国家税务总局江苏省税务局网络安全系统与设备采购项目业务需求

一、项目基本情况

1.项目编号：JSZC-320000-SCZX-G2024-0522

2.项目名称：国家税务总局江苏省税务局网络安全系统与设备采购

3.预算金额：217.324 万元

4.最高限价：217.324 万元

5.采购需求(简介)：拟采购运维堡垒机　4 台、API 接口安全监测系统 2 台、边界防护设备 4 台。技术参数详见招标文件。

6.合同履行期限：自合同签订后 15 个工作日内供货并完成安装软、硬件设备的到货、安装、集成并交付使用。

采购需求

采购标的清单

采购包	序号	采购标的	对应中小企业划分标准所属行业
1	1	运维堡垒机	工业
	2	API 接口安全监测系统	工业
	3	边界防护设备	工业

一、招标设备名称及数量：

序号	设备名称	数量	单位	是否核心产品
1	运维堡垒机	4	台	核心产品
2	API 接口安全监测系统	2	台	
3	边界防护设备	4	台	

二、设备用途

为强化国家税务总局江苏省税务局网络和数据安全防护工作，有效应对内外部威胁风险，实时监控 API 接口活动，对节点出入流量中的入侵攻击、僵尸网络攻击、恶意程序检测，防御识别和阻止未授权的访问、数据泄露等安全威胁，提升运维风险控制与审计能力。项目计划采购 API 接口安全监测设备、堡垒机和边界防护设备等安全设备。

三、技术要求

1、运维堡垒机4台

4 台堡垒机将其两两部署在国家税务总局江苏省税务局互联网区和外联网区做 HA 部署或集群部署。

产品指标项		序号	产品性能参数和要求
规格要求		★	标准 2U 设备； 1+1 冗余电源；≥4 个千兆自适应电口，≥4 个千兆光口（满配光模块），≥2 个万兆光口（满配光模块）；硬盘容量≥24TB，RAID 后实际可用空间≥16TB；设备须提供用于单独管理维护升级的管理接口，不能占用业务口；提供≥20 个免费的国密硬件动态令牌。
管理资源数		★	每台≥1000 个（4 台可以提供资源数≥5000 个，4 台堡垒机在两个网区集群部署，后期可根据采购人需求进行调整)
用户管理要求	管理角色定义	▲	用户管理可对用户角色分权、用户认证及身份识别进行集中统一管理。其中，管理员角色不能有固定的局限性，能够根据工作实际需要灵活调整，可自定义用户的角色，灵活设置具有不同权限的账户，如用户管理员、审计管理员、业务系统管理员等，对应管理员账号可监测管理自己负责的账号、资产组等，进行策略配置、日志审计和资产管理。
	登录安全	★	为了实现登录安全，除支持用户自行设置的本地密码外，还需要支持其他认证方式做组合认证来加强登录验证的安全性，确保一个账号对应一个真实的操作人员，其他认证方式包括但不局限于动态令牌、手机短信、USBKey 等。支持使用国密令牌认证，并且能够和本地密码或者其他认证方式组成双因素认证。
		1	密码到期自动提醒，可以设定用户密码过期前多少天前，当用户登录后主动弹窗提醒或强制要求用户修改密码。
		2	支持使用国密算法保证 HTTPS 协议层面的数据机密性和完整性；开启后支持设置需同时使用支持国密算法的浏览器、国密 USBkey 才能访问堡垒机的功能，只使用国密浏览器无法访问堡垒机，以此种方式对发起连接的客户端身份进行验证。
登录方式		▲	支持 B/S 方式登录，支持主流的浏览器（IE、chrome、火狐、360 等），不需要安装任何插件就可以使用堡垒机的全部功能。 对于一些字符会话，可以直接通过 SecureCRT 等客户端直接访问堡垒机进行运维。 支持软件下载例如：浏览器或 CRT。 支持国产化操作系统登录运维，如银河麒麟、华为欧拉等。 支持 Web、Mstsc、SSH Client 等多种模式登录堡垒机后访问目标资产。支持 HTML5 方式运维，无需安装任何插件。
资源	资源类型	3	支持对用户业务系统所属的服务器主机（Windows\linux）、数据库(Oracle 、 MySQL 、 HBase 、 PostgreSQL 、 redis 、 mongodb ，

管理要求			clickhouse、TDSQL、TDSQL PostgreSQL 版等)、应用系统等资源进行统一管理。支持以可视化方式自定义业务系统架构，并提供目标资源、业务系统灵活管理参数配置等基础功能（设备名、IP、系统账号、密码等）。
	密码管理要求	4	支持对常见数据库及国产数据库的自动改密功能，包括 Oracle、MySQL、HBase、PostgreSQL、redis、mongodb，clickhouse、TDSQL、TDSQL PostgreSQL 版等；支持对 Web 应用的自动改密功能，并且支持随堡垒机提供的改密插件录制向导，通过改密插件自动生成 web 应用的改密脚本。
	连通性验证	5	添加被管理资源后的可以通过 ping 连通性测试和资产登录测试，可以测试运维端口号是否连通；
	IPv6 要求	6	支持部署在 IPv6 环境中，设备接口及部署模式均支持 ipv6 配置；支持对 IPV6 设备进行运维管理。
运维权限设置		7	堡垒机安全管理模块支持基于用户/用户组、设备/设备组、系统帐号、登录时间规则设置访问控制规则，防止非授权访问的问题。
		8	权限支持按照用户（用户组）、资产（资产组）及资产协议和账号进行授权，也能够对用户、资产和账号进行自定义属性，通过这些属性的多条件匹配实现动态授权。
		9	针对一些重要的设备和系统，支持基于运维规则、用户、用户组的高危命令权限控制，当用户试图去执行高危命令时，会被系统自动给予阻断命令、阻断会话、需要审批、直接放行操作；高危命令权限控制要求支持使用通配符和正则表达式匹配。
		10	支持对以 rdp 协议登录到目标设备，可限制剪贴板的文件上行、字符上行、文件下行、字符下行操作，细化运维权限安全。
		11	支持对重要设备启用登录审核功能，运维人员须向管理员申请登录，管理员允许之后才可登录；并且管理员在审批时可以设置审批有效期，及在有效期内是否不限制登录次数。
应用客户端密码代填		12	系统支持各类客户端工具应用发布密码代填，如 Oracle、MySQL、HBase、navicat、PL/SQL 等数据库密码代填，防止用户私自切换数据库实体。
资产访问		13	每个用户都可以按照自己定义的属性，以树状结构方式展现自己可访问的资产信息； 支持批量启动需要巡检的设备，一次性登录选择好的目标设备。 如果需要其他人协助运维，可支持设置共享账户且可以导出，用于不同主机拥有相同账户名及密码的场景。
审计功能	操作审计	14	堡垒机完整记录操作人员在目标设备上进行的 SSH、RDP、Http、Https、SFTP、SCP 等协议的操作行为，包含图形会话审计和字符会话审计，支持对审计记录进行回放、查看、搜索定位等提高审计效率的功能，要求不能有播放乱码或者运维操作命令丢失的现象。 图形会话审计主要以录像方式记录，在录像方式记录用户操作过程的同时，还需要文本方式完整记录用户的键盘操作、复制粘贴操作；要求图形化操作日志的回放支持：（1）多倍速回放（2）自动过滤屏幕静止操作（3）根据时间点直接定位回放； 字符会话主要以文本方式记录，确保支持对各种常规和非常规操作行为（如 TAB 键补全、上下键翻历史命令、复制一段长命令执行等）

