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**

2023年中国（上海）自贸区基础云平台创新区域建设项目

**3项目地点**

上海市浦东新区迎春路520号（采购人指定地址）。

**4 招标范围与内容**

**4.1 项目背景及现状**

国务院在2015年发布《国务院关于促进云计算创新发展培育信息产业新业态的意见》明确提出主要任务：

（一）增强云计算服务能力。

（二）提升云计算自主创新能力。

（三）探索电子政务云计算发展新模式。

（四）统筹布局云计算基础设施。

云计算有助于降低电子政务成本，提高电子政务部署效率，降低信息共享和业务协同难度，提高政府服务效率。目前，北京、广州、深圳、江西、福建、浙江、陕西、贵州等省市分别开展了政务云系统建设。2016年浦东经信委信息中心已建设完成一个政务云数据中心，建立服务于浦东各个委办局IT环境共享的资源池，动态分配系统资源以提高利用率、优化系统资源的使用，并提供按需付费，降低系统的总拥有成本，解决以前烟囱式的建设模式，实现各个厅局业务逐步迁移以及数据交换共享体系的建设。

随着浦东电子政务业务的逐渐发展，以及业务数据量不断的增大，浦东各厅局目前的IT应用系统已经超过300个，数据量已经达到了1.5PB，并且系统数量和数据量还在快速增长中，IT系统结构变的越来越复杂，目前迁移到移动政务云数据中心的数据量将近300TB，并逐步增多，随着业务逐步迁移到统一的云平台，数据量逐步增大，业务负载越来越重。

本项目通过整体规划、整体购买的服务模式，在对区内信息化发展需求、电子政务云进行调研分析的基础上，充分运用云计算、大数据等先进理念和技术，按照“集约高效、共享开放、安全可靠、按需服务”的原则，以“云网合一、云数联动”为构架，建设浦东政务云平台，实现新区各部门基础设施共建共用、信息系统整体部署、数据资源汇聚共享、业务应用有效协同，为公共服务提供有力支持，提高为民服务水平，提升用户现代治理能力。

**4.2 项目招标范围及内容**

项目招标范围及内容主要包括物理托管、网络资源服务、计算资源服务、存储资源服务、安全服务和密码服务。

**4.3本项目工期为**

合同签订后1个月交付，如遇封网等特殊情况，则交付按实际封网天数顺延。服务期从实际交付时间开始计算，服务期限为3个月。

**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、包质量、包安全的方式实施总承包。

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发生设备维修的，采购人不另行支付相关费用。

**7.2 支付方式**

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

7.2.2分期付款的时间进度要求和支付比例具体如下：

（1）第一笔付款-交付付款（80%）：甲方收到乙方关于系统初步验收报告、合同规定的有关资料、以及发票（经审核符合要求）后30日内，向乙方支付货款，但该付款行为不构成对系统的验收；

（2）第二笔付款-最终验收付款（20%）：甲方收到乙方的验收报告（由甲乙双方及有关部门签署）、合同规定的有关资料（一式二份）、发票正本（一份）后30日内，甲方向乙方支付剩余款项。

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）国家标准化管理委员会《电子政务标准化指南-信息共享（征求意见稿）》

（2）国家标准化管理委员会《XML在电子政务中的应用指南》

（3）《政府信息交换语言标准》

（4）《政务信息资源交换体系》GB/T21062

（5）《信息安全等级保护管理办法》（公通字[2007]43号）

（6）《信息安全技术信息系统安全等级保护基本要求》（GB/T22239-2008）

（7）《中华人民共和国计算机信息系统安全保护条例》国务院令147号1994年2月18日

（8）《加强计算机信息网络保密管理的通知》（中保委发[2002]4号）

（9）《计算机软件保护条例》（国务院令2001年第339号）

（10）《计算机场地通用规范》（GB2887-2000）

（11）《电子计算机机房设计规范》（GB50174-93）

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

（13）《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021)

（14）《中华人民共和国密码法》

（15）建设单位提供的设计要求及相关资料

（16）国家相关的政策及法规等

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**

**工作量清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **具体内容** | | **单位** | **资源总量** | **备注** |
| 1 | 物理托管 | 机房机柜服务 | 个 | 20 | ● |
| 2 | 网络资源服务 | 互联网公有IP服务 | 个 | 254 |  |
| 3 | 互联网带宽（骨干级） | GB | 4 | ● |
| 4 | 政务专线 | 10GB/条 | 4 | ● |
| 5 | 应用负载均衡服务 | 每IP | 103 |  |
| 6 | 安全交换区 | 每IP | 254 |  |
| 7 | 计算资源服务 | CPU | 核 | 10984 | ● |
| 8 | 内存 | G | 67660 | ● |
| 9 | 存储资源服务 | 应用存储空间 | TB | 3373.7 | ● |
| 10 | 高性能数据库存储 | TB | 523 | ● |
| 11 | 安全服务 | 网络访问控制服务 | 租户 | 130 |  |
| 12 | 入侵防御服务 | 租户 | 130 |  |
| 13 | 用户管理服务 | 租户 | 130 |  |
| 14 | 用户身份认证服务 | 租户 | 130 |  |
| 15 | 数据库审计服务 | 实例 | 103 |  |
| 16 | 常规安全漏洞扫描 | 次 | 2000 |  |
| 17 | 在线防护WAF | 套 | 103 |  |
| 18 | 网页防篡服务 | 套 | 103 |  |
| 19 | 密码服务 | 安全认证网关服务 | 套 | 10 |  |
| 20 | 时间戳服务 | 套 | 1 |  |
| 21 | 签名验签服务 | 套 | 10 |  |
| 22 | 密钥管理系统 | 套 | 10 |  |
| 23 | 云密码机服务器 | 台 | 4 |  |

**说明：上表中所列为本次招标的主要工作内容，其中“●”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。**

**9.2具体技术质量需求**

**9.2.1总体要求**

系统架构要求：满足电子政务云总体架构，以政府购买服务的方式，统一为浦东新区各委办提供服务。

浦东政务云平台架构要求：政务云平台网络区域按电子政务网络安全要求划分为电子政务外网和互联网两个区域，政务云平台相应划分为两个部分，分别位于电子政务外网区域的政务外网云平台和位于互联网区域的互联网云平台，在符合网络安全等级保护基本要求的前提下，两个云平台之间需使用安全隔离方法保证安全和数据传输；单个云平台内的核心系统尽量采用同一厂商的产品。中标人提供的物理设备需要按独立的机房区域划分给云平台使用。

云资源需求：基线资源池物理建设规模（可用资源量）满足至少物理CPU 10984核，内存67660 GB，存储3896.7 TB，应满足区级的业务需求，在各项资源发放水位高于70%时及时报告招标人。中标人应按照招标人的要求，根据实际需求进行扩容。

云运维管理平台服务：云服务商应使用自主的、适应国际标准的商业化虚拟化软件，并搭建统一的个性化云运维管理平台提供服务。云运维管理平台能够基于自主架构的虚拟化软件，提供云运营管理服务和云运维管理服务，能够对IT基础设施进行统一管理。

安全服务：政务云平台需符合《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求。中标人所提供的加密服务及提供加密服务所需的软/硬件设备符合《中华人民共和国密码法》及国家密码管理部门的相关要求。

**9.2.2 指标要求**

服务指标要求如下：

|  |  |
| --- | --- |
| **指标名称** | **指标要求** |
| 平台可用性 | 中标人应承诺在合同期内用户云服务可用时间的概率不低于99.9%，即实际可用时间/(实际可用时间+不可用时间)。 |
| 数据存储持久性 | 中标人承诺在合同期内数据保存不丢的概率不低于99.99%，即完好数据/(完好数据+丢失数据)。 |
| 数据可迁移性 | 中标人承诺用户能够控制数据的迁移，保证启用或弃用该云服务时，数据能迁入和迁出。 |
| 数据私密性 | 中标人应承诺用户应有加密或隔离等手段保证同一物理资源池的用户数据互不可见。 |
| 资源交付服务响应时间 | 资源开通、变更完成后交付用户时间-收到需求时间，标准需求不超过3个工作日。 |
| 故障恢复时间 | 一般事件需在360分钟内恢复、重大事件需在60分钟内恢复、特别重大事件需在30分钟内恢复。  说明：  一般事件：故障对系统业务无明显影响，仅造成系统报错、非关键应用无法启动、使用不便、操作不畅等。  重大事件：故障造成系统发生中断或系统死机但重启后正常；应用部分不稳定；系统运行正常，但不能进行操作（控制台无响应）。  特别重大事件：故障造成系统失效或崩溃，应用系统无法正常启动运行、网络故障、丢失数据等，且没有临时替代解决方案；系统硬件故障、系统崩溃（死机和）自动重启）且不能再启动、磁盘信息丢失、系统或应用服务无法启动、网络链接失效、文件损毁等。 |

