江苏省政府采购合同（服务）

（合同编号：NBHT20260902477）

项目名称：江苏省自然灾害综合监测预警系统国产化改造及运维

采购编号：JSZC-320000-SCZX-G2026-0361

采购包号：1

甲方（采购人）：江苏省应急管理厅

乙方（中标供应商）：北京辰安科技股份有限公司

甲、乙双方根据本项目采购文件、中标通知书及乙方投标文件，依据《中华人民共和国民法典》《中华人民共和国政府采购法》等有关规定，遵循平等、自愿、公平和诚实信用原则，就江苏省自然灾害综合监测预警系统国产化改造及运维服务事项订立本合同。

一、合同标的及履行要求

1.1 标的名称：江苏省自然灾害综合监测预警系统国产化改造及运维服务。

1.2 项目属性：服务类项目，不包含货物采购；服务中确需使用的软硬件、工具及相关许可，应符合采购文件关于本国产品、正版授权和安全合规的要求。

1.3 服务规模：完成数据库、地图服务、中间件、四大核心业务模块、接口与兼容性的国产化适配改造，并提供系统日常维护、巡检、数据管理、安全加固、性能优化、故障排查与修复等运维服务。

1.4 履行期限：国产化改造期限为 3 个月，自合同生效之日起计算；运维服务期限自合同生效之日起至2027年7月30日。服务期满后是否续签，按政府采购法律法规、采购文件和甲方实际需求另行办理。

1.5 履行地点：江苏省应急管理厅或甲方指定地点。

1.6 履行方式：乙方组建不少于 4 人的专业项目团队，按照采购文件、乙方投标承诺、本合同及经甲方确认的实施方案开展现场与远程服务。

1.7 本合同、采购文件、乙方投标文件、中标通知书、澄清说

明、双方依法形成的书面确认文件及本合同附件均为合同组成部分。合同约定不得对采购文件和投标文件作实质性修改；乙方投标文件作出高于采购文件要求且有利于实现合同目的的承诺，乙方应按该承诺履行。

二、合同金额

2.1 本合同金额为人民币（大写）：捌拾玖万捌仟元（¥898000元）。该金额为完成本合同全部工作并达到验收标准所需的全部含税费用，除依法依规并经双方书面确认的情形外，甲方不再支付其他费用。

三、国产化改造服务内容

3.1 总体要求。乙方应在不影响现有业务连续性的前提下，完成系统数据库、地图服务、中间件及业务模块的国产化迁移和适配，确保改造后功能完整、数据准确、接口稳定、性能满足要求，并具备可回退、可验证、可审计能力。

3.2 数据库适配。乙方应选用符合采购文件要求的国产数据库，支持关系型数据与空间数据存储，兼容 OGC 空间标准，适配 SpringBoot 框架、国产操作系统和国产中间件。乙方应完成 SQL、空间查询、连接池、索引等适配和优化。

3.3 数据迁移。乙方应在实施前提交经甲方确认的数据迁移、备份和回退方案；对灾害案例、监测数据、行政边界、灾害点位等关系型数据和空间数据进行清点、导出、转换、导入和校验。迁移前后应核对数据总量、关键字段、空间坐标、空间关系及抽样记录，确保无丢失、无乱码、无位置偏差。未经甲方书面确认，不得删除原始数据或终止原环境。

3.4 国产地图服务适配。乙方应完成地图服务、空间数据服务迁移和发布，适配 OpenLayers、接口协议、瓦片格式、权限认证及跨域策略；保障地图缩放、平移、定位、数据叠加、渲染、历史灾害推演和专题制图等功能正常。

3.5 国产中间件改造。乙方应完成 Web 中间件和消息中间件适配、应用部署、队列与路由配置、接口兼容修复、国密能力适配及性能调优，确保与国产操作系统、数据库和业务模块协同运行。

3.6 业务模块适配。乙方应完成电子信息图谱可视化、综合监

测分析、气象专题支撑、综合业务管理四个子系统的功能适配，确保森林火险、气体污染物泄漏扩散、太湖蓝藻监测、重大活动保障等特色功能正常运行。

3.7 接口与兼容性。乙方应建立接口清单，完成接口代码、调用协议和认证机制适配及全接口联调。正常网络和合理并发条件下，采购需求明确的接口响应时间应不超过 2 秒。乙方应完成国产操作系统、国产浏览器、国产中间件环境下的兼容性验证，并修复页面、功能和交互异常。

3.8 实施控制。乙方应在合同生效后5个工作日内提交实施计划、里程碑、风险清单、回退方案和人员分工，经甲方确认后执行。涉及生产环境的部署、升级、数据迁移、参数调整、账号权限或接口变更，应事先提交变更申请，说明影响范围、验证方法和回退措施，经甲方批准后实施；紧急处置应先控制风险，并在处置后 1 个工作日内补齐记录。

3.9 上线保障。系统切换前，乙方应完成备份、演练、测试和风险评估；切换期间安排项目经理和核心技术人员保障。出现影响业务的异常时，乙方应按经确认的方案及时回退或采取替代措施，不得在风险未受控情况下继续操作。

四、运维服务内容及标准

4.1 日常维护。乙方负责系统账号和授权维护、专项数据处理、操作问题支撑、系统环境维护以及服务器和相关设备配置信息归档。账号开通、变更、停用和权限调整应以甲方授权为依据并完整留痕。

4.2 常规巡检。乙方每月开展不少于2次巡检，检查服务器日志及资源使用、安全状态、应用和中间件健康性、数据库和备份任务、数据交换、数据资源池计算与存储资源、数据表分区更新等情况。每次巡检应形成报告，列明检查项、发现问题、风险等级、责任人、整改时限和复核结果。

