东莞市生态环境局沙田分局立沙岛有毒有害气体应急预警系统平台信息技术应用创新项目等保测评及商密评估服务

采购需求书

序号	类别	需求
1	项目名称	东莞市生态环境局沙田分局立沙岛有毒有害气体应急预警系统平台信息技术应用创新项目等保测评及商密评估服务
2	项目业主情况	业主名称：东莞市生态环境局沙田分局 地址：东莞市港口大道沙田段660号服务大楼九楼
3	中介服务名称	检验检测服务或信息系统工程监理服务
4	对中介服务机构的资质要求	中介服务机构资质要求： 1.供应商必须是在中华人民共和国境内依法注册的独立法人、其他组织或自然人，具备独立的民事权利能力和民事行为能力，能够独立承担民事责任。 2.供应商应具有以下资质1）有效的网络安全服务认证证书等级保护测评服务认证；2）有效的商用密码检测机构资质证书。 3.本项目不接受联合体投标。 4.需要回避的机构：无。
5	服务内容和服务要求	在采购人授权的范围内，为“东莞市生态环境局沙田分局立沙岛有毒有害气体应急预警系统平台信息技术应用创新项目”提供网络安全等级保护测评服务及商用密码应用安全性评估服务。按照相关国家标准及行业标准、“东莞市生态环境局沙田分局立沙岛有毒有害气体应急预警系统平台信息技术应用创新项目”招标文件、合同、需求规格说明书等有关资料编制测评方案，并提交相关测评报告。 一、网络安全等级保护测评服务： 网络安全等级保护测评包括两个方面的内容：一是安全控制测

		评，主要测评项目的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。安全控制测评使用测评单元方式组织，分为安全技术测评和安全管理测评两大类。安全技术测评包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个方面的安全控制测评；安全管理测评包括；安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五个方面的安全控制测评。安全技术测评通过人员访谈、文档审查和实地察看的方式测评，安全管理测评通过通过人员访谈、文档审查的方式测评。 1）机房环境、配套设施； 2）整体网络拓扑结构； 3）网络设备：包括路由器、核心交换机、汇聚层交换机、无线网络设备、无线接入设备等； 4）安全设备，包括网闸、防火墙、IDS/IPS、防病毒网关、防垃圾邮件网关、抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、无线接入网关等； 5）安全管理中心：安全运维管理系统、数据库审计系统、综合安全审计系统、综合网管系统等； 6）数据库、中间件、终端设施（包括移动终端）、服务器等； 7）业务应用软件、系统管理软件； 8）重要管理终端； 9）网络管理员、系统管理员、审计管理员、业务管理员和安全管理员、安全主管等； 10）涉及到系统安全的所有管理制度、操作规程和记录等。 交付文件包括但不限于如下成果和报告：《网络安全等级保护测评报告》。 二、商用密码应用评估服务

		1）商用密码应用方案评估 密码应用方案包括密码应用解决方案、实施方案、应急处理方案三部分组成，这些方案的模板已经有国家密码管理局制定并发布实施。方案评估不是照本宣科机械式的评估，将与信息系统实际应用需求有效的结合，站在总体设计方案的高度，立足多个层面、多个安全要求进行综合论证，从而判断系统在某些方面是否存在安全风险，通过总体密码设计有效解决相应的安全问题。 交付物要求，出具相应系统的《商用密码应用方案评估报告》，并提交密码局完成备案。 2）商用密码应用安全性评估 为系统进行商用密码应用安全性评估，最终给出测评结论，形成测评报告，服务机构出具《信息系统商用密码应用安全性评估报告》。 从物理和环境、网络和通信、设备和计算、应用和数据 4 个层面对商用密码应用关于信息系统的密码技术设计情况进行分析与评估。 a）物理和环境密码安全设计评估:分析评估密码应用是否合理、合规的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是否得到有效控制。 b）网络和通信密码安全设计评估:分析评估密码应用是否合理、合规的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是否得到有效控制。 c）设备和计算层面评估:分析评估信息系统是否合理、合规的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是否得到有效控制。 d）应用和数据层面评估:分析评估信息系统是否合理、合规的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是否得到有效控制。 e）安全管理评估：分析评估本项目商用密码应用对影响商用密码防护效能的管理制度与措施是否进行规划和设计。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，密钥管理、人员管控，信息系统实施，应急预案。 交付物要求，出具相应系统的《商用密码应用安全性评估报告》，并提交密码局完成备案。 三、人员要求 本次网络安全等级保护测评服务及商用密码应用安全性评估服务要求测评团队按业主方要求提供测评服务，建立项目测评组，务实高效完成测评工作。具体要求如下： 1.项目经理（1 名）：负责项目测评合同的履行、负责项目的测评全过程管理工作。应具备网络安全等级测评师(高级)证书；商用密码应用安全性评估从业人员考核通过证明、注册渗透测试专家证书（CISP-PTS）、注册应急响应工程师证书（CISP-IRE）、网络与信息安全管理师证书（高级）等资质证书。 2.项目技术负责人（1 名），负责项目技术决策、质量把控、合规落地的核心责任人，统筹技术全流程管理。应具备注册信息安全工程师证书（CISP-CISE）、注册渗透测试工程师证书（CISP-PTE）、网络与信息安全管理师证书（中级或以上）、网络工程师证书、信息安全工程师证书以及 CISAW 信息安全保障人员认证证书（应急服务）等资质证书。 3.项目团队成员共 3 人或以上：服务团队测评工程师每名人员应至少具备以下证书：网络安全等级测评师证书(中级或以上)及商用密码应用安全性评估从业人员考核通过证明。 4.项目经理、项目技术负责人和开展测评的工程师按要求在报价方案中给出具体的名单、资质等证明材料并符合采购需求。 5.在合同签订前，须提供以上人员的有效证书复印件及其在供应