**10 技术指标要求**

**10.1系统功能与技术指标**

**10.1.1 云平台能力要求：**

支持x86架构与ARM架构混合部署，并可提供以下能力：弹性计算服务(ECS)、对象存储软件(OSS)、块存储(EBS)、文件存储(NAS)功能等。

**10.1.2云业务管理平台要求：**

提供一套云业务管理平台软件，提供云业务管理和业务云上资源监控等相关服务，能够对云上业务进行有效管理。云业务管理平台软件需支持与中标人所提供的云运维监控平台对接的能力、以及在基础设施层各类服务器及其虚拟化环境中部署的能力。云管理平台可提供北向接口、API接口，接入浦东大数据中心统一云管平台。

**10.1.3虚拟化平台要求：**

虚拟化平台需支持国产化操作系统。虚拟机之间可以做到隔离保护；虚拟机具有自己的资源（内存、CPU、网卡、存储），可以指定单独的IP地址、MAC地址等；当虚拟机操作系统出现故障时，可以自动重启或者迁移该虚拟机，保障业务连续性；支持将多个物理服务器组成集群，可基于CPU、内存、磁盘等资源利用率进行动态资源调整；虚拟化软件可以在线进行版本升级。

**10.1.4云网络系统要求：**

需采用国产化网络设备；核心骨干设备、出口设备、骨干线路等需要支持冗余备份，云内骨干线路带宽≥40Gb带宽，服务器业务≥10Gb带宽，核心骨干设备可以保证大规模业务迁移，无缝扩容需求；支持对云平台内的网络设备进行统一管理；网络控制器需集群部署。

**10.1.5出口网络需求：**

公网IP地址需求：不少于1个C类互联网IP地址，后续可根据实际使用情况扩容。

互联网带宽：需提供至少2\*2GE带宽接入公网，后续可根据实际使用情况扩容。

政务外网带宽：需开通不少于4条10GE传输资源，双路由接入，2条从云平台所在机房至招标人指定的浦东大数据中心世纪大道2001号某机房，2条从云平台所在机房至招标人指定的申港大道200号某机房。

**10.1.6平台高可靠要求：**

云平台使用的网络安全设备、服务器、存储等设备都应具备高可靠性及冗余性，即单个设备或单个节点出现故障时，其他设备/节点可以接管业务。云平台具备高可用和动态迁移功能，发生物理设备故障后，虚拟机可以自动迁移到其他可用资源上运行，确保业务系统不受物理设备故障影响。云平台提供备份/快照功能，能对政务云平台中的物理和虚拟服务器进行备份，防止存储故障导致数据丢失。

**10.1.7云安全需求：**

符合《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求；满足《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021)第三级要求的内容。

**（1）平台安全要求：**

为了保证平台的安全、稳定运营，制定完善的安全运维管理体系，制定完善的安全管理制度规范，对不同的安全区域、安全保护对象明确安全责任人；提供符合信息安全等级保护三级要求的云平台基础安全和应用系统安全的服务内容。

需提供安全监控，安全监控内容包含但不限于网络流量监控、各个安全设备的日志记录监控、安全设备运维操作监控和云资源运行状态监控等，并提供安全事态分析，满足用户不同安全级别业务系统的安全需求。

中标人建设的浦东政务云平台需满足包括但不限于如下安全要求：物理安全、网络安全、主机安全、平台安全等内容。

1）物理安全：中标人用于建设浦东政务云的机房需具备防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应等能力。

2）网络安全：中标人需针对浦东政务云平台按照国家网络安全等级保护基本要求要求建立一套网络安全防护体系，对网络边界处提供访问控制、病毒过滤、防攻击、防入侵、防篡改、内外网数据安全隔离交换等立体安全防护，保护平台内部网络通信安全。提供入侵流量测功能；态势感知通过大数据的离线数据分析能力，对收集的安全日志，进行建模分析，通过大数据手段得出未知威胁攻击、黑客入侵的结论。

访问控制：浦东政务云平台在各网络边界处均应部署安全访问控制设备，包括防火墙、IPS、VPN网关、安全网关等，能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。支持按用户和系统之间的允许访问规则，允许或拒绝用户对受控系统进行资源访。

安全审计：中标人需对浦东政务云平台使用网络设备运行状况、网络流量、用户行为、特权命令等进行日志记录，能够根据记录数据进行分析并生成审计报表，同时对系统审计的记录进行有效安全保护，避免受到未预期的删除、修改或覆盖等不安全操作。

边界完整性检查：中标人通过部署网络行为管理系统、安全审计系统应能够对非授权设备私自连到内部网络的行为及内部网络用户私自连到外部网络的行为进行检查，能根据用户信息、主机信息、IP信息等准确定出非法互联位置，并对其进行有效的网络阻断控制。

入侵防范：配备有IDS或IPS入侵防范、检测系统或安全网关系统，实现的实时防范功能应包括：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等非法网络攻击行为，当检测到攻击行为时，系统将详细记录相关信息，同时在发生严重入侵事件时具备报警、记录功能。

恶意代码防范：中标人在网络的边界处对各种恶意代码进行检测和清除功能，系统应支持自动及手工方式对恶意代码库的升级和检测系统的更新功能。

网络设备防护：中标人所使用的网络设备均应支持对登录用户的身份鉴别功能，支持采用加密用户口令鉴、RADIUS身份认证等方式，可通过命令行、Web、中文图形化配置软件等方式进行配置和管理，并可通过ACL访问控制列表的方式实现对网络设备的管理员登录地址进行限制，所有网络设备用户均应具备唯一标识。

3）主机安全：对主机的物理安全，主机访问控制方面进行保护。

主机访问控制：主机系统应启用主机系统的访问控制功能，依据安全策略控制用户对资源的访问权限，通过系统的技术维护措施严格限制默认账户的访问权限。

4）平台安全：包括虚拟化及云运维管理平台的安全保护，支持物理资源与虚拟资源统一管理。

虚拟化安全：支持有代理或者无代理安全方式进行虚拟环境的整体防护。

浦东政务云平台安全：如果云运维管理平台需要数据库的支持，应保护好云运维管理平台的数据库安全，设置强壮复杂的密码策略、备份数据库和配置相关的网络安全服务；云运维管理平台的访问许可应加强管理，删除不需要的用户账号。

浦东政务云平台访问控制安全：用户在访问浦东政务云平台资源过程中支持使用数字证书进行身份认证，包括但不限于中标人维护人员、委办局操作人员、政务云管理单位监管人员。

5）委办局单位部署在浦东政务云平台中的应用系统在执行国家及本市有关电子政务信息安全管理办法的过程中，若发现重大安全事故或者安全隐患时，中标人需要配合进行安全整改。

**（2）国密安全要求：**

基于密码技术为根本，以《网络安全等级保护基本要求》为目标，充分遵循《信息系统密码应用基本要求》的相关要求，建设面向云租户的云密码服务体系，总体构建以密码技术为核心的云密码服务支撑体系，融合密码应用的不同类别和多种场景。

1）整体体系定位：

本次密码保障体系基于国产密码算法进行建设，为面向上云的信息系统提供密码保障机制，配合整体的国密改造工作，服务对象为浦东新区各委办局适配国密要求的信息系统及国产终端环境。建设一套满足国密要求的云密码保障体系。

