# 采 购 需 求

项目名称：安徽税务2025年全流量检测等安全设备购买

2025 年 07 月

# 目 录

# 1 项目概述

## 1.1 项目背景

### 1.1.1 项目目的、意义及背景

随着发票电子化改革的逐步推进，纳税人数量在急剧增加的同时，对现有网络安全提出了更高的要求。同时为贯彻落实国家税务总局网络安全和信息化领导小组办公室对税务系统安全规范的要求，结合我局现有网络安全现状及实际业务安全需求，通过对安徽省税务局网络安全防护体系进一步优化，提升网络安全防护效果，保障相关系统安全运行。

## 1.2 项目内容

### 1.2.1 项目建设思路

通过部署全流量检测设备、入侵防御设备（IPS）、应用程序接口（API）检测设备、数据加密传输设备、“双向”交换系统扩容设备、动态防御设备等安全设备，对现有的业务系统流量进行多项防护技术的优化整合，提升省局对业务系统流量中的数据进行实时监测、分析和记录的能力。该项目可以有效地提高我省税务系统网络安全防护效能。

### 1.2.2 采购内容

全流量检测设备：通过对业务互联网核心交换南北向全流量实时监听检测，可以捕捉到其中包含的各类数据流量，对数据进行分类、分析和记录。同时可对一定时间范围内业务互联网的流量数据进行留存，便于在发生安全事件时进行溯源排查。

入侵防御设备（IPS）：为业务互联网金税四期相关系统流量新增入侵防御设备，实时发现并阻断其中的异常攻击行为，如漏洞利用攻击、扫描探测攻击、暴力猜解等已知类型的威胁。

应用程序接口（API）检测设备：通过应用程序接口（API）检测设备实现API资产可视，检测API攻击行为、异常行为、数据泄漏事件等API资产风险，并通过精细化策略配置，提高API风险管控能力。

数据加密传输设备：通过在业务互联网和税收业务专网分别部署数据加密传输设备，提供安全通信链路，保护通信数据的机密性和完整性。

双向”交换系统扩容设备： 对现有“双向”交换系统进行扩容，应对金税四期相关系统上线后业务互联网和税收业务专网数据交互的压力，降低数据交互的网络延迟。

动态防御设备：通过在业务互联网部署动态防御设备，提升应用访问的“不可预测性”，提供面向业务层的主动防御，高效甄别伪装和假冒正常访问行为的已知和未知自动化攻击。

### 1.2.3 项目实施要求

#### 1.2.3.1 实施范围要求

中标人按采购人的要求完成相关系统的设备上架（设备应按照采购人要求张贴标签）、电力测试、系统安装、加电调试、策略测试等系统集成工作，以达到项目的设计要求。

#### 1.2.3.2 实施时间要求

本项目由中标人统一供货并负责网络、安全建设集成。中标人需在合同签订后15天内交货，在合同签订后45日内完成项目实施工作并具备验收条件。

项目实施时中标人应充分了解采购人现有环境和应用系统架构，在接到采购人书面通知后10日内完成项目集成实施方案制定。且在整个集成实施过程中，不能影响现有应用系统的正常运行，合理安排系统中断时间，最长不得超过12小时。

#### 1.2.3.3 实施地点要求

本项目实施地点为安徽省税务局。

# 2 投标/响应要求

## 2.1 对供应商的要求

### 2.1.1 必备资质

**2.1.1.1 投标人应遵守有关国家法律、法规和条例,具备《中华人民共和国政府采购法》第二十二条的规定和本文件中规定的条件。**

**2.1.1.2 本项目的特定资格要求**

投标人所投产品厂商应均为中国境内注册，产品拥有自主知识产权，并且为国内研发和生产。数据加密传输设备需具备国家密码管理局颁发的《商用密码产品认证证书》。

### 2.1.2 优选资质/优选指标

**2.1.2.1 相关证书**

| 序号 | 证书名称 | 备注 |
| --- | --- | --- |
| 1 | 信息安全管理体系认证(ISO/IEC 27001) | 证书需在有效期范围内 |
| 2 | 质量管理体系认证证书(ISO9001) | 证书需在有效期范围内 |
| 3 | 隐私信息管理体系认证证书（ISO27701） | 证书需在有效期范围内 |
| 4 | 业务连续性管理体系认证证书（ISO22301） | 证书需在有效期范围内 |

**2.1.2.2 成功案例**

投标人需提供自 2022 年 1 月 1 日以来（以合同签订日期为准）,投标人独立承担的网络安全设备系统集成项目案例。

### 2.1.3 是否允许联合体

否

### 2.1.4 是否专门面向中小企业

本项目不专门面向中小企业采购项目

### 2.1.5 其他要求

1.本项目不接受分包、转包。

2.投标人有义务在中标后，与采购人签订保密协议，对采购人的各类文档、 资料、代码及相关信息具有保密责任，承诺未经采购人书面许可，不得泄露；若中标人不能按要求签订保密协议，采购人有权提出变更中标结果。

