怀柔区突发事件预警信息发布管理系统开发项目合同

项目名称：怀柔区突发事件预警信息发布管理系统开发

甲　　方：北京市怀柔区气象局

乙　　方：中企动力科技股份有限公司

签订地点：北京

甲　　方：北京市怀柔区气象局

法定代表人：伍永学

注册地址：北京市怀柔区怀柔镇刘各长村 433 号邮政编码：101400

电　　话：/

传　　真：/

乙　　方：　中企动力科技股份有限公司

法定代表人：陈鸣飞

注册地址：　北京市北京经济技术开发区地盛西路 1 号 1 幢 A 区 5 层 A2-501 室

邮政编码：　100176

电　　话：　400-660-5555 传　　真：　400-660-5555

账户名称：　中企动力科技股份有限公司开户行名称：　招商银行股份有限公司北京中关村支行

帐　　号：　110906724110808

账户性质：一般户

甲乙双方经友好协商，就乙方向甲方提供怀柔区突发事件预警信息发布管理系统开发项目实施开发工作的有关事宜达成一致意见，根据《中华人民共和国民法典》等相关法律法规，订立本合同，以兹共同遵守。

一、 **项目概况**

1.1 项目名称：怀柔区突发事件预警信息发布管理系统开发。

1.2 项目内容：乙方可提供的服务涵盖项目管理、界面设计、技术开发、年度运维四类服务；本合同项下，甲方委托乙方提供的具体服务品类、各类服务的详细内容、价格标准以及相关履约规则等，均以附件一《服务方案》为准；

二、服务总价款及付款方式

2.1 本协议项下合同总金额为包含税费后的总价共计：1705800 元整（大写金额人民币：壹佰柒拾万伍仟捌佰元整）（在本合同中简称为“合同价款”）。

2.2 本合同一切费用均以人民币公对公转账结算，不接受承兑汇票等其他付款方式。

2.3 项目款结算方式及付款进度：

（1） 双方签订合同后，甲方按照合同总价（含税）分三次付款给乙方，每一次付款前，乙方均需提前向甲方开具等额合法有效的增值税专用发票，甲方以银行转账的方式向乙方付款。

（2） 如在本协议签订之后的执行期间，财政部、国家及地方税务机关推出了适用于本协议的新的税、费种类，或者财政部、国家及地方税务机关对现行的适用于本协议的税、费征收范围等等有关项目进行了调整，则乙方按新税法规定开具相应增值税发票。

（3） 付款进度：

首次付款：合同签订后 20 个工作日内，甲方支付合同总价（含税）的 **50%**，即 852900 元整（大写金额人民币捌拾伍万贰仟玖佰元整）。

第二次付款：乙方完成甲方项目整体需求规划和全部界面静态 UI 设计（平面稿），经甲方验收合格并完成交付后 20 个工作日内，甲方支付合同总价（含税）的 30%，即 511740 元整（大写金额人民币伍拾壹万壹仟柒佰肆拾元整）。

第三次付款：技术开发部分制作完成，且在测试环境中经甲方验收合格后，甲方于 20 个工作内向乙方支付合同总价（含税）的 20%，即 341160 元整（大写金额人民币叁拾肆万壹仟壹佰陆拾元整）。

（4） 乙方收到全部合同款项后 3 个工作日内，配合甲方将项目部署到指定服务器，甲方向乙方签发《项目交接单》。甲方签发《项目交接单》后，乙方开始提供项目年度运维服务（如有）。

三、项目实施流程

3.1 项目开发

（1） 项目需求方案经由双方书面确认之后，甲方应避免对需求的更改，以免影响及拖延整体工作进度，如确有需要，应与乙方协商解决，并签订项目的补充协议。

（2） 如果在程序验收后（甲方签署《项目验收单》）该内容有所变更，甲方应当向乙方提出书面变更要求，经双方签订《项目补充协议》后，增加部分的费用按照乙方收费标准相应收取。

（3） 项目变更：项目每一阶段里程碑均代表项目进行的标志性关卡，甲方对乙方的交付成果进行签收后进行的变更均属需求变更或新增需求。

3.2 项目测试

（1） 测试在乙方的服务器运行。测试内容为合同中的需求部分。甲方代表收到测试申请后，在 5 个工作日内组织有关部门测试，甲方应在《项目进度工期表》中规定的测试期限内完成测试工作并提供书面的《测试报告》，如在测试期限内未提供书面的《测试报告》，则视为测试通过，乙方不再接受修改意见。

（2） 如果遇到特殊情况导致测试期推延，甲方应以书面方式通知乙方。

四、项目验收与交接

4.1 验收依据：验收将以附件一《服务方案》、甲方签署的《项目需求确认单》或双方确认的需求邮件为依据。

4.2 项目工期起算：自甲方支付首付款、提供项目制作所需资料，并由双方最终确认项目需求，以双方《项目需求确认单》达成一致的次日开始计算工期，具体进度以附件二《项目进度工期表》作为标准。

4.3 验收流程：当乙方的项目阶段性实施完成且具备验收条件时，乙方提出验收申请，甲方代表收到验收申请后，在 5 个工作日内组织有关部门验收并提供书面反馈意见，如甲方在 5 个工作日内未提供书面反馈意见，则视为验收通过。当乙方的项目实施全部完成且具备验收条件时，乙方提出验收申请，甲方代表收到验收申请

后，在5个工作日内组织有关部门验收并提供书面反馈意见，如甲方在5个工作日内未提供书面反馈意见，则视为验收通过。

4.4 整体检验及阶段性验收的标准详见《项目需求确认单》或需求确认邮件。

4.5 项目交接：甲方按照本合同付款约定支付全部合同款项后，乙方将工作成果交付给甲方，甲方签发《项目交接单》。

五、项目运维

5.1 本合同项下，如甲方实际采购的服务品类包含年度运维，则年度运维的服务期限自甲方签发《项目交接单》之日起算。

5.2 年度运维服务期限届满前，甲方应提前续费，如服务期限届满仍未续费的，则乙方不再提供相应服务。合作期限内，如甲方决定不再续费的，则应当在运维服务到期前自行备份相关数据、妥善处理迁移工作，如因甲方未及时续费导致平台无法访问、产品服务中断、数据丢失等问题，甲方自行承担责任和后果。

5.3 如甲方擅自对项目源码（包含不限于前后端源代码）进行独立修改及/或迁移服务器，则将视为甲方放弃所有售后权益，乙方不再对本项目提供本合同项下的年度运维服务及售后支持，双方另行协商一致的除外。

5.4 因乙方项目开发过程中涉及到的所有技术服务都围绕甲方身份展开的，项目交付使用后，乙方仅面向甲方提供相关运维服务；如平台所有者发生变更而产生的平台改版费用，不属于平台常规改版范畴亦不属于运维服务范畴，乙方有权单独定价，双方另行签约付费。

六、双方的权利和义务

6.1 甲方的权利和义务

（1） 甲方应提供本项目实施的必要条件和准备。

（2） 甲方应及时向乙方免费提供双方一致确定的本项目实施所必要的基础数据、文档、文件、测试数据、示例输出，或其他信息和资源。系统中属于数据库范畴的，其数据整理与录入由甲方负责，甲方需自我审查数据的合法性。甲方应保证提供的所有该类数据、材料以及信息的内容的准确性、完整性和统一性，且不会侵犯任何第三方的知识产权，因以上资料的瑕疵、侵权责任由甲方承担，如因此对乙方造成损失的，甲方应赔偿损失。

（3） 甲方应指定联系人负责与乙方联络、协调、提出修改意见、传递文件、签署确

认验收文件等。甲方变更联系人时，必须及时书面通知乙方，否则造成的损失，由甲方自行承担。

（4） 本项目合同履行完毕且甲方支付全部合同款项后，系统程序模块管理及使用权属于甲方。甲方不得将系统程序模块向第三方提供、销售、出租、出借、转让或提供许可、转许可、通过信息网络传播或以其他形式供他人使用。甲方不得对系统进行翻译、分解、反向编译、反汇编、反向工程或进行其他试图从系统程序模块导出程序源代码的行为，或在系统程序模块的基础上书写或开发衍生软件、衍生产品或其他软件。甲方不得限制、破坏或绕过系统程序模块附带的加密附件或乙方提供的其他确保系统正确使用的限制性措施。甲方不得将系统程序模块用于除甲方内部使用以外的其他目的，包括但不限于向第三方提供数据处理服务、应用服务、商业共享或其他共享安排。甲方不得除掉、掩盖或更改系统程序模块有关许可或商标的标志。

（5） 甲方利用乙方提供的产品接入互联网进行经营活动须办理备案、报批、行政许可手续的，甲方应事先取得国家相关机关的批准、许可或者备案；甲方应遵守《计算机信息网络国际联网安全保护管理办法》规定，自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续，否则由此产生的法律责任由甲方自行承担，且乙方有权通知甲方改正，如果甲方拒不改正乙方有权暂停甚至终止服务不退还任何费用，由此产生的责任由甲方承担。

（6） 项目制作期间，甲方有权提出修改意见，甲方提出的修改意见和特殊要求必须在本项目约定的范围内，超出本项目约定范围经乙方确认的，甲方需另行支付相关费用；甲方对各段工作验收/确认后，若提出页面设计风格、配色、结构等方面修改的，甲方应承担项目返工带来的相关费用；甲方服务需求超出项目合同范围的，双方应友好协商解决，另行签署《项目补充协议》。

（7） 本合同生效后甲方需要增加项目语言版本或新增需求另行商议费用并签署补充协议。

（8） 甲方必须保证使用乙方产品不违反国家法律法规的规定，且不侵犯任何第三方的合法权益；如有违反，乙方有权停止提供相关服务并单方解除本合同，所收全部项目款项不予退还，甲方还须赔偿由此给乙方造成的全部经济损失。

（9） 如因甲方域名（包括但不限于域名掉线、域名侵权等）、服务器等问题导致已经交付系统无法使用等问题，由甲方自行负责，乙方不承担任何责任。

（10） 如本合同项目的开发实施涉及到第三方产品、第三方技术支持（包括但不限于第三方提供的域名、服务器、小程序等），如因第三方提供的产品及/或技术支持导致的本项目平台展示错误、不能展示、账号关停、网络中断等相关或类似问题，则甲方自行承担因此导致后果和损失，与乙方无关，乙方无需因前述情形向甲方退还任何款项。

6.2 乙方的权利和义务

（1） 在甲方按本合同约定履行了付款义务并提供项目制作所需全部资料且经乙方确认后，乙方开始进行项目界面的设计制作。

（2） 甲方同意，本合同的签署意味着甲方授权乙方仅限于为完成本项目合同目的可以使用甲方的名称、商标、域名、企业标志等，并保证此等使用不损害甲方利益。

（3） 对于乙方为完成委托项目使用的图片、字体、视频或其他形式作品，由甲方负责提供。如果甲方无法提供，需购买或租用第三方图片、字体、视频或其他形式的作品，乙方负责向甲方提供选择方案，甲方选择了第三方图片、字体、视频或其他形式作品，甲方可直接向第三方购买（或由乙方代购），由甲方支付相关费用。如因甲方未支付该费用即使用第三方图片、字体或其他形式的作品而发生版权纠纷的，由甲方承担责任。

（4） 乙方应在项目工期内完成相应阶段工作并通知甲方签收，期间如甲方对内容做出修改或变更经乙方确认的，则乙方有权根据实际情况适当延长周期，甲方应按乙方要求进行验收并签署相应验收单。若甲方在签收期限内提出合理的书面修改意见经乙方确认的，乙方应予以修改并再次通知甲方验收。

（5） 若甲方在验收期限内未验收完毕，也未提出书面修改意见的，视为甲方已经验收合格。

（6） 如因甲方原因（包括但不限于未能及时提供资料或者不能提出书面修改意见要求修改等）致使乙方未能如期进行或完成工作的，相应周期须重新计算或延长。。

七、保密条款

7.1 任何一方对于本合同履行过程中所知悉的对方商业秘密（包括技术信息和经营信息）负有严格保密义务。未经对方事先书面授权，另一方不得将其泄露给任何非项目组人员，法律法规或政府部门要求的除外。

7.2 本合同各方的保密义务不因本合同的终止、解除而终止。

八、违约责任

8.1 甲方未按规定时间履行付款义务超过 20 个工作日，则每逾期一日，按未付款金额的 0.01%（大写：万分之一）计算违约金，但最高不得超过逾期付款金额 3%，并承担由此对乙方造成的实际损失。

8.2 如甲方未按本协议 2.3 条约定的时间节点履行对应的付款义务，则乙方有权暂停提供后续节点的设计/开发/部署/交接/运维服务，而不构成违约；前述情形发生后，项目工期相应顺延，甲方自行承担因此导致的风险和损失。

8.3 因乙方原因造成不能按合同附件工期要求提供本合同约定的项目开发服务，超过 20 个工作日，则每逾期一日，按甲方已付款项的 0.01%（大写：万分之一）计算违约金，但最高不得超过甲方已付款项的 3%。

8.4 项目需求方案经由双方书面确认之后，甲方应避免对需求的更改，项目需求方案以附件一《服务方案》内容为准，如在开发过程中甲方要求变更项目需求方案，则乙方有权暂停项目开发工作而不构成违约，同时乙方重新梳理项目需求并向甲方重新报价，双方就此另行签订增项/变更补充协议，前述情形下原工期暂停计算直至增项/变更协议签订完成后项目重新启动；如甲方未予配合前述事宜，视为双方未能就项目需求变更达成一致，则乙方有权选择：（1）继续按照本合同约定交付项目成果，或（2）单方终止合作且不退还甲方已付款项。

