新乡市政府采购合同

合同编号：新乡政采竞谈-2023-18

需方：新乡职业技术学院

供方：河南合众信泰科技有限公司

供方持签发的成交通知书，根据采购文件、供方的报价等文件[项目编号：**新乡政采竞谈-2023-18**]，按照《政府采购法》《中华人民共和国民法典》等有关法律法规，供需双方经协商一致，达成以下合同条款：

一、本合同名称：信息系统等保测评及安全运营服务项目服务合同。

二、本合同总价为人民币 789500 元（大写：**柒拾捌万玖仟伍佰元整**）。

三、服务要求及供方对服务条件和期限：

服务条件：提供一名长期驻场运维人员岗位，驻场人员 5*8 小时在岗。驻场运维人员由用户方管理，不临时更换和或长期不在岗，如需更换驻场运维人员，将征得用户同意。

服务期限：提供两年安全运营服务(含驻场服务)。

四、售后服务承诺：

1．售后服务响应时间：提供 7×24 小时畅通的热线联系电话,1 个小时内响应并做出问题初步判定。

2．解决问题时间：一线工程师驻场服务，如不能解决，二线工程师将在 4 小时内到达现场，并立即开始现场不间断工作支持服务，如非硬件问题，承诺在 24 小时内解决故障。

3．售后服务机构名称：河南合众信泰科技有限公司

地址：河南自贸试验区郑州片区（郑东）商务内环路 9 号楼 9 层 0901 号

联系方式：4008299916、18037506307

4．其他服务承诺：无。

五、合同履行地点及进度：

1、供方自本项目采购合同签订之日起 90 日历天完成提交等保测评报告。

2、按需方要求在新乡职业技术学院**使用单位指定地点**完成本项目的服务要求。

六、供方在交付验收时应向需方提供产品操作使用说明。

七、人员培训：供方免费对需方人员进行技术培训，直到需方人员熟练操作或掌握为准。

培训地点：新乡职业技术学院使用单位指定地点；

培训时间： 服务有效期内使用单位指定时间段 ；

培训方式： 讲授法、研讨法、模拟或实操演练等 方式

八、验收要求。

1．供方履约完毕及时向需方提出验收申请。

2．需方在收到供方验收申请后 5 个工作日内组织验收。需方成立 3 人以上验收工作组（合同金额在 50 万以上的验收工作组不少于 5 人），按照采购文件规定、成交供应商响应文件承诺，及国家有关规定认真组织验收工作。大型或者复杂的政府采购项目以及需方认为必要的项目，应当邀请国家认可的质量检测机构参加验收工作。如本项目属国家规定的强制性检测项目，需方必须委托国家认可的专业检测机构验收。

3．验收合格后 10 日内，需方出具《新乡市市直政府采购验收报告》。

九、付款程序、方式及期限：

1．供方在需方付款前开具以需方单位名称为抬头的发票。

2．合同签订完毕后采购人向供货方支付合同总金额的 50%的预付款，在测评结束并验收合格 60 天内支付合同总金额 25%的合同款，2 年服务期满后支付剩余合同总金额 25%的合同款。（注：成交供应商需出具预付款保函）

十、违约责任：

需方无正当理由拒收货物、拒付货款，需方应向供方偿付拒收拒付部分设备款总额 3 %的违约金；供方所提供的服务或货物品种、型号、规格、质量不符合国家规定标准及合同要求的，或者供方不能交付货物或完成系统安装、调试的，供方应向需方支付合同金额总值 3%的违约金，需方有权解除合同，并要求赔偿损失。供方如逾期完成的，每逾期一日供方应向需方支付合同金额的 0.1%违约金。

十一、供需双方应严格遵守采购文件要求，如有违反，按采购文件的规定处理。

十二、因货物的质量问题发生争议，由新乡市法定的质量检测机构进行质量检测或鉴定。

十三、项目采购文件及其修改和澄清及供方响应文件、供方在采购中的有关承诺及声明均为本合同的组成部分。

十四、本合同签订和履行适用中华人民共和国法律，因履行合同发生的争议，由供需双方友好协商解决，如协商不成的，任何一方均可向甲方所在地人民法院提起诉讼。

十五、本合同未尽事宜，供需双方可签订补充协议，与本合同具有同等法律效力，但不能违反采购文件及供方的响应文件所规定的实质性条款。

十六、知识产权：

供方须保障需方在使用该项目或其任何一部分时不受到第三方关于侵犯专利权、商标权或工业设计权的指控。如果任何第三方提出侵权指控，供方须与第三方交涉并承担可能发生的一切费用。如需方因此而遭致损失的，供方应赔偿该损失。

