合同编号：

陕西省档案馆2025年商用密码应用安全性评估项目合同书

项　目　名　称：陕西省档案馆2025年商用密码应用安全性评估项目

采购人（甲方）：陕西省档案馆

供应商（乙方）：西安安盟智能科技股份有限公司

签　订　时　间：2025 年 6 月 6 日

采购人（甲方）：陕西省档案馆

地址：西安市长安区子午大道与学府大街十字东北角

邮编：710100　　**电话：**029-89230819

供应商（乙方）：西安安盟智能科技股份有限公司

地址：陕西省西安市高新区丈八街办沣惠南路 34 号摩尔中心 B 座 1704 室

邮编：710000　　**电话：**029-85798722

根据《中华人民共和国政府采购法》、《政府采购竞争性磋商采购方式管理暂行办法》（财库[2014]214 号）及其实施条例、《中华人民共和国民法典》和甲方（采购项目：ZBZB-2025-2608）的竞争性磋商文件、竞争性磋商响应文件等有关规定，为确保甲方采购项目的顺利实施，甲、乙双方在平等自愿原则下签订本合同，并共同遵守如下条款：

第一条　合同期限

在规定时间内（服务期限：合同签订之日起至2025年11月20日前完成）完成甲方要求服务（数字档案馆综合管理平台、电子文件归档及移交进馆平台、档案共享利用管理平台、公共信息服务平台等 4 个系统平台的商用密码应用安全性评估并验收合格。

第二条　服务内容与质量标准

序号	采购项目	单位	数量	合价（元）
1	陕西省档案馆2025年商用密码应用安全性评估项目	项	1	314000.00

一、项目目标

为保障陕西省档案馆数字档案馆系统的安全稳定运行，需对部署在政务外网、互联网和局域网中备案为网络安全等级保护三级以上（包含三级）的信息系统进行商用密码应用安全性评估，包含四个系统平台，分别是局域网中的数字档案馆综合管理平台、政务外网中的电子文件归档及移交进馆平台和档案共享利用管理平台、互联网中的公共信息服务平台。预计 60 天完成测评工作，编制形成商用密码应用安全性评估报告并开展备案，测评机构应协助我馆及相关技术支撑单位落实密码应用安全整改工作。

二、测评范围

序号	系统名称	系统等级
1	数字档案馆综合管理平台	三级
2	电子文件归档及移交进馆平台	三级
3	档案共享利用管理平台	三级
4	公共信息服务平台	三级

三、项目需求

商用密码应用安全性评估就是对采用商用密码技术、产品和服务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。为保障陕西省档案馆数字档案馆系统的安全稳定运行，需对部署在政务外网、互联网和局域网中备案为网络安全等级保护三级以上（包含三级）的信息系统进行商用密码应用安全性评估，包含四个系统平台，分别是局域网中的数字档案馆综合管理平台、政务外网中的

电子文件归档及移交进馆平台和档案共享利用管理平台、互联网中的公共信息服务平台。测评机构需对上述4个测评系统平台进行密码技术应用、密码设备使用以及密码服务实现情况进行密码测评工作。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，编制形成商用密码应用安全性评估报告并提出改进建议，同时按照国家规范要求，测评机构制定测评方案，实施测评，提供整改咨询服务，提出整改意见，跟踪整改进度，为服务项目验收提供依据，协助我馆及相关技术支撑单位落实密码应用安全整改工作，确保被测信息系统达到《信息安全技术 信息系统密码应用基本要求》的要求，也为信息资产安全和业务持续稳定运行提供保障。

商用密码应用安全性评估工作依据《商用密码应用安全性评估管理办法》《信息安全技术信息系统密码应用基本要求》《信息系统密码应用测评要求》《信息系统密码应用测评过程指南》《政务信息系统密码应用与安全性评估工作指南》《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》《陕西省重要网络和信息系统密码应用与安全性评估工作指南》等相关要求进行，评估工作过程分为四项基本测评流程：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、项目文档收集整理。

四、项目服务内容

按照 GM/T39786-2021《信息系统密码应用基本要求》及通过评估的密码应用方案对系统进行评估，采取材料审查、人员访谈、实地查看、配置检查、工具测评等评估方法对系统密码应用情况进行评估分析，核查系统技术应用、密钥管理、安全管理是否符合密评要求；对评估过程中发现的问题进行汇总确认，总结各项评估指标的评估结果，编制评估报告。具体内容包括：

