

政府采购合同

项目名称：呼伦贝尔市党政机关重要网络与信息系统商用密码应用安全性评估项目

甲方：中国共产党呼伦贝尔市委员会保密机要局

地址：内蒙古自治区呼伦贝尔市海拉尔区河东新区党政办公楼中国共产党呼伦贝尔市委员会保密机要局（406室）

乙方：新潮睿石信息技术有限公司

地址：山东省济南市高新区汉峪金谷A3区4栋16层

甲乙双方根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《中华人民共和国民法典》等相关法律法规、规范性文件以及呼伦贝尔市党政机关重要网络与信息系统商用密码应用安全性评估项目

（HSZCS-C-F-260165）的中标（成交）结果、招标（磋商）文件、投标（响应）文件等文件的相关内容，经平等自愿协商一致，就如下合同条款达成一致意见。

一、乙方向甲方提供的服务内容

（一）根据招标（磋商）文件及中标（成交）结果公告，乙方向甲方提供的服务、货物（如有）内容如下：根据GB/T39786《信息安全技术 信息系统密码应用基本要求》、GB/T43206《信息安全技术 信息系统密码应用测评要求》等相关标准对30个等保三级信息系统（相关单位为呼伦贝尔市公安局、卫健委、政数局、文旅广局、档案馆、经开区、退役军人事务局、发改委、教育局，呼伦贝尔市委保密机要局，呼伦贝尔市人民检察院，呼伦湖管理局）及25个等保二级信息系统（相关单位为呼伦贝尔市生态环境局、教育局、商务局、政数局、退役军人事务局、卫健委、外事办、经开区、审计局、国资委、林草局、司法局、住建局、财政局、自然资源管理局、文旅局、科技局、发改委、公安局、呼伦湖管理局、交通运输局）开展密评工作。

（二）服务项目名称、服务具体内容、服务方式、服务要求、服务成果及与之相关的货物等详细内容，见合同附件一服务清单。

二、乙方服务成果的交付时间、地点

(一) 服务期限：自合同签订之日起30个工作日内完成项目服务。

(二) 服务成果的交付要求：依据GB/T39786《信息安全技术信息系统密码应用基本要求》，符合国家及行业规范标准，满足采购人相关要求，并符合GB/T39786《信息安全技术信息系统密码应用基本要求》的系统出具《商用密码应用安全性评估报告》。

服务地点：采购人要求的的服务地点

乙方代表及联系电话：李晖 13947030846

甲方代表及联系电话：陈墨 0470-8776325

注：服务成果分阶段交付的，应分别列明各阶段的交付时间、交付内容。

三、乙方提供服务成果的质量

(一) 乙方提供的服务应同时满足：1. 符合国家法律法规和规范性文件对服务质量的要求；2. 符合甲方招标（磋商）文件对服务的质量要求；3. 符合乙方在投标（响应）文件中或磋商、谈判过程中对服务质量作出的书面承诺、声明或保证。上述质量要求作为甲方对乙方服务质量的验收依据。

(二) 乙方应根据国家法律法规和规范性文件的规定、招标（磋商）文件的相关要求、投标（响应）文件及乙方承诺、声明或保证，向甲方提供相应的服务质量证明文件。

四、乙方服务成果的交付方式及载体

乙方交付服务成果方式及载体应符合国家法律法规和规范性文件的要求，并符合甲方招标（磋商）文件的要求、乙方在投标（响应）文件中对服务成果交付方式及载体作出的承诺。

五、甲方对乙方服务的监督

甲方对乙方提供的服务有权进行监督，当乙方服务质量、服务内容不符合约定时，甲方有权要求乙方及时进行整改，对乙方拒不改正或整改不到位的，甲方有权随时解除合同，并根据具体情况扣除部分或全部服务费用。

六、合同金额

在乙方提供完全符合合同要求的服务的前提下，本合同总金额为886000.00元（小写）捌拾捌万陆仟元整（大写）。

七、付款时间及条件

(一) 支付方式：本合同生效之日起30个工作日内，乙方提供正式发票后，

甲方支付乙方合同总额的50%款项,即人民币¥443000.00元(大写:人民币肆拾肆万叁仟元整);在甲方收到乙方提供的正式版报告30个工作日内,甲方支付乙方合同剩余50%款项,即人民币¥443000.00元(大写:人民币肆拾肆万叁仟元整)。

(二) 乙方账户信息

乙方名称: 新潮睿石信息技术有限公司

开户银行: 齐鲁银行济南历城支行

银行账号: 000000726003800003769

八、知识产权

乙方应保证其提供的服务及服务成果的全部及部分,均不存在侵犯第三方知识产权的情形,其服务成果的所有权由甲方享有。否则,乙方应向甲方承担违约责任及赔偿由此给甲方造成的名誉及经济损失。