十七、合同生效、备案及其他

1．本合同经双方代表签字并加盖公章后生效。

2．需方应在本合同签订后将采购合同副本报新乡市财政局备案。

3．本合同一式 五 份，供需双方各持 二 份，向新乡市财政局备案 一 份。

需方（公章）：新乡职业技术学院

地址：新乡市经济技术开发区经三路六号

法定代表人或授权委托人（签字）：

电话：0373-3720051

开户银行：

账号：

供方（公章）：河南[illegible]信泰科技有限公司

地址：河南自贸试验区郑州片区（郑东）商务内环路 9 号楼 9 层 [illegible] 号

法定代表人或授权委托人（签字）：

电话：0371-65616616

开户银行：中国农业银行股份有限公司郑州商务外环路分理处

账号：16048201040004028

签约时间： 2023 年 09 月 07 日

签约地址：新乡市

后附服务内容及分项报价表

服务内容及分项报价表

序号	招标项目	服务内容	技术要求	单位	数量	单价（万元）	小计（万元）
1	等级保护测评	等级保护备案工作	由我公司完成《信息系统安全等级保护备案表》等材料的整理和当地公安部门的报备工作,并协助取得定级系统的备案证明。	个	4	4	16
		测评依据	按照信息安全等级的测评标准（等保 2.0）进行二级安全等级测评。				
		测评内容	本项目按照信息安全等级保护测评标准对 4 个信息系统进行安全等级测评。测评内容主要包括两个方面：一是单元测评，测评指标与《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）相应等级的基本要求完全一致；二是系统整体测评，主要测评分析信息系统的整体安全性。 单元测评包括安全技术测评和安全管理测评两大部分，其中安全技术测评层面主要包含：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心。安全管理测评层面主要包含：安全管理制度、安全管理人员、安全管理机构、安全建设管理、安全运维管理。 整体测评在单元测评的基础上进行进一步测评分析，在内容上主要包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。 系统整体测评涉及信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关，内容复杂且充满系统个性。因此，全面地给出系统整体测评要求的完整内容、具体实施方法和明确的结果判定方法是很困难的。测评人员应根据特定信息系统的具体情况，结合本标准要求，确定系统整体测评的具体内容，在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，测评安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性等。				
		测评服务	在安全等级测评过程中，每个工作阶段、流程、内容及成果交付严格遵循《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）和《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）文件，根据本项目信息系统已完				

序号	招标项目	服务内容	技术要求	单位	数量	单价（万元）	小计（万元）
			成的定级备案安全等级，开展相应级别的安全等级测评工作，根据测评结果出具相应的单项和整体测评报告，测评报告需得到学校的确认，并协助学校报备案地网监部门备案。测评报告编制的内容及格式严格遵照《网络安全等级保护等级测评报告模板》（2021 版）进行。				
		交付成果	1、项目各阶段的测评过程文档，参照《信息安全技术信息系统安全等级保护测评过程指南》编制。 2、系统等级测评报告。				
		项目工期	合同签订后 90 日历天内提交等保测评报告。				
		其他	所有过程数据提供电子版，所有报告提供纸质和电子版各一份。				
2	驻场运维服务	服务内容	1、提供数据中心资产的安全运维服务，持续性开展网络安全运维保障工作，构建安全资产治理、安全威胁监测、安全事件响应、安全闭环处置的安全运营体系； 2、我公司将结合安全工具发现的资产信息，按照学校格式要求，结合实际情况，对服务范围内资产的进行全面梳理。梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP 地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑等，并将信息同步交付给校方进行存档管理；当资产发生变更时，运维工程师需对变更信息进行持续跟踪、信息确认与记录更新； 3、我公司将协助制定并维护一个安全的资产静态基准，创建符合等级保护要求的信息系统安全基线，并将其落实为有效的系统黄金镜像库、安全软件版本库，安全系统配置库等切实可行的输出。提供其他同类院校 2 项的相关案例截图。 4、我公司将协助制定有效的漏洞和补丁管理计划。定期对资产安全状态进行检查，对发现的脆弱点依据漏洞和补丁管理流程，经过严格的控制流程和测试流程，进行补丁的安装和修复工作。 5、我公司将协助制定有效的变更管理计划，针对合理的资产配置变更需求，进行深度分析、测试、验证。根据变更管理计划，发起变更流程，更新安全配置基线，	年	2	18	36

