第三章　采购需求

前提：本章中标注“★”的条款为本项目的实质性条款，若投标人不满足的，投标文件按无效处理；标注“▲”的条款为本项目的重要条款，若投标人不满足的，将在详细评审中扣分。

一、项目分包情况

标包编码	采购标的名称	数量	单位	单品目采购预算及最高限价（人民币/元）	单包采购预算及最高限价（人民币/元）	本项目采购预算及最高限价（人民币/元）	采购标的所属行业
SCIT-HNZG-2023080007-A包	云资源服务	1	项	1360000.00	3154900.00	5146900.00	软件和信息技术服务业
	云安全服务	1	项	490900.00			
	云密码服务	1	项	200000.00			
	云专线	1	项	1104000.00			
SCIT-HNZG-2023080007-B包	等保测评服务	1	项	720000.00	720000.00		
SCIT-HNZG-2023080007-C包	密码测评服务	1	项	840000.00	840000.00		
SCIT-HNZG-2023080007-D包	线路租赁 1	1	项	216000.00	216000.00		信息传输业
SCIT-HNZG-2023080007-E包	线路租赁 2	1	项	216000.00	216000.00		

二、技术、服务及商务要求

（一）项目概述

1.项目名称：瑞金海南医院购买基础信息化服务项目

2.服务地点：上海、海口、琼海

3.项目工期：36个月

4.资金来源：财政资金

5.标的内容：本次项目由采购人统筹规划，亟需采购三年信息化服务保障采购人的系统正常运行，切实提高医院的信息化水平和医疗服务水平。

服务的具体内容如下：

（1）A包:云资源服务（工期12个月）、云安全服务（工期12个月）、云密码服务（工期12个月）、云专线（工期12个月、36个月）

（2）B包:等保测评服务

（3）C包:密码测评服务

（4）D包:线路租赁1

（5）E包:线路租赁1

（二）服务目标

按照《海南自由贸易港建设总体方案》中“提升乐城先行区发展水平”的要求，围绕“让国人尽快用上全世界最先进的药械、推动中国健康产业发展、助推中国医疗卫生事业改革”三大使命，聚焦医疗卫生供给侧结构性改革、医院共享模式和机制、病人服务保障、监管体制优化等创新“四要素”，结合《智慧海南总体方案（2020-2025年）》中关于“5G和物联网等新型基础设施建设工程”的发展方向，依托上海交通大学医学院附属瑞金医院海南医院暨海南博鳌研究型医院（以下简称“医院”）一院两区的蓝图规划，本项目主要达成以下目标：

1.瑞金海南医院承载着引入高端医疗资源，实现瑞金总院“人才、技术、管理、品牌”向瑞金海南医院平移，在智能影像、智能病理、智能心电、智能超声、云检服务、药学服务、一体化ICU、实时多学科会诊等应用上，能够利用现有优质医疗资源和新型技术手段，将服务延申到乐城园区，提高区域整体医疗服务水平。

2.医院内部信息化建设刚起步，需要建立一套全面支撑医院开展日常诊疗服务、检验检查、运营管理、后勤管理等基础业务场景的基础信息化系统，因此，根据需求结合实际，需提供瑞金海南医院开院必备的25个业务系统服务，参照上海瑞金总医院的标准进行逐步完善建设，同时兼顾考虑本地医院侧的网络调整及安全，以满足医院各项业务的顺利开展。

3.本项目提供服务后，将实现院内信息互联互通并和海南省卫健委“三医联动”平台之间相关数据平台实现互联互通、数据共享。

4.实现医院核心医疗业务信息和病患个人隐私信息安全保障，符合信息安全等级保护2.0和密评相关要求。

（三）项目服务内容

1.购买云资源服务（云服务、云安全服务、云密码服务、云专线）

2.购买等保测评服务

3.购买密码测评服务

4.线路租赁1

5.线路租赁1

A包：云资源服务等

一、分包名称

A包：云资源服务等，标包编号：SCIT-HNZG-2023080007-A包。

二、采购需求

2.1 购买云服务需求

2.1.1 云资源需求

需设计满足本系统的建设所需的硬件资源，云平台应至少可提供IaaS层服务，即支持将基础设施资源（计算、存储、网络带宽等）进行虚拟化和池化管理，实现资源的动态分配、再分配和回收。

云平台可以根据服务需求分配指定的软件（包括操作系统、数据库系统）、计算、存储和网络等资源；提供虚拟机的批量部署功能，能够根据用户要求执行。

虚拟机的启动、停止、重新启动、状态查询、创建模板、模板创建虚拟机等功能。

2.1.2 云服务器需求

支持开通规格可选的云服务器资源，操作系统、系统盘、数据盘、专有网络VPC、安全组、弹性公网IP、IPv6带宽以及设置云服务器的实例名称、登录密码。

支持在线变更云资源规格与云服务器的计费方式,如临时增大服务器硬件性能、增加带宽，并保证在10分钟内完成资源调整。

2.1.3 操作系统需求

支持Linux和Windows操作系统版本，包括CentOS，Ubuntu，Windowsserver2019等，提供在线版本切换。

2.1.4 块存储需求

提供多种形式的块存储服务，存储介质要求支持磁性介质和SSD，以满足不同业务场景的需求。

2.1.5 对象存储需求

支持标准RESTfulAPI接口（兼容AmazonS3API）、丰富的SDK包、控制台；

支持上传、下载文件、管理用于静态Web网站的海量数据；

支持灵活的鉴权、授权机制，支持Bucket以及每个单独文件的读写权限，提供防盗链功能，可屏蔽恶意来源的访问；支持数据SSL加密传输，保证数据安全。

2.1.6 网络需求

支持多种网络接入模式，包括互联网、物理专线以及其他接入；支持将专有网络与物理网络或者不同专有网络之间连接起来，组成一个虚拟的混合网络。

虚拟私有网络支持：云上允许自定义多个互相隔离的网络地址段，支持通过设置路由、访问控制列表（ACL）、防火墙等方式实现外网区、DMZ区、内网区等网络分区和访问控制设置。

2.1.7 备份需求

支持为云服务器下的所有云盘提供手动或自动的在线备份，无需关机；支持对云服务器实时增量备份、恢复数据的能力。

2.1.8 云安全服务需求

需提供25个业务系统云安全服务，按照网络安全等级保护要求根据系统的等级要求进行云安全防护。

2.1.9 应用支撑服务需求

包含云服务与医院系统的互联互通、数据库平台、统一用户、统一门户、权限与认证、数据交换与共享、资源上传下载、更新、与存储服务、缓存服务、查询、展现、过程监督等在内的应用支撑服务。

2.2 密码应用建设需求

《中华人民共和国密码法》中强化了密码应用要求，突出密码应用监管，重点面向关键信息基础设施和网络安全等级保护第三级以上系统，落实密码应用安全性评估和国家安全审查制度。

《GM/T0054-2018信息系统密码应用基本要求》要求所有级别信息系统都应该满足密码算法、密码产品、密码服务的合规性要求。

1、密码算法：应符合国家法律法规及密码国家标准、行业标准要求。一般情况下采用我国公开的SM2、SM3、SM4、SM9算法。

2、密码产品：应通过国家密码管理部门核准。选用获得国家密码管理局颁发的型号证书的产品。

3、密码服务：应通过国家密码管理部门许可。对于电子签名服务、密码服务等新的密码服务应获得许可。

第一年需要对同期工程购买的信息系统服务：门急诊住院管理系统（HIS）、影像管理和报告系统、实验室管理系统、门户网站、患者移动助医系统、互联网医院进行密码应用改造，建设符合《中华人民共和国密码法》以及GB/T39786-2021《信息安全技术信息系统密码应用基本要求》的信息系统，实现对保护对象（重要业务数据、鉴别数据、重要审计数据等）的机密性、完整性、真实性保护。

2.3 网络和部署需求

为了满足瑞金海南医院—云资源的数据传输访问、瑞金海南医院-医疗云（主）、瑞金海南医院-瑞金总院、瑞金海南医院-医疗云（备）访问需求，本次需新建网络线路部分如下：

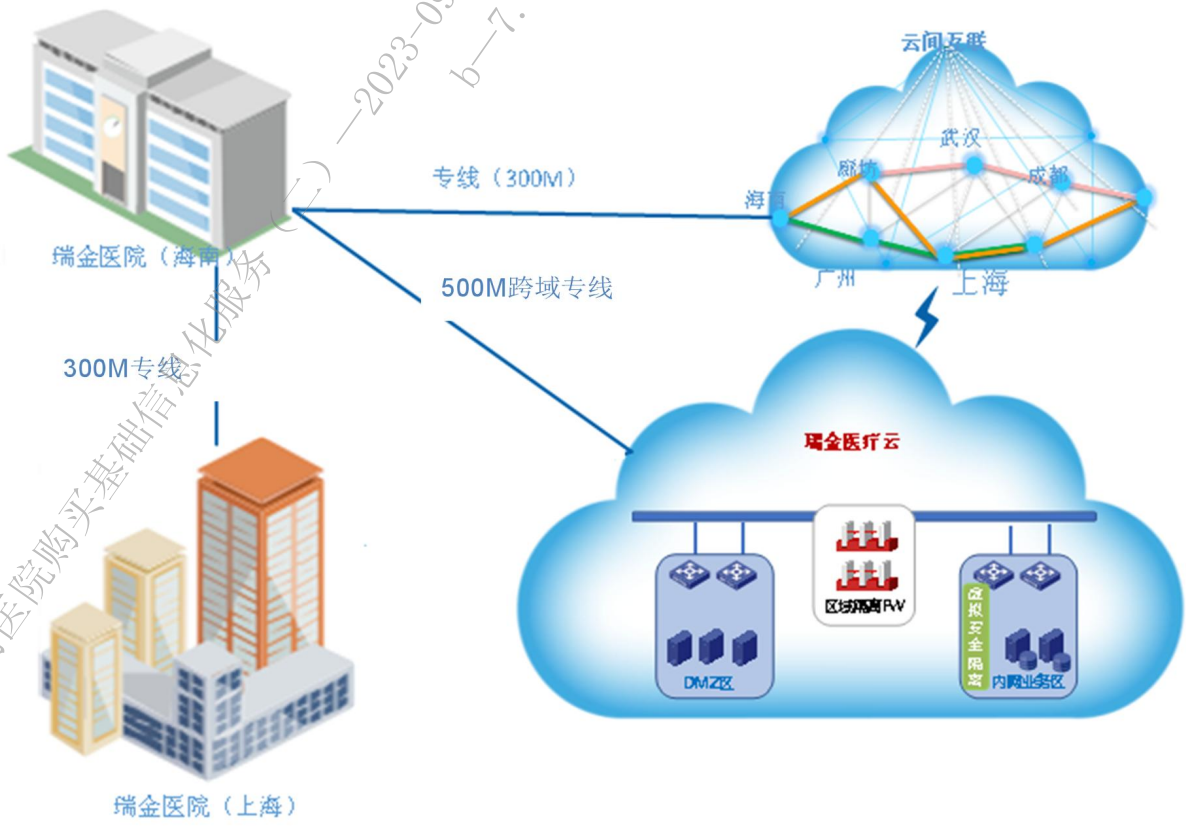
线路类别	地址	数量	带宽
云专网	瑞金海南医院-医疗云 300M	1	300M
点对点专线	瑞金海南医院-医疗云 500M	1	500M
点对点专线	瑞金海南医院-瑞金总院 300M	1	300M

三、服务要求

（一）基本要求

1. 整体架构

本次提供云服务资源架构如下图所示，本项目承接海南院区业务上云需求以应对医疗信息系统敏捷化弹性化需求。



1.1专线需求：

1.1.1瑞金总院和海南分院之间建设点对点300M专线；

1.1.2海南分院与瑞金医疗专有云建设点对点500M专线；

1.1.3海南分院与瑞金医疗专区建设300M专线备份线路以保障业务高可用；

1.2云资源需求：

1.2.1基于信息共享和资源有效利用的基础上，应标单位方案需满足网络即插即用，计算资源可按需分配。随医院上云的需求，网络需具备单节点弹性可扩容，灵活部署，多节点上云可统一管理，灵活部署新增医院节点网络资源，通过部署网络及安全配置，实现对医院云资源的安全访问。可以快速分配云医院的所有服务器、存储、网络、安全、备份设备具备高可靠性及冗余性避免单点故障，避免建设周期、到货周期、部署实施周期等长时间的项目过程，做到实施快捷高效。

1.2.2 投标人提供的云服务资源需满足以下要求

（1）▲大陆地区各省、自治区、直辖市均有云资源池，支持后续异地机房数据级备份的服务要求。（在全国31个省的云资源池具备根据医院需要在全国每个省随时开通云资源的能力，可提供每个省云资源池的证明材料，包括官网的云平台可用区域列表截图及相关证明文档）

（2）▲云平台具备国产化硬件软件适配能力，完成主流硬件厂商（例如鲲鹏、曙光、飞腾、等信创产品）兼容性测试并提供测试报告或兼容性证明。云平台完成主流信创操作系统（例如统信、中标麒麟、银河麒麟等）兼容性测试并提供测试报告或兼容性证明。

（3）云平台满足国家信息安全等级保护等级保护三级评审，并提供相关证明。

（4）▲投标人具有云服务数据的保护能力，通过可信云的评估，达到增强级及以上，并提供相关证明。

2.资源及服务的主要规格参数及技术要求

（1）医疗专有云机房环境

（2）数据中心机房满足T3+标准

（3）云平台满足等级保护三级标准

（4）机房具体环境指标如下：

编号	项目	参数要求
1	环境要求	温度：开机时23°C±1°C，停机时5°C～35°C；相对湿度：开机时40%～55%，停机时40%～70%；温度变化率＜5°C/h，不得结露。
2	结构	抗震：乙级以上，机房活荷载标准值≥6kN/m²，电池室≥8kN/m²，机房外墙不宜设采光窗，耐火等级：一级。
3	后备用电供电电源	主机房由至少2个变电站、至少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，切换时间小于4毫秒，供电系统可用性（由市电至机柜计算）≥99.99%，单相负荷应均匀地分配在三相线路上，并应使三相负荷不平衡度小于20%。
		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小时以上。
4	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类标准以上。
5	无线电干扰场强接地	接地电阻≤1欧姆，接地电位差<1V。
		在频率为0.15～1,000MHz时，不应大于126dB。
6	内磁场干扰	主机房内磁场干扰环境场强不应大于800A/m。
7	静电电位	主机房内绝缘体的静电电位不应大于1kV。
8	机房布线	采用光缆或六类及以上对绞电缆，采用1+1冗余。
9	照明要求	眩光限制按I级以上标准，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。
10	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、新风、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。
11	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，投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。
12	消防	应配置气体消防系统和火灾自动报警系统。

