合同编号：

信息化服务合同

委托方(甲方)：　内蒙古自治区教育考试院

受托方(乙方)：　信元网络技术股份有限公司

采　购　包：　采购包 4：供应链安全测评服务

签 订 地 点：　内蒙古自治区呼和浩特市

签 订 时 间：　2026 年 05 月

甲方：内蒙古自治区教育考试院

地址：内蒙古自治区呼和浩特市赛罕区乌兰察布东街甲81号

乙方：信元网络技术股份有限公司

地址：内蒙古自治区呼和浩特市新城区南店街33号信元网安大楼

甲乙双方根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《中华人民共和国民法典》等相关 法律法规、规范性文件以及 信息化服务 项目NMGZC-G-F-260085的中标（成交）结果、招标（磋商、谈判）文件、投标（响应）文件等文件的相关内容，经平等自愿协商一致，就如下合同条款达成一致意见。

一、乙方向甲方提供的服务内容

（一）根据招标（磋商、谈判）文件及中标（成交）结果公告，乙方向甲方提供的服务、货物（如有）内容如下： 供应链安全测评服务（采购包4）。

（二）服务项目名称、服务具体内容、服务方式、服务要求、服务成果及与之相关的货物等详细内容，见合同附件—服务清单。

二、乙方服务成果的交付时间、地点

（一）服务期限： 合同签订之日起壹年。根据《内蒙古自治区财政厅关于加强政府采购合同签订公告备案管理的通知》（内财购函〔2021〕1149号），采购需求具有固定性、延续性且价格变化幅度小的服务项目可在采购文件中明确签订不超过3年履行期限的政府采购合同，在年度预算能保障的前提下，该项目履行期限为三年，此次采购活动为第一年采购，履行期限内每年服务期结束后，经评估合格，一年一签政府采购合同并分年付款，合同金额按第一年采购金额算，服务内容如有重大变化经甲乙双方协商可终止合同。

（二）服务成果的交付时间和交付要求（如有）：_满足行业标准、采购文件要求及采购人需求。__

（三）服务地点：内蒙古自治区教育考试院。

（四）乙方代表及联系电话：孟祥波13754010880。

（五）甲方代表及联系电话：李卿18004713669 。

三、乙方提供服务成果的质量

乙方提供的服务应同时满足：1.符合国家法律法规和规范性文件对服务质量的要求；2.符合甲方招标（磋商、谈判 ） 文件对服务的质量要求；3.符合乙方在投标（响应）文件中或磋商、谈判过程中对服务质量作出的书面承诺、声明或保证。上述质量要求作为甲方对乙方服务质量的验收依据。

四、乙方服务成果的交付方式及载体

乙方交付服务成果方式及载体应符合国家法律法规和规范性文件的要求，并符合甲方招标（磋商、谈判）文件的要求、乙方在投标（响应）文件中对服务成果交付方式及载体作出的承诺。

五、甲方对乙方服务的监督

甲方对乙方提供的服务有权进行监督，当乙方服务质量、服务内容不符合约定时，甲方有权要求乙方及时进行整改，对乙 方拒不改正或整改不到位的，甲方有权随时解除合同，并根据具体情况扣除部分或全部服务费用。

六、合同金额

在乙方提供完全符合合同要求的服务的前提下，本合同总金额为320000.00元（小写）叁拾贰万元（大写）。

七、付款时间及条件

（一）付款时间及条件

1、合同签订后，**乙方**提供合法发票，达到付款条件（包括采购**人**资**金**到位）30 个**工**作**日**内甲**方支**付合同款的 40%；

2、**乙方**履**行**服务半年，**乙方**提供相应的服务报告及合法发票，达到付款条件（包括采购**人**资**金**到位）30 个**工**作**日**内甲**方支**付合同款的 40%；

3、合同内容履**行**完成并通过验收后，达到付款条件（包括采购**人**资**金**到位），**乙方**提供合法发票，甲**方**在收到发票 30 个**工**作**日**内**支**付合同款剩余的 20%。

（二）履约保证**金**

不缴纳。

（三）乙方账户信息

乙方账户名称： 信元网络技术股份有限公司

乙方指定银行： 光大银行呼和浩特呼伦南路支行

账　　号： 5013 0188 0001 67184

行　　号：3031 9100 0037

八、知识产权

乙方应保证其提供的服务及服务成果的全部及部分，均不存在侵犯第三方知识产权的情形，其服务成果的所有权由甲方享有。否则，乙方应向甲方承担违约责任及赔偿由此给甲方造成的名誉及经济损失。

