连州市区域卫生信息系统云平台服务项目用户需求

一、 项目名称：连州市区域卫生信息系统云平台服务项目

二、 服务要求

中标方必须保证有足够的人员及技术支持负责本项目运维工作，在 30 分钟内响应，如经过远程等方式不能解决的，中标方需保证 4 小时内派技术人员到达现场，24 小时之内解决问题。中标方提供 7×24 小时支持维护服务，包括但不限于邮件、电话、远程维护、现场服务等维护方式。

三、 报价要求

1.投标人的投标报价须以人民币为报价单位。

2.投标总金额包括中标方设计、二次开发、测试、安装、标配工具、运输保险、调试、培训、质保期服务、各项税费及合同实施过程中不可预见费用等。

3.投标人必须按采购需求明细内容逐项列出计费标准，投标人报价需要具有每项明细的数量的月费用、年费用以及一年的总费用等。

四、 侵权责任要求

中标人应保证本项目所涉及的相关技术、服务或其任何一部分不会产生因第三方提出侵犯其专利权、商标权或其他知识产权而引起的法律和经济纠纷。如因第三方提出其专利权、商标权或其他知识产权的侵权之诉，则一切法律责任由中标人承担。

五、 安全要求

中标人所提供的产品需要符合等保和密保要求和标准。在采购人进行等保和密保改造过程中，如投标人所投产品有不满足等保三级和密保要求和标准的，中标人需按相关标准进行功能性改造和完善，并达到等保和密保相关要求。

六、 付款方式

本项目招标完成后双方签订合同确定最终费用，在项目服务期结束后，按实际服务时间一次性全额支付合同应付款。

因采购人使用的是财政资金，按照前款规定的付款时间，采购人在收到中标人发票后向政府采购支付部门提出办理财政支付申请手续（不含政府财政支付部门审核的时间），在规定时间内提出支付申请手续后即视为采购人已经按期支付。

采购内容	采购预算	服务期
连州市区域卫生信息系统云平台服务项目	人民币 XXX 万元	项目验收合格之日起提供一年的云平台运维服务

七、 技术要求

(一)合同生效之日起，中标人需要严格按照招标文件要求完成云平台服务项目的建设。

合同生效之日起30个日历日内完成汇聚机房对接云平台的网络建设、汇聚机房网络设备及云资源池存储的安装调试，并保证能正常使用。如中标人所提供的云平台真实环境达不到采购人招标文件要求的，采购人有权单方面取消中标人的中标资格，所造成的损失由中标人全部承担。

(三)自项目验收之日起开始计算一年运维服务。

一、云资源与配套服务					
序号	设备类型、名称		数量	单位	备注
1	数据库服务器		8	套	本数量为最高采购量，具体以采购人实际使用数量按实际使用月数为计价标准。用于安装采购人系统的各类数据库，使用数据库存储。
2	云服务专属资源包		14	套	本数量为最高采购量，具体以采购人实际使用数量按实际使用月数为计价标准。用于安装业务库服务器、镜像库服务器、应用服务器、备份测试服务器专属云包，支持安装各类Windows、Linux等正版操作系统，操作系统由中标人免费提供。挂载云资源包存储及备份存储。
3	云资源池存储	数据库及虚拟化服务器存储（超高IO）	25	TB	本数量为最高采购量，具体以采购人实际使用数量按实际使用月数为计价标准。Raid5后实际可用存储，不含备份存储。
		云资源包存储（高IO）	55	TB	本数量为最高采购量，具体以采购人实际使用数量按实际使用月数为计价标准。Raid5后实际可用存储，不含备份存储。
		备份存储（普通IO）	125	TB	本数量为最高采购量，具体以采购人实际使用数量按实际使用月数为计价标准。Raid5后实际可用存储，不含备份存储。
		历史数据备份存储（对象存储）	120	TB	本数量为最高采购量，具体以采购人实际使用数量按实际使用月数为计价标准。Raid5后的可用存储，用于历史数据的存储备份。
4	云主机备份		1	项	投标人所提供的云资源池须具有备份服务。
5	云下一代防火墙		1	套	本数量为最高采购量，具体以采购人实际租赁数量按实际使用月数为计价标准。用于对云桌面对云上系统访问流量的防护。
6	云资源池Anti DDos设备		1	套	投标人所提供的云资源池须具有Anti DDos设备。
7	云资源池负载均衡设备		1	套	投标人所提供的云资源池须具有负载均衡设备。
8	云资源池云监控平台		1	套	投标人所提供的云资源池须具有云监控平台。
9	云资源池虚拟化底层防护组件		1	套	投标人所提供的云资源池须具有虚拟化底层防护组件。
二、网络服务					
1	云平台专用光纤电路		2	条	用于连接区域卫生信息系统和云平台的光纤电路
2	云桌面专用光纤电路		1	条	用于连接区域卫生信息系统和云桌面的内部线路

