“市事通•通通检”平台云服务器租赁及等保服务项目

比选文件

南通市质量技术和标准化中心

2024年 12月

目　　录

第一部分　比选公告

项目概况

南通质量基础设施“一站式”服务（市事通•通通检）平台服务器租赁及等保服务项目的潜在供应商应在（ 南通市市场监督管理局网站）获取采购文件，并于 2024 年 12 月9日14点00分（北京时间）前提交响应文件。

一、项目基本情况

项目名称：南通质量基础设施“一站式”服务（市事通•通通检）平台服务器租赁及等保服务项目

项目类型：服务

所属行业：软件和信息技术服务业预算金额：6.6万元

采购需求：根据《网络安全法》、《信息安全等级保护管理办法》 的要求，采购人（南通市质量技术和标准化中心）“市事通•通通检”平台现需租赁云服务器，并提供二级等保服务等，旨在保证系统的正常运行，提高信息系统的信息安全防护能力，降低系统被各种攻击的风险。具体详见比选文件，请仔细研究。

合同履行期限：2024年12月16日前完成。本项目是否接受联合体投标：否。

二、采购文件内容：

详见附件，请仔细研究。

三、供应商的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.未被“信用中国”网站（www.creditchina.gov.cn ）列入失信被 执行人、重大税收违法案件当事人名单、采购严重失信行为记录名单；

四、比选公告期限

自比选公告在南通市市场监督管理局网站发布之日起3日。

五、比选保证金

本项目不收取比选保证金。

六、履约保证金

本项目不收取履约保证金。

七、采购文件的获取，开启时间、地点

1.获取采购文件：

时间：2024年12月3日至2024年12月7日；

地点：南通市市场监督管理局网站；

方式：自行下载。

2.响应文件提交：

截止时间：2024年12月9日14点00分（北京时间）。

地点：**南通市濠东路15号南通市质量技术和标准化中心二楼会议室，如有变动另行通知。**

3.开启

时间：2024年12月9日14点00分（北京时间）。

地点：**南通市濠东路15号南通市质量技术和标准化中心二楼会议室，如有变动另行通知。**

八、凡对本次采购提出询问，请按以下方式联系。

采购人信息

名称：南通市质量技术和标准化中心

联系人：李先生

联系方式：0513-85101118

第二部分　比选须知

一、采购文件由采购人解释。

1.供应商获取比选文件后，应仔细检查比选文件的所有内容，如有内容或页码残缺、资格要求和技术参数含有倾向性或排他性等表述的，请在比选文件发布后3日内以书面形式提出询问或疑问，未在规定时间内提出询问或疑问的，视同供应商理解并接受本比选文件所有内容，并由此引起的损失自负。供应商不得在响应结束后针对比选文件所有内容提出质疑事项。非书面形式的不作为日后质疑提出的依据。

采购项目比选开始后，不再接受参选人对采购文件（含更正公告等）内容的异议或质询（质疑）。

2.参选人应认真审阅采购文件中所有的事项、格式、条款和规范要求等，如果参选人没有按照采购文件要求提交比选文件，或者比选文件没有对采购文件做出实质性响应，其比选将被拒绝，参选人自行承担责任。

二、采购文件的澄清、修改、答疑

1.采购人有权对发出的采购文件进行必要的澄清或修改。

2.采购人可视情取消、延长相关时间。

3.采购人对采购文件的澄清、修改将构成采购文件的一部分，对参选人具有约束力。

4.参选人由于对采购文件的任何推论和误解以及采购人对有关问题的口头解释所造成的后果，均由参选人自负。

5.采购人视情组织答疑会。

三、参选报价

1.本项目不接受任何有选择的报价。

2.参选报价均以人民币为报价的货币单位。

3.报价表必须加盖供应商公章且必须经法定代表人或被委托授权人签署。

4.参选报价出现前后不一致的，按照下列规定修正：

（1）比选文件中报价表内容与参选文件响应文件中内容明细不一致的，以报价表为准；

（2）参选文件中涉及大写金额和小写金额不一致的，以大写金额为准；

（3）单价金额小数点或者百分比有明显错位的，以报价表（参选报价总表）的总价为准，并修改单价；

（4）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价应当由供应商的法定代表人或其授权的代表签字确认后产生约束力，供应商不确认的，其参选报价无效。

5.供应商应详细阅读比选文件的全部内容，根据采购项目需求，准确制定相关工作方案等，必须对本采购项目全部进行报价，如有漏项，视同对本项目的优惠。不按比选文件的要求提供响应文件，导致报价无效，按无效响应处理。

四、参选文件的编写、份数和签署

1.参选人按第六部分“比选文件组成”编写参选文件。参选文件规格幅面A4纸（图纸等除外）；正文使用仿宋体四号字；按照采购文件所规定的内容顺序，统一编制目录，逐页编码，由于编排混乱导致参选文件被误读或查找不到，其责任应当由参选人承担；牢固装订成册，不允许使用活页夹、拉杆夹、文件夹、塑料方便式书脊（插入式或穿孔式）装订；参选文件不得行间插字、涂改、增删，如修补错漏处，须经参选文件签署人签字并加盖公章。

2.比选文件（**资格审查文件、商务技术文件、价格文件、电子响应文件**），明确标注参选人全称、“正本”、“副本”字样。**正本份数：1份，副本份数：1份。**

3.比选文件正本须打印并由参选人法定代表人或授权人签字并加盖单位印章。副本可复印，但须加盖单位印章。

4、**本项目要求提供电子响应文件一份，电子响应文件的内容为资格审查文件、商务技术响应文件、价格文件打印盖章后的响应文件的扫描件（资格审查文件、商务技术响应文件、价格文件需分别逐页连续扫描为三个独立的 PDF 文件），通过 U 盘方式提交，需单独密封提交。**

