**浦东教育城域网升级服务项目招标需求**

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 投标人对所提供的系统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 投标人提供的货物应当是全新的、未使用过的，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 投标人应如实准确地填写投标货物的规格型号、技术参数、品牌、产地等相关信息，因上述信息内容填写不完整、不准确，而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。

★1.5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））

★1.6投标人提供的产品和服务必须符合国家强制性标准。

1.7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。

1.8投标人在投标前应认真了解采购人的使用需求、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。

1.9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。

1.10本项目如涉及软件开发，则开发软件（包括软件、源程序、数据文件、文档、记录、工作日志、或其它和该合同有关的资料的）的全部知识产权归采购人所有。投标人向采购人交付使用的软件系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。支撑该系统开发和运行的第三方编制的软件的知识产权仍属于第三方。如采购人使用该软件系统构成上述侵权的，则由投标人承担全部责任。

1.11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**

浦东教育城域网升级服务项目

**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

沪教委信息〔2018〕28号《上海市教育信息化2.0行动计划（2018-2022）》提出：“教育网络统一接入管理。优化应用运行环境，完善网络缓存、网站加速等配套设施，提升用户上网体验。推动各级各类教育单位实现无线网络高速接入全覆盖，通过教育城域网实现高速互联，提高人均互联网带宽。加强教育网络统一管理、统一监测、统一防护，提高教育网络基础设施的专业服务和运行保障能力。”

2021年7月，教育部等六部委发布《教育部等六部门关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》（教科信〔2021〕2号）指出：“到2025年，基本形成结构优化、集约高效、安全可靠的教育新型基础设施体系，并通过迭代升级、更新完善和持续建设，实现长期、全面的发展。建设教育专网和“互联网+教育”大平台，为教育高质量发展提供数字底座。建设教育专网。按需扩大学校出口带宽，实现中小学固定宽带网络万兆到县、千兆到校、百兆到班，以及部省数据中心、高校超算中心等设施的高速互联。深入推进IPv6等新一代网络技术的规模部署和应用。”

沪教委财务2022年1月《关于征求<进一步促进本市义务教育学校建设的实施意见（意见征求稿）>意见的函》提出：优化学校到区教育信息中心网络链路，学校核心层主干带宽和出口链路达到万兆标准，师生用户可使用互联网出口带宽最低不低于1Mbps。

通过对现有浦东教育城域网的前期调研发现，现有浦东教育城域网主要存在如下几个方面的问题：

（1）现有浦东教育城域网主干网依托运营商网络管线组建MPLS VPN专网，网络架构采用分层设计，分为核心层、汇聚层、接入层。网络按业务划分互联网访问（综合）、财务管理、视频监控、电子巡考、理化实验考试等业务子网，确保各教育业务独立运行不受干扰，也保证了网络与信息的基本安全；原项目建设于2013年，在网运行时间已经较长，随着教育信息系统逐步的迁移上云，各个单位上云访问的需求越来越多，业务模型越来越复杂，亟需采用更先进性的技术对现有浦东教育城域网进行升级，并满足业务网络端到端开通和业务快速部署的服务需求。

（2）教育数据中心承载整个教育城域网的网络出口和安全管理职能。浦东新区教育信息网接入单位超过1000个，而且接入单位以每年超过20所的速度在增加，数据中心对于提供稳定、安全、充足的网络带宽以满足教育单位的日益增加的网络需求至关重要；目前浦东教育数据中心的各类设备最高仅支持40G带宽能力，不能支撑后续60G-100G的目标发展要求。

（3）2013年起，浦东教育局面向所有公办学校接入设备进行统一建设配置，至今已有9年，设备已严重老化，故障维修困难，亟需结合教育城域网升级整体更新，性能上需满足未来8-10年浦东教育信息化发展的要求。

本项目主干网升级及链路服务由运营商另行负责，不在本项目范围内，本项目主要负责浦东教育城域网数据中心和学校侧网络（下图绿色区域部分）的性能和服务能力提升。



图1 浦东教育城域网架构拓扑

4.2 项目招标范围及内容

本次浦东新区教育城域网升级项目建设强调以学校实际需求为导向，以网络基础设备平台为核心，突出‘以人为本’的服务观，突出信息化硬件一流、信息化服务应用有创新，强调服务于学校管理者、教师、学生和家长，为最终用户提供稳定、安全的基础支撑网络服务。

本次项目目标为对浦东教育城域网数据中心和学校侧提升整体设备性能、优化服务模式，构建新一代智能网络，提供高速互联、智能可视、安全稳定的“领先业界”的基础教育城域网络服务，达到浦东教育数字化转型中“教育信息化基础设施领先”的要求。

本次项目招标范围及内容包括：主要包含对浦东新区教育城域网教育数据中心升级服务，提升数据中心设备未来网络带宽性能满足100G带宽要求、上网行为审计及流控等配套服务要求；全域IPV6升级改造服务；学校网络接入能力升级服务； 8年网络运维服务。

4.3本项目服务期：自合同签订之日起8年。

4.3.1整体项目进度安排

根据浦东新区城域网升级服务项目的进度安排情况，需在2023年-2025年间完成整体项目的软硬件升级改造、业务割接和IPv6改造工作，具体各阶段进度安排如下：

（1）2023年完成数据中心设备部署和集成调试。

（2）2023年至2025年分批次完成大部分学校端接入路由器、防火墙设备更新、系统集成、业务割接、系统联调、测试和试运行，并逐步根据学校计划完成学校接入侧接入路由器、防火墙设备的IPV6改造；

（3）2025年完成整体设备更新服务。

（4）2023年至2030年：持续运维服务，保证原系统正常运行。

**5 承包方式**

5.1 依据本项目的招标范围和内容，中标人以包系统设计、包供货、包安装集成调试、包业务割接、包质量、包8年运营服务的方式实施总承包。

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。

**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。

7.1.2本项目合同结算价包括与第三方的原有系统对接、割接升级和优化改造的一切费用，采购人不另行支付相关费用。

7.1.3发生设备维修的，如该设备尚在质保期内的，采购人不另行支付相关费用；如在质保期外的，单价按照投标文件中明确的备品备件单价（含维修人工费）计取，数量按实结算。如投标文件中没有类似备品备件单价可参照的，则由合同双方协商确定维修单价。

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，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）第一年付款：甲方与乙方合同签订后，20日内支付合同总金额的6.5%，年内完成采购人指定的交付任务且验收后支付合同总金额的6%；