序号	服务内容	服务内容子项	工作内容
1	需求沟通确认	需求沟通调研和确认工作实施要求	对安全评估的组织实施流程、风险管控效果、时间节点、交付成果、评估方式等基础信息进行沟通核实，确认服务需求和工作要求
2	基础材料搜集整理和现场沟通采集	按照评估准备实施要求，搜集整理必要素材	通过远程或现场会议方式与业务研发、运维部门技术团队和保障团队沟通评估所需基础素材、文档等必要信息
3	密码应用方案评估	密码应用方案评估	对委托方制定的密码应用方案进行评估，出具《密码应用方案评估报告》
4	协助落实密码应用	按照国家规范要求，测评机构制定	协助我馆向省数据和政务服务中心和省数据和政务服务

序号	服务内容	服务内容子项	工作内容
	升级改造工作	测评方案，实施测评，提供整改咨询服务，	局申请使用数字资源。提出整改意见，跟踪整改进度，为服务密码应用升级改造项目验收提供依据，协助我馆及相关技术支撑单位落实密码应用安全整改工作
5	系统评估	依据 GB/T39786-2021《信息系统密码应用基本要求》等标准进行测评	按照 GB/T39786-2021《信息系统密码应用基本要求》及通过评估的密码应用方案对系统进行评估，采取材料审查、人员访谈、实地查看、配置检查、工具测评等评估方法对系统密码应用情况进行评估分析，核查系统技术应用、密钥管理、安全管理是否符合密评要求。
6	报告编制	编制评估报告	对评估过程中发现的问题进行汇总确认，总结各项评估指标的评估结果，编制评估报告。
7	项目档案	项目文档收集整理	项目文档收集范围齐全、完

序号	服务内容	服务内容子项	工作内容
			整、系统

五、密码测评工作内容

密码测评内容应至少包括《信息安全技术信息系统密码应用基本要求》、《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》中关于三级系统的测评内容指标。

测评层面	测评单元	指标要求
物理和环境安全	身份鉴别	宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性。
	电子门禁记录数据存储完整性	宜采用密码技术保证电子门禁系统进出记录数据的存储完整性。
	视频监控记录数据存储完整性	宜采用密码技术保证视频监控音像记录数据的存储完整性。
网络和通信安全	身份鉴别	应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。
	通信数据完整性	宜采用密码技术保证通信过程中数据的完整性。
	通信过程中重要数据的机密性	应采用密码技术保证通信过程中重要数据的机密性。
	网络边界访问控	宜采用密码技术保证网络边界访问

测评层面	测评单元	指标要求
	制信息的完整性	控制信息的完整性。
	安全接入认证	可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。
设备和计算安全	身份鉴别	应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。
	远程管理通道安全	远程管理设备时，应采用密码技术建立安全的信息传输通道。
	系统资源访问控制信息完整性	宜采用密码技术保证系统资源访问控制信息的完整性。
	重要信息资源安全标记完整性	宜采用密码技术保证设备中的重要信息资源安全标记的完整性。
	日志记录完整性	宜采用密码技术保证日志记录的完整性。
	重要可执行程序完整性、重要可执行程序来源真实性	宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。
应用和数据安全	身份鉴别	应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真

测评层面	测评单元	指标要求
		实性。
	访问控制信息完整性	宜采用密码技术保证信息系统应用的访问控制信息的完整性。
	重要信息资源安全标记完整性	宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；
	重要数据传输机密性	应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。
	重要数据存储机密性	应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。
	重要数据传输完整性	宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。
	重要数据存储完整性	宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；
	不可否认性	在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。
管理制度	具备密码应用安全管理制度	应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等

测评层面	测评单元	指标要求
		制度；
	密钥管理规则	应根据密码应用方案建立相应密钥管理规则；
	建立操作规程	应对管理人员或操作人员执行的日常管理操作建立操作规程；
	定期修订安全管理制度	应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
	明确管理制度发布流程	应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；
	制度执行过程记录留存	应具有密码应用操作规程的相关执行记录并妥善保存。
人员管理	了解并遵守密码相关法律法规和密码管理制度	相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
	建立密码应用岗位责任制度	应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限：
		1)根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操

