间等，扫描任务可设置为低打扰模式，不影响用户正常使用电脑 8、需支持自定义选择扫描任务启动方式，包括系统静默启动和员工点击启动两种 9、需支持自定义渠道，Windows 类支持按照进程名添加，macOS 按照进程名、BundleID 添加，Linux 类支持按照进程名添加 10、需支持截屏固证支持事前事后分开截取，截屏数量支持不低于 3 张，可选择压缩/不压缩上传 11、需录屏固证支持事前事后持续录制，录屏时间支持不低于 5 秒，可选择压缩/不压缩上传 12、需支持对多种用户行为或日志进行组合，形成用户风险行为的模型，通过打分可以快速排列出当前最具威胁的用户。系统预置的行为模型不低于 10 个 13、需支持自由检索所有终端的数据资产，图形化展示文件总数、已分类数据量、未分类数据量等 14、需提供 AI 配置选项，支持对接多种大型 AI 模型，OpenAI，通义千问，KIMI 等
26		安全组件	提供网络数据防泄露系统（DLP）1 套	1	套	峰值性能：≥500Mbps 以《数据安全法》为依据，从认识数据、梳理数据、分析数据（数据分类分级）、使用数据（数据共享与流转）、保护数据（数据加密）、数据交换、数据溯源分析（数据水印和血缘分析）、数据风险识别（机器学习和模型运算）、数据安全管控、用户行为分析，实现数据全生命周期安全（数据安全态势感知）。 技术要求： 1、支持数据库 DML 协议，如对于 MySQL、Oracle 等删、改、查操作 基于关键字和关键短语的识别 2、支持正则表达式描述匹配 3、支持数据校验算法，比如银行卡、身份证等进行校验匹配 4、外部白名单不受邮件策略管控，但可记录外部白名单邮件，支持白名单例外策略设置。 5、支持关键字权重，从而降低误报率 6、文件嵌套敏感内容匹配格式为 BMP、JPG、TIF、PNG 的，含有敏感内容图片 7、能够识别文件是否为压缩文件（如 RAR、ZIP、7Z、TAR、GZ） 8、支持边界条件（如文件大于 1K 同时小于 10MB）,能识别文件大于 1MB、5MB、10MB 的附件 9、可以识别修改后缀后进行压缩，再次修改后缀，并再次压缩文件的复合式规避检测行为 10、支持对上报事件进行查看、可查看到事件 ID，状态，协议，策略，发送者，接收者，事件等信息，也可自定义查询筛选，将事件全部导出、部分导出等。

						11、支持针对上报的敏感内容的事件，显示敏感内容片断。 12、支持通过 syslog、API 及 kafka 与第三方平台通讯。上报事件及策略下发管理。 13、通过管理界面显示防护策略的基本信息及状态，如策略当前的挂起状态、对应对象、策略基本内容属性等。
27		安全组件	提供数据库审计 1 套	1	套	最大硬件吞吐量：≥4.9Gbps，SQL 处理性能：≥10000 条 SQL/s，日志检索性能：≥20000 条/秒；接口：千兆电口≥6 个；万兆光口≥2 个。 支持对用户访问数据库行为的记录、分析和汇报，包括越权查询内置敏感表、篡改内置敏感表等都能够准确识别与告警，避免黑客通过暴库撞库获取账号密码，用来帮助用户事后生成合规报告、事故追根溯源，加强内外部数据库网络行为记录，提高数据资产安全。 技术要求： 1、支持主流数据库：Oracle（Tdata）、SQL-Server、DB2、MySQL（Tdsql）、Informix、Sybase、Cache、MongDB、PostgreSQL；国产化数据库：K-DB，达梦、人大金仓。 2、数据库威胁分析：可以通过自定义交互分析设置正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数这几个维度实时监控内网数据威胁态势并且提供交互式分析视图帮助企业快速溯源。 #3、精细化日志秒级查询：通过 SQL 串模式抽取保障磁盘 IO 的读写性能；分离式存储 SQL 语句保障数据审计速度（需提供截图证明并加盖投标人公章） 4、TB 级日志秒级查询、支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多 SQL 语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询。 5、自定义报表拖拽：通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果。（需提供截图证明并加盖投标人公章） 6、支持以时间、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL 模版为条件的数据库风险查询。 7、支持以风险级别、源 IP、业务主机、数据库用户、风险类型为维度的数据库风险排行。 #8、内置大量 SQL 安全规则包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感

						表、篡改内置敏感表等；（需提供截图证明并加盖投标人公章） 9、可以对 SQL 语句进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施 10、支持 SIP 联动实现数据库的风险进行统一分析预警 11、深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源 IP、源端口、源 MAC、目的 IP、目的端口、数据库用户、数据库类型、操作类型、SQL 语句、SQL 模版、客户端程序名、响应码、影响行数、返回行数、SQL 预计响应时间；
28		配套安全服务	数据资产调研	12	份	对区主要信息系统进行资产调研，梳理设备类型、数量、拓扑图、数据类型、业务交互场景、数据存储方式等内容，确定数据生命周期内的数据流转过程。 编写《数据资产调研表》12 份 交付内容：交付《数据资产调研表》12 份。 不少于 96 工时。
29		配套安全服务	数据评估方案编制	12	份	针对业务系统特点以及数据流转过程，编制风险评估方案，确定风险评估面、评估方式、项目人员、评估分值计算、风险控制、保密措施等内容。 编写《数据安全风险评估实施方案》12 份 交付内容：交付《数据安全风险评估实施方案》12 份。 不少于 96 工时。
30		配套安全服务	数据评估实施	12	份	网络数据风险评估：评估网络通信过程中的数据传输安全问题，对数据的完整性、保密性进行验证。 编写《数据安全风险识别报告》12 份 交付内容：交付《数据安全风险识别报告》12 份。 不少于 48 工时。
31		配套安全服务		12	份	应用数据风险评估：评估应用系统的交互过程中的数据风险，包括身份鉴别措施、API 接口、文件上传点、数据输入点、数据加解密措施、数据验证、数据脱敏等应用过程。对应用系统、服务器、中间件等组件进行漏洞测试及验证。 编写《数据安全风险识别报告》12 份 交付内容：交付《数据安全风险识别报告》12 份。 不少于 96 工时。
32		配套安全服务		12	份	数据库风险评估：评估数据库访问控制机制、数据库安全漏洞、数据审计、数据存储、数据调用过程中的安全风险。 编写《数据安全风险识别报告》12 份 交付内容：交付《数据安全风险识别报告》12 份。 不少于 96 工时。
33		配套安全服务		12	份	终端数据安全风险评估：对业务终端、办公终端、运维终端进行安全扫描，根据文件特点制定安全方案，对终端内的敏感文件进行识别，评估终端设备控制策略的有效性，了解终端设备的对数据泄漏、数据传播可能造成的安全隐患。 编写《数据安全风险识别报告》12 份 交付内容：交付《数据安全风险识别报告》12 份。 不少于 48 工时。

34		配套安全服务		1	份	个人信息风险评估：从个人信息角度展开风险评估，依照《个人信息保护法》对收集的个人信息进行分析评估，识别和评估个人信息处理活动中存在的安全风险。 编写《个人信息风险识别报告》1 份 交付内容：交付《个人信息风险识别报告》1 份。 不少于 12 工时。
35		配套安全服务		1	份	管理风险评估：对企业现行的数据安全管理制度、措施、手段、应急处置等流程进行访谈，明确组织活动以及第三方服务对数据安全的影响。 编写《安全管理风险识别报告》1 份 交付内容：交付《安全管理风险识别报告》1 份。 不少于 16 工时。
36		配套安全服务	数据安全整改建议方案	1	份	针对风险评估的结果，给出数据安全加固建议，分析应用和数据的特定关系，结合数据分类分级结果、投入产出比等因素制定合理的建设方案。 编写《应用系统数据安全整改建议方案》1 份 交付内容：交付《应用系统数据安全整改建议方案》1 份。 不少于 4 工时。
37		配套安全服务	《数据安全测试报告》	1	份	对网络、应用、数据库进行安全测试，出具漏洞测试报告。 编写《数据安全测试报告》1 份 交付内容：交付《数据安全测试报告》1 份。 不少于 4 工时。
38		配套安全服务	《数据安全现状调研评估报告》	1	份	针对数据安全总体评估结论，出具评估报告。 编写《数据安全现状调研评估报告》1 份 交付内容：交付《数据安全现状调研评估报告》1 份。 不少于 4 工时。
39		配套安全服务	数据分类分级实施方案	1	份	制定数据安全分类分级标准以及实施方案，根据数据类型和特点制定扫描和归纳方案。 编写《数据安全分类分级实施方案》1 份 交付内容：交付《数据安全分类分级实施方案》1 份。 不少于 4 工时。
40		配套安全服务	数据资产识别	1	份	梳理需要纳入数据分类分级的数据资产类型与范围，确定数据资产清单。 编写《数据安全分类分级资产清单》1 份 交付内容：交付《数据安全分类分级资产清单》1 份。 不少于 4 工时。
41		配套安全服务	数据资产扫描	1	份	借助数据扫描工具+人工分析的方式对区内所有业务系统、数据库、办公终端上的数据内容进行扫描，区分结构化与分结构数据，梳理数据资产类型与总量。 编写《数据安全分类分级扫描报告》1 份 交付内容：交付《数据安全分类分级扫描报告》1 份。 不少于 12 工时。
42		配套安全服务	体系规划	1	份	体系规划 根据贵单位数据安全现状确定数据安全管理的基线要求。基于实际业务需求分析，设计符合业务发展需要的数据安全体系规划，明确数据安全管理的过程、环节及关联关系。通过数据安全相关技术工具能力组合