			的准确识别，支持任意字符命令处进行操作日志回放
	操作实时监控与控制	15	操作员登录到目标设备上正在进行的任意类型操作，审计管理员可以在运维审计系统的 WEB 界面做到实时监控和切断，做到边操作边审计，真正实现操作过程透明化。
	数据库审计	16	支持数据库客户端工具对 Oracle、MySQL、HBase、PostgreSQL、redis、mongodb，clickhouse、TDSQL、TDSQL PostgreSQL 版等数据库进行操作时，将后台交互的 SQL 语句文本提取，支持以完整的 sql 语句进行文本检索并定位播放，支持将客户端（如 Oracle、MySQL、HBase、navicat、PL/SQL）的操作还原为 SQL 语句用于实现快速检索审计。
	文件传输审计	17	支持对常见文件传输进行操作审计，支持保存 SSH 的 sz/rz 命令（zmodem）和 SFTP/FTP 传输的原始文件；支持对常见文件传输进行操作审计，如 SFTP、RZ/SZ、Windows 剪切板、磁盘映射等操作进行留痕审计，并对上传、下载两个文件传输动作涉及的原文件审计备份下来，方便事后查看审计原文件内容。
	操作审计检索	18	图形操作记录，根据键盘事件、会话指令、文件操作、鼠标轨迹为关键字进行检索定位； 字符操作记录，按照时间、用户账号、目标设备、系统账号、命令关键字进行检索，在最短的时间内找到相关日志内容，实现快速定位； 数据库操作记录，按照 sql 语句关键字进行检索定位； 文件传输审计记录，支持用户、传输动作、设备等条件组合查询，支持对所传输原文件下载查看。
回退支持		19	支持系统升级后回退至升级前的版本，方便用户处理割接过程中的突发情况。
命令审批		★	支持对重要命令进行审核：支持设置对重要命令进行审核，可通过设备内置或自定义的方式设置需审批的命令，并对用户操作命令进行匹配监测。运维人员执行重要命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。
会话访问		20	操作员通过堡垒机进行设备访问操作，同时兼容用户对主流的运维协议支持直接调用本地终端第三方工具（如 mstsc、xshell 等），支持调用 windows、Linux（含银河麒麟、华为欧拉等国产操作系统）终端。
统计报表		21	设备支持报表输出内容自定义，支持的报表类型包括：用户运维报表、资产运维报表、高危命令审计报表。报表内容包括：运维次数、运维时长、活动时长、会话大小、字符命令数、传输文件数、来源 IP 访问数、运维时间分布等。报表可自定义统计周期，支持设置定期自动生成可自定义范围和内容报表。
部署要求		★	要求设备支持并提供以下功能： HA 部署、双活部署模式，支持审计数据能自动同步至备机，可自定义是否同步录像审计。 集群部署模式，中心可采用 HA，支持节点可以横向扩展，实现统一登录入口、统一配置同步、审计日志集中存储、实时会话集中监控，以满足业务增长需求。 同时集群模式下，可选择多种集群选路方式，满

		足不同场景下的访问路径。
设备数据对接	▲	设备支持 SNMP、syslog 等方式读取系统性能指标实时监控功能和告警信息外发，包括不限于 CPU、内存、存储等监控指标，并提供 OID 说明
产品资质	★	1.本设备属于网络关键设备或网络安全专用产品，应严格执行国家互联网信息办公室、工业和信息化部、公安部、财政部和国家认证认可监督管理委员会 2023 年第 1 号《关于调整网络安全专用产品安全管理有关事项的公告》及国家互联网信息办公室、工业和信息化部、公安部和国家认证认可监督管理委员会 2023 年第 2 号《关于调整<网络关键设备和网络安全专用产品目录>的公告》等相关文件要求，所投标(响应)设备或产品至少符合以下条件之一:一是已由具备资格的机构安全认证合格或安全检测符合要求;二是已获得《计算机信息系统安全专用产品销售许可证》，且在有效期内。**（须提供对应证书复印件。）** 2.产品为自主研发，主要程序具备国家版权局颁发的软件著作权登记证书。**（须提供对应证书复印件。）**

2、API接口安全监测系统 2台

2 台 API 接口安全监测系统，一台部署在国家税务总局江苏省税务局互联网区，主要用于检测拦截互联网区服务器和对公网提供 API 接口的服务器恶意流量；一台部署在国家税务总局江苏省税务局业务专网区，主要用于监测审计业务专网区服务器 API 接口调用。

（1）业务专网区 1 台

技术指标项		序号	功能参数
规格	硬件规格	★	标准 2U 机架式硬件设备，1+1 冗余电源； 应用层处理能力≥5Gbps； 提供≥4 个 10/100/1000M 自适应千兆电口；≥2 个千兆 SFP 接口（满配光模块）；≥2 个万兆 SPF+接口（满配光模块）； 设备须提供用于单独管理维护升级的管理接口，不能占用业务口； 支持 IPv4 和 IPv6 环境的部署；
部署	部署方式	★	系统支持硬件旁路监听流量的方式，自动分析网络环境中业务系统关联数据访问信息。
资产梳理	接口解析	▲	设备支持并提供识别流量中的接口，在 web 界面能够查询和查看接口信息，接口信息包括接口地址、所属域名或应用、被访问量、接口包含的敏感信息标签等信息
	接口类型识别	1	设备支持并提供内置识别接口类型，根据接口功能分类包括但不限于登录接口、包含敏感数据的接口、包含脱敏数据的接

			口、上传接口、下载接口等
	账号资产识别与管理	▲	设备支持并提供账号资产识别与管理，支持从流量中解析还原应用系统登录账号，支持账号解析的位置至少包含：请求头、请求体、响应头、响应体，可编辑其他属性，如账号所属终端IP、所属部门等。**（提供设备生产厂商认可的对应功能截图或第三方产品检测报告等相关技术支持资料，功能参数应进行明显标注，采用如箭头、标红或下划线等标注方式，并附功能响应承诺书，承诺功能真实有效，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理）**
	敏感数据识别	2	设备支持并提供内置和自定义敏感数据类型标签包括但不限于：手机号、个人姓名、住址、电子邮箱、生日、民族、性别、银行账户卡号、身份证号、统一社会信用代码、业务系统账号，可以通过 web 进行查看和管理
	接口清单	3	设备支持并提供以表格形式导出 API 接口清单，导出的文件包括接口地址、所属域名或应用、接口包含的敏感信息标签等信息；
	接口管理	★	设备支持并提供手动添加单个 API 接口；设备支持并提供通过 web 页面对自动识别和手动添加的接口进行管理，能够查看接口的 URI、目的 IP、端口、请求数据标签、返回数据标签、首次访问时间、最后访问时间等信息；能够编辑接口名称、接口功能类型、接口标签等信息
风险监测	弱点识别	4	设备支持并提供内置弱点发现规则包括但不限于明文密码传输、弱口令、弱加密、接口执行命令、接口可执行 SQL、接口未鉴权、单次返回大量或多种敏感数据、URL 中包含敏感信息、文件目录暴露、SQL 注入、登录错误提示不合理等。
	自定义弱点检测项	5	设备支持并提供新建自定义的弱点检测项，可以根据需要修改弱点发现规则，如调整各类参数阈值、增加删除弱口令字典等
	内置风险模型规则	▲	设备支持并提供内置风险规则包括但不限于超量爬取、高频爬取、账号访问数据类型和数据量异常、单 IP 访问量异常、路径探测、账号共用、撞库、短信轰炸等；
	自定义风险模型配置与使用	★	设备支持并提供自定义告警策略配置，可针对指定的风险对象建立监测告警模型：指定账号，指定网段，指定时间段，指定应用系统、指定业务系统账号、指定数据项、指定接口,指定风险周期、秒、分钟、天，设定多种风险指标；
	行为基线	6	设备支持并提供基于应用、接口、账号、IP 等维度建立多维度行为基线，设置异常行为检测规则
	旁路阻断	▲	设备支持并提供对自定义恶意 IP 进行旁路封堵(非联动方式)；支持并提供批量导入 IP、导入 IP 可分组管理、自定义封堵 IP 时长。
数据审计	取证溯源	★	设备支持并提供针对监测发现的安全事件提供取证溯源能力，对事件相关的原始数据进行完整证据固定，支持对取证相关数据进行脱敏展示，支持基于角色控制对审计敏感内容的脱敏显示。 设备支持并提供对已记录 API 数据包的来源和目标地址、端口信息、完整 X-Forwarded-For 地址信息进行关键字检索；