2.1 云服务器资源

（1）云服务器（ECS）需满足以下需求：

编号	功能/特性	参数要求
1	登录方式	支持密码、密钥对方式登录。
2	多架构支持	支持x86计算、arm架构、异构计算GPU。
3	实例管理	1）支持对云服务器的创建、删除、变更规格、开机、关机、重启、重置远程连接密码、挂载云硬盘、变更安全组、变更操作系统、绑定/解绑EIP，创建镜像、创建快照，同步云平台数据等；
		2）支持对创建的实例在控制台进行管理，可通过IP、ID进行查看、检索。
4	镜像可选	支撑创建时可选镜像，支持私有镜像上传。
5	数据盘挂载	支持挂载多块数据盘。
6	IPv4/IPv6	支持IPv4/IPv6双栈，支持绑定、解绑。
7	反亲和性	支持虚拟机组管理功能，可以将虚拟机创建到不同宿主机。
8	资源组	支持创建资源组，通过资源组功能可管控不同用户管理不同的云服务器资源。
9	专属宿主机	创建云服务器时支持选择专属宿主机。
10	网卡管理	支持绑定/解绑辅助网卡，更改辅助网卡对应的安全组策略，或针对未关联实例的网卡进行销毁操作。
11	资源动态调整	支持在线虚拟机资源热添加，可以在线调整虚拟机的CPU、内存、硬盘等资源。
12	安全组	提供安全组管理功能，创建安全组，灵活配置安全组规则，并支持查看安全组所关联的云服务器ECS实例信息、辅助网卡信息；支持导入/导出安全组规则。
13	虚拟机回收站	支持虚拟机回收站功能，防止用户误删除，虚拟机在回收站中不占用系统资源。

14	监控功能	支持查看云服务器ECS的CPU使用率、内存使用率、云盘使用率、云盘读/写带宽、云盘读/写IOPS、流入速率、流出速率监控信息。
15	操作日志	支持区分时间段、区分云产品查看、导出操作日志。

2.2. 云存储资源

（1）块存储（BSS）需满足以下需求：

编号	功能/特性	参数要求
1	基本功能	1）用户可以将单独创建的数据盘挂载到ECS实例上。
		2）用户可以将数据盘从ECS实例上卸载下来。
		3）当云盘容量不满足业务需要时，用户可进行弹性扩容。
		4）云盘、快照创建完成后可以修改名称。
2	快照	1）用户可以创建快照来快速保存指定时刻云盘的数据。
		2）用户可以通过快照创建新云盘，新云盘在初始状态就具有快照中的数据。
		3）一旦升级或迁移过程中出现问题，用户可以通过快照及时将业务恢复到快照创建点的数据状态。
		4）用户可以删除不再需要的快照。
3	性能监控	提供包括云盘读写带宽、IOPS等基本性能监控信息。
4	单盘最大IOPS	高效云盘3000、全闪云盘25000。
5	最大吞吐量（MB/s）	高效云盘60、全闪云盘260。
6	访问时延（ms）	高效云盘10~12、全闪云盘4~6。
7	超大容量需求	可提供超数据盘最大可支持32T。
8	高可靠性	采用三副本机制，数据存储的持久性可达99.9999999%，服务可用性99.95%。
9	弹性可扩展	支持通过单台云服务器挂载多块云硬盘的方式扩展存储空间，同时支持对单块云硬盘进行在线扩容。

（2）对象存储（OSS）需满足以下需求：

编号	功能/特性	参数要求
1	存储空间管理	存放对象的容器。OSS提供创建、查看、删除、列举Bucket等功能。
2	对象管理	用户存储在OSS中的每个文件都是一个对象（Object）。OSS提供上传、下载、列举、分段上传、复制、Post表单上传、分享对象URL等功能。
3	权限管理	OSS支持通过用户身份管理与访问控制服务（IAM）、Bucket权限管理、Object权限管理等方式进行权限访问控制。用户可根据需要灵活配置资源的读写权限
4	生命周期管理	通过生命周期规则，用户可以将Bucket内过期的Object、碎片、历史版本删除
5	静态网站托管	用户可以将静态网站上的内容放到OSS存储空间中，通过配置存储空间的静态网站托管功能，让OSS根据配置的规则展现静态网站上的内容，实现在OSS上托管静态网站。
6	跨域资源共享	跨域资源共享是HTML5提供的标准跨域解决方案，OSS支持CORS标准来实现跨域访问。
7	防盗链	OSS支持基于HTTPReferer请求头的防盗链方法。
8	图片处理	OSS提供灵活、多样、实时的图片处理服务，用户可将原始图片上传到OSS中，通过在请求URL中增加处理参数，即可实时对图片进行处理，包括图片缩放、格式转换，添加水印等功能。
9	日志管理	日志管理功能可以记录访问指定Bucket时的详细信息，日志以对象形式存储在用户指定的Bucket中，可对请求进行分析或者审计。

10	版本控制	OSS支持版本控制，对于对象的覆盖和删除操作将会以历史版本的形式保存下来。这样用户在错误覆盖或者删除Object后，能够将Object恢复至历史版本。
11	碎片管理	对象在分片上传过程中，如果未进行分片合并或终止操作，可能产生碎片，用户可以通过碎片管理功能，对碎片进行快速清理，节省存储空间。
12	稳定持久	▲对象存储OSS为用户提供运营商级的安全防护保障，全面保护用户数据的稳定持久，服务设计可用性不低于99.98%，数据设计持久性可达99.9999999999%。需提供数据证明材料，**包括官网的数据截图或相关证明文档**。
13		数据以多副本和纠删码冗余方式存储在不同设备上，确保服务器、网络设备、磁盘等硬件故障时，仍可保证数据可用性和持久性。
14		用户上传对象成功后，可立即读取数据。
15		OSS周期性地校验集群内数据的完整性，及时发现因硬件失效等原因造成的数据损坏，通过冗余数据及时重构并修复损坏的数据。
16	安全可靠	OSS通过可信云认证，数据存储的持久性、数据可迁移性、数据私密性、故障恢复能力等指标，均满足可信云服务认证要求。
17		OSS提供权限访问控制功能，支持存储空间级权限控制、对象级权限控制、用户身份与访问控制（IAM）、防盗链等多种安全权限设置方式，确保用户数据仅能在权限范围内访问。
18		OSS提供多版本管理功能，可随时恢复历史数据版本。
19		OSS支持AWSV4签名方式，HTTP请求参数和头信息均可参与签名计算，签名密钥不固定，有效防止数据在传输过程中被篡改。
20	资源充足	对象存储OSS的数据中心分布在全国31个省和自治区，用户可就近选择数据中心，利用OSS的高带宽、低时延、高可用、低成本等特点，存储用户的海量数据。
21		拥有遍布全国的通信服务网络，具有强大的带宽优势，可轻松应对高峰及突发流量，承载高并发业务压力。同时也可提供网络专线，满足网络延迟和安全等级要求。
22		OSS可大规模在线升级，在线扩容，升级扩容过程中用户无感知，不影响用户业务。用户无需事先规划存储容量，存储空间可按需付费，弹性伸缩。
23	简单易用	OSS提供多种数据访问方式，用户可通过控制台、HTTPRESTfulAPI、SDK等多种途径，轻松便捷地访问OSS。
24		OSS兼容AWSS3标准HTTPRESTfulAPI接口，用户可以使用兼容S3的第三方工具直接访问OSS。
25		OSS支持使用兼容S3接口的SDK访问，用户只需设置访问密钥（AccessKeyId和SecretKey)以及访问域名(Endpoint),即可通过S3SDK访问OSS。支持Java,Python,PHP,Javascript，Android,iOS,Node.js等多种语言SDK。

（3）云服务器备份存储需满足以下需求：

编号	功能/特性	参数要求
1	备份库	支持在线创建云服务器备份库，创建时可自由选择付费类型、云区域、绑定的云服务器，备份库大小、备份策略等属性。
		支持对创建的云服务器备份库进行查看、管理、搜索及刷新。
		已创建成功的备份库，支持再次批量绑定云服务器。
		支持对云服务器的系统盘进行备份，也可选择对云服务器下的系统盘及数据盘同时进行备份。
		支持备份库根据备份策略自动执行备份。
		支持手动对单个/多个云服务器执行云服务器备份操作,并提供全量备份和增量备份两种备份方式。
		支持对云服务器备份库进行扩容、续费和退订。
		支持修改云服务器备份库的名称、查看和搜索备份库绑定的云服务器、查看备份库绑定的云服务器下云盘信息。
		支持查看备份库绑定的云服务器当前已生成备份副本的个数及所占用的备份空间

		支持对备份库绑定的云服务器进行解绑，解绑后系统将彻底删除资源产生的自动备份和手动备份。
		支持对备份库进行绑定/解绑备份策略、更改备份策略等操作。未启用的备份策略可在绑定备份策略时快速启用。
		支持对已到期的云服务器备份库执行删除操作，删除后，系统将自动删除备份库中存放的所有备份。
2	备份副本	支持查看备份库绑定的云服务器所产生的所有备份副本，并支持针对备份副本按不同维度进行检索。
		支持对产生的备份副本执行删除操作。
		支持使用某一时间点的云服务器备份副本恢复云服务器数据，且支持跨云盘进行恢复。
3	备份策略	支持创建及管理备份策略，创建时可以选择备份周期、备份时间点和备份副本保留规则。
4	权限管控	提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。
5	快速恢复业务数据	针对云服务器资源定时进行备份，且在需要时，快速恢复业务数据。

2.3 网络资源

（1）专有网络VPC需满足以下需求：

编号	功能/特性	参数要求
1	基础能力	支持在线创建、删除专有网络VPC。
2	管理功能	1)支持对创建的专有网络进行查看、重命名操作。
		2)支持子网的创建、删除、查询。
		3)支持路由条目的创建、删除、修改以及查询。
		4)支持单栈子网开启IPv6双栈。
		5)提供主子账号功能，授权不同子账号以只读权限或者操作权限操作专有网络VPC资源。
		6)支持在用户创建资源的配额到达规定的上限后，通过工单形式，调整配额大小，满足不同的资源需求量。
		7)支持通过专有网络VPC的对基本云资源和网络资源进行划分隔离。
3	权限管控	提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。
4	网络性能	目前控制台限制用户自定义创建≥5个专有网络VPC，每个VPC可创建≥5个子网，并且可根据需要扩大配额；每个VPC可创建一个路由器，对应一个路由表，每个路由表可创建≥40条路由条目。

（2）弹性公网IP需满足以下需求：

编号	功能/特性	参数要求
1	基础能力	1）支持在线创建弹性公网IP，创建时可选择云区域、带宽值以及设置实例名称。
		2）支持对创建的弹性公网IP在控制台进行管理，进行查看、检索；
		3）支持IPv4以及IPv6带宽功能，最大带宽值可达1000Mbps。
		4）支持对弹性公网IP公网流入速率以及流出速率的监控。
		5）支持在用户创建资源的配额到达规定的上限后，通过工单形式，可调整配额大小，满足不同客户对于资源的需求量。
2	管理功能	1)支持调整带宽值（升配或降配）。
		2)支持绑定/解绑云服务器ECS、裸金属服务器、负载均衡SLB。
		3)支持续费、退订弹性公网IP。
3	权限管控	提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。
4	网络性能	支持带宽值范围为1-1000M。

5	弹性灵活	支持与云服务器、负载均衡等实例灵活地绑定和解绑，支持带宽灵活调整，应对各种业务变化。
6	实时监控	使用提供弹性公网IP以及IPv6带宽的监控数据，了解实例状态。

（3）负载均衡SLB需满足以下需求：

编号	功能/特性	参数要求
1	基础能力	1）支持在线创建负载均衡SLB，创建时根据是否绑定公网弹性IP，分为公网SLB和私网SLB；支持IPv6双栈负载均衡。
		2）支持对创建的负载均衡SLB在控制台进行管理，进行详情查看和检索。
2	管理功能	1）支持对单个负载均衡SLB进行编辑、绑定公网IP、删除操作；双栈的负载均衡还可以绑定IPv6带宽。
		2）支持对负载均衡SLB监听器的添加、修改配置（健康检查、会话保持、分配策略）、删除；支持监听器重定向，设置转发策略、获取客户端真实IP。
		3）支持对负载均衡SLB的后端服务器的添加、修改配置（健康检查、会话保持、分配策略）、删除。
		4）支持对负载均衡SLB的后端服务器的添加、修改配置（健康检查、会话保持、分配策略）、删除。
		5）支持给证书管理和IP地址组管理。
3	端口级负载	支持通过创建多个监听器实现端口级别的流量转发。
4	转发策略	支持通过域名或URL对流量进行转发。
5	轮询策略	用户设置负载均衡监听器转发策略时，可选择加权轮询、加权最少连接、源IP三种模式。
6	健康检查	支持用户自定义健康检查方式，支持自定义检查间隔、最大重试次数、超时时间，负载均衡根据预设的健康检查规则定时检查后端云服务器是否正常运行，一旦检测到云服务器为非健康状态，则不会将访问流量分派到这些非健康云服务器实例。当实例恢复正常，则再次添加到后端云服务器组中提供服务。
7	高可用	支持跨AZ下的高可用。
8	IP地址添加	支持添加VPC外的私网IP地址（例如对象存储IP地址）。
9	证书管理	支持证书管理功能。
10	权限管控	提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。
11	监控指标	支持查看负载均衡服务SLB的监听器、后端服务器不同粒度下不同时间周期内的端口流量进出情况、并发连接数、活跃连接数等监控信息。

（4）共享带宽需满足以下需求：

编号	功能/特性	参数要求
1	基础能力	1）支持在线创建共享带宽，创建时可选择云区域、专有网络VPC、带宽值以及设置实例名称。
		2）支持对创建的共享带宽在控制台进行管理，进行查看、检索。
2	管理功能	1）支持调整带宽值（升配或降配）。
		2)支持添加/移出弹性公网IP。
		3)支持续费、退订共享带宽。
3	生命周期管理	支持创建、退订、删除、续费共享带宽。
4	权限管控	提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。
5	网络性能	支持带宽值范围为5-1000M。
6	带宽共享	可实现互联网带宽消峰填谷，当不同业务访问互联网的流量时，高峰分布在不同时间段内。
7	双栈共享	支持IPv4和IPv6地址共享带宽。

