合同编号：

东西湖区城市运行管理平台建设项目

全过程咨询服务合同书

项目名称：东西湖区城市运行管理平台建设项目全过程咨询服务项目

甲　　方：武汉市东西湖区大数据中心（武汉市东西湖区社会管理网格化服务中心）

乙方 1（牵头单位）：中德华建（北京）国际工程技术有限公司

乙方 2（成员单位）：湖北星野科技发展有限公司

签订地点：湖北省武汉市

签订时间：二〇二三年九月

目 录

合同项目名称：东西湖区城市运行管理平台建设项目全过程咨询服务项目

甲方：武汉市东西湖区大数据中心（武汉市东西湖区社会管理网格化服务中心）

乙方 1（牵头单位）：中德华建(北京)国际工程技术有限公司

乙方 2（成员单位）：湖北星野科技发展有限公司

签订日期：2023 年 9 月 30 日

签订合同地点：武汉东西湖区

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》及有关法律规定，遵循平等、自愿、公平和诚实信用的原则，双方就下述建设项目委托全过程咨询服务事项协商一致，共同达成如下协议。

一、服务内容及服务范围

1、工作内容

全过程工程咨询服务，包括项目管理服务、深化设计服务、跟踪审计服务、信息系统等级测评服务和信息系统安全整改服务、密码应用评审、商用密码应用安全性评估服务、第三方软件测试服务内容。

2、服务范围

1、项目管理服务：对该项目的进度、变更、质量、风险、交付物等多方面进行全过程管理和咨询服务管控，有效保障项目建设的有序推进。

2、深化设计服务：负责完成项目的深化设计，配合完成设计范围的各项专项论证和评估，以及配合完成各类评审会并完成各阶段各项审批手续的办理等工作，设计应满

足现行相关设计标准。按甲方要求按时按质提交设计成果，并取得国家相关职能部门的审核，以及配合完成各项审批手续办理等工作。

3、跟踪审计服务：本项目将引入专业的第三方工程造价咨询机构，加强东西湖区城市运行管理平台建设项目的全过程管理，对建设过程及重点环节进行审计监督，包含本项目的承建方建设阶段全过程造价控制、跟踪审计等内容，保障建设资金合理利用，提高项目投资效益，实现审计工作向事前、事中、事后全覆盖。

4、信息系统等级测评服务和信息系统安全整改服务。

目标：分析甲方信息系统安全建设的情况，根据国家等级保护相关标准，对东西湖区城市运行管理平台建设项目相关系统（第三级）进行等级保护测评工作，提交符合格式要求的测评报告，并协助完成系统测评备案工作。

内容：

（1）对东西湖区城市运行管理平台建设项目相关系统（第三级）按照网络安全等级保护要求做等级保护测评。乙方将派出测评小组进行测评，并根据测评的内容和结果出具相应的测评报告，确认东西湖区城市运行管理平台建设项目相关系统是否通过此次测评达到相应网络安全等级要求。

根据东西湖区城市运行管理平台建设项目相关系统（第三级）信息系统的保护等级，并依据国家信息安全等级保护制度规定，参照 GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》、GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》对信息系统进行测评。

内容包括但不限于以下内容：

①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、安全管理中心五个方面的安全测评。

②安全管理测评：安全管理机构、安全管理制度、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测评。

③系统整体测评：从安全控制点间、区域间对单项测评结果进行分析和整体评价。

（2）整改咨询：针对系统存在的主要问题提出整改建议方案。

（3）系统测评：被测系统完成整改或即将超过合同期限后，出具正式测评报告。

5、密码应用评审

明确密码应用需求。协助甲方依据《政务信息系统密码应用与安全性评估工作指南》（2020 版）、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等标准对重要信息系统面临的安全风险和风险控制需求进行分析，明确物理和环境、网络和通信、应用和数据、设备和计算、应用和数据以及安全管理风险分析和密码应用需求分析，根据各信息系统的网络安全保护等级，协助甲方和承建方编制《政务信息系统密码应用方案》，完成重要信息系统密码应用需求和建设方案。

对编制的《政务信息系统密码应用方案》进行密评。在对政务信息系统的密码应用方案进行密评时，需依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》标准要求，分析密码应用方案是否对信息系统中需要保护的资产、数据提供了体系化、完备、适用的密码保障措施。若信息系统密码应用方案中存在不适用指标,需对不适用指标及其论证材料进行评估，审核不适用的具体原因的合理性，并审核是否存在可满足安全要求并达到等效控制的其他替代性风险控制措施。提交符合格式要求的《密码应用方案密码应用安全性评估报告》。

6、商用密码应用安全性评估服务

根据 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》，选择与之相对应的标准条款，对被测系统所涉及的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理及安全管理等方面进行评估，在评估工作完毕后出具密码应用安全性评估报告。

（1）物理和环境安全

物理和环境安全应包括：身份鉴别、电子门禁记录数据完整性、视频记录数据完整性、硬件密码模块实现等工作单元。

（2）网络和通信安全

网络和通信安全应包括：身份鉴别、访问控制信息完整性、通信数据完整性、通信数据机密性、集中管理通道安全、硬件密码模块实现等工作单元。

（3）设备和计算安全

设备和计算安全应包括：身份鉴别、远程管理身份鉴别信息机密性、访问控制信息完整性、敏感标记完整性、重要程序文件完整性、日志记录完整性、硬件密码模块实现等工作单元。

（4）应用和数据安全

应用和数据安全应包括：身份鉴别、访问控制、数据传输安全、数据存储安全、日志记录完整性、重要应用程序的加载和卸载、抗抵赖、硬件密码模块实现等工作单元。

（5）密钥管理

密钥管理应包括密钥生成、密钥存储、密钥分发、密钥导入与导出、密钥使用、密钥备份与恢复、密钥归档、密钥销毁等工作单元。

（6）安全管理

安全管理应包括制度、人员、建设、应急等工作单元。

7、第三方软件测试服务内容

依据《系统与软件工程 系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则GB/T25000.51-2016》按照甲方提供的东西湖区城市运行管理平台建设的相关资料，乙方针对该系统提供相应的测试服务，并出具符合要求的《测试报告》。

（1）功能测试：性能检测需要成交服务商依据需求规格说明书和系统建设的有关技术要求，结合用户对系统建设的整体功能方向，对系统涉及到的所有业务逻辑、功能逻辑、功能项等进行全覆盖的检测，及时发现软件系统中存在的问题并提出系统改进意见。

