终端检测与响应系统扩容项目

采购需求书

珠海市珠港机场管理有限公司

2024 年 2 月 19 日

一、项目概述

1.项目背景

随着珠海机场信息化建设的全面快速发展，信息系统已经成为珠海机场各项业务工作正常开展必不可少的组成部分。为确保落实国家等级保护制度的相关要求，保证信息系统自身的安全防护能力，本场将按照统筹资源，重点保护，适度安全的原则，对终端检测与响应功能开展升级工作，以满足《网络安全法》等法律法规的合规性要求。

2.项目建设目标

通过本项目建设，落实国家的网络安全法、网络信息安全等级保护政策、标准，提升信息系统的安全防御能力，实现终端检测与响应功能的安全提升，并根据发展需求完成对终端检测与响应功能的升级工作，所使用的信息系统设备需具备防范病毒能力，实现实时监测、发现和应对各类安全威胁，减少安全事件的发生和影响，以满足《网络安全法》、《民用航空网络安全等级保护基本要求》等合规性要求。

本项目需要建设一套终端检测与响应系统,并不少于700台服务器主机提供病毒查杀、主动防御、系统防护等功能，含29个月病毒库、漏洞库、规则库和软件的升级许可。

3.项目建设内容

本项目最高限价：¥362,100.00元

序号	项目	系统描述	数量	单位
1	终端检测与响应系统	1.支持病毒查杀、网马查杀、漏洞管理、微隔离、主动防御等功能； 2.支持已知和未知类型勒索病毒检测查杀,挖矿防御查杀； 3.支持高级威胁防御、渗透攻击防护； 4.支持系统防御，包括系统登录防护、防暴力破解、进程防御、文件访问监控等功能； 5.支持web应用防护； 6.适用于各类型服务器防护，支持包括不限于Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、Centos 5.0 +、	1	套

		Redhat 5.0 + 、Suse 等； 6. 具体功能需求详见第二章节“技术需求”		
2	系统软件授权	为服务器主机提供病毒查杀、主动防御、系统防护等功能，含 29 个月病毒库、漏洞库、规则库和软件的升级许可。	700	个

二、技术需求

指标项	技术参数
部署方式	支持纯软件部署，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署，同时也支持硬件管理平台交付
一体化管控	单一管理控制中心须支持统一管理分别部署在 Windows PC、Windows 服务器、Linux 服务器以及国产化服务器的客户端软件
管理可视化	支持 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能
多维度威胁展示	支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell 后门、高危漏洞及其各自影响的终端数量
	提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数
云端威胁分析	支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。
自动分组	支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组
影子终端发现	支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描，及时发现尚未纳入管控的终端
策略管理	支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录
资产管理	支持系统信息的清点，包括操作系统及其版本、环境变量、内核模块、运行服务、启动项、计划任务、注册表、网络连接、开放共享以及国产化终端替代率
	支持清点系统上的安装包与类库、应用资产的清点，安装包与类库包括系统安装包、Jar 包、Python 包、Npm 包，应用资产包括系统软件、浏览器、office 办公等软件以及数据库和中间件
	支持全网视角的端口和运行进程的清点，在监听端口视角，可以识别风险端口，并支持一键封堵端口和解除封堵
	支持按 Web 站点、服务、应用、框架等多层次来清点主机上的 Web 应用的资产信息
	支持基于单个终端视角的运行状态的监控，包括但不限于进程、服务、网络连接、