2.4 专线资源

（1）专线资源列表

编号	专线名称	数量	带宽（M）
1	瑞金总院和海南分院之间建设点对点专线	1条	300
2	海南分院与瑞金医疗专有云建设点对点专线	1条	500
3	海南分院与瑞金医疗专区备份线路	1条	300

（2）服务内容要求

提供接入医院本地端机房所有设备、电路、线缆，负责调通医院本地端到云生产端、云备份端的网络，为云场景提供可自服务的快捷、弹性、随选的两地组网解决方案，投标人需根据采购人的需求，在医院归属当地需要有接入资源，并可以提供多种保障服务。解决云用户在不同地域，不同网络环境间多云互联互通问题，实现各医院到云的组网。网络可实施：预先接入、多点组网、价格统一、自助服务、即时开通、弹性带宽、QOS 保障等，并能够在未来医院规模扩大时，能够做到弹性扩容，能配合计算资源实时的调整网络资源，能实现网络资源在院端的统一管理。需要在专线出现故障时，能够有备用网络，保证业务的连续性。

（3）服务范围

本地端、云生产端、云备份端，网络专线服务互联互通。

（4）点对点专线服务标准

- 网络性能：▲本项目的点对点专线需采用电路交换，基于二层网络 VC 硬管道进行传输，确保带宽刚性固定分配。出口总带宽需要根据医院的需求合理配置，保证医院应用系统时延≤50ms，云生产端与云备份端按需要配置专线资源，能够保证备份和恢复的需要。
- 网络可靠性：专线需实现链路保护，并独享网络带宽。
- 网络安全性要求：在医院端通过利旧安全设备和网络设备，加强对出口链路的冗余部署，加强网络内部安全，保障网络的安全稳定运行以及重要数据的安全性。
- 线路指标：业务可用率≥99.9%，不可用时间＜1 小时/年，网络线路的丢包率不高于 0.1%。
- 线路维护指标：单条链路断网次数（含巡检维保）：≤5 次/年，线路平均修复时间≤2 小时。

（5）备份线路服务标准

- 网络性能：出口总带宽需要根据医院的需求合理配置，保证医院应用系统时延≤50ms，云生产端与云备份端按需要配置专线资源，能够保证备份和恢复的需要。
- 线路指标：业务可用率≥99.9%，不可用时间＜1 小时/年，网络线路的丢包率≤1%。
- 线路维护指标：单条链路断网次数（含巡检维保）：≤5 次/年，线路平均修复时间≤2 小时

2.5 安全要求

（1）投标人应提供云平台安全解决方案，以公安部《等级保护三级云安全扩展要求》为对标依据，结合云平台功能建设形成云纵深安全防控技术体系，使云平台满足信息安全等级保护三级要求。

（2）投标人需提供云主机安全、云防火墙、Web应用防火墙、堡垒机、数据库审计、漏洞扫描满足应用级等保三测评所需的安全服务与环境。

（3）本次项目需要满足云资源池的三级等保要求，以等级保护安全框架为依据和参考，在满足国家法律法规和标准体系的前提下的安全设计，形成网络安全综合技术防护体系。

（4）以中心安全管理为基本模型进行分级分域设计，保障设计方案的合规性。

（5）叠加安全可视、动态感知、协同防御三种安全能力构建主动防御体系，提供持续安全保护。

（6）每一个逻辑区域有相同的安全保护需求，具有相同的安全访问控制和边界控制策略，区域间具有相互信任关系，而且相同的网络安全域共享同样的安全策略。

（7）云主机安全需满足以下需求：

大类	技术指标	参数要求
形态部署	管理架构要求	采用 B/S 架构设计，管理控制中心高度集成化，无需额外安装或外接数据库即可实现日志存储和分析展示。
	管理控制中心要求	提供已加固的操作系统作为管理控制中心寄宿环境，保证管理控制中心自身安全。
	客户端要求	采用轻量级 Agent 部署，无需依赖虚拟化平台 API 即可实现安全防护；客户端支持手动从控制中心获取安装，也可通过管理控制中心批量远程安装；客户端对 windows 类、linux 类；物理服务器、虚拟服务器、桌面云具备相同的防护和部署模式。
	操作系统支持	产品应至少支持 Windows7/8/10 等云桌面常见操作系统类型，WindowsServer2003/2008/2012/2016 等虚拟化环境常见基于 WindowsNT 的服务器操作系统。
		产品应至少支持 SuSE、RedHat、Ubuntu、Debian、CentOS、Asianux、NeoKylinLinux 等虚拟化环境常见基于 Linux 内核的操作系统。
安全能力指标	文件防护要求	产品除支持一般性病毒木马查杀外，还应支持例如：宏病毒、敲诈勒索软件、注册表病毒、间谍软件、僵尸远程软件等特定恶意文件的查杀；除落地在本地文件系统中的文件外，对网络映射驱动器、移动存储路径、共享目录、局域网路径等扩展路径也能够进行扫描查杀。
		产品应内置 webshell 扫描引擎，针对网站系统恶意 webshell、后门等文件进行扫描防护。
		提供快速扫描、全盘扫描、指定扫描等多种扫描防护模式，支持自定义路径、指定引擎、自定义处理动作的个性化扫描防护。
		提供主动防御保护，智能监控系统文件操作行为，利用文件审计关联技术，实时对病毒木马及恶意相关文件进行拦截和防护。
		产品应支持对病毒文件进行手动加白置黑操作，对目录、文件、扩展名进行信任操作，以提升查杀效率和降低误杀率。
		产品应支持对病毒扫描查杀进行资源占用限制和任务并发控制，防止引发启

		动风暴、扫描风暴，修改资源利用方式无需重启。
	网络隔离和防护要求	产品应支持双向状态防火墙，提供对出入主机流量进行访问控制与隔离；防火墙支持从 IP、端口、方向、协议、优先级方面进行策略控制；支持防火墙策略的批量复制、删除、修改、停用等操作。
		▲产品应支持入侵防御，可对来自网络层的拒绝服务、缓冲区溢出、木马后门、web 攻击、恶意网络扫描、恶意入侵提权等各类威胁流量的检测与防护。
	系统加固要求	产品应支持对主机安全缺陷、配置进行扫描评估。能够对 windows 操作系统上的策略、服务、组件等进行扫描凭，对 linux 操作系统上的账号、服务、安全参数、进程、配置等进行扫描评估。
		产品应支持对主机的安全加固，针对利用虚拟化漏洞的恶意软件、程序进行拦截并阻止其在主机上运行，提供软件、程序的黑白名单，以减少对系统程序的误拦截风险，提供截图证明。

（8）云防火墙需满足以下需求：

大类	技术指标	参数要求
网络支持	路由协议	▲产品需支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持 RIPv1/v2/ng，OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持 PIM-SM（稀疏模式）。
		产品需支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于 12 种路由负载均衡方式，支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP 等方式的链路探测，同时 TCP 与 HTTP 可使用自定义目标端口进行测试。
		产品需支持 ISP 路由负载均衡，最大可支持 8 条链路负载，支持自定义负载权重，支持基于优先级的 ISP 路由链路备份；支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP 等方式的链路探测，同时 TCP 与 HTTP 可使用自定义目标端口进行测试。
	地址转换	产品需支持全面的 NAT 转换配置，包括包括一对一，一对多，多对一的源、目的地址转换，并至少支持 FULL_CONE 模式和 SYMMETRIC 模式。
		产品需支持在会话的源、目的地址同为 IPv4 地址时，可将目的地址转换至指定服务器地址，同时可探测服务器是否存活。
		产品需支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMPTrap、邮件、声音、短信等方式告警。
	IPv6支持	产品需设备接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定。
		产品需支持 IPv6 下静态路由及策略路由、动态路由，动态路由应包括 RIPng、OSPFv3、BGP4+。
		产品需支持 NAT64，包括： 对源地址为 IPv6 地址、目的地址为 IPv4 地址的会话执行源地址转换，将 IPv6 地址转换为 IPv4 地址，实现 IPv6 客户端转换为 IPv4 地址后访问 IPv4 资源 源地址为 IPv4 地址、目的地址为 IPv4 地址的会话执行目的地址转换，将 IPv4 地址转换为 IPv6 地址。实现 IPv4 客户端通过 IPv4 地址访问 IPv6 资源。
		产品需支持 DNS64 功能；支持 IPv6 入站的 DNS 代理功能，即从指定的入接口或源 ISP 接收到的 DNS 解析请求，设备可根据自定义的 IP、域名对应关系，代理 DNS 服务器返回查询结果。
		产品需支持配置基于 IPv6 地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL 过滤、应用识别、反间谍软件等安全功能。
		产品需支持针对 IPv6 流量通过 HTTP、HTTPS 实现 Web 认证，用户身份信息可存储在本地或 ActiveDirectory\Radius\TACACS+\POP3 等第三方服务器；通过 HTTPS 实现 Web 认证必须支持使用本地 CA 颁发的证书同时使用证书验证客户端身份。
访问控制	访问控制	产品需支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。
	流量管理	产品需支持多调度类相互嵌套最大 5 级的带宽管理设置。支持设置每 IP 最大或最小带宽，支持对每 IP 进行带宽配额管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配。

		支持配置基于 IP、用户、应用的流量管理规则，且至少支持对 2900 种应用定制流量管理规则。
攻击防护	网络攻击防护	产品需支持基于不同安全区域防御 DNSFlood、HTTPFlood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施。
		产品需支持可配置阈值的基于安全域或基于二层接口局域网广播防护，防止局域网内广播和多播数据包泛滥。
		产品需支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率。
		产品需支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括 PingofDeath、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片等；并可在设备页面显示每种攻击类型的丢包统计结果。
		产品需支持防御基于安全域的 IP 地址欺骗攻击，指定 IP 或网段必须从特定安全域流入。
	入侵防御	产品需支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护。
		产品需支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息。
		产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息。
		产品需支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持在防火墙间谍软件签名库直接查阅攻击的名称、严重性、描述等信息；间谍软件防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的间谍软件防护。
		产品需支持自定义 TCP、UDP、HTTP 协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的 CVE 编号或 CNNVD 编号。
		产品需支持自定义基于 TCP、UDP、HTTP 协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围。
	SSL解密	▲产品需支持 IPv4 和 IPv6 流量的 HTTPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，并可同时基于安全域、IPv4 和 IPv6 地址进行例外设置。
VPN	IPSecVPN	产品需支持支持 IPSecVPN 功能，支持基于主模式（MainMode）、积极模式（AggressiveMode）、国密三种协商模式建立的网关-网关加密隧道；支持本地 CA 并可为参与 IPSecVPN 隧道建立的设备颁发用于身份认证的证书。
		产品需支持支持 GRE 隧道，支持 GREoverIPSecVPN。
		产品的 IPSecVPN 功能必须支持无损数据压缩算法。
	SSLVPN	产品需支持 SSLVPN，支持使用 SSLVPN 客户端与防火墙建立 SSLVPN 加密隧道，支持对远程用户进行口令认证或证书认证。
安全管理	网络异常感知	产品需支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。
		产品需支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息。
		产品需支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看详情并自动显示关联日志；可基于网络连接、应用名称、威胁事件处置威胁事件。
	安全事件分析	所投设备必须提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防漏洞、防间谍软件等安全模块检查的日志集中显示。
		所投设备必须支持自定义一个或多个过滤条件，防火墙上的全部日志进行模糊检索或指定条件的精确检索,快速定位特定目标当前行为是否存在异常,网络中是否存在异常等问题,并可记录一个或者多个自定义过滤条件历史。
	策略与处置	所投设备可在单条策略中启用入侵防御、终端过滤等安全功能选项。

		所投设备必须支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索，支持策略的复制、调序、查询。
		产品需支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括 1 天、7 天、30 天、90 天、永久等。
		产品需支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果。
运维管理	运维管理	▲产品需支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件。**（提供历史配置文件＞2 个设备截图加盖公章）**
		产品需支持三权分立管理，权限设置至少包括全部权限，仅具有策略变更权限和仅具有日志审计权限、仅具有账户配置权限、虚系统配置管理权限以及虚系统审计权限；并支持以读写、只读、无权限的方式自定义权限管理，权限管理的范围至少包括策略配置、对象配置、网络配置、系统配置、统计分析、威胁处置等。
		产品需支持加密的 WebUI 和 CLI 管理，且支持网页命令行管理（WebUI 中内嵌 CLI 管理界面）。
		产品需支持将告警信息以 SNMPTrap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、CPU 利用率、内存利用率、硬盘利用率、接口带宽利用率等。
		产品需支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器，设备模块至少包括配置、时间、流量、URL 过滤、内容过滤、邮件过滤、行为、威胁等，重要性等级至少包括紧急、警报、严重、错误、告警、通知、信息、调试八种。
		产品需支持通过 TFTP 或 FTP 协议实现 IPS 特征库、威胁情报库、应用识别库等数据库的实时更新。

（9）云Web应用防火墙需满足以下需求：

技术指标	参数要求
Web安全防御	支持 HTTP 协议校验，可根据实际网络状况自定义协议合规标准，过滤非法数据
	支持 HTTP 访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，过滤非法请求
	支持 HTTPS 防护
	应能识别和阻断注入攻击
	支持防扫描陷阱
	支持爬虫防护
	支持文件上传、下载过滤
	支持 XPATH、struct2 检测和防护
	应能识别阻断跨站脚本(XSS)注入式攻击
	应能识别阻断盗链攻击
	应能识别阻断跨站请求伪造攻击
	非法上传检测阻断，包括恶意 WebShell 防护
	对网页请求/响应内容中的非法关键字进行检测、过滤
	应能识别和防止敏感信息泄露
	支持恶意代码攻击、错误配置攻击、隐藏字段攻击、参数篡改攻击、缓冲区溢出攻击防护
	提供多种威胁处理方式：返回错误码、重定向、封禁等
统计及报表	要求至少支持日志告警方式
	系统须能够对遭受攻击按照攻击次数、防护的网站、遭受攻击的网页进行统计并排名
	支持以 Word、PDF、HTML 等通用格式导出报表
升级	支持规则库离线升级和在线升级
	支持每月至少提供一次规则升级；紧急事件 24 小时内提供升级
管理界面	支持 HTTPS、SSH、Console 多种管理方式
	支持配置同步