2）选用安全合规的密码产品服务：

本次建设的密码保障体系，所有密码设备均满足商用密码产品认证的合规产品，并提供密码支撑服务。

3）国产密码适配改造：

本次建设的密码保障体系包括应用系统国密改造适配工作，提供独立的密码改造技术要求、密码接入流程、适配环境，帮助各委办局能快速的推进信息系统国密改造。

**10.1.8 设备托管服务要求：**

需提供数据中心机房空间服务，提供额外设备托管空间服务；需提供机房整机柜出租服务，提供额外设备托管机柜，托管机柜数量不少于20个，单机柜功耗不低于6000W。

**10.1.9 机房技术要求：**

（1）机房空间要求：政务外网、互联网区域使用物理隔离的不同机房，机柜总数量不少于120个，实际使用机柜数量可根据项目需求提供。每机柜提供双路不间断供电，功率不低于6KW。

（2）中标人提供的机房可以按照招标人的要求对资源进行物理和逻辑隔离，满足多个云平台资源区和独立资源区域划分要求。独立区域具有门禁控制，控制权按照招标人要求进行管理。

（3）中标人提供的机房应具备符合国密要求的门禁系统。

（4）机房链路要求：

政务外网接入：要求承载政务云平台的网络和市政务外网骨干传输网络高效安全地衔接，满足各政务部门接入政务云业务系统的网络需要。根据相关安全管理部门的要求，中标人应支撑安全管理部门放置相关设备到中标人机房或进行专网的接入。

互联网接入：要求承载政务云平台的网络和市政务外网互联网统一出口高效安全地衔接，满足各政务部门业务系统接入互联网的需要，需提供互联网骨干级带宽服务及异网接入能力。

（5）机房环境要求：

|  |  |
| --- | --- |
| **项目** | **设计指标** |
| 环境要求 | 温度：开机时23C1C，停机时5C ～35C；相对湿度：开机时40% ～55%，停机时40% ～70%；温度变化率＜5C/h，不得结露。 |
| 结构 | 抗震：乙级以上，抗震烈度7度及以上，机房活荷载标准值≥8kN/m2，电池室≥12kN/m2，机房外墙不宜设采光窗，耐火等级：一级。 |
| 空气调节 | 机房专用空调N+1冗余，制冷量按300W/m2估算，总冷量负偏差不大于5%；空调系统供电应采取双路市电自动切换线路供电，每台空调应采用独立回路供电。 |
| 机房和辅助区应设置空气调节系统，机房应保持正压，主机房与其它房间、走廊间的压差不应小于4.9Pa，与室外静压差不应小于9.8Pa。 |
| 主机房内的空气含尘浓度，在表态条件下测试，每升空气中大于或等于0.5μm的尘粒数，应少于18,000颗。 |
| 供电电源 | 机房市电容量≥10000KVA，由2个供电局向、2个不同路由同时供电，保证电源不同时受到损坏，配备电源自动切换系统。（如有请提供双路市电及市电容量证明材料） |
| 后备用电 | 配备不间断电源系统，N+1的冗余备份UPS系统数量大于一套，所有设备机架供电应由两套不同UPS提供，电池满负荷放电时间不少于30分钟。 |
| 配备柴油发电机组，保障本系统满负荷情况下可靠供电运行72小时。 |
| 电源质量 | 稳态电压偏移范围3%，稳态频率偏移范围0.5Hz，输出电压波形失真度≤5%，允许断电持续时间0～4ms；防雷、防浪涌：保护级别（IEC/VDE标准）达到I级B类标准。 |
| 接地 | 接地电阻≤ 1，接地电位差1V。 |
| 机房布线 | 采用光缆或六类及以上对绞电缆，采用1+1冗余。 |
| 照明要求 | 眩光限制按I级标准，照度按机房≥300Lux 及按现场布局排列，机房内应设置备用照明，其照度为一般照明的15%。机房应设置疏散照明和安全出口标志灯，其照度不应低于0.5LUX。 |
| 机房监控 | 空气质量：对温度、相对湿度、压差、含尘度；漏水监测报警；监控IT设备、空调、动力、供配电系统、不间断电源、电池、柴油发电等设备；采用KVM切换系统。 |
| 安全防范 | 在主要出入口、机房、配套区域采用门禁系统和视频监控系统，机柜区域配备专用门禁和24小时监控系统，视频监控画面可远程调用，中标人需开放相应的接口或者服务提供监控服务，监控录像保存时间大于3个月。 |
| 消防 | 应配置气体消防系统和火灾自动报警系统。 |

