

项目采购编号：JSZC-320400-JZCG-G2024-0326

常州市电子政务网安全保障 服务项目合同书

甲 方：常州市大数据管理中心（常州市电子政务中心）

乙 方：江苏瑞新信息技术股份有限公司

签订时间：2024年9月

项目名称：常州市电子政务网安全保障服务项目

项目编号：JSZC-320400-JZCG-G2024-0326

甲方：（买方）常州市大数据管理中心（常州市电子政务中心）

乙方：（卖方）江苏瑞新信息技术股份有限公司

甲、乙双方根据常州市政府采购中心常州市电子政务网安全保障服务项目公开招标的结果，签署本合同。

一、合同内容

1.1 标的名称：常州市电子政务网安全保障服务项目

1.2 履行时间（期限）：一年

1.3 履行地点：常州市大数据管理中心

1.4 履行方式：现场实施

二、合同金额

2.1 本合同金额为（大写）：壹佰柒拾捌万元整（¥：1780000 元）人民币或其他币种。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供服务（包含与服务相关的货物）的有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同服务（包含与服务相关的货物）或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付的服务（包含与服务相关的货物）的所有权完全属于乙

方且无任何抵押、查封等产权瑕疵。

六、履约保证金

本项目不收取履约保证金。

6.1 乙方交纳人民币___/___元作为本合同的履约保证金。（不得超过合同金额的 5%）。供应商可以自主选择以支票、汇票、本票、保函（保险）等非现金形式交纳或提交，按照省市有关文件精神，鼓励优先采用电子履约保函（保险）形式。

6.2 合同履行结束后，甲方应及时退还交纳的履约保证金。

6.2.1 履约保证金退还方式： /

6.2.2 履约保证金退还时间： /

6.2.3 履约保证金退还条件： /

6.2.4 履约保证金不予退还的情形： /

七、合同转包或分包

7.1 乙方不得将合同标的转包给他人履行。

7.2 乙方不得将合同标的分包给他人履行。

7.3 乙方如有转包或未经甲方同意的分包行为，甲方有权解除合同。

八、合同款项支付

8.1 合同款项的支付方式及进度安排。

8.1.1 预付款支付时间：合同签订后十五个工作日内，甲方向乙方支付合同金额的 50%，即人民币：捌拾玖万元整（¥：890000.00 元）。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

8.1.2 尾款支付时间：服务结束并验收合格，甲方向乙方支付尾款，即人民币：捌拾玖万元整（¥：890000.00 元）。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

九、税费

9.1 本合同执行中相关的一切税费均由乙方负担。

十、项目验收

10.1 甲方依法组织履约验收工作。

10.2 甲方在组织履约验收前,将根据项目特点制定验收方案,明确履约验收的时间、方式、程序等内容,并可根据项目特点对服务期内的服务实施情况进行分期考核,综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

10.3 对于实际使用人和甲方分离的项目,甲方邀请实际使用人参与验收。

10.4 如有必要,甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收,相关意见将作为验收书的参考资料。

10.5 甲方成立验收小组,按照采购合同的约定对乙方的履约情况进行验收。验收时,甲方按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后,验收小组出具验收书,列明各项标准的验收情况及项目总体评价,由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料存档备查。

10.6 验收合格的项目,甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目,甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的,甲方将及时报告本级财政部门。

十一、违约责任

11.1 甲方无正当理由拒绝接受乙方提供服务的,甲方向乙方偿付拒绝接受服务合同价款总值 5% 的违约金。

11.2 甲方无故逾期验收和办理合同款项支付手续的,甲方应按逾期付款总额 5% 每日向乙方支付违约金。

11.3 乙方逾期提供服务的,乙方应按逾期提供服务合同总额每日千分之六向甲方支付违约金,由甲方从待付合同款项中扣除。逾期超过约定日期 10 个工作日不能提供服务的,甲方可解除本合同。乙方因逾期提供服务或因其他违约行为导致甲方解除合同的,乙方应向甲方支付合同价款总额 5% 的违约金,如造成甲方损失超过违约金的,超出部分由乙方继续承担赔偿责任。