测评层面	测评单元	指标要求
		作员等关键安全岗位；
		2)对关键岗位建立多人共管机制；
		3)密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；
		4)相关设备与系统的管理和使用账号不得多人共用。
	建立上岗人员培训制度	应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；
	定期进行安全岗位人员考核	应定期对密码应用安全岗位人员进行考核；
	建立关键岗位人员保密制度和调离制度	应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。
建设运行	制定密码应用方案	应依据密码相关标准和密码应用需求，制定密码应用方案；
	制定密钥安全管理策略	应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环

测评层面	测评单元	指标要求
		节，各环节密钥管理要求参照附录 B；
	制定实施方案	应按照应用方案实施建设；
	投入运行前进行密码应用安全性评估	投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；
	定期开展密码应用安全性评估及攻防对抗演习	在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。
应急处置	应急策略	应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；
	事件处置	事件发生后，应及时向信息系统主管部门进行报告；
	向有关主管部门上报处置情况	事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

第三条　服务费用

1、报价：（小写）314000.00 元，（大写）叁拾壹万肆仟元整，为含税价。

2、本合同执行期间服务总费用不变，甲方无须另向乙方支付本合同规定之外的其他任何费用。

第四条　付款方式

分期付款：

（1）双方签订合同生效之日起 ，达到付款条件起 15 日内，支付合同总金额的 50.00%，共计人民币：壹拾伍万柒仟元整（￥157000.00 元）（含税）。

（2）剩余尾款待项目完工并经甲方验收合格后 ，达到付款条件起 15 日内，支付合同总金额的 50.00%，共计人民币：壹拾伍万柒仟元整（￥157000.00 元）（含税）。

甲方付款前，乙方应提供与付款金额相等的增值税专用/普通发票，否则甲方有权拒绝付款且不视为违约。

第五条　知识产权

1、乙方应保证所提供的服务或其任何一部分均不会侵犯任何第三方的专利权、商标权或著作权。若由此引发纠纷，所产生的一切法律后果应当由乙方自行承担。因此给甲方造成损失的，乙方还应当赔偿甲方遭受的全部损失。

2、甲方为本合同之目的，提供给乙方的所有资料文件及工作成果等，其知识产权仍归甲方所有，乙方不得复制、使用或提供给第三方。

第六条　无产权瑕疵条款

乙方保证所提供的服务的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。如有产权瑕疵的，视为乙方违约。乙方应负担由此而产生的一切损失。

第七条　履约保证金

1、甲乙双方在签订合同后 5 个工作日内，乙方应向甲方指定账户支付履约保证金，履约保证金金额为合同总价的 5%。保证金人民币 15700.00 元，（大写） 壹万伍仟柒佰元整 元。

2、履约保证金的有效期为乙方承诺的履约质保期内、即 2026 年 11 月 20 日之前。

3、履约保证金作为违约金的一部分及用于补偿甲方因乙方不能履行合同义务而蒙受的损失。若乙方违反本合同，甲方有权从履约保证金中直接予以扣除，乙方应及时补足保证金金额。

4、履约质保期结束后，甲方财务部门接到甲方确认本合同服务等约定事项已经履行完毕的正式书面文件后的 30 日内，向乙方无息退还履约保证金。

5、合同期内、质保期内以及质保期届满后，本项目发生任何质量问题，乙方应于接到甲方通知当日派出专业人员到现场进行解决，发生的全部费用由乙方承担，若需重新商用密码应用安全性评估，根据问题内容制定解决方案，经甲方认可后按期到场解决问题，乙方承担全部费用。

6、若乙方未积极解决，甲方有权指定第三方维修解决，产生的费用由乙方承担，可从履约保证金中扣除。

第八条　甲方的权利和义务

1、甲方有权对合同规定范围内乙方的服务行为进行监督和检查，拥有监管权。有权定期核对乙方提供服务所配备的人员数量。对甲方认为不合理的部分有权下达整改通知书，并要求乙方限期整改。