**10.2硬件设备参数指标**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **具体配置要求** | **数量** | **备注** |
| 1 | 软件虚拟化服务器（X86架构） | CPU：≥[hygon7280]\*2；≥[32]\*2核；  内存：内存≥1024GB；频率≥2666MHz；  硬盘：480G[480G\_sata\_ssd]\*1；1600G[1600G\_nvme\_ssd]\*1；  网络接口：≥10GE\*2；双端口10G光口独立网卡；  电源和风扇：配置冗余电源和风扇；  磁盘控制器类型：sas卡（none-raid）\*1，支持的硬盘数量≥12  硬件要求：服务器要求在XC名录中。 | 42 |  |
| 2 | 软件虚拟化服务器（ARM架构） | CPU：≥[kunpeng920-5251K]\*2；≥[48]\*2核；  内存：内存≥384GB；频率≥2933MHz；  硬盘：240G[240G\_sata\_ssd]\*1；1600G[1600G\_nvme\_ssd]\*1；  网络接口：≥10GE\*2；双端口10G光口独立网卡；  电源和风扇：配置冗余电源和风扇；  磁盘控制器类型：sas卡（none-raid）\*1，带宽≥6Gbps，non-raid直通，满足机型磁盘配置需求和盘序要求。  硬件要求：服务器要求在XC名录中。 | 80 |  |
| 3 | 基础管控服务器/管控主机服务器 | CPU：≥[hygon5280]\*2；≥[16]\*2核；  内存：内存≥512GB；频率≥2666MHz；  硬盘：480G[480G\_sata\_ssd]\*1；3840G[3840G\_nvme\_ssd]\*4；  网络接口：≥10GE\*2；双端口10G光口独立网卡；  电源和风扇：配置冗余电源和风扇；  磁盘控制器类型：sas卡（none-raid）\*1，支持的硬盘数量≥12  硬件要求：服务器要求在XC名录中。 | 25 |  |
| 4 | 管理基础服务器 | CPU：≥[hygon7280]\*2；≥[32]\*2核；  内存：内存≥768GB；频率≥2666MHz；  硬盘：480G[480G\_sata\_ssd]\*1；8000G[8T\_sata\_hdd]\*12；1920G[1920G\_nvme\_ssd]\*2；3840G[3840G\_nvme\_ssd]\*2；  网络接口：≥1GE\*2，≥10GE\*4；1GE: 主控芯片型号Intel I350/82580/82576，物理网口10/100/1000Mbps，支持PXE，支持虚拟化应用;10GE: 双端口10G光口独立网卡；  电源和风扇：配置冗余电源和风扇；  磁盘控制器类型：sas卡（none-raid）\*1，支持的硬盘数量≥12  硬件要求：服务器要求在XC名录中。 | 8 |  |
| 5 | 专有网络管理服务器 | CPU：≥[hygon7280]\*2；≥[32]\*2核；  内存：内存≥512GB；频率≥2666MHz；  硬盘：240G[240G\_sata\_ssd]\*1；1600G[1600G\_nvme\_ssd]\*1；  网络接口：≥1GE\*2，≥10GE\*2，≥40GE\*4；1GE: 主控芯片型号Intel I350/82580/82576，物理网口10/100/1000Mbps，支持PXE，支持虚拟化应用;10GE: 双端口10G光口独立网卡；  电源和风扇：配置冗余电源和风扇；  磁盘控制器类型：sas卡（none-raid）\*1，支持的硬盘数量>=12；  硬件要求：服务器要求在XC名录中。 | 4 |  |
| 6 | 对象存储服务器 | CPU：≥[hygon7280]\*2；≥[32]\*2核；  内存：内存≥256GB；频率≥2666MHz；  硬盘：480G[480G\_sata\_ssd]\*2；12000G[12T\_sata\_hdd]\*12；3840G[3840G\_nvme\_ssd]\*2；  网络接口：≥10GE\*2；双端口10G光口独立网卡；  电源和风扇：配置冗余电源和风扇；  磁盘控制器类型：≥sas卡（none-raid）\*1，支持的硬盘数量≥12；  硬件要求：服务器要求在XC名录中。 | 18 |  |
| 7 | 块存储（SSD）服务器 | CPU：≥[hygon7280]\*2；≥[32]\*2核；  内存：内存≥256GB；频率≥2666MHz；  硬盘：480G[480G\_sata\_ssd]\*2；3840G[3840G\_nvme\_ssd]\*10；  网络接口：≥10GE\*2；双端口10G光口独立网卡；  电源和风扇：配置冗余电源和风扇；  磁盘控制器类型：sas卡（none-raid）\*1，支持的硬盘数量≥12；  硬件要求：服务器要求在XC名录中。 | 30 |  |
| 8 | 块存储（高效云盘）服务器 | CPU：≥[hygon7280]\*2；≥[32]\*2核；  内存：内存≥256GB；频率≥2666MHz；  硬盘：≥480G[480G\_m.2\_ssd]\*1；≥8000G[8T\_sata\_hdd]\*36；≥3840G[3840G\_u.2\_ssd]\*2；  网络接口：≥1GE\*2: 物理网口10/100/1000Mbps，支持PXE，支持虚拟化应用; ≥10GE\*2；双端口10G光口独立网卡；  电源和风扇：配置冗余电源和风扇；  磁盘控制器类型：≥sas卡（none-raid）\*1，支持的硬盘数量≥12；  硬件要求：服务器要求在XC名录中。 | 24 |  |
| 9 | 文件存储服务器 | CPU：≥[hygon5280]\*2；≥[16]\*2核；  内存：内存≥ 512GB；频率≥2666MHz；  硬盘：480G[480G\_sata\_ssd]\*1；8000G[8T\_sata\_hdd]\*12；1920G[1920G\_nvme\_ssd]\*2；  网络接口：≥10GE\*2；双端口10G光口独立网卡；  电源和风扇：配置冗余电源和风扇；  磁盘控制器类型：≥sas卡（none-raid）\*1，支持的硬盘数量≥12；  硬件要求：服务器要求在XC名录中。 | 12 |  |
| 10 | 出口交换机 | 1）转发性能：交换容量≥4Tbps；包转发率≥1800Mpps；  2）硬件规格：高度≤1U，固定接口交换机；电源1+1备份，风扇框4+1备份；整机最大功耗≤220W；支持前后、后前风道；  3）端口配置要求：40/100 GE 光接口≥6个；10GE光端口数量≥48个；  4）二层功能：支持Access、Trunk和Hybrid三种模式，支持QinQ，支持M-LAG或vPC等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现），支持DLDP，支持动态MAC、静态MAC和黑洞MAC表项；  5）三层功能：支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议，支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议，支持IP报文分片重组，支持BFD for OSPF，BGP，IS-IS，Static Route，支持IPv6 ND、PMTU发现。 | 4 |  |
| 11 | 核心交换机 | 1）转发性能：交换容量≥600Tbps；包转发率≥200000 Mpps；  2）硬件规格：业务槽位数≥8；交换网板插槽数量≥6, 且支持网板N+M 冗余；风扇框冗余设计，要求风扇框个数>=2；无中板架构；10G/40G/100G端口时延均小于1.2us；DC，AC，HVDC电源模块均支持M+N和N+N；主控引擎与交换网板硬件分离,主控板故障或者更换不影响整机转发性能；严格前后风道；  3）端口配置要求：≥4个36端口40GE以太网光接口板；  4）二层功能：支持端口聚合，802.3ad，支持M-LAG或vPC等类似技术（跨框链路聚合，支持N:1镜像、流镜像、远程端口镜像；  5）三层功能：支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议，支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议，支持路由协议多实例、策略路由，支持VRRP，支持IP分片和重组。 | 4 |  |
| 12 | 万兆接入交换机 | 1）转发性能：交换容量≥4Tbps；包转发率≥1800Mpps；  2）硬件规格：高度≤1U，固定接口交换机；电源1+1备份，风扇框4+1备份；整机最大功耗≤220W；支持前后、后前风道；  3）端口配置要求：40/100 GE 光接口≥6个；10GE光端口数量≥48个；  4）二层功能：支持Access、Trunk和Hybrid三种模式，支持QinQ，支持M-LAG或vPC等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现），支持DLDP，支持动态MAC、静态MAC和黑洞MAC表项；  5）三层功能：支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议，支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议，支持IP报文分片重组，支持BFD for OSPF，BGP，IS-IS，Static Route，支持IPv6 ND、PMTU发现。 | 24 |  |