一、云资源与配套服务				
序号	设备类型、名称	数量	单位	备注
3	对外服务网络出口	2	条	用于对外业务的系统网络
4	数据备份专用电路	2	条	用于连接数据备份服务器
三、云桌面服务				
1	云桌面服务器	20	套	本数量为最高采购量，具体以采购人实际使用数量按实际使用月数为计价标准。用于安装采购人的云桌面软件。
四、汇聚机房服务				
1	汇聚机房运维	1	项	投标人提供 1 年汇聚机房运维服务
五、等保、密保测评服务				
1	三级等保测评	1	次	提供符合采购人要求的等保三级测评服务
2	商用密码测评	1	次	提供符合采购人要求的商用密码测评服务
六、数据迁移服务				
1	数据迁移服务	1	项	将采购人原有数据中心平台的数据迁移至采购人所提供的数据中心平台，并确保数据在迁移过程中的完整性、一致性、可用性和安全性，支持业务系统升级、服务器更换、数据中心搬迁或技术架构优化等。

八、 具体要求

1. 总体要求

1.1 为采购人提供云平台服务，保障采购人原有区域卫生信息系统的应用系统的正常使用，保证采购人医疗业务正常，系统能与云平台无缝融合对接并能与采购人现有的上级平台或系统无缝融合对接。

1.2 要求提供包括但不限于数据一致性、数据完整性、应用会话状态完整性、连接中断、数据恢复等一系列测试，保证系统在云平台运行的安全性和有效性。

1.6 在服务期内，云运营商主机服务配置与业务规模可根据用户的需要进行配置，并可灵活进行调整。采购人申请的云资源服务可以实现快速供应和部署，实现集群内弹性可伸缩计费方式灵活，采购人无需另外支付押金，且有多种方式供采购人选择。

1.7 对于采购人新建接入云平台资源部分，投标人需承诺具有完善的设备供货渠道，完善的项目管理保障体系，成立专门项目小组负责对整个项目的预算、进度、质量等进行审核批准和监督，严格按照项目管理的要求进行科学管理和项目实施，确保按时间进度完成新建资源和采购人所服务的云平台的对接。

1.8 投标人需承诺具有丰富的云计算平台资源和网络资源，包括计算资源、存储资源、端口、设备、电路、安全等，能根据业务的发展情况进行实时扩容，保持网络良好的冗余能力。当数字电路专线和互联网专线遇到电路故障，需要紧急修复的同时，能够紧急调度资源，提供新电路供采购人应急使用，为本项目提供最优的数据中心、光纤电路、对外服务出口等。

1.9 投标人需要承诺对采购人所要求的专线电路提供系统“1+1”保护等自动保护措施，

确保电路的质量和安全可靠性；对采购人专线提供双路由保护接入，分别接入不同的机房。

1.10 投标人以云服务的方式向采购人提供区域卫生信息系统数据中心上云服务，要求基于云平台构建连州市区域卫生信息系统，形成配套的管理机制，实现云平台资源科学配置，对上层应用提供按需的资源服务，实现弹性伸缩、按需使用、快速交付和安全运维的功能，支撑区域卫生信息系统的云化部署，对医疗系统的管理、接口中间件和测试资源等也需要提供云服务支持。

1.11 投标人必须承诺保证对数据库物理服务器、云桌面服务器等提供符合等保三级要求的底层虚拟化安全防护组件，同时需要提供符合采购人需求的正版授权的云服务器操作系统。

2. 服务要求

2.1 投标人需为采购人区域卫生信息系统上云提供基础云平台服务：在云平台层构建较为完整的云管理平台，资源包括但不限于云主机、云存储、云网络、云安全、云等保等云服务，能够满足采购人区域卫生信息系统的部署及后续上线业务应用系统的云资源需求。

2.2 投标人需承诺提供云平台网络安全保障：包括但不限于防火墙、防病毒、安全审计及符合三级等保测评标准的网络安全产品，为采购人业务系统提供云安全服务；项目建成后需达到信息安全等级保护第三级的防护要求；重点解决采购人区域卫生信息系统云业务运行安全、数据库安全、审计安全、数据安全等内容。如在采购人服务期内，属于中标人责任造成的云平台网络安全出现问题，中标人需要全部承担相关法律责任及一切经济损失。

2.3 投标人需提供本地数据中心汇聚机房服务，供采购人汇聚医疗机构专线、云专线等网络出入口的网络安全保护，并提供满足采购人需求的各类网络设备及符合标准的汇聚机房，满足采购人所属医疗机构业务系统使用需求。

2.4 投标人需提供 7*24 小时云运维管理服务：对采购人区域卫生信息系统云平台所有 IT 资源实现统一监控，集中维护；构建 7*24 小时完善的云平台运维服务体系，并为采购人提供一对一专门服务。

2.5 投标人必须负责采购人上云平台的线路、功能联调、网络安全测评，并提供相关的培训，具体要求如下：

2.5.1 线路性能：线路性能的测试过程必须在采购人的参与下进行。测试的过程和结果必须详细记录，经采购人与中标人签字后作为验收的文件之一。

2.5.2 运维服务：投标人应为采购人提供最高级别的服务待遇，并提供一站式服务体系，包括：一站业务受理、一站故障申告、一站技术支持等。为满足采购人在使用过程中提出的需求以及应对可能存在或者发生的故障，需提供相应维护保障服务。服务请求为中标人提供 7×24 小时网络监控服务，并及时向采购人报告异常情况。

2.5.3 应急预案：投标人应为采购人做好各种应急预案，以便在故障发生后及时快速响应，确保采购人云平台的安全、稳定和可靠。

2.5.4 项目管理：投标人应为采购人提交详细工程进度表，投标人应提供齐备的项目团队架构，设置专门的项目负责人，并提供详细的项目团队人员名单和联系渠道，负责项目的协调管理工作。

