广东省韩江流域潮州供水枢纽数字孪生平台建设（2024年）项目安全测评、网络安全等级保护测评、验收测评服务采购需求书

一、项目概况

（一）项目背景

为贯彻落实水利部有关数字孪生水利建设工作部署、落实我省智慧水利建设相关文件要求和《广东省水利厅政务信息化建设规划（2022—2025年）》《局水利发展“十四五”规划》安排，解决潮州供水枢纽工程因运行多年存在的工程监测设施不足、智慧化管理水平不高及防洪调度、水资源配置“四预”能力不足等问题，推进数字孪生技术与省管大型水利工程管理业务深度融合，提升潮州供水枢纽智慧化感知、分析处理及智能化调度能力，需要实施广东省韩江流域潮州供水枢纽数字孪生平台建设（2024年）项目（以下简称“项目”）。

（二）项目主要实施内容

项目主要实施内容为基础设施服务、定制软件开发服务、系统业务运营服务3个部分:

1. 基础设施服务。租用省政数局云上增值安全服务，补充工程温度振动监测设备、库区自动化无人机、下游水文自动监测设备以及闸墩渗流监测设备等专业基础设施，完善枢纽工程感知能力。

2. 软件开发服务。从大屏端、中屏端、小屏端构建枢纽

工程安全运行、防洪调度、水资源配置、水污染应急调度“四预”孪生场景等，并建设平台移动管理程序，开发枢纽智能化管理应用。

3.系统业务运营服务。开展业务管理运营服务，构建枢纽洪水实时预报、水资源配置、防洪调度、突发水污染应急调度、工程安全态势预测等水利专业模型；开展枢纽数据处理运营服务，进行工程数据治理、气象数据解译，构建枢纽可视化模型、预案知识库等，提升枢纽智慧化管理能力。

项目总投资1478万元，于2025年7月正式开工建设，建设总工期18个月（其中试运行期6个月）。

二、测评服务基本情况

根据项目进展情况，现需采购项目安全测评、网络安全等级保护测评、验收测评服务（以下简称“测评服务”）。

（一）测评服务目标

通过测评服务，为信息化系统安全建设和管理提供系统性、针对性、可行性的指导和服务，优化信息安全的配置，对信息系统分级别实施保护，明确各信息化系统安全责任，加强信息安全管理，进一步提高系统的安全防护能力，保障信息网络和信息系统安全；及时发现项目建设过程中存在的质量问题和安全漏洞，检验系统是否达到建设目标，从而加强项目管理，有效提高信息化系统建设水平，实现项目预期建设目标。

（二）测评服务名称：广东省韩江流域潮州供水枢纽数字孪生平台建设（2024年）项目安全测评、网络安全等级保护测评、验收测评服务（编号：HJJ-FX-2026012）

（三）采购人：广东省韩江流域管理局

（四）采购预算：51.38万元

（五）服务地点：采购人指定地点。

（六）服务期限：签订测评服务合同之日起至测评服务通过验收之日为止。

三、测评服务要求

（一）安全测评服务

1.服务内容及服务要求

安全测评服务重点对网络、主机、应用、数据以及系统整体进行安全测评，评估系统是否具备足够的信息安全防护能力，是否满足行业及主管部门的安全管控要求，是否能够持续提供安全、稳定、高效的业务支撑，是否能够保障敏感信息及公众隐私安全等。具体测评对象和数量由采购方指定。测评具体需求见下表。

测评具体需求

安全层面	测评项
网络安全	结构安全、访问控制、安全审计、边界完整性、入侵防范、网络设备防护
主机安全	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制
应用安全	身份鉴别、访问控制、安全审计、通信完整性、通信保密性、资源控制
数据安全	数据完整性、数据保密性、备份和恢复
系统安全	漏洞扫描、渗透测试

须按国家和省级政务信息化有关标准、规范、要求提供服务。

2. 成果交付物

供应商完成安全测评服务后的交付物至少应包括:

（1）《信息系统安全测评报告》（纸质版及电子版各1份）;

（2）《信息系统安全测评整改建议》（纸质版及电子版各1份）。

具体成果交付物系统名称以采购人确认为准。

供应商需形成安全整改建议书和安全测评报告，其中安全整改建议书应包括安全问题清单及整改建议。安全测评报告的内容应包括测评依据、测评过程、测评内容、测评结果及测评结论。