九、违约条款

(一) 甲方逾期支付合同价款的,甲方应自逾期90日后的次日起按每日逾期支付价款的1%向乙方支付违约金,但累计违约金总额不超过合同总金额的5%。因财政资金审批拨付流程非因甲方原因导致付款延迟的,不视为甲方逾期付款。

(二) 乙方逾期提供服务成果的,每逾期1日,应按合同总金额1%向甲方支付违约金;逾期超过15日的,甲方有权单方解除合同,乙方应退还甲方已支付的全部款项。

(三) 乙方交付的服务成果经甲方或甲方委托的第三方验收,不符合合同约定的质量标准或国家相关标准的,或服务成果存在侵权行为的,甲方有权解除合同,乙方应退还甲方已支付的全部款项。

(四) 乙方在参与本项目采购活动过程中,如存在提供虚假承诺、证明、串通投标等违法违规行为,除承担相应的行政责任外,甲方有权解除合同,并要求乙方承担合同总金额10%的违约金,违约金不足以赔偿甲方损失的,甲方有权要求乙方赔偿经济损失。

(五) 乙方及其工作人员对在服务过程中知悉的国家秘密、工作秘密、甲方及相关单位的网络信息系统数据、安全漏洞、密码配置等敏感信息负有保密义务,未经甲方书面同意,不得以任何形式向第三方批漏、复制、留存或用于本项目以外的任何用途。服务完成后,乙方应按甲方要求移交或销毁全部相关资料及存储介质,不得擅自备份留存。乙方违反保密义务的,甲方有权立即解除合同,乙方

应退还甲方已支付的全部款项，并追究乙方相关责任。

（六）因一方违约导致另一方采取法律途径维权的，违约方应承担守约方为此支出的合理费用，包括但不限于案件受理费、保全申请费、律师费、鉴定费、公证费、差旅费等。

十、不可抗力

因不可抗力（指不能预见、不能避免且不能克服的客观情况，包括自然灾害、战争、重大疫情防控措施等）致使一方不能履行合同的，应在不可抗力发生后5个工作日内以书面形式通知对方，并在10个工作日内提供有关机构出具的证明文件。双方不承担违约责任，但受影响一方应采取合理措施减少损失。不可抗力影响消失后，双方继续履行合同。

十一、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成，任何一方均有权向甲方所在地有管辖权的人民法院提起诉讼。

十二、合同保存

合同文本一式6份，采购单位、中标（成交）供应商、采购代理机构、各执两份。合同文本保存期限为从采购结束之日起至少保存十五年。

十三、合同附件

本合同所附下列文件是构成本合同不可分割的部分，与本合同具有同等法律效力：

服务清单（双方应盖章确认）

乙方出具的报价单（函）

中标（成交）结果公告及中标（成交）通知书

甲方招标（磋商、谈判）文件采购要求

甲乙双方商定的其他文件

十四、合同未尽事宜，双方另行签订补充协议，补充协议是合同的组成部分。

十五、本合同由甲乙双方盖章生效。

(盖章页，此页无正文)

甲方名称：中国共产党呼伦贝尔市委员会保密机要局（章）

甲方法定代表人或负责人：（签字）

任世杰

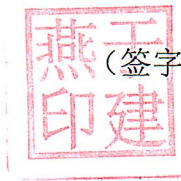
2026年10月8日



乙方名称：新潮睿石信息技术有限公司（章）

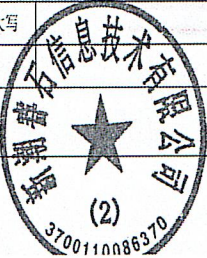
乙方法定代表人或负责人：（签字）

2026年10月8日



附件1：乙方出具的报价单（函）

供应商承诺表（报价-最后报价-新潮睿石信息技术有限公司）

项目名称	呼伦贝尔市党政机关重要网络与信息系统商用密码应用安全性评估项目		
项目编号	HSZCS-C-F-260165		
包号	1	包名称	呼伦贝尔市党政机关重要网络与信息系统商用密码应用安全性评估项目
轮次	1	生成时间	2026年09月07日 13:28:15
投标供应商	新潮睿石信息技术有限公司		
投标总价	大写	886000.00	
		捌拾捌万陆仟元整	
投标单位（盖章）： 			