		商最近三个月内任意一个月为其购买的社保证明以备核实，否则视为放弃本次采购。若发现虚假应标，采购单位有权取消中标服务机构中标资格，并报有关管理部门严肃处理。 （四）测试工具配备要求 根据本项目测试内容，配备不同的测试工具，如等保 2.0 的智能测评系统、测评质量监管工具软件、数据安全测评系统、商用密码数字证书合规性测评软件或工具以及商用密码应用安全性测评作业系统或工具软件等。（注：自主研发的，提供计算机软件著作权登记证书扫描件；非自主研发的，提供合同关键页（合同关键页：合同封面、能体现该测评工具的合同内容、合同签署页）扫描件或发票扫描件）。 (五)保密要求 项目实施过程中，中标服务机构必须采取措施对本项目实施过程中产生的数据、技术文档等资料严格保密，否则，由于中标服务机构过错导致上述资料泄密的，中标服务机构必须承担相应的责任。项目完成后，采购单位、中标服务机构均有责任对本项目的技术和资料保密承担责任。 (六)报价要求 报价必须包括完成本项目规定工作所承担的全部费用、利润、税金、政策性文件规定及合同包含内的所有风险、责任等各项应有费用。
6	合同履行地点和方式	提供服务时间：以合同约定为准 地点：东莞市
7	公开选取方式和计价标准	公开选取方式：方案择优选取。 采购最高限价元。 报价方式：项目最高限价 90400.00 元，最低限价 89000.00 元。 计价标准：暂不做测算与评估，报价不作为方案择优唯一依据，最终结算以财政审核金额为准。
8	服务时间	具体以双方合同约定为准。

9	验收	具体以双方合同约定为准。
10	结算方式	1、签署项目合同后 15 个工作日内，采购单位向中标服务机构支付项目服务费总金额的 50%； 2、所测评的建设项目通过合同验收后 15 个工作日内，采购单位向中标服务机构支付项目服务费总金额的 50%； 3、每次申请付款时，中标服务机构应向采购单位递交等额合规的有效发票。
11	违约责任	具体以双方合同约定为准。
12	补充合同和 解决争议方式	采购合同中如有未尽事宜，双方协商一致后可以签订补充合同，但补充合同不得与相关法律法规和广东省网上中介服务超市相关管理制度相抵触。 双方因履行本合同而发生的争议，应协商、调解解决。协商、调解不成的，依法向甲方所在地人民法院起诉。
13	备注	1.业主单位、中选中介服务机构应当根据相关法律法规的规定自行拟定合同。 2.合同的实质性内容，应当与采购公告、采购结果的内容一致。合同的实质性内容是指合同标的、数量、质量、价款或者报酬、履行期限、履行地点和方式、违约责任和解决争议方法等（即表格中的序号 1-12）。 3.合同的变更、终止等，适用相关法律法规的规定。