（2）性能效率测试：性能检测要求成交服务商站在用户体验的角度，使用专业的负载生成设备，在性能模型的基础上验证系统是否能够达到需求规格说明书中的性能指标，是否符合对系统设计时的性能关注点。

执行性能测试关键评价指标包括：资源指标和系统指标。资源指标与硬件资源消耗直接相关，而系统指标则与信息系统业务模型中的用户场景及需求直接相关。

（3）可靠性测试：通过可靠性测试可验证软件系统在规定的时间内以及规定的环境条件下，完成规定功能的能力。

（4）易用性测试 ：成交服务商应站在使用者的角度对系统的安装、功能、用户界面、系统辅助等易用性因素进行测试，通过各因素的表现，整体评价系统易用性。

（5）可移植性测试：可移植性测试应该遵循以下质量特性进行评价（但不限于）：

①适应性：产品或系统能够有效地、有效率地适应不同的或演变的硬件、软件、或

者其他运行（或使用）环境的程度。

②易安装性：表明在指定环境中，产品或系统能够成功地安装和/或卸载的有效性和效率的程度。

（6）兼容性测试：系统应通过兼容性测试，验证系统与其它软件共存、互操作的依赖程度与用户需求及预期是否相符合。

（7）可维护性：可维护性测试应该遵循以下质量特性进行评价（但不限于）：

①可理解性：用户可通过阅读相关文档，了解程序功能及其如何运行的容易程度。

②可测试性：表明论证程序正确性的容易程度。程序越简单，证明其正确性就越容易。

③可修改性：可修改性表明项目建设中的某系统功能程序容易修改的程度。

④可使用性：项目建设中的某系统功能程序方便、实用、及易于使用的程度。一个可使用的程序应是易于使用的、能允许用户出错和改变，并尽可能不使用户陷入混乱状态。

（8）用户文档测试：文档测试主要包含产品说明测试和用户文档集测试，检测内容包括：

①用户文档集应包含最终用户所需的全部用户文档。

②用户文档集应具备正确性、一致性、易理解性、易学性特性。

（9）安全性测试：主要测试应用系统的身份鉴别。

8、技术服务的方式

提供技术咨询，到场技术服务和提供技术报告。

9、技术及服务要求

服务成果应符合法律、技术标准、现行规范的强制性规定及合同约定。

二、服务期限及支付

1、服务期限

从签订本合同之日起至本项目服务范围内的全部工作内容完成并将成果文件移交使用单位之日止，最终期限与东西湖区城市运行管理平台建设项目实际发生保持一致。

2、服务费用

全过程本项目咨询服务费用为¥2628900.00 元（大写：贰佰陆拾贰万捌仟玖佰元整 ），其中乙方 1 费用为 ¥1526200.00 元（大写：壹佰伍拾贰万陆仟贰佰元整 ），乙方 2 费用为¥1102700.00 元（大写：壹佰壹拾万零贰仟柒佰元整 ）。该金额包括乙方完成本合同全部项目服务内容的全部费用、税费等。甲方不再为此另外支付任何费用。（甲方按照决算审计金额进行最终结算）。

3、人员要求（项目管理）

服务团队人员中须有注册咨询师、注册造价师、注册一级建造师、信息系统监理师等资质及政府部门信息化项目咨询服务经验。

（1）现场驻场服务人员：项目建设期项目管理服务团队驻场人员不得少于 2 人，运维和质保服务期人员不少于 1 人。

（2）咨询服务人员：参与项目咨询、方案审查服务人员不得少于 2 人，人员中须有注册造价师资质、注册咨询师资质。

4、费用支付

双方约定费用支付分四期完成，时间和比例分别为：

（1）乙方 1 费用为 ¥1526200.00 元（大写：壹佰伍拾贰万陆仟贰佰元整 ）。

①第一期：合同签订后甲方收到乙方 1 第一期应付款项足额发票，乙方 1 配合甲方向政府财政部门办理请款手续，完成财政请款和到款流程后 50 天内付款 35%（小写：

534,170 元；大写：伍拾叁万肆仟壹佰柒拾元整）。

②第二期：初验过程中，乙方出具项目管理阶段报告、承建单位绩效考评报告，本阶段项目全过程跟踪审计报告等报告。待承建方初验完成后，甲方收到乙方 1 第二期应付款项足额发票，乙方 1 配合甲方向政府财政部门办理请款手续，完成财政请款和到款流程后 50 天内付款完成 40%的付款；（小写：610,480 元；大写：陆拾壹万零肆佰捌拾元整）。

③第三期：项目上线试运行期间内，乙方完成第三方软件测试及等保测试、密评等工作，出具等保测评报告、密码测评报告、第三方软件测试报告项目管理阶段报告、承建单位绩效考评报告，本阶段项目全过程跟踪审计报告等报告。承建方完成终验后，甲方收到乙方 1 第三期应付款项足额发票，乙方 1 配合甲方向政府财政部门办理请款手续，完成财政请款和到款流程后 50 天内付款 20%（小写：305,240 元；大写：叁拾万伍仟贰佰肆拾元整）。

④第四期：项目进入运维及质保期后，乙方出具项目管理阶段报告、承建单位绩效考评报告，并配合完成决算审计后，甲方收到乙方 1 第四期应付款项足额发票，乙方 1 配合甲方向政府财政部门办理请款手续，完成财政请款和到款流程后 50 天内支付 5%尾款（小写：76,310 元；大写：柒万陆仟叁佰壹拾元整）。

（2）乙方 2 费用为¥1102700.00 元（大写：壹佰壹拾万零贰仟柒佰元整 ）。

①第一期：合同签订后甲方收到乙方 2 第一期应付款项足额发票，乙方 2 配合甲方向政府财政部门办理请款手续，完成财政请款和到款流程后 50 天内付款 35%（小写：385,945 元；大写：叁拾捌万伍仟玖佰肆拾伍元整）。

②第二期：初验过程中，乙方出具项目管理阶段报告、承建单位绩效考评报告，本

阶段项目全过程跟踪审计报告等报告。待承建方初验完成后，甲方收到乙方 2 第二期应付款项足额发票，乙方 2 配合甲方向政府财政部门办理请款手续，完成财政请款和到款流程后 50 天内付款完成 40%的付款；（小写：441,080 元；大写：肆拾肆万壹仟零捌拾元整）。