4.3 数据管理。乙方应执行数据库备份、数据仓表更新检查、多源监测数据同步、质量校核、清洗纠错、存储监控和接口运维。备份策略、保存周期和存放位置按甲方制度执行；乙方应定期验证备份可用性，并按甲方要求开展恢复演练，禁止以“备份任务显示成功”替代恢复验证。

4.4 安全加固。乙方应定期开展系统、主机、数据库、应用接口漏洞扫描，及时处置漏洞、弱口令、配置缺陷和恶意代码风险，优化服务器、数据库、中间件、防火墙及访问控制策略。对高风险隐患应立即采取隔离、封堵等临时措施，并在甲方规定时限内完成修复；无法按期修复的，应提交风险说明、替代控制措施和明确计划，经甲方书面同意后执行。

4.5 性能优化。乙方应监控响应速度、并发负载、接口调用和服务器资源使用，开展应用、数据库、中间件、缓存、SQL、索引及任务调度优化，及时定位并处理慢响应、超时、卡顿等问题。任何优化不得降低安全性、数据完整性或业务功能。

4.6 故障处置。乙方应建立故障受理、分级、定位、处置、恢复、复盘和销号机制。重大系统故障应在 30 分钟内响应、2 小时内恢复正常；日常应用故障应在 60 分钟内响应、4 小时内排除；其他故障及问题应在 60 分钟内响应、24 小时内排除。确因复杂原因无法在上述时限内彻底解决的，乙方应先提供经甲方认可的临时保障措施，持续处置，并及时报告原因、影响、处置进度和预计完成时间。

4.7 服务保障。常规服务按照每周 5 天、每天 8 小时提供；重大故障、网络安全事件、极端天气、重大活动和甲方确定的重要保障期间，乙方应提供 7×24 小时应急响应，并按甲方通知安排现场或在宁技术保障力量。

4.8 报告和台账。乙方应维护巡检、故障、变更、账号权限、数据操作、漏洞整改、备份恢复、应急处置和服务请求等台账；每季度提交运维报告，运维期结束后提交年度运维报告。重大故障恢复后 2 个工作日内提交故障分析报告，说明根因、处置过程、影响范围、改进措施和防复发安排。

4.9 闭环要求。乙方对甲方提出的问题、检查发现的问题和主管部门通报事项，应按时整改并提交证明材料。甲方有权进行复核；未通过复核的，不视为完成整改。

五、项目组织与人员管理

5.1 乙方应配置不少于 4 名专业技术人员。项目经理应具备采购文件要求的信息系统项目管理师、系统架构设计师等相应能力或证书；团队成员应具备数据库、软件设计等与岗位相适应的专业能

力。具体人员以乙方投标文件和本合同附件为准。

5.2 项目经理为乙方履约第一责任人，负责计划、质量、安全、沟通、风险和交付管理。乙方应保证核心人员稳定，未经甲方书面同意不得擅自更换项目经理或关键人员。确需更换的，应提前书面说明并提供资质能力不低于原人员的替代人选，完成工作交接。

5.3 乙方人员应遵守甲方现场、网络、数据、保密和账号管理制度。甲方认为乙方人员不能胜任工作、违反管理规定或存在安全风险的，有权要求乙方限期更换；乙方应及时补充合格人员，不得影响服务连续性。

5.4 乙方应对其人员及其使用的工具、脚本、账号和操作行为承担管理责任。乙方不得以人员离职、内部协作、第三方产品故障或人员不足为由免除合同责任。

六、技术资料、交付物和知识转移

6.1 乙方应按项目进度和甲方要求提交实施方案、架构说明、数据库设计与数据字典、接口清单与文档、源代码及编译说明、部署脚本、配置清单、第三方组件及版本清单、账号权限清单、测试报告、迁移校验报告、巡检报告、运维报告、应急预案、培训材料、用户和运维手册等资料。

6.2 交付的源代码、脚本、配置和文档应与生产环境实际版本一致，能够由具备相应能力的第三方按照文档完成编译、部署、配置和维护。乙方不得以加密、缺失依赖、保留关键参数、设置技术锁或其他方式妨碍甲方自主运维和委托第三方维护。

6.3 乙方应建立版本管理和变更记录，按甲方要求将代码和文档提交至指定的代码、文档管理环境。涉及功能、接口、数据库结构、部署架构和安全配置的变更，应同步更新相关资料。

6.4 乙方应根据甲方安排开展培训和知识转移，培训内容包括系统架构、部署配置、日常运维、故障处置、数据管理、安全操作和应急恢复。培训应有签到、课件和效果反馈记录。

七、知识产权和软件授权

7.1 乙方应保证其提供的产品、代码、组件、地图服务、数据库、中间件、工具和资料来源合法、授权有效，不侵犯任何第三方

知识产权。发生权利纠纷的，由乙方负责处理并承担全部责任；因此影响系统运行的，乙方应及时提供合法、等效且不降低服务水平的替代方案。

7.2 甲方对本项目形成的定制开发成果、适配代码、配置、接口、数据处理规则及文档，享有采购文件、乙方投标承诺和法律规定范围内的使用、复制、修改、维护及委托第三方维护的权利。乙方在合同签订前已拥有的通用产品和背景知识产权仍归乙方或原权利人所有，但乙方应确保甲方在系统使用和维护期间持续、合法使用。

7.3 未经甲方书面同意，乙方不得将含有甲方数据、业务规则、系统架构或安全配置的成果用于本合同之外的目的。

八、网络安全、数据安全和保密

8.1 乙方应遵守现行《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》以及网络安全等级保护、密码应用、保密管理等有关规定，履行安全保护和协助义务。

8.2 乙方应坚持最小权限、专人专号、授权使用原则。未经甲方书面同意，不得擅自开设账号、扩大权限、开放端口、改变安全策略、接入外部网络或使用未经批准的远程运维工具。远程运维应经审批并保留可审计记录。

