**广州医科大学附属番禺中心医院密评项目**

**市场调查公告**

**需求书**

1. 项目背景

为贯彻落实网络安全责任，保障信息系统安全，按照《商业密码应用安全性评估管理办法》、《广东省省级政务信息化项目商用密码应用工作指引》（粤密码协调组〔2020〕2 号）等文件要求，持续深化商用密码应用。

根据本院网络数据安全的工作需求，对2024年已备案的5个等保三级系统（详看表一）需进行商用密码应用建设方案编制、商用密码应用方案评估及商用密码应用安全性评估。现需拟聘请**具有总集能力**或**具有密评资质**的服务商为我院开展2025年度商用密码服务工作，及时发现存在的安全隐患，给出**商用密码应用方案评估报告、信息系统密码应用安全性评估报告**等，加强单位的网络安全防护能力，提高信息安全水平，保障院内业务安全平稳运行。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **责任范围** | **系统名称** | **级别** | **测评年度** | **状态** |
| 1 | 用户侧 | 财务网报系统 | 三级 | 2024 | 完成备案 |
| 2 | 用户侧 | 互联网医院系统 | 三级 | 2024 | 完成备案 |
| 3 | 用户侧 | 集成系统 | 三级 | 2024 | 完成备案 |
| 4 | 用户侧 | HIS系统 | 三级 | 2024 | 完成备案 |
| 5 | 用户侧 | 检验检查系统 | 三级 | 2024 | 完成备案 |

表格1 2024年完成备案的等保三级系统

1. 项目服务清单

|  |  |  |
| --- | --- | --- |
| 序号 | 服务名称 | 服务内容 |
|
| 1 | 商用密码应用建设方案评估 | 1）依据GB/T 39786—2021《信息安全技术信息系统密码应用基本要求》和GM/T 43206—2023《信息安全技术信息系统密码应用测评要求》对指定的5个三级系统的密码应用建设方案开展商用密码应用安全性评估服务。  2）服务期限：服务周期1个月，不含甲方整改时间。  3）交付物：《商用密码应用方案评估报告》  4）具体要求详看项目服务内容一 |
| 2 | 商用密码应用安全性评估 | 依据《密码法》、GB/T 39786-2021《信息安全技术 信息系统密码应用要求》、GB/T 43206-2023 《信息安全技术 信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》等相关文件及标准要求，对采购人的5个三级系统开展密码应用安全性评估等服务，全面分析信息系统的安全保护措施与密评相应等级之间的差距，为系统安全加固和密码技术使用提供整改建议，并根据信息系统实际情况，协助采购人开展密码应用安全整改，提高信息系统密码应用水平。  2）服务期限：服务周期12个月，具体以采购人确认的服务启动报审备案时间之日起至所有合同约定的系统完成所有测评工作止。  3）交付物：《信息系统密码应用安全性评估报告》  4）具体要求详看项目服务内容二 |
| 3 | 商用密码应用建设方案咨询服务 | 1）依据GB/T 39786—2021《信息安全技术信息系统密码应用基本要求》和GM/T 43206—2023《信息安全技术信息系统密码应用测评要求》，为采购人的5个《XX系统商用密码应用方案》进行商用密码应用建设**方案编制**提供专业性**指导服务**，直至并通过主管单位审核，取得主管单位出具的审核意见。  2）服务期限：服务周期1个月，具体以采购人确认的服务启动之日起至所有合同约定的系统完成所有测评工作止。  3）交付物：商用密码应用建设方案编制咨询服务及《方案编写咨询服务过程文档》  4）具体要求详看项目服务内容三 |

项目服务内容

**一、商用密码应用方案评估流程：**

1、方案评估流程：商用密码应用安全性评估主要内容包括技术要求、密钥管理、安全管理三方面，技术要求细分为物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全。