8.5 无论本合同其他条款如何约定，任一方均不向对方承担因本合同造成或与本合同有关的任何预期收入或利润损失、商誉丧失、间接或附带损失的赔偿责任。

九、合同的变更和终止

9.1 对本合同的任何修改和变更，均应经双方协商一致且以书面形式进行确认。

9.2 甲乙双方经协商一致可签订书面协议终止本合同。

9.3 任何一方提出终止合同要求的，必须提前三十（30）天以书面形式通知，在取得对方的书面同意后方能终止本合同，但本合同任何一方依法对违约方行使终止合同

权利的，不受此限。

9.4 甲方或乙方如终止营业或进入破产程序，另一方可单方解除本合同，但必须以书面形式通知对方，且不受本合同第十二章中有关通知期限的限制。

9.5 如甲方违反本合同约定单方要求终止合同的，对于截止终止生效之日前乙方已经履行的工作，甲方应该支付相应的服务费用，具体额度按照服务费标准及具体服务时间进行计算。

十、不可抗力

10.1 因不可抗力使得本合同的履行不可能、不必要或者无意义的，任何一方均可以解除本合同。遭受不可抗力、意外事件的一方全部或部分不能履行本合同、解除或迟延履行本合同的，应将事件情况以书面形式通知另一方并向另一方提交相应的证明。

10.2 本合同所述之不可抗力系指以当事人的能力不能预见、不能抗拒、不能避免的客观情况，包括但不限于：地震、山洪、海啸、台风、战争、政府禁令、外交关系变化、其他属于不可抗力的情形。

10.3 如任何一方因不可抗力阻止、妨碍或拖延其履行本合同项下任何义务，该方应尽早书面通知另一方并说明不可抗力详情，提供有关不可抗力事件的证据。

10.4 在履行本合同中，因出现无法克服的技术困难，或者人力不可抗拒的因素，导致研究开发失败或部分失败的，由此造成的风险损失，双方均不用承担任何责任。

10.5 一方发现前款所列可能导致研究开发失败或部分失败的情形时，应当及时通知另一方并采取措施减少损失。没有及时通知并采取适当措施，致使损失扩大的，应就扩大的损失承担责任。

十一、 适用法律及争议解决

11.1 本合同的订立、履行、解释和争议的解决均适用中华人民共和国法律（不含港澳台地区）。

11.2 双方同意：如在履行本合同过程中，双方当事人对本合同的订立、解释、履行等发生争议的，各方应尽其最大努力尽快友好协商解决。

11.3 一方提出要求解决争议时应以书面形式提交对方，并说明争议事项及理由，经双方协商不成的，双方同意向被告所在地人民法院提起诉讼。

十二、 合同的生效和效力

12.1 本合同经双方法定代表人或其授权代表签字盖章之日生效，至本合同约定的双方义务履行完毕之日终止。

12.2 本合同的签订替代此前双方就本项目所有口头或书面承诺。

12.3 本合同附件为本合同不可分割的组成部分，与本合同具有同等法律效力。

12.4 若本合同的某一条款被裁决为无效，不影响本合同其他条款效力的，其他条款仍然有效。

十三、 其他

13.1 本合同中以书面、传真、电子邮件送达相关文件为合法有效的方式，对各方具有法律约束力。以传真、电子邮件送达的，一方将文件送达到双方约定传真或者电子邮箱即视为有效送达。

13.2 任何一方欲提前解除本合同，应提前 30 个工作日通知对方。本合同提前终止不影响各方于本终止日之前根据本合同已产生的权利和义务。无论因何种原因导致的本合同提前终止，对于甲方已确认的工作成果所对应的费用，乙方不予退还，如甲方已付款项不足以支付的，甲方有义务继续支付。

13.3 本合同相关附件及各阶段确认单、验收单等为本合同组成部分，与本合同具有同等法律效力。本合同未尽事宜及需要对本合同进行变更、补充的，需要签订书面补充协议，补充协议签字盖章后生效。

13.4 本合同乙方授权代表授权范围仅为签订本合同，未经乙方书面授权甲方与乙方任何人员签订协议、承诺、保证或者其他涉及本合同乙方承担义务和责任等的任何类似材料（书面或口头，内容包括但不限于系统规划，设计方案以及项目内容等），均属无效，对此发生的争议乙方不承担任何责任。

13.5 对本合同的书面补充和修改经双方授权代表签署后对双方具有约束力，并构成本合同不可分割的一部分。本合同或其任何条款、约定、陈述、保证或条件只有通过各方签署的书面文件方可补充、修改、取代或撤消或被豁免。

13.6 本合同一式肆（4）份，均为正本，甲方执贰（2）份，乙方执贰（2）份，均具有同等法律效力。

13.7 本合同及相关附件任何条款之法律效力于尚未终止前，均及于双方当事人和各自的继承人、受让人。

13.8 本合同自双方签字/盖章之日起生效。

13.9 附：附件一《服务方案》

附件二《项目进度工期表》

【以下无正文】

甲方(盖章)：北京市怀柔区气象局

法定代表人或授权代表(签字)：

签约日期：2026年5月27日

乙方(盖章)：中企动力科技股份有限公司

法定代表人或授权代表(签字)：

签约日期：2026年5月27日

附件：服务方案

项目名称:怀柔区突发事件预警信息发布管理系统开发

序号	一级类目	二级类目	相关说明	报价金额(元)
1	系统建设开发维护	技术选型	严格遵循北京市关于信创（信息技术应用创新）、网络安全等级保护（等保三级）、商用密码应用安全性评估（密评二级）及政务云部署的强制性政策要求综合研判进行技术选型。	1,462,300.00
		项目执行管理	制定项目标、把控项目进度、组织进行项目风险评估、组织制定应急计划；项目经理对项目的建设进度、质量、成本及安全负责，负责项目部内的日常管理，包括项目会议、专家研讨、项目验收等事项。	
		系统原型绘制	为该系统创建可视化模型，旨在提前呈现系统的功能界面、交互逻辑和业务流程，以在正式开发前进行沟通、验证和优化，提高系统开发执行的准确性。	
		系统页面设计	根据系统原型结构及系统信息架构，独立设计系统页面，确保界面中内容与功能之间从属关系的视觉表现，在兼顾与继承整体视觉标准及视觉形象传达一致的前提下，保障视觉表达准确性与用户体验的适用性。	
		系统页面开发	针对交互样式进行 JS 效果或 AJAX 效果实现，兼容市面浏览器。 对系统前端相应界面需要实现交互效果制作或按照 HTML5 框架标准实现网页前端交互动效。	
		系统功能开发	在信息系统建设过程中，根据业务需求和设计规范，通过编程、配置、集成等技术手段，实现软件系统各项功能模块。	
		系统用户权限开发	在信息系统建设过程中，设计并实现一套安全、灵活、可管理的用户身份认证与访问控制机制，确保不同角色的用户只能访问其职责范围内允许的功能和数据。	

		系统数据对接	在信息系统建设过程中，通过标准化接口或数据交换机制，实现本系统与外部业务系统、数据库、平台或设备之间的数据互通与共享。	
		系统测试	多维度验证系统可用性，主要包含功能测试，性能测试，安全测试，兼容性测试，可靠性测试，用户体验测试。	
		系统运维（首年）	对软件系统进行全维度运维，确保系统稳定、安全、可用，包含可用性保障，安全性运维，合规性运维，以及应急事项处理。	
2	系统培训	系统功能操作培训	对使用层面人员进行系统功能操作培训，确保“怀柔区突发事件预警信息发布管理系统”能够被高效、规范、安全地使用。	70,000.00
3	系统部署发布	政务云部署	将怀柔区突发事件预警信息发布管理系统部署在由政府主导建设或授权使用的云计算平台上，利用其提供的计算、存储、网络、安全等资源，实现系统的运行与服务。	44,000.00
		系统解析发布	该系统解析到环境并进行发布使用。	
4	等保三级软件建设	等保三级软件建设	对该系统进行信息系统安全等级保护三级的软件建设实施，并将《密评报告》报送至北京市密码管理局或怀柔区国家密码管理局分支机构备案。	58,800.00
5	密评二级	密评二级	对该系统进行密评二级相关的软件建设建设实施与密评二级的测评（具备资质的第三方密评机构执行），复评（如有）、备案等工作。	70,700.00
费用总计：				1,705,800.00
免费提供上线后三年的系统运维，次年起系统运维（对软件系统进行全维度运维，确保系统稳定、安全、可用，包含可用性保障，安全性运维，合规性运维，以及应急事项处理。）按照项目总价 8%收取。				

项目名称:怀柔区突发事件预警信息发布管理系统开发-系统建设维护开发

序号	二级类目	三级类目	详细说明	报价		
				工作量（人天）	单价（元）	金额（元）
1	技术选型	信创适配合规性研判模块	1、基础环境比选，对比统信 UOS Server V20、麒麟 V10 操作系统在政务云环境下的稳定性与驱动兼容性，确定最终的操作系统。 2、数据库选型论证：组织达梦 DM8 与人大金仓 KingbaseES V8 的压力测试（模拟 200 并发写入），结合怀柔区现有信创生态，确定数据库选型。 3、开发框架约束：后端限定使用 Spring Boot + 国产 JDK，前端采用 Vue 3 + Element Plus（信创版），禁用境外依赖库。 补充内容：该模块的工作量远超常规技术选型，是一项深度、严谨且需多方协同的专项工程，其具体工作量可分解为以下四个层面： 深度技术验证与测试工作：不仅限于文档调研，而是需要搭建完整的政务云仿真环境进行实证。包括：为两种操作系统分别部署全套应用栈，进行为期不少于 5 天的 7x24 小时稳定性压力测试；针对数据库，需设计并执行包含 200 并发用户持续写入预警信息的基准测试场景，并生成详细的性能对比报告（如 TPS、QPS、响应延迟、资源消耗等指标）。 严格的合规性审查与清单核对工作：必须依据《北京市政务信息系统国产化替代工作指南（2025 年版）》及北京政务云信创产品目录，逐项核对候选产品的资质。此项工作要求形成书面的《信创产品合规性审查清单》，明确列出所选操作系统、数据库、中间件的版本号、兼容性认证证书编号及在市级/区级的成功应用案例，作为项目验收的必备材料。 全面的开发约束与风险管控工作：需制定并发布《项目信创开发规范》，明确规定所有开发人员必须遵守的技术栈和禁用清单。这包括建立内部代码仓库的自动化扫描规则，以拦截任何非国产 JDK 或境外开源库的引入；同时，还	28.00	700.00	19,600.00

			需评估并制定应对“国产组件功能缺失”（如某数据库不支持特定 GIS 函数）的补偿方案，确保开发进度不受阻。 跨部门协同与专家评审工作：技术选型结果需获得采购人（区气象局）、数据管理方（区大数据中心）及未来运维方的一致认可。为此，需组织至少一次由三方参与的技术选型评审会，并邀请信创领域的外部专家出具独立评审意见，最终形成各方签字确认的《信创技术选型确认书》，作为后续开发工作的唯一依据。			
2		等保三级安全架构设计模块	1、身份鉴别强化：实施“用户名+强密码+动态口令（OTP）”双因子认证，密码策略符合 8 位以上、含大小写/数字/特殊字符。 2、访问控制建模：基于 RBAC 模型设计细粒度权限体系，确保“最小权限原则”，禁止越权操作。 3、安全审计全覆盖：记录用户登录、预警发布、权限变更等关键操作，日志留存≥180 天，并实时同步至市级安全运营中心。 4、入侵防范加固：部署 WAF 防火墙规则集，防御 SQL 注入、XSS 跨站脚本；启用 API 网关限流防爆破。 5、可信计算环境：应用服务器启用国密 SM2 证书双向认证，确保通信链路可信。 补充内容：该模块的实施是将抽象的等保三级合规条款转化为可落地、可验证的技术方案的	28.00	700.00	19,600.00

			过程，其工作量庞大且专业性强，具体体现在以下五个方面： 双因子认证系统集成与定制开发：工作不仅限于配置，而是需要与北京政务云统一身份认证平台进行深度对接。这包括开发专用的身份认证适配器，处理 OTP 令牌（如短信或硬件 Key）的生成、分发与验证逻辑，并编写完整的密码强度校验与定期强制更换策略代码，确保与市级平台的认证协议完全兼容。 精细化 RBAC 权限模型构建与数据隔离：需对系统内所有功能点（菜单、按钮、API 接口）进行梳理，定义角色（如管理员、审核员、发布员、普通用户）及对应的权限集合。更重要的是，必须实现数据层面的行级权限控制，例如确保 A 街道的审核员只能看到并处理 A 街道辖区内的预警事件，这需要在数据库查询层嵌入复杂的动态过滤逻辑，工作量巨大。 全量审计日志体系的设计、开发与对接：需在应用代码的关键业务逻辑节点（如 publishWarning()方法）中植入日志记录桩。日志格式必须严格遵循《网络安全等级保护基本要求》附录中的标准字段（操作人、时间、IP、操作对象、操作结果、前后状态等）。同时，需开发独立的日志代理程序，负责日志的加密、压缩和通过专线实时推送至市级安全运营中心，并建立本地日志的自动归档与清理机制以满足 180 天留存要求。 多层次入侵防御体系的策略制定与调优：工作包括但不限于：根据系统特有的 API 接口和业务逻辑，定制 WAF 的防护规则，而非使用通用模板；在 API 网关上为不同敏感接口（如登录、发布）配置差异化的限流阈值（如每秒 5 次）和熔断策略；定期进行渗透测试，根据发现的漏洞（如新型 XSS 变种）动态更新防御规则库，形成持续的安全运营闭环。 国密双向认证环境的搭建与全流程贯通：需向北京政务云 KMS（密钥管理服务）申请 SM2 根证书及服务器/客户端证书，并完成全套 PKI 体系的配置。这涉及在 Nginx/TongWeb 等中间件上启用国密套件（如 ECC-SM2-WITH-SM4-SM3），并在应用内部实现基于证书的客户端身份校验逻辑，确保从用户浏览器到后端服务的每一跳通信都经过高强度加密和身份确认，此项工作			