序号	招标项目	服务内容	技术要求	单位	数量	单价 (万元)	小计 （万元）
			持续优化和维护资产的静态安全性。 6、我公司提供主动的威胁监测和处置服务。基于威胁监测和分析平台，持续监测和分析网络流量，对网络中存在的攻击行为、漏洞利用情况，对监测发现的安全漏洞进行分析验证，同时持续跟踪整改情况，结合威胁情报信息，提供威胁持续监测和安全处置服务；针对每一类威胁，进行深度分析和攻击成功与否验证。分析判断攻击威胁程度和影响范围，排查是否存在其他可疑主机、是否对核心资产造成威胁，协助对资产进行安全加固； 7、我公司将协助建立规范的安全事件响应规范，根据规范，结合网络安全场景，制定行之有效的安全事件响应流程和操作脚本手册。基于威胁监测和态势感知平台对各类安全数据及日志数据进行关联分析与深入挖掘，及时发现各类安全事件并通知客户，同时协助客户开展通报、处置等响应动作，协助快速恢复业务，消除或减轻影响； 8、我公司提供稳定和专业的后台支撑团队，结合现场运维团队，通过管理制度和流程完善、操作系统补丁修复、应用组件配置加固、安全设备策略调整、完善审计跟踪配置方式对安全运维工作中的管理和技术问题进行持续跟踪和处置； 9、为提高运维效率和应急响应速度，保障学校在远程接入/移动接入学校网络的安全性，发挥现有虚拟专网设备的作用，已提供深信服厂商服务承诺函，确保学校现有 VPN 设备的扩容，确保支持 50 个深信服 VPN 并发连接远程接入授权，提供为期一年的软件升级和硬件原厂质保服务，以确保 VPN 设备的正常运行；提供包含软件版本更新和访问控制策略调整在内的人工服务，以确保安全运维工作能够顺利进行。确保其真实性和有效性，承诺函加盖软件服务商公章。				
		服务范围	1、基础设施：虚拟化运维服务：虚拟化基础设施、私有云组件运维、技术支持、记录数据； 2、操作系统运维服务：操作系统安装、配置、加固、故障排除、记录数据； 3、日常运维工作：日常问题及突发事件的及时响应反馈并解决跟进故障处理； 4、机房硬件运维服务：中心机房硬件设备健康巡检、故障排除、设备保修、记录				

序号	招标项目	服务内容	技术要求	单位	数量	单价 (万元)	小计 （万元）
			数据； 5、网络和安全运维服务：网络和安全设备运维管理，策略调整、配置优化、记录数据； 其他 a.配合学校及校园网管理部门为学校的各种活动及建设提供咨询建议和技术支持； b.结合校园网的发展建设提供新增设备与原有设备的集成与互联互通提供咨询建议和技术支持； c.在服务过程中接受学校及校园网管理部门的管理，并在服务过程中和过程后提供各种相应服务文档； d.在校园网管理部门的安排下对学校网络运行的各种工作进行劳务支持。				
		服务方式	派驻 HCIP 级别工程师一名驻场服务，同步用户作息时间，为全部校园网相关设备提供为期两年的运行监控、告警、故障处置、设备设施的日常维护服务、互联互通及相关技术劳务服务等。 提供一个稳定的二线服务团队支持服务，按需协助驻场工程师完成疑难问题定位、排查、处置。				
		响应时间	基本时间响应： 我公司将提供服务期内每周 5 天*8 小时一名工程师驻场服务，每个工作日 24 小时的全天候随时响应服务。我公司将提供 7×24 小时畅通的热线联系电话。响应时间指采购人发现问题，通知到我公司，或我公司在巡检当中发现问题时开始计算，我公司将在 1 小时内完成以下内容的初步判定：问题级别、影响范围、解决所需资源、解决时长，并尽快完成故障排查和故障处理。如果需要协助更换备件或者驻场工程师无法进行故障处理时，采购人有权要求我公司的二线工程师现场处理时，我公司将协助采购人完成相关工作及人员的调配安排。 二线工程师到达现场时间： 当采购人要求我公司提供二线工程师现场支持服务时，我公司从接到采购人电话请求开始，我公司的工程师在 4 小时内到达现场，并立即开始现场不间断工作支持				