| 13 | 综合接入交换机 | 1）转发性能：交换容量≥350Tbps；包转发率≥110000 Mpps；  2）硬件规格：业务槽位数≥4；交换网板插槽数量≥6, 且支持网板N+M 冗余；风扇框冗余设计，要求风扇框个数>=2；无中板架构；10G/40G/100G端口时延均小于1.2us；DC，AC，HVDC电源模块均支持M+N和N+N；主控引擎与交换网板硬件分离,主控板故障或者更换不影响整机转发性能；  3）端口配置要求：≥2个36端口40GE以太网光接口板；≥1个48端口10GE以太网光接口板；  4）二层功能：支持端口聚合，802.3ad，支持M-LAG或vPC等类似技术，支持N:1镜像、流镜像、远程端口镜像；  5）三层功能：支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议，支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议，支持路由协议多实例、策略路由，支持VRRP，支持IP分片和重组。 | 4 |  |
| 14 | 专线接入交换机 | 1）转发性能：交换容量≥4Tbps；包转发率≥1800Mpps；  2）硬件规格：高度≤1U，固定接口交换机；电源1+1备份，风扇框4+1备份；整机最大功耗≤220W；支持前后、后前风道；  3）端口配置要求：40/100 GE 光接口≥6个；10GE光端口数量≥48个；  4）二层功能：支持Access、Trunk和Hybrid三种模式，支持QinQ，支持M-LAG或vPC等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现），支持DLDP，支持动态MAC、静态MAC和黑洞MAC表项；  5）三层功能：支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议，支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议，支持IP报文分片重组，支持BFD for OSPF，BGP，IS-IS，Static Route，支持IPv6 ND、PMTU发现。 | 4 |  |
| 15 | 带外管理核心交换机 | 1）转发性能：交换容量≥650Gbps；包转发率≥180Mpps；  2）硬件规格：高度1U，固定接口交换机；为了提高设备可靠性，支持模块化可插拔双电源；支持48个10/100/1000Base-T以太网端口，6个万兆SFP+；  3）二层功能：支持MAC地址≥32K，支持ARP表项≥8K，支持4K VLAN，支持QinQ，灵活QinQ、支持端口VLAN、协议VLAN、IP子网VLAN，支持组播VLAN，支持IEEE 802.1d(STP), 802.w(RSTP), 802.1s(MSTP)，支持IGMP v1/v2/v3、PIM-SM；  4）三层功能：支持静态路由、RIP v1/v2、OSPF、BGP、OSPFv3，支持IPv4 路由表≥8K，支持IPv6 路由表≥2K，支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、Static Route，支持IPv6、支持IPv4/IPv6双栈。 | 4 |  |
| 16 | 带外汇聚交换机 | 1）转发性能：交换容量≥650Gbps；包转发率≥180Mpps；  2）硬件规格：高度1U，固定接口交换机；为了提高设备可靠性，支持模块化可插拔双电源；支持48个10/100/1000Base-T以太网端口，6个万兆SFP+；  3）二层功能：支持MAC地址≥32K，支持ARP表项≥8K，支持4K VLAN，支持QinQ，灵活QinQ、支持端口VLAN、协议VLAN、IP子网VLAN，支持组播VLAN，支持IEEE 802.1d(STP), 802.w(RSTP), 802.1s(MSTP)，支持IGMP v1/v2/v3、PIM-SM；  4）三层功能：支持静态路由、RIP v1/v2、OSPF、BGP、OSPFv3，支持IPv4 路由表≥8K，支持IPv6 路由表≥2K，支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、Static Route，支持IPv6、支持IPv4/IPv6双栈。 | 4 |  |
| 17 | 边界防火墙 | 1）整机性能：防火墙吞吐量≥2.4Tbps，每秒新建连接数≥4500万，最大并发连接数≥18亿；  2）路由功能：支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议；策略路由支持的匹配条件：源IP/目的IP，服务类型，应用类型，入接口；  3）IPv6：支持IPv6协议栈、IPV6穿越技术、IPV6路由协议；  4）NAT：支持全面NAT功能，对多种应用层协议支持ALG功能；  5）VPN：支持IPSEC双机热备，实现会话同步，设备切换VPN业务不中断；支持URL识别能力和URL地址识别库，云端URL识别库≥1.4亿；  6）协议识别：可识别应用层协议数量≥6000种；  7）可靠性：支持BFD链路检测，支持BFD与VRRP联动实现双机快速切换，支持BFD与OSPF联动实现双机快速切换；支持平滑升级，升级窗口中支持不同版本的软件形成双机热备；实配应用层协议识别及流量控制功能；  8）硬件要求：关键器件使用国产芯片。 | 4 |  |
| 18 | 专线防火墙 | 1）整机性能：防火墙吞吐量≥50Gbps，最大并发连接数≥1800万，每秒新建连接数≥50万；IPSec VPN吞吐量≥30Gbps，SSL VPN吞吐量≥3Gbps；IPSec VPN隧道数≥20000，SSL VPN并发在线用户数≥5000；  2）路由功能：支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议；策略路由支持的匹配条件：源IP/目的IP，服务类型，应用类型，用户(组)，入接口，DSCP优先级；  IPv6：支持IPv6协议栈、IPV6穿越技术、IPV6路由协议；支持IPv6 over IPv4 隧道，6RD隧道；  3）URL过滤：支持URL识别能力和URL地址识别库，云端URL识别库≥1.4亿；  4）协议识别：可识别应用层协议数量≥6000种；  5）可靠性：支持BFD链路检测，支持BFD与VRRP联动实现双机快速切换，支持BFD与OSPF联动实现双机快速切换；  6）硬件要求：关键器件使用国产芯片。 | 4 |  |
| 19 | 流量分析平台（含探针） | 流量分析系统管理平台：  1）硬件要求：关键器件使用国产芯片  2）处理器：CPU≥2颗  3）内存：≥128GB DDR4  4）硬盘：≥32TB  5）监控场景：支持数据中心网络拓扑的visio级定制，监控视图中支持标识镜像点位置、网元位置及连线关系。  6）监控视图：能够根据运维重点组合最需要的数据投屏呈现，支持自定义组合各种业务性能、链路流量的关键指标，指标图表呈现具备3种或以上可选方式。  7）业务SLA报表：支持自动生成指定业务的运行状态报告，能够记录业务所包含的应用数量、业务的总运行时间、故障时间、无故障时间、故障率和无故障率等信息；以及每个应用的总运行时间。  8）调用其他平台接口：流量分析系统支持与主流负载均衡器进行API对接，梳理负载均衡器前后的虚拟系统及真实服务器地址的对应关系，以可视化的方式展示，并提供负载衡器前后的指标多段关联分析功能。  9）平台接口调用：流量分析系统支持resful API、kafka等标准数据接口，将任意维度及指标的分析统计数据输出至外部平台，支持秒级的接口调用频率及秒精度的统计数据查询输出。 | 2 |  |
| 流量分析探针：  1）硬件要求：关键器件使用国产芯片  2）处理器：CPU ≥2颗  3）内存：≥256GB DDR4  4）硬盘：≥128TB  5）性能要求：流量处理：≥10Gbps；数据包处理：≥600万pps；TCP/UDP会话处理≥100万/秒。  6）解码器要求：系统中内置自主产权的数据包解码器，支持在线进行数据包的快速解码分析。  7）数据链路层采集分析：系统支持基于原始数据包的mac层地址统计分析，分析维度包括mac地址、mac会话。  8）IP层采集分析：可以检索并展示流量，包率等曲线，并根据用户所选时间关联分析统计数据。 |
| 20 | 日志审计 | 1）系统结构：国产化硬件平台、国产化安全操作系统及功能软件构成  2）内存：≥64G  3）硬盘：系统盘≥240G SSD；数据盘≥16T，支持Raid5  4）系统性能：日志采集均值≥20000EPS，峰值≥35000EPS，配置不少于500个日志源授权。  5）数据采集：支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于26类300种日志对象的日志数据采集。  6）数据存储：支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数。  7）数据查询：支持对常用查询条件进行保存，可重复使用；支持查询条件缓存，通过快速调用系统右侧隐藏栏中缓存的查询条件，提升常用条件的检索速度。  8）数据分析：提供可视化关联分析规则编辑视图，可根据实际业务编辑关联分析规则；支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警。  9）告警管理：支持实时告警展示，可根据告警规则、告警级别两个维度进行实时告警监视，并可对刷新事件间隔进行设定。  10）统计报表：系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应。 | 2 |  |
| 21 | 网闸 | 1）系统性能：传输速率≥6400Mbps，传输延时≤0.5ms。  2）安全浏览：支持http消息头、消息体，上下行方向，命令及关键字的管控，支持允许、阻断、告警三种处理方式。  3）FTP访问：支持基于FTP协议和TFTP协议的文件传输功能。  4）数据库访问：支持对数据库用户名、命令、关键字等内容进行管控，包括允许、阻断、告警。  5）安全邮件访问：支持发件人、收件人、邮件标题、邮件正文、邮件附件等数据内容过滤。  6）音视频通话访问：支持SIP和RTSP协议。  7）自定义访问：支持自定义的TCP、UDP协议的数据访问功能，用户自定义应用无需对自定义协议软件进行二次修改开发。  8）文件同步：无需在用户服务器上安装任何插件，安全隔离与信息交换系统不开放任何服务端口；支持NFS、FTP等多种文件服务器类型，支持实时同步和周期性同步；  9）数据库同步：无需在用户服务器上安装任何插件；支持同构、异构数据库之间的同步；支持同侧数据库之间的数据同步；支持数据库同步冲突策略处理，包括覆盖、忽略处理方式。  10）安全防护：支持内容过滤引擎、文件过滤引擎、病毒过滤引擎安全防护及单独启停控制；支持病毒库升级，并提供后续升级服务。  11）日志审计：支持日志记录本地数据库存储，也可以将日志传输到独立的日志服务器上，传输日志格式支持syslog和welf，支持日志加密传输。 | 2 |  |