8.3 乙方仅可在履行本合同所必需的范围内处理甲方数据。未经甲方书面同意，不得复制、下载、留存、外传、出售、交换、公开或用于测试、训练及其他用途，不得将甲方数据、代码、日志、文档上传至公共云盘、公共代码托管平台、公共生成式人工智能服务或其他未经批准的平台。

8.4 乙方应对接触甲方系统和数据的人员开展安全保密教育并签署保密承诺。人员离岗、离职或岗位调整时，应立即停用账号、收回介质和资料并完成交接。保密义务不因合同终止而终止。

8.5 乙方应确保运维终端、工具、脚本和移动介质安全可控，不得植入后门、恶意代码、未披露的远程控制功能或高风险组件。乙方应按要求提供第三方组件、开源软件和软件物料清单，并及时处置已知漏洞。

8.6 乙方应完整记录关键运维和安全操作日志，日志保存期限不少于 12 个月；甲方有更高要求的，按甲方制度执行。乙方不得删除、篡改、伪造或规避审计记录。

8.7 发生或可能发生网络安全、数据安全事件时，乙方应立即采取控制措施，并在 30 分钟内向甲方报告，不得迟报、漏报、瞒报；同时保护现场和日志，配合调查、处置、溯源、整改和报告工作。未经甲方授权，乙方不得擅自对外发布信息。

8.8 甲方有权对乙方履行安全义务情况开展检查、审计、扫描和演练，乙方应予配合。发现安全风险的，乙方应按要求整改并完成复核销号。

九、履约担保及考核运用

9.1 乙方应在合同签订后 10 个工作日内，以银行保函形式提交合同金额 10%的履约保证金，履约保函金额为人民币捌万玖仟捌佰元（89800 元），保函有效期应覆盖合同履行及甲方完成履约考核所需期间。

9.2 运维年度结束后 1 个月内，甲方依据采购文件、本合同及《信息系统运维工作考核细则（试行）》对乙方服务进行考核。评级为 A 或 B 且无其他应扣除情形的，甲方退还或解除履约保函；评级为 C 或 D 的，甲方按考核细则及本合同约定扣除相应履约保证金。

9.3 因乙方人员、操作、工具、代码、配置、运维管理、漏洞处置不及时或其他可归责于乙方的网络安全原因，造成信息系统网络安全事件，或者被网信部门及其他有权主管部门通报的，甲方有权根据事件等级、影响范围、持续时间、数据影响、乙方责任程度和整改情况，每次扣除不超过履约保函金额 20%的履约保证金。年度累计扣除金额不超过履约保函总额。

9.4 除第 9.3 条规定的网络安全责任外，乙方未按合同约定履行人员配备、巡检、故障响应与恢复、数据备份、安全整改、变更管理、接口运维、成果交付、培训保障、台账报告、知识转移和退出移交等义务的，甲方有权责令限期整改，并根据违约程度、影响范围、持续时间、整改情况和重复发生次数，按附件 4 所列标准扣除履约保证金。

9.5 对未造成明显业务影响、能够在甲方规定期限内完成整改

的轻微违约，甲方可先给予书面提醒或整改通知；乙方逾期未整改、整改不到位，或者同类问题在 30 日内再次发生的，按一般违约处理。一般违约再次发生、经两次提醒仍未改正、弄虚作假或故意隐瞒的，提升一个档次处理。

9.6 乙方发生一般违约的，每次扣除履约保函金额 0.5%至 2%；发生较重违约的，每次扣除 2%至 5%；发生严重违约的，每次扣除 5%至 10%；发生重大违约或者导致合同目的不能实现的，每次扣除 10%至 20%，甲方并有权依法解除合同。年度累计扣除金额不超过履约保函总额；履约保证金不足以弥补甲方损失的，乙方仍应赔偿差额。

9.7 甲方拟扣除履约保证金时，应向乙方说明事实、依据、违约档次和拟扣金额。乙方可在收到通知后 3 个工作日内提交书面说明和证据；逾期未提交的，视为无异议。甲方可从履约保函、应付合同款或其他应付款项中扣取。履约保函被部分扣取后，乙方应在收到甲方通知后 5 个工作日内补足至合同约定金额。紧急处置、证据保全和损失控制不受前述程序影响。

9.8 履约保证金的扣除不免除乙方继续整改、恢复系统、消除影响、赔偿损失及承担其他法律责任。同一事实同时符合多项扣除情形的，按较重一项执行，不重复扣除；逾期未整改、重复发生、伪造材料或另行造成损害后果的，属于新的独立违约行为，可另行处理。

十、合同款项支付

甲方收到符合要求的履约保函和乙方提供的合法有效票据后 15 个工作日内，通过转账方式支付合同金额的 100%。因乙方未按要求提交保函、票据、收款信息或其他付款所需资料造成的延迟，不视为甲方逾期付款。

十一、项目验收

11.1 甲方依法组织履约验收，可根据项目特点开展国产化改造阶段验收、运维过程考核和合同期满验收。乙方应按甲方验收方案提供测试环境、人员、工具、数据和证明材料。

11.2 国产化改造验收重点包括：数据库和数据迁移准确性，地图服务与空间数据功能，中间件适配，四大业务模块完整性，接口响应与联调，国产环境兼容性，安全扫描和加固，备份回退，源代

码及技术文档完整性。存在未修复的高风险安全隐患、关键数据不一致、核心功能不可用或交付资料严重缺失的，不得通过验收。

11.3 运维服务验收重点包括：人员到位、巡检频次和报告、故障响应与恢复、数据备份和恢复验证、漏洞整改、变更管理、台账报告、培训和知识转移、重大保障及问题闭环情况。

