合同编号：JSRX-20200911-01

招标编号：常采竞磋[2020]0129 号

政务体系建设及证照分离项目风险评估和软件项目三级等保合同（分包 1）

甲　　方：常州市政务服务管理办公室

乙　　方：江苏瑞新信息技术股份有限公司

集中采购机构：常州市政府采购中心

合同编号：常采竞磋[2020]0129 号

签订地点：常州市锦绣路 2 号 1-1 座

签订时间：　2020 年 9 月 11 日

根据常州市政府采购中心的常采竞磋[2020]0129 号招标文件，甲、乙方就乙方中标的“政务体系建设及证照分离项目风险评估和软件项目三级等保合同（分包 1）”项目，本着平等互利的原则，通过共同协商，参照《合同法》、《政府采购法》及有关法律法规，就相关事宜达成如下合同。

一、总则

乙方按甲方要求，为甲方提供“政务体系建设及证照分离项目”信息安全风险评估服务（以下称系统）。服务内容见下表（单位：元）：

序号	项目名称	内容说明	单价	金额	备注
1	“政务体系建设及证照分离项目风险评估和软件项目三级等保合同（分包 1）”项目	“政务体系建设及证照分离风险评估项目”（详细见附件一）	269000	269000	
2	合计：人民币贰拾陆万玖仟元整（￥269000.00 元）				

服务具体要求见集中采购机构的招标文件中项目需求。

二、合同文件

下列文件是构成合同不可分割的部分，并与本合同具有同等法律效力。

1、常采竞磋[2020]0129 号招标文件。

2、乙方提交的投标书。

3、乙方投标书的其他资料及承诺。

三、质量保证

乙方所提供服务须符合国家有关标准和常采竞磋[2020]0129 号采购招标文件（含技术说明）和投标文件的要求。

四、服务期限

合同服务期限：2020 年 9 月 15 日-项目验收完成

五、付款方式

本合同总金额为人民币贰拾陆万玖仟元整（￥269000.00 元）。

按照以下约定执行：签订合同后 10 个工作日内甲方支付乙方合同金额的 70%，即人民币：壹拾捌万捌仟叁佰元整（¥：188300.00 元），余款在项目验收合格后 10 个工作日内支付，即人民币：捌万柒佰元整（¥：80700.00 元）。

六、双方责任与权力

1、甲方责任

（1）提供外包服务范围内的必要信息，包括终端配置、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。

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，服务内容按附件一执行。

（2）与甲方签订保密协议（附件二），遵守甲方的工作纪律。

（3）乙方在人员更换时需要提前 1 个礼拜前报备甲方，经甲方考察同意后，工作交接。

七、违约及赔偿责任

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。

2、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。

3、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。

八、 合同解除

1、有下列情形之一的，甲方可以单方解除本合同部分或全部内容：

（1）乙方未按合同约定的时间履行安全服务等合同义务，延期超过 5 天。

（2）乙方无正当理由明确表示不履行合同。

2、有下列情形之一的，乙方可以单方解除本合同部分或全部内容：

（1）甲方在本合同约定的付款义务期限届满 1 个月后，未履行付款义务。

（2）甲方无正当理由明确表示不再履行合同。

因上述原因导致合同解除后，尚未履行的，终止履行；已经履行的，

结清相应的服务费用；违约方还应按本合同第六条的规定承担违约责任。

九、 争议解决方式

凡因本合同引起的或与本合同有关的任何争议，由常州仲裁委员会仲裁。该仲裁是最终裁决，对双方均具有约束力。仲裁期间，该合同执行不受影响。

十、 其他约定事项

本合同经叁方盖章签字后生效，如有变动，必须经叁方协商一致后，方可更改，本合同一式六份，甲、乙、集中采购机构各持二份。附件为主合同的一部分，具有同等法律效力。

合同如有未尽事宜，经双方共同协商做出补充规定，补充规定与本合同具有同等效力。其他未尽事宜，按《中华人民共和国合同法》的有关规定执行。

附件一：风险评估实施内容

附件二：保密协议

此页无正文

甲方：单位名称（章）：常州市政务服务管理办公室

单位地址：常州市政务服务中心 1-1 号楼 10 楼

法定代表人：

分管负责人：

经办人：

电　话：

乙方：单位名称（章）：江苏瑞新信息技术股份有限公司

单位地址：常州市新北区太湖东路 9-1 号 808 室

法定代表人：

委托代理人：杨粉

经办人：

电　话：0519-81236533　　15851967128

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

附件一：“政务体系建设及证照分离项目信息安全风险评估实施内容

一、项目实施目标

全面给出相应的安全隐患和脆弱性报告，以及安全性整改建议。使用户对系统安全性状况和整体安全状况有全面具体的了解，保护用户不遭受新的安全性威胁带来的损失，保护安全与性能的平衡。达到以下目标:及时提供操作系统安全漏洞信息，并协助作出相应处理或给予建议解决方案；及时发现系统配置漏洞，并协助作出相应处理或给予建议解决方案；及时通报应用软件安全漏洞，并协助作出相应处理或给予建议解决方案；保证操作系统的安全等级与最新安全技术的同步，保障应用系统的安全；及时通报数据备份硬、软件系统的运行情况，对存在的安全隐患给出解决方案。

二、项目实施原则

客观性和公正性原则

测评人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

可重复性和可再现性原则

依照同样的要求，使用同样的测评方式，对每个测评实施过程的重复执行应该得到同样的结果。可再现性和可重复性的区别在于，前者与不同测评者测评结果的一致性有关，后者与同一测评者测评结果的一致性有关。

