2025年度商用密码评估服务项目采购需求

一、投标人资格条件

1.满足《中华人民共和国政府采购法》第二十二条规定，即：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）法律、行政法规规定的其他条件。

2.单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加本项目同一合同项下的政府采购活动。

3.为本采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的，不得再参加本项目的其他招标采购活动。

4.未被列入失信被执行人、重大税收违法失信主体，未被列入政府采购严重违法失信行为记录名单。

5.本项目不接受联合体投标。

6. 密评：投标人应具备国家密码局颁发的《商用密码检测机构资质证书》。

二、采购需求

2.1 项目背景

按照国家相关技术标准关于信息系统密码应用安全性的总体要求，科学合理的检测和评估信息系统风险、协助发现风险和问题，并在此基础上科学规划和设计出完成的安全体系建设和整改方案。实现对信息资产的保密、完整、可控性、不可抵赖和真实性，做到“进不来、拿不走、改不了，看不懂、跑不了、可审计”的网络安全管理目标。具体包括：

1）保障基础设施安全，保障信息系统使用人员的真实性和不可否认性。

2）保障网络连接安全，保障网络传输中的安全，尤其保障网络边界和外部接入的安全

3）保障主机系统的安全、保障操作系统、数据库、服务器、用户终端及相关关键资产的安全。

4）保障应用系统安全，保障应用系统在传输中的保密、完整和可用，防止和抵御当前的安全威胁和攻击。

5）安全管理体系保障，依据国家有关标准和规范要求，结合实际情况，建立一套切实可行的商用密码安全管理体系。

2.2 项目概况

1 项目名称：2025 年度商用密码评估服务项目。

2 项目工期：自合同签订生效后，系统建设完成且具备进场条件之日起 90 个工作日内完成项目（不含甲方系统整改时间，如系统整改造成工期延误，则完成时间顺延）。

3 测评对象：按照第三级级技术标准开展商用密码应用安全性评估服务。

4 服务清单

序号	系统名称	服务内容	系统级别
1	武汉市检查检验互认共享平台	商用密码应用安全性评估	3 级
2	电子健康卡信息系统		3 级
3	武汉市卫生健康信息化与基础建设项目管理系统		3 级
4	基于卫生健康统计数据的移动端管理分析系统		3 级
5	武汉市医学科学研究项目管理系统		3 级
6	干部信息管理平台		3 级

2.3 标准和依据

- ◆ 《中华人民共和国网络安全法》
- ◆ 《中华人民共和国密码法》
- ◆ 《国家政务信息化项目建设管理办法》（国办发[2019]57 号）

- 《国家密码管理局关于进一步加强国家政务信息系统密码应用与安全性评估工作的函》（国密局函 [2020]119 号）
- 《关于进一步加强全省政务信息化项目密码应用有关工作的通知》（鄂密局发[2021]2 号）
- 《商用密码管理条例》）（中华人民共和国国务院令第 760 号修订）
- 《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》（GB/T 39786-2021）
- 《信息安全技术 信息系统密码应用测评要求》（GB/T 43206-2023）
- 《信息系统密码应用测评过程指南》（GM/T 0116-2021）
- 《政务信息系统密码应用与安全性评估工作指南》（2020 版）

（项目执行期间，如国家技术标准调整，按新生效的标准执行）

2.4 测评实施原则

在项目实施过程中必须满足以下原则：

1）保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标方的行为。

2）标准性原则：测评方案的设计与实施应依据国家信息系统安全的相关标准进行。

3）规范性原则：投标人的工作中的过程和文档，具有很好的规范性，依据中国合格评定国家认可委员会检验机构认可资质等质量管理体系规范项目实施流程，可以便于项目的跟踪和控制。

4）可控性原则：密评实施工作进度要跟上项目建设和改造进度表的安排，由，保证工作的可控性。

5）最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

6）整体性原则：测评的范围和内容应当整体全面，包括国家相关要求涉及的各个层面。

2.5 技术要求

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、政务信息系统密码应用与安全性评估工作指南（2020 版）等相关技术标准要求，参照 ISO20000 或 CNAS 检验等信息技术服务体系，对被测信息系统开展商用密码应用安全性评估（项目执行期间，如国家技术标准发生变化，按照新生效的技术标准执行），为采购方开展密码应用方案设计提供技术咨询，评估内容如下：