③第三期：项目上线试运行期间内，乙方完成第三方软件测试及等保测试、密评等工作，出具等保测评报告、密码测评报告、第三方软件测试报告项目管理阶段报告、承建单位绩效考评报告，本阶段项目全过程跟踪审计报告等报告。承建方完成终验后，甲方收到乙方 2 第三期应付款项足额发票，乙方 2 配合甲方向政府财政部门办理请款手续，完成财政请款和到款流程后 50 天内付款 20%（小写：220,540 元；大写：贰拾贰万零伍佰肆拾元整）。

④第四期：项目进入运维及质保期后，乙方出具项目管理阶段报告、承建单位绩效考评报告，并配合完成决算审计后，甲方收到乙方 2 第四期应付款项足额发票，乙方 2 配合甲方向政府财政部门办理请款手续，完成财政请款和到款流程后 50 天内支付 5%尾款（小写：55,135 元；大写：伍万伍仟壹佰叁拾伍元整）。

（3）乙方收款前必须向甲方递交正式增值税普通发票，否则甲方可以拒绝付款，且不承担违约责任。

5、甲方开票信息

企业名称：武汉市东西湖区大数据中心

统一社会信用代码：12420112MB181679XB

地址与电话：武汉市东西湖区临空港大道 189 号 027-83089971

开户银行与账号：交通银行武汉东西湖支行 421421080012001086523

发票类型：增值税普通发票

6、乙方 1 收款信息

账户名称：中德华建（北京）国际工程技术有限公司

开户账号：0200066019021101452

开户银行：工行北京西客站支行

7、乙方 2 收款信息

账户名称：湖北星野科技发展有限公司

开户账号：200762349510266

开户银行：武汉农村商业银行化工新城支行

三、甲方代表与咨询项目负责人

1、甲方代表：李梦雅，邮箱：2790142307@qq.com。

2、乙方项目总负责人：陈玉光，邮箱：964409807@qq.com。

3、乙方项目管理服务负责人：鲁冬训，邮箱：993677546@qq.com。

4、乙方项目深化设计服务负责人：李浩杰，邮箱：225511147@qq.com。

5、乙方项目跟踪审计服务负责人：王晓静，邮箱：281356422@qq.com。

四、验收与交付

1、供应商完成项目验收后，乙方提供项目管理、第三方软件检测、网络安全等级保护测评、商用密码应用安全性评估等报告。由甲方组织专家对乙方提供的项目管理服务、第三方软件检测服务、网络安全等级保护测评服务、商用密码应用安全性评估服务等进行评审，评审合格视为验收通过。

2、验收通过后，乙方需向甲方移交的资料包含但不限于与项目相关的项目管理阶

段报告、项目管理总结报告、绩效考评报告以及其它应当交付的资料、文件等。

3、本合同服务期届满后，乙方需要向甲方交付本项目相关的所有资料。

五、权利和义务

（一）甲方权利和义务：

1、甲方办理法律规定相关手续，并将与咨询服务有关的相应结果书面通知乙方。因甲方原因未能及时办理完毕前述许可、核准或备案手续，导致服务期限延长时，不由乙方承担责任。

2、甲方应向乙方提供咨询服务时所涉及的所有外部关系的协调以及与其他组织联系的渠道，以便乙方收集需要的信息，为乙方履行职责提供外部条件。

3、甲方应在本项目合同中或按本项目合同的规定及时向相关承包商、供应商、承建方本合同之外的其他咨询方等提供乙方及咨询项目总负责人的名称或姓名、管理范围、内容和权限以及其他必要信息。

4、甲方负责就乙方与甲方相关承包商、供应商、承建方本合同之外的其他咨询方等之间职权相重叠或不明确的情况予以协调和明确。

5、甲方应在不影响乙方根据服务进度计划开展咨询服务的时间内，对乙方以书面形式提出的事项做出书面决定。对乙方在贯彻落实甲方意见时提出的有关问题，甲方应及时予以解答。因甲方原因未能答复或答复不及时导致服务期限延长的，不由乙方承担责任。

6、甲方更换代表应提前书面通知乙方，乙方调换项目负责人须经甲方同意。

7、当甲方发现乙方人员不按本合同履行全过程工程咨询职责，或与相关承包商、供应商、承建方串通给甲方或项目造成损失的，甲方有权要求乙方更换不称职的乙方人

员，直到终止合同并要求乙方承担相应的赔偿责任。

8、乙方应保证其所提供的产品及服务不侵犯第三方的知识产权，如有使用第三方产品必须获得正式授权，且包含在合同价格内，甲方不再支付任何第三方软件费用，如因此发生法律纠纷。乙方承担发生的一切法律责任和相关损失(包括但不限于应赔损失、诉讼费、律师费等)。

9、本项目承载和产 生的数据资源归甲方所有，未经甲方书面授权，乙方无权在本项目之外使用上述数据资源，否则甲方有权追究乙方法律责任。

（二）乙方权利和义务

1、乙方应根据合同约定和约定的咨询服务内容以及要求提供咨询服务，组建能够满足咨询服务需要的咨询服务机构。

2、乙方在履行合同义务时，应严格按照国家法律法规、强制性国家标准以及合同约定履行职责，维护甲方的合法利益，保证服务成果的质量，运用合理的专业技术和经验知识，按照有经验的乙方为同等规模、性质和复杂程度的项目提供同等咨询服务时应有的职业标准，谨慎、勤勉地履行其在合同下的责任和义务。

3、法律、法规、规章有相应规定的，乙方及其乙方人员应具有履行咨询服务所需的资质或资格。

4、在本合同期内或合同终止后，未征得甲方有关方同意，乙方不得泄露与本工程、本合同业务有关的保密资料，不得泄露甲方的秘密和设计人、集成商等提供并的秘密。

5、乙方保证自签订本合同时起至履行完毕本合同项下全部义务时止，始终、不间断的具备符合国家法律、法规、部门规章规定的执行本合同所必须的资质。

6、未经甲方的书面同意，乙方不得转让、转移合同涉及的利益和义务，乙方更不

得将本合同项下的咨询服务转让给第三方。

7、乙方有义务指导并协助甲方整合项目信息并编制项目汇报材料。

六、知识产权

1、本合同签订前已经存在的知识产权（包括但不限于著作权、专利权、商标权、计算机软件著作权等）归原拥有方所有。本合同履行过程中产生的技术成果的知识产权(包括但不限于专利权、著作权、商标权，计算机软件著作权等)归甲方所有。