（2）第二年付款：2024年上半年内支付合同总金额的6.5%，下半年内完成采购人指定的交付任务且验收后支付合同总金额的6%；

（3）第三年付款：2025年上半年内支付合同总金额的6.5%，下半年内完成采购人指定的交付任务且验收后支付合同总金额的6%；

（4）第四年付款：2026年上半年内支付合同总金额的6.5%，下半年内完成采购人指定的交付任务且验收后支付合同总金额的6%；

（5）第五年付款：2027年上半年内支付合同总金额的6.5%，下半年内完成采购人指定的交付任务且验收后支付合同总金额的6%；

（6）第六年付款：2028年上半年内支付合同总金额的6.5%，下半年内完成采购人指定的交付任务且验收后支付合同总金额的6%；

（7）第七年付款：2029年上半年内支付合同总金额的6.5%，下半年内完成采购人指定的交付任务且验收后支付合同总金额的6%；；

（8）第八年付款：2030年上半年内支付合同总金额的6.5%，下半年内完成采购人指定的交付任务且验收后支付合同总金额的6%。

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**

（1）《IP网络技术要求--网络性能参数与指标》（YD/T 1171-2001）

（2）《基于云计算的电子政务公共平台技术规范》（GB/T 33780.1-2017）

（3）《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）

（4）《数据中心设计规范》(GB50174-2017）

（5）《综合布线系统工程设计规范》(GB50311-2016）

（6）《通信线路工程设计规范》（GB51158-2015）

（7）《教育部等六部门关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》（教科信〔2021〕2号）

（8）《上海市教育信息化2.0行动计划（2018-2022）》（沪教委信息〔2018〕28号）

（9）《上海市教育数字化转型实施方案（2020-2023）》沪教委信息〔2021〕23 号

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工作量清单**

**9.1.1 工作量清单汇总**

| **序号** | **工作内容** | **服务要求** | **备注** |
| --- | --- | --- | --- |
| 1 | 数据中心升级服务 | 1、投标人提供数据中心网络出口设备、防火墙、内网汇聚路由器、流控设备、SDN控制器、VPN接入、DNS和5G专网UPF独享接入所需的设备及服务；2、投标人提供数据中心本次升级所涉及的网络、安全等各类设备的割接及集成服务；3、投标人提供数据中心本次升级所涉及的网络、安全等各类设备的8年技术支撑服务。 | **●** |
| 2 | 全网 IPV6 升级改造服务 | 1、投标人提供教育城域网全域规划，数据中心、学校接入侧实施服务；2、投标人提供教育城域网全网 IPV6 地址 DHCP管理、分配设备、访问记录审计所需的设备及服务；3、投标人提供教育城域网IPV6/IPV4转换所需的设备及服务；4、投标人提供全区862所学校内网IPv6改造升级的规划、培训及过程中的技术支持服务；5、投标人提供本次全网IPv6升级改造服务后的8年技术支撑服务。 | **●** |
| 3 | 学校侧接入网络升级服务 | 1、投标人提供862所学校侧接入网络出口所需的路由器设备及服务；2、投标人提供780所学校侧接入网络出口所需的防火墙设备及服务；3、投标人提供862所学校侧升级所涉及的设备的割接及集成服务；4、投标人提供本次投入的学校侧相关设备的8年技术支撑服务。 | **●** |
| 4 | 网络运维服务 | 1、投标人提供浦东教育城域网线路割接优化、日常监测、运维管理等服务；2、投标人提供浦东教育城域网升级后的一体化运维平台（含软硬件）及服务；3、投标人提供浦东教育城域网数据中心及学校侧主要网络设备日志数据集中存贮、分析平台，保留 6 月数据所需的设备及服务；4、投标人提供教育城域网互联网出口上网行为管理、存储，保留6个月数据所需的设备及服务；5、投标人按需向招标人提供应急服务、重大活动保障服务；6、投标人提供不少于4名驻场运维服务人员，服务期为8年。 | **●** |
| 5 | 网络安全评估服务 | 投标人提供网络安全评估服务（一次性） | **●** |

**说明：上表中所列为本次招标的主要工作内容，其中备注标记“●”的内容为本项目的核心工作内容，投标人不得减少核心工作内容数量。**

**9.1.2 工作量清单明细**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **分类** | **服务内容** | **数量** | **单位** | **招标服务内容描述** |
| 1 | 数据中心升级服务 | 网络出口设备升级 | 2 | 套 | 1、提供网络出口设备升级所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供网络设备出口升级的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 出口防火墙升级 | 2 | 套 | 1、提供出口防火墙升级所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供出口防火墙升级的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 内网汇聚路由器升级 | 2 | 套 | 1、提供内网汇聚路由器升级所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供内网汇聚路由器升级的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 流控设备更新 | 2 | 套 | 1、提供流控设备更新所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供流控设备更新的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| SDN控制器服务 | 1 | 套 | 1、提供SDN控制器服务所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供SDN控制器服务的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| VPN接入服务 | 2 | 套 | 1、提供VPN接入服务所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供VPN接入服务的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| DNS服务 | 1 | 套 | 1、提供DNS服务所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供DNS服务的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 5G专网接入服务 | 8 | 年 | 1、提供5G专网接入服务需独享UPF，提供一路不低于1G带宽的5G专网接入服务；2、提供5G专网接入服务的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 数据中心割接集成服务 | 1 | 套 | 1、提供数据中心割接集成服务的整体方案设计、割接实施、风险、质量把控和集成等一整套服务；2、提供8年技术运维服务。 |
| 2 | 全网IPV6升级改造服务 | 大网和数据中心改造服务 | 1 | 套 | 1、提供大网和数据中心IPv6改造服务，包括教育城域网IPv6规划，数据中心的IPV6改造、实施；2、提供改造过程中与运营商、学校端的协调与对接服务3、提供8年技术运维服务。 |
| IPV6地址管理和审计系统 | 2 | 套 | 1、提供IPV6地址管理和审计系统服务和所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供IPV6地址管理和审计系统服务的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| IPV6/IPV4转换服务 | 2 | 套 | 1、提供IPV6/IPV4转换服务和所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容），为数据中心和学校所有应用提供转换支持；2、提供IPV6/IPV4转换服务的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 学校内网配置支持服务 | 862 | 套 | 1、提供学校端的IPv6规划、培训，以及改造过程中对学校端的技术支持服务；2、提供862个学校出口设备的IPv6配置服务；3、对学校原集成商、原设备厂商开展内网设备的IPv6改造提供支撑服务。 |
| 3 | 学校侧接入网络升级服务 | 万兆路由器 | 862 | 套 | 1、提供学校侧升级所需的万兆路由器设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供万兆路由器升级的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 万兆防火墙（A型） | 332 | 套 | 1、提供学校侧升级所需的万兆防火墙（A型）设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供万兆防火墙（A型）升级的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 万兆防火墙（B型） | 448 | 套 | 1、提供学校侧升级所需的万兆防火墙（B型）设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供万兆防火墙（B型）升级的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 学校割接服务 | 862 | 套 | 1. 提供862所学校的割接服务；
2. 提供整体的割接项目管理服务。
 |
| 4 | 网络运维服务 | 网络线路监控和调配 | 8 | 年 | 1、提供教育城域网线路割接、调整、日常监测、管理服务；2、提供8年技术运维服务。 |
| 数据中心设备和系统日常运维 | 8 | 年 | 1、提供教育城域网数据中心、学校端设备的统一监控和系统日常运维；2、提供8年技术运维服务。 |
| 一体化监控和运维服务 | 1 | 套 | 1、提供一体化监控和运维服务和所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供一体化监控和运维服务的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 网络日志审计分析服务 | 1 | 套 | 1、提供网络日志审计分析服务和所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供网络日志审计分析服务的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 上网行为审计服务 | 2 | 套 | 1、提供上网行为审计服务和所需的软硬件设备（设备选型要求：需满足“技术指标要求”的内容）；2、提供上网行为审计服务的安装、软硬件调测、业务割接和与原系统间对接等系统集成服务；3、提供8年维保和技术运维服务。 |
| 学校运维服务 | 862 | 套 | 1、提供学校侧教育城域网设备的日常运维服务；含8年内其他增加的学校接入侧运维服务；2、提供8年技术运维服务。 |
| 应急响应服务 | 8 | 年 | 1、提供应急响应服务、重大活动保障服务；2、按需提供应急响应、重大活动保障等服务所需的交通工具。 |
| 驻场服务 | 8 | 年 | 1、提供4名驻场服务工程师，其中不少于1名高级工程师、1名中级工程师和2名初级工程师。 |
| 5 | 网络安全评估服务 | 网络安全评估 | 1 | 次 | 1、第三方专业机构提供的教育城域网网络安全测评，并提供测评报告（一次性）。 |

