合同登记编号：

B	T	J	T	Y	S	J	W	X	B	2	0	2	5	Z	5	2	3	-	5

新疆生产建设兵团政府采购
委托服务合同

项目名称：兵团路网运行监测一体化平台项目

标项号及名称：标项5等保测评及商业密码应用安全评估服务

委托方（甲方）：新疆生产建设兵团交通运输局

受托方（乙方）：新疆量子通信技术有限公司

签订地点：乌鲁木齐市

签订日期：2026年 1 月 19 日

甲方：新疆生产建设兵团交通运输局

乙方：新疆量子通信技术有限公司

为了保护甲、乙双方合法权益，根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及其他有关法律、法规、规章，双方签订本合同协议书。

一、项目管理信息

1、采购组织形式：政府采购

2、采购方式：公开招标

3、项目名称：兵团路网运行监测一体化平台项目（标项5等保测评及商业密码应用安全评估服务）

二、合同标的及金额

序号	报价项目	内容	总价	取费标准说明	备注
1	等保测评及商业密码应用安全评估服务	兵团路网运行监测一体化平台等级保护测评、兵团路网运行监测一体化平台商用密码应用安全性评估	62000.00元	符合国家相关取费标准	不含税：58490.57元，税额：3509.43元。

三、服务内容

1、商用密码应用安全性评估

1.1、项目概述

为贯彻落实《中华人民共和国密码法》、《商用密码管理条例》、《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）、《信息安全技术密码模块安全检测要求》（GB/T 38625-2020）与《商用密码应用安全性评估管理办法》等规范以及系统自身安全需求，对兵团路网运行监测一体化平台项目信息化建设开展密码安全性评估工作，对系统实际情况及系统使用的密码资源情况选择并确定测评对象，在系统真实环境下进行测评，以评估系统的密码应用是否合规、正确、有效；同时提供密码应用技术支持服务，包括但不限于提供密码应用、评估等技术咨询服务、开展相关技术培训、建立系统密码安全管理流程和制度规范等。针对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，协助用户认清风险，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，充分发挥密码保障网络安全核心支撑

作用，增强信息系统网络安全防护能力。

1.2、测评对象

根据相关要求进行商用密码测评并出具测评报告。

序号	信息系统名称	商用密码等级
1	兵团路网运行监测一体化平台	三级

1.3、测评内容

对委托检测系统的关键基础设施、重要应用、网络进行商用密码应用安全性评估。具体包括但不限于商用密码总体要求测评、密码技术应用测评、密钥管理测评、安全管理测评、密码应用建设方案评估。本项目测评工作输出包括且不限于以下成果：出具加盖检测机构印章的纸质《商用密码应用安全性评估测评方案》《商用密码应用安全性评估整改建议》《商用密码应用安全性评估报告》均一式3份。

1.4、测评方案要求

（一）商用密码总体要求测评

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

2、密码技术合规性测评：信息系统中使用的密码技术是否遵循密码相关国家标准和行业标准。

3、密码产品合规性测评：信息系统中使用的密码产品与密码模块是否通过国家密码管理部门核准。

4、密码服务合规性测评：信息系统中使用的密码服务是否通过国家密码管理部门许可。

（二）密码技术应用测评

从物理和环境、网络和通信、设备和计算、应用和数据4个层面对信息系统中应用的密码技术进行分析与评估。

1、物理和环境层面测评：分析评估信息系统是否合理、合规地利用商用密码完整性、真实性功能，对影响信息系统安全防护效能的物理和环境层面因素进行保护。包括但不限于下列典型因素：重要场所的物理访问控制，监控设备的物理访问控制，以及物理访问记录、监控信息等敏感信息数据完整性。

2、网络和通信层面测评：分析评估信息系统是否合理、合规地利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的网络和通信层面因素进行保护。包括但不限于下列典型因素：安全认证连接到内部网络的设备，通信双方的身份认证过程，通信数据完整性，敏感信息数据字段机密性，网络边界访问控制信息完整性，系统资源访问控制信息完整性，安全设备、安全组件的集中管理方式和信息传输通道。