电子响应文件内容应与提交的纸质响应文件内容一致。否则， 由此产生的后果投标人自负。

五、参选文件的密封及标记

1.参选人应将资格审查文件正本、副本合并密封，统一装在一个密封袋内。

2.参选人应将商务技术文件资料正本、副本及图纸类等（如需提供图纸等其它资料的话）合并密封，统一装在一个密封袋或密封箱内（如有A3大小的图纸类，可单独密封）。

3.价格文件须单独密封，不得出现于参选文件其他部分中。

4.密封后参选文件（**资格审查文件、商务技术文件、价格文件、电子响应文件**）封面分别标明采购文件项目名称、边缝处加盖单位骑缝章或骑缝签字。密封完好标准以未泄露响应文件内容为主要判断依据。

5.采购人将拒绝接收未按照采购文件要求密封的参选文件。

六、参选文件的递交时间

参选文件必须在规定的接收截止时间前送达采购人。采购人将拒绝接收在比选截止时间后递交的比选文件。

七、相关费用

1.供应商承担参与比选可能发生的全部费用，采购人在任何情况下均无义务和责任承担这些费用。

第三部分　项目需求

供应商在制作响应文件时仔细研究项目需求说明。项目需求包括技术要求和商务要求:技术要求是指对采购标的功能和质量要求，包括性能、材料、结构、外观、安全，或者服务内容和标准等;商务要求是指取得采购标的的时间、地点、财务和服务要求，包括交付（实施）的时间（期限）和地点（范围），付款条件（进度和方法），包装和运输，售后服务，保险等。

供应商不能简单照搬照抄比选文件项目需求说明中的技术、商务要求，必须作实事求是的响应。如供应商提供的货物和服务同采购人提出的项目需求说明中的技术、商务要求不同的，必须在《商务部分正负偏离表》和《技术部分正负偏离表》上明示。

一、采购内容

包括项目需求和实施要求：

序号	服务内容		数量	功能	备注
1	云主机服务	日志审计	1	4C/8G/数据盘 500G	
2		应用主机	1	8C/16G/数据盘 2T/200M 带宽	
3		数据库主机	1	4C/32G/数据盘 5T	
4		堡垒机	1	4C/8G/数据盘 300G/2M	
5	云等保二级服务	云 防火墙+ 云入侵检测	1	实时检测溢出攻击、 RPC 攻击、WEBCGI 攻击、拒绝服务、木马、蠕虫、系统漏洞等在内的多种网络攻击行为。	
6		云日志审计	1	提供日志收集、存储、查询和统计分析等功能。	10 个日志源授权
7		云主机防护	1	防病毒、防暴力破解	2 个主机授权
8		云堡垒机	1	对访问账号集中管理； 精细的权限规划和运维审计； 提升企业的内部运维风险控制水平。	5 个资产授权
9		漏洞扫描服务	6 次	对客户网络进行定期扫描、发现主机操作系统、网络设备、数据库、安全设备等存在的安全漏洞，弱口令，开发的端口等，并列出安全整改建议。 服务方式：现场扫描和远程扫描 服务范围：主机、网络设备、数据库和安全设备。	一次/2 月

10		渗透测试服务	2 次	模拟黑客可能使用的攻击和漏洞发现技术，对目标信息系统进行渗透测试安全验证，发现逻辑性更强、更深层次的弱点，让管理者能够直观了解自己网络和系统安全状况。关注： 挂马威胁检测，病毒威胁检测，后门威胁检测，通信威胁检测，注入跨站检测。	具体时间由甲方定
11		云 waf	1	为客户提供网站安全的实时防护，能通过恶意特征提取和大数据行为分析识别恶意流量并处理，有效阻断 SQL 注入、跨站脚本、Web Shell、应用层 CC 等攻击，提高 Web 应用的安全性和可靠性。	一个域名（含二级域名）
12		安全运营中心	1	支持通过可视化看板直观查看系统当前安全评分，以及各类资产安全防护的覆盖率	
13	网络安全监控		1	对系统页面可用性、篡改挂马、敏感信息、暗链接检测等提供 24 小时检测，发现问题及时响应。	
14	云备份		1	提供云主机备份功能	5T

二、技术参数

2.1 云主机

服务	参数
云主机	1、弹性云主机具备多种使用规格，可通过控制台调整云主机的 CPU、内存、存储等资源，并可分配独立的 IP 地址。
	2、通过可视化的管理平台， 可以对弹性云主机进行管理，包括对云主机进行开机、关机、重置密码、重装操作系统等操作。
	3、支持多种云主机的登录方式， 可通过 VNC、SSH、MSTSC 等方式分别登录云主机。
	4、提供国产化操作系统。
	5、支持常用的操作系统镜像进行云主机创建，支持将云主机导成私有镜像，并可基于私有镜像创建云主机，实现业务的批量、快速部署。支持将私有镜像共享给其它用户，方便多用户统一部署。
	支持通过云平台管理门户或 API 接口，创建不同规格的云主机，并自定义 CPU、内存、网络、磁盘等云主机规格。
	*云主机可提供主流操作系统并支持国产化操作系统，具体包括麒麟、统信、欧拉等。 **(投标人或所投产品供应商需提供官网截图，并加盖投标人公章)**
	支持云主机的高可用，当出现硬件故障的情况下云主机能够实现自动迁移。