**9.2具体技术质量需求**

**9.2.1建设进度要求**

建设进度要求参见“4.3.1整体项目进度安排”相关要求。

**9.2.2服务质量要求**

**9.2.3.1服务质量指标定义及测量方法**

**（1）基础运维指标定义**

①周期工作

计划型周期性地检查系统运行状态、日志文件、备份数据、输出结果文档。

②服务方式

通过驻场、现场和远程方式进行服务，通过统一每周7天\*24小时受理平台（线上线下协同）受理日常服务需求。

③响应时间

从故障受理到故障进入处理流程的计时要求。

④故障处理

按不同等级和时限要求进行故障处理。

⑤培训

乙方应向甲方提交《培训计划》，并按计划组织培训，培训对象为甲方及甲方最终用户，培训内容包括服务流程和服务资源使用方法等。

⑥文档留存与交付

对于服务中产生的过程性文档（周期性服务报告、运维报告、日志文档、重要数据等）给予归档和妥善保管。

⑦应急流程

面对突发如自然灾害、重特大事故、环境公害及人为破坏的应急管理、指挥、救援计划等紧急事件需按事先制定的应急流程和预案有条不紊地给予响应。

⑧通用服务交付时间

通用服务交付服务响应时间是指乙方接到甲方书面或邮件服务需求后到服务交付的时间。

**（2）个性化指标定义**

①服务可用性

正常服务运行时间除以该年总运行时间，即：

服务可用性=（365×24×60×60秒－应用失效时间之和（秒））/（365×24×60×60秒）。

②业务敏捷上线

网络侧业务快速下发。

③IPV6/IPV4全域服务

浦东教育局资产全域IPV6/IPV4双栈规划和服务开启。

**（3）指标要求和测量方法**

**①周期工作**

按不同报表分不同服务周期，日/月/季/年/按需，五种周期提供过程性文档。

| **序号** | **指标名称** | **测量方法** |
| --- | --- | --- |
| 1 | 周期工作 | 过程性文档按时序要求检查 |

**②服务方式**

提供驻场、现场、远程、线上四种服务方式。

| **序号** | **指标名称** | **测量方法** |
| --- | --- | --- |
| 1 | 服务方式 | 按平台设置和服务模式达标要求检查 |

**③响应时间和故障处理**

| **时间类型** | **故障级别** | **时长** |
| --- | --- | --- |
| 故障响应时间 | 故障响应时间 | 30分钟 |
| 故障修复时间 | 严重故障 | 2小时 |
| 重要故障 | 4小时 |
| 一般故障 | 24小时 |
| 光缆故障 | 24小时 |

故障级别划分：

a、严重故障：浦东教育城域网运行服务大范围中断，城域网无法正常运行，或具有同等危害的事件，且没有临时替代解决方案；

b、重要故障：浦东教育城域网运行个别重要区域中断，无法正常运行，或具有同等危害的事件；

c、一般故障：故障对系统业务无明显影响，仅造成小范围的故障、或使用不便、操作不畅等。

**④培训**

对于甲方工作人员按计划按时间按频次开展系统使用培训服务，并考核结果。

| **序号** | **指标名称** | **测量方法** |
| --- | --- | --- |
| 1 | 培训 | 每年2次培训服务 |

**⑤文档留存与交付**

| **序号** | **指标名称** | **测量方法** |
| --- | --- | --- |
| 1 | 文档留存与交付 | 日常运维过程性文档保存2年；日志文档保存6个月；重要备份数据存期按各系统要求测定（一般不少于6个月） |

**⑥应急流程**

| **序号** | **指标名称** | **测量方法** |
| --- | --- | --- |
| 1 | 应急流程 | 按应急预案进行应急演练，每年不少于1次 |

**⑦通用服务交付时间**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标名称** | **测量方法** |
| 1 | 通用服务交付时间 | 交付时间-提交时间≤10工作日 |

**⑧服务可用性**

| **序号** | **指标名称** | **测量方法** |
| --- | --- | --- |
| 1 | 服务可用性 | 须保证教育城域网核心网络可用性不低于99.9%。即全年失效时间之和不超过365×24×60×0.001=525.6分钟。 |

**9.2.3服务期质量考核要求**

服务期质量考核内容包括基础运维指标和个性化运维指标两个大类，基础型指标包括（周期工作、服务方式、响应时间、故障处理、使用培训、文档留存与交付、应急流程），个性化指标包括（服务可用性）。

9.2.3.1服务考核管理办法

| **序号** | **指标名称** | **测量方法** | **分值(100分制)** | **考核办法** |
| --- | --- | --- | --- | --- |
| 1 | 周期工作 | 过程性文档按时序要求检查 | 20 | 按日/月/季/年/按需五种服务周期考核，每项不合格扣0.5分 |
| 2 | 服务方式 | 按平台设置和服务模式达标要求检查 | 15 | 按统一受理平台/驻场/现场/远程/线上五种服务方式考核，每项不合格扣0.5分 |
| 3 | 响应时间和故障处理 | 按承诺时限检查 | 15 | 按响应时限和四分类故障时限要求考核，每项不合格扣0.5分 |
| 4 | 培训 | 每年2次培训服务（可现场和远程方式） | 10 | 每少1次，扣3分 |
| 5 | 文档留存与交付 | 日常运维过程性文档保存2年；日志文档保存6个月；重要备份数据存期按各系统要求测定（一般不少于6个月） | 15 | 按测量方法项考核，每项不合格扣0.5分 |
| 6 | 应急演练 | 按应急预案进行应急演练，每年不少于1次 | 5 | 每年少于1次扣3分 |
| 7 | 通用服务交付 | 交付时间-提交时间≤10工作日 | 10 | 每大于10个工作日，扣0.5分/次 |
| 8 | 服务可用性 | 须保证教育城域网核心网络可用性不低于99.9%。即全年失效时间之和不超过365×24×60×0.001=525.6分钟。 | 10 | 每月统计，低于99.9%扣0.5分 |

注：100分制考核办法，每年最终得分≥90分为优秀，≥80分为良好，≥70分为一般。

9.2.3.2补偿或赔偿

中标人在上述服务未达到要求时，中标人应在30天内整改，并做出说明，如果中标人在服务周期内（1年为一个周期）重复发生关键事件3次及以上状况，采购人有权根据合同条款提出赔偿诉求。

**10** **技术指标要求**

**10.1设备清单汇总表**

| **序号** | **名  称** | **具体技术参数** | **数量** | **单位** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 1 | 数据中心网络出口设备 | 详见设备技术参数要求 | 2 | 套 |  |
| 2 | 数据中心出口防火墙 | 详见设备技术参数要求 | 2 | 套 |  |
| 3 | 数据中心内网汇聚路由器 | 详见设备技术参数要求 | 2 | 套 |  |
| 4 | 数据中心流控设备 | 详见设备技术参数要求 | 2 | 套 |  |
| 5 | 数据中心上网行为审计设备 | 详见设备技术参数要求 | 2 | 套 |  |
| 6 | 数据中心SDN控制器 | 详见设备技术参数要求 | 1 | 套 |  |
| 7 | 数据中心VPN接入设备 | 详见设备技术参数要求 | 2 | 套 |  |
| 8 | 数据中心DNS | 详见设备技术参数要求 | 1 | 套 |  |
| 9 | IPV6地址管理和审计系统 | 详见设备技术参数要求 | 2 | 套 |  |
| 10 | IPV6/IPV4转换设备 | 详见设备技术参数要求 | 2 | 套 |  |
| 11 | 学校侧万兆路由器 | 详见设备技术参数要求 | 862 | 套 |  |
| 12 | 学校侧万兆防火墙（A型） | 详见设备技术参数要求 | 332 | 套 |  |
| 13 | 学校侧万兆防火墙（B型） | 详见设备技术参数要求 | 448 | 套 |  |
| 14 | 一体化监控和运维系统 | 详见设备技术参数要求 | 1 | 套 |  |
| 15 | 网络安全日志审计系统 | 详见设备技术参数要求 | 1 | 套 |  |
| 16 | 综合布线材料及光模块 | 详见设备技术参数要求 | 若干 | 套 |  |