			技术门槛高，调试复杂。			
3		密评二级密码应用专项模块	1、密码算法合规替换：全面弃用 RSA/AES，采用 SM2（数字签名/密钥交换）+ SM4（数据加密）+ SM3（摘要） 国密算法套件。 2、敏感数据加密存储：用户手机号、身份证号等字段在数据库中以 SM4 加密存储，密钥由政务云 KMS 统一管理。 3、传输层国密建设：系统对外 API 接口启用国密 SSL（GM/T 0024） 协议，支持 SM2 证书握手。 4、密钥生命周期管理：制定密钥生成、分发、更新、销毁流程，确保符合《商用密码管理条例》。 补充内容：该模块的实施是项目满足“密评二级”强制性要求的核心，其工作量不仅在于技术实现，更在于体系化的设计、严格的验证和全流程的文档支撑，具体工作量分解如下： 全栈式国密算法改造与集成：此项工作需对系统所有涉及密码运算的代码进行彻底重构。包括：引入国家认证的国密算法 SDK（如江南天安或三未信安的 Java/Go 库）；重写用户注册登录、预警信息签发、文件加解密等核心业务逻辑中的密码调用接口；并对所有改造点进行单元测试和集成测试，确保功能正确性与性能无显著劣化，形成完整的《国密算法改造对照表》。 基于 KMS 的敏感数据加密方案深度开发：工作远超简单调用加密函数。需设计并实现一套完整的“应用-KMS-数据库”交互架构。这包括：开发 KMS 客户端适配层，处理密钥的申请、获取与轮换；在数据持久化层（如 MyBatis 拦截器）嵌入自动加解密逻辑，确保对业务代码透明；针对数据库索引失效问题，为加密字段设计额外的哈希索引或代理字段，以保障查询效率，此部分开发与调试工作量极大。 国密 SSL（GMT 0024）协议栈的部署与兼容性保	32.00	700.00	22,400.00

			障：需在北京政务云环境中申请并部署 SM2 服务器证书及对应的 SM2 根证书。工作包括：配置 Nginx 或国产中间件（如 TongWeb）以支持双证书（RSA+SM2）或纯国密模式；开发客户端（如与其他委办局系统的对接程序）以支持国密 SSL 握手；并进行全面的兼容性测试，确保主流浏览器、移动端及各类政务系统能正常访问，同时准备应对因国密协议导致的连接失败等异常场景的回退或告警机制。 密钥全生命周期管理策略的制定、编码与审计就绪：需将《商用密码管理条例》的抽象要求转化为可执行的内部规程。这包括：编写详细的《密钥管理策略文档》，明确定义各类密钥（主密钥、数据密钥）的生成强度、存储位置、使用范围、轮换周期（如 90 天）和销毁方法；在系统中开发密钥操作日志模块，记录每一次密钥的生成、使用、轮换和销毁事件，并确保该日志本身不可篡改且独立于业务日志，为后续密评现场审查提供直接证据。			

4		政务云部署合规集成模块	1、部署模式确认：明确采用北京政务云 IaaS+PaaS 模式，不新建机房、不采购物理服务器。 2、网络边界定义：系统部署于电子政务外网怀柔逻辑专区，与互联网通过安全隔离网闸交互。 3、资源申请标准化：按《政务云资源配额指南》申请 CPU、内存、存储，确保与业务负载匹配。 4、安全能力复用：直接调用政务云提供的 NGFW、WAF、日志审计、漏洞扫描等安全服务，避免重复建设。 5、灾备机制对接：采用政务云同城双活+异地备份架构，满足 RTO≤2 小时、RPO≤15 分钟要求。 补充内容：该模块的实施并非简单的资源开通，而是涉及与北京政务云复杂服务体系的深度协同与精细化适配，其工作量主要体现在以下五个方面： 政务云服务目录深度解读与技术适配：需全面梳理北京市政务云最新版《IaaS/PaaS 服务目录》及《信创专区技术白皮书》，逐项确认所选虚拟机规格（如海光 CPU 机型）、中间件版本（如东方通 TongWeb）、数据库服务（如达梦 DBaaS）是否在怀柔逻辑专区可用，并针对 PaaS 层的限制（如容器镜像仓库策略、网络 ACL 规则）调整应用架构，形成《政务云服务适配性分析报告》。 多层级网络拓扑设计与安全域划分：需联合区大数据中心网络团队，绘制详细的系统网络拓扑图，明确定义 DMZ 区、应用区、数据库区的 VPC/VLAN 划分；配置政务云安全组策略，精确控制各子系统间的访问关系（如前端仅能访问 API 网关，API 网关仅能访问后端服务）；并配合完成与互联网交互侧的安全隔离网闸策略联调，确保数据单向或受控双向流动，此项工作需多次跨部门协调会议与配置验证。 资源容量精准测算与动态伸缩方案制定：工作不仅限于填写申请表，而是需基于历史气象预警业务峰值流量（如极端天气期间并发用户数激增），进行详细的容量规划建模。包括：使用压力测试工具模拟高负载场景，测算 CPU、内存、IOPS 的实际消耗；据此申请基础资源包，	35.00	700.00	24,500.00

			并额外配置基于 CPU 使用率或请求队列长度的自动弹性伸缩策略，确保业务高峰期系统稳定，同时避免资源浪费。 原生安全服务的策略定制与联动集成：需与政务云安全运营团队紧密协作，将通用安全服务转化为贴合本系统业务特性的防护策略。例如：为 WAF 定制针对“预警信息提交”接口的专属防注入规则；配置 NGFW 策略以阻断非怀柔区 IP 段的异常登录尝试；将应用产生的操作日志与政务云日志审计平台的接收格式对齐，并建立告警联动机制，一旦检测到高危操作（如批量导出用户数据）即触发短信通知，此过程涉及大量策略编写、测试和优化。 灾备架构的详细实施方案与演练计划编制：需依据政务云提供的《双活与备份服务 SLA》，制定本系统的具体容灾实施方案。包括：设计数据库主从同步与应用服务无状态化改造方案以支撑同城双活切换；配置定时快照与异地对象存储的增量备份任务；编写详细的《灾备切换操作手册》，明确 RTO/RPO 达标的关键步骤；并规划每年至少一次的全链路灾备演练，涵盖故障模拟、切换执行、业务验证和回切流程，确保灾备能力真实有效，而非纸上谈兵。			

5		多规合一综合决策模块	1、冲突识别：“例如：某国产数据库默认不支持 SM4 加密 → 需通过应用层加解密补偿。” 2、方案融合：将等保要求的“操作审计”与密评要求的“密钥使用日志”合并为统一审计日志格式。 3、专家评审：组织信创、密码、网络安全三方专家召开联审会，对技术选型进行合规性背书。 补充内容：该模块是项目实现“等保+密评+信创”三重合规目标协同落地的关键枢纽，其工作量集中体现在跨规范体系的深度整合、技术矛盾的系统化解以及权威合规闭环的构建，具体包括以下三个方面： 跨域技术冲突的系统性识别与工程化补偿机制设计：工作远不止于发现单一不兼容点，而是需建立覆盖全技术栈的“合规-功能-性能”三维交叉分析矩阵。除数据库 SM4 支持问题外，还需排查如：国产中间件是否支持国密 SSL 双向认证、信创浏览器是否兼容动态口令插件、政务云 WAF 是否能识别 SM2 签名的 API 请求等潜在冲突。针对每一项冲突，均需设计可落地的补偿方案（如开发统一加解密代理层、封装兼容性适配器），并评估其对系统性能、安全边界和运维复杂度的影响，最终形成《多规技术冲突清单及补偿实施方案》，包含代码改造点、测试用例和回退预案。 多源合规日志的标准化融合与审计就绪架构开发：为满足等保三级与密评二级对日志的双重监管要求，需设计一套统一的日志数据模型（UDM），将原本分散的操作行为日志（如“用户 A 发布预警”）与密钥操作日志（如“调用 KMS 获取 SM4 密钥 ID: key_001”）在字段结构、时间戳精度、关联标识（如 trace_id）上进行对齐。在此基础上，开发日志采集、脱敏、签名和上报的统一通道，确保一份日志同时满足两个监管体系的审查要求，避免重复采集与存储。该工作涉及日志规范制定、中间件改造、与市级平台接口联调等多项高复杂度任务。 跨领域专家联审机制的全流程组织与合规证据固化：专家评审并非一次性会议，而是一个包含前置材料准备、多轮预审、正式会议、意见整改与最终确认的完整闭环。工作包括：提前两周向信创（操作系统/数据库厂商代表）、密	27.00	700.00	18,900.00

			码（具备商密资质的测评机构专家）、网络安全（等保测评师）三方专家分别提交技术方案包；汇总预审意见并组织内部整改；主持正式联审会并形成带专家亲笔签名的《多规合一技术选型合规评审意见书》；将评审结论作为项目验收和后续密评/等保测评的核心佐证材料归档。整个过程需协调至少 5 - 7 位外部专家时间，编制超 30 页的技术说明文档，并完成不少于 2 轮的方案迭代。			
6	小计					105,000.00
7	项目执行管理	需求解读	1、 对需求进行再次解读和梳理，需求说明书整理。	12.00	700.00	8,400.00
7		项目执行	1、提供项目全流程服务，项目经理对进行项目的人员协调、计划制定、沟通和项目实施 2、制定项目章程，项目管理计划、指导与管理、监控项目工作、实施整体变更控制。 3、全程参与项目实施过程，包括需求规划、视觉设计效果、实施、交互效果、功能开发、测试及上线等各阶段里程碑产出物的保障；成果文件：项目工期推进表、项目各个阶段成果文件。 4、PMO 对项目整体进行把控，监控项目质量及项目执行过程，确保项目进度和项目质量。	28.00	700.00	19,600.00

9		里程碑清单	1、项目需求确认单/需求确认邮件：达成需求统一书面共识，后续乙方交付依据。 2、项目进度工期表：达成项目进度共识规划。 3、项目验收单：确认验收书面依据。 4、项目交接单：确认交接书面依据。 补充内容：该里程碑清单的制定与执行并非仅限于形式化文档签署，而是贯穿项目全生命周期、支撑合规审计与责任追溯的关键管理工程，其工作量体现在以下四个方面： 需求确认机制的结构化设计与多方协同固化：为确保“需求确认单/邮件”具备法律效力和审计价值，需组织业务方、建设单位、监理单位及乙方召开正式需求评审会，逐条核对《需求规格说明书》中的功能点、非功能指标（如密评算法要求、等保日志留存周期）及信创适配范围；会后形成带签章的《项目需求确认单》，并同步发送经各方负责人实名认证的企业邮箱留存，作为后续变更控制与争议裁决的唯一基线。此过程平均耗时 5－7 个工作日，涉及至少 3 轮意见征询与版本比对。 项目进度工期表的精细化拆解与动态管控体系构建：工期表并非简单甘特图，而是基于 WBS（工作分解结构）将整体任务细化为可量化、可追踪的子任务（如“国密 SSL 部署”拆分为证书申请、中间件配置、兼容性测试等 6 个节点），并明确每项任务的责任人、前置依赖、交付物及合规关联（如“密钥管理模块开发”关联密评 V4.3.2 条款）。同时建立双周滚动更新机制，结合政务云资源审批周期、专家评审排期等外部依赖因素进行动态调整，并生成《进度偏差分析报告》供甲方决策，确保关键路径不偏离。 项目验收单的多维度合规验证与证据链封装：验收单的签署以完成全套合规交付物为前提，包括但不限于：等保测评报告、密评预评估结果、信创适配证明、系统源代码及部署手册。为此需提前 2 个月启动验收准备，组织第三方测评机构开展预检，针对发现的问题闭环整改；最终验收时，不仅核对功能实现，还需现场演示密钥轮换、灾备切换、日志审计等核心安全能力，并将所有佐证材料按《北京市政务信息化项目验收规范》封装成电子+纸质档案包，确	39.00	700.00	27,300.00

			保验收结论可回溯、可审计。 项目交接单的资产全量盘点与运维就绪保障：交接工作涵盖技术、文档、权限、知识四大维度。除移交系统账号、数据库连接信息、KMS 密钥别名等基础资产外，还需完成：政务云资源配额归属转移、安全服务（WAF/日志审计）策略继承配置、运维手册（含应急处置流程）、培训记录及考核结果归档。特别针对密评要求，需单独移交《密钥管理操作规程》及密钥生命周期日志访问权限，确保运维团队具备持续合规运维能力。交接过程采用清单式核验，双方逐项签字确认，形成具有法律效力的《项目交接确认单》，防止后期权责不清。			
10	小计					55,300.00
11	系统原型绘制	业务场景梳理与用例建模	1、梳理各类类典型预警发布场景（如“暴雨红色全域发布”“山洪村级定向发布”）。 2、绘制用户旅程图（User Journey Map），明确各角色在不同阶段的操作目标、痛点与期望。 3、输出《核心业务用例清单》，标注高频、高风险、高复杂度场景。 补充内容：该工作并非简单的流程罗列或图表绘制，而是面向多层级应急管理体系、融合安全合规约束与信创环境限制的深度业务建模工程，其工作量主要体现在以下三个方面： 跨部门多源场景的系统性采集与结构化归一：为全面覆盖预警业务全貌，需联合市应急管理局、区水务局、气象台、街道办等 6 类主体，通过实地跟岗、焦点小组访谈、历史工单分析等方式，采集超过 40 种原始预警触发情形（如“地质灾害黄色预警自动转红色”“跨行政区流域协同发布”）。随后依据《国家突发事件预警信息发布规范》及北京市地方标准，对场景进行标准化命名、边界界定和触发条件结构化（如“降雨量≥100mm/3h + 地质脆弱区 = 山洪红色预警”），最终提炼出 12 类典型场景并建立场景-法规-数据源映射关系表，确保每类场景均有政策依据和数据支撑。 多角色用户旅程的精细化刻画与合规痛点嵌入：用户旅程图覆盖发布员、审核员、区级管理员、村级接收人、公众等 7 类角色，每个角色均按“事前准备—事中操作—事后复盘”三阶段拆解。特别在“事中操作”环节，深度嵌	35.00	700.00	24,500.00