3.中标人参加本次项目建设的所有人员，均应和采购人签署保密协议。

4.所有与本项目相关的重要数据、往来信件，在传输、传递过程中均应加密。

5.本项目结束后，中标人应彻底删除招标方相关的网络拓扑、IP 地址、设备配置等信息，并不保留任何电子或纸质的备份。

6.投标人在中标后，即为采购人相关系统和网络信息安全的第一责任人，承担相关法律责任。

## 2.2 技术部分投标/响应内容

### 2.2.1 技术投标/响应总要求

投标人必须针对招标文件有关章节的需求，逐个或分块做出实质性响应回答，其响应应与招标文件内容采用同样的顺序。对每个需求的响应必须遵循如下规则：

（1）重复该需求；

（2）用“是/否”响应来表明该需求是否被满足；

（3）简要描述投标书或投标方案如何满足该需求，如果该响应在投标书其它部分有详述，可在该处简单应答，但必须给出确切的位置索引；

（4）解释投标文件或投标方案与用户需求之间的偏差；用数量来表示的需求，必须用确切的数字、单位来响应。

### 2.2.2 投标/响应方案要求

请投标人根据采购人需求，准备相关投标文档，如项目需求理解、产品指标响应、项目集成实施方案、项目交付方案、项目售后服务保障方案、项目实施应急处置方案、项目保密方案等。

### 2.2.3 产品分项报价要求

本项目报价须包含为完成项目实施内容而产生的全部费用，包括但不限于货物费、运输费、安装调试费、项目实施所需的所有配品配件和连接板卡（线缆），也包括与采购人原有服务器、网络、安全设备等所需连接的所有线缆、配件等。采购人后期不再追加任何费用。投标人需自行考虑各种风险，谨慎报价。投标人需按下表格式进行分项报价:

| 序号 | 产品类别 | 产品名称 | 单价 | 数量 | 合计 |
|---|---|---|---|---|---|
| 1 | 安全设备 | ▲全流量检测设备 | | 1 台 | |
| 2 | 安全设备 | 入侵防御设备（IPS） | | 2 台 | |
| 3 | 安全设备 | 应用程序接口（API）检测设备 | | 1 台 | |
| 4 | 安全设备 | 数据加密传输设备 | | 2 台 | |
| 5 | 安全设备 | “双向”交换系统扩容设备 | | 3 台 | |
| 6 | 安全设备 | 动态防护设备 | | 1 台 | |

# 3 项目需求

## 3.1 总体要求

1.投标人所提供的各类产品其性能必须达到或超过需求中必备性技术指标（标“★”技术指标）的要求。

2.项目实施应包含所需的所有配品配件和连接板卡（线缆），也包括与采购人原有服务器、网络、安全设备等所需连接的所有线缆、配件，应考虑齐全完备。若在具体实施时，所需配品配件及连接板卡（线缆）缺损时，由中标人负责增加解决，且不得因此而增加采购人费用。

3.投标人所投产品应确保技术指标中的真实性，虚假产品资质，技术参数响应一经发现，将报监管部门严肃查处。

## 3.2 采购产品一览表

| 序号 | 产品类别 | 产品名称 | 数量 | 单位 | 备注 |
|---|---|---|---|---|---|
| 1 | 安全设备 | ▲全流量检测设备 | 1 | 台 | 3 年原厂质保 |
| 2 | 安全设备 | 入侵防御设备（IPS） | 2 | 台 | 3 年原厂质保 |
| 3 | 安全设备 | 应用程序接口（API）检测设备 | 1 | 台 | 3 年原厂质保 |
| 4 | 安全设备 | 数据加密传输设备 | 2 | 台 | 3 年原厂质保 |
| 5 | 安全设备 | “双向”交换系统扩容设备 | 3 | 台 | 3 年原厂质保 |
| 6 | 安全设备 | 动态防护设备 | 1 | 台 | 3 年原厂质保 |