序号	商用密码应用安全性评估		
1	密码应用方案评估	密码应用解决方案评估	中标方应对密码应用解决方案的完整性和密码应用设计的合规性、正确性和有效性进行评估。
2		实施方案评估	中标方应检查文档结构是否完整，并审查实施方案是否按照《密码应用解决方案》的设计要求进行编制。
3		应急方案评估	中标方应检查文档结构是否完整，并审查应急方案提出的风险应急预案是否完备、合理、周密。
4	总体要求	密码算法	中标方应验证被测信息系统中使用的密码算法是否当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。
5		密码技术	中标方应验证被测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。
6		密码产品	中标方应验证被测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。
7		密码服务	中标方应验证被测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。
8	物理和环境安全	身份鉴别	中标方应验证被测信息系统在电子门禁系统中是否使用密码技术的真实性服务来保护身份鉴别信息，保证重要区域进入人员身份的真实性。
9		电子门禁	中标方应验证被测信息系统是否使用密码技

		记录数据完整性	术的完整性服务来保证电子门禁系统进出记录的完整性。
10		视频记录数据完整性	中标方应验证被测信息系统是否使用密码技术的完整性服务来保证视频监控音像记录的完整性。
11	网络和通信安全	身份鉴别	中标方应验证被测信息系统是否在通信前基于密码技术对通信双方进行验证或认证，使用密码技术的机密性和真实性服务来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性。
12		访问控制信息完整性	中标方应验证被测信息系统是否使用密码技术的完整性服务来保证网络边界和系统资源访问控制信息的完整性。
13		通信数据完整性	中标方应验证被测信息系统是否采用密码技术保证通信过程中数据的完整性。
14		通信数据机密性	中标方应验证被测信息系统是否采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性。
15		安全接入认证	中标方应验证被测信息系统是否采用密码技术对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。
16	设备和计算安全	身份鉴别	中标方应验证被测信息系统是否使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。
17		远程管理通道安全	中标方应验证被测信息系统是否远程管理时，应使用密码技术建立安全的信息传输通道
18		系统资源访问控制	中标方应验证被测信息系统是否使用密码技术的完整性服务来保证系统资源访问控制信息的

		信息完整性	完整性。
19		重要信息资源安全标记完整性	中标方应验证被测信息系统设备是否使用密码技术的完整性服务来保证设备中重要信息资源安全标记的完整性。
20		重要可执行程序完整性、重要可执行程序来源真实性	中标方应验证被测信息系统是否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。
21		日志记录完整性	中标方应验证被测信息系统是否使用密码技术的完整性功能来对日志记录进行完整性保护。
22	应用和数据安全	身份鉴别	中标方应验证被测信息系统是否使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性。
23		访问控制信息和敏感标记完整性	中标方应验证被测信息系统是否使用密码技术的完整性服务来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性。
24		数据传输机密性	中标方应验证被测信息系统是否采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等。
25		数据存储机密性	中标方应验证被测信息系统是否采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等。
26		数据传输	中标方应验证被测信息系统是否采用密码技

		完整性	术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等。
27		数据存储完整性	中标方应验证被测信息系统是否采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等。
28		重要信息资源安全标记完整性	中标方应验证被测信息系统是否使用密码技术的完整性服务来保证重要信息资源敏感标记的完整性。
29		不可否认性	在可能涉及法律责任认定的应用中，中标方应验证被测信息系统是否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。
30	管理制度	具备密码应用安全管理制度	中标方应验证责任单位是否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制度;
31		密钥管理规则	中标方应验证责任单位是否根据密码应用方案建立相应密钥管理规则;
32		建立操作流程	中标方应验证责任单位是否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
33		定期修订安全管理制度	中标方应验证责任单位系统负责人是否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;
34		明确管理制度发布	中标方应验证责任单位系统负责人是否明确相关密码应用安全管理制度和操作规程的发布流

		流程	程并进行版本控制;
35		制度执行过程记录留存	中标方应验证责任单位是否具有密码应用操作规程的相关执行记录并妥善保存。
36	人员管理	了解并遵守密码相关法律法规和密码管理制度	中标方应验证责任单位相关人员是否了解并遵守密码相关法律法规、密码应用安全管理制度;
37		建立密码应用岗位责任制度	中标方应验证责任单位是否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:
38		建立上岗人员培训制度	中标方应验证责任单位是否建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。
39		定期进行安全岗位人员考核	中标方应验证责任单位是否定期对密码应用安全岗位人员进行考核;
40		建立关键岗位人员保密制度和调离制度	中标方应验证责任单位是否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。
41	建设运行	制定密码应用方案	中标方应验证责任单位是否依据密码相关标准和密码应用需求,制定密码应用方案;
42		制定密钥安全管理策略	中标方应验证责任单位是否根据密码应用方案.确定系统涉及的密钥种类、体系及其生存周期环节;
43		制定实施	中标方应验证建设单位是否按照应用方案实