2.2 云硬盘

服务	参数

云硬盘	可提供多种规格的云硬盘，挂载至云主机用作数据盘和系统盘，其中云硬盘可提供普通 IO、高 IO、超高 IO 等多种云硬盘类型以满足不同的 IO 需求。
	*支持云硬盘共享功能，一块共享云硬盘可同时挂载 16 台云主机。**（投标人或所投产品供应商需提供官网截图，并加盖投标人公章）**
	*云主机支持挂载单个云硬盘最大可达 32TB，满足大容量和大规格云主机业务场景。**（投标人或所投产品供应商需提供官网截图，并加盖投标人公章）**
	云硬盘支持与云主机的挂载与卸载。系统盘在创建云主机时自动添加，用户无需进行挂载操作。

2.3 云防火墙

服务	参数
工作模式	产品支持路由、透明以及混合模式等多种部署方式
路由特性	支持静态路由、策略路由、RIP 、OSPF 、BGP 、IS-IS 等路由协议
安全策略	支持一体化安全策略，能够基于源/目的安全域、源 IP/MAC 地址、目的 IP 地址、地区、服务、时间、用户/用户组、应用层协议、五元组进行安全策略配置
	支持策略风险调优，策略数冗余及命中分析，支持基于应用风险的自动批量和手动逐条策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。
应用识别	★支持至少 6000 条以上的应用识别，且提示风险类型及风险级别，便于用户根据实际情况进行上网行为管理。**（需提供证明材料并加盖公章）**
防病毒	产品支持对 SMTP 、HTTP 、FTP 、SMB 、POP3 、HTTPS 、IMAP 等协议进行病毒防御，支持挖矿行为检测和勒索病毒检测。发现病毒发送的告警信息，支持用户编辑告警内容
	★本地病毒库可以在线更新、本地更新， 云端防病毒，为保证检测时效性，特征缓存数至少保证 20 万条且缓存保留时间不应少于 700 分钟**（需提供证明材料并加盖公章）**
	支持本地沙箱联动
入侵防御	实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。
	产品支持僵尸主机检测功能，可识别主机的异常外联行为
	★支持对检测到的攻击行为的前后报文进行自动化抓包功能，方便用户对攻击行为进行取证**（需提供证明材料并加盖公章）**
攻击防护	★能够防范 DoS/DDoS 攻击：Land、Smurf、Fraggle、Ping of Death、Tear Drop 、IP Spoofing、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口

服务	参数
	扫描等攻击防范，还包括针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood、HTTP Flood、HTTPS Flood、SIP Flood 等常见 DDoS 攻击的检测防御。**（需提供证明材料并加盖公章）**
	支持流量自学习功能，可设置自学习时间，并自动生成 DDoS 防范策略。

2.4 云日志审计

服务	参数
日志采集解析	支持对各类网络设备（路由器，交换机，VPN，负载均衡等）、安全设备（包括防火墙，IDS，IPS，防 DDOS 攻击，Web 应用防火墙等）、主机操作系统（包括 Windows,Linux 等）、各种数据库（Oracle、Sqlserver、Mysql）、各种应用系统（邮件，Web，FTP），终端管理系统告警日志，网络综合审计系统告警日志，上网行为审计系统日志，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；
	★对主动采集，支持特定时间采集，防止业务繁忙影响系统性能；**（需提供证明材料并加盖公章）**
	★日志采集解析至少包括直接信息解析和补全解析，直接信息包括日志中涵盖的信息，比如 IP，端口等，补全信息至少包括资产名称，所属人员，组织，网络区域，业务区域，厂家，操作系统名称，系统类型等；**（需提供证明材料并加盖公章）**
	★日志解析支持自定义解析，自定义解析支持灵活的语法，至少包括字符串函数，字符串函数支持级联语法，条件函数，引用函数等函数；**（需提供证明材料并加盖公章）**
	支持自定义日志解析规则的导出；
告警展示处理	可以根据告警生成工单；
	支持工单的增删改查；
	★具备同类告警合并策略，减少告警数量；**（需提供证明材料并加盖公章）**

2.5 云主机防护

服务	功能组件	参数

资产管理	资产管理	支持同一个控制台统一管理云主机，服务器，容器，镜像资产，支持模糊检索、筛选、开启防护、查看主机资产信息、安全风险等功能，方便用户快速管理服务器。
	容器资产	★支持容器资产指纹，包含容器 ID、宿主 ID、容器名称、容器 IP、地域、保护状态，告警详情，基线详情。**（需提供证明材料并加盖公章）**
主机风险	主机漏洞	支持 linux 及 windows 系统漏洞检测及修复，支持批量修复及一键自动修复；支持应用漏洞及 Web-cms漏洞检测
	暴力破解	★检测 SSH、RDP、MYSQL、SQLSERVER、FTP、redis、mongdb、postgresql 暴力破解行为，进行实时检测、告警、阻断功能， 支持登录白名单配置。支持 SSH、RDP、sqlserver、redis、mongdb、postgresql 爆破成功告警；支持用户自定义暴破阻断规则设定，例如，判断条件规则（1 分钟大于等于 5 次），阻断时长（阻断 15 分钟等）。**（需提供证明材料并加盖公章）**
	合规基线	支持等保 2.0 二级、三级、 CIS、弱口令、中间件基线检测， 支持京东最佳实践基线检测，并提供修复方案。中间件基线需支持 redis，nginx，CIS nginx，tomcat，ElasticSearch，Apache，mysql，MongoDB，CIS 等 MongoDB。
入侵威胁	病毒木马	★需采用云+端的查杀机制，上报到云端控制中心进行病毒样本检测，无需本地存放引擎数据，占用主机资源。必须支持多引擎查杀，并提供商业杀毒引擎证明。支持云沙箱以及威胁情报检测能力。支持检测勒索病毒、 DDoS 木马、远程控制、挖矿类软件等，并告警用户。**（需提供证明材料并加盖公章）**
	系统后门	检测 Rootkit 安装的文件和目录，需已知 rootkit 检测，隐藏进程检测，隐藏执行文件，隐藏网络连接检测，内核模块检测
防勒索	防勒索	★支持勒索病毒已知及未知病毒的检测，支持自定义备份及随时按版本和时间恢复功能**（需提供证明材料并加盖公章）**
容器安全	统一管控	支持容器安全与宿主机安全在同一管控端，而非两个单独产品，支持联动配置策略与资产管控关联
	容器运行时	★支持检测容器运行时 13 项告警检测：包括挖矿进程检测、网页木马检测、反弹 shell 检测、病毒木马检测、非授信进程、启动特权容器、执行 sudo、挂载敏感目录、本地提权、运行黑客工具、恶意文件下载检测、篡改系统日志、篡改 ssh 密钥。**（需提供证明材料并加盖公章）**
	容器基线	支持容器基线检查，包括 Docker 最佳实践，Kubernetes 最佳实践