3、设备和计算层面测评：分析评估信息系统是否合理、合规地利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的设备和计算层面因素进行保护。包括但不限于下列典型因素：登录信息系统设备和计算环境的用户身份鉴别过程，系统设备和计算环境资源访问控制信息完整性，重要信息资源敏感标记完整性，重要程序或文件完整性，信息系统设备和计算环境的日志记录完整性。

4、应用和数据层面测评：分析评估信息系统是否合理、合规地利用商用密码机密性、完整性、真实性以及不可否认性功能，对影响信息系统安全防护效能的应用和数据层面因素进行保护。包括但不限于下列典型因素：登录信息系统应用和数据操作环境的用户身份鉴别过程，系统应用和数据操作环境资源访问控制信息完整性，重要信息资源敏感标记完整性，重要数据传输过程的机密性、完整性，重要信息存储过程的机密性、完整性，重要程序的加载和卸载过程，信息系统应用相关实体行为不可否认性，信息系统应用和数据操作环境的日志记录完整性。

（三）密钥管理测评

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下列典型环节：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。

（四）安全管理测评

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下列典型维度：安全管理制度，人员管理，建设运行，应急处置。

1、安全管理制度维度，包括但不限于下列内容与措施：密码建设、运维、

人员、设备、密钥管理内容，密码相关操作规范、安全操作规范，安全管理制度的合理性和适用性论证与审定，安全管理制度的改进和修订，安全管理制度的发布，安全管理制度的执行。

2、人员管理维度，包括但不限于下列内容与措施：了解并遵守密码相关法律法规密码产品使用，关键岗位划分，相关人员职责与权限划分，岗位责任制与人员制约、监督机制，管理和使用账号，人员培训、人员选拔，人员考核、奖惩与调离，人员保密措施。

3、建设运行维度，包括但不限于下列内容与措施：信息系统规划，信息系统建设方案，信息系统密码产品、服务选用，信息系统运行前与定期评估，信息系统整改。

4、应急处置维度，包括但不限于下列内容与措施：应急预案，应急资源准备，应急情况与处置，上级主管部门应急报告，同级密码主管部门应急报告。

2、网络安全等级保护测评

2.1、测评概述

准确掌握系统当前的安全保护水平与国家网络安全等级保护基本要求、网络安全等级保护测评要求等有关等级保护标准规范要求之间的差距，查找系统中可能存在的安全弱点和缺陷，从而能够有针对性的实施安全建设和整改，综合提升信息系统的安全保障能力和防护水平，符合信息安全等级保护的相关要求，确保信息系统的安全稳定运行。

2.2、测评依据

[本次项目参考的政策文件]

- 《中华人民共和国网络安全法》
- 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）
- 《中华人民共和国密码法》

[本次项目依据的国家标准规范]

- 《计算机信息系统安全保护等级划分准则》（GB 17859—1999）
- 《网络安全等级保护基本要求》（GB/T 22239—2019）
- 《网络安全等级保护测评要求》（GB/T 28448—2019）

- 《网络安全等级保护测评过程指南》（GB/T 28449—2018）
- 《网络安全等级保护定级指南》（GA/T 1389—2017）
- 《网络安全等级保护安全设计技术要求》（GA/T 25070—2019）
- 《信息安全等级保护商用密码管理办法》
- 《信息安全等级保护商用密码技术实施要求》
- 《信息安全等级保护商用密码技术要求》
- 《信息系统密码测评要求》
- 《信息系统密码应用基本要求》GM/T 0054-2018

[其他参考资料]

- 《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）
- 《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）
- 《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）
- 《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）
- 《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671）
- 《信息技术安全技术信息安全管理体系要求》（GB/T 22080—2008）
- 《信息技术安全技术信息安全管理实用规则》（GB/T 22081—2008）
- 《信息系统安全安全管理要求》（GB/T20269）
- 《信息系统安全工程管理要求》（GB/T20282）
- 《信息安全技术 服务器技术要求》（GB/T21082）
- 《信息安全技术 密码模块安全要求》GB/T 37092

2.3、项目服务内容

（一）信息系统定级、协助备案服务

协助用户按照《信息安全技术网络安全等级保护定级指南》（GB/T 22240—2020）要求，指导并协助材料的填写工作，协助完成在本地公安机关的备案工作。

（二）网络安全等级测评服务

依据国家相关网络安全标准和规范，严格遵循《信息安全技术网络安全等级保护测评要求》和《信息安全技术网络安全等级保护测评过程指南》文件，根据本项目信息系统已完成的定级备案安全等级，开展相应级别的安全等级测评工作，测评工作包括技术测评和管理测评两部分，分别为：

