“市事通•通通检”平台云服务器租赁及
等保服务项目

竞争性磋商文件

南通市质量技术和标准化中心

2025年 11月

目　录

第一部分 竞争性磋商公告

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2025 年11 月26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。具体详见竞争性磋商文件，请仔细研究。

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、竞争性磋商公告期限

自竞争性磋商公告在南通市市场监督管理局网站发布之日起3日。

五、竞争性磋商保证金

本项目不收取竞争性磋商保证金。

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：2025年11月17日至2025年11月26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：2025年11月26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：2025年11月26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 竞争性磋商须知

一、采购文件由采购人解释。

1.供应商获取竞争性磋商文件后，应仔细检查竞争性磋商文件的所有内容，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，请在竞争性磋商文件发布后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竞争性磋商文件所有内容，并由此引起的损失自负。供应商不得在响应结束后针对竞争性磋商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。

采购项目竞争性磋商开始后，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竞争性磋商文件，或者竞争性磋商文件没有对采购文件做出实质性响应，其竞争性磋商将被拒绝，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）竞争性磋商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.供应商应详细阅读竞争性磋商文件的全部内容，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。不按竞争性磋商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“竞争性磋商文件组成”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.竞争性磋商文件（**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.竞争性磋商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竞争性磋商截止时间后递交的竞争性磋商文件。

七、相关费用

1.供应商承担参与竞争性磋商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竞争性磋商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	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 云防火墙

服务	参数
工作模式	支持透明、路由、混合、旁路、虚拟线路5种工作模式。
NAT	支持IPv4/IPv6源NAT、目的NAT、静态NAT；
	支持跨协议NAT转换：NAT64、NAT46，具备IVI、嵌入地址、地址池三种转换形式；
	支持NAT地址池内地址可用性探测，至少包括ICMP、TCP探测手段，同时池内地址可基于源目的哈希、轮询、源地址保持等算法使用。
用户策略	支持基于IPv4/IPv6的用户识别、认证和绑定，提供跨3层IP和MAC地址的绑定功能，可手动导入或导出；
	★支持本地认证、Radius认证、LDAP认证、Portal认证、混合认证、远程服务器认证、短信认证、微信认证、免认证、AD域单点登录和访客二维码等用户认证功能，支持配置强制重新登录间隔，支持设置客户端超时时间，支持自定义认证重定向URL；**（需提供证明材料并加盖公章）**
	提供用户账号防暴力破解功能，可根据同用户或同IP设置防护阈值及锁定时间。
攻击防护	支持IPv4/IPv6 DoS/DDoS攻击防护，如HTTP Flood、DNS Flood、SYN Flood、UDP Flood、ICMP Flood，TCP Flood等；
	支持IPv4/IPv6双协议栈异常包攻击防御，如winnuke、land_base、TCP flag、 tear_drop 、ip spoof等；
	支持基于报文有效性检查及用户合法性检查，防止ARP欺骗，支持ARP flood攻击防御，可基于接口设置ARP报文速率；
	支持对设备自身DOS防护和防扫描功能。
入侵防御	实时攻击源阻断、IP屏蔽、攻击事件记录；
	★内置IPS检测引擎，支持命令执行、目录遍历、缓冲溢出、安全绕过、信息泄露等10余种特征类别，特征库数量不少于11000条，兼容CVE/CNCVE，特征库可直接查阅事件名称、CVE ID、受影响的系统、事件详情、处理建议、补丁下载等详细信息，支持事件集自动和手动两种更新方式；**（需提供证明材料并加盖公章）**
	支持自定义IPS特征，可通过IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等协议自定义入侵攻击特征；可拓展协议字段，设置数据包中的匹配内容；支持选择源目的端口、数据长度；包含、等于、不等于、大于、小于等多种匹配条件，支持设置“与”和“或”的匹配顺序；
	支持非法外联防护功能，通过主机流量自学习，智能分析服务器正常外联行为，允许建立合法连接，也可定义外联白名单地址和端口；
	支持IPS高阶告警功能，可细粒度配置多种告警条件，达到告警阈值可外发邮件或syslog，不同告警规则可以发送给不同的用户。
病毒防护	支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀，支持查杀邮件附件、网页下载文件中包含的病毒；
	预定义20种文件类型，如.vb、.cpl、.pif、.xlsx、.wps等，支持自定义扫描文件类型，支持常见的压缩格式文件扫描，如.tar、.rar、.zip等；