		方案	施建设;
44		投入运行前进行密码应用安全性评估	中标方应验证被测系统投人运行前是否进行密码应用安全性评估;
45		定期开展密码应用安全性评估及攻防对抗演习	中标方应验证被测系统运行过程中,是否严格执行既定的密码应用安全管理制度,是否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。
46	应急处置	应急策略	中标方应验证责任单位是否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,是否立即启动应急处置措施.结合实际情况及时处置;
47		事件处置	中标方应验证责任单位在密码应用安全事件发生后,是否及时向信息系统主管部门及归属的密码管理部门进行报告;
48		向有关主管部门上报处置情况	中标方应验证责任单位在密码应用安全事件处置完成后,是否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。

2.6 测试服务成果物

（1）《商用密码应用安全性评估报告》

三、 服务要求

3.1 实施要求

本次项目测评实施及安全服务必须满足以下要求：

1、最小影响要求：投标人在测评实施过程中必须保证系统的正常运行，不

得导致系统运行中断或服务性能明显下降，尽可能降低对系统的负面影响。在进行有风险的操作前必须出具书面材料，明确风险提示，指导采购人做好应急措施，征得采购人书面许可后并选择业务低峰期进行下一步操作。

2、保密要求：对测评或技术服务过程中获取的信息严格保密，包括但不限于采购人网络拓扑结构、IP 地址、业务流程、业务数据、安全隐患等，未经授权不得泄露给任何单位和个人，不得利用保密信息进行任何侵害采购人的合法权益。

3、客观公正性要求：项目实施过程中，必须接受采购人的监督，每个测评环节完成后均由采购人进行审核确认，确保测评工作客观公正性。

4、规范性要求：测评实施等必须严格按照国家商用密码应用安全性评估相关标准进行。投标人须有严格质量控制体系,具备 ISO9001 质量认证体系或 ISO20000 或 CNAS 检验机构认可资质，并参照 ISO9001 或 ISO20000 或 CNAS 检验检测体系流程规范实施过程。

5、可控性要求：项目实施必须制定严格的实施计划及进度安排，经采购人审核确认后执行，确保项目实施的可控性。

3.2 工具及人员要求

1 检测工具配备

投标人应具备专业的漏洞检测工具，其功能应包含 Web 应用扫描工具或模块、主流虚拟机扫描管理系统、弱口令检测等功能，检测前工具应进行校准并升级至最新版本。

2 人员要求

参与项目的测评人员不少于 5 人，需具备专业的测评能力，参与商用密码应用安全性评估的人员需具备商用密码应用安全性评估人员测评能力考核资质证书，其中技术负责人须具备中级（含）以上测评师资质或高级信息系统项目管理师、网络规划设计师资质，具备丰富的技术和项目管理能力。

四、商务要求

1、投标总报价应是交钥匙工程（包括办理相关手续费用、设备运输、安装、调试、割接、培训、验收、服务等费用等全部内容）的最终优惠总价。在合同实施时，采购人将不予支付中标人没有列入的项目费用，并认为此项目的费用已包括在总报价中，采购人提出的设计变更除外。

2、中标人必须按国家有关财税规定开具发票。

3、严禁借用资质，发现借用或假冒资质投标的，采购人有权随时取消其中标资格或终止合同，并按照有关法律法规规定处理。

4、如中标人发生兼并、重组等，由新组建的公司按投标文件承担相应售后服务。

5、供应商具备相应的信息安全服务能力，同类单位三级等保测评案例不少于 10 个，技术需成体系，具备相关工作的管理经验。

6、供应商须省内具有固定的服务网点、技术服务团队及应急保障团队。其中本地应急人员不少于 5 人，须提供有效证明材料。

7、付款方式：根据乙方实际完成的评估系统数量结算。

（1）双方签订正式合同后，乙方向甲方开具相应金额的发票，甲方在 10 个工作日内向乙方支付本合同总价款的 50% ；

（2）乙方按合同要求提交报告后，乙方向甲方开具相应金额的发票，甲方在 10 个工作日内向乙方支付剩余价款。

8、验收标准：根据招标服务需求对信息系统开展商用密码应用安全性评估服务工作，出具符合 GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》的对应《信息系统商用密码应用安全性评估报告》。

9、供应商须按照以上服务要求条款提供规范服务，否则视为无效投标。