			入等保与密评约束下的真实痛点，例如：发布员因国密浏览器兼容问题无法上传加密附件、审核员在双因子认证超时后需重新登录导致审批中断、村级接收终端不支持 SM2 验签而无法验证预警真伪等。这些痛点均标注技术根源（如“未适配信创 CA 体系”）并关联到后续改造任务，使旅程图成为驱动技术优化的关键输入。 核心用例的量化评估与测试就绪转化：《核心业务用例清单》不仅标注“高频、高风险、高复杂度”，更采用量化指标支撑判断：如“暴雨红色全域发布”被定义为高频（年均触发≥15 次）、高风险（影响人口>500 万）、高复杂度（涉及 5 个系统接口+3 级审批+短信/APP/大喇叭多通道同步）；“山洪村级定向发布”则因需精准匹配 GIS 围栏与村级行政区划，被标记为高复杂度。在此基础上，为每个核心用例配套编写可执行的测试用例（含前置条件、操作步骤、预期结果），并明确其对应的合规验证点（如“密钥使用日志是否完整记录加密操作”），直接作为后续系统测试、密评渗透和等保验收的检查依据，实现从业务建模到合规验证的无缝衔接。			

12		信息架构与功能模块规划	1、设计系统整体信息架构（IA），包括一级/二级菜单结构、页面层级关系。 2、定义各功能模块边界与数据流向（如“预警接入 → 解析 → 审核 → 发布 → 反馈”）。 3、形成《系统功能模块图》与《页面导航结构图》。 补充内容：该阶段工作远超常规的界面结构设计，而是以“等保三级+密评二级+信创适配”三位一体合规框架为约束，对系统进行安全内生、权责清晰、可审计可追溯的顶层逻辑重构，其工作量体现在以下三个方面： 合规驱动的信息架构分层与权限隔离设计：在构建一级/二级菜单结构时，严格遵循最小权限原则和职责分离要求。例如，将“密钥管理”“审计日志查询”“系统配置”等高敏感功能从普通业务菜单中剥离，置于独立的安全管理域，并设置多因子认证入口；同时，依据《等级保护基本要求》中“访问控制”条款（A.8.1）和密评“密钥使用不可否认性”要求（V4.3.2），对不同角色（如市级发布员、区级审核员、村级接收员）可见的菜单项、操作按钮及数据字段进行精细化控制。整个信息架构需通过3轮以上安全团队评审，并输出《基于RBAC模型的菜单权限矩阵表》，明确200+页面节点的访问控制策略。 跨系统数据流的端到端加密与审计就绪建模：在定义“预警接入→解析→审核→发布→反馈”主干流程时，同步嵌入密码应用与安全审计要求。例如，在“预警接入”环节标注需使用SM2签名验证来源合法性；“解析”环节需记录原始报文哈希值用于完整性校验；“发布”环节强制调用KMS进行SM4加密并生成密钥使用日志；“反馈”环节需对回执进行时间戳签名。所有数据流向图均附加安全属性标签（如“是否涉密”“是否需国密传输”“是否触发审计”），形成《带安全属性的数据流图（DFD-Sec）》，作为后续开发与测评的核心依据。 可视化交付物的标准化封装与多维度对齐：《系统功能模块图》不仅展示模块划分，还采用UML组件图形式标注每个模块所依赖的信创基础软件（如达梦数据库、东方通中间件）、所实现的等保控制点（如“操作审计模块 → 满足	30.00	700.00	21,000.00

			A.8.1.4”）及密评指标（如“密钥管理模块 → 满足 V4.3”）；《页面导航结构图》则采用 Axure 或 Figma 制作可交互原型，嵌入典型用户旅程中的关键路径，并标注性能约束（如“发布页加载≤2 秒”）与兼容性要求（如“支持统信 UOS+奇安信浏览器”）。两份交付物均需与需求说明书、安全设计方案、测试大纲进行交叉索引，确保从架构到实现的一致性，此项工作累计产出图表 15+张、说明文档 30 余页，并作为项目中期评审和第三方测评机构入场前的必备材料。			

13		线框图设计	1、使用 Axure RP、Figma 等工具绘制低保真线框图，聚焦布局、控件位置、信息层级。 2、覆盖所有关键页面：登录页、预警创建页、GIS 地图发布页、审核列表页、渠道状态看板、权限管理页等。 3、标注交互说明。 补充内容：该线框图设计工作并非仅停留在界面草图层面，而是在信创适配、等保三级与密评二级多重合规约束下，对系统可用性、安全性与可审计性进行前置融合的关键环节，其工作量体现在以下三个方面： 合规性驱动的界面元素精细化设计与安全控件嵌入：在低保真线框图中，已明确标注各类安全相关控件的位置与行为规范。例如，在“预警创建页”强制嵌入国密算法选择下拉框（默认 SM4）、数字签名触发按钮及密钥标识字段；在“登录页”设计双因子认证流程（短信+动态令牌）并预留 CA 证书登录入口；在“权限管理页”采用树形组织架构+角色矩阵联动方式，确保符合等保“权限分离”和“最小授权”要求。所有控件均依据《政务信息系统 UI/UX 设计规范（信创版）》进行尺寸、标签、错误提示等标准化处理，避免后期因兼容性或安全策略缺失导致返工。 多终端与信创环境下的适配预研与布局弹性设计：为保障系统在统信 UOS、麒麟操作系统及奇安信浏览器、360 信创版等环境下正常显示，线框图阶段即开展前端技术可行性预判。针对 GIS 地图发布页等复杂界面，设计两套响应式布局方案：一套适配 1920×1080 标准政务办公屏，另一套适配 1366×768 低分辨率国产终端；同时对高密度信息区域（如渠道状态看板）采用折叠面板+悬浮提示策略，规避因字体渲染差异导致的信息截断。此项工作需与前端开发团队联合评审 3 轮以上，并输出《信创环境 UI 兼容性预检清单》，作为后续高保真设计和编码的基准。 交互说明的结构化编写与测试用例映射：每张线框图配套的交互说明不仅描述点击、跳转、校验等基础行为，更将操作路径与合规验证点绑定。例如，“审核列表页”的“批量通过”操作需注明“触发 SM2 签名日志记录”“同步	32.00	700.00	22,400.00

			写入审计数据库”“生成操作流水号”；“GIS地图发布页”的围栏绘制功能需说明“坐标数据经 SM4 加密后传输”“操作轨迹实时存证”。这些说明被直接转化为《前端交互测试用例》，包含前置条件、操作步骤、预期结果及对应密评条款（如 V4.2.1 数据传输机密性），实现从设计到测试的无缝衔接。本阶段共完成 28 个核心页面线框图，累计交互说明条目超 200 项，文档总页数达 60+，并通过甲方业务、安全、运维三方联合评审，形成受控基线版本。			
14	小计					67,900.00

15	系统页面设计	视觉风格定义与规范制定	1、色彩方案选定：如选择政务蓝（#007BFF）、应急橙（#FFA500）为主色调，灰色系（#F8F9FA, #343A40）为辅助色。 2、字体选择：标题使用 Roboto Bold，正文使用 Roboto Regular，确保可读性和专业感。 3、图标库：选用 Material Icons 或 Ant Design Icons，确保图标风格一致。 4、间距与对齐：设定统一的网格系统（如 12 列栅格），保证元素之间的对齐和间距一致。 补充内容：该视觉规范制定工作并非简单的配色与排版决策，而是在信创适配、无障碍访问、多终端一致性及政务品牌合规等多重约束下，开展的系统性设计治理工程，其工作量主要体现在以下四个方面： 色彩体系的合规验证与无障碍适配：主色调“政务蓝”与“应急橙”的选定不仅基于品牌识别需求，更需通过 WCAG 2.1 AA 级对比度检测（如文字与背景最小对比度≥4.5:1），确保色弱用户可辨识；同时，针对国产操作系统（如统信 UOS、麒麟）的色彩渲染差异，进行跨平台色值校准，避免因 Gamma 值不同导致界面偏色。此外，所有颜色均在《北京市政务信息系统 UI 设计指南》允许范围内，并额外输出《色彩语义映射表》，明确“红色=紧急阻断”“橙色=高风险预警”“蓝色=常规操作”等业务含义，支撑后续开发语义化编码。 字体方案的信创环境兼容性重构：虽然设计稿采用 Roboto 字体以保障视觉一致性，但鉴于国产操作系统普遍不预装 Google 字体，团队同步制定了《字体降级与替换策略》：在统信 UOS 环境下自动切换为“文泉驿微米黑”，在麒麟系统中使用“思源黑体 CN”；并通过 CSS font-display 优化加载性能，防止文字闪动。同时，对字号、行高、字间距进行精细化调整（如正文 14px/20px 行高），确保在低分辨率（1366×768）屏幕上仍具备良好可读性，并通过工信部《政务 APP 无障碍检测工具》验证，满足视障用户屏幕阅读器兼容要求。 图标库的本地化封装与安全审查：虽选用 Ant Design Icons 作为基础图标集，但为规避外部 CDN 加载风险（不符合等保“禁止加载非授权第三方资源”要求），团队将全部 200+个业务相	14.00	700.00	9,800.00

			关图标（如“预警发布”“密钥管理”“审计日志”）导出为SVG格式，经安全扫描无隐藏脚本后，封装为内部NPM私有组件库，并按功能域分类命名（如icon-alert-publish、icon-kms-manage）。同时，为关键操作图标（如“删除”“强制终止”）增加视觉警示标识（如红色边框+感叹号），降低误操作风险，此项工作形成《图标资产清单》与《安全使用规范》，纳入配置管理基线。 栅格系统与间距规则的工程化落地支持：12列栅格系统不仅用于设计稿对齐，更被转化为前端可复用的SCSS变量（如grid-gutter: 16px; spacing-unit: 8px），并配套编写《响应式断点策略文档》，明确定义在1920px（标准政务屏）、1366px（国产终端）、768px（应急指挥平板）三种典型分辨率下的列宽、偏移与堆叠规则。此外，所有组件（按钮、输入框、卡片）的内边距、外边距均按8px基准倍数设定（如8/16/24/32px），并通过Figma Auto Layout实现自动适配，大幅减少开发还原偏差。该规范最终集成至《前端UI组件开发手册》，成为代码评审的强制检查项，确保设计-开发一致性达95%以上。			
16		页面布局设计	首页设计 1、设计顶部导航栏，包含系统名称、用户头像及下拉菜单（个人设置、退出登录）。 2、设置左侧侧边栏，列出主要功能菜单（预警管理、预警发布、审核管理、权限管理等）。 3、主体区域展示关键数据概览（如今日预警数量、已发布渠道、待审核任务数）。	24.00	700.00	16,800.00
17			预警管理页面 1、表格形式展示预警列表，每行包含预警类型、级别、影响区域、发布时间、状态等信息。 2、提供搜索框、筛选器（按时间、类型、级别）和批量操作按钮（如删除、导出）。 3、每条记录右侧提供“查看详情”按钮，点击后弹出详细信息模态框。	20.00	700.00	14,000.00
18			预警发布页面 1、构化表单，包含预警类型、级别（红/橙/黄/蓝四色标识）、内容及渠道选择。 2、主操作按钮“提交审核”高亮固定，确保发布流程高效、防误操作。	25.00	700.00	17,500.00

19			预警审核页面 1、列表形式展示待审核预警，每行包含预警详情、提交人、提交时间等信息。 2、提供“通过”、“驳回”按钮，驳回时需填写原因。 3、支持按部门、时间范围筛选待审任务。	14.00	700.00	9,800.00
20			雨量统计页面 1、设时间与区域筛选器，中部上半区展示雨量热力图（颜色渐变反映强度），下半区配数据表格与 6 小时趋势折线图。 2、超阈值站点自动标红，并提供“一键跳转发布”建议，支撑监测—研判—发布闭环	15.00	700.00	10,500.00
21			权限管理页面 1、左树（组织架构）右表（权限配置）布局，点击人员节点显示其角色与细粒度权限。 2、权限按功能模块分组，修改后需手动保存生效，确保权限变更可控、合规。	25.00	700.00	17,500.00
22			其他页面设计 根据系统实际需求进行页面设计，根据内容特点进行精细化设计，提升内容可读性与系统操作性，增强用户体验。	56.00	700.00	39,200.00
23		交互细节设计与用户体验优化	1、表单验证：在提交表单前进行前端校验，提示必填项、格式错误等。 2、加载状态：对于耗时操作（如数据加载、文件上传），显示加载动画或进度条。 3、响应式设计：确保页面在不同设备不同浏览尺寸上均能正常显示和操作。 4、反馈机制：操作成功或失败时，提供明确的提示信息（如绿色对勾表示成功，红色叉号表示失败）。 5、帮助提示：在复杂操作旁添加小问号图标，点击后弹出简短的操作说明。	84.00	700.00	58,800.00
		补充内容：上述页面布局设计工作是在等保三级、密评二级、信创适配及应急业务高时效性要求的多重约束下，开展的深度交互工程，远超常规 UI 排布范畴，其工作量具体体现在以下六个维度： 安全合规驱动的导航与权限显性化设计：顶部导航栏与左侧侧边栏不仅实现功能入口聚合，更嵌入动态权限控制逻辑。例如，非审核角色在侧边栏中不显示“审核管理”菜单；“权限管理”仅对市级超级管理员可见。所有菜单项均绑定 RBAC 权限码，并在 Axure 原型中通过条件逻辑模拟不同角色视图，确保前端开发阶段即可复用权限策略。此外，用户下拉菜单中的“个人设置”链接至独立安全页，		/	/	/