2、乙方非经甲方书面同意，不得已任何方式向第三方披露、转让和许可本项目的技术资料和文件（依法律、法规、规定。行政或者司法机关要求提供的除外）。除本项目研发工作需要之外，未得到甲方的书面许可，乙方不得以任何方式商业性地利用上述资料和技术。如乙方违反本条的规定，除立即停止违约行为外，还应向甲方承担违约责任，并赔偿甲方的损失。

七、安全及保密要求

1、甲方提供给乙方用于协作项目的各种技术资料（含各种介质）等，需妥善保管，未经甲方同意不得复制、销毁。

2、乙方非经甲方书面同意，严禁将甲方提供的用于协作项目的各种技术资料（含各种介质）等以告知、公布、发布、出版、传授、转让或者其他任何方式使任何第三方知悉。

3、在协作项目执行中，甲方有权对乙方执行保密协议的情况进行监督和检查，对不符合保密条款的行为，乙方应及时纠正或整改。因乙方违反保密条款的，应向甲方承担违约责任，若给甲方造成损失的，甲方有权向乙方追偿。

4、乙双方应严格遵守国家有关保密法律、法规及相关要求。

5、乙方未经对方同意，不得向任何第三方透露本合同内容及合同价款。

6、乙方应对工作过程中自甲方获得的所有数据资料承担保密责任，不得向第三方复制、转让、传播、泄露在项目中接触和了解到的甲方的所有数据资料及相关信息，不得擅自使用与数据库建设有关的电子数据。

7、乙方应当与项目工作人员签订保密协议，加强对工作人员的保密教育，采取必要技术措施，防止数据存取破坏和非法复制。

8、本合同关于保密的规定对乙方的管理人员、一般雇员以及其他受该方当事人委托、聘用直接或间接接触保密信息的单位或人员均有约束。

八、不可抗力

1、不可抗力是指合同当事人在签订合同时不能预见、不能避免且不能克服的自然灾害和社会性突发事件，如地震、海啸、瘟疫、骚乱、戒严、暴动、战争。

2、不可抗力发生后，甲方和乙方应收集证明不可抗力发生及不可抗力造成损失的证据，并及时认真统计所造成的损失书面通知对方。

3、任何一方遇到不可抗力事件，使其履行合同义务受到阻碍时，应立即通知合同对方，书面说明不可抗力和受阻碍的详细情况，并在合理期限内提供必要的证明。

九、违约责任

1、由于乙方原因未按合同约定的时间和质量交付咨询服务成果文件的，每逾期一日，乙方按本合同约定的咨询服务费用0.2%的标准向甲方支付逾期违约金。乙方逾期超过90日的甲方有权单方解除本合同，乙方除退还甲方支付的咨询服务费外，还应按本合同约定的咨询服务费用30%的标准向甲方支付违约金。

2、由于乙方违反合同第六条、第七条内容的，乙方按本合同约定的咨询服务费用

30%的标准向甲方支付违约金。

3、由于乙方除本合同第九条第1、2项以外的违约行为导致甲方单方解除本合同的，乙方除退还甲方支付的咨询服务费外，还应按本合同约定的咨询服务费用25%的标准向甲方支付违约金。

4、甲方逾期支付合同款的，以逾期付款金额为基数，按全国银行同业拆借中心公布的同期贷款利率（LPR）的标准向乙方支付违约金，直至全部付清之日。

5、因乙方原因导致咨询服务进度延误的，乙方应按照违约责任的约定承担违约责任。乙方承担违约责任后，不免除乙方继续完成咨询服务的义务。

十、争议解决

1、因履行本合同产生的争议，甲方、乙方应通过友好协商，解决在执行本合同中所发生的或与本合同有关的一切争端。如从协商开始 30 天内仍不能解决，则向甲方所在地人民法院提起诉讼。

2、甲方支付的诉讼费、律师费由败诉方负担。

3、在诉讼期间，除三方争议的合同内容外，本合同的其它部分内容应继续执行。

十一、双方承诺

1、乙方向甲方承诺，按照法律和技术标准以及合同约定提供全过程工程咨询服务。

2、甲方向乙方承诺，按照法律法规履行项目许可、核准或备案手续，按照合同约定提供开展全过程工程咨询服务活动的依据，按照本合同约定派遣相应的人员，提供咨询服务所需的资料和条件，并按照合同约定的期限和方式支付服务费用。

十二、其他要求

1、本合同甲、乙双方应遵守国家颁布的《中华人民共和国民法典》、《中华人民

共和国政府采购法》，并各自履行应负的全部责任和义务。

2、甲方保证按合同条款规定的时间和方式付给乙方到期应付的合同款，并承担应负的责任和义务。

3、乙方保证按合同条款规定的内容和服务期限向甲方提供合格的货物，并承担应负的责任和义务。

4、合同文件。下列文件为本合同不可分割的部分，与本合同具备同等法律效力：

4.1、招标文件；

4.2、中标的投标文件；

4.3、合同书；

4.4、合同条款；

4.5、武汉市东西湖区政府采购中心发出的中标通知书；

5.1、乙方1与乙方2为本项目中标联合体，本合同中未特殊说明乙方1或者乙方2，“乙方”统指乙方1与乙方2，相应条款内容对乙方1与乙方2均有法律效力，乙方1与乙方2就本合同约定的事项对甲方承担连带责任；

5.2、乙方在项目服务期内，按照项目总承包，总集成，总兜底的要求完成合同。乙方1作为牵头负责单位，负责项目总体进度和质量，充分协调乙方内部资源以支撑本项目全过程；