**注：投标人不得缩减设备数量。**

**10.2设备技术参数要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **名  称** | **技术参数要求** |
| 1 | 数据中心网络出口设备 | 1、交换容量≥2.56Tbps/40.96Tbps、包转发率≥1080Mpps、整机最大路由地址表≥128K；2、设备端口：10G光接口≥48个，100G光接口≥6个；设备配置双电源、双风扇冗余；3、支持横向/纵向虚拟化，支持本地和远程堆叠，支持分布式设备管理，分布式链路聚合，分布式弹性路由，支持跨设备链路聚合M-LAG；4、支持RIP、OSPF、BGP、ISIS等IPv4动态路由协议，支持RIPng、OSPFv3、BGP4+、ISISv6等IPv6动态路由协议，支持等价路由、策略路由；5、支持MPLS、MCE，支持MPLS VPN、MPLS TE；6、支持IPv6 ND（Neighbor Discovery）、支持IPv6 VxLAN over IPv4、支持PMTU发现（Path MTU Discovery）、支持ICMPv6、Telnetv6、SFTPv6、SNMPv6、BFDv6、VRRPv3；7、支持Telemetry可视化功能、支持缓存微突发检测、支持SNMP v1/v2c/v3、支持Netconf和Python、支持分级告警、支持Jumbo Frame；8、含8年产品维保服务。 |
| 2 | 数据中心出口防火墙 | 1、采用控制、数据、业务相分离的全分布式架构，主控引擎、业务引擎、交换引擎、接口单元均硬件槽位分离，所有交换引擎必须为独立形态（非主控集成），占用专用的硬件槽位，实配独立交换引擎N+1冗余，N≥3；2、配置双主控、双电源冗余，配置100G（可切换为40G）光接口≥6个，10G光接口≥48个；配置入侵防御、防病毒、应用识别功能模块授权；3、性能要求：吞吐量≥600Gbps，并发连接数≥2.4亿，新建连接数≥60W/S；4、支持同时具备防火墙、链路负载均衡、入侵防御、防病毒、应用识别和web应用防护等功能；5、支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项（提供功能截图）；6、支持IPV6动态路由协议、IPV6对象及策略、IPV6状态防火墙、IPV6攻击防范、IPV6 GRE/IPSEC VPN、IPV6日志审计、IPV6会话热备等功能；7、支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置；8、含8年产品维保服务及入侵防御、防病毒、应用识别特征库升级服务。 |
| 3 | 数据中心内网汇聚路由器  | 1、采用分布式的硬件转发和无阻塞交换技术；支持双主控、独立交换网板，交换网板；支持业务载板插槽≥8个；2、支持交换容量≥150Tbps，支持包转发率≥24000Mpps，单槽位线速转发不丢包；3、配置双主控、双电源冗余，交换网板≥4；配置100G（可切换40G）光接口≥6个，10G光接口≥8个；配置SRv6功能永久授权；4、IPv4路由表容量≥20M 、IPv6路由表容量≥10M；IPv4转发表容量（FIB）≥3M、IPv6转发表容量（FIB）≥2M；5、支持SRv6 Policy双向隧道来回路径一致；支持SRv6 OAM，支持SRv6 TE policy的ping/tracert功能，以实现设备基本运维能力；6、支持SRv6 Policy多SID-LIST负载分担功能，支持随业务流的检测技术；7、支持全面的快速重路由FRR功能：IP/IPv6/LDP/TE/VPN/VPNv6 FRR，倒换时间均≤50ms，支持LDP, VRRP, OSPF, ISIS, BGP, VRRP6, OSPFv3, ISIS6, BGP4+,MPLS L3VPN, MPLS TE,PIM SM的NSR（不中断路由技术），主备倒换不丢包；8、支持并承诺免费与本项目SDN控制器平台的对接和管理，包括但不限于所需的定制对接开发；9、含8年产品维保服务。 |
| 4 | 数据中心流控设备 | 1、单台硬件支持灵活接口板配置，至少支持1GE、10GE、40GE和100GE接口的灵活配置，配置双电源双风扇，两个电源可以实现负载均衡；2、接口配置：SFP+接口≥8个，100GE(自适应40G)接口≥4个，管理口≥2个，管理口支持主备互为备份；3、单台设备吞吐能力≥100Gbps，可以实现100Gbps的流量线速管理，并发数据流≥72,000,000，并发策略数≥48,000,000，并发用户账号管理≥4,500,000，（提供官网截图证明）；4、设备支持内置或外置无源bypass硬件，设备故障、维护、升级的情况下，实现＜3毫秒的切换时间；当流量满吞吐情况下设备可以实现全线速转发和监控，流控设备控制策略加载后所增加的延时＜1毫秒；5、设备至少支持三级策略管理，要求实现三级嵌套流量控制，可以利用三级策略进行流量区分并同时对三级策略进行执行QOS控制策略；6、设备需支持基于时间段的策略配置。基于不同的时间段，可对某一用户（或用户组）和应用（应用组）的组合实现不同的流量优化策略；7、支持基于每IP的不同应用的新建和并发连接数控制和QoS管理；对不能识别的流量也能进行控制；8、至少支持4个优先级和3个丢弃等级实现不同等级应用的分类转发，可以对关键应用实施入、出的最小带宽保证，对消耗带宽应用实施入、出的最大带宽限制，控制精确到1K；9、能够通过模板配置技术实现批量配置，可以一次配置千条以上的规则，支持用户自定义L4-L7层特征库，支持对HTTP协议的host、URL、Method、Referer User-Agent、Content-Encoding、Length、Content-Type、Location一个或多个参数进行自定义特征库策略；10、硬件支持IPV4和IPV6的识别和控制，要求对IPV6的流量控制与识别与IPV4相同；11、支持全局交叉QOS策略模式，即可以支持至少两个独立交叉的策略表同时执行QOS控制策略，每个策略表至少支持两级细分，支持在对每用户总带宽，每个协议带宽控制的基础之上实现全局的用户组，协议组带宽控制；12、含8年产品维保服务及各类特征库升级服务。 |
| 5 | 数据中心上网行为审计设备 | 1、内存≥128GB，硬盘≥1.92TB SSD，双冗余电源；千兆电口≥4，万兆光口SFP+≥8，40G光口≥2；2、网络层吞吐量≥80G，应用层吞吐量≥60Gb，支持用户数：≥200000，包转发率：≥7.2Mpps，每秒新建连接数：≥300000，最大并发连接数：≥20000000；3、对网络接入的终端进行可视化管理，展示终端详细信息、合规状态等，支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；4、审计SSL网页时，支持加密证书自动分发功能（提供产品界面截图）；5、支持网盘/笔记类应用访问内容和外发文件审计；支持SSH/RDP协议，可对连接开始时间，连接结束时间，传输的流量大小进行审计；支持Teamviewer、向日葵、Anydesk、RDP的远程应用的外发文件审计；6、日志中心可以对上网日志进行大数据分析，并支持多个大数据分析模型，包括全网上网态势分析、办公网上网态势分析、带宽分析、专线质量分析、未关机检测分析、图书馆资源优化；7、配置提供上网行为审计设备配套的审计日志查询、存储软硬件系统，存储可用容量≥120TB（三副本，IOPS≥10万）；8、支持日志数据导出功能和支持通过API接口调用日志数据及分析结果；9、含8年产品维保服务及相关的特征库升级服务。 |
| 6 | 数据中心SDN控制器 | 1、SDN控制器应该支持统一的Portal来访问所有的SDN组件，包括设备管理，业务发放，网络优化，网络监控，支持端到端的网络资源纳管；2、能够同时管理RSVP-TE LSP和SR-TE LSP、SRv6 Policy；控制器需要满足链路利用率阀值可设置两级门限的功能，当全网流量低负载时，通过第一级门限达到全网流量保证，拥塞避免。而当全网流量增长达到高负载时，通过二级门限提高正网络带宽利用率；3、支持带宽、时延、丢包率组合调优，支持应用主备路径、路径自动逃生，SRv6 Policy组提前规划能力，在SRv6 Policy未下发前，提前在控制器软件上根据现网组网和配置规划整网的SRv6 Policy路径及参数，然后统一下发；4、SRv6 Policy满足软锁定功能，链路故障或者带宽越限调优恢复，触发实际路径恢复到软锁定路径上；5、SRv6 Policy/SR-TE可支持基于分片维度的算路，例如：Cost值、动态时延、显示路径、最大剩余带宽等；支持L3 VPN/L3 EVPN + SRv6 Policy、L3 VPN/L3 EVPN + 五元组业务随流丢包检测；6、提供教育城域网SDN控制器上述功能所需的软硬件系统及各类授权（包括但不限于IP网元管理、网络控制、网络分析、业务自动化功能，网络切片功能，网络路径优化功能，VPN业务保障功能，管理基础北向接口）；7、支持并承诺免费与本项目路由器设备的对接和管理，包括但不限于所需的定制对接开发；8、含8年产品维保服务。 |
| 7 | 数据中心VPN接入设备 | 1、硬件规格：内存≥8GB，硬盘容量≥MSATA 64G SSD，冗余电源，兆电口≥6；千兆光口SFP≥4，万兆光口SFP+≥2；2、最大加密流量≥950 Mbps，最大并发用户数≥16000，IPSec最大流量≥500 Mbps，设备最大吞吐量≥4Gbps，最大并发会话数≥350万；3、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；4、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；5、产品应提供HTTPS驱动病毒查杀工具，支持对Windows环境下的针对HTTPS拦截监听的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用SSL VPN；6、支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统；7、支持结合口袋助理等移动APP，实现动态口令认证，增加认证的多样性；8、支持HTP快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议；9、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）；10、含8年产品维保服务。 |