2.5.5 运维服务报告：在整个运维服务周期内，中标人应与采购人建立完善的沟通协调机制，及时提供运维服务的各种报告。包括每日运维服务日志、重大故障维修报告、每月故障总结报告、每季度的设备和系统管理报告、每季度的系统维护总结报告，有针对性的系统优化方案报告等。此外采购人还可根据实际情况需要，要求中标人就特定事件提交说明报告。中标人应提供各种设备管理的原始数据（包括设备故障数据），接受采购人和监理单位的独立检查。若中标人建立了远程集中的设备管理系统，那么中标人应保证该系统的所有设备维护数据真实，没有被篡改或者删除，并向采购人提供该系统的管理数据。采购人也可以随时检查、使用该系统获取设备管理信息。投标人应在投标文件中提供各种报告的实例样本。

2.5.6 数据中心服务：数据中心服务和运维服务，中标人提供的数据中心机房及相关动力，由中标人提供日常运维服务。机房内所有动力配套设备故障产生的所有费用均由中标人全部承担。为保证数据中心机房的稳定性，中标人必须承诺每年至少三次或以上对采购人所租用的云平台资源内所有设备进行日常维护，并把维护的相关分析报告提供给采购人以做备案。如存在相关的线路或设备故障隐患，中标人需要给出相关的处理意见供采购人参考，并按双方达到的协议由中标人免费进行整改、完善。

2.5.7 在服务期内或服务期满后，如因采购人特殊原因不能继续使用中标人云平台的，中标人需承诺采购人可以无条件随时中止合同，不再支付后期的任何服务费用。同时投标人必须承诺采购人放在云平台中的所有程序、应用、数据等资源在采购人不能继续使用云平台时免费提供符合采购人进行数据迁移的光纤线路，并协助采购人能按时按质把云平台中的所有数据迁移到采购人指定的数据中心中。包括但不限于以下：

2.5.7.1 因上级政策要求需要对采购人云平台进行统筹规划使用的；

2.5.7.2 因政策要求采购人不能使用第三方云平台的；

2.5.7.3 因中标人提供的云平台达不到采购人使用要求的；

2.5.7.4 因中标人提供的云平台严重影响采购人业务系统不能正常运行的；

2.5.7.5 因中标人提供的云平台出现网络安全责任事故的；

2.5.7.6 因采购人数据中心建设项目正常投入使用运行的；

2.5.7.7 因其他不可抗力或双方协商一致需终止合作的情形；

2.5.7.8 其他未在列的特殊原因。

2.5.7.9 上述终止情形发生后，中标人须在收到采购人书面通知之日起 5 个工作日内与采购人签订变更协议。

2.5.8 如在项目服务期满后，因采购人数据中心建设项目未正常投入使用的，采购人可根据数据中心建设项目的实际进度，延长本项目的服务期。中标人须在采购人书面提出延期

申请后 10 个工作日内完成延期协议，并确保延期内的服务标准、服务费用、响应时效及运维质量与原合同完全一致。

3. 技术要求

3.1 投标人所提供的云平台建设方案要充分考虑技术的先进性、实用性、开放性、扩展性和经济性等原则，以便达到既能满足现实应用，又能保护投资的目的。

3.2 投标人提供的云平台方案设计功能齐全、运行高效、使用灵活、维护方便、易于扩展、投资省、安全可靠。

3.3 投标人提供的云平台所在资源池，应具备大规模云主机资源的冗余能力，可满足未来采购人区域卫生信息系统扩容的需求，可满足 2 倍突发资源需求的能力。

3.4 投标人提供的云平台支持专线链路互联，云数据中心从机房、网络、数据、管理等方面都具备安全、可信的服务能力。

4. 投标人报价要求

4.1 投标人需按采购人采购需求一览表逐项报价，按一年使用服务期进行报价。每年支付费用以采购人实际使用云平台资源量为准，一年实际支付总费用不得高于招标时所报的采购总金额。

4.2 服务期内，采购人需申请增加的云资源，相应资源费用应按当年资费进行计费，但不得超过招标时的具体项目报价。

4.3 投标人须承诺云平台资源费用和专线费用随政策资费下调调整采购人资费，并以调整后的资费计算当年支付费用。

4.4 投标人报价包括但不限于劳务支出、加班费、安全保险（包括重病或因公致伤、残、死亡）、劳保福利、材料、机器损耗、税费、管理费、工衣、社会保险、网络切换费、第三方机构或人员验收等一切费用的总和，采购人不再另外支付任何费用。

4.5 投标人的投标报价须以人民币为结算单位。

九、 云资源与配套服务

1. 基本需求

采购人区域卫生信息系统云平台服务资源主要包括但不限于数据库物理机、云服务资源包、存储与备份、云资源网络安全、统一运维管理等，拟以云平台为基础建设一个符合采购人需求的云数据中心做区域卫生信息系统的基础支撑，为采购人区域卫生信息系统的各项业务提供各项基础服务。