（10）云堡垒机需满足以下需求：

大类	技术指标	参数要求
组件功能	资源管理	支持 SSH、RDP、VNC、Telnet、FTP、SFTP、DB2、MySQL、Oracle、SQLServer、Rlogin 等协议。
		▲可通过应用发布实现对 MySQL、SQLServer、Oracle、IE、Firefox、Chrome、VNCClient、SecBrowser、VSphereClient、Radmin、dbisql 等应用程序/客户端的扩展支持。
		支持对资源（包括主机、应用、应用服务器和资源账户）及账户批量导入、导出。
		支持内置常用的系统类型，包括 Linux、Windows、H3C、Huawei、Cisco。
		支持资源按标签管理，每个用户可以给每个资源打 10 个标签、支持批量添加和删除标签。
		支持 TELNET、SSH 协议资源使用普通账户自动切换到 root（或 enable）账户。
		支持支持 SSH、RDP、VNC、Telnet、FTP 等协议。
		无需安装任何客户端，便可 windows、linux、MACOS 等类操作系统登录堡垒机，并访问管理资源。
		支持 IE、Edge、Chrome、FireFox、Safari 等主流浏览器。
	资源运维	支持 SSH、RDP、TELNET、VNC 协议资源的批量登录功能，并且支持混合协议的批量登录，支持同时在一个页面运维不同协议的资源。
		支持运维 IPv6 地址的主机，主机协议类型包含：SSH、RDP、TELNET、FTP、SFTP、SCP。
		支持 RDP、SSH、VNC 协议类型主机的文件上传和下载，并进行审计。
		访问图形协议资源时，支持分辨率设置。
		支持 SSHkey 方式登录 SSH 资源。
		支持多台 SSH、TELNET 协议资源批量执行操作指令。
		支持将运维资源列表导出成 XShell 和 SecureCRT 格式的配置。
		支持 XShell、putty、MACterminal 等客户端和 RemoteBroswer（HTML5）访问目标资源。
		支持通过标签筛选资源。
		会话协同过程中，支持参与者控制会话，同时支持创建者强制获取控制权。
		支持字符协议预置命令功能，可添加至少 15 个经常使用的命令在系统当中。
	用户管理	支持本地、RADIUS 和 AD 域等认证类型。
		支持手机短信和动态令牌等多因子认证。
		支持通过来源 IP 控制是否使用多因子方式登录。
		支持通过设置来源 IP 控制和访问时段控制，限制用户访问堡垒机。
		支持用户的 IP 地址（黑名单或白名单）和 MAC 地址限制（黑名单或白名单）限制，非法地址无法登陆。
		支持主账户的生效和失效时间设置。
		支持用户的批量修改，包括重置密码、移动部门、更改角色、修改多因子配置、修改有效期、修改 IP 限制、修改 MAC 限制。
		支持按用户的状态、角色、部门筛选用户。
		支持自定义角色，符合客户复杂多样的业务场景需求。
		支持用户部门分权，不同的用户归属于不同的部门（子部门）。
		支持使用系统公告对所有用户发送消息通知。
		支持用户的批量导入、导出，支持导入用户时创建用户组、并且将用户加入到用户组当中。
	部门管理	支持分属于不同业务部门的的管理员只能管理权限范围内的用户、资源、策略和审计数据，分权管理。
		支持可设置管理员可管理的用户和资源的范围。
		支持部门无限级分组管理。
		支持快速新建、修改部门。
		支持批量新建部门。
		支持快速定位部门的用户和主机，并展示用户数和主机数。
	访问和命令控制	支持同时以用户、用户组、账户、账户组为核心要素，来设置多对多的资源访问授权。
		可根据执行动作、用户、用户组、账户、账户组、命令、命令集、有效期、生效时段为核心要素，细粒度地进行命令操作控制。
		命令权限控制动作包含断开连接、拒绝执行、动态授权和允许执行。
		堡垒机本身预制 Linux 主机和网络设备的基本命令，同时可根据特定场景需要进行自定义命令。
		可以对字符协议的设备的操作行为进行控制。

		支持对 MySQL 和 Oracle 数据库的访问操作控制，支持基于库、表、命令实现对数据库操作的细粒度访问控制。
		支持基于用户组、账户组的模式下，用户组和账户组内的新增成员自动继承访问控制和命令控制关系。
		支持拖动改变策略优先级顺序。
		支持批量启用、禁用策略。
		可根据用户、用户组、账户、账户组、有效期、文件管理控制、文件传输控制（上传、下载）、RDP 剪切板控制、时间限制、IP 限制为核心要素，细粒度地进行访问控制。
		访问控制策略支持配置双人授权候选人，针对核心设备，需要管理员现场审批才能操作。
		支持命令控制策略中对操作命令支持正则表达式和通配符方式设置匹配规则。
	自动运维	支持堡垒机推送账户到 Linux 服务器，通过账户推送，能够自动在服务器创建待推送的账户。
		支持堡垒机从 Linux 服务器拉取账户，通过拉取账户，能够实现服务器账户与堡垒机存储账户进行对比，分析服务器账户密码是否过期、是否有未纳管的服务器账户。
		自动化运维工具，实现对多台 Linux 服务器批量执行命令、批量执行脚本和批量传输文件，支持的脚本包括：Shell 和 Python。
		批量执行命令和批量执行脚本时，能够实时查看命令和脚本的输出，并实时展示执行结果。
		批量传输文件时，能够实时展示传输结果。
		支持将执行命令、执行脚本和文件传输等步骤进行灵活组合成运维任务，运维任务支持手动执行、定时执行和周期执行。
		运维任务的步骤不限制数量。
	工单管理	支持用户向管理员主动申请资源的运维权限。
		工单支持多人多级审批，最大支持 5 级审批。
		工单审批时，可以设置多人审批模式或会签审批模式。
		支持文件管理权限、RDP 剪切板权限、上传、下载权限的申请。
	操作记录	详细记录用户登录资源的所有操作，包括：资源名称、协议类型、主机或应用地址、资源账户、起止时间、会话时长、操作用户、来源 IP、操作记录、文件传输记录、会话协同记录。
		对字符操作命令进行精准识别，准确率达到 100%。
		对数据库操作的 SQL 语句进行识别，准确率达到 100%。
		支持 HTML5 页面展示当前操作用户的登录名作为水印，防止通过截屏方式造成的数据泄露。
		对文件传输协议 FTP、SFTP 的审计，详细记录文件传输操作。
		支持导出历史会话和系统日志的详细记录。
		支持会话结束状态审计。
		支持对剪切板拷贝文件行为和文本信息内容的记录，并支持通过搜索文本内容关键字定位审计回放。
		支持双人授权审计和协同用户审计。
		支持系统内置多种系统报表和运维报表模板，支持按日、周、月为周期，自动生成报表。
		支持主账户状态展示，包含僵尸账户和密码强度。
		报表格式支持 Word、HTML、Excel 和 PDF 格式。
		支持资源登录会话与系统登录会话关联。
		对图形操作过程中的键盘鼠标操作、剪贴板操作、标题栏操作、图形界面文字模糊识别四大类信息，进行文本审计。
		支持 MySQL 数据库下行返回行数记录。
		支持数据库命令级审计，支持的数据库类型包括：DB2、MySQL、Oracle 和 SQLServer。
		支持基于数据库代理的命令级审计和基于应用发布的图形审计的双重审计效果，命令级审计可以重现真实的完整操作命令，图形审计可以直观的查看到真实的操作行为。
	会话回放	支持从一条命令定位到用户的操作过程；回放过程支持暂停和加速播放操作。
		对用户命令操作的输入输出，在同一界面展示。
		支持在线回放过程支持播放速度调整、拖动、暂停、停止、跳过空闲、重新播放等播放控制操作。
		支持 Web 在线视频回放方式重现运维人员对资源的所有操作。
		支持离线回放重现运维人员对资源的所有操作过程，并支持回放文件下载到本地播

		放。
		可根据文本审计的内容为关键字进行图形搜索，搜索出来的结果可以直接定位到相关图形画面进行回放。
		支持对同一虚拟机的审计的任意切换。
	改密计划	可以根据账户、账户组、时间、改密周期、改密方式生成详细的改密计划，到期自动执行。
		支持修改数据库账户的密码，包括 MySQL、Oracle、SQLServer。
		改密方式可以支持随机生成不同密码、随机生成相同密码、手动指定相同密码。
		支持查看改密日志，了解改密账户总数、改密成功数量、改密失败数量和未修改数量。
		改密策略支持是否使用特权账户改密和是否修改特权账户密码的设置。

（11）云数据库审计

大类	技术指标	参数要求
	基本功能	支持 Agent 云解决方案,其 Agent 运行时 CPU 占用率低于 3%，内存占用小于 100M，程序文件小于 2M。
		▲支持传统的数据库:Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓 kingbase、南大通用 Gbase 等数据库的审计,支持后关系型数据库 Cache 的审计。
		支持 Telnet、pop3、smtp、nfs 协议审计，针对 FTP 协议，txt 文件传输可对其内容进行的审计。
		系统包括审计引擎及管理后台软件、策略管理、告警管理、权限管理、系统日志、系统配置等功能，可支持同时审计多个不同类型的数据库,审计数据统一存储、查询、分析、统计。
	审计能力	全面支持后关系型数据库 Cache 的集成工具 Terminal、Portal、Studio、Sqlmanager、MedTrak 工具的审计,其中 Portal 能审计到 Sql 语句、查询 Global、返回结果,Terminal 能审计到 M 语句和返回结果。
		支持数据库绑定变量审计、函数审计(sum 求和函数等）。
		支持 B/S、C/S 应用系统三层架构 http 应用审计，可提取包括应用系统的应用层帐号、数据库帐号、操作系统用户名、客户端主机名、客户端 IP、客户端 MAC 等身份信息，精确定位到人，并可获取 XML 返回结果。
		支持带 COM、COM+、DCOM 组件的三层架构应用审计，可提取包括应用层帐号、数据库帐号、操作系统用户名、客户端主机名、客户端 IP、客户端 MAC 等身份信息，精确定位到人。
		在无需重启被审计数据库的情况下，支持对 MSSQLSserver 加密协议的审计，可正常审计到数据库账号、操作系统用户名、操作系统主机名等身份信息。
		支持超长操作语句审计，针对传统型数据库，至少支持 3 万字节审计而不截断。
	审计策略支持	审计策略支持 18 种以上分项响应条件，可支持数据库操作命令（包括 select、create 等 14 个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、客户端进程名、会话 ID、关键字、时间（含开始结束日期）等。
		支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警。
		支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警。
		可提供通过子对象模式多级关联跨表跨字段的组合规则。
		系统自带审计规则库，用户可自定义审计策略。
		提供系统漏包告警、网络和网卡异常、磁盘存储容量不足等情况时的自动报警提醒。
		系统支持管理界面告警、Syslog 和 SNMPtrap 告警、邮件和短信告警。
	事件查询统计	告警检索效率高达亿条数据分钟级，搜索条件支持全范围搜索（特别要求在超过亿条数据量时），一次性完成搜索的响应时间在分钟级别。
		针对某行为在单位时间内频发进行高度监控/针对单位时间内产生的组合关联行为进行高度监控。
		支持自定义报表，支持 Word、PDF、xls 格式报表导出。
		可集成等级保护报表，确保能通过公安部信息安全等级保护的评测。

		可对可疑监控对象的操作语句进行回放，方便追溯。
	网络审计能力	支持 Telnet、FTP 协议审计，针对 FTP，可对其内容进行的审计。
		支持 HTTP、POP3、SMTP、NFS 网络协议的审计。
		支持与堡垒机联动关联审计运维数据库的操作行为。
	配置管理	提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身审计功能。
		管理员登陆支持静态口令认证，支持密码的复杂性管理，比如大小写、数字、特殊字符、长度等。
		采用 B/S 管理方式，全中文界面。
		可提供审计策略和配置的导入导出。
	数据管理	提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式。
		备份数据可自动存储在指定的 FTP 服务器上。
		审计结果脱敏设置，通过对审计结果中的重要信息进行脱敏处理，防止二次泄密。
		提供配置策略的导出和导入功能。

（12）云漏洞扫描

大类	技术指标及参数要求		
资产管理	资产管理	包括：操作系统、网站、数据库、中间件、网络设备、安全设备、虚拟化设备	
	资产探测	一键探测资产的操作系统类型、开启的端口等；智能识别端口对应的服务以及服务版本	
网站安全监控	监控对象	支持的协议	支持 HTTP、HTTPS 协议
		支持的 WEB 服务器	IIS、Websphere、Weblogic、ApacheTomcat、Nginx 等
		支持的编程语言	Asp、Jsp、.Net、J2EE、Php 等
		支持的数据库类型	Access、Mysql、ORACLE、DB2、PostgreSQL、Sybase、Informix、sqlite、MSSQLSERVER 等
		支持的第三方组件	WordPress、eWebEditor、FCKeditor、Struts2 等国内外常见第三方组件。
	可用性检测	检测网站是否可用	
		检测服务器响应时间	
		检测域名劫持	
	漏洞检测	扫描策略	支持 SQL 注入、XSS 跨站脚本、命令执行、目录遍历、上传漏洞等检测
			自动化解析 json、base64 数据并进行扫描
			追踪最新的安全漏洞，并及时更新
		扫描参数	支持自定义扫描策略
			支持输入 POST 数据
			支持 Web2.0 扫描
			支持 flash 解析
			支持自定义不扫描的目标 URL
			支持自定义扫描深度
			支持输入 Cookie 信息，进行登录扫描
			支持被动扫描，支持用户录入 url
			支持自定义爬虫规则
			支持自定义网站操作系统、数据库、中间件等信息
			支持 BASIC、NTLM 等多种认证方式
			支持 HTTPS 双向认证站点扫描
			支持代理设置