2.6 云堡垒机

服务	参数

支持协议		telnet、ssh、rdp、vnc、xwin、http、https、ftp、sftp、AS400、SQLServer、SYBase、MySQL、oracle、db2、informix， 并可通过应用发布方式扩展支持其他协议；
端口安全技术		采用端口安全机制，不开放或变相开放 3389、22、21、23、5900 等高危端口实现高效协议代理；
RDP 协议代理技术		采用真正意义上的 RDP 协议级代理机制，而非经过多次应用级转换的“RDP 代理”，使得 RDP 运维代理最高效，单台设备即可实现 500 以上的 RDP 并发访问；
设备账号管理	密码托管	支持对已添加的设备账号进行密码托管，从而实现单点登录功能；
	自动发现	支持对已添加设备进行账号扫描，自动发现并添加目标设备上存在的其他账号；
	手动改密	可基于界面手动修改目标设备的账号密码；
	自动改密	★支持定期批量修改目标设备的账号密码，改密功能成熟稳定，具备较强的改密容错机制，保存密码修改的所有历史记录；**（需提供证明材料并加盖公章）**
	密函打印	支持通过密函的方式将密码打印到密码信封，同时支持密码分段模式的密函打印；
访问授权	综合授权	支持细粒度的访问授权策略，可基于用户、用户组、设备、设备组、协议、支持 IP 地址范围、时间等进行灵活授权；可设定当前授权中的资产仅可在授权的时间段内访问、仅可在授权的 IP 地址范围内访问；
	工单授权	支持内建工单授权模式，可由操作员自行申请所需访问的资产，由管理员审批；
	紧急运维码	支持紧急运维码方式授权，在紧急模式下可通过紧急运维码发起临时运维
运维访问	H5 技术	★设备访问支持 html5 技术，在同一 WEB 窗口页签中，无需 JAVA 应用插件，即可实现对目标设备的快速运维；**（需提供证明材料并加盖公章）**
	一次一密	★采用一次一密技术，运维访问过程中，所有账户及密码均加密传输，运维访问安全可靠；**（需提供证明材料并加盖公章）**
黑白名单	命令集	依据文本字符、文件传输命令分类集成命令集，可添加命令参数（支持正则通配符），可设置命令风险级别；
	数据库 sql 语句黑白名单	★不仅支持命令行操作界面的 SQL 语句阻断功能，还支持图形客户端连接工具的 SQL 语句阻断（如 plsql、SQLplus、toad 等），以防止数据库管理员的误操作；**（需提供证明材料并加盖公章）**
运维操作审计	智能分组	可按年月、日智能分组展现，可实时生成分组的会话数和会话流量；

	数据库审计	★不依赖操作录像，亦可实现 100%提取本地客户端与数据库之间交互的每一条 SQL 语句；**（需提供证明材料并加盖公章）**

2.7 云 WAF

服务	功能组件	参数
部署方式	集群部署	支持反向代理模式，支持集群高可用模式（主-主）
应用网关	域名视图	支持列表展示域名、负载实例、VIP、端口、转发策略、WAF状态、日志开关以及详情
	网关配置	支持网关集群与网关节点的关系管理，可用VIP添加。 系统本身模块监控，网关节点状态监控，激活等；网络接口列表展示。
	转发规则	★转发规则控制路径、协议， 转发到某一个应用集群，支持灰度发布、流量比例分配。支持请求头、请求参数、Cookie等高级匹配规则。支持服务端、客户端超时设置；请求头、响应头设置。**（需提供证明材料并加盖公章）**
	应用攻击防护	支持应用攻击防护与自定义攻击防护。
		应用攻击防护支持拦截、检测模式；支持宽松正常严格与自定防护等级，支持拦截返回页面的设置。
		★支持防御 SQL注入、XSS攻击、命令/代码执行、文件包含、木马上传、路径穿越、恶意扫描等 OWASP TOP 10攻击。支持防御 SQL注入、XSS攻击、命令/代码执行、文件包含、木马上传、路径穿越、恶意扫描等 OWASP TOP 10攻击**（需提供证明材料并加盖公章）**
		自定义攻击防护，支持字符串、正则、地域、长度、 IP、SQL注入、XSS等匹配类型
	恶意IP惩罚	IP短时间多次攻击，设定封禁时间，包括攻击阈值、检测时长、封禁时间、动作等设置
	网页防篡改	★支持对网站URL进行缓存配置，配置生效后将锁定网站的返回页面为缓存的正常页面**（需提供证明材料并加盖公章）**
	敏感信息防泄漏	支持规则名称配置，匹配逻辑（精确匹配、包含、前缀匹配），匹配类型（身份证、信用卡，手机号），匹配动作（告警，过滤），URI
	黑白名单	支持白名单、黑名单配置，可匹配IP、URI、Method、Cookie、Geo、Header，组和条件，等匹配方式以及后续执行动作
	CC攻击防御	★支持规则名称，URI配置、统计维度、检测时长，单IP访问次数，支持阻断类型，观察，人机交互，拦截，持续时间配置**（需提供证明材料并加盖公章）**