	计划任务和开放共享信息
	支持对终端账户信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户
风险评估	支持基于系统内置弱密码字典和自定义弱密码字典的检查功能，弱密码检测支持至少包括 SSH、RDP、MySQL、Tomcat、Redis 等应用类型，可按照空密码、自定义弱密码、密码长度小于 8、字符种类小于 3 等常见弱密码类型进行分类查看
	支持勒索风险管理功能，持续跟踪最新的勒索情报和技战法，实时展示出资产中的入侵风险，包括勒索风险端口、勒索应用弱密码和勒索风险漏洞，为用户做勒索风险加固提供数据支撑
	支持暴露面梳理功能，可以快速识别环境中暴露在外网的端口及应用，当检测到有来自于外网的 IP 地址访问时，判定该资产为外网暴露面资产，帮助用户高效梳理资产脆弱面
	支持展示最新公布的热点漏洞信息，并且梳理出其中的高可利用漏洞统一展示在热点漏洞页面，方便运维人员一键对当前已接入的终端进行漏洞检测，同时支持设置热点漏洞定时检测
终端日志报表	支持根据统计周期、终端名称、IP 地址，补丁信息和漏洞等级等多维度的入侵检测日志，杀毒扫描日志，微隔离日志，合规检测日志，管理员操作日志，运维日志，联动日志等的日志查询和检测
升级管理	支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴
管理员管理	支持配置不同的权限角色，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限，并配置可管辖的终端范围，支持管理员账号限制 IP 登录；支持管理员账号采用双因素认证
威胁检测	须具备自研的基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种
	支持通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整客户端的资源占用（CPU、IO 等），为业务让出资源，不卡业务，对业务零摩擦。
	支持非常用登录 IP、非常用登录时间的异常登录检测；支持终端扫描端口的异常扫描检测
	支持通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率
	支持基于本地缓存信誉检测与全网信誉检测，构建企业全网信誉库的检测引擎，做到企业内网一台威胁，全网感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率，减少终端资源开销
	支持针对最新未知的文件，使用 IOC 特征（文件 hash、dns、url、ip 等）的技术，进行云端查询。云端的安全中心，使用大数据分析平台，基于多维威胁情报、云端沙箱技术、多引擎扩展的检测技术等，秒级响应未知文件的检测结果，构架公有云云查体系

	支持一键云鉴定服务，提供云端专家+沙箱+多引擎鉴定能力，结合云端威胁情报对已告警的威胁文件再次进行综合研判并给出 100%黑白结果，用户可自助对管理平台告警的威胁快速判断是否误报和了解威胁详情。
终端自保护	支持 agent 安装目录的文件保护，可以保护 agent 目录和文件实时监控驱动文件，可以保护 agent 的服务/进程/文件不被恶意删除，以免影响正常功能，导致用户的终端受到病毒入侵
	支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz 的自启动，可以防止黑客攻击
	针对 Windows 系统，支持实时监控所有非授信驱动及黑客工具的装载、运行等行为，发现风险行为时进行提示和拦截，同时，支持设置敏感时间段，监控敏感时段内可疑驱动的装载、运行等行为，发现风险行为时进行提示和拦截
业务零侵害	支持开启 agent 自动降级机制，可设置主机资源如 CPU 利用率、剩余内存、等待任务长度、磁盘列队长度达到的阈值，当任意资源达到阈值持续一段时间后，agent 会进入降级状态，当资源占用恢复到正常值时，agent 自动恢复为在线状态
	支持 agent 性能保护兜底机制，可设置 agent 主进程、威胁检测、病毒查杀等进程的资源占用阈值，当进程资源占用达到阈值时，进程会自动重启
文件实时监控	支持实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低 3 种防护级别
Webshell 事件处理	支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件 Hash 值，文件大小，文件创建时间；可配置 WebShell 实时扫描，一旦发现 WebShell 文件，可自动隔离或仅上报不隔离
Windows 服务器加固	支持并提供基于可信鉴定方式的进程防护方式，通过人工智能自学习机制，自动建立信任进程名单，阻断非可信进程的运行并提供配置指引，同时支持通过模板和手动的方式添加信任进程
	支持 windows 服务器 RDP 远程登录保护，可开启 RDP 远程登录二次认证，以防止黑客对服务器的入侵
Linux 服务器加固	支持 Linux 服务器 SSH 远程登录保护，可开启 SSH 远程登录二次认证，以防止黑客利用弱密码脆弱性对服务器的入侵；支持设置验证码验证或自定义密码验证，支持设置登录认证提示、生效时间段和免二次认证白名单
勒索病毒专防	支持基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御
	支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截
	支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具
	支持勒索可疑行为检测，通过行为 AI 能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截（需提供产品截图证