						设计数据安全技术防护体系。 编写《数据安全体系规划设计方案》1 份 交付内容：交付《数据安全体系规划设计方案》1 份。 不少于 20 工时。
43		配套安全服务	组织建设	1	份	在已有的信息安全或者网络安全组织基础上，加入相关数据安全保护职责并在数据安全技术体系建设过程中发挥管理、指导、协调等作用。 编写《数据安全组织建设方案》1 份 交付内容：交付《数据安全组织建设方案》1 份。 不少于 12 工时。
44		配套安全服务	安全策略	1	份	进行数据的详细应用场景分析，明确系统数据的分级及数据全生命周期过程。了解系统内和系统间的业务交互过程及数据流转过程。以此总结典型业务场景，归类后进行数据安全策略设计。 编写《数据安全安全策略加固方案》1 份 交付内容：交付《数据安全安全策略加固方案》1 份。 不少于 20 工时。
45		配套安全服务	制度流程	1	份	以现有信息安全或者网络安全管理办法为基础，制定并发布数据安全相关管理制度。 编写《数据安全制度文档》1 份 交付内容：交付《数据安全制度文档》1 份。 不少于 20 工时。
46		配套安全服务	数据安全培训	1	份	对据安全负责人及相关技术人员和业务运营人员开展数据安全意识、数据安全技术、数据安全应急处置等培训内容。 举办 1 次《数据安全培训》，每次 1 学时 交付内容：1 次《数据安全培训》，每次 1 学时。 不少于 3 工时
47		配套安全服务	数据安全运营	1	项	设计数据安全运营体系，建立健全数据安全运营机制，规范日常数据安全运营、应急演练、协同处置工作流程。 举办 1 次《数据安全应急演练》，举办 1 次《数据安全应急响应》每次 1 学时） 交付内容：1 次《数据安全应急演练》，1 次《数据安全应急响应》每次 1 学时）。 不少于 3 工时
48		配套安全服务	SSL 证书服务	1	个	提供 1 个 daxingedu.cn 域名 SSL 通配符证书一年授权，确保系统安全放护能力和保障制度符合等级保护响应等级要求。
49	学校端安全处置服务	安全服务	学校端网络安全现状分析	268	所	通过网络安全等级保护差距分析工作与安全访谈，分析各教育网接入单位安全现状。 2、通过对学校网络负责人访谈以及现场机房网络设备的梳理，了解学校网络安全建设情况。 3、基于学校的安全防护情况及安全现状，进行安全策略优化、加固 4、通过对学校现状分析结果，给出网络安全建设意见。 此项服务覆盖大兴教委下属 268 所学校。 不少于 536 工时
50		安全服务	学校端恶意代	268	所	通过对学校服务器操作系统和应用的运行环境进行恶意代码安全检查。 不少于 536 工时

			码排查			
51	网站渗透测试服务	安全服务	WEB 渗透测试	10	系统	提供 10 个网站的渗透测试服务，输出渗透测试报告，提出问题整改建议，协助问题整改。渗透人员需具备 CISP-PTE(国家注册渗透测试工程师)资质，针对客户 Web 应用系统，采用自动和手动相结合的测试方式对外部和内部 Web 应用系统进行安全性测试.挖掘 Web 应用系统漏洞，提升应用系统安全性。 交付内容：每系统交付《渗透测试方案》、《渗透测试报告》、《渗透测试复测报告》10 份。
52	安全运营服务	安全服务	应急演练	2	次/年	是指在设计搭建的网络及应用环境中进行模拟入侵及防御的一类演练活动。 服务频次：2 次/年 交付内容：《应急演练报告》2 份。 不少于 38 工时
53		安全服务	安全预警通告	12	次/年	提供最新的安全动态、技术和定制的安全信息，包括实时安全漏洞通知、病毒、补丁升级、定期安全知识库更新等；服务频次：不低于 12 次。 不少于 24 工时
54		安全服务	重要时期安全保障	45	天	重大活动期间，提供安全服务，重保人员至少具备 3 年以上网络安全能力，保证网络安全，负责大兴区教育网安全设备及安全检测系统的日常运维，包括运行状态日检、检测，对安全设备及安全监测系统的策略调优、每天对安全设备日志信息和安全监测系统告警信息进行深入分析，及时发现安全威胁，并进行验证、处置及报告。服务频次：根据用户指定时间确定不少于 45 天； 交付内容：《重保值守报告》45 份。 不少于 1080 工时。
55		安全服务	安全宣讲	2	次/年	协助教委针对学校普通师生，培训常规信息安全政策、平时生活信息安全保护手段、专题互动；提供安全宣讲 ppt、宣传海报、易拉宝、小册子、互动用品 服务频次：2 次/年，提供讲师一名，现场支持人员 2 名 交付内容：《安全宣讲记录》2 份。
56		安全服务	安全培训	2	次/年	针对学校信息安全老师进行技术培训、实操演练；提供互动用品、搭建实操环境。培训材料不少于 50 份 服务频次：2 次/年，提供讲师一名，现场支持人员 1 名 交付内容：《安全培训记录》2 份。
57		安全服务	安全运营报告	12	份	1、按每月安全运营进行安全情况分析、处置、阶段性总结服务，并形成报告进行背书。定期阶段性安全运营情况总结，并形成报告，提交给用户。交付内容：《安全运营报告》12 份， 此项服务对报告进行编写，打印胶装成册 2、提供上半年半年汇报，提供下半年全年安全运营情况汇报，每年提供两次总结 PPT 性安全运营汇报，提供详细安全数据及总结性安全运营报告。 交付内容：《阶段性安全运营汇报》PPT2 份。
58		安全服务	驻场运维（提供：1 名信	365	天	工作内容：日常设备巡检：对 1 台安全态势感知、4 台潜伏威胁探针、1 台防火墙、1 台漏洞扫描设备、1 台日志审计、1 台 VPN、1 套端点安全软件、1 台数据库审计、1 套数据安全检查工具、1 套网络数据防泄密等软硬件进行安全巡检，确保设备硬件与软件平台运行正常；

			息安全专业人员证书的安全运维人员进行保障，驻场运维7*8小时，远程支持7*24小时）			工作内容：对网络安全运行状态监控，对网络安全设备日志进行分析 服务频次：每天查看形成日报、周报、月报（每月打印成册）。 不少于730工时
		安全服务				设备日志分析：针对设备日志报表进行日志分析，发现未知风险点；交付内容：《安全日志分析报告》按月打印成册。 不少于730工时
		安全服务				策略调优服务：通过安全策略的运营（例：自定义策略临时防护）临时应对、规避最新爆发的风险。 交付内容：《安全策略调优报告》按月打印成册。 不少于182.5工时
		安全服务				威胁分析及处置服务：通过态势感知平台实时针对异常流量分析、攻击日志和病毒日志分析，配合学校端防火墙进行联动处置。 不少于182.5工时
		安全服务				安全事件处置：对安全事件进行处置，清除恶意文件、快速恢复业务；交付内容：交付《安全事件处置报告》按实际情况 服务频次：每天进行查看，安全处置。 不少于182.5工时