附件 1：评分指标

部分	评分项	分值	评分标准
技术部分（50 分）	项目总体理解	10	评审委员会根据投标人对本项目服务背景、服务目标、服务原则与服务依据等情况内容的完善性、合理性及可行性进行评价： 1.对项目的需求、目标、意义，以及本项目开展思路和框架有全面、准确的理解，能够明确项目的输出成果，得 8-10 分； 2.能够理解项目的需求、目标、意义，以及本项目开展思路和框架，并能明确项目需求及输出成果，但是理解认识不够准确，得 4-7 分； 3.能够基本理解项目的需求、目标、意义，以及本项目开展思路和框架，对项目的需求及输出成果理解不够明确，得 1-3 分； 4.缺乏对项目总体理解认识的或未提供相应内容的，得 0 分
	项目服务方案	20	根据投标人编制项目服务方案，说明测评流程步骤、测评方法、测评工具介绍、项目管理制度等情况进行评价： 1.测评流程完整详细，评估方法专业规范，测评工具专业可靠，项目管理措施具体齐全、可操作性高，得 14-20 分； 2.测评流程清晰，评估方法基本明确，测评工具可用，项目管理措施基本合理、可操作性高，得 7-13 分； 3.测评流程不清晰，评估方法不明确，未提供测评工具，项目管理措施不合理、可操作性差，得 1-6 分； 4.缺乏服务方案介绍的或未提供相应内容的，得

			0 分。
	进度安排及项目质量保障措施	10	根据投标人编制本项目制定的进度安排及质量保障措施，对项目服务保密措施、风险防范措施的有效性和可操作性等情况进行评价： 1.项目计划明晰，时间把控非常合理，服务内容的安排十分明确、合理，制定了详细、规范的项目计划及保障措施，得 8-10 分； 2.项目计划明晰，时间把控基本合理，服务内容的安排基本明确、合理，制定了详细的项目计划及保障措施，得 4-7 分； 3.项目计划不明晰，时间把控不够合理，服务内容的安排不够明确、合理，没有详细项目计划及保障措施，得 1-3 分； 4.缺乏项目进度及质量保障措施的或未提供相应内容的，得 0 分。
	测试工具的配备能力	10	根据响应供应商提供的测试工具配备情况进行评审： 1、等保 2.0 的智能测评系统； 2、测评质量监管工具软件； 3、数据安全测评系统； 4、商用密码数字证书合规性测评软件或工具； 5、商用密码应用安全性测评作业系统或工具软件。 上述每满足一项得 2 分，最高得 10 分。 注：响应文件中提供购置合同复印件或租赁合同复印件或响应供应商自主知识产权等相关证书复印件，未提供的相应项不得分。
商务部分（40 分）	项目经理资质	10	项目经理（仅限一人）： 1.具有网络安全等级测评师(高级)证书；

			2.具有商用密码应用安全性评估从业人员考核通过证明； 3.具有注册渗透测试专家证书（CISP-PTS）； 4.具有注册应急响应工程师证书（CISP-IRE）； 5.具有网络与信息安全管理师证书（高级）； 每提供上述 1 个证书得 2 分，本项累计最高得 14 分。 注：响应文件中提供以上人员的有效证书复印件及其在供应商最近三个月内任意一个月为其购买的社保证明。不提供或未按要求提供相关证明材料不得分。
	项目技术负责人资质	9	项目技术负责人（仅限一人）： 1.具有注册信息安全工程师证书（CISP-CISE）； 2.具有注册渗透测试工程师证书（CISP-PTE）； 3.具有网络与信息安全管理师证书（中级或以上）； 4.具有网络工程师证书； 5.具有信息安全工程师证书； 6.具有 CISAW 信息安全保障人员认证证书（应急服务）。 每提供上述 1 个证书得 1.5 分，本项累计最高得 9 分。 注：响应文件中提供以上人员的有效证书复印件及其在供应商最近三个月内任意一个月为其购买的社保证明。不提供或未按要求提供相关证明材料不得分。
	服务团队成员资质	6	项目团队成员 3 人或以上：服务团队测评工程师每名人员应至少具备以下证书：网络安全等级测评师证书(中级或以上)及商用密码应用安全性评

			估从业人员考核通过证明。 每人具备以上一项证书得 2 分，本项累计最高 6 分。 注：响应文件中提供以上人员的有效证书复印件及其在供应商最近三个月内任意一个月为其购买的社保证明。不提供或未按要求提供相关证明材料不得分。
	同类业绩	15	根据响应供应商自 2023 年 7 月 1 日至响应文件递交截止时间止承接过的网络安全等级保护测评服务或商用密码应用评估服务相关业绩进行评分：每提供一项有效业绩得 3 分，本项累计最高得 15 分。 注：响应文件中提供合同关键页（包括体现合同标的、合同金额、签字盖章页、签署日期）复印件，业绩日期以合同签订日期为准，不提供或未按要求提供不得分。
价格部分（10 分）	报价	10	报价得分=（基准价/报价）*价格分值【注：最低的报价为基准价】