| 8 | 数据中心DNS | 1、接口≥8个10/100/1000M电口，可扩展2个万兆光口或4个千兆光口；硬盘≥1T以上冗余硬盘，支持raid 0，1；电源≥2；2、QPS指标≥10万QPS，支持HA或负载均衡部署；3、支持标准DNS协议：支持标准DNS协议RFC1034、1035，支持扩展DNS协议RFC2672、2782、3596；记录类型支持A、AAAA、PTR、CNAME、MX、NS、TXT、SOA等类型；4、支持智能出口流量调度技术，实现多出口链路的充分合理利用和快速的自动容灾切换；支持线路检测机制，实现某一线路资源瘫痪时，基于自定义策略，实线路资源的自动切换；5、内置域名库包括但不限于游戏网站、视频动漫、购物网站、下载网站、新闻媒体、网银、国际域名和教育城域网资源等，同时域名库可进行主动编辑和更新升级。可支持100万自定义域名库（如有请提供第三方权威机构出具的专业测试报告）；6、域名请求转发，支持First/RTT、First/Order、Only/RTT、Only/Order和No的转发方式，支持对Forward服务器配置权重。支持对Forward服务器进行健康检查；7、权威解析，支持查询zone配置得到域名的权威解析结果，支持zone配置的动态加载；可以根据父域进行分类层级展示或平铺展示，视图、区、记录支持以树形目录检索，以方便查看有实际含义的记录；8、支持为权威记录等资源列表动态添加多个自定义属性列，方便用户为域名记录灵活添加备注信息；9、支持14种健康监测方式ICMP、UDP、TCP\_SYN、TCP、HTTP、HTTPS、FTP、SMTP、SNMP、TCP\_KEEP、SNMP\_LINK、DNS等；支持会话保持技术，对于一定周期内同一用户相同的域名解析请求，实现解析结果的固定，避免出现频繁的跳动现象，从而实现流量的稳定牵引；10、能够内置防DDOS攻击模块，保护权威DNS和递归DNS的安全，支持防御DNS SERVFAIL攻击，客户端通过发起大量错误域名攻击触发递归无响应从而导致服务器性能拥塞，该设备能够自主识别该类攻击特征，进行攻击防护；11、全局源IP限速、特定源IP限速、限制其DNS查询速率，超过速率的部分丢弃；全局域名限速、精确域名限速、泛域名限速，限制其DNS查询速率，超过速率的部分丢弃；12、支持精确域名封堵、泛域名封堵，允许指定的IP范围内的终端访问DNS服务；13、支持内置威胁情报资源库，对内部受控或恶意终端通过DNS访问非法站点有效阻断，阻断威胁对外连接建立，提升递归访问的安全性；14、威胁情报中心平台可支持资产管理，可自定义属性字段，可关联数据监控拦截信息，生成台账实名管理；支持全球情报资讯查询，可按时间搜索，包括资讯标题、发布时间、资讯描述、参考链接；15、支持对全网发现的所有威胁事件统计，威胁事件分类包括但不限于：传统的僵尸网络病毒、后门木马、蠕虫病毒、检测DDoS木马等，利用高危漏洞样本的攻击、勒索软件等；威胁事件统计包括不限于发现时间，包含域名，严重级别等；16、提供威胁解析识别+阻断的完整威胁防御链，能够将威胁访问在内网进行处置，保障内部网络环境的安全；17、提供多维度的统计报表，包含但不限于：威胁类型TOP、拦截检测趋势、威胁域名TOP、失陷主机TOP、最新检出时间，帮助客户进一步定位内网产生的威胁解析请求的详细信息，如：产生时间、处置结果、关联的终端IP、样本背后隐藏的威胁事件等；18、含8年产品维保服务，含在网两台DNS设备8年维保服务。 |
| 9 | IPV6地址管理和审计系统 | 1、支持内置防DDOS攻击模块，保护权威DNS和递归DNS的安全；支持防御DNS SERVFAIL攻击，客户端通过发起大量错误域名攻击触发递归无响应从而导致服务器性能拥塞，该设备能够自主识别该类攻击特征，进行攻击防护；2、支持全局源IP限速、特定源IP限速、限制其DNS查询速率，超过速率的部分丢弃；全局域名限速、精确域名限速、泛域名限速，限制其DNS查询速率，超过速率的部分丢弃；3、支持精确域名封堵、泛域名封堵；支持云端威胁情报中心，实时分析威胁情报数据，可提供账号进行管理，威胁情报可供DNS设备下载，可扩展更新威胁情报资源库，对内部受控或恶意终端通过DNS访问非法站点有效阻断，阻断威胁对外连接建立，提升递归访问的安全性；4、恶意域名库平台支持下发API接口提供全功能的基于web service的编程接口；对接第三方恶意域名库，支持多源恶意域名库更新可向第三方恶意域名库的源拉取数据以及接收第三方恶意域名推送；5、支持威胁情报中心平台支持自动报告管理，可自定义起始终止时间，按周报，月报发送指定邮箱；支持对全网发现的所有威胁事件统计，威胁事件分类包括但不限于：传统的僵尸网络病毒、后门木马、蠕虫病毒、检测DDoS木马等，利用高危漏洞样本的攻击、勒索软件等；威胁事件统计包括不限于发现时间，包含域名，严重级别等；6、支持全球情报资讯查询，可按时间搜索，包括资讯标题、发布时间、资讯描述、参考链接；（提供功能截图）7、支持对全网发现的所有失陷主机统计，以及失陷主机关联威胁类型，发现时间统计；支持访问的情报域名TOP统计、以及每个域名关联的源IP TOP，情报上下文信息，情报信息包括威胁类型，严重级别，防护策略等；8、告警支持设置各种阀值、事件告警，支持邮件告警、回调告警、SNMP告警、syslog告警、短信告警及声音告警。告警记录内容包括但不限于告警时间，节点名称及IP、告警事件原因；9、系统支持IPV4及IPV6数据中心调度策略，AAAA记录控制：支持AAAA应答控制，在解析结果同时存在A与AAAA记录时，针对部分AAAA记录进行过滤，支持A、AAAA记录同PTR的操作联动；10、含8年产品维保服务。 |
| 10 | IPV6/IPV4转换设备 | 1、采用控制、数据、业务相分离的全分布式架构，主控引擎、业务引擎、交换引擎、接口单元均硬件槽位分离，所有交换引擎必须为独立形态（非主控集成），占用专用的硬件槽位，实配独立交换引擎N+1冗余，N≥3；2、配置双主控、双电源冗余，配置100G（可切换为40G）光接口≥6个，10G光接口≥48个；配置入侵防御、防病毒、应用识别功能模块授权；3、性能要求：吞吐量≥600Gbps，并发连接数≥2.4亿，新建连接数≥60W/S；4、支持同时具备防火墙、链路负载均衡、入侵防御、防病毒、应用识别和web应用防护等功能；5、支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项（提供功能截图）；6、支持IPV6动态路由协议、IPV6对象及策略、IPV6状态防火墙、IPV6攻击防范、IPV6 GRE/IPSEC VPN、IPV6日志审计、IPV6会话热备等功能；7、支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置；8、含8年产品维保服务及入侵防御、防病毒、应用识别特征库升级服务。 |
| 11 | 学校侧万兆路由器 | 1、交换容量≥262Gbps，包转发率≥60Mpps；固定口 ≥6\*10G光，≥16\*GE电，配置冗余交流电源；配置SRv6永久授权；2、支持SR，控制流量按照预先设置的网络节点逐跳转发，支持IPv6-IPv6报文前缀转换，支持IPv6 NetStream；3、MTR多拓扑路由，支持在一个物理网络上实现多个逻辑拓扑，指定不同业务流量走不同的逻辑拓扑路由转发；4、支持OSPFv3 for SRv6、ISIS for SRv6 、SRv6 Policy、EVPN L3VPN over SRv6、EVPN L2VPN over SRv6（VPWS）、EVPN L2VPN over SRv6（VPLS）；5、支持EBFD for SRv6、ESRv6 TI-LFA，ESRv6 Ping、Tracert， SRv6 policy DSCP引流、支持ESRv6 policy Color引流、G-SRv6头压缩，Telemetry功能；6、支持随流检测技术，子接口切片技术；支持对HTTP/FTP等TCP业务流量进行优化传输技术，提高教育城域网带宽利用率；7、支持并承诺免费与本项目SDN控制器平台的对接和管理，包括但不限于所需的定制对接开发；8、含8年产品维保服务。 |
| 12 | 学校侧万兆防火墙（A型）  | 1、采用自主知识产权的专用安全操作系统，内存大小≥16G，硬盘容量≥256G SSD，千兆电口≥16，万兆光口SFP+≥6，电源冗余电源；2、网络层吞吐量≥30G，应用层吞吐量≥20G，防病毒吞吐量≥3.5G，IPS吞吐量≥2.5G，全威胁吞吐量≥1.8G，并发连接数≥410万，HTTP新建连接数≥18万；3、产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略；4、支持内置不低于1万种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则；支持僵尸主机检测功能，可识别主机的异常外联行为。5、支持静态路由、策略路由等常见路由类型，支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等；6、支持全面NAT功能，对多种应用层协议支持ALG功能，包括DNS、FTP、H323、MSN、Netbios、PPTP、RSH、RSTP、SIP、SQLnet等；7、支持对SYN、UDP、ICMP、DNS、ACK等进行DDOS防护；8、含8年产品维保服务及入侵防御、防病毒、应用识别特征库升级服务。 |
| 13 | 学校侧万兆防火墙（B型） | 1、产品采用自主知识产权的专用安全操作系统，千兆电口≥6，千兆SFP接口≥10，万兆SFP+接口≥2，配置双冗余电源；2、网络层吞吐量≥10Gbps，应用层吞吐量≥6Gbps，并发连接数≥220万，HTTP新建连接速率≥6万；3、产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略；4、支持内置不低于1万种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则；支持僵尸主机检测功能，可识别主机的异常外联行为。5、支持静态路由、策略路由等常见路由类型，支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等；6、支持全面NAT功能，对多种应用层协议支持ALG功能，包括DNS、FTP、H323、MSN、Netbios、PPTP、RSH、RSTP、SIP、SQLnet等；7、支持对SYN、UDP、ICMP、DNS、ACK等进行DDOS防护；8、含8年产品维保服务及入侵防御特征库升级服务。 |
| 14 | 一体化监控和运维系统 | 1. 软件要求具备高可靠性、高容错力，在规范书中应详细列出所提供的软件清单和说明；投标人应支持免费更新软件版本；2、系统的存储设计需要满足超3000台网络设备(核心、汇聚、接入等)链路状态、节点流量、专项应用、故障告警等多个指标的监控；3、统一身份认证要求，需面向教育管理方、学校方、运维服务团队，通过对接现有的统一身份认证系统，提供统一登录服务，同时支持分权分域管理，支持不同的用户实现不同的权限功能、操作、可视内容；4、统一云网门户要求，平台需实现云网一体化统一应用门户，用户单点登录之后，可实现云网一体化资产视图展现、云网拓扑视图、运行状态查看、性能分析图形展示、告警统一视图、远程诊断、告警事件流程、工单流转、服务请求、大屏展示、云网一体化运行报告查看功能操作；5、网络运行监控要求，需要为浦东教育专网管理及正常运行提供有力的技术支撑和流程保障，并实现与云管平台的互通和信息共享。需要通过对浦东教育专网全网的设备状态、配置信息、网络接口流量、网络流量分析和告警数据等信息的实时采集和监控，实时掌握整个教育专网的运行情况，及时发现故障与异常，迅速定位，尽快解决、及时调整运行策略，提高系统运行效率；6、网络安全监测要求，以网络安全事件为核心，通过与安全态势感知系统对接，对教育专网网络和安全设备日志、系统运行数据、网络流量等信息的实时采集，以大数据关联分析等方式，实现对教育专网上未知风险的识别、威胁发现、安全事件实时报警及可视化展现；7、业务连续性分析要求，实现对浦东教育云中的核心应用进行监控管理及正常运行提供有力的技术支撑和流程保障。业务连续性分析需展示应用拓扑，直观展示应用关联关系（包括数据库、中间件、应用），应用所关联的云网资源，需要能够对应用本身进行拨测，主动探测应用在线状况及健康度，需要对应用所关联的资源进行监控采集，在云应用视图上统一展现，提高运行维护效率；8、云网一体化系统管理要求，云网一体化系统管理，实现平台基础管理功能，主要包含系统用户管理、系统安全管理、系统运维管理、日志管理、分权分域，以及基于CMDB的数据模型实现云网统一资源纳管，为上述网络运行监控、网络安全监测、云运行监控、业务联系性分析各子系统提供基础资源及配置数据；9、云网一体化可视化呈现要求，现需在云网日常运维的基础上，将浦东教育云网整体网络根据三层网络结构按照核心—汇聚—接入分为三个层级场景进行可视化展示，在此基础上基于浦东区的地图，根据各机房节点的实际地理位置构建模型进行标注，以实际各机房节点间的链接关系构建链路，组成基于地理位置信息的城域网总体运行、分析、感知、运营可视化展示大屏；10、配置提供一体化监控和运维系统上述功能所需的软硬件系统及各类授权；

