国家税务总局南京市税务局

数据安全治理设备竞价文件

1. **采购单位：国家税务总局南京市税务局**
2. **项目名称：国家税务总局南京市税务局数据安全治理设备**
3. **采购商务要求及设备指标参数要求**

**3.1 在线竞价采购商务要求**

1. 本项目在线竞价响应供应商须是符合《中华人民共和国政府采购法》第二十二条的规定，符合《关于规范政府采购供应商资格设定及资格审查的通知》第六条规定且已在政采云税务采购网系统注册并通过资质初审的供应商。
2. 竞价响应供应商须认真审核在线竞价采购文件所有要求，如明知不满足采购文件要求进行恶意竞争的，将根据《政采云平台电子卖场权益维护及纠纷处理规则》和政府采购相关规定，报财政部门、国家税务总局处理，涉嫌犯罪的，移送司法机关处理。请供应商在响应报价前仔细评估自身履约能力，不得实施恶意低价、不按要求报价、中标后无故放弃、不按合同履行等违约行为；对出现此类行为的预成交供应商，将根据在线询价违约处理规则，依法依规提请政采云平台进行处罚，处罚内容包括停止推送报价信息、禁止报价、协议暂停、罚款、诚信体系中记录不良行为或黑名单等，记入政府采购诚信档案。
3. 本项目预算含税金额为45万元，数量1套，项目实施地点为南京市税务局金汇大厦机房。
4. 竞价响应供应商须参照采购需求中建议的品牌提供产品，并确保其所提供的产品为符合生产厂家正规渠道的原装正品。
5. 竞价公告的商品清单中“技术参数或配置要求”表中标记“★”的为主要技术参数；主要技术参数不满足为实质性不响应，其他参数不响应超过三项的视为实质性不响应。
6. 本项目所采购设备及软件须提供不少于3年原厂维保及升级服务，质保期时间自最终验收合格并交付使用之日（以时间在后者为准）起计算。为确保供应商提供的产品品质及后续质保服务，投标产品需要提供由设备生产厂商出具的加盖公章的维保服务承诺函，否则视为竞价不符合技术指标要求，属实质性不响应，本次竞价无效。
7. 竞价成交结果公告公示后必须在七个工作日内与采购单位签定合同，合同签订后1个月内完成全部设备的到货，设备到货后1个月内完成现场集成安装调试，并提供必要的辅材，同时完成相关培训任务。
8. 商务及服务条款、技术参数内要求的相关资料、证书，竞价供应商须在报价同时通过附件向采购单位提供，否则本次竞价无效。如中标人未能履行以下规定程序的，视为未实质性响应本项目采购需求，按税务采购网供应商管理办法处置：（1）投标产品未按照技术参数要求提供主要技术参数证明文件的；（2）技术参数或配置要求中需要提供的技术参数证明文件未能在签订合同前提交原件或原件复印件并加盖产品厂商公章进行核验；（3）无法按时供货；（4）由于投标人原因未在规定的时间内签订合同的。
9. 竞价设备参数指标不得低于附件中设备参数指标。
10. 本项目不接受超预算报价。
11. 本项目不接受联合体参加。
12. 供应商和所供产品必须全部满足技术和商务要求、服务条款和商务条件；供应商担保采购单位使用其提供的产品及服务不侵犯第三方知识产权。合同签署后供应商不满足以上各项要求和指标，采购单位有权终止合同，并且有权要求退赔。
13. 本项目不得以任何形式转包分包，采购单位将对进场施工人员做资格审查，不合格当违约处理。
14. 付款方式：本合同项下的全部货物安装调试完毕并经最终验收合格，且收到货物生产厂商针对本项目开具的维保服务承诺函后30个工作日内，在收到供应商开具的正式发票后，采购单位向供应商支付全部合同价款。