11.4 验收发现问题的，乙方应在甲方规定期限内无偿整改并申请复验。复验仍不合格或乙方拒不整改的，甲方有权依照合同和考核细则扣除履约保证金、要求赔偿、暂停有关操作或依法解除合同。整改和复验不免除乙方逾期责任。

11.5 甲方可邀请实际使用人、其他供应商、第三方专业机构或专家参与验收。验收结果与履约考核、履约保函返还及违约责任挂钩，验收资料应归档备查。

十二、合同变更、转包分包和退出移交

12.1 双方不得擅自变更、中止或终止政府采购合同，不得订立背离采购文件和中标人投标文件实质性内容的协议。确需变更的，应依法履行书面程序。乙方不得因合同变更尚未完成而擅自停止必要的安全保障和故障处置。

12.2 未经甲方依法书面同意，乙方不得转包或分包合同工作，不得将项目实质性交由未在投标文件中披露的第三方实施。乙方使用原厂技术支持，不免除其对甲方承担的合同责任。

12.3 合同期满、解除或终止时，乙方应按甲方要求完成系统、代码、数据、文档、账号、配置、证书、介质、未结事项和风险清单的移交，配合甲方或后续服务单位平稳接续。移交完成后，乙方应删除非依法依规必须保留的甲方数据及副本，并提交书面确认。

12.4 乙方不得以费用争议、合同终止、人员变动或其他原因拒绝移交、设置技术障碍、停止必要配合或影响系统正常运行。

十三、违约责任

13.1 甲方无正当理由逾期验收或办理付款手续的，按逾期付款金额每日万分之五向乙方支付违约金；因乙方原因、财政支付流程或依法暂停支付的除外。

13.2 乙方逾期完成国产化改造或其他合同交付的，应按逾期部

分对应价款每日千分之六向甲方支付违约金。逾期超过约定日期 10 个工作日仍不能完成，或关键成果经两次整改仍不合格的，甲方有权依法解除合同，并要求乙方承担合同总额 5%的违约责任。

13.3 乙方未达到人员、巡检、响应、故障恢复、数据备份、安全整改、变更管理、文档交付、重大保障、培训移交等要求的，甲方有权要求限期整改，并依照本合同第九条、附件 4 和考核细则扣分、扣除履约保证金；造成损失的，乙方应赔偿。

13.4 乙方存在擅自转包分包、擅自停止服务、泄露或违规处理数据、隐瞒安全事件、伪造服务记录、植入后门、拒绝移交、严重侵犯知识产权等行为，或者其违约导致合同目的不能实现的，甲方有权依法解除合同，扣除部分或全部履约保证金，并追究损失赔偿责任。

13.5 乙方承担的违约金、履约保证金扣除和赔偿不足以弥补甲方损失的，乙方仍应赔偿差额。甲方损失包括直接损失以及为调查、应急处置、系统恢复、数据修复、第三方检测、专家论证、诉讼仲裁等支付的合理费用。

十四、不可抗力

14.1 任何一方因不可抗力不能履行合同的，应及时通知对方，并在合理期限内提供证明，采取措施防止损失扩大。根据不可抗力影响，双方依法协商部分或全部免除责任、延期履行或终止合同。

14.2 网络攻击、软硬件故障、人员短缺、第三方服务故障等属于乙方按合同应当预防、处置或具备替代保障能力的事项，除符合法律规定的不可抗力构成要件外，不当然构成免责事由。

十五、争议解决

双方因签订、履行本合同发生争议，应先协商解决；协商不成的，任何一方可向甲方住所地有管辖权的人民法院提起诉讼。争议期间，除争议事项外，双方应继续履行不受影响的合同义务。

十六、合同生效及其他

16.1 本合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

16.2 本合同未尽事宜，依照中华人民共和国现行法律法规、采

购文件及乙方投标文件执行。

16.3 本合同正本一式 4 份，甲方执 2 份，乙方执 2 份，具有同等法律效力。

16.4 本合同附件与正文具有同等法律效力。附件与正文不一致的，以正文为准；与采购文件实质性内容不一致的，依法以采购文件及乙方更优承诺为准。

十七、附件

17.1 本合同附件包括附件 1《网络安全责任标准协议》、附件 2《保密协议》、附件 3《信息系统运维工作考核细则（试行）》、附件 4《履约考核与违约责任衔接表》。

甲方(盖章)江苏省应急管理厅

甲方授权委托代表人：

地址：南京市鼓楼区浦江路 30 号鸿瑞大厦 1 号楼

乙方(盖章) 北京辰安科技股份有限公司

乙方授权委托代表人：

地址： 北京市海淀区丰秀中路 3 号院 1 号楼-1 至 5 层 305

开户银行：中国建设银行北京上地支行

账号：1100 1045 3000 5300 6765

签订日期：2020 年 9 月 5 日

附件 1

网络安全责任标准协议

甲　方：江苏省应急管理厅

乙　方：北京辰安科技股份有限公司

根据《中华人民共和国民法典》及《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等有关法律法规及规范性文件的规定，双方经协商一致，就运维信息平台的服务项目（可选填：①建设信息系统或云平台<以下统称“信息平台”>；②运维信息平台；③检查、监测、测评信息平台；④采购使用云计算服务；⑤采用社会网络平台提供对公服务；⑥采用社会网络平台发布政务信息；⑦采用社会网络平台实施社会管理；⑧采用社会网络平台处理党政事务；⑨其他信息技术）（以下简称“本服务项目”），签订本网络安全责任协议。

一、甲方的权利和义务

1. 本服务项目中产生的政务数据、系统运行数据及收集的个人信息等数据资产（以下简称“外包数据资产”）归甲方所有，甲方可以随时访问、利用、支配该数据资产；同时，乙方应采取必要技术措施防范该数据资产的泄露和流失。