6、服务期限及付款条件。付款条件见上文“第二部分 服务期限及支付”；

7、合同金额。合同总金额为中标公示价人民币2628900.00元（贰佰陆拾贰万捌仟玖佰元整），分项价格在乙方的投标报价表中有明确规定；

8、合同生效。本合同经各方法定代表人或授权代表签字和加盖公章（或合同专用

章）后生效；

9、合同的份数。本合同一式伍份，具有同等法律效力，甲方执叁份，乙方1乙方2各执壹份；

10、合同的失效。本合同在合同价款全部结清后且运维结束时失效。

甲方（盖章）：武汉市东西湖区大数据中心（武汉市东西湖区社会管理网格化服务中心）

法定代表人（盖章）：

委托代理人（签字）：

乙方 1（盖章）：中德华建(北京)国际工程技术有限公司

法定代表人（盖章）：

委托代理人（签字）：

乙方 2（盖章）：湖北星野科技发展有限公司

法定代表人（盖章）：

委托代理人（签字）：

附件：项目服务要求

一、项目概述

本项目为东西湖区城市运行管理平台建设项目，以实现“城市运行管理平台”功能为目标，主要建设内容包括：城市运行态势一张图、无人机智能巡检、一体化指挥调度系统、综合应急指挥调度系统、智能应用场景（含云药房、智慧停车系统）、大数据平台、视频解析平台、时空信息云平台、可视化视频调度平台、统一门户平台、移动平台、数据资源池建设、数据汇聚服务、数据治理服务、数据服务总线、云资源、基础软件、安全设备建设等内容。

二、采购清单

序号	服务内容
1	“一网统览”城市运行管理平台网络安全等级保护测评（第三级）
2	“一网统管”城市运行管理平台网络安全等级保护测评（第三级）
3	区级大数据管理平台网络安全等级保护测评（第三级）
4	时空数据平台网络安全等级保护测评（第三级）
5	统一门户平台网络安全等级保护测评（第三级）
6	应用场景的网络安全等级保护测评（第三级）
7	“一网统览”城市运行管理平台商用密码应用安全性评估（第三级）
8	“一网统管”城市运行管理平台商用密码应用安全性评估（第三级）
9	区级大数据管理平台商用密码应用安全性评估（第三级）
10	时空数据平台商用密码应用安全性评估（第三级）
11	统一门户平台商用密码应用安全性评估（第三级）
12	应用场景的商用密码应用安全性评估（第三级）
13	东西湖区大数据中心信息系统第三方软件测试服务
14	东西湖区大数据中心信息系统项目管理服务

15	东西湖区大数据中心信息系统项目深化设计服务
16	东西湖区大数据中心信息系统项目跟踪审计服务

三、服务内容

（一）项目管理服务

为东西湖区城市运行管理平台建设项目提供项目管理服务，对该项目的进度、变更、质量、风险、交付物等多方面进行全过程管理和咨询服务管控，有效保障项目建设的有序推进。

（二）深化设计服务

负责完成项目的深化设计，配合完成设计范围的各项专项论证和评估，以及配合完成各类评审会并完成各阶段各项审批手续的办理等工作，设计应满足现行相关设计标准。按招标人要求按时按质提交设计成果，并取得国家相关职能部门的审核，以及配合完成各项审批手续办理等工作。

（三）第三方检测服务

依据 GB/T 25000.51-2016 《系统与软件工程系统与软件质量要求和评价（SQuaRE）第 51 部分：就绪可用软件产品(RUSP)的质量要求和测试细则》及国家有关测评标准规范对项目的建设内容实施测试，提供全面、严格的第三方检测服务，出具测试报告。

（四）网络安全等级保护测评服务

依据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》《GB/T 28449-2018 信息安全技术 信息系统安全等级保护测评过程指南》《信息系统安全等级保护测评准则》等标准规范的要求，通过访谈、检查、测试等技术手段对东西湖区城市运行管理平台建设项目全过程咨询和测评管理建设及服务的建设内容进行等级测评，提出安全整改建设建议方案，配合采购人对相关系统进行建设整改、安全整改、制度体系的完善等提供咨询服务，并协助到公安机关办理系统备案手续，使系统能够取得公安机关颁发的《信息系统安全等级保护备案证明》。

（五）商用密码应用安全性评估服务

依据《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 及 CNAS 检验等信息技术服务体系，对东西湖区城市运行管理平台建设项目全过程咨询和测评管理项目建设及服务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），为采购人开展密码应用方案设计，提供技术咨询及评估服务。出具商用密码应用安全性方案评估报告和商用密码应用安全性评估报告。

（六）跟踪审计服务

本项目将引入专业的第三方工程造价咨询机构，加强东西湖区城市运行管理平台建设项目的全过程管理，对建设过程及重点环节进行审计监督，包含施工阶段全过程造价控制、竣工决算审核等内容，保障建设资金合理利用，提高项目投资效益，实现审计工作向事前、事中、事后全覆盖。

四、服务要求

（一）项目管理服务

1、项目实施管理服务

为东西湖区城市运行管理平台建设项目提供项目管理服务，建立健全的项目管理机制：规范管理流程，提供以下服务：

（1）项目干系人管理服务：采集项目干系人，记录干系人信息，汇总业务单位、建设单位、承建单位、监理单位、第三方单位的信息和相关人员信息，管理干系人员信息。

（2）项目计划评审服务：检查项目中的计划文件，针对项目实施的总计划，每个阶段的子计划，比如需求管理计划、编码开发计划、硬件安装计划、变更管理计划、质量管理计划、沟通管理、人员配备管理计划、风险管理计划等进行分析核查。

（3）项目管控计划服务：通过分析项目总计划，针对每个项目，制定管控方案，制定项目管理计划，设置项目的关键检查。

（4）会议服务：安排项目协调例会、专题调度会等会议，掌握项目的实施细节，分析并针对性的提出项目管理的问题和解决方案，提供人员服务及会议场地、专家等费用支出，形成会议纪要。

（5）日常工作跟踪服务：参与项目的日常工作，对深化设计、付款、验收等关键环节、重要文档进行审核把关，配合采购人进行阶段性工作汇报总结等。

（6）方案咨询服务：提供项目咨询服务，组织各节点的专家评审服务，配合采购人形成考察咨询报告。

（7）项目总结报告服务：根据项目情况，汇总承建单位工作情况，周期性编写项目总结报告。

（8）过程文档检查服务：对项目的需求调研报告、编码规范、测试用例、测试报告、培训教材、试运行方案、试运行报告等文件进行检查，确保过程文档的完整、一致、规范和高质量，以保证项目顺利实施。

（9）项目健康度评估服务：项目健康度评估服务基于项目全过程作业数据采集，依据中标人项目管理经验和实践总结定义度量指标和度量方法及工具，在项目设计、实施过程周期性的对项目过程质量执行评估打分，并对扣分项及扣分原因进行详细记录，督促承建方在项目建设过程中改进项目过程质量；通过审查项目技术文档、监理文档、会议纪要、工作记录等资料，监管项目工作推进情况，评价承建单位和监理单位工作情况，给出当前项目健康度状况评估。

