附件一：

服务内容

一、网络安全常规监测采购需求

持续稳定地对82家常州市网络安全工作责任制督查检查单位的互联网网站或重要信息系统开展安全监测服务，每月按时按要求提供月度全市监测报告和事件漏洞预警处置报告。

具体要求：

1.监测数量

提供全市1000条核心资产的日常监测、月度分析和建议服务。

2.疑似篡改监测

监控网站首页、二级栏目以及其他重点栏目内容判断是否被黑客篡改。

3.挂马监测

采用特征分析和沙箱行为等分析技术对网站进行木马监测，从而实现快速、准确的发现和定位网页木马。

4.暗链监测

监测平台采用暗链数据库对比分析、暗链特征提取等技术，及时发现网站中被植入的暗链，及时通告并预警。

5.漏洞安全检测

应用安全漏洞扫描。采用多种扫描工具交叉扫描，避免单一扫描器缺陷。发现容易被黑客利用攻击的脆弱点和漏洞，发现网站系统中存在的安全漏洞和安全隐患，人工进行验证并确认危害程度。

系统安全漏洞检测。采用多种系统漏洞检测工具，重点检测操作系统、数据库、WEB服务器软件、中间件、第三方插件的安全隐患和漏洞，人工进行验证并确认危害程度。

安全漏洞审计。对于无法通过扫描工具自动发现的漏洞，如应用系统的逻辑设计错误、参数篡改等漏洞，要求结合已经建立的安全档案，关注国内外漏洞库、论坛、安全平台等最新的安全漏洞通报。人工确认漏洞对现有系统的危害程度和后果。

安全事件和安全漏洞验证后形成相关报告，配合常州市委网信办进行通报与复测。每月将监测情况进行分析，形成月度全市监测（含常规监测和随机监测）报告。每半年度及全年度形成全市监测报告。

6. 渗透测试

针对给定的系统，制定渗透测试方案以及风险规避和异常状态应急处置预案，报市委网信办批准后，有计划有步骤地执行渗透测试，提供详细的渗透测试报告。开展渗透测试的信息系统数量为 50 个。

7. 履约验收

中标金额的 10%作为履约情况验收保证金。已纳入监测的资产被中央、省委网信部门通报的情况将与年度绩效进行挂钩，按照每个漏洞 1000 元的标准从保证金中进行扣除。

二、网络安全监管平台服务

为常规监测和随机监测，提供互联网基础资产、漏洞、事件等信息的维护管理以及通报-反馈-复测全流程管理服务。

1. 数据可视化展示

实现监管对象数据、巡检数据及事件和漏洞处理数据的可视化展示。包括数据多维度关联查看、分类分维度统计、统一的实时监控页面及根据不同需求自动生成对应的报告。如管辖区域地图展示总体安全情况、漏洞 TOP10、当日安全态势、高危网站数量趋势、同比与环比、未修复情况等。

2. 网络资产管理

提供所有监管对象互联网基础资产管理模块，实现信息资产上报、维护与管理。信息资产字段包括但不限于以下内容：单位信息（所属地区、主管单位、联系人、联系方式、所属单位、注册联系人、注册联系方式）、资产信息（系统名称、域名、IP、操作系统、数据库、网站框架、中间件、开发单位、运维单位等）。

3. 通报反馈复测全流程

畅通监管对象漏洞、安全事件、僵木蠕等恶意程序的整改修复的全程管控，及时对整改情况进行复测，形成通报-修复-反馈-复测的完整的监管业务闭环。

4. 自身数据安全保障

保障网络安全监管平台相关数据的安全。网络安全监管平台相关数据在脱敏前不得直接对互联网开放；用户经过授权可通过互联网下载所管辖的网络资产的安全报告，报告下载完成后系统将不再保留。用户经过授权可通过互联网进行相关整改反馈，整改反馈结果导入到内部数据中心存档。按规定留存平台相关日志。

5.功能模块定制开发

项目承建方需根据常州市委网信办业务需求，在常州市网络安全监管平台基础上，定制开发部分功能(如网安专项行动、网络安全监督检查等功能)，以更好地开展网络安全监管业务。

6.“网安行动”配合

市级“网安行动”和攻防实战演练期间，负责完成攻击测试成果在通报反馈平台的录入、通报和反馈复测工作。

三、技术支撑服务

具体要求：

1.驻场服务

提供3人常驻现场5*8小时服务。

2.应急值守和处置

提供至少1名安全工程师7×24应急响应。

提供特殊时期安全值守服务。特殊时期（如：春节、国庆、元旦、两会等），投标人安排至少1名资深工程师，提供网络安全保障服务，及时应对处置网络安全事件，以免造成严重不良后果。

提供突发网络安全事件现场协查。根据市委网信办要求，提供突发网络安全事件的现场技术支持服务。如某辖市区或单位的网站或重要系统遇突发情况，造成了影响较大的安全事件，应急响应工程师须在半小时内响应，快速确定问题的根源，阻止或最小化安全事件带来的负面影响，有效遏制网络安全事件蔓延。

3.处置建议

针对网站和系统安全监测情况及渗透测试情况，提供具有针对性的处置方案；发生重大网络安全事件，即时通报，并提供明确的事件处置方案建议；月度通报中，对于常见网络安全事件以及安全漏洞进行科学分类，并提供常规处置方案建议；针对网络安全事件较为频发的网站给予安全加固方案建议，协助相关单位完成对安全

设备实施的策略调整和加固措施，并配合网站或系统开发单位、运维单位进行全面的优化升级和加固。

4. 安全通告服务

关注国际国内最新的网络安全漏洞通告预警，发现危害严重、影响范围广的安全漏洞及时向市委网信办进行报告，并提供主流解决方案。

5. 安全咨询和技术支撑服务

依据安全服务的现状，每半年提供监测范围内的全市政务和公共服务领域网络安全态势报告，有针对性地提出网络安全工作的改进措施、建设方案等，并能够提供有针对性的、科学化、体系化的安全解决方案。随时接受市委网信办的技术咨询并按要求提供相关材料及技术支撑。

6. 网络安全防护指数报告

根据网络安全防护指数计算标准，提供年度全市、辖市区、行业主管监管部门和非行业主管监管部门的网络安全防护指数及其分析报告。

7. 信息安全情报收集

定期提供 IT 业界网络安全的最新情报，包括但不限于：网络安全最新发展态势、国际国内网络安全形势、重点安全事件、与服务目标相关的安全建议等。全年不少于 6 份全局性相关报告。

8. 网络安全宣教培训

配合完成全市网络安全宣教培训工作以及市委网信办交办的其它任务。

附件二：市委网信办 2022-2023 年度网络安全监管服务项目（分包 1）安全保密协议

甲方：中共常州市委网络安全和信息化委员会办公室

乙方：江苏瑞新信息技术股份有限公司

为加强甲方市委网信办 2022-2023 年度网络安全监管服务项目（分包 1）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）其他甲方合理认为的建议，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）甲方在特定的情况下有收回所提供的文件、数据及其使用的权利；

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：中共常州市委网络安全和信息化委员会办公室　　乙方：江苏瑞新信息技术股份有限公司

日期：　　日期：