## 3.3 采购产品详细清单及技术指标

采购文件（技术部分）中有标注★号的，为必备服务要求，必须满足，如未作出响应，将导致响应无效；#为重要服务内容、△为一般服务内容。

| 序号 | 指标种类 | 指标名称 | 指标内容 | 重要性 | 是否需要证明材料 |
|---|---|---|---|---|---|
| 1 | 全流量检测设备 | 性能要求 | 标准机架式架构，配置≥4 个千兆电口，≥2 个万兆光口，≥128T 存储硬盘；冗余电源。<br>流量处理能力≥5Gbps。原始数据包存储空间不能低于 80TB | ★ | 否 |
| 2 | 全流量检测设备 | 必备功能 | 1.具备旁路接入功能，通过交换机端口镜像功能或者分流器做流量采集，具备基于 Vlan、GRE、VXLAN、MPLS VPN 等多种形式的虚拟接口设置虚链路采集流量功能；具备 IPV4 和 IPV6 双栈环境部署设备及采集并分析流量功能。<br>2.具备 L2-L7 层网络数据全流量捕获和存储功能，同时具备自定义过滤条件，过滤条件包括但不限于地址、端口、协议、应用等。<br>3.具备多维数据分析和提取功能，提供物理地址、IP 地址、网段、IP 会话、服务端口、协议、TCP 会话、UDP 会话等视图，视图之间支持下钻分析，同一界面不少于 5 个层次的数据钻取分析。<br>4.具备基于 Syslog、Kafka 等多种方式进行数据对接输出功能。<br>5.具备以图形化方式展现网络流量、数据包、TCP 数据包、数据包大小分布、警报、活动-并发会话数、新建-结束会话数、阻断等趋势图的功能。<br>6.具备对任意数据统计列表功能，自定义表头字 | ★ | 否 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 段，并依据所选字段生成数据透视表。<br>7.具备根据自定义配置及从第三方导入的 IP 地址、黑域名、数据包负载特征值的 TCP 通讯进行实时阻断功能。<br>8.根据招标人需求，通过定制开发实现与金税四期安全管理平台的对接。 | | |
| 3 | 全流量检测设备 | 重要功能 | 1.具备通过自定义流量、可疑 IP、可疑域名、特征值、邮件敏感字等警报规则进行检测告警的功能，自定义的特征值规则包含：数据包 payload 十六进制特征、ASCII 码特征、UTF-8 字符串，起始偏移/结束偏移，IP、端口、协议，大小，标志位等；具备使用“与”“或”等方式组合通信特征规则自定义告警功能。<br>2.具备使用 TCP、UDP、HTTP、DNS、ICMP 等协议的元数据建立异常行为模型感知网络异常事件的功能；具备多种元数据定义异常行为功能；具备对异常通讯行为的检测结果进行全流量回溯分析功能。<br>3.具备故障诊断视图功能；具备对数据包进行深层解码功能。<br>4.需内置数据包解码软件，具备在线对数据包进行解码分析功能；具备数据流重组功能，至少支持十六进制、ASCII 码、UTF-8 等方式展现会话内容；具备中英文双语协议数据包 L2-L7 解码、解封装功能；具备以十六进制、ASCII 码、EBCDIC 码等方式展现数据包内容功能；具备安全分析模块功能。<br>5.系统需内置常见网络通讯协议识别功能。 | # | 否 |
| 4 | 入侵防御设备（IPS） | 性能要求 | 2U 架构，配置≥2 个千兆电口、≥2 个万兆 SFP+插槽（2 个万兆多模 SFP+光模块，支持 Bypass）、≥5 个接口扩展槽，冗余电源。整机吞吐率≥40G、最大并发连接数≥1500 万、IPS 吞吐率≥20Gbps。 | ★ | |
| 5 | 入侵防御设备（IPS） | 必备功能 | 1.具备对设备信息进行监控功能，包括：CPU 使用率、内存使用率、磁盘使用率、CPU 温度、并发连接数、连接新建速率、接口带宽使用率、冗余电源、风扇状态等。<br>2.具备威胁分析功能，威胁分析展示包括：威胁事件的失陷/成功/尝试/失败等攻击结果、攻击事件级别、攻击类型分布、攻击阶段、事件详情等信息。<br>3.具备在线更新升级规则库功能。规则库包括但不限于攻击检测规则库、应用识别库、URL 分类库、僵尸主机规则库、威胁情报库、地理信息库，各规则库相互独立。<br>4.具备针对文件、远程访问、数据库、WEB 应用等关联协议类型进行暴力破解检测防御，包括 SMB、TELNET、LDAP、ORACLE、MYSQL、MONGODB、POSTGRESQL、DB2、REDIS、HTTP 等协议的口令暴力破解行为；具备对发生的暴力破解行为事件进行告警、取证和阻断的功能。<br>5.具备隐蔽通信检测功能，可设置相应警告、阻断动作。具备恶意域名检测功能。<br>6.具备僵尸主机与控制主机异常通信行为检测；具 | ★ | 否 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 备对 Windows、Linux、Unix 等多种操作系统的僵尸主机进行检测功能，并可根据规则进行相应警告、联动阻断。<br>7.根据招标人需求，通过定制开发实现与金税四期安全管理平台的对接。 | | |
| 6 | 入侵防御设备（IPS） | 重要功能 | 1.具备对攻击逃逸报文进行深度智能检测功能，包括：IP 分片、TCP 分段、HTTP-Body 压缩、URL 多重编码等类型。<br>2.具备 ARP 攻击检测功能，具备基于 ARP 请求的源 IP 不合法、响应的源 IP 不合法、响应的目的 IP 不合法、请求的源 MAC 与以太网源 MAC 不同、响应的源 MAC 与以太网源 MAC 不同、响应的目的 MAC 与以太网目的 MAC 不同进行检测。 | # | 否 |
| 7 | 应用程序接口（API）检测设备 | 性能要求 | 2U 架构，配置≥6 个千兆电口、≥2 个万兆光口、≥6 个 PCI 扩展槽，冗余电源；<br>默认应用数≥1000，可扩展到不限制；<br>HTTP 流量≥4000Mbps；<br>HTTP 峰值处理能力≥25000QPS；<br>日志存储量≥160 亿条。 | ★ | 否 |