2.2采购标的需满足的服务标准、期限、效率等要求

序号	名称	服务内容	服务标准	服务频率	期限
1	大兴区教育网安全态势感知服务	态势感知平台	存储容量：≥21T，在带宽性能≥1Gbps，存储时长≥1200天，千兆电口≥4个；千兆光口≥2个； 具备威胁检测和攻防对抗功能、事前事中事后全时间检测、情报关联和智能分析、深度挖掘和辅助决策、检测响应和安全闭环、威胁分析与处置服务。	1套/年	1年
2		提供潜伏威胁探针4套	1、硬件指标：千兆电口≥4个，万兆光口≥2个，网络层吞吐量：≥10Gbps（核心交换区）；具备产识别与脆弱性评估、多维度威胁检测、事前事中事后全方位检测、情报关联和智能分析、检测响应和安全闭环、威胁分析与处置服务、平台级联与数据共享。	1套/年	
			硬件指标：千兆电口≥4个，千兆兆光口≥4个；网络层吞吐量：≥4Gbps（其他分支节点）。具备产识别与脆弱性评估、多维度威胁检测、事前事中事后全方位检测、情报关联和智能分析、检测响应和安全闭环、威胁分析与处置服务、平台级联与数据共享。	3套/年	
3		联动模块	包含功能：设备联动处置授权10套	10套	
4		1. 资产脆弱性管理	2. 每周针对新增资产增量评估、资产变更持续检测、高危风险持续复查、指定漏洞定向检测、持续对0Day漏洞进行检测/监控并预警。 2、针对漏洞的特征进行安全防护组件的策略调整和配置。 3、提供对应的漏洞修复方案，持续跟踪漏洞复测情况。 交付内容：《资产台账》12份 不少于120工时。	服务频次：12次/年	
5		未知威胁发现	及时对未公开威胁进行评估、针对高危威胁风险进行通告。 交付内容：《安全态势感知报告》12份 不少于48工时。	服务频率:12次/年，	
6		安全事件处置	针对态势感知平台分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助学校快速恢复业务，消除或减轻影响。 不少于100工时。	服务频次：不少于50次	
7		应急响应（针对下属268所学校）	提供日常的应急技术和应急响应服务，包括帮助用户提供完整的应急技术保障框架和解决方案、为用户定制预警监测解决方案和应急响应服务等。 应急响应流程： 入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。 入侵威胁清除：排查攻击路径，恶意文件清除。 入侵原因分析：还原攻击路径，分析入侵事件原因。 加固建议指导：结合现有安全防御体系，协助进行安全加固、提供整改建议、防止再次入侵。 交付内容：交付《应急响应报告》不少于120次 提供7*24小时的电话支持安全服务，确认需要信息安全专家或安全服务队伍现场支持后，根据安全事件级别进行应急响应。 不少于240工时。	服务频次：按需	

8	数据中心防火墙安全防护服务	提供数据中心防火墙 1 套	网络层吞吐量≥99G；应用层吞吐量≥39G；WAF 吞吐量≥13G；并发连接数≥2000 万；HTTP 新建连接数≥65 万；接口：千兆电口≥4 个；千兆光口 SFP≥4 个；万兆光口≥8 个；包含 Web 安全防护、Web 扫描、实时漏洞分析、敏感信息防泄漏等针对业务安全保障的功能，适用于数据中心、对外发布区域的服务器保护场景。具备 OWASP web 攻击防护、系统/应用漏洞攻击防护、威胁情报预警与处置、专业的网页防篡改、高效精准的黑链检测、多维敏感信息防泄漏、智能化 CC 攻击防护、可视化网站风险展示、自助化快速安全运维、网站安全扫描等功能。	1 套/年	
9		安全策略管理	策略信息收集后，结合实际业务安全需求，对现有安全策略进行差距分析，发现策略缺失、策略冗余、策略未废止等问题，并制定相应工作方案开展策略优化工作； 交付《安全策略调优》12 份。 不少于 48 工时	服务频率：12 次/年	
10		安全加固	根据事件发生的根因、影响范围，针对性给出安全加固方案； 交付内容：交付《安全加固报告》12 份 不少于 96 工时	服务频次：12 次/年	
11	服务器安全防护服务	服务器安全防护软件	需求说明： 500 个服务器端授权；具备虚拟流量可视化、持续检测 Web 后门、暴力破解检测与响应、性能实时查看、僵尸网络检测	500 套/年	
12		虚拟补丁更新服务	针对 WINDOWS 服务器进行补丁更新	1 年	
13		病毒处置服务	针对中毒终端进行病毒查杀和微隔离， 不少于 100 工时。	服务频次：不少于 100 次	
14	安全监控漏洞扫描服务	提供 WEB 安全监控漏洞设备 1 套	需求说明： 默认包含资产数≥50；最大可扩展授权数≥150 漏扫和 WEB 漏扫不限 IP 数：不限制；接口：千兆电口≥4 个；千兆光口≥2 个； 具备资产发现、系统漏洞扫描、WEB 漏洞扫描、弱口令扫描、基线配置核查、合规自检平台	1 套/年	
15		系统漏洞扫描服务	对部署在信息中心的信息系统进行系统漏洞扫描后的服务， 交付内容：交付《主机系统漏洞检测分析报告》12 份。 不少于 672 工时。	服务频次：12 次/年	
16		WEB 漏洞扫描服务	对部署在信息中心的信息系统进行 WEB 漏洞扫描后的服务。 交付内容：交付《Web 漏洞检测分析报告》4 份 不少于 464 工时。	服务频次：4 次/年	
17		配置核查服务	对部署在信息中心的信息系统进行安全评估，配置核查，出具整改报告。 交付内容：交付《配置核查分析报告》12 份。 不少于 96 工时。	服务频次：每季度对重点服务器进行配置核查。	
18	网站云防	网站云防监控	需求说明： 30 个域名云防护服务，单个域名带宽≥50M，并支持根据实际使用情况动态调整。具备整体风险评估、可用性实时监控、篡改实时监控、0DAY 漏洞实时监控	30 个/年	

19	护服务	流量分析	针对网站访问情况进行流量总结统计； 交付内容：交付《月度安全报告》12 份 不少于 48 工时。	服务频次：12 次/年	
20		网站监测预警服务	针对云防护网站提供实时监测，提供预警报告；	服务频次：按需不限次，包含 30 个域名	
21		应急处置服务	针对暗链、挂码等问题网站进行应急响应处置； 交付《应急处置报告》	服务频次：按需不限次	
22	上网行为管理服务	提供上网行为审计设备 1 套	需求说明： 网络层吞吐量（大包）≥59G；带宽性能≥29Gb；支持用户数≥200000；每秒新建连接数≥280000；最大并发连接数≥18000000；接口：千兆电口≥4 个、千兆光口≥4 个、万兆光口≥8 个； 具备身份认证、上网行为控制、流量控制、安全防护、行为审计；	1 套/年	
23	日志审计服务	提供日志审计设备 1 套	需求说明： 默认包含主机审计许可证书数量≥500 个；最大可扩展审计主机许可数≥1500；可用存储量≥8TB（RAID1 模式）；平均每秒处理日志数（eps）最大性能≥6000；接口：千兆电口≥6 个；万兆光口≥2 个。具备数据审计、数据范式化、数据过滤、数据转发、数据分析、事件分析、审计管理、告警监控。 资产：400+服务器日志记录，180 天	1 套/年	
24	VPN 服务	提供 VPN 设备 1 套	需求说明： 提供接入授权≥500 个；设备整机理论最大并发会话数≥60w；接口：千兆电口≥6 个；千兆光口 SFP≥2 个； 具备多种身份认证方式，支持灵活组合，保障接入用户身份安全、多重端点安全机制，支持客户端安全检查、SSL 专线、移动端数据保护、支持多种国际标准算法和国家商密算法，保障传输安全、支持 URL 级权限控制、支持独立日志中心等功能。	1 套/年	
25	数据安全服务	提供数据安全检查工具系统 1 套	峰值性能：≥500Mbps 针对行业客户的监管检查和被监管单位或有业务需要单位的敏感数据安全检查和自查自处理的工具型产品。数据安全检查工具主要是针对主机电脑中存放的涉敏文件进行主动检查并具备处理能力、网络中传输敏感数据的监测以及云 / 存储（ 数据库 ）敏感数据检查，为满足合规检查或常态化自查处理及后续的防泄露建设提供基础输入。	1 套/年	
26		提供网络数据防泄露系统（DLP）1 套	峰值性能：≥500Mbps 以《数据安全法》为依据，从认识数据、梳理数据、分析数据（数据分类分级）、使用数据（数据共享与流转）、保护数据（数据加密）、数据交换、数据溯源分析（数据水印和血缘分析）、数据风险识别（机器学习和模型运算）、数据安全管控、用户行为分析，实现数据全生命周期安全（数据安全态势感知）。	1 套/年	