2、评估准备：评估人员与建设单位进行沟通会议，讲解评估过程，明确必要项目信息，收集有关项目资料。评估准备包括项目启动、信息收集两项主要任务。

3、评估修正：评估人员对密码应用方案进行评估，并将评估后发现的问题和整改建议汇总方案编制方。方案编制方修改完成后，提交给评估人员。若修改后的方案仍然存在评估修正活动，直到确认方案无误。评估修正包括评估方案、修正方案和主要任务。

4、安全性审查：如果方案中使用了包含非标准算法、协议的未经认证产品或服务而导致无法评估时，宜启动安全性审查。由委托单位提出申请，密码管理部门组织安全性审查。

5、报告编制：评估人员对评估过程中获得的系统基本信息、问题记录、密码应用方案进行汇总分析，形成评估结论，并编制评估报告。报告编制包括报告编写、报告确认、报告审核和报告输出四项主要任务。

**二、商用密码测评服务流程：**

（一）依据标准

供应商应依据国家或行业相关标准开展工作，依据标准（包括但不限于）如下：

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 43206-2023 信息安全技术 信息系统密码应用测评要求

GM/T 0002-2012 SM4分组密码算法

GM/T 0003-2012 SM2椭圆曲线公钥密码算法

GM/T 0004-2012 SM3密码杂凑算法

GM/T 0027-2014 智能密码钥匙技术规范

GM/T 0050-2016 密码设备管理 设备管理技术规范

GM/T 0051-2016 密码设备管理 对称密钥管理技术规范

GM/T 0052-2016密码设备管理 VPN设备监察管理规范

GM/T 0116-2021 信息系统密码应用测评过程指南

（二）测评内容

根据采购人信息系统的保护等级，并依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、GM/T 0116-2021 《信息系统密码应用测评过程指南》、GB/T 43206-2023 《信息安全技术 信息系统密码应用测评要求》要求，对被评估系统开展商用密码应用安全性评估，为信息系统的密码安全提供科学准确评价；全面分析信息系统的安全保护措施与密评相应等级之间的差距，为系统安全加固和密码技术使用提供整改建议；配合采购人监督信息系统承建单位根据整改建议进行整改，进一步提高采购人商用密码应用和管理水平。

1.安全通用要求

（1）信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准要求;

（2）信息系统中使用的密码技术应遵循密码相关国家标准和行业标准;

（3）信息系统中使用的密码产品、密码服务应符合法律法规的相关要求。

2.安全技术要求

从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面对信息系统密码应用进行检测评估（包含但不限于以下内容）：

（1）物理和环境测评内容：身份鉴别、电子门禁记录数据存储完整性、视频监控记录数据存储完整性。

（2）网络和通信测评内容：身份鉴别、通信数据完整性、敏感信息或通信报文的机密性、网络边界访问控制信息完整性、安全接入认证。

（3）设备和计算测评内容：身份鉴别、安全的信息传输信道、系统资源访问控制信息完整性、重要信息资源安全标记完整性、日志记录完整性、重要可执行程序完整性、重要可执行程序来源真实性。

（4）应用和数据测评内容：身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性。

3.安全管理要求

对制度管理、人员管理、建设运行、应急处置四个方面的安全管理进行测评，并协助采购人完善商用密码应用安全性管理制度。

**三、商用密码应用方案编咨询服务：**

1、协助采购人进行密码应用现状调研：对本项目涉及的密码应用现状进行调研，重点梳理分析项目涉及网络架构、用户终端、用户角色、重要/敏感信息资源、涉及敏感信息业务流程、现有密码产品及服务情况等。

2、协助采购人对项目商用密码应用整体设计提供咨询：从技术框架、物理与环境安全、网络与通信安全、设备计算安全、应用与数据安全等方面对本项目涉及的系统进行整体密码应用的设计，针对政策法规、标准规范的符合程度进行自我评价，提出包括密码应用部署、密钥管理等方面建设要求，并配套相应的管理体系设计和实施保障体系设计。