11、根据采购人要求在指定场所，提供一套展示浦东教育云网一体化的LED高清大屏显示设备，尺寸不少于12平方米；12、含8年产品维保服务。 |
| 15 | 网络安全日志审计系统 | 1、提供的日志管理平台采用大数据技术，软件、日志解析、日志处理、关联分析、数据存储等均支持分布式；支持集群模式部署，随着日志量增加，支持原先集群基础上进行节点的横向扩展，不影响日志管理平台的正常业务运行；2、日志管理平台需满足业务和数据的高可用性，保障平台的稳定新和可靠性；3、支持Syslog、SNMP Trap、HTTP、JDBC、WMI、FTP、SFTP协议日志收集；支持使用代理(Agent)方式提取日志并收集；4、支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等；5、支持对收集的设备类型日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展；6、三维关联分析，支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件；7、支持在目标主机上安装Agent程序，支持监测目标主机的相关信息；8、支持无限资产授权，日志处理能力不低于20万EPS，检索百亿条日志查询，响应时间小于1秒；后端配套存储容量≥1440TB；9、支持数据存储的高压缩比，并且支持节点的动态扩容和缩容，扩容过程中管理平台业务不中断；10、日志管理平台支持多租户，各租户的数据和权限需满足数据隔离、权限隔离；11、提供日志解析性能监控：解析规则的好坏直接会影响入库速度，在编写解析规则时候平台能显示每一步解析的递归次数和解析耗时，方便运维人员判断解析规则的运行效率；在执行解析入库时，平台会记录每一条规则的解析结果和平均耗时，作为后续规则优化依据；12、支持各个节点数据的性能监控，支持热点数据的分布式限流，限流模式支持EPS、线程数、直接、关联、链路、快速失败和排队等待；13、含8年产品维保服务。 |
| 16 | 综合布线材料及光模块 | 1、100G 10KM模块：24个；2、100G 多模模块：64个；3、40G多模模块：8个；3、10G 10KM模块：742个；4、10G 40KM光模块：1086个；5、10G多模模块：3656个；6、综合布线各类耗材：若干；7、含8年产品维保服务。 |