1、技术测评

（1）安全物理环境：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。

（2）安全通信网络：主要涉及对象为信息系统的网络拓扑结构、路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件，具体的测评内容如下所示：网络架构、通信传输、可信验证。

（3）安全区域边界：通过访谈、检查和测试的方式，主要涉及对象为网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。具体测评内容包括：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、可信验证、安全审计。

（4）安全计算环境：通过访谈、检查和测试的方式，主要涉及的对象为终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、业务应用系统、数据库管理系统、中间件等，具体测评内容包括：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护。

（5）安全管理中心：通过访谈和检查的方式，测评主要涉及的对象为提供集中系统管理功能的系统。具体测评内容包括：系统管理、审计管理、安全管理、集中管控。

2、管理测评

（1）安全管理制度：安全管理制度测评通过访谈和检查的形式评估安全管理制度的制定、发布、评审和修订等情况。主要涉及的对象为安全主管人员、安全管理人员、其他人员、管理制度、操作规程文件等，具体测评内容包括：安全策略、管理制度、制定和发布、评审和修订。

（2）安全管理机构：安全管理机构测评通过访谈和检查的形式评估安全管理机构的组成情况和机构工作组织情况。主要涉及的对象为安全主管人员、安全管理人员、相关的文件资料和工作记录等，具体测评内容包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

（3）安全管理人员：人员安全管理测评通过访谈和检查的形式评估机构人

员安全控制方面的情况。主要涉及对象为安全主管人员、人事管理人员、相关管理制度、相关工作记录等，具体测评内容包括：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理。

（4）安全建设管理：系统建设管理测评通过访谈和检查的形式评估系统建设管理过程中的安全控制情况。主要涉及对象为安全主管人员、系统建设负责人、管理制度、操作规程文件、执行过程记录等，具体测评内容包括：定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择。

（5）安全运维管理：通过访谈和检查的形式测评系统运维管理过程中的安全控制情况。主要涉及人员有安全主管人员、安全管理人员、运维人员，涉及内容有运维管理制度、运维服务团队的管理制度、操作规程文件、执行过程记录等。具体测评内容包括：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理。

根据以上 10 个层面的现场测评结果出具《网络安全等级测评报告》，并到当地公安机关完成备案。

3、服务内容汇总

序号	服务项	系统数量	系统等级	服务年限
1	等级保护测评	1	三级	自合同签订之日起至出具完整的项目测评成果文档并通过甲方审核
2	商用密码应用安全性评估	1	三级	自合同签订之日起至出具完整的项目测评成果文档并通过甲方审核

合同主要条款

1.定义

本合同中和附件中所用的下列术语应解释为：

1.1“甲方”系指买服务的单位。

1.2“乙方”系指提供合同服务和服务的经济实体。

1.3“合同”系指甲方、乙方双方签署的、合同格式中载明的供需双方所达成的协议，包括所有附件、附表和组成合同的所有文件。

1.4“合同价格”系指根据合同规定，在乙方全面正确的履行合同义务时甲方应支付给乙方的货币额。

1.5“服务”系指根据合同所含招标文件中技术规范要求的服务内容及其它类似的义务。

2. 合同标的(详见技术规格及要求)

3. 供货范围

3.1合同的采购范围详见第三章相关条款。

4. 合同价格

4.1合同价格即合同总价小写：¥62000.00元,大写：陆万贰仟元整。

本合同采用的合同价格方式为固定合同总价，包括服务及与合同有关的所有费用。

4.2合同价格在合同执行期内不得变动。

5. 服务期限：自合同签订之日起至出具完整的项目测评成果文档并通过甲方审核。

6. 结算方式：合同签订后支付合同总金额的 60%（¥37200，叁万柒仟贰佰元整）；乙方向甲方提供项目总结报告及完整的项目测评成果文档，并通过甲方组织的专家验收评审，甲方向乙方支付合同总金额的 40%（¥24800，贰万肆仟捌佰元整）。