1.1 云资源池所在机房的环境要求

指标项	具体要求
机房选址与空间布局要求	投标人所提供的云资源池主机房满足等保三级或以上要求，并提供云平台等保三级或以上认证

	机房的全年服务可用性≥99.99%。
	为了方便采购人日后的部署和维护管理工作，投标人提供的备份云资源池应在与主资源池位于不同的区域范围。
主机房监控	机房环境配备大屏幕监控屏，采用多方位自动化信息集中处理及多媒体信息展示方式；控制台采用 UPS 供电，确保监控业务不中断，高等级保障；对机房的动力、空调、消防、环境等进行全面 24 小时集中式监控。
动力保障	云资源池机房需采用双路市电回路接入、双油机供电、N+1UPS 电源供电；配备后备发电机组；合理规划布置变配电房，确保供电高可用性。
空调系统	机房必须设置机房专用的空调系统，应采取 N+1 冗余备份方式设置，避免出现单点故障；高效制冷，确保温度 23±1℃，相对湿度 40%-55%。
柴油机房	柴油机需在两路市电都掉电情况下≤5 秒自动响应，可持续≥72 小时，确保云资源池供电安全
消防系统	机房需具备早期烟雾探测报警设备，可在火灾发生的不可见烟阶段精准地及早发现与定位。
机房安防	机房需配备专用门禁和 24 小时监控系统。
抗震级别	机房需提供基础设施服务，具备乙级抗震等级以上。
运维保障	提供 7*24 热线人工值守以及响应电话，7*24 全天候技术支持响应。
	机房具备环境智能监控，实现对设备电流量的监控、机房温度监控、机房湿度监控。
	本地应急响应时间≤2 小时

1.2 云平台服务能力要求

指标项	具体要求
云平台服务能力要求	提供的云服务通过 ISO 28000 供应链安全管理体系认证
	云平台通过 CSA C-STAR 云计算安全评估证书 Cloud Control Matrix V4
	云平台达到 SPCA 软件能力成熟度等级评估五级（CNAS）
	云服务商通过信息化工程与技术服务能力评价证书 CN-IETS 1 级
	云平台提供的块存储、对象存储、物理机通过云服务可信安全能力检验
	云服务的提供商具备服务器虚拟化著作权证书

1.3 云资源池服务要求

1.3.1 云资源池服务整体需求

序号	资源名称	备注	
1	数据库物理机	支持安装 Linux 运行 ORACLE 11G 或以上数据库，支持 SQL Server 各版本数据库。数据库容灾体系支持数据库存储双活+定时备份等功能。	
2	云计算资源包	提供专用宿主机，虚拟化后，共计可分配资源 CPU≥1584 核，内存≥4560 GB；支持安装各类主流正版操作系统。	
3	云资源池存储	数据库存储	实际可用空间，超高 IO 类闪存或光纤存储。
		云资源包存储	实际可用空间，高 IO 类光纤或 SAS 类存储。
		备份存储	实际可用空间，SATA 类或同等性能存储。
		历史数据备份存储	对象级 Raid 后实际可用空间。
4	云服务备份	云平台需要提供备份功能，支持基于多云硬盘一致性快照技术的备	

		份服务，并支持利用备份数据恢复弹性云主机数据。
5	云下一代防火墙	用于对云桌面对云上系统访问流量的防护。
6	云资源池抗DDoS防护服务	云平台提供云资源池 Anti DDos 设备。
7	云资源池负载均衡设备	云资源池提供负载均衡功能。
8	云资源池云监控平台	云平台资源池提供云资源池云监控平台。
9	云资源池虚拟化底层防护组件	云平台需要提供云资源池虚拟化底层防护组件。

1.3.2 云资源池资源具体参数要求

1.3.2.1 数据库物理机

设备类型	技术指标
数据库物理机	国际或国内主流品牌物理服务器。单台数据库物理机 CPU≥2 * 14 核，主频≥2.3 GHz；内存≥256GB DDR4
	硬盘：≥2 * 600GB，内置式热插拔，用于做系统启动盘+ SDI
	Raid 卡：≥1 RAID Card，支持 RAID0,1,10,1E 等
	网卡≥4 *10 GE 光口/2 网卡，单台网口数量≥8
	电源模块：≥2000W 双冗余电源
	集群要求：每 4 台数据库物理机做一个集群组，共分为 3 个大集群组，两个大集群组间可以相互冗余，共用两套数据库存储，实现数据库间的集群冗余功能。数据库容灾体系需要达到存储双活+连续备份+定时备份功能。

1.3.2.2 云计算资源包

云计算资源包计费标准按采购人实际使用数量进行实际计费，在付款时中标人需要提供给采购人当年实际使用资源包报告或依据并经采购人签名确认后方可计算实际支付费用。

设备类型	技术指标
云计算资源包	云计算资源包单资源包 CPU≥132 核，内存≥380GB；总可用 CPU 核数≥1584 核，总可用内存≥4560 GB
	宿主机硬盘：≥2* 600GB，内置式热插拔内存
	宿主机 HBA/RAID 卡：1* RAID Card，支持 RAID0,1,10,1E 等模式
	宿主机网卡≥4 *10 GE 光口 / 2 网卡，单台网口数量≥10
	宿主机电源模块：≥750W 双冗余电源