			支持设置 UrlRewrite 规则
		漏洞验证	支持数据包调试，验证漏洞
	篡改检测	白名单设置	
		图片 MD5 比较	
		页面标题比较	
		删除链接提醒	
		新链接提醒	
		页面相似度阀值设置	
		定位到篡改的页面源码位置，高亮显示	
	敏感内容检测	自定义敏感关键字	
		身份证信息、银行卡等个人敏感信息识别	
		图片文字识别	
		基于分词的语义分析	
	网马和暗链检测	网马、暗链动态检测	
		支持 Activex 识别	
	钓鱼网站检测	支持钓鱼网站检测	
系统漏洞扫描	扫描对象	Windows 系列：NT、2000、XP、2003、Win7、2008、Win8、Win10 等	
		Linu 系列：AmazonLinux、CentOS、Debian、Fedora、RedHat、SuSE、Ubuntu 等	
		nix 系列：AIX、FreeBSD、HP-UX、Solaris、MacOSX 等	
		应用程序：MicrosoftInternetExplorer、PHP、IIS、Apache、Tomcat、PHP、AdobeFlash 等；	
		数据库：Oracle、Mysql、DB2、Informix、Mssql、Sybase 等	
		虚拟化平台：VmwareEXSi、XenServer 等	
		网络设备：思科等	
		安全设备：juniper 等	
	扫描策略	漏洞规则超过 50000 条	
		覆盖缓冲区溢出漏洞、拒绝服务攻击漏洞、弱口令、信息泄露漏洞等全部常见漏洞	
	扫描参数	支持自定义扫描策略	
		支持设置策略并发数	
		支持 UDP 扫描	
		支持扫描端口服务版本	
		安全扫描，保证扫描过程中目标系统正常运行	
		登录扫描，如 SMB 登录、SSH 登录等	
数据库漏洞扫描	扫描对象	Oracle、Mysql、Sqlserver2000/2005/2008、Sybase、DB2、Informix、Postgresql、Kingbase、达梦、南大通用等	
		支持 Mongodb、Redis 等 nosql 数据库	
	扫描方法	支持授权扫描、非授权扫描	
	扫描策略	漏洞规则库包括 2000 多条策略	
		覆盖权限绕过漏洞、SQL 注入漏洞、访问控制漏洞等	
弱口令扫描	支持对 SMB、FTP、POP3、SMTP、SSH、TELNET、SNMP、RDP、redis、Oracle、MySQL 等协议进行在线弱口令扫描		
	支持对 windows、linux、mysql、weblogic 等密码进行离线破解		
	支持自定义用户名、口令字典		
恶意代码检测	▲木马病毒检查		
	网站恶意代码检查		

报表管理	支持将检查报告以 HTML、Word、PDF 等通用格式导出
	报告包含漏洞详情、漏洞描述、漏洞风险级别、加固建议等
	支持自动上报结果到 FTP 服务器

（13）云综合日志审计

大类	技术指标及参数要求
使用模式	界面 100%都是 B/S 模式，无需安装客户端，WEB 浏览器访问管理中心，浏览器端无需安装 Java 运行环境。支持 chrome 浏览。
管理范围	能够对企业和组织的 IT 资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。
审计对象	支持审计各种网络设备（路由器、交换机、等）配置日志、运行日志、告警日志等；
	支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防 DDOS 攻击，Web 应用防火墙、等）配置日志、运行日志、告警日志等；
	支持审计各种主机操作系统（包括 Windows,Solaris,Linux,AIX,HP-UX,UNIX,AS400）配置日志、运行日志、告警日志等；
	支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等。
	支持审计各种中间件（tomcat、apache、webshpere、weblogic 等）配置日志、运行日志、告警日志等。
	支持各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等。
	以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计。
采集方式	支持通过 syslog、snmptrap、netflow、jdbc、odbc、agent 代理、wmi 等多种方式完成各种日志的收集功能。
	对 windows 服务器（系统、应用和安全）日志和文件类型日志，可免日志代理或插件，支持用户环境中 EVT 格式的业务系统日志采集。
资产管理	按照设备资产重要程度和管理域的方式组织设备资产，提供便捷的添加、修改、删除、查询与统计功能。
	支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息，并对资产进行关键度赋值。
	支持自定义资产属性。
	支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。
日志归一化	支持采集一化后的日志和保留原始日志，方便用户对关键日志快速定位，和事后取证。
	日志收集后进行字段和安全等级的归一化处理，系统归一化字段不少于 50 个字段,并至少有 8 个可自定义字段。
	系统提供灵活简单的归一化方式,对系统新增的日志类型只需修改配置文件即可支持,不需修改系统程序。
日志查询	所有日志采用统一的日志查询界面，支持自定义查询场景，并以树形结构组织保存。
	支持原始消息中的关键字查询，可进行全文检索，查询显示查询记录总数，当前查询耗时。
	查询结果可支持导出、支持对查询结果任意字段进行排序。
实时监视	支持实时的日志滚动显示，可通过雷达图等直观显示目前日志量和日志详细信息。
	支持对实时展示的字段进行选择，调整字段顺序，修改显示字段别名。
	双击单条日志显示详细信息，支持左右布局和上下布局。
	支持自定义实时监视场景，提供可视化规则编辑视图，对关注的事件进行实时展示。
	支持鼠标放在日志对应字段上界面可悬浮提示资产信息和常用端口信息。
实时分析	可对收集的日志进行分类实时分析和统计，从而快速识别安全事故；
	分析统计结果支持柱图、饼图、曲线图等形式并自动实时刷新，图表数据支持数据下钻。
	支持统计分析的时长设定，分析结果支持导出报表 PDF，HTML，RTF,XLS,PNG,DOCX,XLSX。
	支持自定义实时分析场景，提供可视化规则编辑视图，根据实际业务编写分析规则。
	用户在实时监视的过程中如果发现某条事件的相关属性需要持续予以关注，可以将该事件分配到

	黑白名单中。
	支持对于关联事件进行追溯，查看导致该关联事件的所有原始事件。
可视化展现	能够在世界地图上实时定位事件源/目的 IP 地址的地理位置（包括二维及三维显示方式）。
关联分析	系统提供可视化规则编辑器，对告警规则进行增删改查。
	系统内置针对服务器和其他安全设备的访问 ip 地址、访问账户和访问时间的访问控制规则。
	告警规则可按照树型结构组织，并可在该树型结构上直接查看该规则的告警信息，对告警日志可按各告警字段进行分组排序。
	可对不同类型设备的日志之间进行关联分析，支持递归关联，统计关联，时序关联，这几种关联方式能同时应用于一个关联分析规则。
告警管理	通过关联分析，对于发现的严重事件可以进行自动告警，告警内容支持用户自定义字段；告警方式包括邮件、短信、SSyslog 等。
报表管理	提供丰富的报表管理功能，预定义了针对各类服务器、网络设备、防火墙、入侵检测系统、防病毒系统、终端安全管理系统、数据库、策略变更、流量，设备事件趋势以及总体报表，满足等保等其他合规性要求；根据时间、数据类型等生成报表，提供打印、导出以及邮件送达等服务；直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况。报表可以保存为 html，excel，文本，pdf 等多种格式。
	▲提供自定义报表，用户可根据自身需要进行定制。报表可根据设置自动运行,调度生成日报、周报和月报。
备份归档	支持使用在线和离线方式存储数据。
	支持按周期的方式选择备份，支持原始日志与分析后日志分离，支持历史日志恢复导入。
	支持各种配置项的备份和导入。支持各种配置项的一键备份和恢复。
	当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志或接收的日志不再入库，并进行告警；手动备份和恢复时，可以显示恢复和备份的进度。
系统管理	采用基于角色的权限管理机制，通过角色定义支持多用户访问。
	支持禁止与允许用户访问日志审计系统的 IP 地址限制。
	支持三权分立。
	系统自身的健康状况监控，包括 CPU、内存、磁盘的利用率。
	系统口令错误次数可设置，超过错误次数锁定，锁定时间可设置。

（14）云防篡改

大类	技术指标	参数要求
网站防护与恢复	网站防护	▲同时支持核心内嵌及文件驱动过滤两种篡改检测技术。
		网页防篡改系统应该支持 Windows、linux 等主流操作系统网站防篡改。
		提供自我保护机制，网页防篡改客户端需有第三方认证码方可卸载。
		支持对网页防篡改客户端的自动探测功能，方便快捷安装。
		应采用基于文件过滤驱动保护技术、事件触发机制相结合方式的网页防篡改功能。
		支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。
		同时支持防护模式和监控模式两种模式的防篡改模式。
		支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。
		系统支持在断线情况下对网页文件目录的防护功能。
		应支持文件多线程同步，并可以设置文件空闲同步时间周期、发布时间周期等设置。
		应支持 IIS、Weblogic、Websphere、Apache、Tomcat 等服务器。
		应支持超过 40GB 以上网页防篡改保护和恢复功能，以适应客户业务发展需要。
		系统可以从本地或异地备份文件夹自动同步到监测目录中，加强文件安全性。
		提供网页防篡改的发布模式，能和主流的 CMS 系统集成进行内容发布，提供 32、64 位系统集成。
		支持对网站服务器的 CPU、内存、收包量、发包量等信息进行实时监控；

		支持大规模连续篡改攻击防护。
		支持不依赖访问事件篡改后自动恢复功能，可直接由篡改动作触发恢复机制。
日志系统	系统审计	对与系统自身安全相关的下列事件产生审计记录。
		管理员登陆后进行的操作行为。
		对安全策略进行添加、修改、删除等操作行为。
		支持对网页篡改、添加、删除进行日志记录，并针对 IP、文件、进程、攻击类型进行详细记录。
		支持针对时间、IP、主机名文件、进程、攻击类型等进行日志筛选。
管控及网络适应能力		
部署能力	系统支持	支持 B/S 管理方式。
集中监控	集中管理	防篡改管理中心支持通过统一的管理中心进行单点登陆、日志收集。

2.6 密评服务要求

技术参数要求

（1）云服务器密码机要求

▲1.1.产品具有商用密码产品认证证书；**（提供证书复印件加盖公章）**

1.2.服务器密码机 API 接口符合《GM/T0018-2012 密码设备应用接口规范》。规格≥2U;设备具备≥2 个千兆网口；≥2 个万兆网口；冗余电源；

1.3.支持 SM1、SM4 等对称算法；

1.4.支持 SM2 和 RSA 非对称算法；

1.5.支持 SM3、SHA1、SHA256、SHA384、SHA512 等杂凑算法；

1.6.性能参数：

1.6.1 VHSM-32：单台设备可虚拟不少于 32 个虚拟密码机；

1.6.2 SM2：密钥生成（对/秒）≥8000；

1.6.3 SM2：签名/验签(tps)≥120000/80000；

1.6.4 SM2：加密/解密(tps)≥13500/30000；

1.6.5 RSA（1024）：密钥生成（对/秒）≥300、签名/验签(tps)≥10500/80000；

1.6.6 RSA（2048）：密钥生成（对/秒）≥70、签名/验签(tps)≥2900/72000；

1.6.7 SM1：加密/解密≥900Mbps；

1.6.8 SM4：加密/解密≥900Mbps；

1.6.9 SM3：杂凑算法≥900Mbps；

（2）签名验签服务器要求

▲2.1.产品具有商用密码产品认证证书；**（提供证书复印件加盖公章）**

2.2.提供数字签名、签名验证等密码安全能力。支持数据签名与验证、支持文件签名与验证；支持 SM2、SM3、SM4 等密码算法；支持证书有效期验证、CA 根验证、CRL 验证等服务，

支持证书/证书链的导入，支持多 CA 验证，为业务应用提供专用接口；

2.3.签名验签服务器 API 接口符合《通用密码服务接口规范》及《证书应用综合服务接口规范》国家标准接口规范。

2.4.性能参数：

2.4.1 SM2 签名效率≥30000 次/秒、验签速度≥20000 次/秒；

2.4.2 RSA1024 签名效率≥5500 次/秒；RSA1024 验证效率≥40000 次/秒；

2.4.3 RSA2048 签名效率≥2000 次/秒；RSA2048 验证效率≥30000 次/秒；

（3）时间戳服务器要求

▲3.1 产品具有商用密码产品认证证书；**（提供证书复印件加盖公章）**

3.2 符合 GM/T0033-2014《时间戳接口规范》、GM/T0028-2014《密码模块安全技术要求》安全等级第二级要求。

3.3≥4 个 100M/1000MBase-TRJ45 接口，可扩展万兆网卡

3.4 采用国家密码管理局批准的硬件密码卡实现各类密码算法，保证算法的高安全性；

3.5 对称算法：支持国产 SM4 算法和通用算法 3DES、AES；

3.6 摘要算法：支持国产 SM3 和通用 SHA256/SHA384/SHA512 等算法；

3.7 非对称算法：支持国产 SM2 算法和通用 RSA、ECC 等算法。

3.8 性能参数：

3.8.1 时间戳签发速度：≥1000 次/秒；

3.8.2 时间戳验证速度：≥500 次/秒；

3.8.3 授时精度：1ms2.7.4 云管平台技术要求；

（4）平台侧服务器密码机要求

▲4.1 产品具有商用密码产品认证证书；**（提供证书复印件加盖公章）**

4.2 为业务系统提供底层的密码运算和密钥生成；

4.3 支持 SM1、SM2、SM3、SM4 等商用密码算法；

4.4 支持国密标准密码服务接口；

4.5 支持密钥随机数生成、密钥存储保护、密码运算等密码安全功能；

4.6 服务器密码机 API 接口符合《GM/T0018-2012 密码设备应用接口规范》；

4.7 ≥4 个千兆网口,可扩展 2 个光口；

4.8 支持国际通用接口 PKCS#11、JCE 接口；

4.9 性能参数：

4.9.1 SM2 密钥对生成速度：5300 次/秒；

4.9.2 SM2 签名效率≥66000 次/秒、验签速度≥43000 次/秒；

4.9.3 RSA1024 签名效率≥10500 次/秒；RSA1024 验证效率≥80000 次/秒；

4.9.4 RSA2048 签名效率≥2900 次/秒；RSA2048 验证效率≥72000 次/秒；

4.9.5 SM1≥900Mbps、SM4≥900Mbps、AES≥900Mbps、3DES≥400Mbps、SHA256 杂凑算法≥900Mbps、SM3 杂凑算法≥900Mbps。

2.7 密码服务系统要求

▲2.7.1 产品具有计算机软件著作权登记证书；**（提供证书复印件加盖公章）**

2.7.2 每套租户密码资源池至少包含 10 个应用通用授权。

（1）基本功能要求

▲为云平台提供密码资源与服务的管理、云平台应用管理以及状态监管，具体包含密码资源分配和使用统计、用户和权限管理、日志和审计管理、云密码资源调度、云密码服务总线管理。用户管理员界面显示平台整体的密码资源分配和使用情况，可以对自己使用的密码服务功能进行管理操作，包括服务的启动、停止、配置、状态监视、日志、审计等操作。

（2）详细功能要求

2.1 本项目需要包含密码资源层、密码服务层，其中，密码资源层通过将密码专用硬件设备和系统进行抽象，形成可动态分配的密码资源池，并提供统一的密码服务总线供业务系统调用；密码服务层基于密码资源池通过统一的密码服务总线，对云平台上所有业务应用系统提供统一的密码服务。