| 8 | 应用程序接口（API）检测设备 | 必备功能 | 1.具备通过流量解析自动发现应用资产、接口资产、账号资产、敏感数据资产、文件资产和客户端 IP 信息功能。<br>2.内置接口类型识别规则，具备自定义接口类型识别规则功能。<br>3.具备生成 API 接口列表展示接口基本信息、风险及脆弱性标签等信息，并对接口进行标签标识的功能。<br>4.具备展示调用接口的客户端 IP 基本信息、关联信息、风险标签等信息的功能。<br>5.具备展示结构化、半结构化以及非结构化数据基本信息的功能，并能对数据分类分级，并根据需求对非结构化文档进行下载，同时能基于文档的上传下载情况进行分析。<br>6.具备对敏感数据或包含敏感数据的非结构化文件进行溯源的功能，并可通过应用名称、接口、账号和客户端 IP 等条件进行溯源结果的筛选。<br>7.根据招标人需求，通过定制开发实现与金税四期安全管理平台的对接。 | ★ | 否 |
| 9 | 应用程序接口（API）检测设备 | 重要功能 | 1.具备应用关系图谱分析功能，可根据应用域名进行应用查询，并能可视化展示被查询应用与其他应用服务之间的调用关系。<br>2.具备根据会话关联接口请求日志，实现会话还原的功能；可根据会话中的请求顺序进行会话回放。<br>3.具备二次封装接口识别和标识的功能，并能对接口封装前后样例进行对比和查看。 | # | 否 |
| 10 | 数据加密传输设备 | 性能要求 | 2U 架构，配置≥4 个千兆电口、≥4 个千兆光口、冗余电源。IPSec：密文吞吐率 ＞1Gbps、每秒新建隧道数 ≥500、最大并发隧道数 ≥3000。<br>SSL:密文吞吐率 ≥1Gbps、最大并发连接数 ≥5W、 | ★ | 否 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 最大并发用户数 ≥1W、每秒新建连接数 ≥800。 | | |
| 11 | 数据加密传输设备 | 必备功能 | 1.具备 SSL 卸载与代理及安全认证网关功能。SSL 卸载需能对基于 HTTP 和 HTTPS 协议的 WEB 应用进行保护，且能够基于协议（HTTP/HTTPS）、域名、端口号和 WEB 路径对 WEB 应用地址进行标识。<br>2.具备 SM1、SM2、SM3、SM4 密码算法。<br>3.具备国际、国密 SSL 和 IPSec 协议。<br>4.具备基于数字证书实现用户访问业务系统时的安全身份认证功能，具备多证书链功能，可同时支持多个证书颁发机构颁发的证书功能。<br>5.具备在同一个服务实例中配置 RSA 和 SM2 两张站点证书功能，并能同时启用，根据客户端的算法能力进行自动适应。<br>6.具备同时支持 IPv4 和 IPv6 功能，兼容 IPV4 与 IPV6 网络并存。<br>7.具备 IPV6 to IPV4 与 IPV4 to IPV6 模式下的地址转换功能。<br>8.具备 IPv6 over IPv4 隧道协议。<br>9.根据招标人需求，通过定制开发实现与金税四期安全管理平台的对接。 | ★ | 否 |
| 12 | “双向”交换系统扩容设备 | 性能要求 | 2U 架构，配置≥4 个千兆电口、≥4 个万兆光口、≥5 个接口插槽，冗余电源;<br>CPU≥（16 核/2.5GHz）*2;<br>内存≥256G ECC DDR4、内存插槽数≥16 个、可扩展至 1024G;<br>配置≥2 块 240G SSD 系统盘、2*960G SSD 缓存盘、4*4TB SATA 数据盘 | ★ | 否 |
| 13 | “双向”交换系统扩容设备 | 必备功能 | 1.具备物理机 USB 映射功能。<br>2.具备识别假死主机功能，限制重要业务在假死主机上运行。<br>3.具备内存 ECC 自动纠错机制。<br>4.具备虚拟机动态资源添加功能，在虚拟机 CPU 和内存使用不足时自动为虚拟机添加 CPU 和内存资源。<br>5.具备数据重建操作功能，可在重建过程中查看数据重建任务的对象名称、对象类型、数据量和优先级等信息。<br>6.具备针对磁盘进行自动隔离并重建数据、恢复业务性能的功能，并在界面提示告警信息及磁盘隔离原因。<br>7.具备展示虚拟化资源池的使用情况和健康状态功能，包括集群资源情况，各主机资源使用情况以及集群故障与告警信息。<br>8.具备与现网的双向交换系统组成同一集群功能，完成主机系统的平滑扩容。 | ★ | 否 |
| 14 | “双向”交换系统扩容设备 | 重要功能 | 1.在不同场景下满足存储对性能和可靠性的需求，具备为虚拟机的磁盘配置不同存储策略的功能。<br>2.具备图形化展示虚拟机的流量走向与访问关系功能，包括但不限于源对象、源 IP、目标对象、目的 IP、访问次数、服务类型、动作等。 | # | 否 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 3.具备在系统管理平台上通过拖拽虚拟设备图标和连线完成网络拓扑的构建功能，对整个平台虚拟设备实现统一的管理。 | | |
| 15 | 动态防护系统 | 性能要求 | 2U 架构、配置≥2 个万兆光口口、可根据实际网络情况可扩展千兆电口或万兆光口、网卡支持物理 Bypass 模式，冗余电源;<br>网络吞吐量（双向）：＞5Gbps;<br>HTTP 并发连接数：＞500 万;<br>HTTP 新建连接数：＞20000 连接/秒;<br>HTTPS 处理性能>7000TPS | ★ | 否 |
| 16 | 动态防护系统 | 必备功能 | 1.具备实时识别自动化攻击及漏洞隐藏防扫描功能。<br>2.具备插入 X-Forwarded-For 的方式功能，实现源地址透传。<br>3.具备网站访问情况可视化报表，内容至少包括单个或多个网站的访问量、异常数量、请求趋势、响应状态码、来源客户端信息。<br>4.具备根据需求对访问路径开启白名单功能，能够根据需求对来源 IP 开启白名单，批量导入、导出 IP 黑名单。<br>5.具备 Syslog 协议，涵盖系统日志、设备拦截日志等日志传输；兼容 SNMP 协议，并具备 SNMP Trap 功能；开放 RESTful API 接口以实现策略下发与设备管理。<br>6.根据招标人需求，通过定制开发实现与金税四期安全管理平台的对接。<br>7.具备全日志记录功能，完整记录所有正常用户请求和异常攻击请求。并具备基于查询语句、逻辑运算和模糊查询等多样化检索查询方式。 | ★ | 否 |
| 17 | 动态防护系统 | 重要功能 | 1.具备唯一标识功能，能够针对每个访问被保护网站的客户端生成唯一标识；具备收集客户端环境信息并有效识别用户的键盘和鼠标行为事件的功能。<br>2.具备抵御网页后门及重放攻击等恶意行为，拦截攻击者通过自动化程序发起的撞库攻击或者暴力破解的功能，并能拦截攻击者通过爬虫或其他自动化工具对网站上的页面、数据或敏感信息发起的爬虫搜索。 | # | 否 |