**3.2 技术参数和配置要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
|  | 硬件平台配置要求 | ★1台，2U机架式服务器硬件平台（非工控机），双电源，2颗CPU，单颗CPU内核≥16核，内存≥256GB，固态硬盘容量≧1.8Tb，SAS硬盘容量≥24TB，RAID 5，可使用硬盘槽位≥12个，≥2个千兆电口，≥2个万兆光口 |
|  | 流量镜像采集工具 | ★1台，旁路部署，支持 4 个 100GE QSFP28/40GE QSFP+（配置2个40GE QSFP+多模 MPO接口模块），24 个 10GE SFP+/1GE SFP 业务接口（配6个万兆光口模块和6个千兆光口模块）和24个千兆电口，接口子卡可替换，1+1 冗余电源，整机报文转发吞吐量不小于664Gbps； |
|  | ★支持基于硬件的OSI L2-L4层流量过滤，可基于源MAC、目的MAC、源IP、目的IP、协议号、源端口、目的端口、物理端口号、VLAN的报文过滤,支持自定义其中的任意组合；支持基于协议与应用的分类过滤策略，支持URL过滤规则；支持报文去重，自定义报文去重参数，包括但不限于：五元组、tcpflag、ip\_id、payload、checksum；支持无限次报文去重；支持配置报文去重窗口时间；支持对接入的HTTPS、FTPS、POP3S、SMTPS、IMAPS协议加密流量进行解密，TLS版本需支持1.2和1.3； |
|  |
|  | 支持命令行管理和配置，支持关闭Telnet，启用SSH对设备进行命令行管理配置；支持图形化管理和配置； |
|  | 使用许可 | ★本项目产品管理的数据库实例、表、字段、数据文件等不受许可数量限制 |
|  | 数据库资产管理 | 支持多种数据源，包括但不限于：Oracle、SQL Server、MySQL、PostgreSQL、Hive、Greenplum、ElasticSearch、南大通用GBase、人大金仓、达梦、Gauss DB等多种数据库及数据仓库。 |
|  | 可根据指定IP段的范围进行搜索，自动发现数据库的基本信息，包括：数据库服务器IP地址、端口号、数据库类型等。 |
|  | 用户可对自动发现或手动添加的数据库编辑信息，包括数据库版本号、描述、组织机构、所属业务系统等。 |
|  | 敏感数据自动发现 | ★内置敏感数据特征库，能够自动识别身份证、通用证件号、银行卡号、电话号码（手机、座机）、中文姓名、中文地址、企业名称、日期、税号、统一社会信用代码、组织机构代码、工商注册号、海关编号、ip地址、mac地址、车牌号、车架号、港澳通行证等敏感信息。 |
|  | 针对数据库资产进行字段内容级的深度扫描，基于预置的敏感数据特征库，通过扫描发现数据库中存储的敏感数据，帮助梳理敏感数据在数据库资产中的分布情况。 |
|  | 针对文件系统进行文件内容的深度扫描，基于预置的敏感数据字典库，扫描发现文件系统中存储的敏感数据，帮助梳理敏感数据在文件资产中的分布情况。 |
|  | 用户可在WEB界面对敏感数据的特征规则进行配置和管理，支持自定义具有行业特性的敏感特征模板 |
|  | 数据分类分级 | ★支持基于模板设置分类分级规则：规则至少支持库名、表名、表描述、字段名、字段描述、匹配方式和匹配内容；规则支持正则、精确匹配等；支持规则条件表达式，可设置多个条件之间的与或逻辑关系。支持根据税务行业分类分级规范自定义数据分类分级模板。 |
|  | 根据选定的分类分级标准进行数据库关联，系统根据对应的分类分级的规则，通过特征分析等方法进行识别，利用精准匹配，对目标数据自动分类分级。对于未识别的数据字段和识别后需要修改的字段，用户可手动编辑该字段的分类分级结果，最终以用户手动修改为准，修改后同步更新至分类分级列表中。 |
|  | 可以创建分类分级任务，系统按照设定的分类分级模板对字段或数据内容进行匹配识别，用户可手动编辑字段的分类分级结果，修改后同步更新至分类分级列表中。 |
|  | 分类分级结果支持手工导出和提供开放接口供其它系统调用，用于数据库安全审计、数据脱敏等策略使用。 |
|  | 数据安全事件监测 | 支持针对网络流量中可能存在的数据安全异常行为进行监测；支持通过内置的异常行为告警规则及用户根据模板自定义的规则，对命中数据安全规则的流量进行告警，通过列表的方式展示安全事件，事件类型包括但不限于网络扫描、漏洞利用、可疑流量、恶意程序、流量内容监测等 |
|  | 数据资产安全态势 | 支持大屏展示数据资产安全态势，包含：数据库连接统计分析、文件系统统计分析、业务系统统计分析、数据存储资产类型统计、分类分级进展、分类分级占比、敏感数据扫描进展、命中敏感词特征性、敏感等级占比、实时数据库访问等信息 |
|  | 数据风险安全态势 | 支持大屏展示数据安全风险态势，包含：流量统计与分析、漏洞统计与分析、异常行为资产排名、安全事件与趋势等信息 |
|  | 任务管理 | 资产发现任务：系统可支持用户自定义IP段的范围进行数据库搜索扫描 |
|  | 敏感数据发现任务：系统支持定时、定期自动执行敏感数据发现任务的功能。支持按照日期、时间对任务进行定时。 |
|  | 产品资质 | ★提供国家版权局颁发的《计算机软件著作权登记证书》。 |