			设备支持并提供对收集的网络流量进行全量审计和分析，可基于主体用户账号/用户访问 IP 等进行检索，可通过选中一次访问事件进行账号/用户的访问轨迹查看
数据分析	数据流向分析	7	设备支持并提供针对敏感数据绘制包含但不限于应用、接口、访问源、应用账号等信息的访问流向图，对敏感数据数量进行统计展示与列举分析
	资产信息分析	▲	设备支持并提供以应用和接口视角查看指定应用和接口的资产信息，包括但不限于敏感数据分布、访问趋势变化、风险情况等
	应用数据分析	8	设备支持并提供显示指定应用的所有接口以及接口类型、数据类型、数据流向、风险点等信息
	接口数据分析	9	设备支持并提供展示接口列表以及各接口访问量，能够按时间检索访问指定接口次数 IP 地址 TOP10、指定时间段内访问次数 IP 地址 TOP10、指定时间段内单个 IP 地址所有的访问行为
报表输出	风险审计报表	10	设备支持并提供以 docx、csv、pdf 等文件格式导出报表，支持并提供多种数据报表功能，报表内容可自定义，包含审计的应用数量、所属接口数量、审计事件数量、事件类型（登录、文件上传、下载、服务接口等）、告警事件数据等
	自定义审计报表	▲	设备支持并提供报表可自定义输出内容，支持按应用筛选导出审计报表，包含接口数量、审计事件数量、事件类型（登录、文件上传、下载、服务接口等）、告警事件数据等；支持并提供按应用风险情况导出审计报表，包含风险数量、各应用风险等级分布、风险事件类型分布情况等；支持并提供按弱点分析情况导出审计报表，包含审计应用清单、应用接口弱点数量、接口弱点类型统计、应用接口弱点类型分析等**（提供设备生产厂商认可的对应功能截图或第三方产品检测报告等相关技术支持资料，功能参数应进行明显标注，采用如箭头、标红或下划线等标注方式，并附功能响应承诺书，承诺功能真实有效，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理）**
管理功能	设备数据对接	▲	设备支持 SNMP、syslog 等方式读取系统性能指标实时监控功能和告警信息外发，包括不限于 CPU、内存、存储等监控指标，并提供 OID 说明
	设备账号管理	11	设备支持并提供账号支持三权分立模式，可新建和配置用户管理员、审计管理员、业务系统管理员账号，并能够以应用系统所属分配操作权限，实现权限和数据隔离，对应管理员账号可监测自己负责的域名、账号、资产组，进行策略配置、日志查看和资产管理
质保	原厂质保	★	提供 3 年的质保服务、软件版本升级及使用培训
资质要求	产品资质	★	1.本设备属于网络关键设备或网络安全专用产品，应严格执行国家互联网信息办公室、工业和信息化部、公安部、财政部和国家认证认可监督管理委员会 2023 年第 1 号《关于调整网络安全专用产品安全管理有关事项的公告》及国家互联网信息办公室、工业和信息化部、公安部和国家认证认可监督管理委员会 2023 年第 2 号《关于调整<网络关键设备和网络安全专用产品目录>的公告》等相关文件要求，所投标(响应)设备或产品至少

			符合以下条件之一:一是已由具备资格的机构安全认证合格或安全检测符合要求;二是已获得《计算机信息系统安全专用产品销售许可证》，且在有效期内。**（须提供对应证书复印件。）** 2.产品为自主研发，主要程序具备国家版权局颁发的软件著作权登记证书。**（须提供对应证书复印件。）**

（2）互联网区 1台

技术指标项		序号	功能参数
规格	硬件规格	★	标准 2U 机架式硬件设备，1+1 冗余电源； 应用层处理能力≥5Gbps； 提供≥4 个 10/100/1000M 自适应千兆电口；≥2 个千兆 SFP 接口（满配光模块）；≥2 个万兆 SPF+接口（满配光模块）； 设备须提供用于单独管理维护升级的管理接口，不能占用业务口； 支持 IPv4 和 IPv6 环境的部署；
部署	部署方式	★	系统支持硬件旁路监听流量的方式，自动分析网络环境中业务系统关联数据访问信息。
资产梳理	接口解析	▲	设备支持并提供识别流量中的接口，在 web 界面能够查询和查看接口信息，接口信息包括接口地址、所属域名或应用、被访问量、接口包含的敏感信息标签等信息
	接口类型识别	1	设备支持并提供内置识别接口类型，根据接口功能分类包括但不限于登录接口、包含敏感数据的接口、包含脱敏数据的接口、上传接口、下载接口等
	账号资产识别与管理	▲	设备支持并提供账号资产识别与管理，支持从流量中解析还原应用系统登录账号，支持账号解析的位置至少包含：请求头、请求体、响应头、响应体，可编辑其他属性，如账号所属终端 IP、所属部门等。**（提供设备生产厂商认可的对应功能截图或第三方产品检测报告等相关技术支持资料，功能参数应进行明显标注，采用如箭头、标红或下划线等标注方式，并附功能响应承诺书，承诺功能真实有效，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理）**
	敏感数据识别	2	设备支持并提供内置和自定义敏感数据类型标签包括但不限于：手机号、个人姓名、住址、电子邮箱、生日、民族、性别、银行账户卡号、身份证号、统一社会信用代码、业务系统账号，可以通过 web 进行查看和管理
	接口清单	3	设备支持并提供以表格形式导出 API 接口清单，导出的文件包括接口地址、所属域名或应用、接口包含的敏感信息标签等信息；
	接口管理	★	设备支持并提供手动添加单个 API 接口；设备支持并提供通过 web 页面对自动识别和手动添加的接口进行管理，能够查看接口的 URI、目的 IP、端口、请求数据标签、返回数据标签、首次访问时间、最后访问时间等信息；能够编辑接口名称、接口功能类型、接口标签等信息
	接口主动发现	▲	设备支持并提供扩展 API 接口资产的主动扫描发现功能，通过添加扫描任务可以自动发现 API 接口资产、API 接口风险和暴露的敏感信息。**（提供设备生产厂商认可的对应功能截图或第**

			三方产品检测报告等相关技术支持资料，功能参数应进行明显标注，采用如箭头、标红或下划线等标注方式，并附功能响应承诺书，承诺功能真实有效，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理）
风险监测与防护	弱点识别	4	设备支持并提供内置弱点发现规则包括但不限于明文密码传输、弱口令、弱加密、接口执行命令、接口可执行 SQL、接口未鉴权、单次返回大量或多种敏感数据、URL 中包含敏感信息、文件目录暴露、SQL 注入、登录错误提示不合理等。
	自定义弱点检测项	5	设备支持并提供新建自定义的弱点检测项，可以根据需要修改弱点发现规则，如调整各类参数阈值、增加删除弱口令字典等
	内置风险模型规则	▲	设备支持并提供内置风险规则包括但不限于超量爬取、高频爬取、账号访问数据类型和数据量异常、单 IP 访问量异常、路径探测、账号共用、撞库、短信轰炸等。
	自定义风险模型配置与使用	★	设备支持并提供自定义告警策略配置，可针对指定的风险对象建立监测告警模型：指定账号，指定网段，指定时间段，指定应用系统、指定业务系统账号、指定数据项、指定接口,指定风险周期、秒、分钟、天，设定多种风险指标；
	行为基线	6	设备支持并提供基于应用、接口、账号、IP 等维度建立多维度行为基线，设置异常行为检测规则。
	自定义防护规则	▲	设备支持并提供当请求触发防护规则时，可以设定多种拦截策略，如：阻挡，延时等；且可配置上述拦截策略按百分比随机响应。 设备支持并提供根据 API 接口的异常行为进行基于 referer、请求方式、参数、频率等进行多维度组合定义拦截防护。
	旁路阻断	▲	设备支持并提供对自定义恶意 IP 进行旁路封堵(非联动方式)；支持并提供批量导入 IP、导入 IP 可分组管理、自定义封堵 IP 时长。
数据审计	取证溯源	★	设备支持并提供针对监测发现的安全事件提供取证溯源能力，对事件相关的原始数据进行完整证据固定，支持对取证相关数据进行脱敏展示，支持基于角色控制对审计敏感内容的脱敏显示。 设备支持并提供对已记录 API 数据包的来源和目标地址、端口信息、完整 X-Forwarded-For 地址信息进行关键字检索； 设备支持并提供对收集的网络流量进行全量审计和分析，可基于主体用户账号/用户访问 IP 等进行检索，可通过选中一次访问事件进行账号/用户的访问轨迹查看
数据分析	数据流向分析	7	设备支持并提供针对敏感数据绘制包含但不限于应用、接口、访问源、应用账号等信息的访问流向图，对敏感数据数量进行统计展示与列举分析
	资产信息分析	▲	设备支持并提供以应用和接口视角查看指定应用和接口的资产信息，包括但不限于敏感数据分布、访问趋势变化、风险情况等
	应用数据分析	8	设备支持并提供显示指定应用的所有接口以及接口类型、数据类型、数据流向、风险点等信息
	接口数据分析	9	设备支持并提供展示接口列表以及各接口访问量，能够按时间检索访问指定接口次数 IP 地址 TOP10、指定时间段内访问次数