九、违约条款

（一）甲方没有正当理由逾期支付合同款项的，每延期一日，甲方应按照逾期支付金额 未付部分的0.05%承担违约责任。延期达到 120 日，乙方有权解除合同，并要求甲方赔偿由此造成的经济损失。

（二）甲方存在其他违反本合同的行为，应承担相应的违约责任（注：可以根据情况进行细化）；违约金不足以赔偿乙方损失的，乙方有权要求甲方赔偿由此造成的经济损失。

（三）乙方逾期提供服务成果的，每延期一日，乙方应按照未完成部分对应合同金额的 0.05% 承担违约责任。延期达到 120 日，甲方有权解除合同，拒付延期部分的相应服务款项，并要求乙方赔偿甲方的经济损失。

（四）乙方交付的服务不符合质量要求，或其服务成果存在侵权行为的，甲方有权解除合同，并要求乙方支付合同总金额 10%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（五）乙方在参与本项目采购活动过程中，如存在提供虚假承诺、证明、串通投标等违法违规行为，除承担相应的行政责 任外，甲方有权解除合同，并要求乙方承担合同总金额10%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求 乙方赔偿经济损失。

（六）乙方存在其他违反本合同的行为，应承担相应的违约责任；违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

十、不可抗力

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在 30 天内提供有关不可抗力的相关证明。合同未履行部分是否继续履行、如何履行等问题，由双方协商解决。

十一、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成，可以采用下列第（二）种方式解决：

（一）提交 甲方所在地 仲裁委员会仲裁。

（二）向 甲方所在地有管辖权的 人民法院起诉。

十二、合同保存

合同文本一式 四 份，甲乙双方各执二份。合同文本保存期限为从采购结束之日起至少保存十五年。

十三、合同附件

本合同所附下列文件是构成本合同不可分割的部分，与本合同具有同等法律效力：

1、服务内容

2、保密协议

3、中标通知书

十四、双方约定的其他事宜

无。

十五、合同未尽事宜，双方另行签订补充协议，补充协议是合同的组成部分。

十六、本合同由甲乙双方法定代表人/负责人或授权代表签字并加盖公章或合专用章后生效。

（以下无正文）

甲方（采购人）：内蒙古自治区教育考试院（盖章）

法定代表人/负责人或授权代表（签字）：

地 址：内蒙古自治区呼和浩特市赛罕区乌兰察布街甲 81 号

电 话：

开户银行：

帐 号：

年 月 日

乙方（供应商）：信元网络技术股份有限公司（盖章）

法定代表人/负责人或授权代表（签字）：

地 址:内蒙古呼和浩特市新城区南店街 33 号信元网安大楼

电 话:0471-4599666

开户行及行号：光大银行呼和浩特呼伦南路支行 5013 0188 0001 67184

开户行行号：3031 9100 0037

年 月 日

附件 1、服务内容

一、服务概述

内蒙古自治区教育考试院现有的7个关键业务系统—包括考生综合服务平台、试卷扫描系统、网上阅卷系统、网报志愿系统、网上录取系统、国家教育考试综合管理平台以及办公自动化及网站发布系统——均已按照国家网络安全等级保护三级标准接受全面安全评估，并由具备相应资质的专业测评机构实施。7个关键业务系统均已依据网络安全等级保护三级要求，构建了较为完善的安全防护体系。在安全管理区集中部署入侵检测、APT检测、堡垒机、日志审计、VPN网关等安全设备；核心区以高性能核心交换机为枢纽，串联WAF、防火墙、负载均衡等设备，形成纵深防御；数据库区则通过边界防火墙、数据库防火墙与审计系统实现细粒度访问控制。运维与业务终端分别通过SSH/HTTPS和HTTPS协议进行安全访问，确保内外操作隔离可控。

各系统普遍通过VPN、SSH、HTTPS等加密通道支持远程运维与业务访问，结合日志审计与访问控制机制，有效保障了数据交互与系统运行的安全性。整体来看，各系统在网络分区、安全设备部署、访问控制策略等方面均体现了“分区分域、纵深防御、集中管控”的安全原则。