序号	招标项目	服务内容	技术要求	单位	数量	单价 (万元)	小计 （万元）
			服务，如非硬件问题，承诺在 24 小时内解决故障。 现场不间断工作支持服务： 在用户校园网设备、设施及相关业务及应用系统发生故障、重大事件、关键时点或重大活动及紧急工作等情况下，我公司将派相应级别且能解决问题的二线工程师到达用户现场，按用户要求，立即开始不间断服务，直至系统能够满足采购人业务及工作正常进行的要求。				
		服务人员	驻场工程师资质： 驻场工程师具有计算机相关专业本科毕业，有两年以上工作经验。熟悉网络设备、安全设备、机架及线缆等系统集成相关设备的操作及维护等运维管理操作；熟悉服务器、存储、虚拟化、数据库等运维管理操作； 二线服务项目的人员： 1、我公司服务人员具有路由交换方向（IE）工程师证书； 2、我公司服务人员具有服务器与存储方向（IE）工程师认证证书； 3、我公司服务人员具有安全方向（IE）工程师证书； 4、我公司服务人员具有虚拟化工程师虚拟化认证工程师（VCP）证书； 5、我公司服务人员具有数据中心工程师数据库方向认证（OCM 证书）； 6、我公司服务人员具有信息安全工程师信息安全保障人员证书； 7、已提供以上人员近一年连续三个月的加盖公章个人社保证明材料；				
		工作管理	驻场工程师人数及上岗： 提供一名长期驻场运维人员岗位，驻场人员 5*8 小时在岗。驻场运维人员由用户方管理，不得临时更换和或长期不在岗，如需更换驻场运维人员，将征得用户同意。 对供应商所提供服务的管理： 我公司所提供的各种服务及派驻的工程技术人员严格遵守学校与网络管理部门的各项管理及规章制度。我公司所提供的各种服务及派驻人员接受网络管理部门的直接管理，配合网络管理部门的各项工作。由网络管理部门对相关服务及驻场人员进行考核、监督及评价。我公司派驻人员将服从管理。				

序号	招标项目	服务内容	技术要求	单位	数量	单价 (万元)	小计 （万元）
			日常设备设施巡检及维护： 提前做好设备巡检等日常维护措施，由驻场专责工程师每天到现场对所有设备进行巡检，检查系统的物理运行环境及运行状态和系统日志，并向网络管理部门汇报巡检情况。 校园网业务或设备设施出现故障后的紧急处理： 解决网络设备设施和基础环境设施运行过程产生的问题，保障各项系统正常运行。根据故障现象对设备进行故障分析定位、测试、诊断，并制定业务恢复和故障解决技术方案,我公司保证优先实施业务恢复，在恢复业务的前提下，再进行彻底的故障修复。技术方案经用户网络管理部门批准后，由我公司的技术人员具体实施方案；或在用户主管人员允许的情况下，由我公司的技术人员进行具体实施。如果硬件设备出现故障时，排除故障；若是保修期内，协助我公司和生产厂家解决问题，保修期外协助用户协调备件，费用由用户承担。我公司将提供书面故障处理日志、软硬件及设备配置变动日志和故障分析报告。 协助用户进行系统升级、扩充和优化服务： 根据用户系统的运行使用情况，我公司及时向用户提出系统安全及系统优化的合理建议，确保用户系统安全正常运行。当用户的各项系统或设备出现与其它系统或设备或第三方厂家系统或产品需要协调的问题时，我公司将根据网络管理部门要求派工程师到现场协助协调、解决问题或提出合理化建议。我公司根据网络管理部门的应用要求，重新配置、优化系统资源，包括网络、服务器、存储、安全设备等设备设施的资源调配和调整，操作系统的安装、配置和升级，基础数据库软件的升级等。 文档管理 和信息支持服务： 我公司将每日、每周及每月对巡检及日常运维中的问题及各种记录、日志进行分析和总结，同时以日报、周报和月报的形式将结果反馈给采购人。建立专门的系统维护档案及日志，我公司的工程师第一次到现场服务巡检时，将核对并记录所负责维护的设备详细配置清单、所使用的操作系统、版本号、系统的使用情况及系统的配置参数。建立和完善主机系统的技术档案，同时对用户系统提供相应的技术支持的				