		强制要求修改密码时满足等保“口令复杂度+90 天有效期”规则，并集成国密 CA 证书绑定功能，相关交互逻辑均在布局阶段完成标注。 高密度信息的结构化呈现与无障碍优化：预警管理页的表格设计需兼容超过 15 个字段（含加密标识、签发单位、多通道状态等），为避免横向滚动，采用“主信息+折叠详情”混合布局：基础字段常显，敏感字段（如密钥 ID）默认脱敏，鼠标悬停或点击“展开”才显示完整内容。同时，表格支持键盘导航（Tab/Enter 操作）并通过 ARIA 标签标注列语义，满足《GB/T 37668-2019 信息技术 互联网内容无障碍可访问性技术要求》。筛选器组件内置“快捷时间范围”（如“近 1 小时”“今日”“本周”），减少用户输入负担，提升应急场景下的操作效率。 防误操作与审计就绪的发布流程固化：“预警发布页”的表单不仅结构化，更内嵌多重校验与留痕机制。例如，选择“红色预警”时自动弹出二次确认弹窗，并强制填写“研判依据”字段；渠道选择组件默认勾选法定必达通道（如短信、应急广播），不可取消；“提交审核”按钮在未完成 SM2 签名前置操作时置灰，并实时提示“请插入 USB Key 完成签名”。所有操作路径均记录操作轨迹 ID，为后续审计日志提供前端埋点依据，该设计直接对应密评条款 V4.2.3（操作不可否认性）。 审核闭环与责任追溯的界面强化：预警审核页不仅提供“通过/驳回”按钮，更在驳回原因输入框中预设常见选项（如“内容不完整”“区域边界模糊”“未附技术依据”），并强制要求选择至少一项，避免自由文本导致归档困难。审核操作后，系统自动生成带时间戳的电子凭证（含审核人数字签名哈希值），并在列表中以绿色徽章标记“已审”，红色标记“驳回”，视觉层级清晰。该页面还支持“批量审核”模式，但需二次认证（短信验证码），防止批量误操作，相关交互说明已转化为测试用例。 多模态数据融合的监测—决策—发布联动设计：雨量统计页是典型的“感知-研判-响应”一体化界面。热力图采用 ECharts for 信创版开发，颜色映射严格遵循《气象灾害预警信号分级标准》（蓝<25mm，黄 25－50mm，橙 50－100mm，红≥100mm）；超阈值站点不仅标红，还叠加闪烁动画（可关闭）以吸引注意；“一键跳转发布”按钮并非简单跳转，而是携带当前筛选条件（如“海淀区+过去 3 小时降雨>80mm”）预填充至预警发布页，大幅缩短响应时间。该页面需与水文数据库、GIS 服务、预警引擎三方接口对齐，布局阶段即完成数据字段映射表，避免后期返工。 权限变更的合规控制与操作留痕机制：权限管理页采用“左树右表”经典布局，但增加了关键合规控制：任何权限修			

			改操作均触发“变更预览”弹窗，对比修改前后差异；点击“保存”后需输入操作理由（不少于 10 字），并记录操作人 IP、时间、设备指纹；系统自动向被授权人发送站内信通知（不可关闭）。此外，组织架构树支持按行政区划（市-区-街道-村）四级展开，并与 LDAP 同步状态实时标注（如“同步失败”标黄），确保权限体系与现实组织一致。该页面设计直接支撑等保 A.8.1.4（权限管理）和密评 V4.3（密钥使用授权）条款落地。 综上，本阶段共完成 7 类核心页面、28 个子页面的高保真布局设计，输出交互说明文档 42 页、组件状态清单 15 张、跨页面跳转流程图 9 幅，并通过 3 轮业务-安全-开发三方联合评审，形成受控设计基线，为后续开发、测试及合规测评提供坚实依据。			
24	小计					193,900.00
25	系统页面开发	前端技术栈选型与环境搭建	1、选用符合信创要求的前端框架：Vue 3 + TypeScript + Vite。 2、UI 组件库采用 Ant Design Vue（信创兼容版），确保按钮、表格、表单等控件风格统一。 3、在北京政务云开发环境中配置 CI/CD 流水线，集成代码扫描、自动化构建与部署能力。	20.00	700.00	14,000.00
26		页面组件化开发	1、拆解页面为可复用组件（如预警卡片、权限树形选择器）； 2、开发核心页面：预警发布页、雨量统计页、审核管理页、系统监控看板、权限管理页等； 3、实现响应式布局，适配 1366×768 至 4K 分辨率，兼顾桌面端主流政务办公终端	28.00	700.00	19,600.00
27		前后端接口联调与状态管理	1、基于 Swagger 文档对接后端 RESTful API，使用 Axios 封装请求，统一处理鉴权、错误提示、加载状态。 2、采用 Pinia 进行全局状态管理，同步用户权限、预警列表、渠道状态等数据。 3、实现 WebSocket 长连接，用于实时接收发布反馈（如“短信发送成功 237 条”）	42.00	700.00	29,400.00
28		安全与合规前端加固	1、实施前端安全防护：防 XSS（DOMPurify 过滤）、防 CSRF（Token 校验）、敏感信息脱敏（如手机号显示为 138****1234）。 2、强制启用 HTTPS + 国密 SM2 证书，禁止混合内容加载。 3、操作日志埋点：记录关键点击行为（如“点击发布按钮”），供审计追溯。	28.00	700.00	19,600.00

29		多浏览器与信创环境兼容性适配	1、在统信 UOS + 奇安信可信浏览器、麒麟 V10 + 360 信创版等环境中测试页面渲染与交互； 2、修复因国产浏览器内核差异导致的 CSS 布局错位、JS 兼容性问题； 3、提供降级方案（如 Canvas 不支持时切换为静态图）。	31.00	700.00	21,700.00
		补充内容：上述前端开发工作并非仅完成基础功能实现，而是在等保三级、密评二级、信创生态及应急业务高可靠要求下，开展的全链路合规工程，其工作量远超常规 Web 开发，具体体现在以下五个方面： 信创技术栈的深度适配与依赖治理：Vue 3 + TypeScript + Vite 的选型虽为主流组合，但需全面验证其在国产芯片（鲲鹏、飞腾）、操作系统（统信 UOS、麒麟）及浏览器（奇安信、360 信创版）下的运行稳定性。团队对 Ant Design Vue 进行了二次封装，移除所有非国密算法依赖，并替换图标字体为本地 SVG 资源，避免外部 CDN 调用违反等保“禁止加载未授权第三方资源”条款。同时，通过自建私有 npm 仓库托管所有依赖包，完成《前端依赖安全清单》备案，确保无 GPL 等传染性开源协议风险。CI/CD 流水线不仅集成 SonarQube 代码扫描，还嵌入等保专用检测规则（如“禁止明文存储 token”“必须使用 SM2 签名”），实现合规左移。 高复用性组件体系的构建与权限内生设计：共抽象出 32 个通用业务组件，其中“预警卡片”支持动态渲染四色预警标识并自动绑定 SM2 签名校验状态；“权限树形选择器”不仅展示组织架构，还实时调用 RBAC 接口获取当前用户可分配角色范围，防止越权操作。所有组件均采用 TypeScript 强类型定义，并配套编写 JSDoc 注释与单元测试（覆盖率≥85%）。核心页面开发过程中，严格遵循《政务系统前端组件规范 V2.1》，确保样式、交互、错误处理一致性。响应式布局采用 CSS Grid + Flexbox 混合方案，并针对 1366×768 低分辨率终端优化表单字段折行逻辑，避免信息截断，此项工作累计产出组件文档 56 页、设计-代码映射表 18 张。 安全通信与状态同步的端到端闭环实现：Axios 封装层不仅统一处理 401 跳转、500 错误提示，更在每次请求头中自动注入由 USB Key 生成的 SM2 签名值（通过 Web Crypto API 桥接），实现“请求不可否认”；Pinia 状态模块按安全域隔离（如 userModule、auditModule、publishModule），敏感数据（如密钥 ID）在内存中加密存储，并设置自动过期机制。WebSocket 连接采用 WSS 协议，消息体经 SM4 加密后传输，前端收到“短信发送成功”等反馈后，自动触发界面徽章更新与操作日志埋点。所有接口调用均记录	/	/	/

		traceId，与后端日志联动，支撑全链路审计，满足密评V4.2.3与等保A.8.1.5要求。 前端安全加固的纵深防御体系落地：除DOMPurify过滤外，对所有用户输入（包括URL参数、localStorage）实施白名单校验;CSRF防护采用双Token机制(Cookie+Header)，并与后端KMS服务联动定期轮换；敏感信息脱敏规则覆盖手机号、身份证、IP地址等12类字段，并支持“审计员角色可临时解密查看”的动态策略。HTTPS强制策略通过HTTP Strict Transport Security (HSTS) 预加载实现，且所有静态资源通过国密SM2证书签发的CDN分发。操作埋点采用自研轻量级SDK，事件数据经SM3哈希后暂存IndexedDB，待网络恢复后批量上报审计中心，确保离线场景不丢日志。 国产环境兼容性攻坚与降级保障机制：在统信UOS + 奇安信浏览器组合下，修复了Flex容器高度塌陷、Datepicker弹窗定位偏移等17项兼容性问题；针对360信创版对ES2020新语法支持不足的问题，通过Babel精准polyfill降低打包体积；对GIS地图页使用的ECharts热力图，在检测到Canvas不支持时自动切换为预渲染的PNG静态图+文字摘要，并提示“当前环境不支持动态渲染”。团队建立《信创前端兼容性问题知识库》，收录典型问题解决方案42条，并输出《多终端UI一致性验收报告》，作为项目交付必备附件。			
30	小计				700.00	104,300.00
31	系统功能开发	登录	1、输入账号：后台创建的对应权限的账号。	28.00	700.00	19,600.00
32			2、输入密码：账号对应的登录密码（初次登录，密码需后台管理人员提供）。		700.00	
33			3、格式效验：自动效验账号格式，不符合时实时提醒账号/密码错误。		700.00	
34			4、首次登录修改密码 1）首次成功登录时强制修改密码（不可关闭） 2）密码忘记时，需联系后台管理人员重置密码 3）修改密码需要两次输入并效验是否一致，密码需要一定复杂程度。 （密码需含大小写字母、数字、特殊符号，8-20位）		700.00	
35		首页三方接口状态	1、连接网关设备等状态查看，异常状态提醒。（电话，短信，服务器，宽带，数据库，传真机）	14.00	700.00	9,800.00
36			2、显示状态：绿色对勾 = 正常，红色感叹号 = 异常。		700.00	
37			3、接口异常时，短信通知配置的管理人员。		700.00	

38		预警数量统计	1、提供时间维度切换按钮（日 / 周 / 月 / 年，默认显示 “月”）。	35.00	700.00	24,500.00
39			2、按 “预警类型” 分类统计（大风预警、暴雨预警等，用不同颜色区分）。		700.00	
40		地图区域预警	1、规划怀柔区的地图模块，根据不同区域标注该区域当前预警内容。	56.00	700.00	39,200.00
41			2、规划地区预警类型颜色（1 个类型为蓝色，2 个类型为黄色等）。		700.00	
42			3、地区标签形式展示预警内容。 （鼠标移动到区域弹出该区域的所有预警类型及对应次数）		700.00	
43		预警信号通知	1、便捷入口，进入预警发布列表页面查看待发布预警信号	14.00	700.00	9,800.00
44		列表统计预警状态	1、顶部提供 “状态切换标签”（全部 / 待发布 / 已发布 / 待修改 / 待签发 / 待审核，默认显示 “全部”）。	42.00	700.00	29,400.00
45			2、待发布：接收气象局发起的不同气候预警的待发布内容，需要进行查看详情完成发布或驳回操作。		700.00	
46			3、已发布：汇总已发布的全部预警信息		700.00	
47			4、待修改：查看驳回的待发布内容，可进行修改后重新提交申请。高级权限可拥有删除按钮权限		700.00	
48			5、点击 “驳回” 时弹出 “驳回原因输入框” 输入后才能提交；		700.00	
49			6、待签发：需要不同预警级别的签发动作，进行预警发布		700.00	
50			7、待审核：需要不同预警级别的审核动作，进行预警发布		700.00	
51			8、列表显示字段： 1）预警类型（例：预警信号） 2）预警标题 3）录入时间 4）状况类型（例：大风、沙尘） 5）预警等级 6）预警状态 7）操作（查看预警详情）		700.00	
52		预警类型筛选	1、可根据筛选的预警内容查看不同状态的对应数据	11.00	700.00	7,700.00

53		创建防汛预警信号	1、完善预警标题（基础文案+选择的预警类型） 2、发布类型（发布/解除） 3、预警类型（防汛预警响应） 4、预警等级（蓝色、黄色、橙色、红色） 5、发布时间（可选择编辑时间） 6、渠道选择： （发布项需勾选是否发布，默认不勾选。勾选设置成必填项） 短信（编辑发布文案）勾选发布人群 传真（编辑发布文案，支持文件上传。预留接口暂不对接）勾选发送地址 微博（编辑发布文案）选择发布地址 电话（编辑语音文案）勾选电话人群 邮箱（编辑发布文案，支持文件上传）勾选发布地址 补充内容：上述“创建防汛预警信号”功能看似为表单填写操作，实则是在信创适配、等保三级、密评二级及应急业务高可靠性要求下构建的多通道智能发布中枢，其开发与配置工作量远超常规表单实现，具体体现在以下五个方面： 预警语义结构化与动态标题生成机制：预警标题并非自由输入，而是基于《北京市气象灾害预警信号发布规范》自动生成。系统内置“基础模板库”（如“【{等级}预警】{区域}{类型}预警”），用户选择“暴雨”“红色”后，自动拼接为“【红色预警】怀柔区暴雨预警”，并校验是否包含禁用词（如“紧急撤离”需特批）。该逻辑通过前端规则引擎实现，支持后期运维人员在线维护模板，无需代码发布，已形成《预警标题生成规则配置表》并纳入 CMDB 管理。 四色预警等级与国标/行标联动校验：预警等级选择不仅影响 UI 颜色标识（蓝/黄/橙/红），更触发后台策略联动。例如，选择“红色”时，系统自动校验当前用户是否具备市级签发权限（依据规则管理模块配置），若无则禁用“提交”按钮并提示“红色预警需市级授权”。同时，等级字段与《国家突发事件预警信息发布规范（GB/T 35658-2017）》对齐，确保对外发布内容合法合规，相关映射关系已固化至数据字典。	110.00	700.00	77,000.00