1.3.3 云资源池存储要求

云资源池存储计费标准按采购人实际使用数量进行实际计费，在付款时中标人需要提供给采购人当年实际使用存储量报告或依据并经采购人签名确认后方可计算实际支付费用。

1.3.3.1 数据库存储

指标项	具体要求
基本要求	数据持久性要求≥99.99995%及以上
	硬盘读写时延 0.5ms~2ms
	共享云硬盘最多可挂载≥16 台云主机，可支持物理主机挂载。
	通过数据冗余和缓存加速等多项技术，提供高可用性和持久性。
	支持共享云硬盘，可以创建共享云硬盘，最多同时挂载到多台云主机上。
备份策略	支持云硬盘备份，可以手动执行备份，也可以通过设置备份策略进行自动备份。
IOP	单盘 IOPS≥20000
吞吐量	单盘最大吞吐量≥350MB/s
容量	单盘最大容量≥32TB

1.3.3.2 云资源包存储

指标项	具体要求
基本要求	数据持久性要求≥99.99995%及以上
	硬盘读写时延在 1ms~3ms
	共享云硬盘最多可挂载≥16 台云主机上，可支持物理主机挂载。
	通过数据冗余和缓存加速等多项技术，提供高可用性和持久性。
	支持共享云硬盘，可以创建共享云硬盘，最多同时挂载到多台云主机上。
备份策略	支持云硬盘备份、手动执行备份，支持设置备份策略进行自动备份。
IOP	单盘 IOPS 最大≥3000
吞吐量	单盘最大吞吐量≥150MB/s
容量	单盘最大容量≥32TB

1.3.3.3 备份存储

指标项	具体要求
基本要求	数据持久性要求≥99.99995%及以上
	硬盘读写时延在 5ms-10ms
	共享云硬盘最多可挂载≥16 台云主机上，可支持物理主机挂载
	通过数据冗余和缓存加速等多项技术，提供高可用性和持久性。
	支持共享云硬盘，可以创建共享云硬盘，最多同时挂载到多台云主机上。
备份策略	支持云硬盘备份、手动执行备份，支持通过设置备份策略进行自动备份。
IOP	单盘 IOPS 最大≥1000
吞吐量	单盘最大吞吐量≥90MB/s
容量	单盘最大容量≥32TB

1.3.3.4 历史数据备份存储

指标项	具体要求
基本要求	备份对在线业务运行无影响，无需停机。首次为全量备份，后续增量备份节约存储空间，存储空间按需分配，弹性扩展，缩短备份时长、降低初期投资。
	支持一次性备份和周期性备份。一次性备份是指用户手动创建的一次性备份任务。周期性备份是指采购人通过创建备份策略并通过备份主机的方式创建的周期性备份任务。
	数据自动加密保存到对象存储中，数据持久性≥99.999999999%（11 个 9）。
备份策略	增量备份，缩短大量备份时长，存储空间按需分配；增量恢复，仅恢复到最近一个备份时间点的变化数据，恢复效率≤1 分钟。投标人需要提供一台云主机用于对采购人的历史数据备份进行恢复，并能保证恢复后的数据与能在采购人的应用中正常使用。

1.3.3.6 云业务备份

基本功能	备份配置方式：一次性全量备份和周期性增量备份
	备份恢复：全量和增量备份都可以快速、方便的将数据恢复至备份副本所在时刻的状态。
	备份安全：云主机备份通过云主机与对象存储的结合，将数据库物理机及云主机的数据备份到对象存储中，保障采购人的备份数据安全
	不能与数据库物理服务器、云计算资源包不能位于同一机房的同一集群内

1.3.3.7 云资源池抗 DDoS 防护服务提供不低于 50Gbps 的抗 DDoS 防护能力

设备类型	技术指标
云资源池 Anti DDos 设备	扩展槽位≥8
	扩展接口板：FW-LPUF-120≥2 个子槽位 ，FW-LPUF-240≥2 个子槽位
	扩展子口：≥24 x GE (SFP); 5 x 10GE (SFP+); 6 x 10GE (SFP+); 12 x 10GE (SFP+); 1 x 40GE (CFP); 1 x 100GE (CFP)
	协议滥用类攻击防护功能：LAND；Fraggle；Smurf；Winnuke；Ping of Death；Tear Drop；TCP Error Flag 等攻击
	提供的设备每秒清洗流量不少于 5G
	Web 应用防护功能：HTTP Get Flood；HTTP Post Flood；HTTP Slow Header；HTTP Slow Post；HTTPS Flood；SSL DoS/DDoS；WordPress 反射放大攻击；RUDY；LOIC；支持报文合法性检查。
	扫描窥探型攻击防护功能：端口扫描；地址扫描；TRACERT 控制报文攻击；IP 源站选路选项攻击；IP 时间戳选项攻击；IP 路由记录选项攻击等。
	DNS 应用防护功能：DNS Query Flood；DNS Reply Flood；DNS 缓存投毒攻击；支持源限速。
	网络型攻击防护功能：SYN Flood；SYN-ACK Flood；ACK Flood；FIN Flood；RST Flood；TCP fragment Flood；UDP Flood；UDP Fragment Flood；IP Flood；ICMP Flood；TCP 连接耗尽攻击；Sockstress；TCP 重传攻击；TCP 空连接攻击。
	SIP 应用防护功能：SIP Flood/SIP Methods Flood 防范，包括：Register Flood；Deregistration Flood；Authentication Flood；Call Flood；支持源限速。
	UDP 反射放大攻击防护功能：NTP 反射放大；DNS 反射放大；SSDP 反射放大；Chargen 反射放大；TFTP 反射放大；SNMP 反射放大；NetBIOS 反射放大； QOTD 反射放大；Quake Network Protocol 反射放大；Portmapper 反射放大；Microsoft SQL Resolution Service 反射放大；RIPv1 反射放大；Steam Protocol 反射放大。
	过滤器功能：支持 IP 报文过滤器；TCP 报文过滤器；UDP 报文过滤器；ICMP 报文过滤器；DNS 报文过滤器；SIP 报文过滤器；HTTP 报文过