2.8 安全运营中心

服务	功能组件	参数
安全可视	安全仪表盘	支持通过可视化看板直观查看系统当前安全评分，以及各类资产安全防护的覆盖率
		能够直观呈现当前资产企业版授权状态，以及日志保存最大天数、 病毒库最近更新时间， 最近安全扫描时间
		支持基于安全告警事件、安全漏洞信息、基线检查信息等维度，统计当前系统中存在的风 险情况
	安全大屏	★支持将安全能力统一管理、集中大屏呈现； 支持大屏展示整体安全态势、 网络安全态 势、主机安全态势、纵深防御态势等数据信息、具备大屏告警能力**（需提供证明材料并加盖公章）**
		支持自定义大屏 logo 与标题
	攻击面概览	★支持分类统计各类资产（云主机、 容器、物理服务器、网站）在线数量统计，通过进 行资产扫描，对外暴露的端口和应用进行看板可视化呈现，可以直观呈现当前资产，存活 公网 IP 数量、开放端口数量、暴露端口及应用类型数量，并可以支持自定义违规端口和应 用，并将端口和应用按照 TOP10 进行分类统计**（需提供证明材料并加盖公章）**
		支持进行攻击源 IP 统计分析，包括攻击总次数，攻击 IP 总数，并支持按照攻击源检测引 擎进行分类统计分析，支持自定义规则制定聚合攻击网段排名，呈现攻击源 IP 地址位置分 布（国家-省份-城市）
资产管理	资产导入	支持自动同步和手动导入两种方式汇集资产相关信息，支持异构云平台和云外 IDC 机房 中的资产导入，同时支持单个资产添加和批量资产导入两种导入方式
	资产看板	★支持将资产按照至少八种资产类型进行划分（包括但不限于：云主机、 容器、网站、 物理服务器、公网 IP、内网 IP、其它云产品、其它物理设备） **（需提供证明材料并加盖公章）**
		支持按照资产总量、存在风险的资产、未受保护的资产、待确认的资产进行计数统计。 支持自动绘制资产变化的统计趋势图
威胁检测	安全告警	★支持包括但不限于 9 类安全检测引擎，终端安全检测引擎、web 攻击检测引擎、ddos 攻击检测引擎、应用安全检测因、网络入侵检测引擎、威胁诱捕检测引擎、威胁情报检测引擎、文件沙箱检测引擎、AI 异常检测引擎**（需提供证明材料并加盖公章）**

2.9 云等保咨询服务

服务	参数
等保定级（1 年一次）	了解客户网络拓扑结构，分解业务系统边界，针对业务系统填报定级备案表；
等保备案	按照定级备案要求，向公安网监处进行报备，获得备案回执

（1 年一次）	
等级保护 差距评估服务 （1 年一次）	**漏洞扫描检测服务：**对客户网络进行定期扫描、发现主机操作系统、网络设备、数据库、安全设备等存在的安全漏洞，弱口令，开放的端口等，并提出安全加固建议。
	渗透测试服务：模拟黑客可能使用的攻击和漏洞发现技术，对目标信息系统进行渗透测试安全验证，发现逻辑性更强、更深层次的弱点，让管理者能够直观了解自己的业务系统、网络及应用层安全漏洞和风险。出具渗透测试报告。
	基线评估服务：对业务系统所有涉及的网络安全设备、主机、数据库、中间件等进行基本配置检查，对不合规的事项提出整改建议。
	管理评估服务：评估安全管理体系，完善管理制度，弥补管理制度缺失项，落实日常运维记录，表单等内容；
等保方案制定 与建设整改 （1 年一次）	**协助制定安全防护建设方案：**协助客户、优化防护方案； 制定安全部署方案；
	配合客户做好设备建设和策略配置，协助出优化方案
	安全运维策略添加与优化：添加防护策略，日常防护优化，保障业务系统安全；
	安全配置整改加固：协助对系统漏洞、网站配置不安全项、应用跨站、后门等脆弱点进行安全整改；
	管理整改：对管理上缺失的制度、流程， 缺失记录、表单等进行弥补；
协助等保测评 （1 年一次）	准备等保测评资料，现场回答测评公司问题，解释答疑；
安全运维服务 （1 年两次）	**日志分析：**收集日志信息，并根据安全动态结合安全工程师的安全经验，分析指定设备的特定时间的日志信息，发现面临的安全风险，并提出建议。 **服务器运维：**用户远程操作都需要通过堡垒机进行，对远程访问人员的所有操作行为进行记录和审计。 **策略优化添加：**添加安全策略，策略优化，并根据检查结果提供改进建议。 **漏洞扫描服务：**提供远程或本地的远程服务器和 WEB 系统的安全检测服务，提供检测报告供用户方进行安全加固和整改。 **安全巡检：**检查设备硬件和软件运行状态，建立运维基线标准。 **系统升级：**安全设备系统升级，维护
安全应急	受到安全攻击、安全事件的应急响应处理；
安全通告 （1 年两次）	负责接受、处理和公开披露的安全漏洞，通过定期的信息安全漏洞信息通报、态势分析报告、研究报告及技术培训与咨询等途径， 帮助用户及时发现并排除自身的信息安全隐患，降低信息安全事件发生的可能性，提高信息安全威胁应对与风险管理的能力和水平。

