项目编号/包号：常采竞磋[2022]0068号—分包2

政府采购合同

（服务类）

项目名称：常州市政府采购智能开评标系统安全风险评估项目

甲方：常州市政府采购中心

乙方：江苏瑞新信息技术股份有限公司

签订地：江苏常州

签订日期：2022 年 8 月 日

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规之规定及常州市政府采购中心采购编号为常采竞磋[2022]0068号采购文件及投标（响应）文件，按照平等、自愿、公平和诚实信用的原则，经甲乙双方协商一致，约定以下合同条款，以兹共同遵守、全面履行。

一、合同组成部分

下列文件为本合同的有效组成部分，对甲乙双方均具有法律约束力。如果下列文件内容出现不一致的情形，那么在保证按照采购文件确定事项的前提下，组成本合同的多个文件的优先适用顺序如下：

1.1 本合同及其补充合同、变更协议；

1.2 中标通知书；

1.3 投标文件（含澄清或者说明文件）；

1.4 招标文件（含澄清或者修改文件）；

1.5 其他相关采购文件。

二、服务

服务名称：常州市政府采购智能开评标系统安全风险评估项目；

三、 价款

本合同总价为：￥29500 元（大写：贰万玖仟伍佰元人民币）。

分项价格：

序号	分项名称	分项价格
1	资产收集服务	5000
2	脆弱性识别服务	5000
3	渗透测试服务	10000
4	风险评估报告分析编写服务	5000
5	系统整改后复测服务	4500
总价（含 6%税）		29500 元整

四、结算方式

本合同总金额为人民币：贰万玖仟伍佰元整（¥29500.00 元）；

按照以下约定执行：合同签订后，甲方向乙方支付合同总价的 50%，即人民币：壹万肆仟柒佰伍拾元整（¥：14750.00 元）；

项目提交评估报告整改完成并验收通过后，甲方向乙方支付合同尾款，即人民币：壹万肆仟柒佰伍拾元整（¥：14750.00元）；

甲方支付乙方每笔款项的另一前提是收到乙方开具的正式发票。

五、实施时间

合同服务期限：2022年8月31日-2023年9月1日，常州市政府采购中心智能开评标系统建设项目完成终验之前，若遇到突发安全应急事件，工程师必须在1个小时之内到达现场，3个小时内应提供解决方案。7*24小时内，须有技术人员能联系上并随时提供响应服务。

六、双方责任及权利

6.1 甲方责任

（1）提供信息安全评估范围内的必要信息，包括系统配置、网络配置等。

（2）提供乙方服务人员在甲方服务或者待命的临时办公场所和必要的条件。

6.2 乙方责任

（1）乙方服务人员按照甲方要求提供及时的现场服务，服务内容按附件2执行。

（2）向甲方签署保密承诺（附件1），遵守甲方的工作纪律。

（3）乙方在人员更换时需要提前2日报备到甲方，经甲方考察同意后，工作交接。

七、权利与义务

7.1服务公司在响应方式上如有违反，甲方有权采取惩罚措施：

7.2应急响应超过规定时间，一次可扣除合同金额1%作为处罚。

7.3因乙方维护不当或工作失职，导致网站及信息系统中断超过24小时，甲方有权解除劳动合同。

7.4甲方有义务配合乙方做好系统维护工作，及时通知甲方配置变更，安全策略变更等情况。

7.5甲方有义务配备必要的软件、硬件设施，满足系统可靠、稳定运行的要求

7.6甲方自行变更设置及其它原因引起的故障，乙方不承担责任。

八、违约责任

8.1本合同生效后，甲乙双方应履行本合同约定的义务，任何一方不履行或

者不完全履行本合同约定的义务和保证的，应当承担相应的违约责任，并赔偿因此给对方造成的损失。

8.2 乙方未按本合同约定的时间履行安全服务等本合同项下义务的，每延迟一天，应按照合同价款的万分之二向甲方支付违约金，但违约金总额不得超过价款总额的 10 %。

8.3 由于甲方原因延迟付款，每延迟一天应按未付相应金额的万分之二向乙方支付违约金，但违约金总金额不超过未付相应金额的 10%。若因财政拨付周期或支付进度等问题导致支付逾期付款，甲方不承担违约责任。