27		提供数据库审计 1 套	最大硬件吞吐量：≥5Gbps，SQL 处理性能：≥10000 条 SQL/s，日志检索性能：≥20000 条/秒；接口：千兆电口≥6 个；万兆光口≥2 个。 支持对用户访问数据库行为的记录、分析和汇报，包括越权查询内置敏感表、篡改内置敏感表等都能够准确识别与告警，避免黑客通过暴库撞库获取账号密码，用来帮助用户事后生成合规报告、事故追根溯源，加强内外部数据库网络行为记录，提高数据资产安全。	1 套/年	
28		数据资产调研	对区主要信息系统进行资产调研，梳理设备类型、数量、拓扑图、数据类型、业务交互场景、数据存储方式等内容，确定数据生命周期内的数据流转过程。 编写《数据资产调研表》12 份 交付内容：交付《数据资产调研表》12 份 不少于 96 工时。	12 份	
29		数据评估方案编制	针对业务系统特点以及数据流转过程，编制风险评估方案，确定风险评估面、评估方式、项目人员、评估分值计算、风险控制、保密措施等内容。 编写《数据安全风险评估实施方案》12 份 交付内容：交付《数据安全风险评估实施方案》12 份 不少于 96 工时。	12 份	
30		数据评估实施	网络数据风险评估：评估网络通信过程中的数据传输安全问题，对数据的完整性、保密性进行验证。 编写《数据安全风险识别报告》12 份 交付内容：交付《数据安全风险识别报告》12 份 不少于 48 工时。	12 份	
31			应用数据风险评估：评估应用系统的交互过程中的数据风险，包括身份鉴别措施、API 接口、文件上传点、数据输入点、数据加解密措施、数据验证、数据脱敏等应用过程。对应用系统、服务器、中间件等组件进行漏洞测试及验证。 编写《数据安全风险识别报告》12 份 交付内容：交付《数据安全风险识别报告》12 份 不少于 96 工时。	12 份	
32			数据库风险评估：评估数据库访问控制机制、数据库安全漏洞、数据审计、数据存储、数据调用过程中的安全风险。 编写《数据安全风险识别报告》12 份 交付内容：交付《数据安全风险识别报告》12 份 不少于 96 工时。	12 份	
33			终端数据安全风险评估：对业务终端、办公终端、运维终端进行安全扫描，根据文件特点制定安全方案，对终端内的敏感文件进行识别，评估终端设备控制策略的有效性，了解终端设备的对数据泄漏、数据传播可能造成的安全隐患。 编写《数据安全风险识别报告》12 份 交付内容：交付《数据安全风险识别报告》12 份 不少于 48 工时。	12 份	
34			个人信息风险评估：从个人信息角度展开风险评估，依照《个人信息保护法》对收集的个人信息进行分析评估，识别和评估个人信息处理活动中存在的安全风险。 编写《个人信息风险识别报告》1 份 交付内容：交付《个人信息风险识别报告》1 份	1 份	

			不少于 12 工时。		
35			管理风险评估：对企业现行的数据安全管理制度、措施、手段、应急处置等流程进行访谈，明确组织活动以及第三方服务对数据安全的影响。 编写《安全管理风险识别报告》1 份 交付内容：交付《安全管理风险识别报告》1 份 不少于 16 工时。	1 份	
36		数据安全整改建议方案	针对风险评估的结果，给出数据安全加固建议，分析应用和数据的特定关系，结合数据分类分级结果、投入产出比等因素制定合理的建设方案。 编写《应用系统数据安全整改建议方案》1 份 交付内容：交付《应用系统数据安全整改建议方案》1 份 不少于 4 工时。	1 份	
37		《数据安全测试报告》	对网络、应用、数据库进行安全测试，出具漏洞测试报告。 编写《数据安全测试报告》1 份 交付内容：交付《数据安全测试报告》1 份 不少于 4 工时。	1 份	
38		《数据安全现状调研评估报告》	针对数据安全总体评估结论，出具评估报告。 编写《数据安全现状调研评估报告》1 份 交付内容：交付《数据安全现状调研评估报告》1 份 不少于 4 工时。	1 份	
39		数据分类分级实施方案	制定数据安全分类分级标准以及实施方案，根据数据类型和特点制定扫描和归纳方案。 编写《数据安全分类分级实施方案》1 份 交付内容：交付《数据安全分类分级实施方案》1 份 不少于 4 工时。	1 份	
40		数据资产识别	梳理需要纳入数据分类分级的数据资产类型与范围，确定数据资产清单。 编写《数据安全分类分级资产清单》1 份 交付内容：交付《数据安全分类分级资产清单》1 份 不少于 4 工时。	1 份	
41		数据资产扫描	借助数据扫描工具+人工分析的方式对区内所有业务系统、数据库、办公终端上的数据内容进行扫描，区分结构化与分结构数据，梳理数据资产类型与总量。 编写《数据安全分类分级扫描报告》1 份 交付内容：交付《数据安全分类分级扫描报告》1 份 不少于 12 工时。	1 份	
42		体系规划	体系规划 根据据安全现状确定数据安全管理的基线要求。基于实际业务需求分析，设计符合业务发展需要的数据安全体系规划，明确数据安全管理的过程、环节及关联关系。通过数据安全相关技术工具能力组合设计数据安全技术防护体系。 编写《数据安全体系规划设计方案》1 份 交付内容：交付《数据安全体系规划设计方案》1 份 不少于 20 工时。	1 份	
43		组织建设	基于际情况，在已有的信息安全或者网络安全组织基础上，加入相关数据安全保护职责并在数据安全技术体系建设过程中发挥管理、指导、协调等作用。	1 份	

			编写《数据安全组织建设方案》1 份 交付内容：交付《数据安全组织建设方案》1 份 不少于 12 工时。		
44		安全策略	进行数据的详细应用场景分析，明确系统数据的分级及数据全生命周期过程。了解系统内和系统间的业务交互过程及数据流转过程。以此总结典型业务场景，归类后进行数据安全策略设计。 编写《数据安全安全策略加固方案》1 份 交付内容：交付《数据安全安全策略加固方案》1 份 不少于 20 工时。	1 份	
45		制度流程	以现有信息安全或者网络安全管理办法为基础，制定并发布数据安全相关管理制度。 编写《数据安全制度文档》1 份 交付内容：交付《数据安全制度文档》1 份 不少于 20 工时。	1 份	
46		数据安全培训	对的数据安全负责人及相关技术人员和业务运营人员开展数据安全意识、数据安全技术、数据安全应急处置等培训内容。 举办 1 次《数据安全培训》，每次 1 学时 交付内容：1 次《数据安全培训》，每次 1 学时 不少于 3 工时。	1 次	
47		数据安全运营	设计数据安全运营体系，建立健全数据安全运营机制，规范日常数据安全运营、应急演练、协同处置工作流程。 举办 1 次《数据安全应急演练》，举办 1 次《数据安全应急响应》每次 1 学时） 交付内容：1 次《数据安全应急演练》，1 次《数据安全应急响应》每次 1 学时） 不少于 3 工时	各 1 次	
48		SSL 证书服务	提供 1 个 daxingedu.cn 域名 SSL 通配符证书一年授权，确保系统安全放护能力和保障制度符合等级保护响应等级要求。	1 个/年	
49	学校端安全处置服务	学校端网络安全现状分析	通过网络安全等级保护差距分析工作与安全访谈，分析各教育网接入单位安全现状。 2、通过对学校网络负责人访谈以及现场机房网络设备的梳理，了解学校网络安全建设情况。 3、基于学校的安全防护情况及安全现状，进行安全策略优化、加固 4、通过对学校现状分析结果，给出网络安全建设意见。 不少于 536 工时	268 所	
50		学校端恶意代码排查	通过对学校服务器操作系统和应用的运行环境进行恶意代码安全检查。 不少于 536 工时	268 所	
51	网站渗透测试服务	WEB 渗透测试	提供 10 个网站的渗透测试服务，输出渗透测试报告，提出问题整改建议，协助问题整改。渗透人员需具备 CISP-PTE(国家注册渗透测试工程师)资质，针对客户 Web 应用系统，采用自动和手动相结合的测试方式对外部和内部 Web 应用系统进行安全性测试.挖掘 Web 应用系统漏洞，提升应用系统安全性。 交付内容：每系统交付《渗透测试方案》、《渗透测试报告》、《渗透测试复测报告》	10 个系统	
52	安全运	应急演练	是指在设计搭建的网络及应用环境中进行模拟入侵及防御的一类演练活动。	服务频次：2 次/年	