3、提供密码应用方案编制咨询服务：根据GB/T39786-2021《信息安全技术信息系统密码应用基本要求》、国家密码管理局《商用密码应用安全性评估管理办法(试行)》等相关标准要求，同时结合采购人信息化建设实际，协助采购人对本项目涉及的系统按照等级保护三级级要求完成密码方案编制工作，输出项目商用密码应用方案，并根据商用密码测评机构和省密码管理局有关审核意见，及时响应修改完善商用密码应用方案，通过省密码管理局审核，取得省密码管理局出具的审核意见。

1. 成果交付

服务商完成服务后的交付物至少应包括：《商用密码应用方案评估报告》、《信息系统密码应用安全性评估报告》、《方案编写咨询服务过程文档》（具体文档名称以采购人确认为准）。

1. 项目的实施要求

#### 1、实施要求

1. 投标人必须具备独立完成本项目的能力；
2. 投标人提供的资格、资质等证明文件应真实有效；
3. 投标人应对了解到的信息保密，并提供保密承诺；
4. 投标人应在项目现场实施周期内，中标方必须为本项目成立评估小组，所需电脑等设备自行提供；
5. 项目必须按照商用密码应用安全性评估的标准要求开展。

#### 2、人员要求

投标供应商服务期间需至少派遣1名测评师(通过商用密码应应用安全性评估考核)在现场和2名通过商用密码应用安全性评估考核人员组成服务项目团队提供商用密码应用安全性评估工作。

#### 3、质量保证

投标供应商应制定质量计划作为项目策划的一部分，质量计划应包括下列内容：

(1) 质量目标，尽可能以定量形式给出。

(2) 对质量活动的具体职责，诸如：评审和测试、配置管理和更改控制、对缺陷的控制及纠正措施。

(3) 质量计划应顺次列出从整体规划到成果提交全过程中的每一个工序(阶段)及其相应的控制规程和控制措施。

(4) 质量计划应在工作开始前提交采购人项目总负责人审核认可，并设置采购人参加的控制点。

(5) 采购人代表有权在工作时间内进入投标供应商与合同执行有关的工作场所进行质量控制与评价活动，投标供应商应为采购人的活动提供必要的条件，并给予必要的支持。

(6) 采购人对投标供应商进行的一切质量控制与评价活动，不能减免投标供应商的合同责任。

(7) 文件控制，必须对工作的执行和验证所需要的文件(例如规程、细则等)的编制、审核、批准和发放进行控制以保证参与活动的人员能使用完成该项活动所需的正确文件及适合版本记录，应建立并保存足够的质量保证记录(包括检查、确认及评审等记录)，记录应能体现质量的客观证据。

(8) 投标供应商须按照合同规定向采购人提交各种有关文件记录，并对文件记录的内容及其有效性负全部责任。

## 四、其它约定

1、签订合同：中标人应于接到中标通知书10个工作日内与招标人签订正式合同。

2、交货（服务）地点：广州医科大学附属番禺中心医院

3、服务期限：自签订合同之日起至提交《商用密码应用方案评估报告》、《信息系统密码应用安全性评估报告》、《方案编写咨询服务过程文档》（具体文档名称以采购人确认为准）并且备案成功为止。

4、服务技术要求：此项目需按照国家最新的密评标准实施。

5、验收要求：项目时间自本项目启动之日起至《商用密码应用方案评估报告》、《信息系统密码应用安全性评估报告》、《方案编写咨询服务过程文档》（具体文档名称以采购人确认为准）并且备案成功止；在通过项目交付物审核之后，本项目完成验收。

6、付款条件：签订合同后首付30%；出具《商用密码应用方案评估报告》、《信息系统密码应用安全性评估报告》、《方案编写咨询服务过程文档》（具体文档名称以采购人确认为准），并备案成功，收到发票后一个月内支付合同金额的70%。