▲2.2 管理与配置：支持对数据加密服务、签名验签服务、密钥管理服务、国密 VPN 服务、个人数字证书服务（智能密码钥匙）服务等的配置与管理。

2.3 日志审计：支持对密码服务操作日志的记录与审计功能。

▲2.4 态势分析：支持对密码服务调用次数的态势分析功能。

（3）密码服务要求

▲3.1 支持 SM2、SM3、SM4 国密算法，实现对敏感数据的加密。具体包括数据加密、数据解密、数据批量加密、数据批量解密、文件加密、文件解密等。

▲3.2 支持 SM2、SM3、SM4 国密算法，提供数字签名、签名验证、证书验证等密码服务。支持数据签名与验证、支持文件签名与验证；支持证书有效期验证、CA 根验证、CRL 验证等服务，支持证书/证书链的导入，支持多 CA 验证，为业务应用提供专用接口。

▲3.3 支持 SM2、SM3、SM4 国密算法，提供密钥托管相关的支持活动，如密钥托管服务、密钥安全隔离和存储服务等，对每个应用数据进行加密密钥分配，并保存在数据密文中，

使用时通过检索数据加密密钥的主密钥通过密钥运算进行解密，实现用户数据在数据库中的安全存储，对用户数据库中重要的表、记录、字段进行自动的加解密。通过密钥管理系统对数据进行加密存储，可对敏感信息关键字段选择性加密，实现密文数据上查询、更新和常用统计分析等功能。

3.4 支持 SM2、SM4 国密算法，为云平台业务系统的实体签发代表身份的的数字证书服务，提供统一的网络身份认证和验证管理，实现用户的身份确认。通过 CA 给用户发放数字证书，用户可以通过所颁发的证书实现网上办公中的电子签名及数据加密等功能。

3.5 支持 SM2、SM3、SM4 国密算法，提供基于国密 SSL 加密链路的 HTTPS 代理服务，对云平台业务系统的网络加密传输以及云平台与经由互联网连接的实体网络通信时进行安全防护，包括通道加密及用户身份鉴别，密码应用要求主要涉及通信过程中实体身份真实性、数据机密性和数据完整性，以及网络边界访问控制和设备接入控制。

▲3.6 支持 SM2 国密算法，为云上应用系统提供精准、安全和可信时间认证服务，支持基于 NTP 协议与时间源进行时间同步，确保所签发时间戳时所获取时间的有效性，包含签发时间戳、验证时间戳、证书解析、证书有效性验证、时钟同步等功能。

▲3.7 支持 SM2、SM3、SM4 国密算法，为云上租户提供国密浏览器服务；支持 SSL 单项及双向链接；支持国密网站、国密应用自动识别及国密标识展现；支持浏览器内核隔离域，能将不同的页面、插件和扩展运行在不同的隔离域；支持利用已有的沙箱机制，对沙箱里的应用进行控制，使网页中的代码（包括木马病毒）运行在封闭的沙箱里，无法和操作系统建立通信。

（4）功能概述

4.1 数据加解密服务

支持国产 SM2、SM3、SM4 密码算法，实现对敏感数据的加密。具体包括数据加密、数据解密、数据批量加密、数据批量解密、文件加密、文件解密等。

4.2 签名验签服务

支持 SM2、SM3、SM4 国密算法，提供数字签名、签名验证、证书验证等密码服务。支持数据签名与验证、文件签名与验证、证书有效期验证、CA 根验证、CRL 验证等服务，支持证书/证书链的导入与多 CA 验证。

4.3 时间戳服务

支持国产 SM2 密码算法，提供精准、安全和可信时间认证服务，支持基于 NTP 协议与时间源进行时间同步，确保获取时间的有效性，包含签发时间戳、验证时间戳、证书解析、证书有效性验证、时钟同步等功能。

4.4 密钥管理服务

支持国产 SM2、SM3、SM4 密码算法，提供密钥托管相关的支持活动，如密钥托管服务、密钥安全隔离和存储服务等，可对敏感信息关键字段选择性加密，实现密文数据上查询、

更新和常用统计分析等功能。

4.5 数字证书服务

支持国产 SM2、SM4 密码算法，为云上业务系统的实体签发代表身份的的数字证书服务，提供统一的网络身份认证和验证管理，实现用户的身份确认与网上办公的电子签名及数据加密等功能。

4.6 移动端数据安全服务

支持国产 SM2 密码算法，提供移动终端上的身份防伪造、数据防篡改、信息防被窃等密码服务。手机盾密码服务实现了传统 U 盾功能，不依赖硬件密码芯片，用软件实现密码设备、密码运算和 CA 数字证书的全部功能。

4.7 SSLVPN 安全传输服务

支持 SM2、SM3、SM4 算法，提供基于国密 SSL 加密链路的 HTTPS 代理服务，对云上业务系统的网络加密传输以及云平台与经由互联网连接的实体的网络通信进行安全防护，包括通道加密、用户身份鉴别。

4.8 密码应用管理

通过云密码管理平台提供密码资源管理、租户应用管理以及状态监管，具体包含密码资源分配和使用统计、用户和权限管理、日志和审计管理、云密码资源调度、云密码服务总线管理。

（二）项目进度要求

本期项目进度要求：在采购合同签订后，投标人应将即将实施的项目进度按如下表要求进行，需保证项目实施在一个月内完成。

序号	进度安排	工作任务	进度要求
1	系统评估	网络规划、数据评估、系统评估	小于 5 天
2	上云试用	服务器配置、专线带宽、网络流量	5 天
3	部署实施	网络搭建、系统迁移、数据迁移	5 天
4	系统测试	功能测试、架构测试、性能测试	3 天
5	系统割接	数据同步、域名切换、管控工具	3 天

（三）项目实施要求

1.实施质量要求

所提供产品在正式交付用户运行前，需要对系统进行全面、彻底的检验审查，将错误控制在最小范围，不能出现不稳定、不可靠、运行结果不正确的事故，特别不能够存在导致数据损坏、安全失控、系统崩溃等问题。

2.实施人员要求

项目实施过程中，投标人应严格按照响应文件中所承诺提供的项目人员进行施工。未经采购人建议或许可，项目经理和技术总监及各分项目负责人在项目结束前不得变更。

3.安装、调试

投标人应为本项目提供技术咨询服务，投标人负责与采购人现使用的云服务器进行技术对接的部署及调试。

4. 过程管理及电子文档要求

项目的工作内容及成果文档的提交应覆盖以下内容，电子文档是成果不可分割的部分。提供的技术手册包括以下文档：运行维护手册、使用操作手册、系统的验收报告、项目工作报告。

（四）维护要求

1. 投标人提供热线电话、电子邮件和在线网站等技术支持方式，提供 7*24 小时电话响应服务。投标人提供 7*24 小时的云机房现场运维服务，重大节点强化保障，确保云平台整体可用性。

2. 日常监控、巡检：对云平台进行日常监控、巡检，包括监控告警的处理，巡检异常的处理等；投标人需制定维护管理规定，并按照规定中的维护项目、周期和要求，制定详细的作业计划并执行。

3. 故障处理：处理发生的各类软硬件、通信线路等故障，确保上层业务系统能够正常稳定运行；其中故障处理流程需要电子化并规定处理时限及当前处理环节的责任部门和责任人。

4. 系统中断：投标人在成交后由于维护原因，需中断系统进行平台升级操作时，提前至少 72 小时（重大自然灾害除外）通知用户做好相关准备工作，征得采购人同意后方可实施。

5. 安全加固：对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加固。

6. 节假日保障：重大节假日期间进行云平台运行和信息安全的重点保障。故障处理和响应：投标人需对合同服务出现的故障响应做出相关保证。投标人应建立完善的云故障管理体系，管理体系涵盖故障处理的故障等级、职责分工和处理界面，每个处理流程留有记录并在每个处理环节中落实到投标人的部门和相应的处理接口人。按照故障等级不同，需要有不同的处理时长和故障恢复时限。

7. 应急演练与应急响应：投标人应协助用户建立系统安全事件管理和应急响应机制；根据云平台高可用设计特性和各组件的重要性进行针对性演练，制订应急预案，每年组织至少 2 次应急演练；当发生较大或重大应急事件时，投标人需在采购人的牵头下实施应急响应操作，针对重大事故在事后制定重大事件报告。

（五）售后服务响应

配备专业化的售后服务团队和专业技术人员 7*24 小时维护。当发现故障发生时，能在 15 分钟内向采购人通告故障情况，每 15 分钟通告故障处理情况，直到故障消除，并在故障消除后 30 分钟内通知用户。对于重大故障和超时故障，必须在故障处理完毕后三个工作日内向采购人提供纸质文件方式的故障处理报告。对于主用设备故障，能在 30 秒内完成切换，使应用系统快速恢复。

对于平台运行故障，必须在收到故障通知后 2 小时内解决，并恢复正常运行。硬件设备出现故障时，应进行紧急备件更换，保证采购人的业务系统正常运行。

★（六）保密与责任

投标人严格遵守国家有关法律、行政法规和管理规章；严格执行信息安全管理规定《互联网信息服务管理办法》、《计算机信息网络国际联网安全保护管理办法》、《互联网电子公告服务管理

规定》、《互联网网络安全应急预案》、《电信业务经营许可管理办法》、《木马和僵尸网络监测与处置机制》（工信部保【2009】157 号）等有关法规和行政规章制度，不得利用相关业务服务从事危害国家安全、泄露国家秘密、违法犯罪、妨碍社会治安等活动。

投标人负有保密义务，承担保密责任。投标人不得出于非法目的泄露采购人业务系统信息，不得损害采购人业务系统数据安全，未经采购人书面同意不得披露、更不得转卖采购人的任何数据与信息。若一经发现，采购人有权要求立即删除、限期整改、暂停甚至终止合作，并要求承担相应法律责任。

（七）服务人员要求

1.本项目的项目经理需具备相关云计算项目实施经验。

2.供应商需配备机房驻点专业工程技术服务团队。

（八）商务要求

★1.服务期限：自合同生效之日起 30 日内完成服务交付，自服务交付验收通过之日起，云服务、密码服务和云专线服务服务期为一年，上海瑞金医院到瑞金海南医院专线服务期为三年。

★2.服务地点：云供应商机房。

★3.付款方式：

3.1 第一年服务费：

中标后，采购合同签订之前 5 日，中标人向采购人交采购合同金额 5%的履约保证金。合同签订生效后，采购人收到中标人的增值税普通发票后，10 个工作日内向中标人一次支付云服务、密码服务、网络专线服务第一年度服务费用。

3.2 第二年服务费：

第一年服务期满，且服务验收合格后，在第二年度服务期开始后一个月内，采购人收到中标人的增值税普通发票后,10 个工作日内向中标人一次支付瑞金海南医院至瑞金总院网络专线第二年度服务费用。

3.3 第三年服务费：

第二年服务期满，且服务验收合格后，在第三年度服务期开始后一个月内，采购人收到中标人的增值税普通发票后,10 个工作日内向中标人一次支付瑞金海南医院至瑞金总院网络专线第三年度服务费用。

3.4 三年服务期满后，通过采购人验收合格之日起 5 日内退还中标人的履约保证金。

★4.验收标准：按国家行业标准及招标文件及投标文件的技术参数约定标准进行验收。

四、购买服务清单和技术参数要求

序号	名称	服务内容	技术参数要求	服务期限（年）
1	云资源服务	25个业务系统所需云资源： 1、CPU(核)：≥1974核； 2、内存（GB）：≥3412GB； 3、数据存储（TB）：≥128T； 4、云服务器：≥117台；	详见（一）基本要求	1
2	云安全服务	云安全服务： 1、云主机安全：≥117个资产； 2、云防火墙：≥1套； 3、云堡垒机：≥117个资产； 4、云防篡改：≥6个根目录； 5、云综合日志审计：≥117个资产； 6、云数据库审计：≥31个实例； 7、云漏洞扫描：≥2个URL； 8、云WEB应用防火墙：≥2个IP； （满足医院通过等保三级所需的云安全产品）	详见（一）基本要求	1
3	云密码服务	1、基于国产密码标准体系和密码管理体系，以保护云上业务系统的数据资产为中心的、自主可控的、符合国密要求的一套密码服务产品，通过密钥管理、签名验签、CA数字证书认证、云密码机、时间戳、手机盾、云VPN这7种密码服务，为网络基础资源、信息设施、计算分析、网络通道、接入终端、设备控制、应用服务等，提供身份鉴别、访问控制、机密性、完整性、抗抵赖性的立体纵深的密码安全服务。 2、标准版：提供以下7种密码安全服务。 （1）云密码机：支持国产SM2、SM3、SM4密码算法，实现对用户可选择性的敏感数据加密。 （2）签名验签：支持国产SM2密码算法，提供数据签名与验证、文件签名与验证、证书有效期验证、CA根验证、CRL验证等服务。 （3）时间戳服务：支持国产SM2密码算法，提供可靠的时间信息，证明某份文件（或某条信息）在某个时间(或以前)存在，保障证据的不可抵赖性和完整性。 （4）密钥管理：支持国产SM2、SM3、SM4密码算法，提供密钥托管相关的支持活动，如密钥托管服务、密钥安全隔离和存储服务等。 （5）CA数字证书：支持国产SM2密码算法，为云上业务系统的实体签发代表身份的的数字证	详见（一）基本要求	1

序号	名称	服务内容	技术参数要求	服务期限（年）
		书服务，提供统一的网络身份认证和验证管理。 （6）移动端数据安全：支持国产SM2密码算法，用软件实现密码设备、密码运算和CA数字证书全部功能，实现业务信息在移动终端上的安全性，包括用户身份防伪造、数据防篡改、信息防被窃。 （7）SSLVPN安全传输：支持SM2、SM3、SM4算法，提供国密SSL加密链路，为终端与云上业务系统、不同VPC间的业务系统提供安全的传输通道，保障数据传输的机密性和完整性。		
4	云专线	瑞金海南医院-医疗云 300M*1条	详见（一）基本要求	1
5	点对点专线	瑞金海南医院-医疗云500M*1条	详见（一）基本要求	1
6	点对点专线	瑞金海南医院-瑞金总院 300M*1条	详见（一）基本要求	3

B包:等保测评服务

（一）项目服务范围

委托获得公安部认证资质的测评机构，对采购人的6个信息系统安全保护状况开展等级测评，按系统出具《网络安全等级保护等级测评报告》，并结合采购人单位的实际情况，提出整改建议.