			IP 地址 TOP10、指定时间段内单个 IP 地址所有的访问行为
报表输出	风险审计报表	10	设备支持并提供以 docx、csv、pdf 等文件格式导出报表，支持并提供多种数据报表功能，报表内容可自定义，包含审计的应用数量、所属接口数量、审计事件数量、事件类型（登录、文件上传、下载、服务接口等）、告警事件数据等
	自定义审计报表	▲	设备支持并提供报表可自定义输出内容，支持按应用筛选导出审计报表，包含接口数量、审计事件数量、事件类型（登录、文件上传、下载、服务接口等）、告警事件数据等； 支持并提供按应用风险情况导出审计报表，包含风险数量、各应用风险等级分布、风险事件类型分布情况等；支持并提供按弱点分析情况导出审计报表，包含审计应用清单、应用接口弱点数量、接口弱点类型统计、应用接口弱点类型分析等**（提供设备生产厂商认可的对应功能截图或第三方产品检测报告等相关技术支持资料，功能参数应进行明显标注，采用如箭头、标红或下划线等标注方式，并附功能响应承诺书，承诺功能真实有效，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理）**
管理功能	设备数据对接	▲	设备支持 SNMP、syslog 等方式读取系统性能指标实时监控功能和告警信息外发，包括不限于 CPU、内存、存储等监控指标，并提供 OID 说明
	设备账号管理	11	设备支持并提供账号支持三权分立模式，可新建和配置用户管理员、审计管理员、业务系统管理员账号，并能够以应用系统所属分配操作权限，实现权限和数据隔离，对应管理员账号可监测自己负责的域名、账号、资产组，进行策略配置、日志查看和资产管理
质保	原厂质保	★	提供 3 年的质保服务、软件版本升级及使用培训
资质要求	产品资质	★	1.本设备属于网络关键设备或网络安全专用产品，应严格执行国家互联网信息办公室、工业和信息化部、公安部、财政部和国家认证认可监督管理委员会 2023 年第 1 号《关于调整网络安全专用产品安全管理有关事项的公告》及国家互联网信息办公室、工业和信息化部、公安部和国家认证认可监督管理委员会 2023 年第 2 号《关于调整<网络关键设备和网络安全专用产品目录>的公告》等相关文件要求，所投标(响应)设备或产品至少符合以下条件之一:一是已由具备资格的机构安全认证合格或安全检测符合要求;二是已获得《计算机信息系统安全专用产品销售许可证》，且在有效期内。**（须提供对应证书复印件。）** 2.产品为自主研发，主要程序具备国家版权局颁发的软件著作权登记证书。**（须提供对应证书复印件。）**

3、边界防护设备4台

根据接入模式要求，四台设备两两主备部署，将采用串联方式部署在国家税务总局江苏省税务局广域网边界。

指标项	序号	技术参数指标

基本参数	★	≤2U，≥4 个自适应千兆电口，≥4 个千兆 SFP 接口（满配光模块），≥4 个万兆 SFP+插槽（满配光模块），1+1 冗余电源，整机吞吐率≥15Gbps，最大并发连接数≥300 万，IPS 应用层吞吐率≥10Gbps，支持 HA 模式，包含边界防护设备规则库三年升级许可，病毒库三年升级许可，三年硬件维保服务。提供 IPv6 支持。
软件	★	软件系统采用自主知识产权的专用安全操作系统，具备多核平台并行处理特性。提供多操作系统引导。
接入模式	★	要求设备提供路由、交换、虚拟线、聚合、监听、混合部署等多种接入模式，支持并提供主备配置同步功能。
入侵防御引擎	1	系统应具备：融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵防御。
	2	要求提供攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据。
攻击防御类型	▲	要求提供检测包括扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击等在内的网络攻击事件的功能。**（提供设备生产厂商认可的对应功能截图或第三方产品检测报告等相关技术支持资料，功能参数应进行明显标注，采用如箭头、标红或下划线等标注方式，并附功能响应承诺书，承诺功能真实有效，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理）**
	3	要求提供针对 HTTP、DNS、SMTP、POP3、IMAP、FTP 进行智能检测，支持报文乱序和重组依然识别传输过程中的文件。
	4	要求提供对 SMTP、IMAP、POP3、FTP、SMB、TELENT、LDAP、ORACLE、MYSQL、MSSQL、MONGODB、POSTGRESQL、DB2、REDIS、CLICKHOUSE、 HTTP 等服务的弱口令检测，至少提供弱口令字典暴力破解和口令强度两种方式，可自定义口令强度规则，如密码长度、密码字符类型等。支持对发生的弱口令事件进行取证和在线阻断。
	5	要求提供暴力破解检测，包括 SMTP、IMAP、POP3、FTP、SMB、TELENT、LDAP、ORACLE、MYSQL、MSSQL、MONGODB、POSTGRESQL、DB2、REDIS、CLICKHOUSE、HTTP 等服务的登录行为检测。对请求响应流量进行分析，研判登录成功和异常登录失败行为，提供可自定义检测周期和检测次数的功能。提供对发生的暴力破解行为事件进行取证功能。
DDoS 检测防御	6	要求系统提供 DDoS 检测、阻断及防御基线自学习功能，能够进行自学习配置、自学习结果查看、防护配置设置。可设定学习时长，根据周期内流量状态自动学习，设置检测流量阈值。流量异常触发阈值系统自动进行告警并处置防御。
僵尸主机防御	▲	采用僵尸主机与控制主机异常通信行为检测的方式，具有独立的僵尸主机特征库，能够对僵尸主机行为进行监测，包括僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT 等多类型的僵尸主机行为。**（提供设备生产厂商认可的对应功能截图或第三方产品检测报告等相关技术支持资料，功能参数应进行明显标注，采用如箭头、标红或下划线等标注方式，并附功能响应承诺书，承诺功能真实有效，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该**

		指标按不满足处理）
	7	提供隐蔽通信检测，提供对 HTTP、FTP、SMTP、IMAP、POP3、Telnet 等服务的隐蔽通信检测。
病毒防御	8	提供对恶意程序实现特征检测、机器学习检测、内置虚拟沙箱检测等多种检测方式，并且多种检测方式相互独立、互不影响；提供专业沙箱设备联动检测。
	9	提供对文件还原捕获，可自定义捕获文件大小，最大支持还原 100M 大小的文件；提供对恶意文件、疑似恶意文件、无风险文件还原。
	10	提供按恶意程序类型、文件类型、应用协议类型对恶意程序图形化统计。提供对恶意程序 Top10 统计，并且统计传输次数。提供展示恶意程序处置事件趋势。
	11	提供机器学习检测功能，能够对目标文件实时检测实时还原效果，不依赖规则库检测实现对未知恶意程序检测。
加密流量防护	▲	要求提供对 SSL/TLS 加密的流量进行解密，实现对 HTTPS、IMAPS、SMTPS、POP3S、RDP 等加密流量的分析检测防护。**（提供设备生产厂商认可的对应功能截图或第三方产品检测报告等相关技术支持资料，功能参数应进行明显标注，采用如箭头、标红或下划线等标注方式，并附功能响应承诺书，承诺功能真实有效，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理）**
信息展示	12	系统应提供不同时间周期的告警及信息图形化展示功能，支持攻击事件、阻断、攻击源、被攻击主机数量展示。
	13	要求提供僵尸主机监控，可按照自定义方式展示僵尸主机事件、联动阻断、控制主机、僵尸主机等数量，具备控制主机地理分布、僵尸主机事件分布、Top10 控制主机、僵尸主机事件等内容监控能力。
日志系统	14	要求提供安全日志配置，可按照信息、通知、警示、错误、严重、告警、紧急等日志级别，管理日志是否记录本地数据库、记录时间、syslog。
	▲	提供外发日志服务器时，自定义传输协议、编码格式 UTF8/GB2312、合并传输。**（提供设备生产厂商认可的对应功能截图或第三方产品检测报告等相关技术支持资料，功能参数应进行明显标注，采用如箭头、标红或下划线等标注方式，并附功能响应承诺书，承诺功能真实有效，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理）**
报表系统	15	提供报表模板的创建维护，可按照源地址、目的地址、风险等级等条件，生成攻击检测、僵尸主机等不同模板。
	16	提供手动报表导出，可按照攻击检测、僵尸主机等报表业务，源地址、目的地址、风险等级等报表条件，报表模板、时间等条件导出报表，并支持自定义页眉、标题、说明等报表定制。
	17	提供自动报表生成，可定义任务名称、报表条件、报表业务、导出时间等内容，报表自动生成。
设备数据对接	▲	设备支持 SNMP、syslog 等方式读取系统性能指标实时监控功能和告警信息外发，包括不限于 CPU、内存、存储等监控指标，并提供 OID 说明
产品资质	★	1.本设备属于网络关键设备或网络安全专用产品，应严格执行国家