## 3.4 服务要求

| 序号 | 指标种类 | 指标名称 | 指标内容 | 重要性 | 是否需要证明材料 |
|---|---|---|---|---|---|
| 1 | 服务要求 | 服务要求 | 1.中标后提供产品原厂商针对此项目授权书及售后服务承诺书。<br>2.提供现场安装调试及实施服务；提供现场培训。<br>3.中标人需免费提供三年针对所投标设备的原厂硬件质保、软件升级、特征库更 | ★ | 否 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 新。 | | |

### 3.4.1 集成实施服务要求

中标人按采购人的要求完成相关系统的设备上架（设备应按照采购人要求张贴标签）、电力测试、系统安装、加电调试、策略测试等系统集成工作，以达到项目的设计要求。

### 3.5 其他要求

投标人所投产品必须是原厂新品且完全兼容采购人现有安全防护体系，若实际不满足要求或不兼容，采购人可以终止合同，投标人承担法律责任并赔偿采购人的全部损失。

## 4 人员要求

### 4.1 团队要求

### 4.1.1 基本要求

中标人应成立针对本项目的专业技术团队，配置 1 名项目经理，团队人员总数（不含项目经理）不少于 4 人，保障本项目的实施管理与监督。

### 4.1.2 优选资质/优选指标

| 序号 | 人员类别 | 人员岗位 | 人员要求 | 是否作为加分项 |
|---|---|---|---|---|
| 1 | 信息系统项目管理师 | 项目经理 | 具有中华人民共和国人力资源和社会保障部、工业和信息化部颁发的信息系统项目管理师技术资格证书 | 是 |
| 2 | 网络规划设计师 | 实施人员 | 具有中华人民共和国人力资源和社会保障部、工业和信息化部颁发的网络规划设计师技术资格证书 | 是 |
| 3 | 注册渗透测试工程师 | 实施人员 | 具有中国信息安全评测中心颁发的注册渗透测试工程师（CISP-PTE）认证证书 | 是 |

## 5 管理实施要求

1.投标人须成立完备的技术服务组织架构，具备完善的技术服务体系，以保障本项目完整顺利实施。投标响应文件中应对此进行详细阐述，包括但不限于以下内容:（1）服务组织架构（2）服务人员配置及技术能力（3）服务响应流程（4）服务质量承诺（5）服务质量监督机制

2.中标人负责项目文档资料管理，对于项目施工过程中的施工方案、验收报告等所有资料进行归类整理并装订成册，提交采购人留存。建立日常响应维修、健康检查报告，并进行汇总。