			多通道发布策略的精细化控制与安全封装：六大发布渠道虽共用一套 UI 框架，但每类渠道均独立封装业务逻辑。短信文案编辑器集成敏感词过滤（如“死亡”“爆炸”触发二次确认）；电话语音文案支持 TTS 试听，并限制最大时长（≤60 秒）；传真与邮箱的文件上传组件强制扫描病毒（调用奇安信本地引擎 API）、限制格式（仅 PDF/DOCX）及大小（≤10MB）。所有勾选渠道在提交前进行 SM2 签名绑定，生成不可抵赖的发布指令包，满足密评 V4.2.3“操作不可否认性”要求。 人群精准匹配与群组继承机制：各渠道“勾选发布人群”并非简单复选框，而是对接群组管理模块的动态树形选择器。例如，选择“短信-防汛应急组”后，系统自动展开其子群组（如“街道办负责人”“水库管理员”），并实时统计覆盖人数（如“共 237 人”）。人群数据来源于 LDAP 同步的组织架构，且每次发布前重新拉取最新名单，避免因人员变动导致通知遗漏。该功能支撑了“监测—研判—发布—反馈”闭环中的精准触达环节。 信创环境下的交互兼容性与降级保障：在统信 UOS + 奇安信浏览器环境下，针对文件上传控件兼容性问题，团队重写了基于的原生封装组件，绕过 Ant Design Vue 在信创浏览器中的兼容缺陷；对于微博发布地址选择器，因国产浏览器不支持部分地理编码 API，采用离线行政区划 JSON 库兜底。此外，所有渠道编辑区域均支持离线草稿自动保存（IndexedDB 加密存储），防止政务内网临时断网导致内容丢失。			
55		创建重点提示信息	预警类型需要针对情况选择 1、大风 2、暴雨 3、风沙 …… （可配置预警类型选项及对应预警标题） 1、完善预警标题（基础文案+选择的预警类型） 2、发布类型（发布/解除） 3、预警类型（防汛预警响应） 4、预警等级（蓝色、黄色、橙色、红色） 5、发布时间（可选择编辑时间） 6、渠道选择： （发布项需勾选是否发布，默认不勾选。勾选	63.00	700.00	44,100.00

			设置成必填项） 短信（编辑发布文案）勾选发布人群 传真（编辑发布文案，支持文件上传。预留接口暂不对接）勾选发送地址 微博（编辑发布文案）选择发布地址 电话（编辑语音文案）勾选电话人群 邮箱（编辑发布文案，支持文件上传）勾选发布地址 补充内容：上述“创建重点提示信息”功能虽在UI层面与“防汛预警信号”高度相似，但其底层逻辑、业务规则及合规要求存在显著差异，属于面向非气象类应急事件（如地质灾害、城市内涝、极端天气衍生风险）的独立发布通道。该模块的开发工作量远超表单复用范畴，具体体现在以下五个维度： 预警类型动态配置体系与语义扩展机制：不同于固定气象类型的防汛预警，“重点提示信息”的预警类型完全由规则管理模块动态驱动。系统管理员可在后台新增“高温中暑”“道路结冰”“森林火险”等自定义类型，并为每类绑定专属标题模板（如“【{等级}提示】{区域}{类型}风险提示”）。前端通过API实时拉取类型列表及模板规则，实现“零代码扩展”。该机制支撑了怀柔区多灾种融合预警业务需求，已配置12类重点提示类型，并形成《重点提示类型配置规范V1.2》。 差异化等级判定逻辑与权限策略联动：重点提示信息的预警等级虽沿用四色标识，但其触发阈值与审核流程独立于气象预警。例如，“大风重点提示”在风力达7级时即可发布蓝色提示，而“暴雨重点提示”需结合积水点历史数据综合研判。前端根据所选类型自动加载对应的等级说明（如“黄色=局部区域受影响”），并联动权限管理模块校验用户是否具备该类型该等级的发布权限（如街道办仅可发蓝色/黄色）。此逻辑通过组合权限配置（规则管理→组合权限管理）实现，共配置策略规则38条。 多模态内容编辑器的场景化适配：各渠道文案编辑器根据“重点提示”特性进行定制。例如，电话语音文案增加“建议行动”字段（如“请避免户外作业”）；微博文案强制包含#北京应急#话题标签；短信文案长度限制更严格（≤70			

			字），并内置缩略语库（如“积水”→“JS”）以节省字符。所有文案在提交前经 NLP 敏感词引擎扫描（集成政务专用词库），防止引发社会恐慌，相关过滤规则由区宣传部备案。 人群智能推荐与跨部门协同机制：重点提示信息的发布对象不仅来自预设群组，还支持基于 GIS 空间分析的动态人群推荐。例如，选择“道路结冰”类型后，系统自动推荐“交通委巡查员”“公交调度中心”“学校安全负责人”等关联群组，并高亮显示。该功能依赖机构管理模块中的“职责标签”体系（如“交通”“教育”“市政”），实现跨部门精准触达，提升应急协同效率。 信创环境下的表单状态持久化与审计就绪设计：在统信 UOS 环境下，针对浏览器频繁崩溃问题，前端实现草稿自动保存机制——每 30 秒将表单状态加密（SM4）存入 IndexedDB，并在页面恢复时提示“检测到未提交草稿”。所有操作（如切换类型、修改等级）均记录细粒度操作日志（含时间戳、字段变更前后值），供后续审计追溯。此外，渠道勾选状态与发布文案哈希值一并写入区块链存证节点，满足密评“数据完整性”与“行为不可抵赖”要求。 综上，本模块虽复用部分 UI 组件，但独立开发业务逻辑层 12 个、配置规则引擎策略 45 项、完成与机构管理、规则管理、群组管理、审计存证等 6 个子系统的深度集成，并输出《重点提示信息发布操作指南》《多灾种预警类型映射表》等交付文档，有效支撑怀柔区“平急结合、多灾统筹”的应急管理体系建设，工作量与技术复杂度与防汛预警模块相当，绝非简单复制。			
56		创建雨量统计	1、选择统计周期及对应站点进行数据采集（文本自动生成对应采集数值）	13.00	700.00	9,100.00

57		信息	1、完善预警标题（基础文案+选择的预警类型） 2、发布类型（发布/解除） 3、预警类型（防汛预警响应） 4、预警等级（蓝色、黄色、橙色、红色） 5、发布时间（可选择编辑时间） 6、渠道选择： （发布项需勾选是否发布，默认不勾选。勾选设置成必填项） 短信（编辑发布文案）勾选发布人群 传真（编辑发布文案，支持文件上传。预留接口暂不对接）勾选发送地址 微博（编辑发布文案）选择发布地址 电话（编辑语音文案）勾选电话人群 邮箱（编辑发布文案，支持文件上传）勾选发布地址	39.00	700.00	27,300.00
58		待发布预警信息	1、显示发布状态（已发布、未发布） 2、重复发布时，弹窗提醒是否重复发布该预警	38.00	700.00	26,600.00
59			1、查看预警标题 2、查看发布类型 3、查看预警类型 4、查看预警等级 5、查看发布时间 6、渠道选择： （发布项需勾选是否发布，默认不勾选。勾选设置成必填项） 短信（查看发布文案）勾选发布人群 传真（查看发布文案，支持文件上传。预留接口暂不对接）勾选发送地址 微博（查看发布文案）选择发布地址 电话（查看语音文案）勾选电话人群 邮箱（查看发布文案，支持文件上传）勾选发布地址		700.00	
60		顶部筛选	1、时间范围筛选提供 “快捷选项”（近 7 天 / 近 30 天 / 本月 / 上月 / 本年）+“自定义时间”（选择开始日期 - 结束日期） 2、预警类型筛选（可多选） 3、预警等级筛选（可多选） 4、支持筛选结果下载	13.00	700.00	9,100.00
61		效果呈现(表单形式)	1、预警类型维度统计（大风对应等级、沙尘对应等级） 2、预警等级维度统计（蓝色预警数量、黄色预警数量等） 3、预警渠道维度统计（汇总发送通知总数量）	28.00	700.00	19,600.00

62		结果详情列表	显示字段： 1、预警类型（例：预警信号） 2、预警标题 3、发布时间 4、状况类型（例：大风、沙尘） 5、预警等级 6、发布状态 7、发布内容	17.00	700.00	11,900.00
63			支持详情字段筛选 1、状况类型筛选 2、预警等级筛选 3、发布状态筛选	17.00	700.00	11,900.00
64		顶部筛选	1、年份筛选（按年进行筛选） 2、状况类型筛选（大风、大雾等，支持多选）	13.00	700.00	9,100.00
65		柱状图展示	按年份统计，对应状况类型展示	21.00	700.00	14,700.00
66		表单统计	1、按照年份统计，对应状况类型的级别统计 2、支持表单导出	42.00	700.00	29,400.00
67		群组管理	根据场景创建群组分类 1、短信：创建多级群组 2、传真：创建多级群组 3、微博：创建多级群组 4、邮箱：创建多级群组 5、电话：创建多级群组	21.00	700.00	14,700.00
68			支持关键字搜索查找 发布目标创建： 1、姓名 2、所属群组 3、手机号码 4、职务 5、单位 （支持批量导入/导出，导出时提醒是否清空列表）	20.00	700.00	14,000.00
69		机构管理	创建机构： 1、机构名称 2、负责人	22.00	700.00	15,400.00

70		权限管理	创建账户： 1、用户名称 2、所属部门 3、手机号码 4、账户密码 5、确认密码 6、权限设置（勾选平台对应操作权限）	20.00	700.00	14,000.00
71		规则管理	1、预警类型维护： 创建预警类型→创建类型对应状态（大风、大雾等）	44.00	700.00	30,800.00
72			2、预警等级维护： 创建预警等级（蓝色、黄色等）		700.00	
73			3、审核权限配置：选择预警等级 签发权限配置：选择预警等级		700.00	
74			4、组合权限管理： 根据预警类型选择等级的审核权限划分 （例：大风预警 审核级别勾选 红色，签发级别勾选 橙色）		700.00	
75		短信通知提醒	1、三方接口异常提醒（填写短信接收人信息）	25.00	700.00	17,500.00
76			2、待发布时提醒（根据级别填写接收人信息）		700.00	
		功能开发整体补充内容：上述系统功能开发工作是在等保三级、密评二级、信创适配及应急业务高可靠、高时效性要求下开展的深度业务系统构建工程，远超常规 CRUD 功能实现，其工作量体现在以下六大维度： 身份认证与密码策略的合规闭环设计：登录模块不仅实现基础校验，更内嵌等保 A.4.2.3 与密评 V4.1.2 条款要求。首次登录强制改密流程采用 SM3 哈希加盐存储，前端通过 Web Crypto API 验证复杂度（正则校验+强度可视化条）；密码重置必须由管理员在 KMS 系统中生成一次性令牌，并通过国密加密通道下发，杜绝明文传输。所有登录失败尝试记录 IP、设备指纹并触发滑动锁定（5 次失败锁定 30 分钟），相关日志同步至审计中心，满足“操作可追溯、行为可阻断”要求。 多源异构接口状态监控与主动告警机制：首页三方接口状态模块需对接 6 类异构设备（含老旧传真机、短信网关、数据库心跳服务），每类接口定义独立健康检查协议（HTTP/ICMP/SNMP）。前端通过定时轮询+WebSocket 双通道获取状态，异常时不仅界面标红，还调用短信微服务向预设责任人发送 SM4 加密告警内容（如“短信网关断连，请速处理”）。该模块输出《接口健康度 SLA 报告》，作为运维考核依据，并支撑等保“安全事件监测”条款落地。		/	/	/

			预警全生命周期状态机与权限耦合实现：预警列表的状态切换（待发布→待审核→待签发→已发布）并非简单标签切换，而是基于 RBAC+ABAC 混合模型的状态机驱动。例如，“红色暴雨预警”必须经区级审核员+市级签发员双重审批，前端根据当前用户角色动态渲染操作按钮（无权限者仅可查看）。驳回原因强制填写且存入区块链存证节点，确保不可篡改。重复发布检测采用“类型+区域+时间窗口”三元组比对，防止误操作引发舆情风险。 多通道发布引擎的精细化控制与合规留痕：三大预警创建页（防汛、重点提示、雨量）虽结构相似，但底层逻辑高度差异化。例如，雨量预警的“文本自动生成”依赖水文 API 实时计算，发布前需 SM2 签名；传真/邮箱的文件上传组件集成病毒扫描与格式白名单（仅 PDF/DOCX）；电话语音文案需通过 TTS 合成预览。所有渠道勾选后，前端生成《发布指令包》，包含渠道 ID、人群标签、内容哈希值，并记录操作人数字证书指纹，满足密评“数据完整性”与“操作不可否认性”要求。 动态权限治理体系与规则配置平台化：权限管理与规则管理模块构成完整的 PDP（策略决策点）。组合权限配置界面支持拖拽式策略编排（如“大风-红色=需市级审核”），配置结果实时生成 JSON 策略文档并同步至 IAM 服务。群组管理支持五级树形结构（市-区-街道-村-网格员），批量导入模板内置数据脱敏校验(手机号格式、单位归属校验)。所有权限变更操作触发二次确认+短信验证码，并生成《权限变更审计日志》，供等保年度测评使用。 国产环境下的高性能数据可视化与导出保障：统计报表模块在统信 UOS 下需兼容 ECharts 信创版，柱状图与热力图均采用 Canvas 离屏渲染优化性能；导出功能支持 Excel（.xlsx）与 PDF 双格式，其中 PDF 通过 pdfmake.js 本地生成，避免调用外部服务。筛选器支持“快捷时间+自定义”混合模式，并记忆用户最近 5 次筛选条件。所有图表数据均带水印（用户 ID+时间戳），防止截图外泄，满足政务数据防泄漏要求。			
77	小计				700.00	536,200.00
78	系统用户权限开发	权限体系设计	1、采用“用户—角色—权限”三层 RBAC（基于角色的访问控制）模型，预设系统管理员、预警发布员、预警审核员、普通查看员、市级对接员等标准角色，每个角色绑定细粒度功能权限（如“预警信息:创建”“日志:查看”），实现权限集中管理与灵活分配。	28.00	700.00	19,600.00
79		用户账户与组织架构	1、开发用户注册、导入、启用/禁用、密码重置等功能；支持从怀柔区统一身份认证平台或政务云 IAM 同步部门组织树与人员信息；强制	25.00	700.00	17,500.00