连续性原则

确保在高速变化的信息安全环境中，在有效的服务期间内，保证甲方风险评估结论的准确性和及时性，对于甲方单位新增设的信息资产和服务，或新建立的信息化项目，进行局部系统的重新评估。从经济上，降低了甲方单位的成本，从信息安全性上，保证信息安全评估的动态稳定性。

扩展性原则

在风险评估过程结束后，倡导信息安全评估过程要保持扩展性，从扩展的属性上进一步加强评估结束后被评估用户单位的安全管理有效性和可用性。

保密原则

在风险评估过程中，需严格遵循保密原则，甲方与乙方签订保密协议，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。

互动原则

在整个风险评估过程中，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，进而更好的进行风险评估工作。

最小影响原则

风险评估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。

规范性原则

信息安全风险评估服务的实施必须由专业的评估服务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，并提供完整的服务报告。

质量保障原则

在整个风险评估过程中，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、项目测评技术要求

按照《GB/T 20984-2007》风险评估要求,对信息系统进行安全评估，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与等级保护相应等级基本要求之间的差距，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

对信息系统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。

3、管理体系规划设计

针对信息系统的安全需求，规划设计管理体系，包括组织体系和制度体系。

4、技术体系规划设计

针对信息系统的安全需求和信息安全方针策略，规划设计技术体系，包括技术防护体系、技术管控体系和技术恢复体系。

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、《信息安全管理体系要求》（GB/T 22080-2008）

5、《信息安全管理实用规则》（GB/T 22081-2008）

6、《信息系统安全管理要求》（GB/T 20269-2006）

7、《信息安全事件分类分级指南》（GB/Z 20986-2007）

8、《信息安全事件管理指南》（GB/Z 20985-2007）

9、《信息系统灾难恢复规范》（GB/T 20988-2007）

10、《信息安全应急响应计划规范》（GB/T 24363-2009）

四、项目安全评估过程

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

在常州市政务服务管理办公室相关部门的授权下，对常州市“政务体系建设及证照分离项目进行渗透测试，并提供相关渗透测试报告。

8、系统加固服务

依据评估结果，和常州市政务服务管理办公室共同制定系统加固实施方案，依据方案实施加固，并输出完整的系统加固实施记录。

提交测评成果：投标人必须在项目建设的各个阶段及时提交测评成果，主要包括（但不限于）以下内容：

《“政务体系建设及证照分离项目信息安全风险评估报告》

《“政务体系建设及证照分离项目弱点评估报告》

《“政务体系建设及证照分离项目复测报告》

附件二：常州市“政务体系建设及证照分离”信息安全风险评估项目保密协议

保 密 协 议

甲方：常州市政务服务管理办公室

乙方：江苏瑞新信息技术股份有限公司

签订地点：常州市政务服务中心 1-1 号楼 10 楼

签订日期：2020 年 9 月 11 日

为加强常州市政务服务管理办公室信息安全风险评估相关系统数据的安全保密管理，贯彻落实《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施办法》、《中华人民共和国网络安全法》等有关法律法规，确保数据的安全保密，促进数据合法、有效利用，防止发生失泄密事件，防范非法使用行为，本着平等、自愿、协商一致、诚实信用的原则，就乙方为甲方提供信息安全技术支持服务（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（在项目中向社会公众提供信息公开和服务的图片、网页、信息数据不包含在内）；

（二）甲方在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）甲方在项目实施中涉及的业务及技术文档，包括方案设计细节、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）乙方明确所接收的文件（包括电子和纸质）为甲方所有，甲方拥有以上文件的知识产权。乙方承认甲方在本协议规定的保密信息上的利益和一切有关的权利，乙方应当考虑甲方的利益对该信息予以妥善保存，防止有意或无意的泄漏；

（二）乙方应采取尽可能的措施对所有来自甲方的信息严格保密，包括执行有效的安全措施和操作规程；

（三）甲方为基础数据的管理和提供方，甲方拥有所有数据的全部所有权，乙方需在甲方的授权下使用数据。乙方承诺对甲方以书面、口头、电子文本、电子数据等方式提供的保密信息承担保密义务；

（四）乙方同意仅在为实施本项目时使用保密信息，绝不为与该项目无关的目的使用保密信息；

（五）未经甲方的事先书面批准，乙方不得直接或间接以任何形式或任何方式把保密信息和其中的任何部分，披露或透露给任何第三方（仅可向有知悉必要的乙方内部人员披露，同时仅为甲方项目所需使用）。乙方有义务妥善保管上述文件和数据，不得复制、泄漏或遗失。乙方亦不得依据甲方提供的任何保密信息，就任何问题，向任何第三方作出任何建议；

（六）若乙方确有需要向第三方展示甲方数据信息及成果，需提前向甲方以一事一议的形式提交书面申请，由甲方签字盖章同意后方可施行。未经同意，严禁乙方将甲方数据向第三方展示。如有违反，乙方须承担全部后果，甲方有权向乙方追责；

（七）项目维护过程中，如因业务需要，乙方需采购第三方软件或软件服务的。乙方需以数据最小化为原则，明确数据范围及用途，并与第三方签订数据安全保密协议，确保甲方数据安全；

（八）乙方需加强自身保密意识及保密措施，从管理及技术方面保障甲方数据安全，与员工签订保密协议，约束监督员工，防止个别员工将甲方数据泄露；

（九）乙方的职员违背上述承诺，向第三方披露保密信息，或依据该等保密信息向第三方作出任何建议，都将被视为乙方违反本协议；

（十）甲方保留在甲方认为必要的情况下收回所提供的文件、数据及其使用权的权利；

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）本协议未尽事宜，由甲乙双方协商解决；

（二）本协议自甲、乙双方盖章之日起生效。

甲方：（章）常州市政务服务管理办公室

乙方：（章）江苏瑞新信息技术股份有限公司