# 6 风险管控要求

项目实施期间，中标人须做好本项目各项安全保障工作，对人员管理、网络和数据安全、项目进度和质量等制定风险管控预案和防范措施。

1.安全风险管理

中标人应充分预估项目实施中存在的安全风险，包括并不限于：技术服务人员人身伤害风险、网络和数据安全要求等，制定可靠的安全保障措施。

2.进度风险管理

中标人应充分预估项目实施中存在的影响项目进度的风险，包括并不限于工作量变更、人员变更等，制定可靠的进度保障措施，确保项目按期完成。

3.服务保障要求

中标人是本项目技术服务与质量保障的主要承担者和责任人，必须能依据招标书中各项需求提供及时、高效的技术保障与服务。在合同规定的技术服务范围及期限内，不得另行收费。

4.质量保障要求

中标人必须向用户免费提供电话、E-Mail 等技术支撑方式。现场实施过程中避免对生产系统、业务连续性造成任何负面影响。例如系统、应用异常，产生垃圾数据，数据紊乱等。整改过程中，应提供整改需求说明及整改内容，并协助完成整改。

# 7 履约验收要求

## 7.1 总体要求

| 验收名称 | 验收要求 |
| --- | --- |
| 第 1 次验收-产品到货验收 | 包括全部设备的型号、规格、 数量、外型、配件、包装及资料、文件的验收。 |
| 第 2 次验收-项目初验 | 集成实施完成后，中标人负责进行现场测试，保障系统运行稳定，业务系统无影响。提交集成实施竣工文档、项目实施流程及项目实施质量总结报告。 |
| 第 3 次验收-2026 年度项目运行验收 | 提交 2026 年度设备运行报告、设备健康检查报告，保障系统运行稳定，业务系统无影响。 |
| 第 4 次验收-2027 年度项目运行验收 | 提交 2027 年度设备运行报告、设备健康检查报告，保障系统运行稳定，业务系统无影响。 |
| 第 5 次验收-2028 年度项目终验 | 提交合同剩余期限的设备运行报告、健康检查报告以及项目竣工文档。 |

## 7.2 具体要求

1.产品到货验收

中标人负责协调各硬件提供商向采购人统一发货，在产品到达采购人单位之后，配合采购人按验收要求对采购的设备进行验收，包括全部设备的型号、规格、数量、外型、配件、包装及资料、文件（如装箱单、保修单、随箱介质等）的验收。中标人需配合采购人对产品的性能和配置进行测试检查，并提交到货验收报告。

2.项目初验

本项目现场实施完成后，中标人需配合采购人完成项目初验，并向采购人提交完整的技术资料，包括拓扑图、设备配置参数、系统维护手册等。

3.项目年度运行验收（2026 年度和 2027 年度）

中标人应配合采购人对项目进行年度运行验收。

4.2028 年度项目终验

中标人在完成项目约定的所有实施内容后，向采购人提交验收申请。采购人在收到验收申请后成立验收小组（不少于 3 人），按项目招标文件组织项目终验。本项目的实施过程中将产生大量的技术及管理文档，中标人应协助采购人，负责建立、维护、交接项目实施过程中产生的各类文档，

确保项目文档的完整性和准确性。中标人应在验收时，将项目实施过程中产生的各类文档装订成册，提交采购人进行审核，包括设备集成实施方案、设备运行情况报告、采购人要求的其他与项目相关的资料和文档等内容。

验收通过后，采购人出具终验报告，作为项目尾款支付的依据。

# 8 其他要求

## 8.1 必备要求

### 8.1.1 通用必备要求

1.本项目中如涉及商品包装和快递包装的，其包装需求标准应不低于《关于印发<商品包装政府采购需求标准（试行）>、<快递包装政府采购需求标准（试行）>的通知》（财办库〔2020〕123 号）规定的包装要求，如有其他包装需求，详见采购文件技术部分相关章节。

2.本项目中如涉及网络关键设备或网络安全专用产品的，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。

3.本项目中如涉及国家强制性产品认证证书（CCC 认证证书）、电信设备进网许可证、无线电发射设备核准证等市场准入类资质的，应严格执行国家相关法律法规的要求。

以上相关要求，由供应商在响应时应答，在履约验收中，采购人将按照采购文件、中标/成交供应商响应文件、采购合同等对中标/成交供应商提供的货物和服务进行验收，必要时依法依规开展相应检测、认证。

## 8.2 付款安排建议

| 付款名称 | 付款要求 | 付款比例(%) |
|---|---|---|
| 第 1 次付款 | 项目完成初验后 | 50.0 |
| 第 2 次付款 | 完成 2026 年度项目验收 | 20.0 |
| 第 3 次付款 | 完成 2027 年度项目验收 | 20.0 |
| 第 4 次付款 | 2028 年完成项目终验后 | 10.0 |