| 22 | 入侵防御系统 | 1）性能要求：整机最高可扩展至500Gbps；单槽位扩展IPS吞吐量≥80Gbps。  2）入侵防护功能：配置入侵防护功能模块；能够防范各种应用层攻击，包括但不限于：后门程序，木马程序，间谍软件，蠕虫，僵尸主机，异常代码，协议异常，扫描，可疑行为审计类等，能够对跨站攻击、SQL注入等WEB攻击行为进行有效防护。  3）DDoS防护：配置攻击防护功能模块；支持SYN Flood、SYN ACK、UDP Flood等DDoS防护，支持HTTP Flood、 HTTPS Flood等应用层DDoS防护。  4）防病毒功能：支持对SMTP、POP3、HTTP、FTP协议实现病毒扫描检测。  5）响应方式：支持日志告警、会话阻断、IP隔离、等多种响应方式。  6）升级服务：支持应用威胁签名库的在线升级、离线升级多种升级方式；支持每周定期升级威胁签名库、病毒库，遇到重大安全事件，支持即时升级。  7）报表：支持安全威胁的分析报表，提供基于威胁名称、威胁类型、威胁应用类型等呈现方式；支持应用流量的分析报表，支持按日、周、月、导出报表。  8）硬件要求：关键器件使用国产芯片。 | 4 |  |
| 23 | 租户侧加密机 | 1）符合国家密码管理局相关管理要求。  2）整机性能：SM2签名速率≥15000次/秒；SM2验签速率≥14000次/秒；SM3计算速率≥700 Mbps；SM4算法加解密速率≥700Mbps；单台最大支持虚拟加密机(VSM)数量≥32个,最少支持虚拟加密机(VSM)数量≤16个；  3）密钥算法支持：支持国密算法SM1、SM2、SM3、SM4；  4）虚拟化功能：单台云密码机可虚拟多个密码机VSM，提供弹性分配、虚机迁移、运算速度分配等云化功能，提高密码设备资源利用率。VSM可根据应用的需求动态伸缩，按需调配资源，同时应用所需的加解密功能也应能动态的按需加载；  5）密钥管理：支持密钥的安全生成（二级、三级模块）、存储、备份、恢复；  6）安全性：提供丰富基于口令、智能密码钥匙、数字证书等多种身份认证机制，各VSM安全隔离，各VSM密钥安全隔离；  7）接口支持：支持JCE、PKCS#11CSP、国密SDF等多种标准密码应用接口；密码机服务应符合《GB/T 36322-2018\_信息安全技术密码设备应用接口规范》；  8）管理要求：密码管理中心实现贯穿整个密码服务体系的管理中心，对设备和密码平台的使用均能进行管理；  注册管理：要求应用及密码设备在使用密码服务前，需要先接入服务进行注册认证,确保自己是合法对象，否则无法接入密码服务体系，应用无法使用密码服务。  虚拟服务管理：支持实时监控虚拟服务的状态是否关闭。当虚拟服务退出或者异常关闭的时候，资源回收服务会自动释放被租户占用的密码算法能力，更改剩余密码算法能力和各个密码设备负载信息；   1. 密钥管理：支持租户密钥生命周期安全管理包括密钥生成、传输、存储、使用、导入、导出、销毁，系统保证租户密钥私钥不以明文形式出现在密码设备之外，不被任何人非法使用。 | 4 |  |
| 24 | 态势感知平台（含探针） | 态势感知平台：  1）首页工作台：支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示。  2）安全态势可视化：支持立体、平面、球面等多种维度的网络实体关系透视。  3）监测中心：支持告警数据自动化归并，并通过告警列表条目颜色区分“已读告警”和“未读告警”。  4）分析中心：应内置包括规则模型、关联模型、统计模型、情报模型、AI模型等不少于5类安全分析模型  5）响应中心：支持通过单条告警、聚合告警添加白名单，快速过滤误报； 支持前端拖拽式交互设计安全风险分析研判策略和联动响应剧本。  6）运营中心：支持用户自定义编辑报告模板，选择的相应统计报表组成要展示的报告内容。  7）资产中心：支持人工录入、流量自动发现、主动扫描、web自动发现、资产同步等不少于5种的资产数据接入方式。  硬件要求：关键器件使用国产芯片。 | 2 |  |
| 探针：  1）性能要求：吞吐率≥5Gbps  2）探测扫描检测：具备端口扫描、主机存活扫描、服务扫描、Web扫描、扫描器指纹检测等600种以上的探测扫描检测规则，可针对任意单条规则进行启用和禁用。  3）恶意程序检测：具备挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell、恶意邮件等17000种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用。  4）配置风险检测：具备弱口令风险、明文传输风险、HTTP配置风险、中间件配置风向、数据库配置风险、服务配置风险等300种以上配置风险检测规则。  5）主机和账号异常检测：支持端口异常、主机对外扫描、主机对外攻击等主机异常检测，对任意单条检测规则支持启用和禁用。  6）告警研判：支持从请求头、请求体、响应头、响应体四个方面展示告警详情，并对攻击报文进行高亮显示；对攻击结果的判定，支持识别成功、尝试和失败行为；支持对威胁告警进行调查分析，针对威胁告警支持原始数据包取证分析，告警详情支持查看、下载PCAP包，在告警页面支持一键添加白名单。  7）告警归并：支持展示高度聚合告警列表，对告警进行自动归并；支持多维度告警查询，支持威胁告警快速过滤，包括筛选、排除操作（需提供软件功能截图证明支持以上全部功能）。  8）资产发现：支持根据探针的内部IP配置或从态势感知平台同步的内部IP配置从流量中进行资产信息的识别，资产信息包括IP、MAC地址、首次发现时间、最近活跃时间、资产类型、发现来源、服务与端口、标签。  9）流量采集：支持自定义流量采集策略，包括过滤策略和采集策略，支持根据IP和协议进行过滤，包括DNS、FTP、HTTP、HTTPS、IMAP、KRB5、LDAP、POP3、RDP、SMB、SMTP、SSH、TELNET、TLS等。  10）指纹识别：支持对Web类、FTP、TELNET等类型的资产指纹进行识别，识别信息包括指纹名称、分类、标签、厂商名称、官网链接、产品链接、产品描述、对应资产接口等；支持区分每个资产接口的最新指纹和历史指纹。  11）文件还原：支持文件还原，用户可新增指定后缀文件进行文件还原，具体协议包括HTTP、SMTP、POP3、IMAP、FTP、SMB、NFS等，还原文件支持推送沙箱进行安全检测。  数据同步：自定义配置：可在前端页面自定义配置与态势感知平台之间的数据传输类型、各类型数据均支持任意字段的发送配置。   1. 硬件要求：关键器件使用国产芯片。 |
| 25 | 漏洞扫描设备 | 1）性能要求：任务并发数≥15，单任务并发IP数≥90；  2）系统漏扫功能要求：用户可自定义扫描范围、扫描端口、扫描使用的参数集等具体扫描选项。具备弱口令扫描功能，支持弱口令扫描协议数量≥22种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典（需提供软件功能截图证明支持以上全部功能）；  3）网站漏扫功能要求：支持将漏洞以紧急、高危、中危、低危、信息进行危害程度的分类，并且可根据用户需要自定义漏洞等级。支持Web2.0扫描，采用自主研发的网页执行模块，执行网页中的JavaScript脚本获取其中的链接。支持对Struts2远程命令执行漏洞进行命令执行和文件上传的渗透测试验证操作；  4）数据库扫描功能要求：支持达梦、人大金仓的授权数据库漏洞扫描；配置授权扫描时能够远程登录目标数据库以验证能否成功登录目标数据库，防止因输错密码或网络限制等未能成功授权扫描。数据库扫描的漏洞库数量大于3000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD等国际、国内漏洞库标准兼容。数据库扫描支持的检测类型大于10种，至少包括弱口令、执行权限过大、访问控制漏洞、提权漏洞、缓冲区溢出漏洞、缺省配置、访问权限绕过、PL-SQL注入、危险程序、安全信息查看等。  基线核查要求：支持主流操作系统的基线配置检查，包括但不限于Windows、Linux、Suse、HP-UX、Solaris、AIX、Debian。支持的数据库基线配置检查包括但不限于Informix、DB2、MySQL、SQL Server、Oracle。在资产管理页面可直接对单个资产或批量资产下发扫描任务。  5）报表管理：支持导出的报告类型≥5种，包括HTML、WORD、PDF、EXCEL、XML报告格式。  6）硬件要求：关键器件使用国产芯片。 | 2 |  |
| 26 | SSL VPN | 1）符合国家密码管理局相关管理要求。  2）总体要求：支持SM2、SM3、SM4算法，具有密钥协商、身份认证、SSL隧道加密等功能。  3）性能要求：最大并发用户数≥6000； 最大并发连接数≥5800； 每秒新建连接数≥100；吞吐率≥ 55Mbps。  4）功能要求：支持国密SSL协议；支持端到端的全链路加密。支持日志完整性保护、syslog功能；具备SSL服务端动态选择证书的能力（SM2、RSA自适应）。应用支持：支持B/S应用；支持C/S应用，支持FTP、telnet、远程桌面以及通用的C/S应用：支持基于IP的所有应用。 | 2 |  |
| 27 | 平台侧堡垒机 | 1）硬件要求：关键器件使用国产芯片。  2）性能：最大支持150路图形会话或400路字符会话并发；最大支持300个被管资源数。  3）硬盘：内置≥4TB硬盘。  4）其他：支持液晶屏。 | 2 |  |