随着教育信息化发展，内蒙古自治区教育考试院在考试报名、考试管理等业务中高度依赖各类信息系统和第三方技术服务，系统供应链结构复杂，涵盖多来源、多环节、多技术栈的软硬件及开源组件。在此背景下，从供应链全生命周期视角，系统性开展供应链安全治理工作，通过技术检测、 险分析和管理评估相结合的方式，全面识别和管控供应链安全 险，构建安全可控、责任清晰、可持续运行的供应链安全治理体系。投标时供应商需提供技术服务方案、质量保障方案、进度保证措施、突发事件应急处理方案、 险防范措施和保密措施。

1.需求分析

结合实际情况，当前供应链安全主要面临以下需求：

（1）供应链组件与系统 险识别：现有系统使用大量第三方软件和开源组件，需进行漏洞关联分析、依赖溯源、敏感信息检测，并建立整改与复测机制。

（2）重点产品技术安全验证：核心业务系统和关键供应链产品需通过黑盒测试进行安全评估，识别高危漏洞和业务逻辑 险。

（3）供应商安全能力差异化管理：因供应商类型复杂、能力差异大，需建立覆盖技术、管理和服务的安全能力评价体系，实现分类分级管理。

（4）持续治理与 险闭环管理：需通过常态化 险分析、检测、整改和评估，形成闭环治理机制，实现 险的动态管控与持续降低。

2.服务方案设计

（1）服务目标：

围绕“可识别、可评估、可管控、可追溯”的总体要求，构建符合实际的供应链安全治理体系，具体包括：全面识别 险、实现闭环治理、提升供应商管理精细化水平、增强治理支撑能力，以及构建安全可控的治理体系。

（2）服务依据：

严格依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络安全等级保护基本要求》《软件供应链安全要求》及《信息系统安全运维管理指南》等法律法规与标准。

（3）服务原则：

依法合规、 险导向、全生命周期治理、技术与管理并重、分级分类与精准管控、持续改进。

（4）服务范围：

内蒙古自治区教育考试院正在使用的所有信息系统及其部署运行环境的供应链安全，定期开展供应链安全检查，实现业务系统和供应商全方位安全治理。供应链安全 险分析供应链产品黑盒技术测试供应商安全能力（供方）评价。

二、服务内容

通过开展供应链安全 险分析、供应链产品黑盒技术测试及供应商安全能力（供方）评价，全面提升供应链安全 险的识别、评估与持续管控能力，实现对

供应链产品　险、供应商安 全能力及整体　险态势的可视化、量化和动态掌控，有效支撑供应链准入管理、　险预警与决策研判，推动形成安全可控、责任清晰、　险可管的供应链安全治理体系。

1.供应链安全　险分析

供应链组件安全　险分析聚焦于相关的供应链信息系统组件资产　险分析，主要包括组件漏洞　险分析、敏感信息泄露及证书　险分析、漏洞安全　险检查修复闭环等技术层面内容。

（1）组件漏洞　险分析

将软件与软件漏洞进行自动关联，分析软件存在哪些已知漏洞，并展示详细漏洞信息，漏洞信息是展现任务中使用的开源软件的漏洞信息，包含漏洞编号、漏洞危险等级、解决方案、漏洞利用难度等信息。

（2）敏感信息及证书　险分析

通过分析二进制软件提取敏感隐私泄露，多维度评估二进制软件安全性。对开源软件的许可协议信息，包括许可协议简称、全称、　险等级、影响开源软件、影响项目等进行分析。

（3）漏洞检测结果分析及修复闭环检查

根据组件应用广泛度、漏洞严重程度、修复工作量选取开源组件，将待修复的组件清单及检测结果交由有关人员进行工作评估和漏洞修复，修复过程中可以根据服务给出的推荐版本或最新版本的修复建议，进行开源组件版本升级。组件升级后，测试人员应对组件影响的功能进行全面的功能和兼容性测试，防止对系统现有功能和兼容性带来影响。功能测试完成后，安全团队可对升级后的应用系统进行开源组件复测和系统漏洞复测，确保应用系统升级同时未引入新的安全漏洞，形成　险修复闭环。

2.供应链产品黑盒技术测试

供应链产品黑盒技术检测针对重点关注的供应链产品，以人工为主，工具为辅的形式，模拟真实的外部攻击者，以攻击者思路，对供应链产品进行全方位的安全评估与测试，发现并验证供应链产品中存在的漏洞和安全　险。