三、服务期

签订合同日起，至 2025 年 12 月31日。

四、项目管理及验收

第三方应按采购项目需求提供技术服务。服务期满由采购人组织

验收。

五、付款方式

甲方在合同签订之日起 7个工作日内向乙方支付 50%合同款。服务合同期满前一个月，甲方对服务质量进行考核，考核通过后，甲方支付乙方剩余合同款。

第四部分　开启和评审

一、采购人组织评审。

参选人的法定代表人或授权人须持有效身份证参加比选会议。

二、评委会由有关专家和采购人代表组成，按照公平、公正、择优的原则进行独立评审。

由采购人代表对参选人资格性审查，对未通过审查的供应商，应现场告知原因。评委会对合格供应商的比选文件进行评审。

（一）评审内容

1.比选资格是否符合

2.比选文件是否完整；

3.比选文件是否恰当地签署；

4.是否作出实质性响应（**是否有实质性响应，只根据比选文件本身，而不寻求外部证据）；**

5.是否有计算错误。

（二）相应的规定

1.如果单价汇总金额与总价金额有出入，以单价金额计算结果为准；

2.单价金额小数点有明显错位的，应以总价为准；

3.正本与副本有矛盾的，以正本为准；

4.若文件大写表示的数据与数字表示的有差别，以大写表示的数据为准。

三、陈述、演示、答疑、澄清

1.如评委会认为有必要，参选人按评委会的要求作陈述、演示、答疑及澄清其比选内容。时间由评委会掌握。

2.重要澄清答复应是书面的，但不得对比选内容进行实质性修改。

3.对采购过程提出质询的，为各采购程序环节结束之日；

其中：对评审过程中涉及到的密封检查、身份核对、澄清等和程序性事项，供应商如有异议的，必须当场提出。否则，均视为供应商无异议。无论是否成交，供应商事后不得再就前述事项提出任何异议或质询投诉。

四、出现下列情形之一的，作无效比选处理;

1.未按照采购文件规定要求签署、盖章、密封、提交的;

2.不具备采购文件中规定的资格要求的;

3.报价超过采购文件中规定的预算金额或者最高限价的;

4.比选文件含有采购人不能接受的附加条件的;

5.不符合采购文件中规定的其他实质性要求的。

五、出现下列情形之一的，作废标处理

1.符合条件的供应商或者对比选文件作实质响应的供应商不足3家的;

2.出现影响采购公正的违法违规行为的;

3.参选人的报价均超过了采购预算，采购人不能支付的;

4.因重大变故，采购任务取消的。

上述均保留评委会认定可以确定为无效比选或废标的其他情况。

六、采用综合评分法。分资格审查、商务技术响应文件、价格响应文件三部分评审，总分值为100分，加分和减分因素除外。

评委在认真审阅比选文件的基础上，根据各比选文件的商务、技术部分的响应情况，对各评分项目进行评分，不得统一打分。

（一）参选人资格性审查

参选人资格审查不合格的，其比选文件判定为无效比选文件。合格的，评委对其比选文件继续评审。

(二)评分标准与权重

采用综合评分法，根据评分从高到低排序确定成交供应商，评分标准如下:

（三）商务技术分: 80 分

各供应商得分为评审小组成员评分的算术平均分，分值保留小数点后两位。

序号	评审内容	评审要点	分值
1	投标人资质	1、投标人具有ISO9001证书的，得1分; 2、投标人具有ISO27001证书的，得1分; 3、投标人所投云平台供应商在2023年上半年公有云Iaas厂商市场份额占比前三的，得2分; 4、投标人所投云平台具备GPU云主机云服务安全、块存储安全、负载均衡安全、云边协同AI数字孪生、云专网等可信云认证证书的，以上每有1个得1分，最多得2分; 注：以上证书需提供证书原件清晰扫描件并加盖投标供应商公章,证书需在有效期内。	6
2	投标人同类项目案例	投标人自2017年1月1日以来重要行业客户云主机或二级以上等保咨询及测评服务或安全服务等案例，每1个得1分，满分5分。 注：需提供包含合同首页、合同签字盖章页的复印件。	5

3	技术参数响应	投标所投产品完全满足项目招标功能要求， 其中技术参数要求中打“★”项每出现1项负偏离， 扣1分； 其他项不满足每项扣0.5分，扣完为止， 本项最多得20分。 注：投标时需提供证明文件，并加盖公章。	20
4	云服务能力	供应商采用的云服务（云资源服务）中： 1、云主机具备云主机数据存储持久性不低于 99.9999999%，单可用区业务可用性不低于 99.975%，同一区域多可用区业务可用性不低于99.995%。 2、具备云硬盘服务能力，云硬盘数据存储持久性不低于99.9999999%的，且云硬盘数据可销毁性支持数据销毁，业务可用性不低于99.975%的。 3、具备对象存储服务能力，对象存储数据存储持久性不低于99.9999999999% ，且服务可用性不低于99.995%的。 4、具备云备份服务能力，云备份数据存储持久性不低于99.9999999% ，同时业务可用性不低于99.9%。 以上每满足1项得1分，最高得4分，需提供国家认可的第三方评测机构的官网证明截图并加盖投标供应商公章。	4
5	投标人项目组人员素质及资质情况	项目管理团队成员， 具有华为云计算HCIE高级认证证书、华为云计算HCIP证书认证证书、信息安全保障人员认证证书、高级工程师，每提供一个种类的证书得1分，本项最多得4分。	4
6	技术方案	提供技术方案，方案设计合理、内容完整详细得（10,15]分；内容较为完整，内容粗略得（5,10]分；内容比较欠缺不清晰，[5，0]分。	15
7	实施方案	提供实施方案，方案设计合理、内容完整详细得（10,15]分；内容较为完整，内容粗略得（5,10]分；内容比较欠缺不清晰，[0,5]分。	10
8	售后服务方案	提供售后服务方案，方案设计合理、内容完整详细得（6,8]分；内容较为完整， 内容粗略得（3,5]分； 内容比较欠缺不清晰，[0,3]分。	8
9	服务响应	承诺零时延响应， 一般线路故障4小时内修复，得4分。故障发生后能根据要求提供故障分析报告，维修承诺达标的得4分。	8