（二） 网络安全等级保护测评服务

1.服务内容及服务要求

对于本次新建的广东省韩江流域潮州供水枢纽数字孪生平台进行网络安全等级保护测评服务，充分考虑网络安全现状、基于最新信息安全理论基础，通过应用国内各种最先进安全技术和最完善安全管理手段，按国家信息系统分等级保护标准体系要求，对信息系统按不同按等级保护信息系统标准设计，保证网络系统和应用系统安全稳定运行，保证各应用系统的应用安全，保障信息的机密性、完整性、抗抵赖性和可用性，形成涵盖整个系统的信息网络、应用和管理等各个层面的安全策略及安全总体方案，同时为将来的信息系

统发展提供可兼容的空间，最大程度地降低信息网的信息安全风险，确保整体信息安全目标的实现。

具体服务要求如下：

（1）安全物理环境

根据信息系统机房和现场安全测评记录，针对机房和现场在“物理位置选择”“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”和“电磁防护”等安全物理环境方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。（本项以广东省政务云平台等级保护测评报告为测评依据）

（2）安全通信网络

根据信息系统安全通信网络测评记录，针对通信网络方面在“网络架构”“通信传输”“可信验证”等方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

（3）安全区域边界

安全区域边界现场测评包括“边界防护”“访问控制”“入侵防范”“恶意代码和垃圾邮件防范”“安全审计”“可信验证”等边界区域防范措施进行检查。（本项以广东省政务云平台等级保护测评报告为测评依据）

（4）安全计算环境

安全计算环境现场测评包括“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”等几个方面的测评。

（5）安全管理中心

安全管理中心现场测评包括“系统管理”、“审计管理”、“安全管理”、“集中控制”等方面。

（6）安全管理制度

根据现场安全测评记录，针对信息系统在安全管理制度方面的“安全策略”、“管理制度”、“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

（7）安全管理机构

根据现场安全测评记录，针对信息系统在安全管理机构方面的“岗位设置”、“人员配备”、“授权和审批”、“沟通和合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

（8）安全管理人员

根据现场安全测评记录，针对信息系统在安全管理人员方面的“人员录用”、“人员离岗”、“安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

（9）安全建设管理

根据现场安全测评记录，针对信息系统在安全建设管理方面的“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”以及“服

务供应商选择”等测评指标，判断出与其相对应的各测评项的测评结果。

（10）安全运维管理

根据现场安全测评记录，针对 信息系统在安全运维管理方面的“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”以及“外包运维管理”等测评指标，判断出与其相对应的各测评项的测评结果。对运维管理方面与ITIL 体系的融合适应性进行评估。

通过现场测评，逐项找出系统现状与国家相关标准要求之间的差距，进行逐项分析、整体分析，给出差距分析报告，并给出整改建议方案。

待整改完毕后，进行结果确认，完成网络安全等级保护测评，出具测评报告，并协助采购人将测评报告报当地公安机关备案。

（11）须按国家和省级政务信息化有关标准、规范、要求提供服务。

2. 网络安全等级保护测评成果交付物

（1）《信息系统网络安全等级保护整改建议》（纸质版及电子版各 1 份）；

（2）《信息系统网络安全等级测评报告》（纸质版及电子版各 1 份）。

具体成果交付物系统名称以采购人确认为准。

3.其他

本项目平台等保级别拟定为二级，最终以评审专家评审结果为准。若最终评定级别为二级以上级别，本项目将不再另增加测评费用。

（三）验收测评服务

依据国家标准及系统需求规格说明书的要求，检验系统是否满足用户需求，保证信息系统项目质量，客观公正评测是否满足信息化建设项目的招标文件、合同文件的要求，通过评估系统的需求符合性，对系统功能、可靠性、效率等方面进行专业的测试，验证建设项目的建设内容是否达到建设目标，形成项目的验收测评报告，作为该项目验收的依据。

1.内容及服务要求

测评机构在验收过程中作为独立的第三方机构，应对其实施测评的信息化项目进行客观，专业的测试，并提供权威的测评结论。应遵照有关规定和规范，制订服务项目的测评方案，并根据测评方案中规定的指标和评判标准对指定测评对象(包括软硬件)实施检测，包括但不限于建设内容检查，应用系统，信息资源共享，公共信息平台等不同类型项目的测评，国(地)标等信息化标准审核，"数字政府"总体设计架构符合性审核等工作。在实施检测前与实施检测后分别提交详细的服务测评方案(包括对每种测评类型所采用标准，检

测方法和检测工具的详细描述)及第三方测评报告，服务验收测评报告中应包括服务符合性检查的所有内容。

（1）建设内容检查服务

包括但不限于以下工作：对照审核意见和立项方案备案稿逐项核查项目内容完成情况，检查项目管理是否规范，检查项目管理档案是否完整。按《软件工程软件开发成本度量规范》(GB/T36964-2018)和《省级政务信息化服务预算编制规范和标准》开展系统已建功能点评估，出具系统验收功能点计数项清单作为系统规模评估结果。