		互联网信息办公室、工业和信息化部、公安部、财政部和国家认证认可监督管理委员会 2023 年第 1 号《关于调整网络安全专用产品安全管理有关事项的公告》及国家互联网信息办公室、工业和信息化部、公安部和国家认证认可监督管理委员会 2023 年第 2 号《关于调整<网络关键设备和网络安全专用产品目录>的公告》等相关文件要求，所投标(响应)设备或产品至少符合以下条件之一:一是已由具备资格的机构安全认证合格或安全检测符合要求;二是已获得《计算机信息系统安全专用产品销售许可证》，且在有效期内。**（须提供对应证书复印件。）** 2.产品为自主研发，主要程序具备国家版权局颁发的软件著作权登记证书。**（须提供对应证书复印件。）**

商务要求

投标人需提供对项目背景、采购内容、服务要求、项目重点难点等内容的综合解读，形成项目理解分析。

（一）项目实施

投标人需理解采购人需求，提供项目实施方案，方案需满足以下要求：

1、项目管理要求

（1）项目实施原则

为保障项目的顺利实施，在项目实施过程应遵循以下原则：

1）规范性原则

中标供应商应采用项目管理方法，按照采购人的要求在人员、质量和时间进度等方面进行严格管控。中标人必须配合采购人组织的监督工作，并按采购人要求对发现的问题及时进行整改，

2）标准化原则

项目实施过程应严格遵守国家和税务部门的相关法规、标准。

3）完整性原则

中标供应商应按照采购人的要求，保证实施内容、实施流程的完整性，保证实施过程科学完整。

4）兼容性原则

本项目采购的设备须与国家税务总局金税四期安全管理平台完全兼容，与采购人前期建设无缝接轨。

5）保密性原则

在进行集成和实施过程中，特别是信息安全等级保护等，中标供应商及实施工作人员应按照采购人的要求签署相关的保密协议，采取严格的管理措施，确保实施中涉及到的任何信息，不会泄露给第三方单位或个人，或利用这些信息损害采购人利益。

6）最小影响原则

中标供应商在实施过程中，应充分考虑项目实施对目标系统的正常运行可能产生的不利影响，并采取必要的措施将风险降到最低。

（2）项目实施时间

从签署合同起计算，中标供应商须在 5 个工作日内将货物送至采购人指定地点，工程实施完成时间为 15 个工作日，中标供应商应完成软、硬件设备的到货、安装、集成。

2、具体实施要求

中标供应商应向采购人提供产品和服务，承担与采购人业务系统建设的衔接责任，承诺与本项目的相关单位（包括其它项目集成商等）进行积极主动的合作，中标供应商必须服从采购人的统一协调，在实施方案设计、设备供货、系统集成、技术支持、运行维护等方面相互配合。中标供应商应在项目实施时免费提供相关设备和辅料配件等。

项目实施过程中设备的软硬件出现问题，全部由中标供应商负责解决。标书中的设备、软件产品等方面的配置或要求中出现不合理或不完整的问题时，中标供应商有责任和义务提出补充修改方案并征得采购人同意后付诸实施。

3、设备安装集成要求

中标供应商必须按照项目技术要求和产品技术操作规范，遵照项目操作标准完成设备的安装。

（1）硬件产品安装

合同签订后，中标供应商应与采购人协商进行设备安装前的现场勘查，提交现场勘查报告。对于不能满足设备安装运行需求的，应提出改造建议。

硬件设备的安装要制定具体的现场安装计划，严格按照规定的时间、地点、环境进行安装，保证设备达到标书和产品技术规范中的安装和性能要求。

现场安装实施过程中，须由实际生产厂商技术人员对各单位技术人员进行设备安装和基本操作技能的现场培训。现场培训作为设备安装工作流程的一部分及验收必备的条件之一。

（2）软件产品安装

对于软件要求在标书规定的环境下，实现正常运行，并实现标书和产品技术规范中的功能安装和性能要求。

4、项目管理和人员要求

采购人负责监督和管理整个项目的实施。

中标供应商应充分理解本项目的技术及实施复杂度，组建相应的专职技术及项目团队，参与本项目的各类人员应具备相应的技术及工程管理能力。

项目经理要求具备网络安全设备部署的项目管理经验，熟悉税务系统行业情况。从设备到货之日起，本项目的项目经理需驻场采购人办公地点，听从采购人安排，负责项目整体实施的全部工作，直至项目实施验收完成，驻场时间不少于约定时间，项目实施期间，项目经理不得更换。投标书中应详细列出项目经理的基本信息及能力证明（必须附相应的技能证书）。

项目实施人员应与投标文件中所提供的人员名单相符，未经采购人许可不

得随意变更。

中标供应商在项目实施过程中，需进行规范化管理，要有项目管理组织、项目沟通计划、项目进度计划、项目验收计划等方案，确保实施质量。

中标供应商必须在实施方案中制定详细的任务分解，每个任务的交付物等。

中标供应商须制定本项目管理实施所需的相关文档，负责相关文档的汇总整理，按阶段提交进度报告。

5、项目施工安全及保密要求

中标供应商应在施工中坚持“安全第一，预防为主”的安全生产方针，从技术上、组织上、制度上采取一系列措施，形成安全管理系统，切实做好安全施工和劳动保护工作。中标供应商应在项目实施前，详细分析在本次项目实施过程中可能存在的影响现有系统安全性与稳定性的技术风险，并采取必要的风险控制措施。任何由中标供应商在项目实施工作中对采购人造成的负面影响，其后果都须有中标供应商承担。

（1）施工安全管理要求

1）中标供应商对项目的安全施工负责，负责贯彻落实安全生产责任制度、安全生产规章制度和操作规程，确保安全生产费用的合理使用，并根据工程的特点组织制定安全施工措施，消除安全事故隐患，及时、如实报告生产安全事故。

（2）采购人将在实施过程中对中标供应商的项目实施质量进行严格考核：

1）采购人根据项目各个工作的人员配备情况、工作质量、时效性、工作覆盖情况、成果产出物等要求进行考核，每出现一次或有一项未到达要求或出现工作失误，将按次扣除 1000 元，该累计扣除金额将在项目后续付款进行扣除。如工程实施完成时间结束时，项目实施仍存在未达到工作质量要求情况，将额

外扣除本项目合同金额 5%的费用，中标供应商项目实施团队应在 10 个工作日内全部改正实施完成，保障项目实施质量满足要求，确保设备正常运行。

2）在项目实施过程中由于中标供应商原因导致的终端违规外联、业务系统中断、业务处理能力明显下降或业务数据丢失等重大安全事件，经采购人认定，按次扣除本项目合同金额 5%的费用，最高扣除金额不超过本项目合同金额的 20%，该累计扣除金额将在项目后续付款进行扣除。

6、设备适配测试要求

（1）采购人保留对招标文件中设备基本参数要求的逐项测试权利，且所投产品须能完全兼容采购人现有安全管理平台，中标供应商须承诺配合采购人做好各类设备以 SNMP、syslog 等方式的日志解析及对接采购人现有安全管理平台工作。测试费用由中标供应商承担，若到货后经测试实际不满足要求或不兼容，采购人可以作退货处理并终止合同，中标人承担法律责任并赔偿采购人的全部损失。