	明）
终端合规检查	支持一键式操作对指定 Windows 终端/终端组进行通用安全检查基线、等保二级基线、等保三级基线、CIS 系统基线、CIS 应用基线、以及基于以上基线规则原型的自定义基线的合规性检查，可视化展示终端的基线合规检查结果，并对不合规的检查项提供设置建议
	支持一键式操作对指定 Linux 终端/终端组进行通用安全检查基线、等保二级基线、等保三级基线、CIS 系统基线、CIS 应用基线、以及基于以上基线规则原型的自定义基线的合规性检查，可视化展示终端的基线合规检查结果，并对不合规的检查项提供设置建议
暴力破解检测	支持统计单个攻击源及分布式攻击源的暴力破解检测，支持按照 RDP、SMB 和 SSH 类型进行封堵并自定义爆破阈值，可对封停时间进行自设置
威胁处置	支持构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置
	支持强力专杀云端下发通道，支持在管理端批量下发强力专杀工具到内网各终端快速响应终端威胁。
漏洞防护	支持对 Windows 终端的漏洞情况进行扫描，并查看漏洞具体情况及 KB 号，并显示具体修复情况
	支持流行 Windows 高危漏洞的轻补丁免疫防御，支持 Windows 补丁批量一键修复
	支持对 Linux 终端扫描系统漏洞、提供漏洞分析详情和修复建议。
轻桌管	支持拦截已安装软件的恶意广告弹窗，保持工作环境清净无打扰
	支持分组的 USB 存储是管控防护启用，不允许指定终端分组下的终端使用 USB 存储设备
	支持 Windows 系统的违规外联动能，有效帮助管理员规范终端上网行为
windows 智御	支持对 Windows 停更的系统提供专项防护，包括 0day 漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能；
	支持对已停止更新的 Windows 系统的全网一键清点，管理员可快速筛选出全网已停止更新的 Windows 系统的数量和具体的终端；
	支持与同厂商的安全态势感知平台进行安全联动，支持管理员在安全态势感知平台管理界面下发快速查杀任务，并查看任务状态、结果并进行处置
	同厂商的安全态势感知平台检测到某主机有僵木蠕毒的 C2 通信时，支持手动或自动化将恶意域名信息下发到本产品做 C2 通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离，且安全态势感知平台对此事件不再重复告警。
	支持为同厂商的安全态势感知平台提供溯源举证功能，即本产品检测到僵木蠕毒的恶意域名访问时，会共享事件信息给同厂商的安全态势感知，并且可以在安全态势感知侧进行威胁事件的溯源分析，定位到该主机上发起恶意域名访问的具体进程、及其进程链信息，并且安全态势感知根据返回的举证信息，联动客户端对恶意进程进行处置
	支持将本产品检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到同厂商安全态势感知平台，安全态势感知平台进行分析和展示（提供产品证明截图）

	支持将采集终端资产信息（包括操作系统、硬件、软件、账户、监听端口、运行进程等）上报同厂商的安全态势感知平台，并由安全态势感知平台统一组织主机资产的可视化呈现
	支持将主机上采集的流量上报至同厂商的安全态势感知的探针，尤其补充主机之间的东西向流量，供安全态势感知做全面的流量分析和检测，支持流量转发协议VXLAN/GRE，支持设置流量转发阈值、流量采集五元组过滤
下一代防火墙的联动响应	支持与同厂商的防火墙进行安全联动，管理员可以在防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息
	同厂商的防火墙检测到某主机有僵木蠕毒的C2通信时，支持手动或自动化将恶意域名信息下发到本产品做C2通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离且防火墙的此事件不再重复告警
	支持为同厂商的防火墙提供溯源举证功能，即本产品检测到僵木蠕毒的恶意域名访问时，会共享事件信息给同厂商的防火墙，并且可以在防火墙侧进行威胁事件的溯源分析
上网行为管理的联动响应	支持与同厂商的上网行为管理平台进行安全联动，支持管理员在上网行为管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息
	支持管理员在同厂商的上网行为管理平台界面下发一键隔离指令，对终端恶意文件进行隔离，防止病毒进一步扩散
MSS安全服务的联动响应	支持与同厂商的安全云管、云脑、安全托管服务产品对接，向本地化赋予本地化云端能力
	支持将检测出来的威胁事件上报到同厂商的安全云管、云脑和安全托管服务产品，进行联合分析溯源终端威胁事件

三、供应商资质要求

1.供应商须持有合法有效的企业法人营业执照。

2.供应商为合法的授权代理商，提供厂商出具的代理证明或项目授权文件以及售后服务承诺函，相关所提及产品应与授权代理产品一致。同一品牌厂商与其授权代理商不能同时参与本项目的报价，如厂商和授权代理商同时报价参与本项目，只接受厂商报价。

3.供应商具备中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书，以上资质出具证书复印件证明加盖单位公章。