（1）技术测试范围

供应链黑盒技术检测主要覆盖以下技术测试范围：

评估目标系统的暴露面（如系统名称/版本、应用指纹、应用入口、管理入口等），基本特征信息是否可以被远程探测和获取。

评估目标系统是否存在常　Web类漏洞，包括注入、跨站脚本攻击（XSS）、缓冲区溢出、任意文件上传、任意文件下载等。

评估目标系统身份认证和密码的安全性（如用户枚举、默认或可猜解/遍历用户账户、暴力破解、认证模式绕过、CAPTCHA安全性、双因素认证安全性、记住密码和密码重置弱点、注销和浏览器缓存弱点、认证信息是否暴露在url或cookie等）。评估目标系统的认证密码的安全强度是否足够。评估系统身份认证方式是否存在安全漏洞。

评估目标系统的授权机制是否存在漏洞。评估是否存在绕过授权模式、是否存在越权/非授权访问漏洞、是否存在非授权提权漏洞。

评估目标系统的会话安全机制（如是否存在敏感信息泄露、会话篡改、会话劫持、会话重放等）。评估攻击者是否可以假冒受害客户端执行操作。评估攻击者是否可以破坏会话传输的完整性和机密性。

评估目标系统是否存在不安全的直接对象引用。评估目标系统是否每次都验证用户是否有权访问目标对象。评估攻击者是否可以操控这些引用去访问未授权数据。

评估目标系统的安全配置安全性。如应用程序、框架、应用程序服务器、web服务器、数据库服务器和平台的配置是否存在安全漏洞。（如未更改默认账户/密码、未使用的网　、未安装补丁的漏洞、未被保护的文件和目录、未禁用或删除多余的端口/服务/网　/账户/权限等。）

评估攻击者利用错误的安全配置是否可以访问目标系统未授权的数据或功能。 评估目标系统在业务逻辑层面是否存在安全漏洞。评估目标系统历史是否存在通用漏洞，通过技术手段验证当前使用版本是否受漏洞影响。

（2）安全管控与质量管控

黑盒技术检测的测试人员接入公安部 统一的安全管控平台开展，平台全面记录测试人员的流量和行为，对所有操作和行为进行实时审计。一方面确保黑盒测试过程的安全性，保证过程可审计和可溯源；另一方面，通过测试过程数据全面评估黑盒测试的全面性，确保所有功能、所有接口均进行了覆盖各类攻击手法的全方位黑盒技术检测。

（3）漏洞协助整改及修复闭环检查

所有的黑盒测试发现的安全漏洞，需提供相关漏洞的安全修复建议。

3.供应商安全能力（供方）评价

供应商安全能力评价围绕供应链供方在信息系统安全、软硬件安全、管理安全及服务保障能力等方面的综合表现，建立系统化、可量化的安全评估体系，对供应商整体安全能力进行客观评估与分级管理。通过对供应商安全治理体系、技术能力和服务能力的综合分析，识别其在供应链安全中的薄弱环节和潜在 险，为供应链需方、监管方提供科学、可比、可追溯的决策依据，推动供应商持续提升自身安全能力。

（1）信息系统与软硬件安全能力评估

评估供应商在信息系统建设、运行维护及软硬件产品安全方面的能力，包括系统架构安全性、漏洞管理机制、安全加固水平、产品安全设计及更新维护能力等，识别其在技术层面的安全 险。

（2）安全管理与组织保障能力评估

评估供应商在安全管理制度、组织架构、安全职责划分、人员管理及安全培训等方面的建设情况，重点关注安全制度的完整性、执行有效性以及监督问责机制，识别管理层面的合规与 险问题。

（3）安全服务与持续保障能**力**评估

评估供应商在安全服务**支**撑、应急响应、漏洞处置、事件通报及持续运维保障等**方面**的能**力**，分析其在突发安全事件中的响应效率与协同能**力**，判断其对供应链整体稳定性的影响程度。

（4）供应商安全分类分级管理

基于评估结果，对供应商安全能**力**进**行**分类分级管理，明确不同等级供应商在准**入**、合作范围、监管频率等**方面**的管理策略，为供应链　险管控提供分层、精准的治理依据。