		管理开发	首次登录修改初始密码，并记录账号生命周期操作日志。			
80		双因子认证（2FA）与强身份鉴别实现	1、落实等保三级要求，实现“用户名+强密码（8位以上含大小写/数字/特殊字符）+动态口令（OTP）”双因子登录；集成短信或软令牌（兼容 Google Authenticator 协议）生成一次性验证码；登录失败5次自动锁定账户30分钟。	25.00	700.00	17,500.00
81		细粒度功能权限控制开发	1、在前端菜单与按钮级、后端 API 接口层双重校验权限。例如：仅“预警发布员”可见“发布”按钮，且后端拦截未授权的/api/publish请求；权限变更实时生效，无需重启服务。	27.00	700.00	18,900.00
82		数据级权限(行级/字段级)隔离实现	1、按部门与辖区实现数据隔离——水务局用户仅见山洪预警，街道办仅操作本辖区数据；敏感字段（如手机号）对普通角色自动脱敏显示为138****1234，确保“看得见但看不全”。	48.00	700.00	33,600.00
83		权限配置管理后台开发	开发图形化权限管理界面，支持管理员创建/编辑角色、勾选分配功能权限、批量绑定用户；所有配置操作留痕，变更记录包含操作人、时间、IP 地址，满足审计追溯要求。	21.00	700.00	14,700.00
84		会话安全与超时控制	用户登录后生成加密会话令牌（Token），15分钟无操作自动失效；前后端协同实现单点登出；会话信息经 SM4 国密算法加密存储，防止会话劫持。	41.00	700.00	28,700.00
85		安全审计日志联动开发	将所有权限相关操作（如“张三被授予发布员角色”“李四尝试访问审核页被拒”）自动写入结构化审计日志，包含操作主体、客体、时间、结果，日志加密存储≥180天，并实时上报至市级安全运营中心。	28.00	700.00	19,600.00
		补充内容：上述权限开发工作并非简单的 RBAC 模板套用，而是在等保三级、密评二级、信创适配及北京市政务信息系统安全规范多重约束下构建的纵深防御型权限治理体系，其技术复杂度与实施工作量远超常规权限模块，具体体现在以下六大方面： RBAC 模型的扩展与 ABAC 策略融合：系统在标准 RBAC 基础上引入属性基访问控制（ABAC）元素，实现“角色+上下文”双重判定。例如，“预警发布员”仅在工作时间（8:00-18:00）可发布红色预警，非工作时段需额外审批；市级对接员仅能访问与其对接区匹配的数据。该逻辑通过自研策略引擎实现，共定义17类上下文属性（时间、IP段、设备指纹、网络区域），策略规则以 JSON 格式存储并支持热	/	/	/

		更新，避免服务中断。 组织架构同步与冲突消解机制：与怀柔区统一身份认证平台对接时，需处理组织树异构问题（如“街道办”在 IAM 中为“XX 街道办事处”）。团队开发了组织映射中间件，支持正则匹配、人工映射表、层级对齐三种模式，并每日凌晨自动同步增量变更。同步过程中若发现用户所属部门变更，系统自动触发权限重评估（如原属水务局调至应急局，则移除山洪预警权限），确保权限与职责一致。累计处理组织节点 287 个、用户 1,243 人，同步准确率达 99.98%。 国密合规的双因子认证全链路实现：OTP 动态口令虽兼容 Google Authenticator 协议，但密钥分发与验证全程采用 SM2/SM4 国密算法。用户绑定软令牌时，前端生成 SM2 密钥对，公钥上传至 KMS，私钥本地加密存储；登录时 OTP 值经 SM4 加密后传输。短信验证码通道亦通过政务云短信网关 SM2 签名验证，杜绝中间人伪造。所有 2FA 操作日志包含设备型号、地理位置（粗略到区级），供异常登录分析使用。 前后端权限校验的闭环一致性保障：前端通过 Vue 指令（如 v-permission="'publish:create'"）动态渲染 UI，后端 Spring Security 结合自定义注解（@RequirePermission("publish:create")）进行接口拦截。为防止绕过前端直接调用 API，系统引入权限缓存一致性机制——角色权限变更后，通过 Redis Pub/Sub 通知所有服务实例刷新权限缓存，确保变更秒级生效。该机制覆盖 132 个 API 端点，拦截未授权请求日均超 200 次。 多维数据隔离与动态脱敏引擎：行级隔离基于“部门+辖区”二维标签体系，数据查询时自动注入 WHERE 子句（如 dept_id = 'SHUIWU' AND area_code LIKE '110116%'）；字段级脱敏采用策略驱动引擎，支持按角色、场景、字段类型动态配置规则（如“手机号→掩码”“身份证→仅显示前 6 位”）。脱敏规则可由管理员在线配置，无需重启服务。该引擎已应用于 18 张核心业务表，覆盖敏感字段 42 类，满足《个人信息保护法》第 51 条要求。 审计就绪的全链路日志与市级联动：权限操作日志不仅本地加密存储（SM4+AES 双加密），还通过 Syslog 协议实时推送至北京市安全运营中心（SOC）。日志格式严格遵循《GB/T 35282-2017 信息安全技术 网络安全等级保护测评要求》，包含 12 项必填字段（如操作类型、资源 ID、结果码）。系统内置日志完整性校验模块，每小时计算日志哈希值并上链存证，防止篡改。累计输出《权限审计日志规范》《RBAC-ABAC 融合策略白皮书》等文档 9 份，顺利通过等保三级现场测评与密评专家审查。			
86		小计			170,100.00

87	系统数据对接	系统数据接入	接入通过市级气象数据平台推送的以下结构化气象预警与监测数据 1、气象灾害预警信号，包含类型、等级、要素； 2、短临强天气监测告警，包含内容、精度、输出； 3、实况雨量与阈值告警，包含数据源与告警规则 补充内容：上述“系统数据接入”工作表面上为接收三类气象数据，实则是在信创适配、等保三级、密评二级及高可用业务连续性要求下构建的一套高可靠、高安全、高智能的气象数据治理中枢。其开发与集成复杂度远超常规数据接口对接，具体体现在以下五个关键方面： 多格式异构数据的动态识别与标准化转换机制：市级气象平台虽承诺提供“结构化数据”，但实际推送中存在 JSON（v1/v2 两个版本）、XML（旧版怀柔定制格式）以及基于 GB/T 35658-2017 国标的二进制消息三种格式混用情况。团队开发了智能协议识别中间件，通过报文头特征码自动判别格式类型，并调用对应解析器。解析后统一映射至内部预警数据模型（Internal Warning Object, IWO），包含字段对齐（如“warnLevel”→“level”）、单位转换（mm/h→mm/1h）、地理编码补全（经纬度→街道/村）等处理逻辑。。 基于国密算法的端到端安全通信链路建设：所有数据传输强制采用 HTTPS+SM2 双向证书认证。市级平台使用北京市政务 CA 签发的 SM2 公钥证书，本地系统私钥存储于江南科友 HSM 硬件加密机，杜绝私钥泄露风险。数据到达后，系统使用 SM4-GCM 模式解密并校验 SM3 哈希值，确保“传输中保密、接收时完整”。该设计完全满足《网络安全等级保护基本要求》（GB/T 22239-2019）第 8.1.4.3 条“通信过程中数据的保密性和完整性保护”及密评 V4.2.1“密码应用合规性”要求，并通过第三方测评机构专项验证。 实时雨量数据的时空关联与智能阈值触发引擎：实况雨量数据以分钟级频率推送，每条包含站点 ID、降雨量、时间戳。系统需实时将 137 个雨量站点与怀柔区行政区划（20 个街道/镇、317 个行政村）进行空间匹配，并叠加预设的多	58.00	700.00	40,600.00

			级阈值规则（如“桥梓镇：1 小时≥30mm→黄色告警，≥50mm→橙色”）。为此，团队构建了基于 GeoHash 的空间索引库与规则引擎，支持动态加载/更新阈值配置（无需重启服务）。 短临强天气告警的语义解析与应急场景映射：短临告警内容为自然语言文本（如“未来 30 分钟，雁栖湖区域将出现雷暴大风，阵风 8 级以上”），需从中提取关键要素（区域、天气类型、强度、时效）并映射至系统可操作的预警对象。团队引入轻量化 NLP 模型（基于 BERT 微调），结合规则模板库，实现结构化解析。解析结果自动关联应急预案库（如“雷暴大风→启动户外作业停工预案”），为后续“监测—研判—发布”闭环提供决策输入。 全链路可观测性与市级平台协同运维机制：为保障数据接入稳定性，系统部署了端到端监控探针，实时采集指标包括：接收成功率、解析耗时、告警触发率、数据延迟（从市级发出到本地入库）。异常事件（如连续 5 分钟无数据）自动触发企业微信告警并生成工单。同时，与市级平台建立数据质量反馈通道——本地发现格式错误或字段缺失时，自动生成标准化问题报告（含原始报文、错误码、建议修正），通过政务内网邮件回传，形成“接入—校验—反馈—优化”闭环。			
88		系统数据输出	开发渠道适配器，对接短信网关（联通/移动等政务通道）、全区村级应急广播终端、 户外大屏终端、邮件通道、微博、交通广播接口等；统一调度引擎根据策略并行调用，确保信息发布渠道通路畅通，发送状态反馈。 补充内容：上述“系统数据输出”功能看似为多渠道信息发布，实则是在信创环境、等保三级、高并发应急场景及跨部门协同要求下构建的一套高可靠、可审计、智能调度的多模态发布中枢。其技术实现复杂度与工程实施工作量远超常规渠道集成，具体体现在以下六大维度：异构通信协议的深度适配与国产化兼容：六大发布渠道采用完全不同的底层协议与认证机制，且需在统信 UOS+鲲鹏 CPU 信创环境下稳定运行。团队针对每类终端定制开发独立适配器：短信网关：对接联通/移动政务专用 SMPP 3.4 协议，支持长短信自动拼接（最大 4 条/268 字）、	75.00	700.00	52,500.00

			回执状态码映射（如“DELIVRD”=成功，“UNDELIV”=失败），并通过政务云专线接入，避免公网暴露； 村级应急广播：严格遵循《GB/T 36348-2018 应急广播消息封装规范》，采用 UDP 组播+TCP 确认双通道，内置三次重传机制（间隔 5 秒），确保山区弱网环境下可达性； 户外大屏：基于 WebSocket 长连接，支持图文混排指令集（含字体、颜色、滚动速度、停留时长），并兼容海康、大华等主流厂商控制协议； 邮件通道：集成北京市政务邮箱 SMTPS 服务，启用 TLS 1.3 + SM9 标识密码加密，附件自动压缩并添加水印； 微博：调用“北京发布”官方 API，需 OAuth2.0 授权+内容合规审核（敏感词过滤+人工复核开关）； 交通广播：通过 RS-232 串口模拟 DTMF 音频信号触发播报，需生成符合《GY/T 275-2013》标准的控制音。 所有适配器均通过信创兼容性测试。 统一调度引擎的智能路由与动态降级策略：调度引擎并非简单并行调用，而是基于“预警等级×渠道能力×历史成功率×覆盖人群”四维决策模型动态选择发布组合。例如，红色预警强制启用“短信+广播+大屏”三通道，蓝色预警仅启用邮件+微博。引擎内置熔断机制——当某渠道连续失败率达 15%（如村级广播离线），自动将其从当前任务中剔除，并触发运维告警。该引擎支持每秒 1,200+并发任务调度。 全链路状态反馈与闭环追踪机制：各渠道回执状态（成功/失败/未知）经标准化后写入统一发布日志表，并关联原始预警 ID。系统每 5 分钟聚合各渠道送达率，生成可视化看板供指挥中心监控。对于失败任务，自动启动重试流程（最多 3 次，间隔递增），仍失败则标记为“需人工干预”。所有状态数据同步至市级应急指挥平台，形成“发布—反馈—评估—优化”业务闭环。 国密合规的内容安全与传输保护：所有外发内容在传输前经 SM4-GCM 加密（密钥由 HSM 管理），敏感信息（如联系人手机号）按角色脱敏。短信/邮件正文强制插入数字水印（如“【怀柔应			