2. 甲方建立对本服务项目的常态化网络安全监督管理，可采取随机抽查、派驻人员或委托第三方机构等方式，对本服务项目网络安全管理情况开展常态化检查评估，通报问题隐患，责令限期整改；乙方应配合检查并及时整改。

3. 甲方应提供乙方必要的工作条件，并按照最小必要原则授予乙方提供服务所需的相应权限，授权期满后及时收回相关权限，乙方应予以协助配合，不得设置后门程序或者恶意程序。

4. 本服务项目终止时，甲方要求乙方销毁或转让相关数据，乙方应予以配合实施，并向甲方提供《网络安全承诺书》，承诺采取必要措施保证相关数据不可恢复，不私自留存、非法买卖或提供给第三方，不公开、披露、利用在服务中知悉的各类信息，否则乙方应承担一切法律责任。

5. 在接受服务过程中，甲方发现乙方存在如下情形之一的，可以单方解除

服务合同，且仅支付乙方相应服务期限内合理费用的 80%；乙方应及时返还多收取的价款：

（1）乙方规模能力、经营范围、资本构成、高管背景、技术水平、安全团队以及企业信用等方面发生重大变化，可能造成本服务项目存在重大网络和数据安全风险的；

（2）乙方（含相关工作人员及委托服务的第三方）因涉嫌违反网络安全、数据安全和个人信息保护相关法律法规，正接受有关主管部门立案调查（乙方应主动告知甲方该情况），甲方经评估后认为，乙方继续本服务项目可能存在重大网络和数据安全风险的；

（3）因乙方对服务合同中约定的网络和数据安全保护措施建设、使用不到位等，导致发生网络和数据安全事件，或者产生网络和数据安全风险隐患被省级以上有关主管部门通报的；

（4）乙方违反本协议的约定、承诺或保证，尚未造成严重后果，甲方责令限期整改，乙方拒不整改或者整改不到位的；

（5）因乙方原因造成重大网络舆情的。

6. 在接受服务过程中，甲方发现乙方存在如下情形之一的，可以单方解除服务合同，并要求乙方返还全部合同价款，同时追究乙方的法律责任；乙方应及时返还已收取的合同价款：

（1）在服务合同签订前的三年内，乙方因违反网络安全、数据安全和个人信息保护相关法律法规，受到过行政处罚、刑事处罚，或者仍在接受有关主管部门立案调查，但未主动告知甲方该信息的；

（2）乙方在本服务项目中的相关管理人员、操作运维人员经公安或国安部门背景审查存在问题，甲方要求乙方更换相关人员，乙方拒不更换的；

（3）违反网络安全、数据安全和个人信息保护等相关法律法规，拒不按照甲方要求改正、补救的。

（4）违反网络安全、数据安全和个人信息保护相关法律法规的规定，或者违反本协议的约定、承诺或保证，导致本服务项目发生重大网络和数据安全事件，或造成其他严重后果的。

二、乙方的权利和义务

1. 在签订服务合同前，乙方应向甲方如实、完整提供其规模能力、经营范围、资本构成、高管背景、技术水平、安全团队、信用等级等经营管理信息，以及近三年因违反网络安全、数据安全和个人信息保护有关法律法规规章而受到约谈、行政处罚或刑事处罚等信息；未经乙方同意，甲方不得公开或向第三方提供上述信息。

2. 乙方应当严格按照网络安全、数据安全和个人信息保护相关法律法规、国家标准及政策文件的规定提供相关服务，确保外包数据资产的保密性、完整性、可用性。

3. 乙方应建立相对独立的管理技术团队，具体提供服务的相关人员应为乙方正式员工，并指定网络安全负责人。

4. 乙方不得转包、分包合同任务；确需分包的，应报经委托单位同意，并在分包合同中明确相应的网络安全义务和责任，但不得对合同任务主体和关键部分进行分包。

5. 乙方应严格按照法律法规规定及服务合同约定，收集、使用、存储、处理数据和个人信息。

6. 乙方应将政务数据与其他数据分开存储、处理，未经甲方同意，不得变更用途、用法，不得访问、修改、公开、披露、利用、转让、销毁、私自留存或向第三方提供；合同终止时，应当按照甲方的要求及时处理。

7. 乙方在本服务项目中涉及采购相关产品和服务的，应当严格遵守如下规定要求：

（1）建设政务信息平台的，应当优先采用安全可信的软硬件产品；确无相关安全可信产品的，应当研究制定针对性措施防范安全风险；

（2）建设云平台的，应当选择供应链来源可靠的云平台管理软件、业务系统以及服务器 CPU、操作系统、数据库等；

（3）使用云计算服务（含 PaaS、IaaS、SaaS 等）的，应当按要求采用安全可信的云计算服务，并明确云服务商的网络和数据安全责任；

（4）使用商用密码的，应当符合国家密码管理规定。

8. 乙方发现本服务项目中存在网络安全漏洞、缺陷或其他严重网络安全风险，应及时向甲方报告，或者直接向同级网信、公安部门报告；未经网信或公安部门同

意，不得公开或向第三方提供。

9. 乙方应严格落实相关开放性、兼容性标准和规范要求，优先采用通用系统解决方案，避免因采用特定的技术架构、应用接口、数据格式等，导致后续扩建、运营、维护等被绑定，形成技术壁垒或者市场垄断而引发重大技术风险。

10. 乙方发生业务转型、合并重组、投资并购等重大事项，或者管理技术团队人员发生重大变更，可能影响服务项目的网络和数据安全的，应提前向甲方报告。

11. 乙方建设、运维的政务信息平台注册用户超过100万人或者涉及人民群众出行、教育、求职、医疗、缴费等重要业务，乙方应每年向甲方提交网络安全报告，报告至少包括网络安全管理、数据安全管理、平台关键软件和核心硬件供应链安全、管理技术团队变化等情况。