8.4 乙方不履行或履行义务不符合本合同约定，甲方依本合同约定解除合同的，乙方应按合同总额的 10 %向甲方支付违约金。

8.5 乙方若因服务的质量问题或违反本合同的其它约定，给甲方造成了损害，乙方应承担赔偿责任。

九、知识产权归属

9.1 甲方有权在履行本协议时及在其自身营运过程中永久地自由使用，以使用为目的复制、修改、变动本技术成果，不需乙方同意或向乙方支付任何费用。

9.2 本合同提及的所有权利仅限于因执行本合同而产生的并由双方所确认的技术成果，并且不得解释为一方授权另一方使用自身所持有的或所使用的任何专利、商标、专有技术、商业秘密等知识产权。

十、合同争议的解决

本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；不愿和解、调解或者和解、调解不成的，应当选择下列第 2 种方式解决：

10.1 将争议提交 常州 仲裁委员会依申请仲裁时其现行有效的仲裁规则裁决；

10.2 向 甲方所在地有管辖权的 人民法院起诉解决。

十一、 其他约定事项

其他未尽事宜参照相关法律，双方协商解决

本合同经双方盖章签字后生效，如有变动，必须经双方协商一致后，方可更改，本合同一式肆份，双方各持贰份。

附件 1:《保密协议》

附件 2:《评估内容说明书》

（此页无正文）

甲方：常州市政府采购中心（盖章）

法人代表或委托代理人：

电话：

日期：2022.9.1

乙方：江苏瑞新信息技术股份有限公司（盖章）

法人代表或委托代理人：

电话：15851967178

日期：2022.9.1

开户行：江南农村商业银行常州市三井支行

账号：8923 2041 1030 1201 0000 63073

附件 1：常州市政府采购智能开评标系统安全风险评估项目保密协议

保 密 协 议

甲方：常州市政府采购中心

乙方：江苏瑞新信息技术股份有限公司

为加强常州市政府采购中心“常州市政府采购智能开评标系统安全风险评估项目”安全风险评估的信息技术资料和数据的保密管理，双方根据国家有关法律、法规，本着平等、自愿、协商一致、诚实信用的原则，就乙方为甲方提供安全技术支持服务（下称项目）等工作中的保密事宜达成如下协议：

一、 保密信息

（一）在项目中所涉及的项目设计、图片、开发工具、流程图、工程设计图、计算机程序、数据、专利技术、招标文件等内容。

（二）甲方在合同项目实施中为乙方及乙方工作人员提供必要的数据、程序、用户名、口令和资料等；

（三）甲方应用软件在方案调研、开发阶段中涉及的业务及技术文档，包括税收政策、方案设计细节、程序文件、数据结构，以及相关业务系统的硬软件、文档、测试和测试产生的数据等；

（四）其他甲方合理认为，并告之乙方属于保密的内容。

二、保密范围

（一）甲方已有的技术秘密；

（二）甲方敏感信息和知识产权信息；

（三）乙方持有的科研成果和技术秘密，经双方协商，乙方同意被甲方使用的；

三、保密条款

（一）乙方应严格保守甲方的有关保密信息，不得以其他任何手段谋取私利，损害甲方的利益。

（二）未经甲方书面许可，乙方不得以任何名义向有关单位或个人泄漏甲方保密信息。

（三）未经甲方书面许可，乙方不得对有关保密信息进行修改、补充、复制。

（四）未经甲方书面许可，不得将保密信息以任何方式（如 E-mail）携带

出甲方场所。

四、保密信息的所有权

以上所提及的保密信息均为甲方所有。

五、保密期限

（一）本协议的保密期限为5年。

（二）在本协议失效后，如果本协议中包括的某些保密信息并未失去保密性的，本协议仍对这些未失去保密性的信息发生效力，约束双方的行为。

（三）本协议是为防止甲方的保密信息在协议有效期发生泄漏而制定。因任何理由而导致甲、乙双方的合作项目终止时，乙方应归还甲方所有有关信息资料和文件，但并不免除乙方的保密义务。