	营服务		交付内容：《应急演练报告》2 份 不少于 38 工时		
53		安全预警通告	提供最新的安全动态、技术和定制的安全信息，包括实时安全漏洞通知、病毒、补丁升级、定期安全知识库更新等； 不少于 24 工时	服务频次：不低于 12 次。	
54		重要时期安全保障	重大活动期间，提供安全服务，重保人员至少具备 3 年以上网络安全能力，保证网络安全，负责大兴区教育网安全设备及安全检测系统的日常运维，包括运行状态日检、检测，对安全设备及安全监测系统的策略调优、每天对安全设备日志信息和安全监测系统告警信息进行深入分析，及时发现安全威胁，并进行验证、处置及报告。 交付内容：《重保值守报告》45 份 不少于 1080 工时。	服务频次：根据用户指定时间确定不少于 45 天；	
55		安全宣讲	协助教委针对学校普通师生，培训常规信息安全政策、平时生活信息安全保护手段、专题互动；提供安全宣讲 ppt、宣传海报、易拉宝、小册子、互动用品 交付内容：《安全宣讲记录》2 份	服务频次：2 次/年，提供讲师一名，现场支持人员 2 名	
56		安全培训	针对学校信息安全老师进行技术培训、实操演练；提供互动用品、搭建实操环境。培训材料不少于 50 份 交付内容：《安全培训记录》2 份	服务频次：2 次/年，提供讲师一名，现场支持人员 1 名	
57		安全运营报告	1、按每月安全运营进行安全情况分析、处置、阶段性总结服务，并形成报告进行背书。定期阶段性安全运营情况总结，并形成报告，提交给用户。交付内容：《安全运营报告》12 份， 此项服务对报告进行编写，打印胶装成册 2、提供上半年半年汇报，提供下半年全年安全运营情况汇报，每年提供两次总结 PPT 性安全运营汇报，提供详细安全数据及总结性安全运营报告。交付内容：《阶段性安全运营汇报》PPT2 份；	《安全运营报告》12 次/年 《阶段性安全运营汇报》2 次/年	
58		驻场运维（提供：1 名信息安全专业人员证书的安全运维人员进行保障，驻场运维	工作内容：日常设备巡检：对 1 台安全态势感知、4 台潜伏威胁探针、1 台防火墙、1 台漏洞扫描设备、1 台日志审计、1 台 VPN、1 套端点安全软件、1 台数据库审计、1 套数据安全检查工具、1 套网络数据防泄密等软硬件进行安全巡检，确保设备硬件与软件平台运行正常； 工作内容：对网络安全运行状态监控，对网络安全设备日志进行分析 不少于 730 工时	服务频次：每天查看形成日报、周报、月报（每月打印成册）	

		7*8 小时，远程支持 7*24 小时）	设备日志分析：针对设备日志报表进行日志分析，发现未知风险点；交付内容：《安全日志分析报告》按月打印成册； 不少于 730 工时	12 次/年	
			策略调优服务：通过安全策略的运营（例：自定义策略临时防护）临时应对、规避最新爆发的风险。 交付内容：《安全策略调优报告》按月打印成册； 不少于 182.5 工时	12 次/年	
			威胁分析及处置服务：通过态势感知平台实时针对异常流量分析、攻击日志和病毒日志分析，配合学校端防火墙进行联动处置。 不少于 182.5 工时	1 年	
			安全事件处置：对安全事件进行处置，清除恶意文件、快速恢复业务；交付内容：交付《安全事件处置报告》按实际情况 不少于 182.5 工时	服务频次：每天进行查看，安全处置	

2.3为落实政府采购政策需满足的要求

数据中心相关设备和服务应优先采用国家鼓励的先进技术、工艺、产品和装备，不得使用国家公布的淘汰或禁止的技术、工艺、产品、装备及相关物质。

2.4采购标的的其他技术、服务等要求

本项目服务人员要求从事专职安全服务工作满 2 年，从事服务教育行业安全服务满 2 年，熟练操作服务工具，处置过学校安全事件，具有具备 CISP 等相关安全证书。驻场人员承担北京市大兴区教育网安全设备日常运维及部署、协助制定网络安全规范与方案、协助优化现有网络安全架构、定期评估网络安全风险、网络安全故障排查及安全应急响应和项目管理汇报等工作。同时配备远程专家团队支持。

2.4.1 服务时间：

在 7×8 小时工作时间内设置由专人职守的热线电话，接听内部的服务请求，并记录服务台事件处理结果。

在非工作时间设置有专人 7×24 小时接听的移动电话热线，用于解决内部的网络安全问题以及接听 7×24 小时发网络安全情况。

2.4.2 服务响应时间：

当出现网络安全问题时，服务方提供全年 7*24 小时的电话远程技术支持，同时派出服务工程师前往现场进行安全处置。20 分钟内完成应急响应，2 小时内提交处理整改方案，4 小时以内整改处理。

当服务工具出现故障时服务方接到告知后，30 分钟内携带相同性能设备赶往现场更

换，并将故障设备带回维修。维修完成后免费送至现场安装、调试。

2.4.3 重大活动保障要求

国家重大活动期间及中高考等大型考试期间等特殊时期,网络安全服务单位需 7*24 对业务进行网络安全保障。

要求网络安全服务单位对可能出现的特殊时期，如自然灾害、重大社会事件、停电、设备损毁等进行应急服务和抢修。就保障大兴区教育网安全，提出相应的技术措施和管理措施。

突发事件发生时，网络安全服务人员应迅速赶往突发事件现场，立即对现场进行处理并及时向业主通报处理过程及结果。网络安全服务单位必须进行全天 24 小时值守，保障大兴区教育网安全。

2.4.4 行为规范要求

(1) 遵守各项规章制度，严格按照相应的规章制度办事。

(2) 与运行维护体系其他部门和环节协同工作，密切配合，共同开展技术支持工作。

(3) 出现疑难技术、业务问题和重大紧急情况时，及时向负责人报告。

(4) 现场技术支持时要精神饱满，穿着得体，谈吐文明，举止庄重。接听电话时要文明礼貌，语言清晰明了，语气和善。

(5) 遵守保密原则。对被支持单位的网络、主机、系统软件、应用软件等的密码、核心参数、业务数据等负有保密责任，不得随意复制和传播。

2.4.5 现场服务支持要求

网络安全服务人员要做到耐心、细心、热心的服务。工作要做到事事有记录、事事有反馈、重大问题及时汇报。严格遵守工作作息时间，严格按照服务工作流程操作。

(1) 现场服务工程师应着装整洁、言行礼貌大方，技术专业，操作熟练、严谨、规范；现场支持时必须遵守单位的相关规章制度。

(2) 现场服务工程师在进行现场服务工作时必须在保证数据和系统安全的前提下开展工作。

(3) 现场服务时出现暂时无法解决的故障或其他新的故障时，应告知用户并及时上报负责人，寻找其他解决途径。

(4) 问题解决后，现场服务工程师要详细记录问题的发生时间、地点、提出人和问题描述，并形成书面文档，必要时应向用户介绍问题出现的原因及预防方法和解决技巧。

2.4.6 保密要求

(1) 针对大兴教育网的保密信息，如内部安全设备、服务器、应用系统等产生的各种信息及数据。

(2) IP 地址分配；

(3) 网络拓扑结构；

(4) 有关服务器系统（包括硬件和软件）和应用系统的信息；

(5) 其他与电子政务平台有关的信息；

(6) 系统登陆密码；在项目讨论过程中，信息提供方和接受方之间所有往来的书面资料，电子文档资料及访谈记录等与本项目相关的信息，都将被视为保密信息。

(7) 为避免在计算机信息网络安全评估项目中发生泄密事件，给计算机信息网络带来不必要的损失，分别从项目和资料进行保密控制，确保项目的正常进行。

(8) 项目保密

(9) 双方单位签订项目保密协议，项目实施单位与安全服务人员签订保密承诺书，明确双方的保密义务、职责和违约处罚，根据的需要确定保密内容和期限。

(10)对于双方互相提交的文档资料，部分涉及计算机信息系统需保密的电子文档仅限于提供给签立保密协议的核心项目组成员；对于进行解密处理的电子文档仅限于项目组内使用，受项目保密协议约束。

2.5需由供应商提供设计方案、解决方案或者组织方案的采购项目，应当说明采购标的的功能、应用场景、目标等基本要求

采购标的功能：

采用规范化的运维管理，专业的安全数据分析和事件处置方法，通过可信、可控和可量化的高质量安全服务，建立北京市大兴区教育网网络安全运维体系，全面加强大兴区教育网网络安全、系统安全、信息安全、应用安全、数据安全、终端安全，保障终端、网络、系统和服务器安全，加强系统和应用软件安全管理和升级维护，从而更好的全面提高大兴区教育网网络和信息安全保障水平，保障大兴区教育网信息系统的各项业务应用以及业务数据的安全可靠。主要包括：(1)大兴区教育网安全态势感知服务，(2)数据中心防火墙安全防护服务，(3)服务器安全防护服务，(4)安全监控漏洞扫描服务，(5)网站云防护服务，(6)上网行为管理服务，(7)日志审计服务，(8）VPN 服务，(9)数据安全服务，(10)学校端安全处置服务，(11)网站渗透测试服务，(12)安全运营服务。

应用场景：

北京市大兴区教师进修学校拟通过网络级数据安全整体保障项目的开展，根据大兴区教育网安全服务实际业务需求及相关法律法规要求，优化和完善网络安全、数据安全管理体系，并采取全面的技术、管理评估，评估相关重要系统和数据的安全性状况，完善大兴区教育网安全状况，确保大兴区教育网的安全稳定运行及数据资产的安全。