说明：以上技术要求中，“★”为关键性指标，不允许偏离。单个产品型号无法满足全部需求的，可以通过多个产品型号组合，须在报价时写明所有产品型号。

建议品牌：安华金和、中新赛克等

**3.3 项目实施要求**

1. 采购单位监督和管理设备集成安装实施工作。
2. 供应商所提供的产品及配件必须是原厂原包装全新正品，产品质量符合国家相关标准及安全规范。设备到货时，所有外包装箱箱体无严重破损或变形，封条应完整无缺，内包装应符合标准运输包装要求，拆箱后设备主体外表无任何磕碰、碎裂、划伤痕迹。运输途中设备出现任何问题，全部由供应商负责解决。
3. 供应商须对采购文件要求的技术参数逐一测试，不满足技术要求的货物将被拒收。
4. 供应商必须按采购单位要求完成设备的安装、配置、测试、优化等工作，包括网络布线、系统配置、操作系统安装、管理控制台配置。供应商须提供本次项目采购所有设备需要的强弱电缆、光纤、跳线等材料和配件。
5. 供应商应针对南京市税务局涉税费系统深入研究数据业务现状，综合形成数据分类分级和安全治理解决方案，从制度建设、数据分类分级到分类分级结果应用，提供完善的、流程化的路径指引，为数据分类分级和安全治理提供有力支撑：

（1）梳理数据资产现状。针对以电子形式记录的数据表、数据项、数据文件等数据内容，整理和识别已收集的数据资源，形成数据资源列表。汇总数据资源调研结果，以及数据安全分类分级工具自动识别数据源结果，初步整理输出单位数据资产清单。根据初步资产清单制定符合单位实际业务场景和数据情况的分类分级标准。

（2）完善数据分类分级标准规范。落实国家相关法律法规、监管机构对数据安全管理的要求（包含但不限于《网络安全法》《数据安全法》《个人信息保护法》《信息安全技术 政务信息共享 数据安全技术要求》等），在完善的数据分类分级模型、方法指导下，根据政策法规形成数据分类分级标准，明确各类数据的保护要求及措施，形成分类分级标准和策略文档。

（3）开展数据资产分类分级。根据数据分类分级管理规范要求，通过数据安全分类分级工具和人工审核修改的方式开展数据分类分级，形成数据分类分级清单。分类分级对象约2600张数据表、74000个数据字段。

（4）实施数据安全风险评估。对照《中华人民共和国数据安全法》《江苏省数据安全风险评估规范》以及总局、省局和南京市其它数据安全、分级分类方面的规范及要求，对南京市税务局数据共享交换平台、房产一体化平台系统等三个应用系统开展安全风险评估。识别数据处理活动、数据安全威胁、数据安全脆弱性、数据安全措施，并对照数据分类分级管控要求找出不足。围绕数据、数据处理活动，对已识别的数据安全威胁、脆弱性、安全措施进行风险分析预评价，明确风险接受程度及风险处置措施，编制《数据安全风险评估报告》，给出数据安全整改建议，并制定详细的数据防护治理方案。按采购单位要求，开展一次数据安全应急演练。

（5）增强数据安全防护能力。基于数据分类分级结果，结合数据场景设计方案，明确不同敏感级别的数据安全管控策略和措施，依据现有监管要求建立数据安全管理体系框架。优化和完善数据安全管理制度及管控策略，明晰各级别数据的安全管理要求，构建各业务领域的场景化数据安全矩阵。基于数据安全生命周期内，对于现有的各系统业务流转中的敏感数据，提出相应的安全管控策略及工具，实现数据安全全生命周期保障。包括但不限于终端数据安全建设、网络数据防泄漏建设、数据权限管控、业务系统数据保护、数据交换安全、数据安全态势感知、数据泄漏实时监测等方面。