10.3系统对接要求

浦东教育城域网升级服务项目需要与原有浦东教育城域网的各个业务单元进行对接，包括原骨干网、数据中心、学校侧接入等，以确保浦东教育城域网在升级改造过程中新老网络系统各业务单元切换平滑、对业务的影响面最小，具体系统对接要求参见“9.1.2 工作量清单明细”相关要求。

**11质量标准和验收方案**

11.1质量标准

11.1.1 中标人所交付的信息系统应满足本项目合同文件明确的功能性、使用性要求。信息系统的质量标准按照国家标准和招标需求确定，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招标目的的特定标准确定。

11.1.2 中标人所交付的信息系统还应符合国家和上海市有关系统运行安全之规定。

11.2系统测试及验收方案

11.2.1 采购人应依据信息系统项目工程的条件和性质，按照招标文件明确的要求向中标人提供信息系统的施工、安装和集成环境。如采购人未能在该时间内提供该施工和安装环境，中标人可相应顺延交付日期。如对中标人造成经济损失，采购人还应依本合同规定承担违约责任。

11.2.2中标人应负责系统及系统设备在实施现场就位安装和调试、操作培训等的全部工作，按照合同文件工作与管理要求负责对项目进度的安排、现场的安全文明施工统一管理和协调，严格遵守国家、本市安全生产有关管理规定，严格按安全标准组织项目实施，采取必要的安全防护措施，消除安全事故隐患。由于中标人管理与安全措施不力造成事故的责任和因此发生的费用，由中标人承担。

11.2.3中标人应在进行系统交付前5个工作日内，以书面方式通知采购人并向采购人提供完整的竣工资料、竣工验收报告及竣工图。采购人应当在接到通知与资料的5个工作日内安排交付验收。中标人在交付前应当根据合同文件中的检测标准对本项目进行功能和运行检测，以确认本项目初步达到符合本合同交付的规定。

11.2.4中标人应按照合同及其附件所约定的内容进行交付，如果约定采购人可以使用或拥有某软件源代码的，中标人应同时交付软件的源代码并不做任何的权利保留。所交付的文档与文件应当是可供人阅读的书面和电子文档。

11.2.5采购人在本项目交付后，应当在5个工作日内向中标人出具书面文件，以确认其初步达到符合本合同所约定的任务、需求和功能。如有缺陷，应向中标人陈述需要改进的缺陷。中标人应立即改进此项缺陷，并再次进行检测和评估。期间中标人需承担由自身原因造成修改的费用。

11.2.6如果由于中标人原因，导致系统在试运行期间出现故障或问题，中标人应及时排除该故障或问题。以上行为产生的费用均由中标人承担。

11.2.7如果由于采购人原因，导致系统在试运行期间出现故障或问题，中标人应及时配合排除该方面的故障或问题。以上行为产生的相关费用均由采购人承担。

11.2.8系统试运行完成后，采购人应及时进行系统验收。中标人应当以书面形式向采购人递交验收通知书，采购人在收到验收通知书后的5个工作日内，确定具体日期，由双方按照本合同的规定完成系统验收。采购人有权委托第三方检测机构进行验收，对此中标人应当配合。

11.2.9如果属于中标人原因致使系统未能通过验收，中标人应当排除故障，并自行承担相关费用，同时延长试运行期10个工作日，直至系统完全符合验收标准。

11.2.10如果属于采购人原因致使系统未能通过验收，采购人应在合理时间内排除故障，再次进行验收。

11.2.11采购人根据信息系统的技术规格要求和质量标准，对信息系统验收合格，签署验收意见。

**12人员及设备配备要求**

为使服务按质、按量、按时及有序推进，投标人对本项目必须具备完善和稳定的管理组织机构。投标人需按照服务内容所需的岗位，组建服务团队，指派具备服务支撑经验的人员担任服务负责人和相关专业技术人员，具备良好的沟通协作能力和专业技能，能与用户及合作伙伴进行良好的沟通。

根据项目质量和进度的需要，投标人应及时组织相应的项目管理人员和技术部署人员。投标人必须无条件接受采购人任何形式的合理监督检查，并承担因人员不足、不到位所导致影响项目质量、进度的违约责任。