（四）价格分：20分

价格分统一采用低价优先法计算，即满足比选文件要求且最后报价最低的供应商的价格为基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：

报价得分=（基准价/最终投标报价）×价格权值×100

七、推荐中选服务单位

采用综合评分法的，评审结果按评审后得分由高到低顺序排列。得分相同的，按比选报价由低到高顺序排列。得分且比选报价相同的并列。采取随机抽取的方式确定。

成交供应商无故弃标，或者因其自身原因不再具备成交资格等，按相关规定处理；采购人可以按照评审委员会评审结果，按综合得分从高向低排序，由其他成交候选人递补，或重新组织采购。

八、其他注意事项

1.在比选时间，参选人不得向评委询问情况，不得进行旨在影响评审结果的活动。

2.评委会不得向参选人解释落选原因。

3.在比选、评审过程中，如果参选人联合故意抬高报价或出现其他不正当行为，采购人有权中止比选或评审。

4.凡在比选过程中，采购人已提示是否异议的事项，参选人当时没有提出异议的，事后参选人不得针对上述事项提出质询。比如：采购人在比选中提示评委是否回避，参选人现场未提出异议的，事后不得针对评委回避事项提出质询。

九、成交通知

中选结果在南通市市场监督管理局网站公示，公告期限为1个工作日。《成交通知书》一经发出，如采购单位改变中选结果，或者中选供应商放弃中选的，各自承担相应的法律责任。《成交通知书》是采购合同的组成部分。

十一、其他

当成交供应商无正当理由放弃中选，被查实存在影响成交结果的违法行为等情形，采购人有权按照政府采购相关法律法规的规定对其采取惩戒措施，包含但不限于列入采购失信人黑名单等措施。

当成交供应商放弃成交、因不可抗力不能履行合同，或者被查实存在影响成交结果的违法行为等情形，不符合成交条件的，采购人可以按照评标委员会提出的成交候选人名单排序依次确定其他成交候选人为成交人，也可以重新采购。

第五部分　合同签订与验收付款

一、成交供应商和采购人在接到《成交通知书》后3日内按照采购文件确定的事项签订采购合同。所签合同不得对采购文件作实质性修改。采购人不得向成交供应商提出不合理的要求作为签订合同的条件，不得与成交供应商私下订立背离采购文件实质性内容的协议。

二、采购文件、成交人的响应文件及评审过程中有关书面澄清、承诺等均应作为合同附件，具有同等的法律效力。

三、成交人不得采用转包、分包的形式履行合同，否则，采购人有权终止合同，造成采购人损失的，成交人应承担相应赔偿责任。

四、采购人和成交人应相互配合，按采购合同约定积极组织本项目的实施，确保项目按时完成。

五、成交人履约到位后，应以书面形式向采购人提出验收申请。采购人接到申请后应及时组织验收。

六、采购人、成交人不按采购合同规定履约，出现违约情形，应当及时纠正或补偿，造成损失的，按合同约定追究违约责任；履约中发现有假冒、伪劣、走私产品、商业贿赂等违法情形的，应由采购人移交工商、质监、公安等行政执法部门依法查处。

七、按采购合同约定支付的项目合同价款。

第六部分 响应文件组成

响应文件由资格审查证明材料、商务技术文件、价格文件、电子需要文件四部分组成。

一、资格审查证明材料（不能出现商务技术文件、价格文件）

1.投标人符合投标人资格要求的承诺函（格式见附件 1）；

2.法定代表人身份证明书（格式见附件 2）；

3.法定代表人授权委托书原件，比选代表本人身份证复印件（格式见附件 3）；

4.有效的营业执照复印件加盖公章。

二、商务技术文件（不能出现价格文件）

1. 商务技术评分标准中须提供的相关得分佐证材料；

2. 商务部分正负偏离表；（格式见附件4）

3. 技术部分正负偏离表；（格式见附件 5）

4. 供应商认为需要提交的其他商务技术材料。

三、价格文件

1. 报价总表（格式见附件 6）；

2. 分项报价表（格式见附件 7）；

3. 供应商信用承诺书（格式见附件8）。

四、电子响应文件（U 盘）

附件 1

符合本项目投标人资格要求的承诺函

我单位参加_____（项目名称），_____（项目编号）投标活动。针对本项目投标人资格要求做出如下承诺：

1.我单位具有独立承担民事责任的能力；

2.我单位具有良好的商业信誉和健全的财务会计制度；

3.我单位具有履行合同所必需的设备和专业技术能力；

4.我单位有依法缴纳税收和社会保障资金的良好记录；

5.我单位参加采购活动前三年内，在经营活动中没有重大违法记录；（“较大数额罚款”认定为 200 万元以上的罚款，法律、行政法规以及国务院有关部门明确规定相关领域“较大数额罚款”标准高于 200 万元的，从其规定。）