12. 乙方应定期组织本服务项目相关人员开展网络安全培训，规范安全操作规程，增强安全风险意识，不断提升相关人员网络安全防护能力水平。

13. 乙方应积极配合网信、公安、审计、保密、密码管理等部门开展网络安全检查、测评、审计等监督管理工作，如实、完整提供相关网络安全管理情况，不得拒绝、隐匿、瞒报。

14. 乙方应当严格遵守并履行《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等有关法律法规中的相关规定和法定义务。

三、违约责任

1. 乙方违反网络安全、数据安全和个人信息保护相关法律法规，或者违反本协议约定、承诺或保证的，甲方应当结合问题性质、事件等级、影响范围、持续时间、数据影响、乙方责任程度和整改情况进行处理。一般性隐患或者未造成严重后果的问题，以限期整改、专项排查、增派人员、提高监测频次和考核扣分等措施为主；构成严重违约或者重大违约的，按照主合同第九条规定处理，可以部分或者全部向履约保函开立机构提出索赔；造成甲方损失的，乙方应当依法赔偿。

2. 因甲、乙双方共同责任造成甲方损失的，乙方须按比例承担相应的法律责任。

四、协议期限与生效

与服务合同起止期限相同，但相关法律法规规定的网络和数据安全责任义务不受该期限的限制。本协议自甲乙双方盖章之日起生效。

甲方（签盖）

江苏省应急管理厅

甲方代表：

日期：2026年9月5日

乙方（签盖）

北京辰安科技股份有限公司

乙方代表：

日期：2026年9月15日

附件 2

保密协议

甲方：江苏省应急管理厅

乙方：北京辰安科技股份有限公司

因乙方接受甲方 自然灾害综合监测预警系统国产化改造及运维 任务，乙方同意保守甲方的保密信息并遵守下列条款：

一、**保密内容**

1、本协议所约定的“**保密信息**”指乙方因参与甲方负责或组织的项目建设、运维、咨询、评审验收等工作，直接或间接的通过甲方途径获得、使用、浏览、存储的**信息资源**和**技术资源**。

1）“**信息资源**”指乙方在完成该项工作过程中所使用或可能接触到的不属于乙方所有的信息。

2）“**技术资源**”指乙方在完成该项工作过程中所使用或可能接触到的不属于乙方所有的产品、工具、方案、方法、手段、数据、结果、报告、设备、计算机软件、账号、密码、协议、参考资料、功能界面、说明书等；

2、“**保密信息**”包括（但不限于）书面的、口头的、图形的、电磁的或其他任何形式的信息。

二、**保密义务**

1、乙方对**保密信息**负有保密义务，不得侵害、外泄或以任何直接或间接的方法使任何第三人知悉或使用。一切以直接、间接、口头或书面等形式提供涉及保密内容的行为均属泄密。

2、凡存储或曾经存储过**保密信息**的介质，均属保密介质。乙方保证保密介质的使用安全，做好保密介质的管理工作，不能随意摆放。

3、乙方保证参与甲方工作过程中严格遵守甲方关于网络安全的相关规定。所使用的电脑软、硬件设施都满足甲方的安全要求；需要在政务内网工作时，做好政务内网与外网的隔离，连入政务内网的机器、存储设备不能接入外网。

4、乙方结束甲方委托的工作时，要销毁工作期间使用的相关纸质文件和电子文档，不能保存与**保密信息**相关的文件。

5、因乙方违反上述协议或管理不当造成**保密信息**泄露，甲方将立即书面通知乙方所属单位和乙方，并据此终止乙方在甲方的工作，且乙方愿意承担民事和法律责任并赔偿甲方的损失。

三、保密期限

对于国家有明确规定的**保密信息**，按国家规定执行；对于国家没有明确规定的**保密信息**，需永久保密。

四、其他条款

1、本协议书各条款相互独立，不因本协议书内任一条款无效而使本协议全部或一部分失效。

2、本协议书一式贰份。甲、乙双方各执壹份，具备同等的法律效力。

3、本协议书自工作开始之日起生效。

甲方（签盖）

江苏省应急管理厅

甲方代表：戴新立 王正宁

日期：2026 年 9 月 5 日

乙方（签盖）

北京辰安科技股份有限公司

乙方代表：

日期：2026 年 9 月 5 日

附件 3

信息系统运维工作考核细则（试行）

为加强厅局信息系统运行维护管理，规范日常运维工作，保障厅局信息系统安全高效运行，根据厅局《信息系统运维管理办法》特制定本细则。

一、指导思想

通过建立定性定量指标体系对各运维支撑单位进行评分、评级，加强信息系统运维工作规范化、专业化、流程化，提高运维技术支撑单位工作质效，确保信息系统稳定运行。

二、适用对象

本细则适用于厅局机关投资建设的各类信息系统，包括信息化基础设施、业务系统、内部管理系统及为保障信息系统运行所建立的信息化支撑体系。

三、评分评级办法

评分总分为100分，评级分为4个等级(A B C D)，和评分具体对应如下表：

分数范围	评　级
90-100	A
80-90（不含）	B
70-80（不含）	C
70以下	D

系统类：

系统类项目评分由六部分组成——文档管理分、项目质量分、运维质量分、处室评价分、网络安全专项扣除分、服务加分项。每项得分总分均为100分，其中文档管理分占权重20%，项目质量分30%，运维质量分40%，处室评价分10%。系统运维情况的评分、评级结论将作为合同付款及后续厅局其他系统招标的重要参考依据。