**10.3软件技术方案**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **模块名称** | **具体功能要求** | **备注** |
| 1 | 云业务管理平台 | 1）功能要求：   1. 支持查看历史告警。 2. 提供云环境中的云产品资源实例提供租户级的资源监控能力；提供云产品资源实例提供租户级的告警通知能力。 3. 支持以组织和资源维度统计统计资源报表、配额报表和云监控报表；支持异步导出的各类统计分析报表 4. 支持创建/修改/删除/查询资源集；支持查看/跳转到资源集所有的资源实例；通过资源集管理用户、用户组；支持对于不同的region区域，设置每个云产品可以使用的资源量，支持对于region和集群，设置不同的名称，便于管理 5. 创建/修改/删除/恢复/禁用/激活/查询用户、查询/修改/重置密码、变更归属、角色授权、用户组管理、登录策略设置 6. 支持创建/修改/删除/查询用户组、添加/删除用户；支持用户组与角色关联 7. 按时间/按组织维度计量、计量报表查询、计量报表导出   2）安全性要求：   1. 提供统一的用户密码策略配置，支持强密码、密码有效时间以及锁定策略； 2. 提供日志审计功能，保留所有用户的操作日志，并支持日志的过滤和导出功能。 3. 创建/修改/删除/禁用/激活登录策略、支持白名单、支持黑名单、关联用户、关联组织；支持按照登陆时间和IP地址的白名单/黑名单策略；支持设置能看见并使用这个登陆策略的组织 |  |
| 2 | 云运维管理系统 | 1）支持展示云平台部署产品概览。  2）支持看出每个集群的详细信息。  3）支持任务管理，支持展示系统中任务的整体运行情况。   1. 支持查看当前系统中等待介入、运行中、失败和已完成任务数量的统计信息。单击各统计数值，会跳转到对应的任务页面。 2. 支持查看最近24小时内正在运行中的任务。 3. 支持查看最近7天任务的运行趋势。 4. 支持修改任务的灰度策略即调整机器的执行批次。 5. 支持查看任务的执行情况。 6. 支持导出历史告警列表。   4）告警监控管理：   1. 支持查看告警源详情。 2. 支持根据监控项类型、产品、服务、等级、状态、开始日期、结束日期及过滤内容来进行过滤查询。 3. 支持告警处理，导出告警列表里的告警信息，支持告警屏蔽，支持为已屏蔽的告警解除屏蔽。 4. 支持按关键字查询相应的告警事件，可以根据业务需要，查询、添加、修改以及删除告警联系人和联系人组。   5）云资源管理：   1. 支持云主机库存情况查看，云主机库存详情中主要提供按区域、实例类型和日期分页查询某类实例在某个日期的库存情况。 2. 支持块存储、NAS、对象存储库存情况查看，历史可用库存（TB）显示近五天存储的库存可用情况；当前已用库存（TB）显示当前存储已用库存和百分比；存储库存详情中可按日期分页查询存储库存详情。 3. 支持负载均衡服务库存情况查看。 4. 支持显示云平台物理网络拓扑，支持显示网络设备网元和互联链路，网络设备和互联链路应支持按颜色区分链路状态。 5. 支持动态拓扑和基准拓扑展示功能，动态拓扑可以动态刷新拓扑状态，基准拓扑表示网络的目标状态。   6）用户权限管理：   1. 支持用户管理、用户组管理、双因素认证、角色管理、部门管理、菜单管理、Region授权管理、云操作系统日志、操作日志、授权信息。 2. 统一账号管理&角色权限管理，能实现对云平台所有的组件进行运维或者免登录跳转运维。   7）支持云平台运维工作自动化，可向批量资源完成运维操作，提供基础设施，云环境，操作系统，应用层的自动化运维能力。   1. 脚本管理，提供脚本库存放运维脚本，支持系统内置脚本，并支持运维人员自定义和导入脚本。 2. 软件包管理：提供软件仓库能力，可以上传和下载软件包，支持压缩包，JAR包等格式。 3. 运维作业：支持运维作业定义，运维作业可以手动触发和定时触发。 4. 运维流程编排：支持图形化方式编排运维流程。 |  |
| 3 | 弹性计算服务 | 1）功能要求：   1. 支持云主机生命周期管理和维护。 2. 支持对云主机CPU、内存、硬盘等基础指标进行监控，同时支持对云主机系统中的各进程CPU、内存、打开文件数进行监控，为用户提供系统级、主动式、细粒度监控服务。   2）可靠性：   1. 支持云主机按宿主机，机架，网络交换机物理拓扑的调度能力，提升业务的可靠性。控制台上分散策略支持严格分散和尽量分散两种可选。 2. 支持云主机热迁移，运维人员可以手工指定迁移任务的带宽限制，降低迁移流量对正常业务的干扰。 3. 支持云主机高可用（宕机迁移），当某台物理节点发生意外故障，在其上运行的云主机能够在其他正常的物理节点上重新启动，保障业务的连续性。   3）安全性   1. 支持云主机磁盘国密算法加密，能够对云盘中的数据、云盘和实例间传输的数据、云盘创建的所有快照进行加密处理，保障数据的安全性。 2. 支持云主机网络防ARP欺骗，云平台应阻止用户非法修改IP地址和MAC地址后发出的数据包，提升安全性。 3. 支持用户通过VNC方式远程访问云主机，同时支持用户设置云主机VNC密码（非系统密码），并能在用户VNC访问时进行VNC密码认证，保证终端用户对云主机的安全访问。 4. 支持用户通过快照对云主机的数据进行备份，通过快照进行云服务器的数据恢复，可以为每块磁盘创建64个快照。 |  |
| 4 | 弹性计算块存储服务 | 1）总体要求：为云主机提供的低时延、持久性、高可靠性的数据块级存储设备。  2）功能要求：支持在线扩展容量，扩容期间无需关闭虚拟机，无需卸载云盘；系统盘在线扩容不停业务。支持磁盘的创建、删除、卸载、扩容、挂载、查询、初始化等功能。  3）功能指标：单个云盘最高支持32TB容量。  4）安全性：支持分布式EC和三副本数据冗余保护，三副本模式下，数据三副本支持分布在3个机柜或3对接入交换机上。 |  |
| 5 | 文件存储服务 | 1）总体要求：为云主机提供的低时延、持久性、高可靠性的数据文件级存储设备。  2）功能要求：   1. 支持NFS v3.0/4.0，SMB2.1/3.0协议。 2. 支持多个文件系统组成全局命名空间。 3. 支持将NAS指定文件或目录归档到对象存储，可以按照不同时间段规则进行选择性归档。 4. 支持目录级容量Quota 管理。   3）可靠性：提供三副本数据保护，数据三副本支持分布在3个机柜或3对不同接入交换机上。（如有系统功能界面截图等相关证明材料，请在投标文件中提供）  4）安全性：支持通过权限组对访问主机的IP地址进行读写访问权限控制，允许授权对象对文件系统进行只读操作或读写操作，当同一个授权对象匹配到多条规则时，高优先级规则将覆盖低优先级规则。 |  |
| 6 | 对象存储服务 | 1）总体要求：对象存储服务支持RESTful API接口、兼容Amazon S3接口，通过开发工具包SDK或直接通过RESTful API进行基础和高级对象存储操作，提供key-value键值对形式的对象存储服务  2）功能要求：   1. 支持原生图片处理服务: 创建图片处理规则、图片格式转换、图片效果处理、添加文字或图片水印、高级编辑自定义图片处理样式等。 2. 支持对象的简单上传、追加上传、下载、删除、列举、复制，获取对象的元数据、创建多段上传任务。支持列举存储空间、创建存储空间、删除存储空间、列举存储空间内对象、获取存储空间的元数据。 3. 支持生命周期管理、定义和管理存储空间内所有对象或对象的某个子集的生命周期、变更容量和变更归属。 4. 3）功能指标：单个对象最大支持48.8TB，单租户支持最大10000个bucket并提供界面截图；每个bucket的生命周期最多可容纳1000规则。   4）安全性：支持客户端加密功能，可以使用客户端加密SDK，在本地进行数据加密，并将加密后的数据上传到对象存储，既支持云平台密钥管理系统托管的用户主密钥，也支持用户自主管理的密钥。支持服务器端的加密功能，用户能够使用密钥管理系统上创建的密钥进行加密。可以使用国密算法对bucket内保存的数据以及单独object进行加密存储。 |  |
| 7 | 专有网络服务 | 1）总体要求：支持用户创建自己的专有网络，同时支持自定义配置IP地址、子网、路由表。支持不同VPC之间的安全隔离。  2）功能要求：   1. 支持ENI弹性网卡（elastic network interface）绑定云服务器，在多个云服务器间自由迁移。支持为ENI绑定EIP。 2. 支持IPSEC VPN服务，支持IPsec-VPN建立专有网络（VPC）到本地数据中心的VPN连接，IPsec-VPN支持IKEv1和IKEv2协议，同时支持API方式配置。 3. 支持SSL VPN服务，支持通过SSL-VPN功能远程接入VPC，修改SSL服务端的名称、本端网段、客户端网段信息，支持创建SSL客户端证书，支持AES128、ASE192、AES256加密算法。支持API方式配置。 4. 支持共享VPC，支持按租户和资源集的VPC资源共享。VPC的所有者可以将VPC共享给同一组织的租户。 5. 支持在控制台上针对VPC配置多个CIDR地址段；支持新CIDR地址段的扩容。 6. 支持用户可以创建网络ACL配置入向/出向规则，进行网络访问控制功能，从而实现对一个或多个子网流量的访问控制。 |  |
| 8 | 负载均衡服务 | 1）总体要求：负载均衡服务采用通用服务器架构实现。提供4层TCP/UDP和7层HTTP/HTTPS协议类型的服务。  2）功能要求：   1. 七层负载均衡模式下支持配置域名或者URL转发策略，将来自不同域名或者URL的请求转发给不同的ECS处理。 2. 四层负载均衡支持TCP/UDP监听在后端应用服务器无插件模式下直接获取客户端源IP地址。七层负载均衡支持后端服务器应用程序通过HTTP头字段的X-FORWARD-FOR获取客户端源IP地址，支持从HTTP头字段扩展方式获取负载均衡实例Id和负载均衡VIP地址信息。 3. 四层负载均衡支持提供主备服务器Active-Standby模式，负载均衡监听的后端添加主备两台后端应用服务器，当主机健康检查正常时，流量将直接转发至主机；当主机健康检查失败，流量将切换至备机，主备服务器不需要依赖Keepalived、pacemaker等应用高可用组件。 4. 负载均衡支持4层一致性hash、轮询(RR)，加权轮询(WRR)和最小连接数(WLC)等调度算法，在上述每种调度算法4层支持TCP源地址会话保持，7层支持HTTP Cookie会话保持。 5. 负载均衡支持公网和私网类型实例。支持私网实例绑定公网IP地址，提供同一个实例同时支持公网和私网客户端访问的功能。支持ping 私网负载均衡的IP地址用于VIP探活。 6. 负载均衡支持配置性能保障型实例，针对不同的业务类型配置不同的规格，其中规格涉及并发连接数、每秒新建连接数、每秒查询请求数。支持单实例监听带宽配置，针对同一个VIP内不同的监听端口配置不同的带宽限制值。 7. 支持配置多种实例规格，不同规格实例限定最大支持连接数，可以变更实例规格。（如有系统功能界面截图等相关证明材料，请在投标文件中提供） |  |
| 9 | 云虚拟化平台安全服务 | 1. 提供流量安全监控、态势感知、Web应用防火墙、云安全管理中心、敏感数据包含、数据库审计、数据梳理及脱敏系统、云堡垒机、漏洞扫描。主机安全防护、密钥管理服务、伪装欺骗系统等安全功能服务。 2. 支持动态脱敏功能，可通过调用ExecDatamask接口对数据进行动态脱敏。（如有系统功能界面截图等相关证明材料，请在投标文件中提供） 3. 支持端口扫描欺骗策略，可添加需要防护的IP和端口，对恶意端口扫描行为进行欺骗。（如有系统功能界面截图等相关证明材料，请在投标文件中提供） |  |