（10）问题跟踪闭环服务：根据项目资料及相关专题会的内容情况，按照项目建设要求及目标，及时发现项目建设过程中的问题，提出合理化建议，并编写项目问题跟踪报告。

（11）软件开发咨询服务：提供人员服务，形成咨询服务报告。

（12）流程合规性检查跟踪督导服务：提供人员服务，形成督办单。

2、项目验收管理服务

（1）验收资料完备性评估服务：对项目验收材料的完备性审查。按照验收规范，对验收材料的完备性审查，并出具《完备性审查意见表》。

（2）验收资料符合型性评估服务：对项目验收材料的符合性进行审查。包括对立项、采购、建设、验收等各阶段的各类项目资料进行符合性审查，并出具《符合性审查意见表》。

（3）项目现场检查服务：组织开展项目现场检查工作，对系统功能性能、采购设备型号、到货上线、测试等情况进行确认核查，并出具《现场检查意见表》。

（4）评审意见整理服务：参与项目验收评审，现场记录并整理专家组及部门评审意见。

（5）专家意见跟踪复核服务：跟踪项目建设单位对专家意见的响应情况，复核评审意见是否落实，落实结果是否达标。

（6）验收服务：配合采购人组织项目验收。

3、项目管理系统平台服务

提供符合本项目交付实施、验收管理等业务需求的项目管理系统平台，对本项目的项目管理提供信息化工具，实现项目信息集中展现、管理流程规范、建设任务可见、文档集中管理等目标。

4、人员要求（项目管理）

服务团队人员中须有注册咨询师、注册造价师、注册一级建造师、信息系统监理师等资质及政府部门信息化项目咨询服务经验。

（1）现场驻场服务人员：项目建设期项目管理服务团队驻场人员不得少于2人，运维和质保服务期人员不少于1人。

（2）咨询服务人员：参与项目咨询、方案审查服务人员不得少于2人，人员中须有注册造价师资质、注册咨询师资质。

（二）深化设计服务

1、完成项目深化设计

对东西湖区城市运行管理项目完成项目的深化设计，配合完成设计范围的各项专项论证和评估，以及配合完成各类评审会并完成各阶段各项审批手续的办理等工作，设计应满足现行相关设计标准。

2、完成项目深化设计的审批

按招标人要求按时按质提交设计成果，并取得国家相关职能部门的审核，以及配合完成各项审批手续办理等工作。

（三）跟踪审计服务

1、服务目标

跟踪审计服务工作内容为在服务范围内，根据采购人授权，依据国家有关法律、法规、技术规程、规范、标准以及信息化建设文件，对待审计的项目的工作量、进度、投资、变更进行全方位、全过程、全流程资金跟踪审计，确保项目资金的收、支、管等环节能进行有效监督，提升资金使用的效率和效果。具体包括但不限于下列目标。

（1）根据国家及省级有关建设项目全过程跟踪审计的法规、政策、文件规定。按照独立、客观、公正、公平的原则，及时完成采购人委托的结算审计、造价审核等工作，出具相关报告并保证报告的真实性、准确性、合法性。

（2）遵守职业道德，维护采购人的利益，做到公正、合理、合法，并严守秘密。

（3）指导采购人及参建单位建立完善的设计、验收、付款、管理等制度，保证项目建设规范运行，建设资金合法使用。

（4）监督并指导参建单位在项目实施过程中制定组织措施、经济措施、技术措施和合同措施以保证工程项目按预算或概算投资执行。

（5）协助采购人控制建设项目实施过程中的变更及造价，提出合理化建议，公平、公正的对建设项目工程造价进行全过程跟踪审核，以控制建设项目成本。

（6）对采购人提供的任务清单（模块功能点、人工、设备、服务等），提高任务清单的编制质量和精确度，切实防止漏项缺项，按任务清单计价规范及相关合同要求进行审核。

（7）确定工程造价控制目标，制定工程造价控制办法，审核资金使用计划，审核工程计量支付并提供付款建议，审核工程变更费用，审核索赔与现场签证费用，进行成本分析与造价控制目标的动态调整，提供产品、人工、服务等方面的价格信息咨询。

（8）审核相关项目参建单位提交的进度款申请、变更签证等，以及所有与工程总造价相关的文件及材料设备。

（9）配合采购人做好与项目建设方、项目管理方、监理方的协调工作，审核项目合同款支付，根据各方提供的进度款资料进行审核及绩效评估，并出具报告。

（10）做好日常现场工作记录，特别是测试工程、关键工序、关键节点等，及时向采购人反映跟踪审计过程中发现的问题。

（11）按采购人要求提供跟踪审计过程中的相关电子资料或纸质资料，按要求定期对跟踪审计情况进行汇报，并按照采购人要求出具报告。

（12）完成竣工结算的相关资料收集整理工作，对项目参建单位报审的工程结算进行审核，提供工程造价的控制与管理方面的其他技术咨询服务，完成项目竣工结算相关工作并按照采购人要求出具报告，配合审计部门的复核及决算审计。

2、项目服务内容

本项目跟踪审计的具体服务内容包括项目工程量核算和资金使用相关行为的审计工作，可按开工前阶段、实施阶段和竣工结算阶段展开。

（1）开工前阶段

1）对项目已经产生的跟踪审计范围内文件的合规合法性进行审查。

2）对项目已经发生的投资的合理性进行审计。

3）负责编制建设项目全过程跟踪审计工作计划。

4）根据承建方的任务清单、招投标文件和合同提出造价控制目标。

5）采购人要求的与项目相关的其他跟踪审计服务。

（2）建设实施阶段

1）审查合同是否认真履行，确保合同的真实、合法、合理以及有效地执行。

2）提供造价咨询服务；对项目工作量、造价的合理性以及资金使用支付的合规、合法性给出结论性意见，并按照采购人要求出具报告。

3）配合采购人加强对工程的管理，提高项目实施质量。

4）参加项目建设例会，配合采购人做好建设协调工作。

5）根据服务范围的项目合同付款约定，对付款条件、付款金额进行复核。按时审核工程量进度表，并签发付款意见。

6）督促项目参建单位完成竣工结算的资料整理收集工作。开展项目跟踪审计的各项检查、计量、取证、核对及其他工作；熟悉有关资料，审查项目参建单位所提供资料的合法性、真实性、完整性；向各分包单位明确审计要求，进一步了解项目的有关情况。