四、项目要求

1.货物要求：

供货时，软件授权名称须为项目使用人珠海市珠港机场管理有限公司，并能通过序列号、官方热线电话、email等方法进行查验。

2.货物质量和合法来源保障：

为了保障产品质量及售后服务，供应商提供的所有授权必须为原装、全新、未经激活的产品。应在确定供应商后10天内提供所投授权的合法来源证明和采购清单中所要求的相关证书复印件，送至本单位签收（注明提交时间）。如提供的证明文件不全或存在虚假情况，我方将向有关部门举报虚假事件，供应商商须承担因此造成的一切法律责任，包括但不限于税款、滞纳金、罚款等损失。

3.项目报价及部署调试要求：

报价须包含所有费用（包含但不限于：软件费、办证费、设备费、人工费、材料费、安装费、运输费、保险费、管理费、利润、税金等），不得事后再议价，需送货上门以及提供本项目各类设备及软件等的安装调试服务。

供应商应派经机场方认可的有经验和能力、具有相应资质的技术人员，项目人员配备不少于3人（含项目经理），人员要求如下：

- 1名项目经理要求5年或以上中大型项目管理经验，具备PMP、信息系统管理师级别认证；
- 1名资深技术专家要求3年以上网络信息安全实施、运维经验，具备安全领域的CISSP认证；
- 1名中级安全工程师要求2年以上大型信息系统实施经验，具备CISP认证。
- 供应商在签订合同前，提供上述人员资质证书复印件及上述人员近六个月内任意三个月的社保记录作为证明材料。
- 参与项目实施及售后运维的专职人员在项目实施期间未经机场方同意不得擅自变动既定人员安排；如确需变动，需提前一周向机场方提出申请，申请通过后方可变动。

供应商须完成现场所有设备、授权的软件安装部署，应根据现场实际情况，制定部署方案，供应商对项目的规划和实施步骤加以说明，应做出整个项目分阶段的详细进度计划图，以及对进度完成的保证措施和可能造成项目延期补救方法，并列明本次项目分阶段完成的时间表。

项目部署期间，须保持珠海机场的其他生产系统运行不可中断，供应商须对设备系统不间断运行提出安全的部署措施。若实际实施中必须停用或重新启动所需设备，供应商需得到机场方现场管理人员审核确认方才可执行，若未经现场管理人员的审核确认造成的一切损失，均由供应商承担。

项目部署期间，珠海机场生产系统如遇因本项目而导致的技术故障，供应商须联合厂商进行及时的功能性技术调整。同时应兼容本场现有的终端检测与响应系统，各个业务系统能够平滑过渡，以保证珠海机场业务及部署的系统和设备可安全的、稳定的运行。

4.安全性要求

系统可根据不同的维护级别，进行维护权限的设置。对于系统人机界面操作，系统要有相应的操作可查纪录。本系统能提供全方位的系统日志功能，可监控系统运行情况，支持操作审计功能。

为保证系统的安全稳定运行，在整个项目建设的过程需要充分考虑系统的安全防护措施，本次项目建设的系统集成安全要求包括但不限于以下内容：

- 要求提供对第三方服务的服务地址安全管理、服务请求安全处理策略、安全审计日志、客户端安全证书和基本认证信息，确保服务集成的安全性；
- 要求所有数据传输均采用数据加密方式（SSL 或其它），并提供数据交换集成的全程监控运维工具来监控数据包的的运行过程进行全程监控，以确保数据交换集成的安全性；
- 数据访问日志能记录对数据库进行的所有操作，包括增加、删除、修改和查询的 SQL 语句，是否写数据访问日志可以通过系统配置文件来配置；
- 程序异常日志必须能记录程序发生错误的异常信息；
- 系统日志应能记录应用程序发生错误时所产生的异常信息；
- 系统能提供系统异常事件的日志查询界面，同时提示相关原因及解决办法；
- 调用系统内部所涉及模块内部或模块与模块之间的关系；
- 具有自定义指标和级别的日志功能，自定义指标可以增加记录消耗 CPU 值，IO 值，响应时间等，有利于性能调优和故障排除；
- 系统能记录用户登录、退出系统的情况，记录用户的活动和操作数据情况；
- 系统能提供普通用户或系统管理员变更组织、人员信息、权限、口令等信息的情况记录；
- 系统能记录应用系统的系统配置参数、主要设置和核心数据等变更情况；

- 系统能记录敏感、关键信息的查看情况，能记录用户修改、删除日志的情况；
- 所有系统日志容量至少支持保存六个月。
- 支持对系统各业务之间、平台/系统之间、模块之间数据流转进行分析，划分系统主数据、流程数据，保证系统数据的准确性、唯一性，同时能够对数据进行区分管理。