项目目标：

通过外购安全专家服务和人员，协助大兴区教育网定期检查信息系统中是否存在安全隐患、跟踪并获得相应的漏洞补丁、及时修复信息系统安全问题。降低信息系统中安全隐患被非法利用的可能性或在被利用后能及时加以响应。

3. 履约验收方案

3.1履约验收主体

北京市大兴区教师进修学校

3.2履约验收时间

服务期限结束后 30 天内完成最终验收。

3.3履约验收方式

对所有服务项目的交付成果验收，包括但不限于产品、文档、软件、硬件等进行现场验收和材料核验。

3.4履约验收程序

验收准备阶段：

成立项目验收小组，具体负责验收事宜。验收小组包括采购人、供应商和第三方专业机构或专家。

编写验收计划，明确验收的内容、标准、方法和时间安排。

验收实施阶段：

对安全服务进行全面检视，包括服务的质量、效果和是否符合合同约定的标准，并检查交付文档和交付物内容与合同内容的符合性。

验收评估阶段：

根据验收标准对安全服务质量进行评估，评价其是否达到预期效果。

对服务供应商的服务及交付物进行评估，包括响应速度、问题解决能力、文档规范性等。

验收报告阶段：

编写验收报告，详细记录验收过程和结果，包括各项标准的达标情况及总体评价。

验收报告由验收双方共同签署，作为合同履行的证明。

3.5履约验收内容

服务内容	交付详情
提供服务工具：态势感知平台（含 10 个联动授权）	提供态势感知平台设备 1 套/年（含 10 个联动授权）
提供服务工具：潜伏威胁探针（部署于核心交换区）	提供潜伏威胁探针设备（部署于核心交换区）1 套/年
提供服务工具：潜伏威胁探针（部署于其他安全节点）	提供潜伏威胁探针设备（部署于其他安全节点）3 套/年
提供服务工具：数据中心防火墙	提供数据中心防火墙设备 1 套/年
通过服务工具：服务器安全防护软件	服务器安全防护软件 500 终端授权/年
提供：服务工具 WEB 安全监控漏洞设备	提供服务工具 WEB 安全监控漏洞设备 1 套/年
提供服务工具：网站云防监控	提供 30 域名网站云监控 1 年
提供服务工具：上网行为审计设备	提供上网行为审计设备 1 套/年
提供服务工具：日志审计设备	提供日志审计设备 1 套/年
提供服务工具：VPN 设备	提供 VPN 设备 1 套/年
提供服务工具：数据安全检查工具系统	提供数据安全检查工具系统 1 套/年
提供服务工具：网络数据防泄露系统	提供网络数据防泄露系统 1 套/年
提供服务工具：数据库审计	提供数据库审计设备 1 套/年
资产脆弱性管理	12 次/年，交付《资产台账》12 份

未知威胁发现	12 次/年，交付《安全态势感知报告》12 份
安全事件处置	服务期内不少于 50 次，提供安全时间处置记录 50 份，提供安全事件处置记录 50 份
应急响应	针对下属 268 所学校，服务期内不少于 120 次，交付《应急响应报告》120 份
安全策略管理	12 次/年，交付《安全策略调优》12 份
安全加固	12 次/年，交付《安全加固报告》12 份
虚拟补丁更新服务	1 年授权
病毒处置服务	服务期内不少于 100 次
系统漏洞扫描服务	12 次/年 每次 28 系统（总服务器不少于 300 个） 交付《主机系统漏洞检测分析报告》12 份
WEB 漏洞扫描服务	4 次/年，共 28 个系统，交付《Web 漏洞检测分析报告》4 份
配置核查服务	12 次/年，交付《配置核查分析报告》12 份
流量分析	12 次/年，交付《月度安全报告》12 份
网站监测预警服务	按需不限次，包含 30 个域名
应急处置服务	按需不限次
编写《数据资产调研表》	交付 12 份
编写《数据安全风险评估实施方案》	交付 12 份
编写《网络数据风险评估报告》	交付 12 份
编写《应用数据风险评估报告》	交付 12 份
编写《数据库风险评估报告》	交付 12 份

编写《终端数据安全风险评估报告》	交付 12 份
编写《个人信息风险识别报告》	交付 1 份
编写《安全管理风险识别报告》	交付 1 份
编写《应用系统数据安全整改建议方案》	交付 1 份
编写《数据安全测试报告》	交付 1 份
编写《数据安全现状调研评估报告》	交付 1 份
编写《数据安全分类分级实施方案》	交付 1 份
编写《数据安全分类分级资产清单》	交付 1 份
编写《数据安全分类分级扫描报告》	交付 1 份
编写《数据安全体系规划设计方案》	交付 1 份
编写《数据安全组织建设方案》	交付 1 份
编写《数据安全安全策略加固方案》	交付 1 份
编写《数据安全制度文档》	交付 1 份
举办数据安全培训	举办 1 次《数据安全培训》，1 学时
数据安全运营	举办 1 次《数据安全应急演练》，举办 1 次《数据安全应急响应》每次 1 学时）
提供 daxingedu.cn 域名通配符 SSL 证书	1 年
学校端网络安全现状分析	服务覆盖下属 268 所学校
学校端恶意代码排查	服务覆盖下属 268 所学校

WEB 渗透测试	10 系统，交付《渗透测试方案》、《渗透测试报告》、《渗透测试复测报告》10 份
应急演练	2 次/年，交付《应急演练报告》2 份
安全预警通告	12 次/年，交付《安全预警通告》12 份
重要时期安全保障	45 天，交付《重保值守报告》45 份
安全宣讲	2 次/年，交付《安全宣讲记录》2 份
安全培训	2 次/年，交付《安全培训记录》2 份
安全运营报告	12 次/年，交付安全运营报告》12 次/年。
阶段性安全运营汇报	2 次/年《阶段性安全运营汇报》2 次/年。
驻场运维：日常设备巡检	每天对设备进行检查和监控确保设备安全运行形成日报、周报、月报（每月打印成册））
驻场运维：设备日志分析	每天对设备日志进行监控分析生成《安全日志分析报告》按月打印成册
驻场运维：策略调优服务	每天对设备策略进行监控和优化生成《安全策略调优报告》按月打印成册
驻场运维：威胁分析及处置服务	通过态势感知平台实时针对异常流量分析、攻击日志和病毒日志分析，配合学校端防火墙进行联动处置。每天监控即时处置
驻场运维：安全事件处置	每天监控，对出现的安全事件进行处置，清除恶意文件、快速恢复业务。形成《安全事件处置报告》
安全服务工单	安全服务期间所产生的工作记录单

3.6履约验收验收标准

根据我区财政局的文件要求，完成本项目的财政支出、预算、绩效评价和财政事前

或事后评审及招投标等相关工作。

1.功能性：交付成果是否满足项目的功能要求，是否满足项目需求。

2.性能：交付成果的性能是否满足合同要求，能否满足项目需求和响应时间要求等。

3.安全性：交付成果是否符合安全标准和合规要求，是否能有效保护系统和数据的安全。

4.可靠性：交付成果的可靠性和稳定性，是否能满足项目的长期运行要求。

5.时效性：当发起服务需求后，现场驻场人员立即响应服务要求，当驻场人员无法处置需要高级技术工程师/专家到场处置时，应在接到服务需求后 90 分钟内到达现场进行处置。7*24 远程技术支持。

6.文档完整性和准确性：交付的文档是否齐全、清晰并准确记录了交付成果的功能和操作方法。

3.7履约验收其他事项

3.7.1 风险控制

1.交付成果质量不达标：在预验收和正式验收过程中，如果发现交付成果质量不达标，需及时与服务提供商沟通，提出问题并要求改进。

2.验收过程延迟：若服务提供商未按时交付交付成果或需求方未按时进行验收，需要及时沟通解决问题，并延后验收时间安排。

3.验收意见不一致：若需求方和服务提供商对交付成果的评估结果存在分歧，需通过沟通协商解决，并最终达成一致。

3.7.2 验收后的补救措施

若交付成果在验收过程中被发现存在不符合合同要求的情况，需服务提供商承担相应的责任并采取补救措施进行修复和改进。

3.7.3 验收结果的利用

验收结果将作为决策的重要依据，确认是否接受交付成果。如果验收结果符合合同要求，服务提供商将付款，同时进入后续的项目交付和运维阶段。

3.7.4 验收方案的变更

如需修改本履约验收方案，应经双方协商一致，并由签约代表进行签署、确认变更。

4、其他要求

1. 质量保证

设备发生故障时，携带同性能设备对故障设备进行更换，同时按照原设备配置完成调试。故障设备保修，待设备完成维修后，将设备换回。

2. 响应时间

风险隐患或网络安全事件后立即响应,30 分钟内服务人员须上报采购方管理人员并提供免费技术咨询，1 小时内完成应急处置，并配合完成后期的情况分析、整改报告等工作。

3、交付要求

合同签订后，按照规定的服务起止日期执行

第六章　　拟签订的合同文本

政府采购合同

（合同模板仅供参考，以双方协商后签订的合同为准）

合同编号：

项目名称：信息化运行维护费-1 2024年大兴区教育网安全服务项目

项目编号：

甲　　方：北京市大兴区教师进修学校

乙　　方：

签署日期：　　年　　月　　日

合 同 书

甲方（采购人）：北京市大兴区教师进修学校

法人代表：

项目负责人：

联系电话：

乙方（中标人）：

法人代表：

项目负责人：

联系电话：

北京市大兴区教师进修学校（甲方）__信息化运行维护费-1 2024年大兴区教育网安全服务项目__(项目名称)中所需__信息化运行维护费-1 2024年大兴区教育网安全服务项目__(服务内容)经__北京驰度项目管理咨询有限公司__(采购代理机构)以__11011524210200020248-XM001__号招标文件在国内 （**公开**/邀请）招标。经评标委员会评定_____(乙方)为中标人。甲乙双方同意按照下面的条款和条件，签署本合同。下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