2026年09月07日

中标通知书

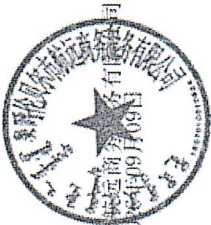


项目编号：HSZCS-C-F-260165

新潮普石信息技术有限公司：

中国共产党呼伦贝尔市委员会保密机要局于2026年09月07日就呼伦贝尔市党政机关重要网络与信息系统商用密码应用安全性评估项目（项目编号：HSZCS-C-F-260165）进行竞争性磋商采购，现通知贵公司中标，请按规定时限和程序与采购人签订采购合同。

中标合同包号	合同包1
中标合同包名称	呼伦贝尔市党政机关重要网络与信息系统商用密码应用安全性评估项目
中标金额(元)	885,000.00
合计金额(大写):	捌拾捌万陆仟元整



呼伦贝尔市皓远商务咨询有限公司

附件3：甲方招标（磋商、谈判）文件采购要求

一、具体需求

为呼伦贝尔市本级重要网络与信息系统提供商用密码应用安全性评估服务，使信息系统能够合规、正确、有效地使用商用密码技术、产品及服务，达到商用密码应用安全性评估合规要求，通过商用密码应用安全性评估。

本项目根据GB/T39786《信息安全技术 信息系统密码应用基本要求》、GB/T43206《信息安全技术 信息系统密码应用测评要求》等相关标准对30个等保三级信息系统（相关单位为呼伦贝尔市公安局、卫健委、政数局、文旅广局、档案馆、经开区、退役军人事务局、发改委、教育局，呼伦贝尔市委保密机要局，呼伦贝尔市人民检察院，呼伦湖管理局）及25个等保二级信息系统（相关单位为呼伦贝尔市生态环境局、教育局、商务局、政数局、退役军人事务局、卫健委、外事办、经开区、审计局、国资委、林草局、司法局、住建局、财政局、自然资源管理局、文旅局、科技局、发改委、公安局、呼伦湖管理局、交通运输局）开展密评工作。

1、商用密码总体要求

密码算法合规性要求：信息系统中使用的密码算法符合法律法规的规定和密码相关国家标准、行业标准的有关要求。

密码技术合规性要求：信息系统中使用的密码技术遵循密码相关国家标准和行业标准。

密码产品合规性要求：信息系统中使用的密码产品与密码模块通过国家密码管理部门核准。

密码服务合规性要求：信息系统中使用的密码服务通过国家密码管理部门许可。

2、密码技术应用要求

从物理和环境、网络和通信、设备和计算、应用和数据等安全层面对信息系统提供密码应用服务。

物理和环境层面要求：分析评估信息系统物理环境是否合理、合规、正确、有效地利用商用密码技术，在物理和环境层面进行密码保护。对物理访问身份鉴别，保证重要区域进入人员身份的真实性。保证电子门禁及视频监控记录数据的完整性。

网络和通信层面要求：分析评估信息系统是否合理、合规、正确、有效地利用商用密码技术，在网络和通信层面进行密码保护。对用户进行身份鉴别，保证网络和通信中用户身份的真实性；保证系统中通信数据完整性；保证系统中通信过程中重要数据的机密性；保证系统中网络边界访问控制信息的完整性；保证安全接入认证。

设备和计算层面要求：分析评估信息系统是否合理、合规、正确、有效地利用商用密码技术，在设备和计算层面进行密码保护。对登录设备的用户进行身份鉴别，保证用户身份的真实性；建立远程设备管理的安全信息传输通道；保证系统资源访问控制信息、日志记录、重要可执行程序完整性，以及重要可执行程序的来源真实性。

应用和数据层面要求：分析评估信息系统是否合理、合规、正确、有效地利用商用密码技术，在应用和数据层面进行密码保护。对登录用户进行身份鉴别，保证应用系统用户身份的真实性；保证系统中重要数据在传输和存储中的机密性；保证系统中重要数据在传输和存储中的完整性；保证系统应用的访问控制信息、重要信息资源安全标记的完整性，以及数据原发行为和接收行为的不可否认性。

3、密钥管理要求

对影响商用密码防护效能的密钥生命周期相关环节，以及相关环节管理和策略制定的全过程进行分析与评估。密钥生命周期相关环节包括但不限于：密钥生成、密钥存储、密钥分发、密钥导入、密钥导出、密钥使用、密钥备份、密钥恢复、密钥归档、密钥销毁等。

4、安全管理要求

对影响商用密码防护效能的管理制度与措施进行分析与评估，管理制度与措施包括但不限于：安全管理制度、人员管控、信息系统实施、应急预案等。

5、其他要求：无

二、服务内容

参照GB/T39786《信息安全技术 信息系统密码应用基本要求》要求，结合呼伦贝尔市本级重要网络与信息系统商用密码应用现状，综合考虑呼伦贝尔市本级重要网络与信息系统商用密码服务需要，开展商用密码应用安全性评估。