2、负责检查监督乙方管理工作的实施及制度的执行情况。

3、根据本合同规定，按时向乙方支付应付服务费用。

4、国家法律、法规所规定由甲方承担的其它责任。

第九条　乙方的权利和义务

1、对本合同规定的委托服务范围内的项目享有管理权及服务义务。

2、根据本合同的规定向甲方收取相关服务费用，并有权在本项目管理范围内管理及合理使用。

3、及时向甲方通告本项目服务范围内有关服务的重大事项，及时配合处理投诉。

4、接受项目行业管理部门及政府有关部门的指导，接受甲方的监督。

5、乙方应与甲方协商制定详细且可行的实施方案，并进行实际工作部署，以保证最佳的工作效果，并按照实际情况填写相应的工作计划完成表；甲方对乙方制订的实施方案、实施情况以及乙方工作人员是否严格遵守本合同所约定的义务进行监督。

6、乙方须有具备密码应用安全管理制度、密钥管理规则、保密管理制度、人员管理制度。参与本项目的主要技术人员要登记备案，杜绝工作人员对档案及档案信息的私自复制行为。

7、本合同履行过程中，项目经理及工作人员应当保持稳定，不得随意更换。若项目经理及工作人员出现严重过失行为、有违法行为不能履行职责、涉嫌犯罪、不能胜任岗位、严重违反职业道德等情形，乙方应当立即告知甲方，并及时进行更换。

8、本项目不得分包、转包。

9、乙方工作人员在本合同履行期间产生劳动争议及其他纠纷（包括但不限于如下情形：乙方工作人员在工作期间，如因其过错造成第三人的财产损失或人身伤害；乙方工作人员在非工作时间（包括上下班在途时间）所发生的事故；乙方工作人员私自外出期间以及工作期间内，因自身突发疾病而发生的意外伤亡等），均由乙方负责处理，并承担全部法律责任，与甲方无关。

10、国家法律、法规所规定由乙方承担的其它责任。

第十条　违约责任

1、甲乙双方必须遵守本合同并执行合同中的各项规定，保证本合同的正常履行。

2、如因乙方工作人员在履行职务过程中的的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方对此均应承担全部的赔偿责任。

3、因乙方原因未能在本合同约定工作期限内完成商用密码应用安全性评估服务项目，则乙方应自逾期之日起每天按合同总价款的3‰支付延期赔偿金，如乙方累计逾期达30日，甲方有权单方解除合同或要求乙方继续履行，并要求乙方支付合同总价款20%的违约金，同时乙方向甲方支付延期赔偿金的责任不予免除。

4、乙方未全面履行合同其他义务或者发生违约，甲方有权单方面解除合同，要求退还已支付费用且乙方应承担相应的违约责任，并赔偿由此给甲方造成的全部经济损失（包括直接损失及间接损失）。除本合同另有约定外，乙方承担违约责任的金额为本合同总金额的20%。

5、违约一方除应当承担上述责任外，还应当赔偿因此导致的守约方全部损失，包括但不限于诉讼费、律师费、鉴定费等为维护自身权益的合理支出。

第十一条　不可抗力事件处理

1、在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2、不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3、不可抗力事件延续 10 天以上，双方应通过友好协商，确定是否继续履行合同。

第十二条　合同的变更和终止

除《中华人民共和国政府采购法》第 49 条、第 50 条第二款规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止合同。

第十三条　解决合同纠纷的方式

1、在执行本合同中发生的或与本合同有关的争端，双方应通过友好协商解决，经协商在__10__天内不能达成协议时，则采取以下第__1__种方式解决争议：

（1）向甲方所在地有管辖权的人民法院提起诉讼；

（2）向当地仲裁委员会按其仲裁规则申请仲裁。

2、在仲裁期间，本合同应继续履行。

第十四条　合同生效及其他

1、合同经双方法定代表人或授权委托代理人签字并加盖单位公章后生效。

2、合同执行中涉及采购资金和采购内容修改或补充的，须经政府采购监管部门审批，并签书面补充协议报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。

3、本合同一式捌份，自双方签章之日起起效。甲方肆份，乙方贰份，政府采购代理机构壹份，同级财政部门备案壹份，具有同等法律效力（合同执行完毕后，自动终止，合同的服务承诺则长期有效）。