11.4 乙方所提供服务的标准不符合合同规定及招标文件规定标准的，甲方有权拒绝接受服务，并可单方面解除合同。

十二、不可抗力事件处理

12.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

12.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

12.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十三、解决争议的方法

13.1 双方在签订、履行合同中所发生的一切争议，应通过友好协商解决。如协商不成，由甲方住所地人民法院管辖。

十四、合同生效及其它

14.1 合同经双方法定代表人或授权委托代理人签字并加盖单位公章后生效。

14.2 本合同未尽事宜，遵照《民法典》、《政府采购法》有关条文执行。

14.3 本合同正本一式四份，具有同等法律效力，甲方、乙方各执两份。

甲方：	乙方：江苏瑞新信息技术股份有限公司
地址：	地址：常州市新北区太湖东路 9-2 号 3 楼
法定代表人或授权代表：	法定代表人或授权代表：杨粉
经办人：	经办人：蒋春燕
联系电话：	联系电话：0519-81236533
	签订日期：2024 年 9 月 10 日

附件 1:《保密协议》

保 密 协 议

甲方：常州市大数据管理中心（常州市电子政务中心）

乙方：江苏瑞新信息技术股份有限公司

为加强“常州市电子政务网安全保障服务项目”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》《中华人民共和国密码法》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，就乙方为甲方提供软件修改完善、数据处理和技术支持服务（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 and 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) 常州市大数据管理中心 乙方：(章) 江苏瑞新信息技术股份有限公司

附件 2：《安全服务项目内容》

一、体系建设咨询服务

乙方协助常州市大数据管理中心完成网络安全规划编制，并对网络安全规划进行跟踪验证。针对常州市电子政务网的安全建设，遵循“三同步”原则-同步规划、同步建设、同步运行。基于常州市电子政务网信息化顶层设计和新兴技术发展方向，识别信息安全建设任务，制定未来 1-3 年的信息安全规划，增强常州市电子政务网抵御信息安全风险的能力，为常州市大数据管理中心信息化战略的实现提供坚实的信息安全保障。细化信息安全目标和任务，梳理安全工作路线，制定信息安全分段建设计划，实现安全管理与成本的相对平衡以及安全支持创新发展。

安全保障方案制定

针对电子政务网面临的安全威胁，制定完善的安全保障方案，包括网络安全防护、数据安全保护、身份认证与访问控制等措施。

网络管理流程优化

分析现有网络管理流程中存在的问题，提出优化建议，包括故障处理流程、配置管理流程、性能管理流程等。

技术支持与培训服务

提供必要的技术支持和培训服务，帮助政府部门掌握电子政务网管理体系的实施要点和操作技巧。

二、电子政务网资产安全服务

资产梳理

乙方通过数据清理、人工校正、技术探测等多种手段形成电子政务外网资产底数，通过识别资产重要性，标识重点资产库，利用动态检测、对比技术，建立常态化数据更新机制，有效支撑电子政务网的网络安全管理各项工作。

输出成果

资产梳理的输出成果如下：

《网络资产清单》

服务频率:一次全量普查,定期更新。

重点资产重点监测

(1) 渗透测试:乙方在常州市大数据管理中心授权的前提下,以模拟黑客攻击的方式,对电子政务网上的重要系统(约250个系统和3000个主机)的安全漏洞、安全隐患进行全面检测,最终目标是查找业务系统的安全漏洞、评估业务系统的安全状态、提供漏洞修复建议。

输出成果

渗透测试的输出成果如下:

《系统渗透测试服务报告》

《系统渗透测试服务复测报告》

服务频率:每季度覆盖全量重点资产。

(2) 变更安全测试:乙方针对常州市大数据管理中心自建的业务系统在变更后需要进行安全测试,确保风险隐患得到解决方可上线,变更主要包括网络、主机、应用系统和数据四个层面。

网络安全:测试网络设备的配置是否安全,网络通信是否存在泄露风险,网络访问控制是否有效等。

主机安全:测试主机系统的安全配置是否符合标准,是否存在漏洞和风险,主机的访问控制、日志审计等安全功能是否有效。

应用安全:测试应用系统的身份认证、授权访问、数据保护等安全功能是否正常,是否存在代码漏洞和逻辑错误。

数据安全:测试数据的加密、备份、恢复等安全措施是否有效,数据在传输和存储过程中是否存在泄露风险。

输出成果

变更安全测试的输出成果如下:

《测试服务报告》

《测试服务复测报告》

服务频率:重要系统发生变更时

一般资产安全服务

(1) 上线前检测: 部署于电子政务外网系统在上线前, 进行所有上线系统(约 100 个系统)或版本的安全检查工作, 新系统或版本经过相关测试达到要求后, 进入权限开通等流程, 检查内容包括但不限于应用层安全检测、主机层检测、逻辑漏洞检测、第三方组件漏洞检测、合规性检测等。

(2) 日常安全监测: 对于托管在常州市电子政务网的系统采用平台和人工的方式开展监测服务, 利用现有奇安信态势感知平台、全知 API 数据安全监测平台、安骑士云主机监测平台等平台, 统筹各方资源进行监测、季度人工渗透测试全年覆盖全量资产、预警、完成风险闭环管理, 月度形成监测月报。

一般资产安全服务的输出成果如下:

《测试服务报告》

《测试服务复测报告》

服务频率

动态监测, 季度人工渗透测试全年覆盖全量资产

三、辅助服务

流量洞察

乙方提供流量探针设备或软件, 实时捕获、分析和储存原始数据包, 依托网络编程、网络测量、自动化运维、分布式存储、机器学习、数据分析等多领域前沿技术, 对攻击中广泛采用的 0day、Nday 漏洞、特种木马、渗透入侵等技术进行深度分析, 并结合数据智能分析引擎、网络攻击行为特征、网络威胁情报库、资产指纹库、应用指纹库等, 挖掘网络空间中的已知和未知攻击威胁, 发现僵尸网络、木马病毒、挖矿病毒等恶意软件, 保障信息系统的安全稳定运行。

输出成果

流量洞察服务的输出成果如下：

《流量分析报告》

服务频率：每日分析，每月形成分析报告

应急响应

服务期限内，乙方提供 7×24 小时的远程安全应急响应，接到安全事件通知后，立即以远程方式对安全事件进行分析、抑制、溯源，如果远程无法进行应急，则指派经验丰富的安全服务工程师，赶到用户现场进行应急处理。最大程度降低安全事件对客户带来的损失。

根据甲方单位的信息安全组织和信息安全现状，结合甲方业务系统的特点，分析业务系统可能会发生的安全事件类别以及可能造成的影响范围、严重程度等，和客户一起，建立相应的应急响应预案，并指导客户对预案进行演练。

通过建立应急响应预案，可以在安全事件发生前进行演练防患于未然，当安全事件发生时，可根据预案进行快速响应，从而在最短的时间内找到安全事件源头，恢复系统的正常运行。

输出成果

应急响应服务的输出成果如下：

《常州市大数据管理中心业务系统安全事件应急预案》

《常州市大数据管理中心业务系统安全事件应急响应报告》

服务频率：出现安全事件时，立即进行应急响应。

重保保障

重要时期安全保障，在重大会议、节假日等特殊时期内，乙方安排安全攻防经验丰富的安全专家，对业务系统进行重保前专项安全检查、现场值守与发生异常情况的应急响应。

当目标遭受黑客入侵攻击时，乙方值守人员立即对入侵事件进行分析、检测、抑制、处理，查找入侵来源并恢复系统正常运行，完成后给出应急响应报告，报告中将还原入侵过程，同时给出对应的解决建议。

输出成果

安全保障的输出成果如下：

《常州市大数据管理中心重要时期安全保障日报》

《常州市大数据管理中心重要时期安全保障周报》

《常州市大数据管理中心重要时期安全保障工作总结》

《常州市大数据管理中心重要时期安全保障应急预案》

《常州市大数据管理中心重要时期安全保障应急响应报告》



服务频率：重保时期

驻场实施服务

在服务期内至少安排 3 名工程师现场服务，具体工作由按照实际工作情况安排，工作时间参照甲方工作作息时间执行。现场服务人员应具备具有二年以上网络安全工作经验，熟悉用户环境及设备配置，能独立解决网络安全问题。

关注最新安全漏洞通告及重大安全事件通告，及时了解最新的漏洞信息和影响范围。

对常州市大数据管理中心系统所使用的操作系统、数据库、中间件等架构等信息进行收集、统计。

针对最新爆出的安全漏洞进行匹配，及时出具漏洞预警报告提交至常州市大数据管理中心，配合各部门进行漏洞整改。及时的规避新安全漏洞带来的风险。