（2）中标供应商须承诺提供结合税务应用系统进行网络和数据安全模型定制服务，识别税务人应用系统的账号、数据等关键信息，配合实现模型的建立和测试验证。要求质保期内每年至少配合完成 3 个模型建设。

（3）中标供应商应承诺针对国家税务总局江苏省税务局涉税费系统深入研究数据业务现状，质保期内，如因采购人应用系统增加或调整，涉及本产品的功能修改等需求，中标供应商应免费提供相关服务。

（二）技术培训

投标人需理解采购人需求，提供培训方案，方案需满足以下要求：

1、培训目标

中标供应商应制定与采购人后续使用场景相结合的培训方案，对采购人的运行维护人员进行培训，使其掌握日常运行和维护系统的技能，直至全面掌握

为止。包括（但不限于）故障排除、寻求供应商支持等，保证平台网络的正常运行；对最终平台使用人员和管理人员进行培训，使其对总体流程和系统的集成性有大致的理解，完全掌握系统的应用，保证系统正常应用，掌握设备基本的维护方法。为采购人基础设施及配套基础软件建设项目的最终用户提供有效的、全面的和标准的文档，为系统后续的稳定应用提供保障。

2、培训要求

（1）中标供应商制定培训方案应结合本项目实施及后续运维需求。

（2）中标供应商应制定相应的培训措施保证培训质量。

（3）现场培训不少于一次。

（4）培训内容、方式和地点须根据采购人要求进行定制。中标供应商提供授课工程师、教材以及相关辅助资料。

（三）应急响应及安全保障服务

投标人需理解采购人需求，提供应急响应及安全保障服务方案，方案需满足以下要求：

1、提供重要时期安全保障期间应急响应支持。质保期内，如遇国内重大活动及会议、国家攻防演习等重要时期，经采购人通知，中标供应商须提供应急响应服务，承诺每年提供不少于 60 人天的安全技术人员到国家税务总局江苏省税务局配合完成应急响应支持工作，对相关安全系统与设备进行现场监测与处置，直至重要时期结束，参加应急响应支持的人员须具有至少两年的网络安全服务相关工作经历。

2、提供重大安全事件应急响应服务。当发生外部黑客入侵、数据泄露、木马病毒等重大安全事件时，中标供应商须提供相关安全系统与设备的事件检测与分析、风险抑制、问题处置、协助业务恢复等服务，最大化降低安全事件带

来的影响，如电话沟通无法解决，须安排安全技术专家在 1 小时内到达现场，协助用户解决安全事件，并提供安全事件的分析和溯源，最终出具安全事件处理报告。如设备发生故障，需保证工程师到达现场后 4 小时内解决故障，如果故障严重，超过 8 小时内故障仍未解决，优先提供备机，然后进行离线处理。

（四）项目验收

本项目验收包括设备到货验收、初始验收及项目最终验收三个阶段。投标人需理解采购人需求，提供项目验收方案，方案需满足以下要求：

1、总体要求

（1）验收工作由采购人组织实施，由采购人、中标供应商及产品设备原厂商共同完成。

（2）中标供应商应在项目验收、测试时提供相关的测试环境及必要的设备和工具，使用的各类支撑工具应保证采购人在全系统合法免费使用，中标供应商承担由于知识产权等纠纷导致的所有责任。需要委托第三方机构进行测试的，费用由中标供应商承担。

（3）中标供应商提供的各类文档应内容完整、描述清晰、版本最新，各类方案要求实现目标明确、工作措施得力、可操作性强、具有前瞻性。产出物应提供电子和纸质两种介质，并保持版本一致。

（4）对验收中发现的问题，中标供应商应提出有效解决办法和措施，经采购人确认后实施。根据采购人要求，中标供应商应组织各个产品实际生产厂商对集成工作的评价结果，此结果将作为验收通过标准之一。

2、到货验收

卖方或制造商所提供设备必须是原厂新品且对货物的质量、规格、性能、制造商对货物的质量、规格、性能、数量和重量等进行详细而全面的检验，并

交与买方出厂检验合格证和交货检验记录。设备到货验收由中标供应商和项目单位共同完成，项目单位和中标供应商按项目实施计划进行设备到货验收。

（1）设备到货验收由中标供应商和项目单位共同完成，中标供应商应向采购人提供详细的供货清单，当货物到达采购人指定的安装现场后，双方依据供货清单共同对货物进行开箱检验，按标书要求对全部设备的型号、规格、数量、外型、包装及资料、文件（如装箱单、保修单、随箱介质等）进行逐项检查，经双方验收合格后即时签署《到货验收单》。《到货验收单》一式二份，一份由采购人留存，作为付款的依据；一份由中标供应商留存，作为要求付款的凭证。

（2）中标供应商应保证一次开箱合格率大于或等于 99%。随货物应附有装箱单、质量合格证书、保修证书、产品使用说明书及其他随箱的技术资料。

（3）如检验时，发现货物数量不足、规格与合同要求不符、货物短缺或损伤，供货商应及时补足或更换，并在 3 个工作日内送达采购人指定地点，相关费用供应商承担。同时，供货商保证向采购人提供的技术资料真实、清晰、正确和完整。

3、实施验收

设备初始验收由中标供应商和项目单位共同完成，项目单位和中标供应商按项目实施计划进行设备初始验收，陆续完成设备开机加电、低阶实施等安装配置调试工作，而后在确保运行稳定和售后响应及时的情况下，中标供应商可以书面提请验收，采购人对本项目进行项目实施验收。验收内容主要包括本项目采购文件的“设备技术指标”规格技术参数内容。供应商应提供包括但不限于以下验收材料：

（1）技术文件，包括产品安装、运行、使用、测试、诊断和维修等的技术文件；

（2）系统配置，包括配置图和配件清单；

（3）安装指南，包括项目中所有软硬件产品安装指南；

（4）实施方案，包括设备连接图，规划等；

（5）系统测试文档，包括针对本项目的系统适配测试方案，并提供相应的测试记录和测试结果文档；

（6）到货验收单，包含设备到货后检验情况；

（7）验收报告，在系统验收时收集各项验收数据，汇总成册，并配合采购人对设备进行综合评估；

（8）过程文档，对项目实施过程跟踪记录，并提供过程记录文档；

（9）变更文档，对项目计划、项目内容、变更会议等项目实施过程中的变更情况等进行记录，并提供变更文档；

（10）培训记录，中标供应商向采购人培训设备软硬件功能的记录；

（11）中标供应商提供的三年原厂质保的承诺函。

4、项目终验

设备质保期满，中标供应商应书面提请项目终验，双方就设备在质保期间运行情况共同进行验收。

2.中标供应商保质保量、按整体解决方案如期完成设备集成全部工作，满足业务系统的全部建设要求。

3.中标供应商应按照采购人要求，移交本包实施过程中的各类文档，并经过采购人验收签字。

4.中标供应商应就集成工作，采取文档讲解、会议研讨、培训、在日常工作中进行传帮带等方式，完成对采购人的知识转移工作。

供应商应提供包括但不限于以下验收材料：

每季度巡检报告、每年度网络和数据安全模型定制服务完成情况、质保期

间维保记录、项目终验报告等。

（五）付款要求

1、合同签订后，全部设备到货、安装、配置、调试完成并经采购人项目实施验收合格后，中标供应商按采购人要求提供付款申请、付款明细、发票、中标或成交通知书复印件、履约保证金付款证明、合同约定的其他资料，支付80%的款项；全部设备在采购人处正常试运行满 90 天且未发生因设备功能原因产生的重大安全事件，中标供应商按上述要求提供相关材料后，支付剩余 20%的款项。

2、履约保证金：中标供应商接到中标通知书后 5 日内，向采购人提交履约保证金。履约保证金为合同金额 5%。质保期结束并完成全部售后服务，经由采购人项目终验合格后，全额无息返还。

3、误期赔偿费约定：如果中标供应商没有按照合同规定的时间交货和提供服务，采购人有权从货款或履约保证金中扣除误期赔偿费而不影响合同项下的其他补救方法。赔偿费按每日加收合同金额的 0.5%计收，直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的 15%。