6.1 本合同使用的货币种类为人民币。

6.2 费用的支付：电汇。

7. 服务内容

7.1本合同服务内容为满足招标文件的要求。

7.2 乙方应按时向甲方报送项目测评成果文档的各项统计报表数据。

7.3 服务期间，如需要追加预算，乙方应提前 15 日以书面形式向甲方提出申请，甲方做出追加预算调整后，双方签订补充协议。

7.4 在未得到甲方允许时，乙方不得将系统数据转交给第三方。

8. 违约责任

8.1 甲、乙双方在合作过程中，本着互惠互利的原则且必须严格遵守中国政府及相关行业制定的有关法律法规，守法经营。

8.2如任何一方违反本协议所规定的义务，违约方在收到守约方要求纠正其违约行为的书面通知之日，应立即停止其违约行为，并在10日内赔偿守约方因此产生的所有损失。

8.3合同期内，双方均不得无故单方终止协议。遇有不可抗力因素即在本协议期限内发生得不可预见不可避免且无法克服，非任何一方所能控制且使任何一方无法完全履行本协议的，包括但不限于地震、台风、火灾、水灾、战争、罢工、暴动、政府行为等，导致的双方或一方不能履约或不能完全履约时，甲乙双方互不承担违约责任。

8.4甲乙双方任何一方违反本合同约定，导致另一方经济、名誉等方面的严重损失，则另一方有权解除本合同，并向责任方索赔。

9. 不可抗力

9.1如果双方任何一方由于战争、严重的火灾、水灾、台风和地震以及其他双方同意属于不可抗力的事故，致使合同的履行受到影响时，履行合同的期限应予以延长，延长的期限应相当于事故所影响的时间。

9.2受事故影响的一方应在不可抗力发生后尽快以传真通知另一方，并在事故发生后 2 天内，将有关部门出具的证明文件用特快专递寄给另一方，如果不可抗力影响时间延续 2 天以上时，双方应通过友好协商在合理的时间内达成进一步履行合同的协议。

10. 税费

10.1本合同价格为含税价。乙方提供的服务等所有税费已全部包含在合同价格内，由乙方承担。

11. 合同争议的解决

11.1甲乙双方因本协议的履行而发生的争议，应由双方友好协商解决，如有争议发生之日起六十日内协商解决不成，任何一方均有权将争议提交本合同签订地(乌鲁木齐市)所在地的人民法院管辖。本协议未尽事宜，双方共同协商签订补充协议，补充协议为本协议不可分割的组成部分，并与本协议具有同等法律效力。

11.2在诉讼期间，除了必须在诉讼过程中解决的那部分问题外，合同其余部分应继续履行。

12. 违约终止合同

12.1在甲方对因乙方违约而采取的任何补救不受损害的情况下，甲方可向乙方发出终止部分或全部合同的书面通知书。

A.如果乙方未能按合同规定的期限或甲方同意延长的限期内提供部分或者全部服务。

B.如果乙方未能履行合同规定的其他任何义务。

在上述任一情况下，乙方在收到甲方发出的违约通知后 7 天内，或经甲方书面认可延长的时间内未能矫正其过失。

12.2在甲方根据12.1条规定，终止了全部或部分合同，甲方可以依其认为适当的条件和方法购买类似未交的服务，乙方应对购买类似服务所超出的费用部分负责。但是，乙方应继续执行合同中未终止部分。