第十五条　保密条款

本项目中涉及的保密条款见合同附件：保密协议。

甲方：陕西省档案馆　（盖章）

法定代表人（授权代表）：

地　　址：西安市长安区子午大道与学府大街十字东北角

开户银行：中国光大银行西安东大街支行

账　　号：78600188000071603

电　　话：029-89230819

传　　真：029-89230817

签约日期：2025年 6月6 日

乙方：西安安盟智能科技股份有限公司（盖章）

法定代表人（授权代表）：

地　　址：陕西省西安市高新区丈八街办沣惠南路 34 号摩尔中心 B 座 1704 室

开户银行：中国民生银行股份有限公司西安土门支行

账　　号：691122778

电　　话：029-85798722

传　　真：

签约日期：2025年 6月6日

附件：保密协议

甲方（委托方）：陕西省档案馆

乙方（受托方）：西安安盟智能科技股份有限公司

按照甲乙双方约定，乙方向甲方提供网络安全技术服务，为确保服务实施过程中涉及的技术信息和技术资料不被泄露，甲乙双方达成如下协议：

一、保密信息定义

1. 项目实施过程中涉及的技术信息和技术资料，包括但不限于IP 地址规划、网络架构、网络拓扑、软件系统架构、源代码、配置信息、应用系统数据、系统说明书、维护手册，以及项目实施过程中的会议文件，备忘、变更、传真、邮件等相关资料；

2. 项目实施过程中各有关当事人拥有的商业秘密、敏感信息、知识产权等，已经公开的知识产权信息除外；

3. 项目实施过程中使用的测评设备/工具、测评方法、测评流程、及数据分析工具、方法、流程等；

4. 项目实施过程中产生的新技术信息和技术资料；

5. 甲乙双方之间工作往来的人员电话、即时通讯、传真，信函，电子邮件等；

6. 经甲乙双方在项目实施过程中确认的需要保密的其他信息。

二、甲方责任

1. 甲方为承担本协议约定的保密责任，应妥善保管有关的文件和资料，未经乙方的书面许可，不对其复制，仿造等；

2. 甲方应对有关人员进行有效管理，以确保本协议的履行。在本协议约定的保密期限内，甲方如发现有关保密信息被泄露，应及时通知乙方，并采取积极的措施避免损失的扩大；

3. 对不再需要保密或已经公开的技术信息和资料，甲方应及时通知乙方。

三、**乙方责任**

1. 乙方应将甲方信息系统涉及的保密信息仅用于本测评项目的调研、方案编制、现场测评和报告编制工作。

2. 乙方对从甲方处获得的技术信息和技术资料负有保密责任，未经甲方同意不得提供给任何第三方。

3. 乙方为承担本协议约定的保密责任，应妥善保管有关的文件和资料，未经甲方的书面许可，不对其复制，仿造等；

4. 乙方应对有关人员进行有效管理，以确保本协议的履行。在本协议约定的保密期限内，乙方如发现有关保密信息被泄露，应及时通知甲方，并采取积极的措施避免损失的扩大。

5. 乙方在实施相关工作过程中，需要向本项目的有关方面（包括：承担相关工作的其他成员、聘请的专家、政府主管部门）提供保密信息时，必须取得甲方的书面许可，或者由甲方负责提供。

6. 乙方工作人员在甲方现场工作时不得使用个人 U 盘或移动硬盘等拷贝设备，若确需数据拷贝，须经甲方书面同意并在甲方监督下，由乙方现场经理用指定设备拷贝。乙方应当在完成委托事项或本合同终止或解除时将保密资料原件全部返还甲方，并销毁所有复制件。乙

方应当妥善保管保密资料，并对保密资料在乙方期间发生的被盗、泄露或其他有损保密资料保密性的事件承担全部责任，因此造成甲方损失的，乙方应负责赔偿。

7. 完成项目后，乙方应对本项目的数据资料承担保密责任，保密期限为长期，不受本合同履行期限的限制。

四、**违约责任**

违反本协议的约定，由违约方承担相应法律责任，并赔偿由此产生的一切损失。双方在履行协议中产生的纠纷，应通过友好协商解决。如协商不成，双方约定的纠纷裁决地点为甲方所在地人民法院。

五、**保密期限**

本协议自盖章（签字）之日或者自双方中的一方取得有关文件、资料之日起，以时间在前的为准。合同终止（无论履约完成或中途终止）后三年内，双方仍有义务继续保守对方的秘密。

甲方： 陕西省档案馆　　**乙方：** 西安安盟智能科技股份有限公司

日期： 2025 年 6 月 6 日　　**日期：** 2025 年 6 月 6 日