（六）质量保证及售后服务

投标人需理解采购人需求，提供售后服务方案，方案需满足以下要求：

1、技术支持后援及售后服务响应要求

在服务的实施过程中，如果需要实际生产厂商、相关中标供应商等各方的协助和合作时，由中标供应商负责组织协调。要求中标供应商必须能提供及时、高效的技术支持与售后服务，确保工程能按设计方案的各项指标要求和实施计划顺利完成，并在工程验收合格后，能长期稳定运行。

本项目所有硬件产品技术支持和售后服务时间，自项目实施验收完毕之日起计算，质保期为 3 年。中标供应商必须提供生产商质保服务，质保信息可通过生产商官方渠道查询验证。

中标供应商应在达到以下要求的基础上，根据招标方的实际情况详细制定有针对性的技术支持和售后服务方案。应详细阐述项目方案、技术支持与保修服务体系，各类设备服务响应流程，技术支持与保修服务投入人员情况，备品备件方案，相关协作方案，服务质量监督机制等与保障本项目完整顺利实施的相关内容。

对实际生产厂商的服务要求：

（1）实际生产厂商必须有完善的技术支持服务体系，能够向采购方提供统一快捷的技术支持服务。投标书中需详细列出各分公司地址、负责人、联系电话（包括手机和固定电话）、人员状况和相关证明文件等。

（2）在服务期内，实际生产厂商应指定一名项目经理作为统一提供服务的接口人，为采购人提供主动式服务，并由该项目经理负责响应、协调、处理采购人的具体服务需求，协助进行配置管理，包括客户记录、更新、管理设备基础信息、常用配置信息及必要的系统、网络拓扑信息等。

（3）在服务期内必须提供每季度一次的实际生产厂商现场设备巡检，巡检中应对系统性能、运行状况、稳定程度等进行评估，并根据用户需求经确认后进行优化，每次巡检结束后，需向最终用户提交巡检报告；在服务期结束前 3 个月内，中标供应商及实际生产厂商必须对本项目中的所有设备运行情况进行一次全面巡检。用户单位签字盖章的巡检报告将作为项目最终验收报告内容和退还履约保证金的必备条件。

（4）中标供应商应对硬件产品提供实际生产厂商技术支持与售后服务。

对中标供应商的服务要求：

（1）中标供应商必须有完善的技术支持服务体系，能够向采购方提供统一快捷的技术支持服务。投标书中需详细列出公司（或办事处、技术支持服务中心等）地址、负责人、联系电话（包括手机和固定电话）、人员状况和相关证明文件等。

（2）在服务期内，中标供应商应保持技术支持人员的相对稳定，同时提供作为互备的 2 名项目接口人，可指定其中 1 人为主，人员需为经采购人认可的专职技术人员，按照采购人要求统一调度，承担运维、应急响应等服务任务。

（3）中标供应商在应答时应详细阐述所提供技术支持与售后服务的内容与范围。服务维保期范围内至少包括运维支持、软件升级、设备维修、技术咨询、各种突发事件的应急策略、定期巡检等。

（4）中标供应商必须向采购人提供一站式服务，即一点受理后，必须负责全程跟踪服务。中标供应商统一负责并统筹安排和协调本包中所包括的所有硬件设备及相关的软件产品的现场技术支持和保修服务。

（5）产品所具有的先进技术应在生产环境和服务过程中加以实际应用，以此作为产品技术性价值的体现，检验技术实用性的同时也进行使用经验的积累。中标供应商须承诺产品具有的先进技术为成熟可靠的技术，可用于实际生产环境和提供服务，并对应用该技术产生的效果负责。中标供应商提供服务支持时，除非采购人特别要求，所宣传的设备或方案所包含的先进技术应作为默认的使用方案或操作方案，否则，中标供应商须对不适合使用此技术的原因进行分析和说明，并提交正式文档。

（6）功能性服务：

功能性服务主要指不涉及添加新的硬件，仅对设备、软件进行操作实现功能变更的服务，包括但不限于：对设备的重新安装、配置修改或功能的重新设定，硬件的微码、固件等的升级，设备资源的重新规划、配置、划分，结构调

优，操作系统及管理软件等相关软件的重新安装、版本升级、配置修改及功能的重新设定。

服务期内，根据采购人需求，中标供应商须响应并提供对功能性服务的咨询、规划、具体实施以及必要的培训。服务实施时要求预先评估、制定服务计划，并根据服务的内容和性质提供相应的培训。

实际生产厂商必须提交系统的维护技术，交付全部设备维护密码（授权），用户有权自行修改配置，自行维护设备，但并不因此影响用户本身享有的原厂维保服务权利。

2、保修及系统维护服务响应要求

（1）服务方式

中标供应商和实际生产厂商必须向采购人免费提供技术支持电话、E-Mail 和 Internet 网站技术支持方式，并应建立提供专门的服务号码和账户，实际生产厂商必须向用户单位提供 7×24 小时授权工程师电话响应服务。能够在互联网站上查询、下载相关技术资料、提交问题并获得支持。E-MAIL 最迟次日回复。

（2）响应时间

①电话服务请求的响应时间应少于半小时，实行“一站式”服务，即一点受理后负责全程跟踪服务；

②中标供应商须承诺实际生产厂商在 2 小时内对使用单位所提出的维修要求作出实质性响应，并且对使用单位的故障报修进行响应；

（3）设备保修

服务期内，必须由实际生产厂商专业技术人员负责对设备免费进行现场维修更换，更换的设备或部件必须是来自实际生产厂商的设备或备件。

现场维修时含有数据的硬盘、磁带等存储类零部件不得带出机房，维修更

换下来的此类部件所有权归采购方所有。

（4）故障处理报告

故障解决后 24 小时内，中标供应商及实际生产厂商应向用户单位提交故障处理报告。说明故障种类、故障原因、故障解决中使用的方法及故障损失等情况。按季向采购人提交上期故障受理报告、故障分析报告和汇总情况。

（5）供应商应提供所投产品三年原厂质保服务（从实施验收合格后开始计算）。

（6）供应商应提供对所投产品的日常升级服务，保证设备的安全稳定运行。免费对软件版本、规则库、病毒库等进行升级。

（7）发生非人为因素故障，中标方确保在七日内免费对产品进行补充或者更换配件或整机。

（8）中标方确保所有替代零配件是全新未使用的。

（9）供应商应提供对质保期内设备系统的重大变更调整服务，调整期间需原厂提供现场支持服务，服务不限于系统重新规划、重新安装、故障排错、版本更新等内容。

（10）技术服务人员在进行具体操作和配置时，必须做好事先准备工作，充分预估可能产生的风险和造成的损失，对于因准备不充分、操作不当、误操作等导致的设备故障、应用风险、网络中断、数据丢失等事故和造成的损失，供应商须承担全部责任，并对造成的损失进行赔偿。

（七）保密要求

投标人需理解采购人需求，提供项目保密方案，方案需满足以下要求：

1、响应单位应在投标文件中签署并提交保密承诺书。须在签订合同的同时，签订保密协议，项目实施前，参加项目实施工作的所有人员签订个人保密承诺书。若中标供应商中标后不能按要求签订保密协议，采购人有权提出变更中标

结果。

2、中标供应商应严格遵守保密承诺，确保采购人提供的图纸、技术文档等项目资料不外泄。不得向第三方泄露采购方名称、部署位置、采购产品、使用方式、运行情况等涉及设备使用的任何信息。

3、中标供应商在进行集成和实施过程中，特别是信息安全等级保护等，中标供应商及实施工作人员应遵守采购人提出的关于本项目的保密要求，采取严格的管理措施，确保实施中涉及到的任何信息，不会泄露给第三方单位或个人，或利用这些信息损害采购人利益。在项目实施期间及项目实施完成后，必须退还采购人项目实施过程中涉及到的所有文档资料，清除技术检查工具中所有相关数据。若发生信息外泄，采购人有权依法追究中标供应商的法律责任。

（八）其他要求

1、本项目不得转包或分包，一旦发现转包或分包情况，采购人有权立即终止合同并收回合同全部款项，同时追究响应单位相关法律责任。

2、中标供应商存在以下情形的，视为未实质性响应本项目采购需求，采购人可根据实际情况进行相应处理：

（1）“三、项目技术需求”、“四、服务要求”中各加★项均为实质性要求，不接受负偏离。采购方有权要求供应商承诺其真实性，在合同签订前由采购人对技术参数、实际功能进行测试，如未通过实际测试的，将取消其供应商资格，采购人有权拒绝与其签订合同，并由其承担所有责任；