序号	信息系统名称	安全保护等级
1	门急诊住院管理系统（HIS）	第三级S3A3G3
2	影像管理和报告系统	第三级S3A3G3
3	实验室管理系统	第三级S3A3G3
4	门户网站	第三级S3A3G3
5	互联网医院	第三级S3A3G3

6	患者移动助医系统	第三级S3A3G3

（二）项目服务内容

序号	服务名称	服务内容	服务范围
1	网络安全等级保护测评服务	依据《网络安全等级保护基本要求》等有关管理规范和技术标准，对等级保护对象的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个层面的安全测评；完成测评工作后，出具《网络安全等级保护等级测评报告》，并提出整改建议。	本项目中需开展等保测评的6个三级（S3A3G3）信息系统
2	网络安全培训服务	信息安全意识教育；信息安全事件动态及解读；信息安全基本防护技能；《网络安全法》和网络安全等级保护要求解读。	

（三）项目服务要求

3.1 网络安全等级保护测评服务

投标人自合同生效且收到采购人开工令之日起60个工作日内，完成网络安全等级保护测评服务。投标人对采购人的6个三级（S3A3G3）信息系统完成等级保护对象要素进行确认、分析和梳理，提出详细的等级测评方案。对等级保护对象的整体保护状况和等级保护组件，逐一进行网络安全等级保护等级测评，等级测评的内容包括以下内容:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个层面的测评；完成测评工作后，出具《网络安全等级保护等级测评报告》，针对等级保护对象安全建设提出整改建议。

3.1.1 测评实施过程

投标人在测评过程中，按照《信息安全技术网络安全等级保护测评过程指南》等标准开展测评实施工作，等级测评过程分为四个基本测评活动:测评准备活动、

方案编制活动、现场测评活动、报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。测评双方之间的沟通与洽谈应贯穿整个等保测评过程。

3.1.1.1 测评准备活动

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。

测评准备工作应包括工作启动、信息收集和分析、工具和表单准备。

详细要求见下表:

项目内容	工作内容	成果输出
项目启动	1.组建测评项目组	向测评委托单位提交《项目计划书》、《提供资料清单》
	2.编制《项目计划书》	
	3.确定测评委托单位应提供的资料	
信息收集分析	1.整理调查表单	《等级保护对象调查表》
	2.发放调查表单给测评委托单位	
	3.协助测评委托单位填写调查表	
	4.收回调查结果	
	5.分析调查结查	
工具和表单准备	1.调试测评工具	确定测评工具(测评工具清单)《现场测评授权书》打印各类表单:风险告知书、文档交接单、会议记录表单、会议签到表单
	2.模拟被测定级对象架构,熟悉被测定级对象	
	3.准备和打印各类表单	

3.1.1.2 方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。

方案编制活动应包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表:

工作内容	工作详细任务	输出成果
1.测评对象确认	分析并确定被测定级对象 识别并描述被测定级对象的整体结构 识别并描述被测定级对象的边界 识别并描述被测定级对象的网络区域 识别并描述被测定级对象的主要设备 确定测评对象 描述测评对象	《测评方案》的测评对象部分
2.测评指标确定	确定被测定级对象业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	根据被测定级对象的A类、S类及G类基本安全要求的组合情况,从GB/T22239、行业规范中选择相应等级的基本安全要求作为基本测评指标	
	根据测评委托单位及被测定级对象业务自身需求,确定特殊测评指标。	
	根据测评委托单位及被测定级对象业务自身需求,确定特殊测评指标。	
	对确定基本测评指标和特殊测评指标进行描述,并分析给出指标不适用的原因	
3.测评内容确定	确定每个测评对象对应的每个测评指标的测评方法	《测评方案》的单项测评实施部分
	确定实施测评的单项测评内容	
4.工具测试点确定	确定工具测试环境 确定工具测试工具 确定工具测试的测评对象 选择测试路径 确定测试工具的接入点 本次项目测评需要使用到如下工具: 漏洞扫描工具;	《测评方案》的的工具测试方法及内容部分

	Windows主机安全配置检查工具； Linux主机配置检查工具； 网络及安全设备配置检查工具； 病毒检查工具； 木马检查工具； 网站恶意代码检查工具； 在线检查工具(网站安全检查工具)； 终端安全检查工具； 口令破解工具； 渗透测试工具； SQL注入验证检查工具； 在线数据库安全检查工具。	
5.测评指导书开发	确定单个测评对象，内容包含测评对象的名称、位置信息、用途、管理人员等信息	测评指导书、测评结果记录表格
	确定单项测评实施活动,包括测评项、测评方法、操作步骤和预期结果等四部分	
	确定单项测评、整体测评表述形式	
	根据测评指导书,形成测评结果记录表格	
6.测评方案编制	明确项目整体情况和测评活动依据	向测评委托单位提交经过评审和确认的《测评方案》、《风险规避实施方案》
	根据测评协议书和被测定级对象情况,估算现场测评工作量	
	根据测评项目组成员安排,编制工作安排情况	
	根据以往测评经验以及被测定级对象规模,编制具体测评计划,包括现场工作人员的分工和时间安排	
	汇总上述内容及方案编制活动的其他任务获取的	
	内容形成测评方案文稿	
	评审和提交测评方案	

	根据测评方案制定风险规避实施方案	

3.1.1.3 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作主要取得报告编制活动所需的、足够的证据和资料。

现场测评活动应包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表:

工作内容	工作详细任务	输出
1.现场测评准备	测评委托单位对风险告知书签字确认	会议记录，风险告知书，测评方案和现场测评工作计划，现场测评授权书
	测评委托单位协助测评机构签署现场测评授权书	
	召开现场测评首次会	
	双方确认测评计划和测评方案	
	双方确认配合人员、测评环境等各种现场测评需要的资源	
2.现场测评和结果记录	确认测评对象的关键数据已经进行了备份	《各类测评结果记录/测评证据和证据源记录/文档交接/规划记录单》 访谈结果:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理安全测评的测评结果记录或录音; 文档审查结果:安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评的测评结果记录; 配置核查结果:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录表格
	确认具备测评工作开展的条件，测评对象工作正常，系统处于一个相对良好的状况	
	根据测评指导书实施现场测评，获取相关证据和信息	
	测评结束后，双方确认测评工作是否对测评对象造成不良影响,测评对象及系统是否工作正常	
3.结果确认和资料归还	汇总测评记录，对漏掉和需要进一步验证的内容实施补充测评	
	召开现场测评结束会，测评双方对测评过程中得到的证据源记录进行确认	
	测评人员归还借阅的所有文档	

	资料，并由测评委托单位文档资料提供者签字确认	工具测试结果:安全物理环境、安全通信网络、安全区域 边界、安全计算环境、安全管理中心测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 实地察看结果:安全物理环境、安全通信网络、安全区域 边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评结果记录 测评结果确认:现场核查中发现的问题汇总、测评证据和证据源记录、测评委托单位的书面认可文件

3.1.1.4 报告编制活动

在现场测评工作结束后,应对现场测评获得的测评结果(或称测评证据)进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。报告编制活动应包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险分析、等级测评结论形成及测评报告编制七项主要任务。

详细要求见下表:

工作内容	工作详细任务	工作依据（模版）
1. 单项测评结果判定	分析测评项所对抗威胁的存在情况	测评报告的等级测评结果记录部分
	分析单项测评项的测评证据,并与要求内容的预期测评结果相比较,给出单项测评结果和符合程度得分	
	综合判定单项测评项的测评结果	
2. 单元测评结果判定	汇总不同测评对象对应测评指标的单项测评结果情况	测评报告的单元测评小结部分
	判定每个测评对象的单元测评结果	

3.整体测评	分析不符合和部分符合的测评项与其他测评项(包括安全控制点、安全控制点间、区域间)之间的关联关系及对结果的影响情况	测评报告的整体测评部分
	根据整体测评分析情况,修正单项测评结果符合程度得分和问题严重程度值	
4.系统安全保障评估	根据整体测评结果,计算修正后的每个测评对象的单项测评结果和符合程度得分	测评报告的系统安全保障评估部分
	根据各对象的单项符合程度得分,计算安全控制点得分	
	根据安全控制点得分,计算安全层面得分	
	根据安全控制点得分和安全层面得分,总体评价被测定级对象已采取的有效保护措施和存在的主要安全问题情况	
5.安全问题风险分析	针对整体测评后的单项测评结果中部分符合项或不符合项所产生的安全问题,结合关联测评对象和威胁,分析可能对定级对象、单位、社会及国家造成的安全危害	测评报告的安全问题风险分析部分
	结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等综合分析可能造成的安全危害中的最大安全危害(损失)结果	
	根据最大安全危害严重程度进一步确定定级对象面临的风险等级,结果为“高”“中”或“低”	
6.等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	计算定级对象综合得分，形成等级测评结论，形成等级测评结论	
7.测评报告编制	概述测评项目情况，整理前面几项任务的输出/产品	经过评审和确认的被测定级对象等级测评报告
	针对被测定级对象存在的安全隐患，提出处置建议	
	根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息,对测评报告进行评审	
	评审通过后,由项目负责人签字确认并提交给测评委托单位	

3.1.1.5 测评实施活动文档

测评机构在上述各阶段活动的测评实施服务过程中,根据服务规范和测评委托单位要求，提供系统、完整、清晰的服务日常报告。

提供的服务文档应至少但不限于如下文档:

(1)测评准备活动阶段:

《项目计划书》；

《等级保护对象调查表》；

《会议记录表》；

(2)方案编制活动阶段：

《网络安全等级保护测评方案》；

《测评指导书》；

《风险规避实施方案》；

(3)现场测评活动阶段：

《现场测评授权书》；

《文档交接单》；

《会议记录》；

(4)报告编制活动阶段：

按系统提交《网络安全等级保护等级测评报告》，并针对该信息系统提出安全整改建议。

3.2 网络安全培训服务

提供一年两次的网络安全培训服务，面向单位全部人员、技术部门专业人员开展网络安全意识教育；网络安全事件动态及解读；网络安全基本防护技能；《网络安全法》、网络安全等级保护要求等法律法规解读的培训；完成以下目标：

- 理解并掌握《中华人民共和国网络安全法》主要内容；
- 提高相关网络安全人员安全防护意识；
- 了解并掌握日常安全防护技巧

（四）项目管理要求

项目实施过程中，投标人应遵循国家标准、行业标准。

4.1 项目实施要求

在项目实施中投标人必须做到：

1. 提供项目实施组织架构；
2. 提供详细的项目实施方案和计划进度说明书；
3. 投标人应定期向采购人汇报项目的实施进度，包括但不限于项目经理在项目期间每周至少来采购人现场1次进行工作汇报，且电话要保持7*24小时通畅；

4. 为保障项目服务响应速度，投标人承诺项目实施期间及售后服务期内，提供本地化技术支持服务，对于采购人的电话咨询和常规服务请求在30分钟内予以答复，紧急服务请求在4小时内到达采购人现场；

5. 严格按照双方确定的计划进度保质保量完成工作；

6. 规范项目实施过程中的文档管理；

7. 项目实施中要引入风险管理、质量管理、成本管理；

8. 实施人员必须签署《保密协议》，按照《保密协议》的要求开展相关工作。

4.2 实施团队要求

本项目实施团队成员名单及职责分工明确，项目期间在项目本地部署测评师团队，项目经理需具有等保测评服务项目管理经验，且每周到项目现场不少于一天，实施测评工作的技术人员必须具备公安部信息安全等级保护评估中心颁发的《信息安全等级测评师证书》（以下统一简称为“测评师证书”），且在项目现场随身佩戴《测评师证书》备查。

4.3 项目验收

投标人必须书面通知采购人所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经采购人认定后方可执行。

（五）商务要求

★**1. 服务期限：**三年，合同一年一签，每年度服务验收通过后，签下一年服务合同。每年开展1次等保测评服务。收到采购人下达测评通知书后90天内交付《信息系统网络安全等级保护测评报告》。

★**2. 服务地点：**采购人指定地点。

★**3. 付款方式**

3.1第一年服务费：

采购合同签订之后5日内，中标人向采购人交采购合同金额5%的履约保证金。合同签订生效后，采购人收到中标人的增值税普通发票后，10个工作日内向中标人一次支付第一年度等保测评服务费用。

3.2第二年服务费：

第一年服务期满，且服务验收合格后签订第二年服务合同，在第二年度服

务期开始后一个月内，采购人收到中标人的增值税普通发票后，10个工作日内向中标人一次支付第二年度等保测评服务费用。

3.3第三年服务费：

第二年服务期满，且服务验收合格后签订第二年服务合同，在第三年度服务期开始后一个月内，采购人收到中标人的增值税普通发票后，10个工作日内向中标人一次支付第三年度等保测评服务费用。

3.4三年服务期满后，通过采购人验收合格之日起5日内退还中标人的履约保证金。

★4.验收

4.1 验收组织

成立由采购人、中标人以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

4.2 验收标准

(1)完成了本项目等保测评工作；

(2)提交本项目服务成果；

(3)提交项目实施阶段所有的过程文档。

5.售后服务要求

为保证本项目顺利进行，自合同签订生效之日起，投标人在服务期内提供网络安全咨询服务,包括等级保护政策/标准咨询；等级保护安全安全检查咨询；并针对测评发现的问题，提供后续的跟踪指导服务：提出安全整改建议，协助指导安全整改工作，出具整改报告。

6.服务考核及付款

6.1服务质量考核

本项目中为了更好地体现中标人的服务质量和能力,采购人每年对中标人进行一次服务考核，采用打分评估的方式进行开展，服务考核满分 100 分。采购人将根据考核结果，按合同款项支付要求向中标人支付服务考核款。

考核得分=100-扣分项

评分标准及细则

考核指标	考核内容	考核标准	分值

服务时效	测评服务时间	未按采购人要求时间进场，扣10分	10
		在采购人规定时间前完成测评服务的并交付报告的得10分，否则不得分。	10
服务质量	提供技术咨询服务	根据《信息系统安全等级保护基本要求》等国家标准规范，根据整改项提供相应的整改意见，并在被测评单位整改过程中提供技术咨询服务得20分，整改意见少于整改项或整改意见与整改项数量匹配但整改意见有缺陷，以上情形每存在1项扣2分，扣完为止。	20
	出具测评报告	测评服务完成后按采购文件标准出具《网络安全等级保护测评报告》且内容完整的得20分，未能按时出具的扣10分，内容不完整的扣5分，未出具测评报告的不得分。	20
服务保障	服务保障情况	信息化系统测评服务完成后1周内完成档案资料（包含但不限于测评报告、原始测评记录、漏扫报告等资料的纸质档案和电子档案）的归集、装档和移交工作的，得20分；缺1项扣2分，没资料的不得分。	20
		若发现系统重大安全问题，立即向被测评单位反馈沟通的得20分，否则不得分。	20
合计			100