	滤器。
	地理位置过滤功能：支持基于源 IP 的地理位置进行阻断、限速。
	攻击特征库功能：支持 RUDY；slowhttptest；slowloris；LOIC；AnonCannon；RefRef；ApacheKill；ApacheBench；支持每周自动更新。
	IP 信誉功能：支持每日自动更新，快速阻断攻击；支持本地业务访问 IP 信誉，支持基于本地业务访问会话建立动态 IP 信誉，快速转发业务访问流量，提升用户体验。

1.3.3.8 云资源池云监控平台

基本功能	为采购人所使用的多种云产品提供监控：支持对弹性云主机、云硬盘、弹性负载均衡、RDS、弹性伸缩服务、可以通过实例监控查看已使用的各服务实例的历史性能数据曲线，系统会自动识别用户已试用的实例，无需采购人手动添加、无需额外安装其他插件。
	多指标监控：支持针对云主机、云硬盘、弹性伸缩和 RDS 几类产品进行多个性能指标的数据监控，为用户提供性能历史曲线，多维度监控资源动态。 产品的监控指标展示包括但不限于： 云主机指标：支持对 CPU 使用率、内存使用率、网络流出速率、网络流入速率、磁盘写操作速率、磁盘写速率、磁盘使用率、磁盘读操作速率、磁盘读速率等指标监控。 弹性伸缩指标：支持实例数指标监控。 云硬盘指标：支持对磁盘写操作速率、磁盘写速率、磁盘读操作速率、磁盘读速率等指标监控。 虚拟私有云指标：支持对上行带宽、下行带宽等指标监控。
	支持查看和导出监控数据包括但不限于： 用户可登录控制中心查看一个月内的监控数据，可自定义数据查看时段、原始数据聚合时段以及原始数据聚合方式。支持用户导出 2 天内的原始监控数据。 支持查看历史监控数据时提供了监控固定时长和自定义时长两种方式。 固定时长支持最近 3 小时、12 小时、24 小时、1 周、1 个月等时间段，作为用户监控周期。 自定义时长支持用户在最近一个星期内选择检测时间起点和终点，作为用户监控周期。
	告警规则包括但不限于： 云监控可设置自定义告警规则，对云主机进行全面有效监控。当告警规则被触发时，平台将显示告警提示，并以短信或邮件的方式为用户发送告警通知。 用户在添加告警规则时，单个指标可以选择多个实例、达到批量添加监控对象的目的。 当告警规则对应的实例不再使用或已被删除，可手动删除该告警规则。
	提供具有云资源池云监控平台的全控权限，可根据采购人的需求自行定义策略。

1.4 云桌面物理服务器具体参数要求

设备类型	技术指标
数据库物理机	支持国际或国内主流品牌物理服务器。单台数据库物理机 CPU≥2 * 14 核，主频≥2.3 GHz；内存≥192GB DDR4
	硬盘：≥2 * 600GB，支持内置式热插拔，用于做系统启动盘+ SDI；
	Raid 卡：≥1 * RAID Card，支持 RAID0,1,10,1E 等
	网卡≥4 *10 GE 光口/2 网卡，单台网口数量≥8
	电源模块：≥2000W 双冗余电源

十、 网络服务

为保证采购人数据中心汇聚机房和云平台的对接，保证网络的可靠性及稳定性，保证物理链路的冗余，避免单节点故障，投标人需要提供 2 条云平台专用光纤电路；同时为保证采购人的应用，中标人需要在汇聚机房中提供两条对外服务网络出口。

1.网络需求

序号	名称	具体要求	数量	单位
1	云平台专用光纤电路	连接采购人数据中心汇聚机房和云平台，对称带宽≥1Gb	2	条
2	云桌面专用光纤电路	用于连接数据中心汇聚机房和云桌面，对称带宽≥1Gb	1	条
3	对外服务网络出口	对称速率，出入方向吞吐量≥200Mb,提供 8 个固定 IP 地址	2	条
4	数据备份专用电路	用于连接数据备份服务器	2	条