（2）应用系统测试

包括但不限于以下工作：功能测试，安全性测试，可靠性测试，性能测试，容错性测试，回归测试，可维护性测试，可移植性测试，易用性测试，适应性测试，接口测试，用户文档测试。

（3）信息资源共享测试

包括但不限于以下工作：完整性，一致性，准确性检查，内部数据库整合检查，数据格式规范性检查，信息资源目录注册完整性检查，共享信息资源提供检查，共享信息资源应用检查。

（4）公共信息平台测试

包括但不限于以下工作：信息门户测试，公共云平台测试，应用支撑平台测试，服务接口测试。

（5）国家或省各项信息化建设标准审核

包括但不限于以下工作：根据国家及省相关标准规范，检测并审核信息化项目建设是否满足相关标准。

（6）“数字政府”总体规划架构符合性审核

包括但不限于以下工作：审核项目技术架构，技术路线等是否满足省“数字政府”总体规划架构等。

（7）测试方法的响应情况

包括但不限于以下工作：检查各项测试内容所参照的技术标准的完备性，测试方法的规范性。

（8）测试工具的配备情况

包括但不限于以下工作：检查各项测试内容使用的测试工具的齐备性和充分性。

（9）标准规范要求

须按国家和省级政务信息化有关标准、规范、要求提供服务。

2.验收测评成果交付物

验收测评服务的成果交付物至少应包括:

（1）《测评方案》（纸质版及电子版各1份）;

（2）《问题清单》（纸质版及电子版各1份）;

（3）《测评报告》（纸质版及电子版各1份）。

具体成果交付物系统名称以采购人确认为准。

四、供应商资格要求

1.具备独立法人资格（需提供证书复印件）。

2.具有中国合格评定国家认可委员会(CNAS)颁发的检验机构认可证书(含CNAS实验室认可证书)或省级以上（含省、自治区、直辖市）质量监督部门颁发的检验检测机构资质认定证书(CMA)，证书须在有效期内(需提供证书复印件)。

3.具有公安部第三研究所颁发的网络安全服务认证证书等级保护测评服务认证或网络安全等级测评与检测评估机构服务认证证书，证书须在有效期内（需提供证书复印件）。

4.报价供应商未被列入“信用中国”网站失信被执行人、重大税收违法案件当事人名单，且未被“中国政府采购网”列入政府采购严重违法失信行为记录名单。

5.本次采购不接受联合体投标；不允许合同分包（须提供承诺）。

五、具体需求

（一）信用综合评价需求

供应商信用要优，具体参照在广东省网上中介服务超市的综合评价得分。

（二）服务报价需求

供应商需在指定的服务金额范围内进行报价，最低报价不是中选的唯一依据。

（三）经验业绩需求

供应商的水利信息化项目测评服务经验业绩要丰富，2023年1月1日至今，需承担过广东省水利信息化项目的安全测评服务（或安全检测）、网络安全等级保护测评服务、验收测评服务（或软件测评服务或系统测评服务）等三类测

评中至少 2 类服务业绩。承担测评服务经验业绩类别多者、数量多者、资金规模大者优先。

以上业绩需提供合同关键信息页扫描件，包括但不限于合同首页、合同内容、盖章页、签订时间等。

（四）团队人员配置需求

服务商应指派固定的团队为测评服务提供专业服务，团队成员不得少于 6 人。人员组成如下:

1.项目经理 1 人。负责测评服务总体管控、质量保障、沟通协调等。需至少具备以下条件之一:

（1）具有人社部门（原人事部门）或工信部门颁发的信息系统项目管理师证书;

（2）具有人社部门（原人事部门）或工信部门颁发的信息安全工程师或网络工程师;

（3）具有人社部门（原人事部门）或工信部门颁发的软件评测师;

（4）具有人社部门（原人事部门）或工信部门颁发的软件设计师;

（5）具有公安部网络安全等级保护评估中心（原公安部信息安全等级保护评估中心）或中关村信息安全测评联盟或公安部关键信息基础设施保护中心颁发的信息安全等级测评师证书或网络安全等级测评师证书。

2.技术负责人 1 人。负责测评服务总体技术把控、关键节点审核等。需至少具备以下条件之一:

（1）具有人社部门（原人事部门）或工信部门颁发的信息安全工程师或网络工程师;

（2）具有人社部门（原人事部门）或工信部门颁发的软件评测师;

（3）具有人社部门（原人事部门）或工信部门颁发的软件设计师;

（4）具有中国信息安全测评中心颁发的注册信息安全工程师（CISE）;