服务	参数
	★支持病毒防护沙箱联动功能，能够将灰文件信息同步云端进行分析，并且返回分析结果；**（需提供证明材料并加盖公章）**
	支持200万余种病毒的查杀，病毒库支持在线或者离线升级；
	支持基于MD5的自定义病毒签名设置例外特征，对特定的病毒特征不进行查杀。
防暴力破解	★支持ttelnet、ftp、imap、pop3、smtp、rlogin、http、oracle、postgres、mysql等常见协议的防暴力破解功能，针对每种协议可自定义检测时长和阈值，并自动将攻击者加入黑名单。**（需提供证明材料并加盖公章）**
应用识别	具备对应用程序的识别和控制能力， 产品内置不少于5000种应用特征，基于覆盖平台、流行度、风险等维度内置不少于20种应用分类，如即时通讯、社交网络、电子邮件、在线视频、文件共享、P2P下载、电子商务、炒股软件、网络游戏、搜索引擎、数据库、代理翻墙等，支持在线更新或手动更新；
	支持常见的国内应用如微信、QQ、新浪微博等，国际应用如Google、Facebook、Twitter等，工业应用协议Modbus、IEC60870-5-101、IEC60870-5-102、IEC60870-5-103、IEC60870-5-104、S7Comm、PMU等；
	支持自定义应用，可基于协议、端口、IP、域名等维度定义应用。
资产管理	支持对IPv4/IPv6资产进行手动添加、扫描发现和流量自学习，支持资产信息列表的导入导出；
	用户可基于资产重要程度、所属部门、操作系统类别等维度修改资产属性信息，同时可与漏洞扫描模块联动，检查资产服务协议开放情况；
	支持通过EDR获取资产IP、操作系统、在线状态等信息，自动同步至防火墙，并支持端点资产病毒检测和响应，联动隔离中毒终端。

2.2 云日志审计

服务	参数
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）**

2.3 云主机防护

服务	参数
架构支持	虚拟化防护软件至少支持Ctrix XEN、VMWare、Hyper-V、H3C、华为、青云、EasyStack、云宏等多种虚拟化平台并可在同一管理平台进行统一管理；
	对windows和linux具备相同的代理部署形式，并且具备统一管理的功能。
病毒查杀功能	除文件类病毒外还需支持对宏病毒、注册表病毒、内存或服务类病毒的查杀，提高虚拟化安全防护等级，对已经运行的病毒进程可以执行关闭。
	★支持通过管控中心设置同一物理机上最大运行的任务数量。**（需提供证明材料并加盖公章）**
	支持本地杀查缓存，优化本地虚拟化环境支持
	能够对虚拟机内部全部文件进行病毒的扫描
	能够对虚拟机内部系统目录进行病毒的快速扫描
	能够对虚拟机内的文件进行进行监控，防止病毒运行
	可以单独配置敲诈者病毒防护功能，防止文件被加密无法打开
	支持隔离网环境的私有云查杀功能以保证内网环境下的病毒查杀率
主机加固	支持对全网虚拟机安全基线进行扫描，并输出扫描结果，以打分形式呈现

服务	参数
功能	支持对安全基线扫描结果分组的一键修复功能，可在控制中心一键下发
	★支持对防暴力破解配置白名单策略，白名单可以配置IP或IP段。**（需提供证明材料并加盖公章）**
管理功能	可提供开放的管理API供其他系统集成
	特征库升级包含自动升级、手动导入的方式
	可以根据不同网络环境提供在线升级和隔离网升级，并提供相应工具
	控制中心可锁定被防护服务器的防病毒策略，保持不被修改
日志报表	记录扫描日志并包括以下字段:计算机名，上报时间，IP地址，文件名，威胁名称，扫描方式，处理结果
	提供多种日志的查看方式，包括报表；实时告警板；日志查询

2.4 云堡垒机

服务	参数
身份认证	支持多因子认证，方式包括手机令牌、谷歌认证、360ID、FreeOTP、手机短信、动态令牌、USBKey、微信小程序等多因子认证方式。
	支持不同的用户配置不同的多因子认证方式，例如user01配置手机令牌、USB Key，user02配置手机短信。
	★支持认证方式组合使用，例如使用AD域+手机短信、AD域+Radius认证、Radius认证+手机令牌等多种组合方式登录。**（需提供证明材料并加盖公章）**
	支持登录失败次数锁死设置，可锁定主账户或IP，可配置解锁时长，到期自动解锁，也可以手动解锁
	支持用户的登录时间、来源IP地址和来源MAC地址限制（黑名单或白名单），限制非法时间和非法地址登录堡垒机

资源账户改密	支持以账户、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
	★改密完成之后，通过邮件将密码发送给指定的管理员，需要指定2个管理员，管理员A收到前半段密码，管理员B收到后半段密码（**需提供证明材料并加盖公章**）
	支持随机生成不同、相同密码或者手动指定密码，改密日志内容包括改密账户总数，成功、失败和未修改数量
	支持修改数据库账户的密码，包括MySQL、Oracle、SQL Server
	支持设置是否使用特权账户改密、是否修改特权账户密码
资源运维	不限操作系统类型，无需安装任何客户端插件，使用浏览器通过H5方式即可直接运维SSH、RDP、Telnet、VNC和应用发布资源
	通过H5运维RDP资源时，支持自定义分辨率
	支持通过Web页面调用本地 计算机的Navicat、MySQL Administrator、MySQL CMD、PLSQL、SSMS、DB2CMD等客户端工具访问数据库资源
	支持直接使用Xshell、SecureCRT、Putty、MSTSC等客户端访问目标资源，无需通过Web页面调用