（一）文档管理分

新建项目需要根据规定，建立项目文档管理库，在系统开发不同阶段提交不同的文档并根据项目更新进行实时迭代。在需求分析阶段需提交软件规格需求说明书和开发实施方案；在系统设计阶段需提交系统概要设计说明书、详细设计说明书、数据库设计说明书、接口规格说明书；在开发阶段需提交开发环境搭建视频与使用手册、及时提交更新代码、补充代码注释；测试阶段需提交软件测试报告；部署与交付阶段需提交系统运维手册/方案、用户使用手册。

已建系统需补齐所有阶段所需提交的文档，中心将根据文档总体情况进行打分。

针对运维技术支撑单位，每年年终进行一次评分。

（二）项目质量分

项目质量分满分100分，主要考核系统建设公司和维保

公司所交付的项目质量水平，包括4个方面内容：代码有效注释率（30 分）、项目与文档的一致性（30 分）、数据落地（30分）及资源监控的情况（10分）。

代码注释率方面：新建系统必须按照细则要求，在代码的关键和复杂部分添加注释，且代码注释覆盖率大于30%。已开发系统应按照要求补齐代码注释。

项目与文档一致性方面：服务方维保过程中交付的代码内容、组件版本、基础配置等要和文档严格一致。

数据落地方面：建设和运维单位，应保证存量及后续迭代开发的增量数据全部及时、完整地落入数据资源池。

资源监控方面：系统应具备设备资源监控的能力，在资源占用率过高、通讯接口中断等异常情况下，以短信方式通知项目经理和中心系统运维负责同志。

（三）运维质量分

运维质量初始分为100分，具体扣分判定标准如下：

1、运维响应速度

响应超时（5 分）：系统出现问题后，服务方响应时间超过1小时。

问题解决延迟（5 分）：系统出现问题后，服务方未能在4小时内修复问题或提出限时解决方案。

服务改进滞后（5 分）：服务方未能根据反馈时间节点及时改进服务。

服务改进有效性（5 分）：服务方根据要求修改后，未能达到甲方要求，或未能有效修复问题。

2、故障严重程度

故障影响面（8 分）：用户数超 100 人的系统发生 2 小时以上的故障。小于 100 人的系统扣 4 分。

3、系统稳定性

系统频繁故障（10 分）：1 个月内出现 2 次及以上系统故障，影响业务连续性。

4、服务质量

处室投诉（5 分）：因服务方服务质量问题导致的处室投诉。

5、服务连续性管理

服务水平协议未达成（10 分）：服务方未能满足合同中规定的服务水平协议要求。

6、变更管理

变更未评估（3 分）：服务方在进行系统变更前未进行充分评估，导致系统不稳定。

变更未通知（3 分）：服务方在进行可能影响厅局业务正常开展的系统变更时未提前通知甲方。

变更未达预期效果（5 分）：变更前未做好版本测试，导致变更失败或变更未达预期效果。

7、人员培训和管理

人员技能不足（5 分）：服务方运维人员缺乏必要的技能和资质，影响服务质量。

人员流动率高（5 分）：服务方运维团队人员年度内流动率高（≥30%），导致服务连续性受到影响。

条件不满足（10 分）：服务方未按合同要求配备驻场人员，如使用相同人员履行厅内多个驻场服务等。

8、沟通和协作

沟通不畅（3 分）：服务方与厅局沟通不及时，导致信息传递不畅和误解。

协作不力（3 分）：服务方在跨部门协作时表现出协作不力，影响问题解决效率。

9、日常巡检

巡检至少每两周一次，年终评分时年度总巡检记录不低于 24 次，少 1 次扣 3 分；每月巡检不低于 2 次，少 1 次扣 3 分。

10、信息化运维能力

自动化运维（5 分）：服务方未实施自动化运维工具，不能够持续监控系统性能和健康状态，且未和厅内短信平台对接。监控内容包括但不限于：应用服务器、中间件、网络硬件设备、数据库服务器等。

11、灾难恢复计划

未制定灾难恢复计划（5 分）：服务方未制定详细的灾难恢复计划，未定期进行演练。

（四）处室评价分

处室评价包含系统功能的完整性、流畅性、准确性、服务方人员专业素养、服务方响应积极性、后期维保的完成度等方面内容。若系统维保工作涉及多个处室，则每个处室均出具一份评价表打分，最终得分取平均分。

系统脱保交由专业维保公司后，评分方式与对原建设公司评分方式相同，每年进行一次。

（五）网络安全专项扣分

省厅高度重视网络、数据安全及信息系统保密工作，网络安全工作是信息系统运维工作的底线、红线，此栏目所涉及的扣分项直接作用于考核总分，不再进行加权计算。

网络安全事件（3 分）：存在安全漏洞被网信、公安、保密等单位通报的，每出现一次扣 3 分。

安全防护缺失（2 分）：服务方未能按照厅局或政务云要求落实基本的安全防护措施。

存在高危漏洞（2 分）：在厅局自行组织的安全检查中，服务方系统存在高危漏洞，每出现一次扣 2 分。

未提供网络安全（数据安全、信息保密）承诺（2 分）：在运维服务过程中，未按照省厅要求提供网络安全、数据安全、保密承诺等。

材料信息不匹配（8 分）：提供的人员材料如无犯罪记录等存在造假，或人证不对应的情况。

数据丢失（10 分）：因服务方原因导致数据丢失或损坏。

数据泄露（15 分）：因服务方原因导致敏感信息泄露。

（六）服务加分项

主动服务（10 分）：服务方主动通过技术创新、服务升级等方式，超额完成运维服务并对运维服务质效有正向推动的，科信处、应急管理服务中心将视情况进行加分，

加分项不计入加权，一个服务周期内最多加分一次。

（七）评级说明

评价得分计算公式=0.2*文档管理评分+0.3*项目质量分+0.4*运维质量分+0.1*处室评价分-网络安全扣分项+服务加分项。

服务类：

服务类项目评分总分为100分，由六部分组成——服务方案分、服务质量分、档案管理分、处室评价分、网络安全专项扣分、服务加分项。每项得分总分均为100分，其中服务方案分占权重15%，服务质量分50%，档案管理分25%，处室评价分10%。