a. 本合同书

b. 中标通知书

c. 补充协议或附件

d. 招标文件 (含招标文件补充通知)

e. 投标文件 (含澄清文件)

第一章 服务内容及合同期限

第一条 乙方为甲方提供项目服务，在采购人指派下开展各项工作。甲方向乙方支付服务费。

第二条 合同期限：2024年12月1日至2025年11月30日。

第二章 服务要求

第三条 服务工作内容：乙方按照 信息化运行维护费-1 2024 年大兴区教育网安全服务项目 的要求，根据甲方的实际需求提供服务

第三章 双方权利义务

第四条 甲方的权利与义务

1．甲方有权对乙方就服务项目所做工作进行监督检查，乙方同意在服务项目进行过程中接受甲方的监督检查。

2．在本合同生效后，甲方应向乙方提供与本项目相关的、必要的信息，并为所供信息的准确性、真实性、完整性负责。提供形式需经双方认可。

3．甲方应严格按照本合同约定的期限和方式支付服务费和其他合理费用。

4．合同生效后，甲方应配置与此次项目相关人员配合乙方开展工作，涉及与入驻单位的沟通，甲方应给与充分的配合与协调。

5．甲方因违约或其他不正当行为给乙方或任何第三人造成损失，甲方应承担赔偿责任。

第五条 乙方的权利与义务

1．乙方应尽一切努力，按照本合同及其附件的约定高效和经济地向甲方履行服务义务,并对服务的品质负责。

2．乙方应根据甲方实际情况，制定并实施符合甲方实际需求的服务方案并向甲方提供该方案。

3．乙方的工作人员在履行与本合同有关的服务中不得为私利而接受贸易佣金、回扣或类似款项。

4．乙方及其雇员或代理人因违约或其他不正当行为给甲方或任何第三人造成损失，乙方应承担全部赔偿责任。

5．乙方应根据项目的进展定期与甲方的相关负责人员进行交流汇报，告知项目的实施状况。

第四章 保密条款

第六条 任何一方在签署或履行本合同过程中对知晓的对方未公开的商业秘密及其他资料和信息，未经对方书面同意不得使用或向第三方泄露，否则应承担由此给另一方造成的损失，但甲方为履行本合同目的使用乙方提供的服务除外，法律另有规定的除外。

第七条 乙方须保证参与本项目的雇员对本项目中所获知的甲方相关信息保密，不得使用或向第三方泄露。

第八条 保密信息包括但不限于以下内容：工作流程、规章制度、数据资源、客户信息、员工信息、协议内容、经营状况指标、不公开的任何资料、合作伙伴及合作关系细节、未来商业计划、涉及商业秘密的业务函电等。

第九条 任何一方违反本条约定的保密事项，造成对方损失的，应承担损失（包括但不限于经济、名誉方面的损失）赔偿责任。赔偿金额为合同金额的 5%。

第十条 乙方保证提交甲方之研究资料及任何信息没有侵犯任何第三方的制式产权及其它权益。

第五章 费用及支付

第十一条 合同款计算方式，自签订合同之日起 1 年时间，年服务费人民币 元整（大写：_____）。

第十二条 支付方式和支付时间

1.合同款分 2 次支付，甲乙双方签订服务合同后 15 日内，乙方向甲方支付合同总金额的 3%作为履约保证金，甲方向乙方支付合同首付款人民币： 1100000.00 （大写：壹佰壹拾万元整）；项目结束通过验收后，剩余款项的结算以审计金额为准，审计结束后于 30 个工作日内付给乙方并同时无息退还履约保证金。

乙方应在甲方付款前向甲方开具并送达相应金额的发票，否则甲方付款时间可以顺延。

2.服务费甲方可通过银行汇款方式向乙方支付。

乙方账户名称：

开户银行：

账号：

3.付款前乙方向甲方开具等额增值税普通发票。

第六章 违约责任

第十三条 双方应相互尊重彼此享有的合同权利，并采取一切合理的手段达成本合同。故双方一致表示，希望本合同在相互间公正实施，不损害任何一方的利益。

第十四条 任何一方违反本合同项下的义务，须向对方承担违约责任，造成损失的，须承担赔偿责任。赔偿额应相当于因违约所造成的实际损失。

第十五条 乙方未按期提供合同约定的服务或提供的服务不能满足甲方的需求，甲方有权要求其采取补救措施。经甲方书面催促，乙方在一个月的宽限期内仍未按约定提供服务的，甲方有权解除本合同并不再支付剩余合同款项。合同解除后，乙方应返还已

收取的未提供服务的费用和利息，并按照本合同剩余项目服务费用的 20%作为违约金支付给甲方，具体金额双方按实际履行情况另行书面确认。

第十六条 甲方无故延迟支付服务费用，由此造成工作停滞、延误的，乙方不承担延迟履行的责任。经书面催告，甲方在一个月的宽恕期内仍未按约定支付服务费用的，乙方有权解除合同。合同解除后，甲方应按照合同剩余项目服务费的 20%作为违约金支付给乙方并赔偿乙方为准备履约合同而花费的合理费用，具体金额双方按实际履行情况另行书面确认。

第十七条 保密信息的收受方违反保密协议的规定，致使保密信息泄露的，收受方应向披露方承担赔偿责任，同时有义务采取有效措施阻止信息进一步扩散。

第七章 争议解决

第十八条 双方当事人应尽全力友好协商解决因本合同而产生的或与本合同有关的一切争议。

第十九条 双方如不能友好协商解决因本合同而产生的或与本合同有关的争议，任何一方均可向甲方所在地有管辖权的人民法院提起诉讼。

第八章 通知

第二十条 甲乙双方因履行本合同而相互发出或提供的所有通知、文件、资料等，均应按照本合同所列明的通讯地址、电话号码、传真号码、电子邮件等通知方式进行传达。一方如果迁址或变更相关号码，应当及时书面通知对方。通过邮寄方式的，挂号寄出或者投邮当日视为送达，以传真或电子邮件方式的，发出视为到达。

第二十一条 一方变更通知或通讯地址，应当变更之日起 5 日内，以书面形式通知对方，否则，由未通知方承担由此而引起的相关责任。

第九章 验收标准

根据我区财政局的文件要求，完成本项目的财政支出、预算、绩效评价和财政事前或事后评审及招投标等相关工作。

第十章 生效及其他事项

第二十二条 本合同一式柒份，甲乙双方各执叁份，采购代理机构执壹份，具有同等法律效力。

第二十三条 本合同自甲乙双方签字盖章之日起生效，本协议签订后如需修改变更，须经甲乙双方协商达成一致后，以签订补充协议进行修改。补充协议与本合同具有同等

法律效力。补充协议也本合同不一致的，以补充协议所载内容为准。

（以下无正文）

（本页为签署页）

甲 方（签章）：　　乙 方（签章）：

甲方代表（签名）：　　乙方代表（签名）：

开户行：　　开户行：

账号：　　账号：

地址：　　地址：

电话：　　电话：

签订日期：　　年　月　日　　签订日期：　　年　月　日

第七章　投标文件格式

投标人编制文件须知

1、投标人按照本部分的顺序编制投标文件，编制中涉及格式资料的，应按照本部分提供的内容和格式（所有表格的格式可扩展）填写提交。

2、对于招标文件中标记了“实质性格式”文件的，投标人不得改变格式中给定的文字所表达的含义，不得删减格式中的实质性内容，不得自行添加与格式中给定的文字内容相矛盾的内容，不得对应当填写的空格不填写或不实质性响应，否则**投标无效**。未标记“实质性格式”的文件和招标文件未提供格式的内容，可由投标人自行编写。