商用密码应用安全性评估技术要求：

1、商用密码应用安全性评估（简称“密评”），即对采用商用密码技术、

产品和服务所集成建设的网络和信息系统密码应用的合规性、正确性、有效性进行评估。

本项目针对呼伦贝尔市本级重要网络与信息系统进行密码技术应用、密码设备使用以及密码服务实现情况进行密评工作。密评工作的主要目的是评估系统在密码应用和管理方面的合规性、正确性和有效性，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等方面进行密码应用安全性评估，通过测评项目的实施，根据被测信息系统安全状况，给出测评结果并提出改进建议，以确保被测信息系统达到GB/T 39786《信息安全技术 信息系统密码应用基本要求》的要求，也为其信息安全和业务持续稳定运行提供保障。

2、密评工作技术要求

商用密码应用安全性评估工作依据GB/T39786《信息安全技术信息系统密码应用基本要求》、GB/T43206《信息安全技术 信息系统密码应用测评要求》、GM/T 0116《信息系统密码应用测评过程指南》标准，工作过程分为四项基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评双方之间的沟通与洽谈贯穿整个测评过程。

测评准备活动：本活动是开展测评工作的前提和基础，本活动的主要任务是掌握被测系统的详细情况，准备测评工具，为编制测评方案做好准备。

方案编制活动：本活动是开展测评工作的关键活动，本活动的主要任务是确定与被测系统相适应的测评对象、测评指标及测评内容等，形成测评方案，为实施现场测评提供依据。

现场测评活动：本活动是开展测评工作的核心活动。主要任务是按照测评方案的总体要求，分步实施所有测评项目，包括单项测评、测评单元和整体测评等方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的密码应用安全性问题。

分析与报告编制活动：本活动是给出测评工作结果的活动，是总结被测系统商用密码整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和GB/T 39786《信息安全技术 信息系统密码应用基本要求》等标准的有关要求，通过单项测评结果判定、测评单元结果判定、整体测评和风险分析等方法，找出整个系统商用密码的安全保护现状与相应等级的保护要求之间的差距，并分

析这些差距导致被测系统面临的风险，从而给出测评结论，形成测评报告文本。

整改咨询阶段：建设整改咨询工作以测评发现的问题为重点，编写信息系统密评整改建议；开展建设整改工作时，投标方提供建设整改相关的咨询服务。

3、密评工作服务要求

服务质量保证：测评机构应根据质量体系要求建立科学的质量保证体系，从人员配备、工具保障以及科学的测评方法论、工作过程等多方面保证项目实施过程的质量。通过“测评准备—方案编制—现场测评—编制测评报告”4个环节严格执行，并在重要环节进行文档评审，保证报告结论准确性。

测评工具配备：要求在密评工作过程中配备专用密评工具，可实现密码算法校验、数字证书校验、协议分析、随机数检测、电子签章校验等，确保密码合规、有效。要求在密评工作过程中配备密码应用安全测评工具（包括但不限于：密码算法校验工具、协议分析工具、数字证书校验工具、随机数检测工具）、密评报告编制工具、密评项目管理工具、密码应用安全测评辅助工具（包括但不限于：端口扫描工具、源代码审计工具、密码应用验证工具等）

测评人员配备：本项目要求密评人员不少于10人。具备丰富的项目实施经验和技能能力（拟派项目人员均具备商用密码应用安全性评估人员相应测评能力考核证书）。

4、实施原则

为保障项目的顺利实施，在项目实施过程须遵循以下原则：

（1）规范性原则

加强项目管理，在人员、质量和时间进度等方面进行严格管控。

（2）标准化原则

测评过程须严格遵守国家的相关法律、法规、规范、标准等相关要求。

（3）完整性原则

在测评过程中，必须确保测评数据、过程记录的完整性。评测内容要综合考虑所有评测对象的技术措施，并建立完整有效的评测流程，保证不存在影响评测结果的疏忽或遗漏。

（4）保密性原则

在测评过程中，切实加强对人员、技术等方面的组织管理；与所有相关人员签署具有法律意义的保密协议，确保在项目实施过程中涉及的所有信息，不会泄

露给第三方单位或个人，不得擅自利用这些信息。投标方的任何工作人员均须与被测单位签署《保密承诺书》，对知悉的事项及信息予以保密，所有资料、技术文档应妥善保管，不得遗失、转借、复印，不得以任何形式向第三方透露；所有密码应用解决方案和采集汇总后的数据严谨通过互联网等公共信息网络、普通邮政进行传递，严禁在连接互联网计算机存储、处理。