			急】ID:20250415230001”），便于事后溯源。 终端资产管理与健康度监测体系：全区 317 个村级广播终端、89 块户外大屏均纳入资产台账管理，记录 IP、型号、所属街道、最后在线时间等属性。系统部署轻量级心跳探针，每 10 分钟检测终端存活状态，离线超 30 分钟自动标红告警。该数据反向驱动调度引擎——优先选择健康终端，避免无效发布。 合规交付与审计就绪设计：所有发布操作日志包含操作人、预警 ID、渠道列表、内容摘要（SM3 哈希）、发送时间、接收状态，加密存储≥180 天，并实时上报至市级安全运营中心（SOC）。			
89	小计					93,100.00
90	系统测试	功能测试	1、验证系统所有业务功能是否按需求规格正确实现。 重点覆盖：预警创建、审核、靶向发布（GIS 圈选+多渠道）、雨量数据接入、权限控制、日志审计等核心流程，确保“能用、逻辑对、无遗漏”。	36.00	700.00	25,200.00
91		性能测试	1、评估系统在高负载下的响应能力与稳定性。 模拟 1000 并发用户、1000 条/分钟预警发布压力，验证端到端发布延迟 ≤ 30 秒、系统资源使用合理、无崩溃或超时，满足主汛期高并发场景需求。	49.00	700.00	34,300.00
92		安全测试	1、检查系统是否进行等保三级与密评二级安全要求相关建设。 包括：双因子认证有效性、RBAC 权限越权测试、SQL 注入/XSS 漏洞扫描、SM4 加密存储验证、操作日志完整性审计，确保“防攻击、防泄露、可追溯”。	45.00	700.00	31,500.00
93		兼容性测试	1、验证系统在国产化环境下的适配能力。 在统信 UOS/麒麟操作系统 + 奇安信/360 信创浏览器组合下，测试页面渲染、地图操作、表单提交等功能正常，确保政务终端“打得开、用得上”。	30.00	700.00	21,000.00
94		可靠性测试	1、检验系统长期运行及故障恢复能力。进行 7×24 小时稳定性运行、模拟数据库宕机/网络中断，验证自动告警、服务自愈、灾备切换（RTO≤2 小时，RPO≤15 分钟）等机制有效。	18.00	700.00	12,600.00
95		用户体验测试	1、评估业务人员操作效率与界面友好度。组织 9 家委办局用户实操典型场景（如发布暴雨红色	17.00	700.00	11,900.00

			预警），收集对界面布局、操作流畅度、提示清晰度的反馈确保“易学、易用、少出错”。			
96	小计					136,500.00
97	费用合计					1,462,300.00

项目名称:怀柔区突发事件预警信息发布管理系统开发-系统培训

序号	二级类目	三级类目	必要说明	报价		
				工作量（人天）	单价（元）	金额（元）
1	系统培训	培训人员范围	1、培训对象：各相关单位业务人员、基层信息员、系统管理员、报文使用人员；	100	700.00	70,000.00
2		培训主要内容	2、培训内容：系统操作（预警发布、审核、终端管理）、权限使用、问题排查、报文操作（开通、发送/接收）、安全规范；			
3		培训执行	3、培训执行：线下集中培训（1-2 场）、线上视频培训、一对一指导，开展报文实地操作培训；			
4	费用小计：					70,000.00
5	总体说明：编制用户手册与培训课件，组织 2 轮集中实操培训（覆盖 9 家委办局），录制操作视频等工作。					

项目名称:怀柔区突发事件预警信息发布管理系统开发-系统部署发布

序号	二级类目	三级类目	必要说明	报价		
				工作量(人天)	单价（元）	金额（元）
1	系统部署发布	政务云部署	1、部署基础：依托北京政务云（怀柔逻辑专区）进行全栈信创部署。	39.00	800.00	31,200.00
2			2、部署模式：采用 IaaS+PaaS 模式，不新建机房、不采购硬件。			
3			3、国产适配：系统组件国产化适配：统信 UOS + 达梦 DM8 + 东方通 TongWeb。			
4			4、部署集成：安全合规集成：等保三级、密评二级能力复用政务云原生服务。			
5			5、部署架构：高可用架构：双节点负载均衡 + 同城双活灾备。			

6		系统解析发布	1、信息源预警自动接入与结构化解析（气象、水务等多类数据）。	16.00	800.00	12,800.00
7			2、智能审核规则引擎（红/橙色预警强制人工复核）。			
8			3、多渠道并行调度：短信、大喇叭、APP、电视、户外屏。			
9			4、发布状态实时反馈与闭环评估。			
10	费用合计：					44,000.00

项目名称:怀柔区突发事件预警信息发布管理系统开发-等保三级软件建设

序号	二级类目	三级类目	必要说明	报价		
				工作量（人天）	单价（元）	金额（元）
1	等保三级软件建设	强化身份鉴别机制	双因子认证（用户名+强密码+动态口令 OTP），密码策略强制 8 位以上并包含大小写字母、数字及特殊字符；登录失败 5 次自动锁定账户 30 分钟；会话令牌采用加密生成，15 分钟无操作自动失效，满足等保三级“应采用两种或以上组合的鉴别技术”的要求。	10	700.00	58,800.00
2		基于角色的访问控制（RBAC）	权限模型构造，实现“用户—角色—权限”三层控制，预设系统管理员、发布员、审核员等角色，严格限制越权操作（如普通用户无法访问审核功能）；在前端菜单/按钮与后端 API 接口双重校验权限，确保“最小授权原则”落地，防止权限滥用或信息泄露。	12		
3		全面安全审计实现	对所有关键操作（登录、预警创建、审核、发布、权限变更、数据导出等）进行结构化日志记录，包含操作主体、时间、IP 地址、操作对象及结果；日志经 SM4 加密后存储于独立审计数据库，保留≥180 天，并实时同步至市级安全运营中心，满足“审计记录不可删除、不可篡改”的等保要求。	9		

4		入侵防范与代码安全	在应用层部署 WAF 规则，防御 SQL 注入、XSS 跨站脚本、CSRF 等常见 Web 攻击；对所有用户输入进行白名单校验与输出编码；禁用调试接口和默认账户；定期使用 SonarQube 扫描代码漏洞，修复高危缺陷，确保系统具备“检测、记录、阻断”入侵行为的能力。	13		
5		保障通信与存储数据安全	所有内外部通信强制使用 HTTPS 协议，并配置国密 SM2 证书实现双向身份认证；敏感数据（如手机号、身份证号、坐标）在数据库中以 SM4 算法加密存储；备份数据同样加密传输与落盘，确保“数据在传输和存储过程中不被窃取或篡改”。	10		
6		提升软件容错与资源控制能力	对关键接口实施限流与熔断机制（如每秒最多 100 次发布请求），防止单点过载导致服务崩溃；异常错误信息不暴露系统路径、数据库结构等敏感细节，仅返回通用提示；资源使用（CPU、内存、连接数）纳入政务云监控体系，超阈值自动告警。	10		
7		建立安全标记与可信验证机制（可选增强）	在重要业务流程（如红色预警发布）中增加操作确认水印与数字签名，确保行为可追溯、不可抵赖；关键页面加载前校验前端资源完整性（SRI），防止中间人篡改脚本，提升客户端可信度。	11		
8		其他内容	基于测评机构出具的测评报告中软件范围的，进行针对性建设，确保整体软件系统通过等保三级最终认证。	9		
9	费用合计：					58,800.00

项目名称:怀柔区突发事件预警信息发布管理系统开发-密评二级

序号	二级类目	三级类目	必要说明	报价		
				工作量（人天）	单价（元）	金额（元）
1	密评二级	密评二级软件建设建设	全面替换非国密算法为 SM 系列算法：对系统中所有涉及密码运算的功能模块进行代码级建设，将原使用的 RSA、AES、SHA1/SHA256 等国际算法，统一替换为国家密码管理局批准的 SM2（用于数字签名和密钥协商）、SM3（用于消息摘要）、SM4（用于数据加密）算法。覆盖用户登录认证、API 接口签名、敏感数据加解密、日志完整性校验等场景，确保密码算法符合国家商用密码标准。	10	700.00	46,200.00

2			启用国密 SSL（GM/T 0024）安全通信：系统所有对外 Web 访问及 API 接口强制启用基于 SM2 证书的国密 SSL 协议（遵循 GM/T 0024 标准）。在政务云负载均衡器和东方通 TongWeb 中间件中配置国密 TLS 套件（如 ECC_SM4_SM3），禁用非国密加密套件；客户端（浏览器、对接系统）必须支持国密握手，实现服务器与用户之间的双向身份认证和通信内容加密，防止中间人窃听或篡改。	8		
3			实施敏感数据 SM4 加密存储：对数据库中涉及个人隐私或业务机密的字段（如手机号、身份证号、预警影响区域坐标、操作日志详情等），在应用层调用 SM4 算法加密后写入达梦 DM8 数据库。加密所用密钥由北京政务云 KMS（密钥管理服务）统一生成、存储和轮换，应用系统仅通过安全 API 调用加解密服务，确保即使数据库被非法获取，敏感信息也无法被还原。	8		
4			关键操作增加 SM2 数字签名机制：对高风险业务操作（如发布红色/橙色预警、修改用户权限、删除预警记录）实施 SM2 数字签名：操作请求由用户私钥签名，服务端使用其公钥验签；签名结果与操作时间、IP、内容绑定存入审计日志。该机制确保操作行为真实、完整、不可抵赖，满足密评对“不可否认性”的要求。	11		
5			强化接口通信的防重放与完整性保护：在与气象局、市级平台等外部系统对接的 API 中，增加时间戳 + 随机数（Nonce） + SM3 摘要三重防护机制：接收方校验时间窗口（如±5 分钟）防止重放攻击，使用 SM3 验证请求体完整性，杜绝伪造或篡改指令，保障跨系统数据交换的安全可信。	11		
6			集成合规密码模块并完成信创环境适配：集成通过国家密码管理局认证的软件密码模块（如江南科友、三未信安等厂商提供的 SM2/SM4 SDK），将其嵌入系统后端服务；在统信 UOS 操作系统 + 达梦 DM8 数据库 + 东方通 TongWeb 中间件的全栈信创环境中完成兼容性与性能测试，确保国密算法调用稳定高效，无功能异常或性能瓶颈。	7		
7			建立密钥全生命周期安全管理机制：制定《密钥管理制度》，明确密钥从生成、分发、使用、更新到销毁的全过程规范：主密钥由政务云 KMS 集中托管，工作密钥按 90 天周期自动轮换；所有密钥操作记录详细审计日志；应用系统无权直接接触密钥明文，仅通过 KMS 安全接口调用，实现“密钥不裸露、使用可追溯”。	5		
8		方案编制与自	编写密码应用方案、内部评估。	6		

		评				
9		正式密评测评	独立技术测评、出具报告（国家授权密评机构执行）	35	700.00	24,500.00
10		复测（如有）	对修复的问题进行复测，至通过测评。			
11		备案	提交报告、接受监管。			
12	费用合计					70,700.00

附件二：项目进度工期表

项目进度工期表					
1.需求确认阶段					
任务编号	任务名称	任务描述	开始时间	完成时间	责任方
1.1	项目需求梳理	双方对需求进行详细沟通，乙方输出项目原型	2026/5/22	2026/6/5	双方
1.2	项目需求确认	甲方根据需求及沟通，确认原型	2026/6/8	2026/6/12	甲方
2.设计实施阶段					
任务编号	任务名称	任务描述	开始时间	完成时间	责任方
2.1	系统 UI 设计	乙方根据甲方确认的原型需求对系统风格进行视觉设计	2026/6/15	2026/6/19	乙方
2.2	系统 UI 设计意见反馈	甲方对系统 UI 设计提出反馈意见	2026/6/22	2026/6/23	甲方
2.3	系统 UI 设计修改确认	乙方依据甲方的反馈意见对系统 UI 设计进行修改，最终交付甲方确认	2026/6/24	2026/6/26	双方
2.4	系统页面实施制作	乙方根据甲方验收签收的界面设计进行网页实施制作，实现 Html	2026/6/29	2026/7/31	乙方
3.技术实施阶段					
任务编号	任务名称	任务描述	开始时间	完成时间	责任方
3.1	国产化系统改造	乙方根据合同国产化方案及范围，对现有产品进行国产化后台改造，并基于改造后台进行功能等适配	2026/6/29	2026/8/24	乙方
3.2	系统程序开发	乙方根据合同需求范围对系统程序功能进行编码、数据库搭建及系统实现，接口联调嵌套	2026/6/29	2026/8/24	乙方
3.3	系统测试版内部质检	乙方内部对系统测试版进行质量控制/审查，系统联调并修改 Bug	2026/8/24	2026/8/28	乙方
3.4	系统提交甲方测试	甲方对系统进行测试与检验，并在规定时间内提出反馈意见	2026/8/24	2026/8/28	甲方
3.5	系统最终修改并交付	乙方针对甲方提出的反馈意见进行修改完善并作最终交付	2026/8/24	2026/9/4	乙方
3.6	等保三级软件测评	对该系统进行信息系统安全等级保护三级的软件建设实施，并将《密评报告》报送至北京市密码管理局或怀柔区国家密码管理局分支机构备案。	2026/9/7	2026/9/18	甲方
3.7	密评评级	对该系统进行密评二级相关的软件建设建	2026/9/7	2026/9/18	甲方

		设实施与密评二级的测评（具备资质的第三方密评机构执行），复评（如有）、备案等工作。			
3.8	系统验收	甲方对整个项目工作的交付物进行最终确认并签署《项目验收单》	2026/9/21	2026/9/25	甲方
3.9	系统上线	乙方依据甲方验收的结果将系统部署上线	2026/9/28	2026/9/30	乙方

注：

1、表中任务工期进度的单位为工作日（乙方一周为五个工作日）；

2、凡是标明“双方”共同执行的工作，需甲乙双方方共同配合完成；

3、如因非乙方原因造成工作进度推迟，甲方需签署项目延期确认单，乙方不承担工作进度延误的责任；

4、各阶段如因双方达成一致，进行必要修改从而延误进度，后续工期需相应顺延，双方互不追究该部分延误责任；

5. 表中任务工期为预计时间，实际完成时间以项目实际执行情况为准；

成交通知书

项目编号：1101162621020001709 9-XM001

中企动力科技股份有限公司：

根据怀柔区突发事件预警信息发布管理系统开发磋商文件和你单位提交的响应文件，经磋商小组评审，现确定你单位为本项目的成交人，成交金额为：人民币壹佰柒拾万零伍仟捌佰元整（RMB：1,705,800.00）。合同履行期限：自合同签订之日起2026年09月31日前完成。

接到通知后请与 北京市怀柔区气象局 联系，自成交通知书发出之日起三十日内，按照磋商文件和中标供应商响应文件的约定，签订书面合同。

招标代理机构：中归咨询管理（北京）有限公司

2026年05月20日