3、全部声明和问题的回答及所附材料必须是真实的、准确的和完整的。

一、投标文件格式

投标文件封面（非实质性格式）

投 标 文 件

项目名称：
项目编号：

投标人名称：

1 资格证明文件
1-1 营业执照等证明文件

1-2 投标人资格声明书（实质性格式）

投标人资格声明书

致：采购人或采购代理机构

在参与本次项目投标中，我单位承诺：

（一）具有良好的商业信誉和健全的财务会计制度；

（二）具有履行合同所必需的设备和专业技术能力；

（三）有依法缴纳税收和社会保障资金的良好记录；

（四）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（重大违法记录指因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，不包括因违法经营被禁止在一定期限内参加政府采购活动，但期限已经届满的情形）；

（五）我单位不属于政府采购法律、行政法规规定的公益一类事业单位、或使用事业编制且由财政拨款保障的群团组织（仅适用于政府购买服务项目）；

（六）我单位不存在为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后，再参加该采购项目的其他采购活动的情形（单一来源采购项目除外）；

（七）与我单位存在“单位负责人为同一人或者存在直接控股、管理关系”的其他法人单位信息如下（如有，不论其是否参加同一合同项下的政府采购活动均须填写）：

序号	单位名称	相互关系
1		
2		
…		

上述声明真实有效，否则我方负全部责任。

投标人名称（加盖公章）：_____

日期：_____年_____月_____日

说明：供应商承诺不实的，依据《政府采购法》第七十七条“提供虚假材料谋取中标、成交的”有关规定予以处理。

1-3 中小企业声明函（实质性格式）

中小企业声明函（工程、服务）格式

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

1.（标的名称），属于（采购文件中明确的所属行业）行业；承建（承接）企业为（企业名称），从业人员_____人，营业收入为_____万元，资产总额为万元，属于（中型企业、小型企业、微型企业）；

2.（标的名称），属于（采购文件中明确的所属行业）行业；承建（承接）企业为（企业名称），从业人员_____人，营业收入为_____万元，资产总额为万元，属于（中型企业、小型企业、微型企业）；

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：_____

日 期：_____

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

残疾人福利性单位声明函格式

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**（请进行勾选）：**

□不属于符合条件的残疾人福利性单位。

□属于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：

1-4 投标保证金凭证/交款单据电子件

2　投标书（实质性格式）

投标书

致：（采购人或采购代理机构）

我方参加你方就_____（项目名称，项目编号）组织的招标活动，并对此项目进行投标。

1. 我方已详细审查全部招标文件，自愿参与投标并承诺如下：

（1）本投标有效期为自提交投标文件的截止之日起_____个日历日。

（2）除合同条款及采购需求偏离表列出的偏离外，我方响应招标文件的全部要求。

（3）我方已提供的全部文件资料是真实、准确的，并对此承担一切法律后果。

（4）如我方中标，我方将在法律规定的期限内与你方签订合同，按照招标文件要求提交履约保证金，并在合同约定的期限内完成合同规定的全部义务。

2. 其他补充条款（如有）：_____。

与本投标有关的一切正式往来信函请寄：

地址_____　　传真_____

电话_____　　电子函件_____

投标人名称（加盖公章）　_____

日期：_____年_____月_____日

3　授权委托书（实质性格式）

授权委托书

本人_____（姓名）系_____（投标人名称）的法定代表人（单位负责人），现委托_____（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、递交、撤回、修改_____（项目名称）响应文件和处理有关事宜（除合同签约以外），其法律后果由我方承担。

委托期限：自本授权委托书签署之日起至响应有效期届满之日止。

代理人无转委托权。

投标人名称（加盖公章）：_____

法定代表人（单位负责人）（签字或盖章）：_____

委托代理人（签字或盖章）：_____

日期：_____年_____月_____日

法定代表人（单位负责人）有效期内的身份证电子件：

委托代理人有效期内的身份证电子件：

说明：

1.若供应商为事业单位或其他组织或分支机构（仅当招标文件注明允许分支机构投标的），则法定代表人处的签署人可为单位负责人。

2. 若投标文件中签字之处均为法定代表人（单位负责人）本人签署，则可不提供本《授权委托书》，但须提供《法定代表人（单位负责人）身份证明》；否则，不需要提供《法定代表人（单位负责人）身份证明》。

3.供应商为自然人的情形，可不提供本《授权委托书》。

附：法定代表人（单位负责人）身份证明

致：（采购人或采购代理机构）

兹证明，

姓名：____性别：____年龄：____职务：____

系_____（投标人名称）的法定代表人（单位负责人）。

附：法定代表人（单位负责人）有效期内的身份证电子件。

投标人名称（加盖公章）：_____

法定代表人（单位负责人）（签字或盖章）：_____

日期：_____年_____月_____日

4　开标一览表（实质性格式）

开标一览表

项目编号：_____　　项目名称：_____

包号	投标人名称	投标报价	
		大写	小写

注：1.此表中，每包的投标报价应和《投标分项报价表》中的总价相一致。

2.本表必须按包分别填写。

投标人名称（加盖公章）：_____

日期：_____年_____月_____日

5　投标分项报价表（实质性格式）

投标分项报价表

项目编号：_____ 项目名称：_____报价单位：人民币元

序号	分项名称	数量	单价（元）	合价（元）	备注/说明
1					
2					
3	…				
			总价（元）		

注：1.本表应按包分别填写。

2.如果不提供分项报价将视为没有实质性响应招标文件。

3.上述各项的详细规格（如有），可另页描述。

投标人名称（加盖公章）：_____

日期：_____年_____月_____日

6　合同条款偏离表（实质性格式）

合同条款偏离表

项目编号：_____　　项目名称：_____

序号	招标文件条目号（页码）	招标文件要求	投标文件内容	偏离情况	说明
对本项目合同条款的偏离情况（应进行选择，未选择**投标无效**）： □**无偏离**（如无偏离，仅选择无偏离即可；无偏离即为对合同条款中的所有要求，均视作供应商已对之理解和响应。） □**有偏离**（如有偏离，则应在本表中对偏离项逐一列明，否则**投标无效**；对合同条款中的所有要求，除本表列明的偏离外，均视作供应商已对之理解和响应。）					

注：“偏离情况”列应据实填写“正偏离”或“负偏离”。

投标人名称（加盖公章）：　　_____

日期：_____年_____月_____日

7　采购需求偏离表（实质性格式）

采购需求偏离表

项目编号：_____　　项目名称：_____

序号	招标文件条目号(页码)	招标文件要求	投标响应内容	偏离情况	说明
对本招标文件中的所有商务、技术要求的偏离情况（应进行选择，未选择**投标无效**）： □**无偏离**（如无偏离，仅选择无偏离即可；无偏离即为对招标文件中的所有商务、技术要求，均视作供应商已对之理解和响应。） □**有偏离**（如有偏离，则应在本表中对偏离项逐一列明，否则**投标无效**；对招标文件中的所有商务、技术要求，除本表列明的偏离外，均视作供应商已对之理解和响应。）					

注：“偏离情况”列应据实填写“正偏离”或“负偏离”。

投标人名称（加盖公章）：　　_____

日期：_____年_____月_____日

8 中标服务费承诺书（实质性格式）

致:北京驰度项目管理咨询有限公司

我们在贵公司组织的_____项目（项目编号：_____）采购中若中标，我们保证在领取中标通知书的同时按招标文件的规定，向贵公司一次性支付应当交纳的中标服务费用。

收费标准依据国家计委印发的计价格[2002]1980 号关于《招标代理机构服务费管理暂行办法》的通知、发改办价格[2003]857 号令及发改价格[2011]534 号令，以中标金额为基数，按差额定律累积法计算。

特此承诺！

承诺方名称：_____

承诺方公章：_____

地址：_____

电话：_____ 传真：_____

电传：_____ 邮编：_____

日期：_____

9 项目实施方案

内容自拟。

10 拟投入本项目团队人员汇总表

拟投入本项目团队人员汇总表

序号	姓名	学历	专业	技术职称	相关工作年限	在本项目拟任职务

11 近年类似业绩及证明文件

近三年类似业绩清单及证明文件

序号	项目名称	合同主要内容	合同总金额	委托方	合同签订时间	备注

注：

1、提供投标人近三年以来（2021年10月1日起至今、以签订日期为准）承担过类似项目业绩

2、应提供有效的证明材料（提供合同首页、服务主要内容页、盖章页等关键页、以签订日期为准）需提供合同复印件加盖公章。

投标人名称（加盖公章）：　　_____

日期：_____年_____月_____日

12 招标文件要求提供或投标人认为应附的其他材料