7）负责对工程清单、工程变更进行对比控制。定期组织召集采购人、项管、监理、参建单位等开会研讨，解决建设项目中有关工程量变更、造价等问题。

8）协助采购人、项管、监理共同做好项目建设中涉及的各种货物、服务等采购流程，对参建单位的采购行为进行监督和审核，督促参建单位规范其采购行为。

9）负责会同采购人、项管、监理等对工程进度款拨付进行严格审核并提供预付、支付合同款项的依据。

10）协助采购人、项管、监理对项目实施过程中的组织设计、进度计划等进行监督管理。

11）负责对采购人同意变更的工作量进行造价核算，结合任务清单以当时市场价、

信息价为标准，给采购人提出合理建议，最大限度降低投资额，避免结算超预算。

12）根据建设项目的具体情况，预测建设项目风险及可能发生索赔的诱因，制定防范性对策，规避或减少索赔事件的产生；协助采购人做好反索赔工作，督促参建单位履行合同约定义务，保证工程质量和按时竣工。

13）全面掌握并审查项目的批复立项资料、设计资料、历次调整概算的资料、相关的招投标资料、合同及结算资料、深化设计、任务清单、工程进度资料、初步验收资料和竣工决算报告等审查竣工工程内容是否按合同要求全部完成并及时办理工程决算，审查实际实施中出现的设计、合同、工程量等情况的变更资料，以及工程检查验收等各种签证是否真实、完整，变更的内容是否符合客观实际。

14）协助采购人、项管、监理等对已完成工程量进行确认；参加预算外工程量的计量、审查工作，严格把关。协助监理对工程数量、质量的监控，未经采购人核实确认的工作量不列为结算总价。

15）监督并指导参建单位事先编制好项目实施过程的资金使用计划,确定、分解投资控制目标，进行投资跟踪控制，定期进行投资实际支出与计划目标值的比较，及时采取纠正措施纠正实施过程中的偏差。

16）定期对项目的完成情况进行绩效评估。

17）采购人要求的与项目相关的其他跟踪审计服务。

（3）竣工结算阶段

1）审核服务范围内的项目工作量计算是否准确，变更部分与现行规定有无冲突，清单子目录套用是否正确，计价是否符合合同约定等。

2）审核项目相关模块功能点、人工、设备、服务等费用情况。

3）严格按建设项目招投标文件及合同规定对所完成项目工程量进行验收，审核招标工程标底和工程量计价清单的执行情况。

4）督促参建单位完成对竣工结算的资料整理工作，开展项目跟踪审计的各项检查、计量、取证、核对及其他工作。

5）把握好分项（子项）验收、初步验收、终验、运维和质保服务期间的跟踪审计协调工作，及时办理资料的交接手续，对工程投资的节约和超支情况进行汇总分析，对剩余资产进行妥善处理。

6）项目全部竣工并完成工程结算造价审核工作后，对工作量、造价的合理性以及资金使用支付的合规、合法性给出结论性意见，并按照采购人要求出具报告。

7）对项目的最终完成情况进行绩效评估。

8）参加项目验收工作并协助采购人、项管、监理等对已完成工程量进行确认。参加预算外工程量的计量、审查工作，严格把关。协助监理对工程数量、质量的监控。

9）采购人要求的与项目相关的其他跟踪审计服务。

3、团队人员要求

（1）组建项目全过程跟踪审计人员团队，并在合同生效至项目终验结束期间提供不少于 2 人的驻场服务，项目负责人需有注册造价师证书。

（2）驻场跟踪审计团队人员：不少于 2 人，其中具有经济类中级及以上职称不少于 1 人，造价工程师资质证书的人员不少于 1 人。

（3）项目终验结束后至本项目服务期结束期间，中标人按照采购要求提供服务，人员团队中需包括具有中级及以上职称不少于 1 人、造价工程师资质证书的人员不少于 1 人，并根据采购人需求提供项目驻场服务。

4、其他要求

（1）投标人应响应采购文件全部内容，并严格按照签订的项目合同全部内容提供优质而高效的服务。

（2）投标人须承诺对待工作认真负责，高效优质。

（3）投标人须对投标信息的合法性、真实性和有效性负责。

（4）投标人应自觉遵守国家和省、市有关法律法规和规定，接受采购人及相关行政监督部门、主管部门的监督，并严格遵守相关管理制度、办法并接受采购人的监督管理。

（四）第三方软件检测服务

1、服务内容及范围

序号	服务内容	系统名称
1	软件测试服务	城市运行管理平台

根据相关文件及标准要求，对需要进行测试的信息系统进行软件测试包括，功能、性能、兼容性、可靠性、易用性、信息安全性、维护性、可移植性、用户文档集测试，

出具符合要求的相关报告。

2、工作内容

●结论报告

依据《系统与软件工程　系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品(RUSP)的质量要求和测试细则GB/T 25000.51-2016》、GB/T 25000.10-2016《系统与软件工程 系统与软件质量要求和评价（SquaRE）第10部分：系统与软件质量模型》等标准的要求，对需要进行软件测试，出具符合要求的相关报告。

●回归测试

完成项目问题整改后，对整改后的信息系统进行复测，出具正式的相关报告。

●相关标准规范

采购内容需求执行的国家相关标准、行业标准、地方标准或者其他标准、规范。

序号	名称	标号或文号
1	《系统与软件工程系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则	GB/T 25000.51-2016》
2	《系统与软件工程 系统与软件质量要求和评价（SquaRE）第10部分：系统与软件质量模型》	GB/T 25000.10-2016

●测评实施原则

在项目实施过程中必须满足以下原则：

保密原则：对实施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采购人的行为。

标准性原则：项目的设计与实施应依据相关标准和规范进行。

规范性原则：投标方的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

可控性原则：项目安排工作进度要跟上进度表的安排，保证工作的可控性。

最小影响原则：实施工作应尽可能小的影响系统和网络，并在可控范围内；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。