2.云平台专用光纤电路需要提供双物理路由冗余备份。

3.技术参数要求

3.1 云平台专用光纤电路和云桌面专用光纤电路要求如下：对称带宽≥1Gb，专享网络带宽，点对点独享。对外服务网络出口出入方向吞吐量≥200Mb。

3.2 云平台专用光纤电路吞吐量为 100%，平均时延≤20ms；平均丢包率≤0.1％；网络可用率＞99.9％，上行带宽和下行带宽对称。

3.3 互联网出口光纤电路吞吐量为 100%，平均时延≤20ms；平均丢包率≤0.1％；网络可用率＞99.9％，上行带宽和下行带宽对称。

3.4 数据备份专用电路吞吐量为 100%，平均时延≤20ms；平均丢包率≤0.1％；网络可用率＞99.9％，上行带宽和下行带宽对称。

4.电路测试内容

投标人应在投标响应文件中对电路性能测试给出具体测试的内容和方法。测试内容至少

包括电路网络性能测试、带宽和网络通信压力测试、故障恢复测试等内容。

5.电路测试标准

要求投标人对各线路网络性能的测试至少要包括但不限于以下指标，并达到相关要求：

5.1 云平台专用光纤电路平均时延≤3ms；互联网出口光纤电路平均时延≤20ms。

5.2 当光纤电路发生故障时，主备用电路切换时间（自愈时间）<50ms。

5.3 线路丢包率<0.1%。

6.测试确认

测试过程必须在采购人的参与下进行，测试的过程和结果必须详细记录，经采购人和中标人双方盖章签字确认后作为验收文件之一。

7.运行要求

光纤电路需要满足等保三级要求。如采购人在无增加云平台服务资源的情况下，中标人提供的云平台专用光纤电路和互联网出口光纤电路在传输时延率及采购人使用系统达不到要求时，采购人需与中标人进行协商解决，并达到采购人的正常使用要求。

8.投标人需承诺提供的清远市级线路到主云资源池主机房的主核心线路带宽速率必须≥100Gb，提供给采购人使用的线路带宽速率达到瓶颈时自动扩容；投标人提供的主云资源池与备份云资源池之间的主核心线路带宽速率必须≥10Gb。投标人所提供的光纤电路必须要保证与采购人现有下属所有医疗机构原有的各类线路的连通，并保证系统的正常使用。同时投标人需承诺采购人上云平台后，采购人原有医疗机构对接上级平台或系统的专线或线路能保证与云平台的正常接入。

十一、 测评服务

1. 服务要求

1.1. 等级保护测评服务

网络安全等级保护测评包括两个方面的内容：一是安全控制测评，主要测评项目的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

安全控制测评使用测评单元方式组织，分为安全技术测评和安全管理测评两大类。

安全技术测评包括但不限于：安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等的安全控制测评；安全管理测评包括但不限于；安全管理制度、安全管理机构、安全管理人员、安全建设管理和系统运维管理等的安全控制测评。

安全技术测评通过人员访谈、文档审查和实地察看的方式测评，安全管理测评通过人员

访谈、文档审查的方式测评。

1.1.1. 等级保护测评对象

（1）机房环境、配套设施；

（2）整体网络拓扑结构；

（3）网络设备：包括但不限于路由器、核心交换机、汇聚层交换机、无线网络设备、无线接入设备等；

（4）安全设备，包括但不限于网闸、防火墙、IDS/IPS、防病毒网关、防垃圾邮件网关、抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、无线接入网关等；

（5）安全管理中心：包括但不限于安全运维管理系统、数据库审计系统、综合安全审计系统、综合网管系统等；

（6）数据库、中间件、终端设施（包括移动终端）、服务器等；

（7）业务应用软件、系统管理软件；

（8）重要管理终端；

（9）网络管理员、系统管理员、审计管理员、业务管理员和安全管理员、安全主管等；

（10）涉及到系统安全的所有管理制度、操作规程和记录等。

1.1.2. 等级保护测评的其他技术服务

在等保测评需要进行渗透测试来辅助完成项目整体网络的等保测评工作，对操作系统、数据库、Web 发布系统、Web 程序等层面存在的安全漏洞进行准确查找，同时利用渗透性技术检测，发现未知应用系统漏洞和安全隐患。包括但不限于弱口令、本地权限提升、远程溢出、数据库查询等。渗透测试结束后提供详细的渗透测试报告，并在报告中给出漏洞修复建议。

1.1.3. 交付物

服务中产生的全部档案资料版权归采购方所有，中标人未经采购方允许的情况下，不得以任何形式向第三方提供安全技术文档的全部或部分内容，交付文件包括但不限于如下成果和报告：《网络安全等级保护测评报告》、《获得公安部门的《信息系统安全等级保护备案证明》、《报告回执》。

1.2. 密码应用安全性评估服务

1.2.1. 商用密码总体要求评估

密码算法合规性评估：本项目商用密码应用关于信息系统使用的密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。

密码技术合规性评估：本项目商用密码应用关于信息系统使用的密码技术是否遵循密码

相关国家标准和行业标准。

密码产品合规性评估：本项目商用密码应用关于信息系统使用的密码产品与密码模块是否通过国家密码管理部门核准。

密码服务合规性评估：本项目商用密码应用关于信息系统使用的密码服务是否通过国家密码管理部门许可。

1.2.2. 密码技术应用评估

从物理和环境、网络和通信、设备和计算、应用和数据 4 个层面对商用密码应用关于信息系统的密码技术设计情况进行分析与评估。

物理和环境密码安全设计评估:分析评估密码应用是否合理、合规的利用商用密码完整性、真实性功能，对影响信息系统安全防护效能的物理和环境层面因素是否得到有效控制。

网络和通信密码安全设计评估:分析评估密码应用是否合理、合规的利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的网络和通信层面因素是否得到有效控制。