6.我单位满足法律、行政法规规定的其他条件。

承诺人名称（公章）：

日期：_____年____月____ 日

附件 2

法定代表人身份证明

先生/女士：现任我单位_____职务，为法定代表人，特此证明。 身份证号码：

注：提供法定代表人的身份证复印件盖公章

附件 3

法定代表人授权委托书

本人------（姓名）系————（授权单位名称）的法定代表人，现委托-------（姓名）（身份证号————————）为我方代理人，以我方名义全权处理与本次采购项目（编号：----------）有关的一切事务，其法律后果由我方承担。

本授权书于---年---月---日起生效。代理人无转委托权。

代理人(被授权人):------

授权单位名称（盖章）：-----

授权单位法定代表人（签字或盖章）：-----

XXXX 年 XX 月 XX 日

注：提供投标代表本人身份证复印件盖公章

附件 4

商务部分正负偏离表

（由供应商据实填写，表格不够自行添加）

序号	货物或服务名称	采购文件要求的商务条款	响应文件响应情况	偏离说明
1				
2				
3				
4				

注：

1. 供应商提交的响应文件中与采购文件第三部分“项目需求”中的商务部分的要求，应逐条填列在偏离表中。

2. 如对商务部分条款无任何偏离，参选人仅需在本偏离表中填“无偏离”即可。当本表为空时，视为参选文件对商务部分条款全部满足，无偏离。

3.“偏离说明”一栏选择“正偏离”、“负偏离”、“无偏离”进行填写。正偏离、负偏离、无偏离的确认，由比选小组认定。

4.供应商若提供其他增值服务，可以在表中自行据实填写。

附件 5

技术部分正负偏离表

（由供应商据实填写，表格不够自行添加）

序号	货物或服务名称	采购文件要求的技术要求	响应文件响应情况	偏离说明
1				
2				
3				
4				

注：

1. 供应商提交的响应文件中与采购文件第三部分“项目需求”中的技术部分的要求，应逐条填列在偏离表中。

2. 如对技术部分条款无任何偏离，参选人仅需在本偏离表中填“无偏离”即可。当本表为空时，视为参选文件对技术部分条款全部满足，无偏离。

3.“偏离说明”一栏选择“正偏离”、“负偏离”、“无偏离”进行填写。正偏离、负偏离、无偏离的确认，由比选小组认定。

4.供应商若提供其他增值服务，可以在表中自行据实填写。

附件 6

报价总表

供应商全称（加盖公章）：
项目名称：
项目编号：
分包号：

比选货物、服务名称	总报价
	大写： 小写：元（人民币）

日期：
填写说明：
1、报价总表必须加盖供应商公章（复印件无效）。
2、如有分包，供应商参与任何一个包的标的，都需单独填写报价总表。

附件 7

分项报价明细表

供应商（盖章）：

序号	名称	规格型号	品牌	单位	数量	单价	金额	备注
1								
2								
3								
4								
合计								

附件 8

供应商信用承诺书

为营造公开、公平、公正的公共资源交易环境，树立诚信守法的投标人形象，本人代表本单位作出以下承诺：

一、本单位对所提交的单位基本信息、单位负责人、项目负责人、技术负责人、从业资质和资格、业绩、财务状况、信誉等所有资料，均合法、真实、准确、有效，无任何伪造、修改、虚假成分；

二、严格依照国家和省、市、县关于政府采购等方面的法律、法规、规章、规范性文件，参加公共资源交易招标投标活动；积极履行社会责任，促进廉政建设；

三、严格遵守即时信息公示规定， 及时更新公共资源交易中心主体信息库中信息；

四、自我约束、自我管理，守合同、重信用，不参与围标串标、弄虚作假、骗取中标、干扰评标、违约毁约、恶意投诉等行为， 主动维护公共资源交易招标投标的良好秩序；

五、本单位自愿接受政府采购有关行政监督部门的依法检查。如发生违法违规或不良行为或存在其他法律法规对招标投标行为予以限制的情形，自愿接受政府采购有关行政监督部门依法给予的行政处罚（处理）， 并依法承担相应的法律责任；

六、自觉接受政府部门、行业组织、社会公众、新闻舆论等监督；

七、上述承诺已向本单位员工作了宣传教育；

如有违反上述承诺的不良行为，本单位同意将其予以上网公示。

投标供应商全称(盖公章)：

法定代表人（签字或盖章）：

时间：　年　月　　日

附件 9

质疑函范本

一、质疑供应商基本信息

质疑供应商：

地址：邮编：

联系人：联系电话：

授权代表：

联系电话：

地址：邮编：

二、质疑项目基本情况

质疑项目的名称：

质疑项目的编号：包号：

采购人名称：

采购文件获取日期：

三、质疑事项具体内容

质疑事项 1：

事实依据：

法律依据：

质疑事项 2

……

四、与质疑事项相关的质疑请求

请求：

签字(签章)：　　公章：

日期：

质疑函制作说明：

1.供应商提出质疑时，应提交质疑函和必要的证明材料。

2.质疑供应商若委托代理人进行质疑的，质疑函应按要求列明“授权代表”的有关内容，并在附件中提交由质疑供应商签署的授权委托书。授权委托书应载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.质疑供应商若对项目的某一分包进行质疑，质疑函中应列明具体分包号。

4.质疑函的质疑事项应具体、明确，并有必要的事实依据和法律依据。

5.质疑函的质疑请求应与质疑事项相关。

6.质疑供应商为自然人的，质疑函应由本人签字；质疑供应商为法人或者其他组织的，质疑函应由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。