序号	招标项目	服务内容	技术要求	单位	数量	单价 (万元)	小计 （万元）
			电子文档。我公司对用户的所有保修设备，均根据每次的电话记录、预防性维修报告和故障维修报告建立技术文档，详细记录设备型号、故障时间、故障类型、所有日志内容包括但不限于校园网设备巡检日志、软硬件及设备配置变动日志、设备维护日志、网络故障处理日志、网络故障受理记录、5*8 小时值班日志、网络运行情况分析及汇总报告、周报及月报等。 保密服务承诺： 服务期内，我公司将签订保密协议，承诺严格保护用户系统、数据、信息的安全，在服务期满后永久不得泄露用户所有信息。由于我公司违反保密协议而导致的泄密或破坏，由我公司负全责，并由我公司赔偿用户所有损失。我公司提供服务期内保护用户系统、数据、信息的安全，以及服务期满后永久保守用户信息秘密的承诺书。 监督与投诉受理： 用户可对我公司所提供服务质量及驻场人员工作表现进行监督，结合故障处理的用户回访满意率做出综合评价。如因我公司的服务质量对用户造成重大影响，用户根据我公司的服务考核表现有权利要求我公司撤换驻场工程师或改善服务质量，直至要求终止服务合同，并提供相应赔偿，我公司将向用户支付合同总额 10%的赔偿金。除正常的技术支持热线以外，我公司另设立客户投诉渠道受理用户对我公司服务的投诉。我公司保证从受理用户投诉到向用户初次回复处理意见的时间不超过 8 小时。我公司对投诉的处理以投诉问题得到解决和用户满意为结束，时间不超过 15 个自然日。违反保密规定、泄露系统信息、影响数据安全的，用户有权终止合同，并对于构成犯罪的依法追究当事人相关责任，同时，我公司向用户支付合同总额 20%的违约金。 培训服务： 针对本项目建立技术交流、培训机制，根据用户要求提供四次，每次 1 人以上的本地或异地培训。培训内容理论兼顾实际操作，培训内容包括日常管理、紧急故障处理办法、相关新技术的介绍及软硬件基础知识等，培训知识点包括但不限于现有各项设备设施。				