## 8.3 其他要求

### 8.3.1★供应链安全管理要求

1.人员资格要求

（1）签订承诺书。中标人应严格落实国家税务总局网络安全和保密管理要求，承担现场实施人员的网络安全和保密管理责任，按采购人要求签订协议和承诺书。

（2）设置网络安全负责人。中标人为本项目配备一名网络安全负责人，该负责人具备独立决策能力并保持相对稳定，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。

2.日常行为规范要求

中标人负责对技术支持人员进行资格条件、工作胜任力以及网络安全能力评估，对技术支持人员承担的工作进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、工作秘密和税费数据等信息泄露、信息系统越权访问和网络攻击等风险。

3.违约惩戒措施

供应商对供应链安全管理责任落实不到位，造成安全事件或产生不良影响的，采购人按照法律法规及合同约定进行处理。

中标人应承担本项目中供应链厂商的相关网络安全责任，对未能及时履行供应链厂商相关网络安全责任的，应立即按照采购人要求进行整改。

### 8.3.2★廉政要求

#### 8.3.2.1 总体要求

为进一步落实全面从严治党要求，构建亲清新型政商关系，加强税务信息化项目建设过程中的党风廉政建设和反腐败工作，确保项目建设规范、廉洁推进，中标人在参与税务部门信息化项目工作过程中，需严格遵守法律法规、规范履行合同，积极协助税务部门开展廉政风险防控工作。请严格遵守并落实如下要求:

1.积极发挥廉政风险防控正向作用。中标人有义务配合税务部门在信息化项目工作中加强廉政风险防控，执行有关措施。

2.健全廉政风险防控机制。中标人有责任在项目管理机制中健全内部廉政防控措施，包括但不限于：对参与本项目的员工提出廉洁行为规范；指定专人对项目实施各环节进行廉政监督；在项目验收过程中提交本项目廉政情况报告等。

3.杜绝违纪违法行为。中标人及相关项目人员必须严格遵守党纪国法，坚守职业道德，杜绝任何形式的利益输送、权力寻租等违纪违法行为，对采购人工作人员不得实施以下行为:

（1）以各种形式和名义提供礼品、礼金、电子红包、支付凭证、商业预付卡、名贵特产、有价证券、股权、其他金融产品等财物。

（2）以各种形式和名义提供宴请、旅游、健身、娱乐、私人会所等活动安排；代付加班餐费、打车费等。

（3）以讲课费、咨询费等名义，提供或变相提供报酬。

（4）借款、借房、借车，报销应由个人负担的费用。

（5）以无偿、象征性地收取费用等方式提供家政、司机等服务劳务。

（6）其他通过任何形式行贿或输送利益的行为。

4.信守承诺。中标人应承诺在项目实施过程中，严格遵守国家法律法规合法、诚信经营，杜绝商业贿赂、规范经营活动、公开透明合作、严格内部管理，并签订《税务信息化项目服务商廉洁承诺书》提交采购人负责项目实施的单位。

5.自觉接受监管。中标人有义务配合税务机关的正常业务监管以及纪检监察、外部审计、督察内审等监督机构对税务信息化项目全过程的监督检查工作，如实提供相关资料和信息，不得隐瞒、篡改或销毁与项目建设有关的文件、数据等资料。

6.举报和反馈意见。项目执行过程中，中标人有权举报、反馈甲方索贿受贿、吃拿卡要、违反中央八项规定精神等违纪违法行为。项目验收前，应填写《税务信息化项目服务商廉政反馈书》，提交甲方税务机关网络安全和信息化领导小组办公室。

让我们在廉洁、诚信、公平、公正的基础上开展合作，共同为高水平建设效能税务、高质量推进中国式现代化税务实践贡献力量。

**8.3.2.2 廉政承诺**

中标人在中标（成交）后需签署《税务信息化项目服务商廉洁承诺书》，并提交至采购人项目实施单位。

# 税务信息化服务商廉洁承诺书

为深入贯彻落实党中央关于全面从严治党的决策部署，进一步加强税务信息化项目合作中的廉政建设，防范廉政风险发生，确保项目公开、公平、公正推进，我司郑重承诺如下:

**一、合法合规经营。**严格遵守国家法律法规及税务部门的相关规定，坚持廉洁从业、诚信经营的原则。在合作过程中不以任何形式进行利益输送，维护良好的政商关系。

**二、杜绝商业贿赂。**加强内部管理，我司及我司员工均不对甲方工作人员实施以下行为:

（一）以各种形式和名义提供礼品、礼金、电子红包、支付凭证、商业预付卡、名贵特产、有价证券、股权、其他金融产品等财物。

（二）以各种形式和名义提供宴请、旅游、健身、娱乐、私人会所等活动安排；代付加班餐费、打车费等。

（三）以讲课费、咨询费等名义，提供或变相提供报酬。

（四）借款、借房、借车，报销应由个人负担的费用。

（五）以无偿、象征性地收取费用等方式提供家政、司机等服务劳务。

（六）其他通过任何形式行贿或输送利益的行为。

**三、规范经营活动。**严格按照合同约定履行义务，保证项目质量，按时完成建设任务；在合作过程中不以任何借口拖延工期、虚报成本或谋取私利。

**四、公开透明合作。**我司承诺在项目实施过程中保持公开透明，主动接受税务部门及纪检监察机构的全程监督，并积极配合任何有关廉洁从业的调查工作。

**五、严格内部管理。**加强企业内部廉洁教育，确保员工知晓并遵守相关法律法规及廉洁要求；加强项目实施全过程廉洁监督；对于违反廉洁承诺的员工，将严肃处理，并承担相应责任。

**六、积极参与监督。**在税务信息化项目实施过程中，如发现任何违纪违法行为，将如实反馈问题和意见。

承诺单位（盖章）：----------

法定代表人或授权代表签字：----------

日期：XX 年 XX 月 XX 日

备注：本承诺书一式两份，一份由承诺单位留存，另一份交税务部门备案。

# 税务信息化廉政情况反馈书

| 项目基本情况 | |
|---|---|
| 项目名称（编号） | XXX 税务信息化项目　项目编号 |
| **服务商名称** | XXX 公司 |
| **联系人及电话** | 联系人：　职务：　电话：123-4567890 |
| **项目情况概述** | |
| **廉洁承诺履行情况** | |
| 反馈项 | 反馈内容 |
| **杜绝商业贿赂** | 向税务工作人员及其家属赠送礼品、礼金或提供任何形式的宴 |

| | |
|---|---|
| | 请、娱乐活动情况。 |
| **规范经营活动** | 按照合同要求，按时完成各阶段任务，确保项目质量和进度情况。 |
| **公开透明合作** | 在项目实施过程中保持信息公开透明，主动接受相关部门的监督和检查情况。 |
| **税务人员履职期间廉政情况** | |
| **税务人员履职过程存在违纪违规行为** | 否 |
| | 是（说明具体情况） |

提交单位（盖章）：XXX 公司

法定代表人或授权代表签字：----------

### 8.3.3 售后服务要求

中标人应根据采购需求，结合项目实际，提供售后服务保障方案，方案至少应包括但不限于以下内容：1.产品维护；2.技术支持服务体系；3.响应时间；4.健康检查方案。

中标人在合同期内需每年进行 4 次健康检查，检查完成后需提交健康检查报告。

1.自项目初验通过之日起，所有硬件在质保期内损坏，需在 72 小时内免费上门免费更换，本项目所有更换后的故障硬盘、故障 SD 卡等数据存储配件，所有权归采购人，由采购人保留。正式更换备件应来自原厂商

备件库，不得以其它方式替代。设备更换时，应提供不低于现有型号性能的备机。

2.中标人应有完善的售后服务体系和专业的服务团队并提供电话、传真、互联网、E-MAIL 和现场等方式的技术支持手段，服务请求的响应时间应少于 1 小时。

3.解决故障时，应保护好数据，做好故障恢复的方案，保证恢复到故障点前的业务状态。现场支持服务依故障的关键、和严重程度分别要求为:

| 严重程度响应时间 | 故障恢复时间 |
| --- | --- |
| 系统瘫痪，业务系统中断 | 4 小时 |
| 系统部分功能故障，业务系统轻微影响 | 24 小时 |
| 系统性能问题，造成性能下降，业务系统无影响 | 72 小时 |

4.售后维保服务期内如遇采购人全系统的网络调整和优化，中标人应提供技术人员参与，并保证该项目与全系统的有效衔接和平稳运行。

### 8.3.4 保密要求

1.投标人及参与项目的所有人员应严格遵守采购人的保密要求，签订保密协议和保密承诺书，并由投标人担保。

2.投标人对于采购人提供的资料，以及本项目实施过程中所涉及的所有文档、数据、介质和相关信息保密，未经许可，不得以任何形式向第三方传播。保密期限不受本项目期限的限制，在本项目履行完毕后，保密信息接受方仍应承担保密义务。

3.投标人应对参与项目的所有人员进行背景调查，并由投标人担保。

4.如因投标人一方的原因造成泄密，采购人将保留追究其法律责任的权利。

### 8.3.5 知识产权要求

1.项目交付过程中所产生的所有技术成果（包括相关技术资料、配置文档等）归采购人所有。采购人享有永久使用权、复制权和修改权。除本

项目工作所需外，未经采购人书面同意，投标人不得擅自使用、复制采购人的商标、标志、数据信息、文档及其他资料。

2.投标人应保证为本项目安装的软件为在中国境内具有合法版权或使用权的正版软件且无质量瑕疵。

3.投标人应保证其所提供的产品及服务不侵犯第三方的知识产权，否则，由此给采购人造成的一切损失由投标人承担。对本项目内由投标人采购的第三方工具软件，投标人须确保无知识产权纠纷。

4.投标人确保所提供的相关服务资源符合相关知识产权规定，一旦发生知识产权纠纷，所有责任则由投标人独自承担。