2.5 云WAF

服务	参数
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参数合规标准，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，支持上传证书及密钥
	支持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LDAP、XPATH、struct2/xworks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

审计及告警	支持日志定期自动备份导出
	★要求攻击日志具备详细的攻击和原始报文摘要**（需提供证明材料并加盖公章）**
	支持日志可视化，可对访问日志、攻击日志等日志进行二次分析，并通过饼图、曲线图及柱图等对分析结果进行图形化统计
监控及报表	★支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标服务器、攻击类型、攻击趋势、流量趋势及实时事件的动画统计**（需提供证明材料并加盖公章）**
	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、攻击类型、攻击时间（或者发现攻击的时间）等进行统计并排名
	支持以Word、PDF、HTML等通用格式导出报表

2.6 安全运营中心

服务	参数
安全可视	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
	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
	支持自定义大屏logo 与标题
	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
	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	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
	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）

服务	参数
	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	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

2.7 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（1 年一次）	按照定级备案要求，向公安网监处进行报备，获得备案回执
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；

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2026 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竞争性磋商会议。

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竞争性磋商文件进行评审。

（一）评审内容

1.竞争性磋商资格是否符合

2.竞争性磋商文件是否完整；

3.竞争性磋商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，只根据竞争性磋商文件本身，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、答疑及澄清其竞争性磋商内容。时间由评委会掌握。

2.重要澄清答复应是书面的，但不得对竞争性磋商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，作无效竞争性磋商处理;

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.竞争性磋商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竞争性磋商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竞争性磋商或废标的其他情况。

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。

评委在认真审阅竞争性磋商文件的基础上，根据各竞争性磋商文件的商务、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，其竞争性磋商文件判定为无效竞争性磋商文件。合格的，评委对其竞争性磋商文件继续评审。

(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、投标供应商具有ISO9001质量管理体系认证证书，得1分； 2、投标供应商具有ISO27001信息安全管理体系认证证书，得1分； 注：提供有效期内的证书扫描件加盖投标供应商公章，不提供不得分。	16
		1、投标人所投云产品厂商在2024年下半年公有云laas厂商市场份额占比前三的，得4分，市场份额占比第四、五的，得2分。（提供IDC中国的证明截图并加盖投标人公章）； 2、投标人所投云产品厂商具有ITSS云服务（SAAS云）证书，一级得4分，二级得2分。（提供有效期内的证书扫描件加盖投标供应商公章） 3.投标人所投云产品厂商具有ITSS云服务（IAAS公有云)证书，一级得4分，二级得2分。（提供有效期内的证书扫描件加盖投标供应商公章） 4.投标人所投云产品厂商具有保密管理体系认证证书的得2分。（提供有效期内的证书扫描件加盖投标供应商公章）	
2	**投标人同类项目案例**	投标供应商自2020年1月1日以来具有类似案例的，提供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	**投标人项目组人员素质及资质情况**	1. 本项目拟派团队的项目负责人具备注册信息安全专业人员（CISP）、云计算安全认证证书（CCSK认证）、ITIL服务管理证书和信息系统项目管理师的，有一个得1分，同时具备的得5分。 2. 除项目经理外本项目拟派项目组其他团队人员中具备PMP、信息安全工程师证书、系统集成项目管理工程师的，有一个得1分，共3分。 注：以上人员不得重复，提供相关证书复印件及2025年任意一个月为其缴纳的社保证明材料并加盖公章，不提供不得分。	8
5	**技术方案**	提供技术方案，方案设计合理、内容完整详细得（6,10]分；内容较为完整，内容粗略得（3,6]分；内容比较欠缺不清晰，[0，3]分。	10
6	**实施方案**	提供实施方案，方案设计合理、内容完整详细得（6,9]分；内容较为完整，内容粗略得（3,6]分；内容比较欠缺不清晰 ，[0,3]分。	9
7	**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（3,6]分；内容比较欠缺不清晰，[0,3]分。	8
8	**服务响应**	承诺零时延响应，一般线路故障4小时内修复，得2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2分。	4

（四）价格分：20分

价格分统一采用低价优先法计算，即满足竞争性磋商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，按竞争性磋商报价由低到高顺序排列。得分且竞争性磋商报价相同的并列。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.在竞争性磋商时间，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.在竞争性磋商、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，采购人有权中止竞争性磋商或评审。

4.凡在竞争性磋商过程中，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：采购人在竞争性磋商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，竞争性磋商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，由竞争性磋商小组认定。

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，由竞争性磋商小组认定。

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：

竞争性磋商货物、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。