（5）影响最小原则

在项目实施的过程中，须充分考虑到相关活动对系统正常运行的不利影响，采取必要的措施将相关风险降到最低。

5、密评工作交付

根据项目内容要求，以电子版或纸版形式按需求输出成果，并针对咨询进行及时反馈，方式不限于现场支撑、邮件、电话或报告。主要产出物包括但不限于：

交付物：

符合GB/T39786《信息安全技术 信息系统密码应用基本要求》的系统出具《商用密码应用安全性评估报告》。

6、测评依据

（1）依据标准和规范

GB/T 39786《信息安全技术 信息系统密码应用基本要求》 GB/T 43206《信息安全技术 信息系统密码应用测评要求》 GM/T 0116《信息系统密码应用测评过程指南》

《信息系统密码应用高风险判定指引》

《商用密码应用安全性评估量化评估规则》

《商用密码安全性评估 FAQ》

（2）参考标准和规范

GB/T 20518《信息安全技术 公钥基础设施数字证书格式规范》

GB/T 25056《信息安全技术 证书认证系统密码及其相关安全技术规范》

GB/T 32905《信息安全技术 商密3 密码杂凑算法》

GB/T 32907《信息安全技术 商密4 分组密码算法》

GB/T 33560《信息安全技术 密码应用标识规范》

GB/T 35276《信息安全技术 商密2 密码算法使用规范》

GB/T 35291 《信息安全技术 智能密码钥匙应用接口规范》
GB/T 36322 《信息安全技术 密码设备应用接口规范》
GB/T 36968 《信息安全技术 IPsec VPN 技术规范》
GB/T 37033 《信息安全技术 射频识别系统密码应用技术要求》
GB/T 37092 《信息安全技术 密码模块安全要求》
GB/T 38540 《信息安全技术 安全电子签章密码技术规范》
GB/T 38556 《信息安全技术动态口令密码应用技术规范》
GB/T 38629 《信息安全技术 签名验签服务器技术规范》
GB/T 38636 《信息安全技术 传输层密码协议(TLCP)》
GM/T 0018 《密码设备应用接口规范》
GM/T 0024 《SSL VPN 技术规范》
GM/T 0025 《SSL VPN 网关产品规范》
GM/T 0026 《安全认证网关产品规范》
GM/T 0027 《智能密码钥匙技术规范》
GM/T 0030 《服务器密码机技术规范》
GM/T 0036 《采用非接触卡的门禁系统密码应用技术指南》
GM/T 0050 《密码设备管理 设备管理技术规范》
GM/T 0051 《密码设备管理 对称密钥管理技术规范》
GM/T 0104 《云服务器密码机技术规范》
GM/Y 5001 《密码标准应用指南》
GM/Y 5002 《云计算身份鉴别服务密码标准体系》
GM/Z 4001 《密码术语》
GW 0013 《政务云安全要求》
GW 0202 《国家电子政务外网安全接入平台技术规范》
GW 0206 《接入政务外网的局域网安全技术规范》

7、测评原则

在开展信息系统密码应用安全性评估工作中，主要遵循以下原则：

(1) 客观公正性原则

测评实施过程中，保证在符合国家密码主管部门要求及最小主管判断情形下，按照与被测单位共同认可的密评方案，基于明确定义的测评方式和解释，实施测

评活动。

（2）可重用性原则

测评工作可重用已有测评结果，包括商用密码检测认证结果和密码应用安全性评估的测评结果等。所有重用结果都以已有测评结果仍适用于当前被测信息系统为前提，并能够客观反应系统当前的安全状态。

（3）可重复性和可再现性原则

依照同样的要求，使用同样的测评方法，在同样的环境下，不同的密评人员对每个测评实施过程的重复执行应得到同样的结果。可重复性和可再现性的区别在于前者关注同一密评人员测评结果的一致性，后者则关注不同密评人员测评结果的一致性。

（4）结果完善性原则

在正确理解GB/T 39786《信息安全技术 信息系统密码应用基本要求》

各个要求项内容的基础上，测评所产生的结果客观反应信息系统的密码应用现状。测评过程和结果基于正确的测评方法，以确保其满足要求。

8、形成密码应用安全性评估报告

针对每个被评估系统编制密码应用安全性评估报告，报告按照国家密码管理局要求包含的内容编制或参考模板编制。协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议。

9、供应商提供服务期间应保证被测单位重要网络与信息系统数据安全，如发生数据损坏、丢失、泄露及系统瘫痪等情况，由供应商进行数据恢复并承担由此产生的经济及法律责任。