6.2 考核付款细则

根据服务最终的考核得分后，应当支付服务款依据服务考核评分结果所在区间，根据下面标准计算得出：

6.2.1 考核得分在80—100分，应支付服务款为**当年服务款×100%**

6.2.2 考核得分在70—79分，应支付服务款为**当年服务款×90%**

6.2.3 考核得分在60—69分，应支付服务款为**当年服务款×80%**

6.2.4 考核得分在60分以下，应支付服务款为不超于**当年服务款×70%，且视为当年服务验收不合格，下年度的合同不再续签。**

C包：密码测评服务

（一）项目目标

项目的总体目标是：依据GB/T39786-2021《信息安全技术信息系统密码应用基本要求》，对购买瑞金海南医院基础信息化服务项目开展密码应用安全性评估，通过评估工作深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全水平奠定基础，推动国产密码应用工作的进一步落实，保障和促进采购人信息化安全体系建设健康发展。同时，也指导采购人的信息安全保障体系建设，增强密码安全管理意识，促进安全管理水平的提高。

（二）项目内容

根据GB/T39786-2021《信息安全技术信息系统密码应用基本要求》从物理和环境、网络和通信、设备和计算、应用和数据、安全管理等方面对信息系统开展密码应用安全性评估，分析信息系统与基本要求之间的差距，出具《信息系统密码应用安全性评估报告》，提出具有针对性的整改意见，并根据信息系统及安全防护措施的现状，提供其他安全服务，确保信息系统的安全运行。

（三）项目需求

3.1 需求内容

（1）对购买瑞金海南医院基础信息化服务项目信息系统进行摸底、分析和梳理，提出详细的测评方案。

（2）针对购买瑞金海南医院基础信息化服务项目信息系统进行密码应用安全性评估，内容包括：物理和环境、网络和通信、设备和计算、应用和数据、安全管理等。

（3）完成评估工作后，针对评估发现的问题，向采购人提交改进建议；采购人根据整改建议，对信息系统进行密码应用安全性整改，解决存在的问题，根据整改后的结果，出具测评报告。

（4）服务保障工作：评估报告提交1年内，围绕评估发现的问题和针对性改进建议，投标人应向采购人提供咨询服务。

3.2 服务清单

序号	评估对象	系统等级
1	门户网站	三级
2	门急诊住院管理系统（HIS）	三级
3	互联网医院	三级
4	实验室管理系统	三级
5	影像管理和报告系统	三级
6	患者移动助医系统	三级

3.3 项目成果交付

交付成果包括但不限于以下内容：

（1）《信息系统密码应用安全性评估测评方案》

（2）《信息系统密码应用安全性评估报告》；

（3）《信息系统密码应用安全性评估整改建议》。

针对服务清单中的系统上述材料各贰份。

3.4 测评方案

按照商用密码应用安全性分类分级评估的要求，依据《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）要求及信息系统等级保护定级情况进行评估，包括但不限于以下内容：

测评单元			测评指标
技术要求	物理和环境安全	身份鉴别	a）宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；
		电子门禁记录数据存储完整性	b）宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；
		视频监控记录数据存储完整性	c）宜采用密码技术保证视频监控音像记录数据的存储完整性。
	网络和通信安全	身份鉴别	a）应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；
		通信数据完整性	b)宜采用密码技术保证通信过程中数据的完整性；
		通信过程中重要数据的机密性	c)应采用密码技术保证通信过程中重要数据的机密性；
		网络边界访问控制信息的完整性	d)宜采用密码技术保证网络边界访问控制信息的完整性；
		安全接入认证	e)可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。
	设备和计算安全	身份鉴别	a)应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；
		远程管理通道安全	b)远程管理设备时，应采用密码技术建立安全的信息传输通道；
		系统资源访问控制信息完整性	c)宜采用密码技术保证系统资源访问控制信息的完整性；
		重要信息资源安全标记完整性	d)宜采用密码技术保证设备中的重要信息资源安全标记的完整性；
		日志记录完整性	e)宜采用密码技术保证日志记录的完整性；
		重要可执行程序完整性、重要可执行程序来源真实性	f)宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。
	应用和数	身份鉴别	a)应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；

	据安全	访问控制信息完整性	b)宜采用密码技术保证信息系统应用的访问控制信息的完整性；
		重要信息资源安全标记完整性	c)宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；
		重要数据传输机密性	d)应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；
		重要数据存储机密性	e)应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；
		重要数据传输完整性	f)宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；
		重要数据存储完整性	g)宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；
		不可否认性	h)在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。
管理要求	管理制度	具备密码应用安全管理制度	a）应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；
		密钥管理规则	b）应根据密码应用方案建立相应密钥管理规则；
		建立操作规程	c）应对管理人员或操作人员执行的日常管理操作建立操作规程；
		定期修订安全管理制度	d）应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
		明确管理制度发布流程	e）应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；
		制度执行过程记录留存	f）应具有密码应用操作规程的相关执行记录并妥善保存。
	人员管理	了解并遵守密码相关法律法规和密码管理制度	a）相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
		建立密码应用岗位责任制度	b)应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限： 1)根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位； 2)对关键岗位建立多人共管机制； 3)密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任； 4)相关设备与系统的管理和使用账号不得

			多人共用。
		建立上岗人员培训制度	c)应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；
		定期进行安全岗位人员考核	d)应定期对密码应用安全岗位人员进行考核；
		建立关键岗位人员保密制度和调离制度	e)应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。
	建设运行	制定密码应用方案	a）应依据密码相关标准和密码应用需求，制定密码应用方案；
		制定密钥安全管理策略	b）应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术信息系统密码应用基本要求》附录A;
		制定实施方案	c）应按照应用方案实施建设;
		投入运行前进行密码应用安全性评估	d）投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；
		定期开展密码应用安全性评估及攻防对抗演习	e）在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。
	应急处置	应急策略	a）应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；
		事件处置	b）事件发生后，应及时向信息系统主管部门进行报告；
		向有关主管部门上报处置情况	c）事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

3.5 服务考核及付款

3.5.1 服务质量考核

本项目中为了更好地体现中标人的服务质量和能力，采购人每年对中标人进行一次服务考核，采用打分评估的方式进行开展，服务考核满分 100 分。采购人将根据考核结果，按合同款项支付要求向中标人支付服务考核款。

考核得分=100-扣分项

评分标准及细则

考评指标	考评内容	考评标准	分值
服务时效	测评服务时间	未按采购人要求时间进场，扣10分	10
		在采购人规定时间前完成测评服务的并交付报告的得10分，否则不得分。	10
服务质量	提供技术咨询服务	依据 GB/T 39786— 2021《信息安全技术信息系统密码应用基本要求》、GM/T 0115-2021《信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》，根据整改项提供相应的整改意见，并在被测评单位整改过程中提供技术咨询服务得20分，整改意见少于整改项或整改意见与整改项数量匹配但整改意见有缺陷，以上情形每存在1项扣2分，扣完为止。	20
	出具测评报告	测评服务完成后按采购文件标准出具《商用密码应用安全性评估报告》且内容完整的得20分，未能按时出具的扣10分，内容不完整的扣5分，未出具测评报告的不得分。	20
服务保障	服务保障情况	信息化系统测评服务完成后 1 周内完成档案资料（包含商用密码应用安全性评估基本情况调查表、商用密码应用安全性评估报告的纸质档案和电子档案）的归集、装档和移交工作的，得20分；缺1项扣2分，没资料的不得分。	20
		若发现系统重大安全问题，立即向被 测评单位反馈沟通的得20分，否则不得分。	20
合计			100

3.5.2 考核付款细则

根据服务最终的考核得分后，应当支付服务款依据服务考核评分结果所在区间，根据下面标准计算得出：

3.5.2.1 考核得分在80—100分，应支付服务款为**当年服务款×100%**

3.5.2.2 考核得分在70—79分，应支付服务款为**当年服务款×90%**

3.5.2.3 考核得分在60—69分，应支付服务款为**当年服务款×80%**

3.5.2.4 考核得分在60分以下，应支付服务款为不超于**当年服务款×70%，并视为当年服务验收不合格，下年度的合同不再续签。**

（四）服务要求

评估项目实施过程中，投标人应遵循国家标准、行业标准。

（1）项目实施要求

在项目实施中投标人必须做到：

1）提供项目实施组织架构；

2）提供详细的项目实施方案和计划进度说明书；

3）严格按照双方确定的计划进度保质保量完成工作；

4）项目实施中要引入风险管理、质量管理；

5）签署《保密协议》。

（五）服务保障

（1）投标人必须确保能建立一支具有一定服务能力的管理团队，并合理调配各岗位人员，保障服务工作相关岗位人员需要。

（2）投标人从购买瑞金海南医院基础信息化服务项目进场之日起5个工作日内要完成评估系统确定和测评方案编制。

（3）投标人需在购买瑞金海南医院基础信息化服务项目验收之前完成并提交密码应用安全性评估报告。

（4）服务期间提供7×24服务响应，技术人员能够在4小时之内到达现场，并且现场支持的技术人员具备商用密码应用安全性评估人员测评能力考核证书。

（5）服务期间提供应急保障工作，针对应急、攻坚克难等事宜提供保障方案，包括高层支撑和响应时间等。

（6）严守工作秘密。投标人必须与采购人签署保密协议，工作人员须与单位签署《保密承诺书》，对知悉的事项及信息予以保密，所有资料、技术文档妥善保管，不得遗失、转借、复印，不得以任何形式向第三方透露；所有密码应用解决方案和采集汇总后的数据严禁通过互联网等公共信息网络、普通邮政进行传递，严禁在连接互联网计算机上存储、处理。

（7）严格遵循操作规程，承担服务工作质量责任。

（六）商务要求

★1.服务期限：三年，合同一年一签，每年度服务验收通过后，签下一年服务合同。每年开展1次评估服务。收到采购人下达测评通知书后90天内交付《信息系统密码应用安全性评估报告》。

★2.服务地点：采购人指定地点。

★3.付款方式

3.1 第一年服务费：

采购合同签订之后5日内，中标人向采购人交采购合同金额5%的履约保证金。合同签订生效后，采购人收到中标人的增值税普通发票后，10个工作日内向中标人一次支付第一年度密码测评服务费用。

3.2 第二年服务费：

第一年服务期满，且服务验收合格后签订第二年服务合同，在第二年度服务期开始后一个月内，采购人收到中标人的增值税普通发票后，10个工作日内向中标人一次支付第二年度密码测评服务费用。

3.3 第三年服务费：

第二年服务期满，且服务验收合格后签订第三年服务合同，在第三年度服务期开始后一个月内，采购人收到中标人的增值税普通发票后，10个工作日内向中标人一次支付第三年度密码测评服务费用。

3.4 三年服务期满后，通过采购人验收合格之日起5日内退还中标人的履约保证金。

★4.验收

4.1项目验收

投标人必须书面通知采购人所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经采购人认定后方可执行。

4.2验收组织

成立由采购人以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

4.3验收要求

（1）信息系统密码应用安全性评估测评方案；

（2）信息系统密码应用安全性评估报告；

（3）信息系统商用密码应用安全性评估整改建议；

（4）整体性的汇总报告

D包：线路租赁1

1.采购清单

序号	名称	服务内容	服务期限（年）
1	点对点专线	瑞金海南医院-海南省政务云专网300MB/s*1条	3

2.技术要求

2.1 端到端链路的传输比特差错率(误码率)：≤1.0×10E-7（提供网管截图或承诺函加盖投标人公章）；

2.2 单条链路可用率≥99.9%，不可用时间＜1小时/年；

2.3 网络线路的长期丢包率应不高于0.1%(提供网管截图或承诺函加盖投标人公章)；

2.4 单条链路断网次数（含巡检维保）：≤5次/年；

2.5 线路平均修复时间≤2小时；

2.6 两端节点采用光纤接入的方式,从通信运营商机房分别引接光缆接入到目标地点，保证网络各节点电路接入的高可靠性；

2.7 ★本次项目招标要求该点对点线路带宽≥300MB/s；

2.8 ★本项目的点对点专线基于MSTP技术，采用电路交换，基于二层网络VC硬管道进行传输，确保带宽刚性固定分配；

2.9 承载点对点专线的传输网络,应具备网络全程双路由保护及50ms的保护倒换时间；

3.施工、测试、开通与运行服务质量要求

3.1 投标人必须按照采购人进度要求完成电路的调测；

3.2 ★交付期限：投标人应于合同签署后20个工作日内完成电路和业务调测开通，提交测试开通报告，按采购人要求时间开通，服务期限为3年；

3.3 电路建设、测试和优化期间，运营商必须根据采购人要求积极配合工作。

★4. 付款方式

采购合同签订之后5日内，中标人向采购人交采购合同金额5%的履约保证金。合同签订生效后，中标人为采购人开通网络线路，采购人收到中标人递交的的增值税普通发票后，于10个工作日内向中标人支付该笔款项，服务费一年一付。

E包：线路租赁2

1.采购清单

序号	名称	服务内容	服务期限（年）
1	点对点专线	瑞金海南医院-海南省政务云专网300MB/s*1条	3

2.技术要求

2.1 端到端链路的传输比特差错率(误码率)：≤1.0×10E-7（提供网管截图或承诺函加盖投标人公章）；

2.2 单条链路可用率≥99.9%，不可用时间<1小时/年；

2.3 网络线路的长期丢包率应不高于0.1%(提供网管截图或承诺函加盖投标人公章）；

2.4 单条链路断网次数（含巡检维保）：≤5次/年；

2.5 线路平均修复时间≤2小时；

2.6 两端节点采用光纤接入的方式,从通信运营商机房分别引接光缆接入到目标地点，保证网络各节点电路接入的高可靠性；

2.7 ★本次项目招标要求该点对点线路带宽≥300MB/s；

2.8 ★本项目的点对点专线基于MSTP技术，采用电路交换，基于二层网络VC硬管道进行传输，确保带宽刚性固定分配；

2.9 承载点对点专线的传输网络,应具备网络全程双路由保护及50ms的保护倒换时间；

3.施工、测试、开通与运行服务质量要求

3.1 投标人必须按照采购人进度要求完成电路的调测；

3.2 ★交付期限：投标人应于合同签署后20个工作日内完成电路和业务调测开通，提交测试开通报告，按采购人要求时间开通，服务期限为3年；

3.3 电路建设、测试和优化期间，运营商必须根据采购人要求积极配合工作。

★4. 付款方式

采购合同签订之后5日内，中标人向采购人交采购合同金额5%的履约保证金。合同签订生效后，中标人为采购人开通网络线路，采购人收到中标人递交的的增值税普通发票后，于10个工作日内向中标人支付该笔款项，服务费一年一付。