设备和计算层面评估:分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的设备和计算层面因素是否得到有效控制。

应用和数据层面评估:分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性以及不可否认性功能，对影响信息系统安全防护效能的应用和数据层面因素是否得到有效控制。

1.2.3. 安全管理评估

分析评估本项目商用密码应用对影响商用密码防护效能的管理制度与措施是否进行规划和设计。管理制度与措施包括但不限于：安全管理制度，密钥管理、人员管控，信息系统实施，应急预案等。

1.2.4. 交付物

项目成果包括但不少于下列文档：《商用密码应用安全性评估报告》

1.3. 服务依据

在本项目测评过程主要执行标准如下：

1. 《中华人民共和国网络安全法》
2. 《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》
3. 《GB/T25070-2019 信息安全技术 网络安全等级保护安全设计技术要求》
4. 《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》
5. 《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》

6. 《GB/T 39786-2021》《信息安全技术 信息系统密码应用基本要求》

7. 《GB/T 43206-2023》《信息安全技术 信息系统密码应用测评要求》

8. 《GM/T 0116-2021》《信息系统密码应用测评过程指南》

9. 《政务信息系统密码应用与安全性评估工作指南》

10. 《商用密码应用安全性评估测评作业指导书（试行）》

11. 《商用密码应用安全性评估量化评估规则》

12. 《信息系统密码应用高风险判定指引》

1.4. 服务原则

项目的方案设计与实施应满足以下原则：

符合性原则：应符合国家信息安全等级保护制度及密码法相关法律法规。

标准性原则：方案设计、实施与网络安全体系的构建应依据国内、国际的相关标准进行。

规范性原则：项目实施应由专业的测评师依照规范的操作流程进行，在实施之前将详细量化出每项测评内容，对操作过程和结果提供规范的记录，以便于项目的跟踪和控制。

可控性原则：项目实施的方法和过程要在双方认可的范围之内，实施进度要按照进度表进度的安排，保证项目实施的可控性。

整体性原则：等级保护测评、商密评估的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。

最小影响原则：项目实施工作应尽可能小的影响网络和信息系统的正常运行，不能对信息系统的运行和业务的正常提供产生显著影响。

保密原则：对项目实施过程获得的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据和结果进行任何侵害客户利益的行为。

同时，在测评实施的过程中遵循以下原则：

客观性和公正性原则：虽然测评工作不能完全摆脱个人主张或判断，但测评人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

经济性和可重用性原则：基于测评成本和工作复杂性考虑，鼓励测评工作重用以前的测评结果，包括商业安全产品测评结果和信息系统先前的安全测评结果。所有重用的结果，都应基于结果适用于目前的系统，并且能够反映出目前系统的安全状态基础之上。

可重复性和可再现性原则：不论谁执行测评，依照同样的要求，使用同样的测评方式，对每个测评实施过程的重复执行应该得到同样的结果。前者与不同测评者测评结果的一致性有关，后者与同一测评者测评结果的一致性有关。

结果完善性原则：测评所产生的结果应当证明是良好的判断和对测评项的正确理解。测评过程和结果应当服从正确的测评方法以确保其满足了测评项的要求。

十二、 数据迁移服务要求

1.服务要求

系统数据迁移为了充分保护、继承原有系统的信息资料和成果，保证既往的历史信息与新系统延续性，更好地利用原有系统的信息资料，防止因为新的系统上线而影响正常工作。基于上述目的，要求对现有数据进行仔细的分析、整理、审核，同时要对现有的数据进行进一步规范和标准化，以适应系统信息化不断发展的需求，以及适应新的系统的要求。对数据转移的策略与原则：

(1)基本保证转移数据和原数据的一致性；

(2)尽可能采用数据自动转换，以减少用户重新输入数据的需求；

(3)减少用户的重复劳动；

(4)降低数据转换成本和周期；

(5)保证历史信息的继承性。

1.1 资源保护原则

(A)必须保证原系统数据的正确性和准确性。

(B)对原有系统的数据在一段时间内进行保护。

(C)当原有系统的基础数据发生变化时进行并行维护。

1.2 数据过滤原则

(A)在不影响新系统运行的前提下，放宽数据过滤条件。

(B)对于错误的数据分错误级别进行标识，方便手工调整数据。

(C)对于过时的无用的数据，通过一定的条件进行筛选。

(D)对于有些数据，严重影响系统运行的，则必须在转换前进行处理。

(E)对于新系统中需要的关键数据，原系统中不存在或者不满足的，需要在数据转换前手工补录。

(F)对于原系统拥有，但新系统不需要的数据，不进行转换。

(G)对于原系统有严重错误数据，不进行转换。

1.3 数据照搬原则

对原系统的数据，原则上不要做修改或拆分，在必要的情况下，可对原数据进行调整，以满足新系统的需要。

1.4 新原系统对照原则

(A）在原系统中的数据在新系统找不到对应表，如不是关键数据的，在新系统中用不着，可不进行转换。

(B）对于新系统要使用的数据，如原系统这边没有对应表，在数据转换前要进行手工维护，确保数据的正常对照。

(C）当原系统中的字段长度比新系统对应字段的长度长，如不是关键字段的，新系统应修改字段长度；如是关键字段的，则需要进行截取或者改用其他不重要的字段进行存取。