序号	招标项目	服务内容	技术要求	单位	数量	单价（万元）	小计（万元）
			培训能达到用户独立进行运维管理，能独立应对、处理各种紧急故障，熟练掌握校园网及机房内的运维安全设备操作。				
		运维效果	1.系统运行稳定、可靠：通过对系统的合理规划和日常维护，保障校园网设备及系统和主要业务能够稳定、可靠地运转。 2.灾难性崩溃的快速响应与恢复：当系统遇到灾难性崩溃时候，我公司将快速响应与对系统进行恢复，我公司的二线工程师将在 8 小时内赶赴现场，并在尽可能短的时间里对系统灾难进行恢复。 3.投资保护：保障用户的系统投资能够得到最大限度的回报。在保障系统正常运行的基础上，对用户业务系统提供合理化建议及优化方案，使得用户运维设备和系统在现有硬件环境下发挥最优性能。 4.我公司具备 ITSS 信息技术服务标准符合性证书（二级）认证证书。				
3	安全运营服务	安全评估	1、风险评估：针对业务系统的弱点进行评估。包含应用系统、操作系统、业务系统部署位置、安全域划分、安全设备防护等等评估内容。 在测试过程中将对可能发现的安全隐患给予说明，同时给出该隐患的解决建议。服务完毕后，出具《网络安全风险评估报告》，报告内容包含以上所有项目。服务频率 2 次/年 2、运维管理评估：对核心资产的密码、日志、版本信息、安全策略等进行检测，发现风险点并给出解决建议。 3、新系统上线前安全评估：本服务对新上线的系统，进行上线前的安全配置核查及风险评估，新系统评估通过后，才可以正式上线进行系统接入，正式上线运营。完成评估后，出具《业务上线评估报告》，频率：1 份/次 4、威胁分析：通过对网络流量进行过滤分析，及时发现危险行为和攻击目标、攻击方式，对重点目标进行风险判断，给出针对性防护建议并协助用户处理。 5、主机安全检查：检测重点主机是否存在木马、后门等恶意程序，分析日志信息，查看是否存在入侵痕迹。 6、人工验证：对所有漏洞信息、威胁信息都要进行人工验证，保证不出现误报，	次	4	5.7375	22.95

序号	招标项目	服务内容	技术要求	单位	数量	单价（万元）	小计（万元）
			验证完毕后，出具《系统整改建议书》，对所有检测过程发现的安全风险提出解决建议，并协助整改。				
		安全加固	1、补丁加固：对评估过程中发现的系统补丁漏洞进行加固（有条件的情况下会进行测试），此过程将与用户进行充分沟通 2、配置参数加固：对评估过程中发现的配置类问题进行加固，如权限设置、策略配置、参数设置等。 3、安全管理加固：对评估过程中发现的组织、人员、安全域规划等方面的安全风险提出解决建议。 4、整改完毕后，出具《整改加固报告》，对所有整改项目作详细说明。				
		安全监测	7*24 小时实时监测互联网可达的学校门户网站，及时发现网站的运行状态、中高危漏洞、暗链、挂马、违规关键字等，经过人工验证后第一时间通知用户整改。如招标方需要，可通知安全加固团队介入协助。每个月出具一份《月度网站监测报告》。 我公司具有信息安全风险评估服务资质二级认证证书。				
		应急响应	1、安全应急：当招标方发生安全事件，如网络拥塞、中病毒、网站被入侵，服务团队会第一时间响应，协助用户解决问题、查找原因、给出加固建议并协助用户进行加固。 2、技术支持：当上级机关对用户进行安全检查时，或当招标方收到上级或公安机关通报后，提供技术支持，协助整改。 3、每次应急响应结束后，出具《应急响应报告》。				
		重保支持	1、在国家或行业重要会议、活动期间，网络安全保障技术支持，包含重保前的摸底加固、重保中的监测响应、重保后的总结改进。 提供 20 人天的 7*24 小时技术支持，含漏洞发现、安全加固、威胁发现、应急处置等； 2、我公司具有信息系统安全运维服务资质二级认证证书； 3、我公司具有信息系统安全集成服务资质二级认证证书；				
		服务人员	我公司提供两人的 CISP 认证人员（成员具备 3 年以上安全服务工作经验，组长				

序号	招标项目	服务内容	技术要求	单位	数量	单价 (万元)	小计 （万元）
			具备 5 年以上安全服务工作经验）； 2、安全服务团队成员有一位持有 CISSP 认证工程师证书；				
		服务期限	提供两年安全运营服务。				
4	安全培训与咨询服务	安全技术培训	面向技术人员，介绍常见网络攻击类型、安全日志分析方法、安全软件的使用、应急响应和处置思路、网络安全事件响应案例讲解。	年	2	2	4
		安全意识培训	包含从网络上存在的安全风险到企业和个人如何防范风险，及介绍常用的安全技巧注意事项，来降低威胁。				
		等保咨询	1.安全建设现状调查和摸底，提供信息安全建设规划和蓝图设计，等保政策解读：等保政策、行业安全政策解读，信息安全实践方法建议。 2.我公司具有 ISO20000 信息技术服务管理体系认证证书； 3.我公司具有 ISO27001 信息安全管理体系认证证书。				
合计				78.95 万元			