13. 禁止分包

13.1本项目禁止分包。

14. 适用法律

本合同按中华人民共和国的法律进行解释。

合同生效及其他：

14.1合同在甲方、乙方双方签字后即开始生效。

14.2本合同一式四份，以中文书写。甲、乙双方各执两份。

14.3招标文件、投标单位的投标文件、评标答疑记录及中标通知书都是本合同不可分割的一部分。

14.4 如需修改或补充合同内容,经协商，甲乙双方应签署书面修改或补充协议，该协议将作为本合同不可分割的一部分。

此页无正文

甲方（盖章）：

新疆生产建设兵团交通运输局

统一社会信用代码：

11990000010628600A

地址：乌鲁木齐市天山区建设路36号

法定代表人或授权代表（签章）：

日期：2026.1.19

乙方（盖章）：

新疆量子通信技术有限公司

统一社会信用代码：

9165010077039769XQ

地址：新疆乌鲁木齐市沙依巴克区文化宫路59号吉祥苑小区1栋B座805室

法定代表人或授权代表（签章）：

银行账号：991908365210000

开户行信息：招商银行股份有限公司乌鲁木齐人民路支行

日期：2026.1.19

附件

安全保密协议

甲方单位：新疆生产建设兵团交通运输局

乙方单位：新疆量子通信技术有限公司

本协议于2026年1月19日起生效

根据我国有关网络安全及信息保密相关法律法规，本着平等、自愿、公平、诚信的原则，双方就甲方信息化系统建设运维、业务数据服务及后续合作过程中有关数据安全保密事项达成以下协议，并由双方共同遵守。

一、保密内容和范围

甲乙双方确认，乙方承担保密义务的甲方信息包括但不限于以下内容：

1.1技术信息：同甲方业务相关的程序、代码、流程、方法、文档、数据等内容；

1.2业务信息：同甲方业务相关的人员、财务、策略、计划、资源消耗数量、通信流量大小等业务信息；

1.3安全信息：包括账号、口令、密钥、授权等用于对网络、系统、进程等进行访问的身份与权限数据，还包括对正当履行自身工作职责所需要的重要、适当和必要的信息。

二、保密义务

2.1乙方明确所接收的保密信息及其载体均为甲方所有。乙方承认甲方在本协议规定的保密信息上的利益和/或一切有关的权利，乙方应当考虑甲方的利益并对该信息予以妥善保管。

2.2乙方遵守相关法律、法规、政策、规章、制度和协议，基于授权的基础上，合理使用甲方信息，不得以任何其他手段获取、授权或协议规定以外的甲方信息。

2.3乙方未经授权，不应在工作职责授权范围以外使用、分享甲方信息。未经授权，不得泄露、披露、转让以下信息：

(1)技术信息：同甲方业务相关的程序、代码、流程、方法、文档、数据等内容；

(2)业务信息：同甲方业务相关的人员、财务、策略、计划、资源消耗数量、通信流量大小等业务信息；

(3)安全信息：包括账号、口令、密钥、授权等用于对网络、系统、进程等进行访问的身份与权限数据，还包括对正当履行自身工作职责所需要的重要、适当和必要的信息。

2.4乙方对违反协议或可能导致违反协议、规定、规程、法律的活动、策略或实践，一经发现，应立即通告甲方。

2.5检测结束后，乙方应返还甲方本协议中规定的信息和甲方数据。所有由甲方提供给乙方的材料，包括但不限于文件、设计和清单应仍为甲方的财产，且甲方要求时应立即归还原件和所有据此制作的副本。

2.6乙方需约束其员工、关联方服务商履行同等保密义务，并由乙方与接触保密信息的乙方员工、外包人员等签订同等保密协议，对其行为承担连带责任。

三、违约责任

乙方承认并明确同意：其对本协议的任何违约仅有法律的救济尚且不足，并且因其违约行为而造成的甲方损失是难以用金钱

来衡量的。因此，当乙方出现任何违约情形时，甲方有权要求乙方立即返还相关保密信息，且乙方有义务立即采取合理补救措施。同时，乙方还应赔偿：

(1)因乙方违约行为，而使甲方遭受的全部经济损失(包括直接损失和间接损失)；

(2)甲方因调查乙方的违约行为、采取补救措施而支出的所有合理费用(包括但不限于甲方向乙方及第三方追索、取证、调研而发生的仲裁费、诉讼费、律师费、交通费、劳务费等)。

四、保密期限

甲、乙双方确认，乙方的保密义务自其接触、知悉本协议第一条所述的保密信息时开始。无论乙方是否继续为甲方提供信息化系统建设运维服务，乙方都应对其服务期限内知悉的涉密信息承担保密义务。

五、如果发生争议，双方均可向甲方所在地有管辖权的人民法院提起诉讼。

六、如果所涉及的保密信息依照国家主管机关或相关法律、法规另有规定的，适用其相关规定。

甲方：新疆生产建设兵团交通运输局（盖章）

法定代表人：

2026年 1月19日

乙方：新疆量子通信技术有限公司（盖章）

法定代表人：

2026年 1月19日