六、关系限制

本协议不作为双方建立任何合作关系或其他业务关系的依据。

七、违约责任

乙方未遵守本协议的约定泄露或使用了保密信息甲方有权终止双方的合作项目，乙方应按合作项目金额作为违约金支付甲方，并按照有管辖权的人民法院认定的赔偿金额赔偿甲方遭到的其他损失，甲方有权进一步追究其一切相关法律责任。

八、其他事项

（一）本协议以中文做成，一式肆份，由甲、乙方各执贰份，各份协议具有同等法律效力。

（二）本协议未尽事宜，由甲乙双方协商解决。

（三）本协议自甲、乙双方签字之日起生效。

甲方：（章）常州市政府采购中心

经办人（签字）：

乙方：（章）江苏瑞新信息技术股份有限公司

经办人(签字)：

附件 2：评估内容说明书

一、项目目标

为准确识别信息安全各种风险和威胁，规避或减少信息安全事件造成的不良影响和损失，常州市政府采购中心拟采购信息安全风险评估服务，评估常州市政府采购中心智能开评标系统建设项目。

1.根据信息安全风险级别，运用科学方法和手段，系统地分析网络和信息系统所面临的威胁及其脆弱性，评估安全事件一旦发生可能造成的危害程度，提出针对性的信息安全解决方案和加固建议，为网络、软硬件系统的安全与稳定运行提供有力的保障。

2.通过专业的安全服务和管理，及时协助信息安全管理人员发现和处理服务范围内的设备及系统安全事故，提供有针对性的安全咨询及安全规划方案，最大限度保障网络和信息安全。

二、项目实施原则

1.保密原则

在运维过程中，需严格遵循保密原则，采购人与成交人签订保密协议，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害用户利益。

2.互动原则

在整个运维过程中，强调用户的互动参与，每个阶段都能够及时根据用户的要求和实际情况对评估的内容、方式做出相关调整，进而更好的进行项目服务工作。

3.最小影响原则

工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应做出说明。

4.规范性原则

本项目的安全评估服务的实施必须由专业人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的运维报告。

5.质量保障原则

在整个项目服务过程中，将特别重视项目质量管理。项目的实施将严格按照项目实施方案和流程进行，并由项目协调小组从中监督，控制项目的进度和质量。

三、测评技术要求

按照《GB/T 20984-2007》风险评估要求，对常州市政府采购中心智能开评标系统建设项目系统上承载的数据、业务和应用等进行安全评估，明确信息系统存在的问题和不足，主要包括：

1、差距分析

通过、调查问卷、人员访谈、文档查看、现场勘查、人工检查、记录分析、技术测试、渗透测试等方式进行安全技术和安全管理方面的评估，判断安全技术和安全管理的各个方面，给出差距分析结果，提出信息系统的安全保护需求。

2、风险评估

对常州市政府采购中心智能开评标系统建设项目的重要资产进行风险评估，分析并确定不能接受的安全风险，然后确定额外安全措施并判断对超出等级保护基本要求部分实施额外安全措施的必要性，提出信息系统的额外安全保护需求。

四、技术标准

1.《信息安全风险评估规范》（GB/T 20984-2007）

2.《信息安全风险管理指南》（GB/Z 24364-2009）

3.《信息系统安全等级保护基本要求》（GB/T 22239-2008）

4.《信息安全管理实用规则》（GB/T 22081-2008）

5.《信息系统安全管理要求》（GB/T 20269-2006）

6.《信息安全事件分类分级指南》（GB/Z 20986-2007）

7.《信息安全事件管理指南》（GB/Z 20985-2007）

8.《信息系统灾难恢复规范》（GB/T 20988-2007）

9.《信息安全应急响应计划规范》（GB/T 24363-2009）

五、安全评估内容

本次安全评估内容遵循国家信息安全相关标准及技术规范要求，从物理环境、网络平台、主机层、应用系统等方面，对常州市政府采购中心智能开评标系统建设项目进行信息安全风险评估，出具安全风险评估报告，明确系统存在