投标人在项目部署过程中出现资源、进度、质量协调控制不力的情况，采购人有权要求更换相关项目人员，投标人必须予以配合，并确保不影响项目建设的进度和质量。

项目服务团队的岗位及人数要求如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **岗位名称** | **负责事项** | **数量要求** | **技能要求** |
| 1 | 项目经理 | 项目整体负责 | 1 | 高级工程师，如有PMP项目管理证书请提供 |
| 2 | 技术负责人 | 整体技术方案负责 | 1 | 高级工程师，如有云计算架构师、PMP/PRINCE2、CDCP认证专业证书请提供 |
| 3 | 项目实施团队 | 技术支持（网络、安全、云平台）、项目集成实施团队 | 22 | 具备中级工程师及以上证书不少于10人，具备PMP、网络、云平台、安全专业资格证书之一不少于12人 |
| 4 | 运维经理 | 项目整体运维负责 | 1 | 具备高级工程师及以上证书，如有CCNP、HCIP或同等及以上专业认证资格证书请提供 |
| 5 | 项目运维团队 | 驻场人员4人（数据中心服务2人、学校服务2人）外线运维人员24人（8个片区，每片区3人，含割接、运维服务） | 28 | 具备中级工程师及以上证书不少于5人，具备网络、云平台、安全专业资格证书之一不少于10人 |
|  | 合计 |  | 53 |  |

12.2其他要求

（1）投标人应保证在项目过程中，项目经理或指定联络人全程现场办公；

（2）投标人应保证项目组成员稳定，减少核心人员流失，项目经理或指定联络人在项目实施期间不得退出或更换，若因特殊原因需调整，需经采购人同意。

（3）提供完整的项目人员配置成员名单与项目各实施阶段进行对应，并提供团队成员从事相关工作年限、学历、职称、职业资格、在职证明等信息。

**13安全生产、文明施工（安装）与环境保护要求**

13.1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。

13.2在项目实施期间为确保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。

13.3中标人现场服务负责人应具有专业证书，其它人员必须持证上岗。中标人应对服务期间自身人员和第三方人员安全与财产负责。

**14售后服务要求（包括延伸服务要求）**

**14.1 具体服务承诺**

中标人需提供全部采购内容的运维服务，按照服务质量保证的服务标准提供各种售后服务。在中标人服务期内，负责本项目的维护工作，确保系统安全、稳定、正常地运行并对由于设计、功能的缺陷而产生的故障负责。中标人提供面向教育局和相关学校的每周7天×24小时的运维服务保障。在此期间如发生系统运作故障，或出现瑕疵，中标人将按照售后服务的承诺提供保修和维护服务。中标人提供运维热线电话、电子邮件和在线网站等技术支持方式：

（1）电话支持：客户通过拨打中标人指定的运维热线电话，提供每周7天×24小时电话响应服务。由中标人工程师进行电话支持。

（2）远程技术支持：在采购人保证服务器网络联通的情况下，通过远程诊断、电话支持、电子邮件等方式进行技术支持。

（3）现场支持：如果不能通过远程技术支持方式解决系统的技术故障，在用户提出现场支持要求后的24小时内，中标人将派遣工程师赶赴现场分析故障原因，制定故障排除方案，提供故障排除服务。

**14.2 免费质保期间的服务承诺**

14.2.1质保期内日常维护方案

（1）中标人需提供项目免费质保期为八年。在浦东新区范围内具有固定的维护技术团队，且能提供良好的技术支持；投标人需根据项目情况在投标文件中提供相应运维服务方案。

（2）质量保质期内，由采购人负责日常性管理工作，包括信息更新、数据维护和系统管理，中标人负责本项目所涉及的技术性维护，其工作范围为：软件日常运行维护、软件版本升级和错误更正；合同所界定的功能范围内的局部调整。

（3）当出现故障时，采购人应立即通知到中标人。如属于严重故障，中标人立即委派工程师进行处理；如属于一般故障，中标人委派工程师在一小时内开展问题处理工作；必要时到现场进行紧急处置。

（4）中标人在约定的时间内未能弥补缺陷，采购人可采取必要的补救措施，但其风险和费用将由中标人承担，采购人根据合同规定对中标人行使的其他权利不受影响。

如遇功能变更，双方协商解决。

14.2.2项目服务期间平台发生故障后的应急响应方案的要求

应急响应要求：每周7天×24小时，方式：手机、微信、E-mail

14.3免费质保期后的服务承诺

14.3.1质保期外的服务需求：

（1）质量保证期过后，应提供免费电话咨询服务，并应承诺提供产品上门维护服务。

（2）质量保证期过后，采购人需要继续由原供应商或制造商提供售后服务的，该供应商或制造商应以优惠价格提供售后服务。

14.3.2投标人需提供

（1）日常维护方案及收费标准（人工）。

（2）系统发生故障后的应急响应方案及收费标准（人工）。

**15 项目的保密和知识产权**

15.1 中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。

15.2采购人委托开发软件（若有）的知识产权归采购人所有。中标人向采购人交付使用的信息系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。

15.3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。

15.4 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。

15.5如采购人使用该标的物构成上述侵权的，则中标人承担全部责任。

**16 技术培训**

**16.1技术文件**

中标人应为所有被培训人员提供培训用文字资料及本系统的详细技术文件。

培训结束后10个工作日内向采购人提交完整的培训过程材料，包括：培训总结报告、培训方案、学员须知、学员签到记录表、参训学员名单信息和考核结果、培训课程安排表、培训专家授课课件、学员培训满意度测评问卷及问卷分析报告等。

**16.2技术服务**

（1）投标人应具有健全的培训管理制度和管理流程、培训计划。

（2）培训目标为项目所涉及的主管部门、学校信息化负责人、学校人工智能教师等，投标人需采取集中培训、入校培训、远程培训等多种形式的培训组织方式。培训内容包括软件的使用及维护培训，使受训者能够独立、熟练地完成系统运行维护与操作，实现依据本合同所规定的系统运行保障的目标。

（3）投标人应在投标文件中详细说明技术指导和技术支持的范围和程度。

（4）培训时间与日期应在软件开发完毕后由采购人和中标人共同商定，并提供具体的培训方案。

四、投标报价须知

**17 投标报价依据**

17.1 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、工作量清单、项目现场条件等。

17.2招标文件明确的项目范围、实施内容、实施期限、质量要求、售后服务、管理要求与标准及考核要求等。

17.3工作量清单说明

17.3.1 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。

17.3.2采购人提供的工作量清单是依照采购需求测算出的主要工作内容，允许投标人对工作量清单内非核心工作内容进行优化设计，并依照优化后的方案进行报价。各投标人应认真了解招标需求，如发现核心工作内容和实际采购需求不一致时，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，应以工作量清单为准。

**18****投标报价内容**

18.1 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）应包括项目软硬件产品、前期调研、方案设计、硬件集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务这一系列过程中所包含的所有费用。

18.2 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。

18.3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。

18.4 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。

**19投标报价控制性条款**

19.1 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（如有要求）均不得超过对应的预算金额或最高限价。

19.2 本项目只允许有一个报价，任何有选择的报价将不予接受。

19.3 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。

★19.4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：

19.4.1减少工作量清单中核心工作内容数量，或设备材料参数指标中核心设备数量；

19.4.2 投标报价和技术方案明显不相符的。

五、政府采购政策

**20 节能产品政府采购**

20.1 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）和《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“节能产品品目清单”中的，在技术、服务等指标同等条件下，应当优先采购节能产品。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产品。

20.2投标人如选用节能产品的，则应在投标文件中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；反之，该产品在评标时不被认定为节能产品。

**21环境标志产品政府采购**

21.1 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）和《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“环境标志产品品目清单”中的，在性能、技术、服务等指标同等条件下，应当优先采购环境标志产品。

21.2投标人如选用环境标志产品的，则应在投标文件中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；反之，该产品在评标时不被认定为环境标志产品。

**22 促进中小企业发展**

22.1 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》。

22.2 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》。

22.3 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。

22.4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。

22.5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。

22.6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。

**23****促进残疾人就业（注：仅残疾人福利单位适用）**

23.1 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。

23.2 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。