（6）交付文档要求：本项目需提交的交付文档包含不限于： 《数据分类分级标准》、《数据安全管理制度》、《数据资产清单》、《敏感数据风险评估报告》、《数据安全防护优化方案》、《数据安全治理平台总体设计》。

（7）实施团队要求：项目团队人员数量应不少于4人，项目成员团队成员应具备完成同类项目的经验，具备相应的学历证书、资质证书，且必须全职、全程参与本项目工作。项目团队成员应具备ORACLE OCP、CCRC-DSO（中国网络安全审查技术与认证中心数据安全官认证证书）认证、数据安全能力成熟度模型测评师证书或CISP-DSG（注册数据安全治理专业人员）认证等证书。

**3.4 售后服务要求**

1. 为保证数据安全，本次采购所有设备的存储介质（含机械硬盘、固态盘）在质保期内发生故障更换后，所有权仍归采购单位，其他单位和人员不得带离现场。
2. 供应商在质保期内必须提供所有设备整机（包括所有相关部件）的硬件质保服务和软件的维护、配置，在质保期内提供非人为损坏造成的设备故障免费维修，免费技术咨询、免费设备软件版本升级、协助安装操作系统、制作设备标签等维保服务。
3. 本项目质保期内的设备维护保障服务和部件备件供均为全包模式。维修维护所需用的专业化工具和装备，均由供应商自备，不再另收取需方费用。
4. 供应商应对本次采购所有设备免费提供必要的操作系统、相关设备硬件系统的微码、补丁等升级服务、安全漏洞修补、系统统资源优化等服务。供应商服务过程中所提供的软硬件产品，须保证拥有合法的使用权。
5. 采购单位提出技术支持请求后，供应商须在1小时内响应；当系统发生硬件故障时，在4小时内提供现场服务，在服务人员到现场后6小时内尽力恢复系统正常运行；如设备故障6小时内无法恢复，并影响业务系统正常运行，需在确认无法恢复后10小时内采取更换备品、备件等应急措施，使业务系统尽快恢复运行；当更换备品、备件不能解决硬件故障时，应在故障发生24小时内提供同档次或更高配置的设备对故障设备进行替换，完成配置，保证业务正常运转，直至故障设备修复后重新部署回原节点。
6. 供应商如未能在上述规定时间内解决故障并恢复系统运行，采购单位有权动用设备原厂商的技术力量和备品、备件，或请其他专业公司进行维修，所有费用由供应商支付。
7. 在质保期内如采购单位有需求，供应商免费对参保设备提供配置调整和调试服务，为采购单位提供参保设备上架、下架、跳线理线（包括网线和电源线）、制作标签等服务工作；协助采购单位做好配置管理，对维保设备配置信息进行采集、更新和统计，维护相关设备配置信息表。
8. 如采购单位因某一时期运维工作内容增加、紧急事件处理等需增加现场技术支持人员服务的，供应商需安排相应技术人员免费协助开展相关工作。

**3.5绿色数据中心要求**

本项目所采购的产品需满足《绿色数据中心政府采购需求标准（试行）》（财库【2023】7号）中“数据中心信息（IT）设备及配套设备要求”的通用要求，项目验收时需提供第三方检测报告或第三方认证证书，无法提供的视为验收不通过，供应商需承担违约责任。

**3.6 其他要求**

一、供应商及其工作人员，应当遵守国家税务总局、江苏省税务局及南京市税务局的相关安全保密规定，在签订合同时，同时要与采购单位签订保密协议，双方必须对合作过程中涉及的税务工作信息资料、秘密、业务需求、协议、系统设计、技术成果等内容和相关事务保密。

二、供应链安全管理要求：按照采购单位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。包括配合开展背景审查、设置网络安全负责人、加强安全意识和技能考核、及时报告重大事项、建立应急响应机制等承诺条款（详见附件承诺书）。

以上关于供应链管理的要求，在签订合同时必须做出遵守承诺，未签署承诺书的视为无效合同。

**附件： 税务信息化供应链安全管理承诺书**

国家税务总局南京市税务局：

为确保国家税务总局南京市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.**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。

15.**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。

16.**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。

17.**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。

18.**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。

19.**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。

20.**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：