（一）服务方案分

服务方案分总分100分，重点评估服务方案的系统性、合规性和可操作性，主要从方案完整性、逻辑严谨性、与合同条款一致性三个维度评分，确保服务实施的基础规范性和风险可控性。

扣分项：

1、服务方案未满足省厅要求（10 分）。未能完全理解省厅服务要求梳理服务计划清单，每缺少或不满足一项扣10分。

2、人员配置信息缺失（8 分）。未提供服务团队（含驻场人员）人员配置信息（含人员学历、专业、职称、资质证明、岗位职责、工作任务等）。

3、应急响应预案缺失（8 分）。未按要求编制《应急

响应预案》（含风险清单、应对措施、应急响应流程等）。

（二）服务质量分

1、服务质效

响应超时（5 分）：甲方提出服务需求后，服务方响应时间超过 1 小时。

问题解决延迟（5 分）：服务出现问题后，服务方未能在 4 小时内修复问题或提出限时解决方案。

服务改进滞后（5 分）：服务方未能根据反馈时间节点及时改进服务。

处室投诉（5 分）：因服务质量问题导致的处室投诉的。

服务流程不到位（8 分）：未按合同约定执行服务流程，每次扣 8 分。

故障事件（20 分）：因服务方服务质量问题导致出现影响甲方正常工作的故障事件。

服务内容不符合（10 分）：服务内容和服务方案存在不匹配，每不满足/缺少一项扣 10 分。

2、人员管理

人员技能不足（5 分）：服务方运维人员缺乏必要的技能和资质，影响服务质量。

人员流动率高（5 分）：服务方运维团队人员年度内流动率高（≥30%），导致服务连续性受到影响。

条件不满足（10 分）：服务方未按合同要求配备驻场人员的。

资质缺失（5 分）：服务人员资质不符合合同要求，每

人次扣5分。

行为违规（5 分）：驻场服务人员存在不符合省厅运维服务规定的行为。

（三）档案管理分

服务档案缺失（5 分）：巡检记录、服务记录、培训材料、问题清单、服务过程会议纪要、问题跟踪单、问题处置单等未通过厅内运维管理平台归档，每项扣5分。

（四）网络安全专项扣分

网络安全事件（10 分）：因服务方服务问题导致省厅被公安、网信、保密部门通报的。

安全防护缺失（2 分）：服务方未能按照厅局要求落实基本的安全防护措施。

未提供网络安全（数据安全、信息保密）承诺（-2分）：在运维服务过程中，未按照省厅要求提供网络安全、数据安全、保密承诺等。

数据丢失（10 分）：因服务方原因导致省厅数据丢失或损坏。

数据泄露（15 分）：因服务方原因导致省厅敏感信息泄露。

（五）处室评价分

处室评价包含服务方人员专业素养、服务方响应积极性、服务的完整度等方面内容。若服务工作涉及多个处室，则每个处室均出具一份评价表打分，最终得分取平均分。

（六）服务加分项

主动服务（10 分）：服务方主动通过技术创新、服务升级等方式，超额完成运维服务并对运维服务质效有正向推动的，科信处、应急管理服务中心将视情况进行加分，加分项不计入加权，一个服务周期内最多加分一次。

（七）评级说明

评价得分计算公式=0.15*服务方案分+0.5*服务质量分+0.25*档案管理分+0.1*处室评价分-网络安全专项扣分+服务加分项。

四、结果运用

评分等级作为履约保函返还、延期或者索赔的重要依据。评级为A或B，且乙方已完成全部合同义务和整改事项的，按约返还履约保函。评级为C的，原则上先责令专项整改；整改完成、未造成严重后果的，可以不提出索赔，存在严重违约、同类问题反复发生或者整改不到位的，可以部分索赔。评级为D的，应当根据违约性质、实际影响、乙方责任程度和整改情况，决定不提出索赔、部分索赔或者全部索赔；存在拒不履行主要合同义务、重大网络安全或者数据安全事件、弄虚作假、拒绝移交，或者违约致使合同目的不能实现等重大情形的，可以全部索赔。有关通报、监管处理等事项，按照法律法规和规定程序办理。

附件 4

履约考核与违约责任衔接表

违约等级	触发条件	处理原则
一般违约	根据《信息系统运维工作提示制度（试行）》规定，达到工作提示情形的，省应急管理服务中心向乙方下发《信息系统运维工作提示通知书》。	责令限期整改；可以要求重新履行、补齐材料、补足服务工时或者采取其他必要补救措施；不向履约保函开立机构提出索赔。
较重违约	根据《信息系统运维工作警示通知制度（试行）》规定，达到工作警示情形的，省应急管理服务中心向乙方下发《信息系统运维工作警示通知书》。	限期提交原因分析和专项整改报告；可以要求增派或者更换人员、提高巡检和值守频次、乙方负责人到场；原则上不向履约保函开立机构提出索赔。
严重违约	根据《信息系统运维工作督办制度（试行）》规定，达到工作督办情形的，省应急管理服务中心向乙方下发《信息系统运维工作督办通知书》。	实行专项督办并要求乙方负责人到场；根据问题影响、乙方责任程度和整改情况，可以按照主合同规定程序向履约保函开立机构提出部分索赔。
重大违约	发生重大网络安全或者数据安全事件、严重影响重要业务、拒不履行主要合同义务、弄虚作假、拒绝移交，或者严重问题久拖不改，江苏省应急管理服务中心向省厅科信部门报告，由科信部门对相关单位进行约谈。	根据事件的影响程度，可以按照主合同规定程序向履约保函开立机构提出部分或者全部索赔。