的安全隐患、提出整改建议，并在完成安全整改后进行系统复查，出具整改确认报告。

具体内容分类为：物理安全、网络安全、主机安全、应用安全、数据安全、管理安全。

1.物理安全

物理安全主要涉及的方面包括环境安全（防火、防水、防雷击等）设备和介质的防盗窃防破坏等方面。具体包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

2.网络安全

网络安全主要关注的方面包括：网络结构、网络边界以及网络设备自身安全等，具体的评估点包括：结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护。

3.主机安全

主机系统安全涉及的评估点包括：身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、入侵防范、恶意代码防范和资源控制。

4.应用安全

应用系统安全的评估点包括：身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制、代码安全。

5.数据安全

明确需要保护的数据，评估点包括：数据的保密性、完整性、备份和恢复措施的有效性。

6.管理安全

协助整理各类安全管理制度、安全管理台账。

六、安全评估过程

1.资产边界分析

（1）分析待评估资产范围。

（2）划分内部资产子系统。

（3）对各子系统进行边界确认。

（4）确定最终资产子系统边界。

2.资产识别

（1）根据资产表格进行资产审计。

（2）分组对本地、非本地区域资产进行有效录入登记。

（3）每类资产明细需要审计资产详细配置与当前状态。

3.威胁识别

（1）从物理准入控制、机房温湿度控制、机房防尘、机房电源、接地、机房屏蔽、以及防雷、防火、防盗等多个方面进行物理威胁识别。

（2）从网络拓扑、地址分配、VLAN 划分、路由协议、准入控制、访问控制等多个方面进行网络威胁识别。

（3）从系统来源、系统补丁、账号安全、密码安全、审计安全、服务安全、恶意代码防护等多方面进行系统威胁识别。

（4）从应用服务平台、数据库安全、中间件安全、代码安全、数据安全、账号安全、密码安全、审计安全等多个方面进行应用威胁识别。

（5）从组织架构、人员安全、管理规定、合规性、应用连续性要求等多个方面进行管理威胁识别。

4.脆弱性识别

（1）从物理准入控制、机房温湿度控制、机房防尘、机房电源、接地、机房屏蔽、以及防雷、防火、防盗等多个方面进行物理脆弱性识别。

（2）从系统来源、系统补丁、账号安全、密码安全、审计安全、服务安全、恶意代码防护、日常运维等多方面进行系统脆弱性识别。

（3）从网络拓扑、地址分配、VLAN 划分、路由协议、准入控制、访问控制、日常运维等多个方面进行网络脆弱性识别。

（4）从应用服务平台、数据库安全、中间件安全、代码安全、账号安全、密码安全、审计安全、日常运维等多个方面进行应用脆弱性。

（5）从数据备份及恢复、应急响应、灾备与冗余等多方面进行数据脆弱性识别。

5.已有安全措施登记

（1）识别已有操作系统安全策略。

（2）识别已有应用系统安全策略。

（3）识别已有网络系统安全策略。

（4）识别已有安防系统安全策略。

（5）识别已有机房系统安全策略。

6.风险分析

（1）根据收集的用户数据进行分析，评估要素关系映射。

（2）根据评估要素关系进行风险值计算。

（3）形成风险评估报告。

（4）针对风险评估报告的解决方案。

7.应用系统渗透性测试

在常州市政府采购中心的授权下，对常州市政府采购中心智能开评标系统建设项目进行渗透测试，并提供相关渗透测试报告。

七、提交成果

1.《常州市政府采购中心智能开评标系统建设项目信息安全弱点评估报告》

2.《常州市政府采购中心智能开评标系统建设项目信息安全风险评估报告》

3.《常州市政府采购中心智能开评标系统建设项目信息安全风险评估复测报告》