（2）投标产品不满足技术参数等项目需求方案的，采购人有权拒绝与其签订合同，取消其供应商资格并由其承担所有责任；

（3）由于投标人的原因未在规定的时间内签订合同的，采购人有权拒绝与其签订合同，取消其供应商资格并由其承担所有责任；

（4）中标后中标供应商须在中标后 15 个工作日内向采购人提供三年原厂

质保的承诺函，规定时间内未能提供的，采购人有权拒绝与其签订合同，取消其供应商资格并由其承担所有责任；

（5）无法按时供货交付的，采购人有权拒绝与其签订合同，取消其供应商资格并由其承担所有责任。

（6）中标单位需要满足税务供应链管理要求，并与采购人签订供应链安全管理承诺书（详见附件）。

（九）遵守税务信息化供应链安全管理的要求：

★税务信息化供应链安全管理承诺书（按照采购人关于加强税务信息化供应链安全管理工作的具体要求，作为信息化资源和服务提供的供应商，有义务保证所提供产品、服务和管理的安全性。投标人必须做出承诺，未签署承诺书的视为无效投标（承诺书详见合同附件））。（以下内容不得删减）

国家税务总局江苏省税务局：

为确保国家税务总局江苏省税务局税务信息化供应链安全，我单位郑重承诺：

1.配合开展背景审查工作。遵守国家网络安全政策法规和税务机关各项网络安全规章制度，与局方签订保密协议，提交单位网络安全承诺书，项目实施人员及驻场人员提交个人网络安全承诺书及包括无犯罪记录证明在内的背景审查材料。定期对聘用离职税务人员情况进行排查，建立相关资料档案，确保人员安全可信。

2.设置网络安全负责人。建立网络安全负责人制度，为本项目配备一名具备独立决策能力并保持相对稳定的负责人，在项目实施的全过程负责网络安全工作，组织落实各项网络安全要求。

3.加强安全意识和技能考核。项目实施前，确保对参与人员开展了网络和

数据安全法律法规、税务系统网络和数据安全相关规定要求、安全技能、保密常识等方面的教育培训并考核合格；项目开展期间，配合局方检查我单位对项目参与人员开展相关安全培训、考核及警示教育情况，确保通过教育培训不断提高我单位项目参与人员的网络和数据安全意识及保密意识。

4.及时报告重大事项。及时向局方报告我单位发生的可能影响网络安全的重大事项，包括负责人及重要工作人员变更、业务转型、合并重组、投资并购等。

5.建立应急响应机制。项目开发建设前，我单位将编制并提交基于项目场景的供应链安全事件应急响应预案，明确相关职责和应急处置流程；根据应急响应预案定期进行应急演练；配合局方定期检查我单位开展应急演练的记录等情况，确保快速有效处置供应链安全事件。

6.开发场所安全管理。配合局方核查我单位的软件研发工作场所及开发测试环境，保证搭建专用的开发测试环境，配置安全可信的开发管理工具，设置可靠的权限管理策略，确保项目研发安全可控、开发场所安全可控可信。

7.局方开发环境安全管理。在局方开展软件开发测试工作的现场工作人员，将严格遵守局方供应链厂商管理规范，未经批准不使用自带电脑和移动存储介质，不变更办公场所和办公设备，不安装非必要的应用程序和组件，不擅自复制、使用和修改文档、数据以及其他开发测试资料。

8.产品和服务安全管理。我单位提供的产品及服务满足国家认可的网络安全规范和认证要求，我单位负责的定制开发软件将配合局方开展网络安全“三同步”测评，我单位在项目中使用的重要供应链产品将按照局方要求形成供应链产品清单提交局方审核。

9.第三方组件安全管理。我单位将在局方统一管理下定期对提供的产品进行安全风险评估和漏洞扫描，做好漏洞评估、漏洞修复和版本升级工作，形成

第三方组件（含自行开发且多项目共用的基础框架及组件）清单和安全分析报告，及时更新第三方组件相关信息并报送局方。我单位将采取有效措施保障第三方组件安全，原则上禁用存在高风险隐患或已停止维护的第三方组件。我单位确保产品中使用的开源代码符合开源许可协议要求。

10.代码平台安全管理。项目开发建设时，如需设立代码管理平台，我单位将配置独立的、不与互联网连接的内部代码管理平台，搭建具备权限管控功能的统一版本控制系统，将全部源代码纳入管理，并制定安全编码规范，严禁开发人员未经授权或越权访问和违规开发。我单位将配合局方开展安全审查，严禁将源代码上传第三方平台，严禁使用互联网代码托管平台，防止代码泄露和后门植入。

11.源代码安全自查。我单位将设置专用代码审计场所，采用工具与人工核查相结合的方式开展工作，形成源代码审计报告提交局方。我单位将采取必要的手段确保源代码不外泄，对审计中发现的问题及时解决。

12.测试数据安全管控。为保障测试数据安全，我单位将明确脱敏字段需求，规范测试数据使用权限，切断数据拷出途径，根据局方规定申请用于测试的税务脱敏数据，并确保测试数据安全。

13.安全“三同步”管理。应用系统开发上线前，我单位将配合局方安全管理要求，形成供应链产品清单、第三方组件使用清单、源代码审计报告等相关内容，汇总至系统安全“三同步”材料一并提交局方审核。

14.系统变更管理。我单位承诺，在发生应用系统小版本升级更新且不涉及发布互联网新接口链接情况时，将认真做好系统安全性测试，报局方相关系统业主和运营主管部门审批同意后发布。在发生应用系统重大功能变更、新功能模块上线、在互联网发布新接口链接等情况时，除报局方业主、运营部门审批同意外，还将报请局方安全主管部门审批同意后发布。

15.权限和数据安全管理。我单位工作人员遵从局方最小化授权要求，按照工作所需向局方提前申请各类账户，不试图获取超范围权限，获得批准后使用。我单位工作人员遵从局方运维规范，未经同意不擅自访问、修改或删除税费数据，不私自截留涉税相关数据，不变更涉税相关数据用途、用法，不公开、转让或向第三方提供涉税相关数据，配合局方做好税费数据操作全程记录和留痕工作。

16.基础设施安全管理。我单位工作人员遵从局方日常运维行为安全管理要求，未经局方批准不进入基础设施场地，未经授权不访问、维护、维修基础设施，运维期间不携带个人电脑、U 盘、未授权软件安装包等工具，不向第三方提供基础设施场地设计图、设备部署图等有关信息。

17.风险隐患管理。我单位将及时向局方报告发现的网络安全漏洞、缺陷、数据泄露或其他重大网络安全风险，不公开或向第三方提供。我单位将定期检查所使用产品及第三方组件，存在高危漏洞的及时通过限制访问、更新补丁、版本升级、设备防护等措施进行加固处置；对于停止维护的产品及第三方组件，评估是否存在高危漏洞，如存在无法修复的高危漏洞，将考虑升级版本或更换产品及第三方组件。

18.自查报告要求。我单位将配合局方严格落实供应链厂商在风险控制、审计巡查、应急处置等方面的工作要求，根据各项要求的落实情况，撰写年度供应链安全自查报告并提交给局方。

19.履约履职要求。我单位将严格遵守采购合同、项目采购需求说明书、协议、承诺书等文件中的安全相关条款，若履行网络安全责任不到位、造成安全事件或产生不良影响的行为，依照相应条款处理。

20.安全审查要求。我单位按照《网络安全审查办法》的要求，承诺不利用提供产品和服务的便利条件非法获取数据、非法控制和操纵设备，无正当理由

不中断产品供应或必要的技术支持服务等，否则依照法律规定处理。

21.项目验收要求。我单位将落实局方供应链安全管理各项规定，按照国家相关法律法规开展安全审查、安全评估、渗透测试等，并将落实情况作为项目验收材料提交局方审核。

我单位承诺遵守相关法律法规及本承诺书有关规定。若违反相关规定，贵单位有权对我单位及工作人员的违规违纪行为按签订合同、协议、承诺书等相关条款进行处理。涉嫌违法犯罪的移交有关部门依照相应法律法规处理。

承诺单位（公章）：

日期：