（5）具有公安部网络安全等级保护评估中心（原公安部信息安全等级保护评估中心）或中关村信息安全测评联盟或公安部关键信息基础设施保护中心颁发的信息安全等级测评师证书（高级）或网络安全等级测评师证书（高级）。

3.实施工程师团队，不少于4人。负责测评服务具体实施。团队成员需至少具备以下条件之一:

（1）具有人社部门（原人事部门）或工信部门颁发的软件评测师;

（2）具有公安部网络安全等级保护评估中心（原公安部信息安全等级保护评估中心）或中关村信息安全测评联盟或公安部关键信息基础设施保护中心颁发的信息安全等级测评师证书或网络安全等级测评师证书。

团队人员配置满足所需条件多者优先。以上人员需提供需提供人员身份证、资格证书复印件，以及在本单位任职的相关证明材料复印件，如：加盖政府有关部门印章的2026年1月以来任意一个月的的《社会保险参保人员证明》（至少须含养老保险）或单位代缴个人所得税税单等。

（五）测试工具需求

测评工作应遵循可控性原则，供应商需至少提供如下测

试工具之一:

（1）漏洞检测、扫描与渗透测试等相关工具;

（2）数据安全测评工具;

（3）恶意文件分析系统工具;

（4）软件测试用例设计系统工具;

（5）软件测试缺陷跟踪系统工具。

以上测试工具需具有合法授权（需提供计算机软件著作权登记证书或采购合同）。按需提供测试工具类别多者优先。

注：以上信用综合评价、服务报价、经验业绩、团队人员配置和测试工具的条件具备满足情况，影响整体方案择优。

六、采购方式

测评服务在广东省网上中介服务超市“检验检测服务”类进行采购，采用“方案择优选取”方式进行采购，报价方式选择“服务金额”，其中最低金额为 41 万元（约下浮 20%），最高金额为 51.38 万元。报价方案将在满足采购文件资质要求的前提下，综合考虑供应商在广东省中介服务超市的综合评分、服务报价、经验业绩、团队人员配置等基础上进行综合评分并择优选取。

七、验收要求

供应商完成合同约定所有测评服务工作，按要求提交成果交付物，由供应商发起验收申请，采购人进行验收。

八、承包方式

本服务为固定总价承包，包含完成合同服务内容所需的一切费用。

九、付款方式及要求

（一）首期款：签订合同后，采购人收到供应商支付申请和符合国家税务机关规定的正式发票后，采购人向供应商支付合同金额总价的 30%;

（二）进度款：项目通过完工验收且采购人收到供应商支付申请和符合国家税务机关规定的正式发票后，采购人向供应商支付至合同金额总价的 60%。

（三）尾款：测评服务通过采购人完工验收，且采购人收到供应商支付申请和符合国家税务机关规定的正式发票后，采购人向供应商支付合同剩余尾款。

因测评服务的资金来源为财政资金，使用省财政资金集中支付，具体支付额度及时间以省财政最终审定并下达的经费预算和时间为准。财政资金下达后，采购人在前款规定的付款时限内提出支付申报手续，即视为采购人已经按期支付。

十、保密要求

1.供应商需签订保密协议。

2. 双方在订立合同、合同履约过程中，知悉的商业秘密或者其他应当保密的信息，不得泄露或者不正当地使用；泄露、不正当地使用该商业秘密或者信息，造成对方损失的，应当承担赔偿责任。

十一、知识产权归属约定

供应商应保证本项目的技术、服务或其任何一部分不会产生因第三方提出侵犯其专利权、商标权或其他知识产权而引起的法律和经济纠纷；涉及到第三方提出侵权或知识产权的起诉及支付版税等费用由供应商方承担所有责任及费用，供应商还应当承担由此造成采购人损失。采购人基于本合同约定委托供应商定制开发的产品、程序、服务等的知识产权归采购人所有。

十二、报价须知。

(1) 报价供应商必须认真阅读采购需求中所有的事项，格式，条款和采购人需求等，对照资格要求逐项响应。报价供应商没有按照采购需求文件要求提交全部资料或资料缺项的，报价供应商代表与报价文件中所指定的人员不符的，报价不符合采购需求文件要求的，视为无效报价;

(2) 报价供应商必须保证递交的报价文件中材料的真实，且报价文件须加盖公章，否则视为无效报价。报价文件需写明供应商的名称(加盖单位公章)，联系人及联系电话;

(3) 报价供应商将正式报价文件(含公司营业执照副本)的盖章版纸质文件及存有电子版扫描文件的存储介质邮递至广东省汕头市龙湖区韩江路40号广东省韩江流域管理局。电子版报价文件须与纸质版报价文件一致，如不一致则以纸质版报价文件为准。