**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验收方案**

11.2.1 本项目验收将由采购人组织进行，采购人也可委托第三方组织验收。

11.2.2 政务云平台（包括政务云和互联网两个区域），应满足《GBT2223 9-2019信息安全技术网络安全等级保护基本要求》三级要求、《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021)第三级要求，并由中标人提供网络安全三级等保测评报告、密评测评报告（相关测试费用包含在本项目报价中）。

**12人员及设备配备要求**

（1）中标人应为浦东政务云单独建立运维管理组织，配置相应团队。

（2）岗位要求详见人员岗位配置表：

**人员岗位配置表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **岗位名称** | **具体要求** | **数量要求** | **备注** |
| 1 | 项目经理 | 具有高级工程师或同等级别证书，承担过同类项目经验。请提供相关证明资料。 | 1 |  |
| 2 | 运维工程师 | 具有同类项目维护经验，负责项目整体运维。  其中1人为运维工程师负责人。  如有信息安全、云相关专业认证证书，请在投标文件中提供。 | 8 |  |
| 3 | 运营工程师 | 具有同类项目运营经验，负责项目整体运营。  其中1人为运营工程师负责人。  如有云相关专业认证证书，请在投标文件中提供。 | 2 |  |
|  | 合计 |  | 11 |  |

投标时请附有相关证明资料（包括但不限于资格证书、近3个月内的在职证明材料等）。

（3）中标人应在项目服务期内配合各业务部门做好应用上云及迁移工作，确保平稳过渡、顺利迁移。

（4）配合需求单位对上云及迁移业务系统进行调查摸底、制定上云及迁移方案，提供架构设计咨询，在系统上云迁移前期提供迁移支持服务。提供服务方案，应配合各需求部门做好上云及整体迁移工作。

（5）中标人应制定政务云平台使用规范、政务云安全防护管理办法等规范标准，协助各级部门进行相关业务应用系统的部署、运行和安全保障。

**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安装、调试服务所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由投标人自行负责。

13.2在项目安装、调试实施期间为确保安装作业区域及周围环境的整洁和不影响其他活动正常进行，中标人应严格执行国家与上海市有关安全文明施工（安装）管理的法律、法规和政策，积极主动加强和落实安全文明施工（安装）及环境保护等有关管理工作，并按规定承担相应的费用。中标人若违反规定野蛮施工、违章作业等原因造成的一切损失和责任由中标人承担。

13.3中标人在项目供货、安装实施期间，必须遵守国家与上海市各项有关安全作业规章、规范与制度，建立动用明火申请批准制度，安全用电等制度，确保杜绝各类事故的发生。

13.4中标人现场设备安装负责人应具有专业证书，安装人员必须持证上岗。中标人应对设备安装、调试期间自身和第三方安全与财产负责。

13.5中标人在组织项目实施时必须按安装施工计划协调好现场施工（安装）工作，在项目验收合格移交前对到场货物承担保管责任。中标人在项目实施期间必须保护好施工区域内的环境和原有建筑、装饰与设施，保证环境和原有建筑、装饰与设施完好。

13.6各投标人在投标文件中要结合本项目的特点和采购人上述的具体要求制定相应的安全文明施工（安装）和安全生产管理措施，同时应适当考虑购买自己员工和第三方责任保险，并在报价措施费中列支必须的费用清单。

**14售后服务要求（包括延伸服务要求）**

**14.1具体服务承诺**

云平台运维提供热线电话、电子邮件等技术支持方式，提供每周7天×24 小时电话响应服务。投标人提供每周7天×24 小时的运维服务保障。

（1）日常监控：

对云平台进行日常监控，包括监控告警的处理等。

（2）故障处理：

处理发生的云平台软硬件、通信线路等故障，确保云平台能够正常稳定运行；其中故障处理流程需要规定处理时限及当前处理环节的责任部门和责任人。

（3）安全服务：

提供政务云平台各个基础组件进行安全策略配置、安全扫描和系统漏洞的安全加固服务。提供政务云常规安全保障和监控预警工作。

（4）节假日保障：

重大节假日期间进行政务云平台运行和信息安全的重点保障工作。中标人如具备本市重大事件运营保障能力和经验，请在投标文件中提供相关证明文件。

**14.2 具体制度要求**

中标人应建立完善的政务云运维和安全管理制度，建立的制度包括但不限于：

（1）政务云日常运行维护管理制度。例如：故障处理、配置变更、安全策略优化、运行监控等。

（2）运维人员管理制度。如：运维团队人员服务管理、机房进出人员管理等。

**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采购人具有源代码修改权和永久使用权。采购人对本次开发的软件拥有产权，具有软件开发平台的永久使用权，中标人在售后维护期内（包括续签的售后服务期）应提供软件开发平台的后续升级及因开发平台升级导致的应用软件升级服务。

15.6 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：

中标人提供本系统的详细技术文件。

16.2技术服务：

（1）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。

（2）投标人应在投标文件中提出保修期之后的设备返修流程，包括返修时间，替用设备，以及返修价格。

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）应包括项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、智能化安装工程、硬件集成实施、软件开发和集成实施、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、投入使用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；

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。