5.技术培训要求

供应商须对机场方的技术人员进行技术培训。须提供详细的系统使用操作指引培训计划，计划需包括培训内容、培训时间。供应商提供的负责培训的人员应具备同类项目五年以上的经验。技术培训费用应包含在总价中。

技术培训至少应包括下列内容：

- 系统原理、架构构成和功能的描述。
- 常见故障的处理或排除。
- 系统各部件的检查、调整和维护。
- 对使用者关于系统操作平台设备等操作技能的培训。

6.项目质保期：

自验收合格之日起对本项目的项目质量保证期不少于 29 个月（若国家和/或生产厂家对本项目所涉及产品的质量保证期的规定高于本项目要求的，应按国家和/或生产厂家的规定执行，若文件中承诺高于该期限，按照供应商承诺）。在保修期内提供上门升级维护服务。

7.售后服务要求：

- 项目维保期：项目验收后提供 29 个月（2024 年 5 月-2026 年 9 月）包含但不限于原厂（上门/远程故障处理、软件升级、技术电话咨询等）维保服务（提供原厂售后服务文件）。
- 原厂维护服务：必须在华南地区有 3 名或以上技术人员提供服务，以保证紧急情况下技术人员可及时到场解决。
- 维护期内现场支持，解决日常维护当中的问题，包括但不限于操作使用、技术讲解、问题排故、功能性需求调整、软件版本升级、bug 修复、补丁安装、病毒库升级、规则库升级、漏洞库升级等。
- 维护期内，对影响生产的故障提供 7*24 小时服务，15 分钟内电话响应。
- 维护期内，每天（包括周六周日），在维修响应时间内，我方可随时通过电话或 email 就有关技术问题向供应商或厂家的技术人员进行咨询;我方电话享有

高度的优先级，优先处理我方电话求助，直至得到我方满意的结果；专业的技术工程师可以保证快速有效的支持。

- 提供项目验收后 29 个月主动式的每周巡检和分析服务，依据我方要求检查软件的运行情况，并出具巡检报告；供方在重要节日（如:春节、劳动节、中秋节、国庆节等国家法定节假日)、重大活动及机场重保期间前必须按需方要求对软件的健康情况进行一次全面的巡检和分析。

8.服务承诺：

供应商中选后 10 天内开出服务承诺函并加盖公章，服务承诺的内容包含对本项目提供的所有服务（如质保服务、培训服务、售后服务等)。

9.项目实施要求：

供应商应严格按照采购需求约定的时间完成项目实施的全部工作，项目总周期为90天（其中含试运行阶段30天)，其具体开始的日期以合同签订的时间为准。

供应商在合同签订之日起60天（含非工作日）内完成安装调试完毕（用户根据实施进度需要延迟的除外)。

项目完工交付后 30 天内，供应商提供《系统试运行报告》，甲方根据《系统试运行报告》对系统试运行情况进行确认。

甲方根据供应商已提供本项目规定的全部货物、服务和项目相关资料等包括但不限于：

- 需求清单内所有软件产品相关授权证书（含相应模块)。
- 需求书内要求的相关证明文件。
- 初次部署及测试报告。
- 相关产品应用培训资料。
- 安装实施过程中涉及到的相关资料文件等。

11.付款方式：

本项目的安装、调试、验收合格，双方签署最终验收文件，且甲方收到乙方开具全额增值税专用发票及其他必要文件后 60 个工作日（以甲方终验合格时间、收到发票时间两者孰晚开始计算)，甲方通过银行转账方式向乙方支付本合同含税总价的 95 %。

质保金为本合同含税总价的 5 %，如无质量异议，且乙方全面履行本合同义务，则质保期满后 60 个工作日无息退还给乙方。

如果双方发现存在发票遗失的情况，乙方应按照相关法律规定的要求配合甲方进

行发票遗失的处理。如果因乙方的原因导致任何延期开具和交付发票的情况，甲方有权就因此而产生的损失要求乙方进行赔偿。

如果乙方未能按照合同约定向甲方开具并及时交付合法有效的发票，或者乙方虽然按约定向甲方交付发票，但交付发票的真实性和有效性存在问题致使甲方遭受损失或者税务机关处罚的，乙方应当承担因此造成的一切法律责任，包括但不限于税款、滞纳金、罚款等损失。

我公司可满足以上需求并报价：

（加盖公章及骑缝章）