三、技术参数

序号	建设名称	指标项	指标要求	数量	单位
1	供应链组件安全险分析	√ 组件漏洞险分析	分析软件存在哪些已知漏洞，并展**示**详细漏洞信息，包含漏洞编号、漏洞危险等级、解决**方**案、漏洞利**用**难度等信息，精确定位应**用**开发中使**用**的开源组件版本，深层分析该开源组件间的依赖关系，可视化呈现开源组件依赖分析流，追踪溯源开源组件漏洞可能的影响范围。	2	次年
		√敏感信息及证书险分析	分析**二**进制软件提取敏感隐私泄漏，多维度评估**二**进制软件安全性，进**行**密钥泄露、MAC 地址泄漏、TOKEN 泄漏、IP 地址泄露、URL 泄露、EMAIL 地址泄露、路径地址泄漏检测。识别开源软件的许可协议信息，包括许可协议简称、全称、　险等级、影响开源软件。		
2	供应链产品**黑**盒技术测试	√ 系统暴露**面**评估	评估系统名称/版本、应**用**指纹、应**用入口**、管理**入口**等基本特征信息是否可以被远程探测和获取。	2	次年
		√ 系统	评估**目**标系统是否存在常　Web 类		

		WEB 漏洞评估	漏洞，包括注**入**、跨站脚本攻击（XSS）、缓冲区溢出、任意**文**件上传、任意**文**件下载等。		
		√ **身**份认证和密码安全性评估	评估**目**标系统**身**份认证和密码的安全性（如**用户**枚举、默认或可猜解/遍历**用户**账**户**、暴**力**破解、认证模式绕过、CAPTCHA 安全性、双因素认证安全性、记住密码和密码重置弱点、注销和浏览器缓存弱点、认证信息是否暴露在 url 或 cookie 等）。评估**目**标系统的认证密码的安全强度是否**足**够。评估系统**身** 份认证**方**式是否存在安全漏洞。		
		√ 授权机制评估	评估是否存在绕过授权模式、是否存在越权/**非**授权访问漏洞、是否存在**非**授权提权漏洞。		
		√ 安全配置安全性评估	估评估应**用**程序、框架、应**用**程序服务器、web 服务器、数据库服务器和平台的配置是否存在安全漏洞。评估攻击者利**用**错误的安全配置是否可以访问**目**标系统未授权的数据或功能。		
		√ 漏洞协助整改及修复闭环检查	针对测试发现的问题提供相关漏洞的安全修复建议，并协助**用户**对相关漏洞进**行**整改，形成 险修复闭环。		
3	供应商安全能**力**（供**方**）评价	√信息系统与软硬件安全能**力**评估	评估供应商在信息系统建设、运**行**维护及软硬件产品安全**方面**的能**力**，包括系统架构安全性、漏洞管理机制、安全加固**水**平、产品安全设计及更新维护能**力**等，识别其在技术层**面**的安全 险。	2	次年
		√信息系统与	评估供应商在安全管理制度、组织架构、安全职责划分、**人**员管理及		

		软硬件安全能力评估	安全培训等方面的建设情况，重点关注安全制度的完整性、执行有效性以及监督问责机制，识别管理层面的合规与 险问题		

四、服务交付

根据内蒙古自治区教育考试院需求，客观、公正、严谨开展分析评估工作，并在服务过程中和服务结束后根据各个服务内容分类，提供包含（但不限于）以下文档：

1.《供应链安全 险分析报告》包含但不限于评估项目概述、评估范围与对象、软件成分分析结果详情、 险组件详情、安全漏洞详情、供应链安全 险分析总结。

2.《供应链产品黑盒技术检测报告》包含但不限于评估项目概述、评估范围与对象、技术检测结果详情、技术检测总结。

3.《供应商安全能力（供方）评价报告》包含但不限于评估项目概述、评估范围与对象、单项评估结果情况、供应商安全能力评估总结。

附件 3 中标通知书

中 标 通 知 书

项目编号：NMGZC-G-F-260085

信元网络技术股份有限公司：

内蒙古自治区教育考试院于2026年04月21日就信息化服务（项目编号：NMGZC-G-F-260085） 进行公开招标采购，现通知贵公司中标，请按规定时限和程序与采购人签订采购合同。

中标合同包号	合同包4
中标合同包名称	供应链安全测评服务
中标金额(元)	320,000.00
合计金额(大写)：叁拾贰万元整	

内蒙古自治区公共资源交易中心

2026年04月21日