整体性原则：项目实施的范围和内容应当整体全面，涵盖服务范围内的每一个功能

点。

3、整体要求

（1）投标人应详细描述本次软件测试和源代码安全审计的整体实施方案，包括项目概述、计划方案、实施过程中需使用测试设备清单、时间安排、阶段性文档提交等。

（2）投标人应详细描述测评人员的组成、及各自职责的划分。

（3）投标供应商必须具备丰富的项目经验，参与项目的测评人员不少于 3 人；投标人应提供本项目的高级测评师的或 NSATP-A 注册网络安全渗透评估专业人员证书；供应商应具有中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类一级）或质量管理体系认证证书(ISO9001)或软件企业证书。

（3）本次软件实施过程中所使用到的各种工具软件应符合国家相关要求，经招标人确认后由投标人提供并在软件测试中使用。

（4）投标人应指定参与项目的测评人员具有工业和信息化教育与考试中心颁发的软件测试专业技能证书。

●专用工具要求

本项目涉及工程实施和验收测试所需的工具，由投标人负责提供。在使用前，应对工具进行测评，如果需要则对工具进行软件升级。

●安全管理要求

为做好全过程的安全保密工作，在项目实施前、中、后三个阶段都要做好安全保密工作。

(1) 项目实施前

1）对实施人员要进行安全保密教育，制定安全保密措施；

2）签订安全保密协议。

(2)项目实施开展中

1）对系统配置、相关项目等信息进行严格的安全保密管理；

2）项目实施工具应经过严格测试和检验，确保不对被测试系统造成损失；

3）对被测单位信息系统发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围；

4）对测试项目资产信息、项目文档进行严格的保密管理；

(3) 项目实施开展后

1）认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏；

2）在其他风险测试任务或宣传材料中不涉及被测单位的秘密、敏感情况。

●售后服务

提供安全咨询服务

4、测评风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在项目实施过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责软件测试和源代码安全审计过程中的安全保密管理工作，对项目活动、项目人员以及相关文档和数据进行安全保密管理，对项目实施过程进行监督。

项目实施工作中可能出现的安全风险点，按照测试对象周密制定测试方法，根据被测试对象的不同采取相应的风险控制手段。不限于以下方法：

1）操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

2）人员与数据管理

必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测试与被测试单位之间应签署长期保密协议，实施人员与被测试单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

3）厂商协作

厂商需要提供各应用系统的名称、版本、开发语言等信息，在测试之前，分析可能存在的问题。

4、项目实施内容

序号	项目名称	模块	功能及技术参数
1	功能性测	功能完备性	功能集对指定的任务和用户目标的覆盖程度；

2	试	功能正确性	软件或系统提供具有所需精度的正确的结果和程度；
3		功能适合性	功能促使指定的任务和目标实现的程度；
4	性能效率测试	时间特性	产品或系统执行其功能时，其响应时间、处理时间及吞吐率满足需求的程度。
5		资源利用性	产品或系统执行其功能时，所使用资源数量和类型满足需求的程度。
6		容量	产品或系统参数的最大限量满足需求的程度。
7	兼容性测试	共存性	在与其他产品共享通用的环境和资源的条件下，产品能够有效执行其所需的功能并且不会对其他产品造成负面影响的程度。
8		互操作性	两个或多个系统、产品或组件能够交换信息并使用已交换的信息的程度。
9	易用性	可辨识性	用户能够辨识产品或系统是否适合他们的要求的程度
10		易学性	在指定的使用周境中，产品或系统在有效性、效率、抗风险和满意度特性方面为了学习使用该产品或系统这一指定的目标可为指定用户使用的程度。
11		易操作性	产品或系统具有易于操作和控制的属性的程度。
12		用户差错防御性	系统预防用户犯错的程度。
13		用户界面舒适性	用户界面提供令人愉悦和满意的交互的程度。
14	可靠性测试	成熟性	系统、产品或组件在正常运行时满足可靠性要求的程度。
15		容错性	尽管存在硬件或软件故障，系统、产品或组件的运行符合预期的程度。
16		易恢复性	在发生中断或失效时，产品或系统能够恢复直接受影响的数据并重建期望的系统状态的程度。
17	信息安全性测试	保密性	产品或系统确保数据只有在被授权时才能被访问的程度。
18		完整性	系统、产品或组件防止未授权访问、篡改计算机程序或数据的程度。
19		抗抵赖性	活动或事件发生后可以被证实且不可被否认的程度。
20		可核查性	实体的活动可以被唯一地追溯到该实体的程度。
21		真实性	对象或资源的身份标识能够被证实符合其声明的程度。
22	可移植性测试	适应性	产品或系统能够有效地、有效率地适应不同的或演变的硬件、软件、或者其他运行（或使用）环境的程度。
23		易安装性	在指定环境中，产品或系统能够成功地安装和/或卸载的有效性和效率的程度。

24		易替换性	在相同的环境中，产品能够替换另一个相同用途的指定软件产品的程度。
25	维护性测试	模块化	由多个独立组件组成的系统或计算机程序，其中一个组件的变更对其他组件的影响最小的程度。
26		可重用性	资产能够被用于多个系统，或其他资产建设的程度。
27		易分析性	可以评估预期变更（变更产品或系统的一个或多个部分）对产品或系统的影响、诊断产品的缺陷或失效原因、识别待修改部分的有效性和效率的程度。
28		易修改性	产品或系统可以被有效地、有效率地修改，且不会引入缺陷或降低现有产品质量的程度。
29		易测试性	能够为系统、产品或组件建立测试准则，并通过测试执行来确定测试准则是否被满足的有效性和效率的程度。
30	用户文档集测试	完备性	用户文档完整的说明软件包的功能以及在程序中用户可以调用的功能。
31		正确性	所检测用户文档的信息正确，没有歧义和错误的信息。
32		一致性	所检测用户文档自身内容或相互之间没有矛盾，并且不与产品说明矛盾每个术语的含义在文档中保持一致。
33		易理解性	所检测用户文档对正常执行工作任务的一般用户是易理解的，通过使用适当的术语、大量的图形表示、详细的解释以及引用有用的信息源来表达。
34		易学性	所检测用户文档可为用户学会如何使用该软件提供帮助。
35		可操作性	所检测的用户文档都有详细的目录表。

（五）网络安全等级保护测评服务

1、工作内容

1）定级备案服务

协助采购人需要进行测评的信息系统进行定级、备案材料的编写，协助采购人到公安监管等部门办理备案手续，确保信息系统安全保护等级定级准确、备案完整。

2）信息系统安全等级保护测评服务

依据《GB/T 22239-2019 信息安全技术信息系统安全等级保护基本要求》、《GB/T 28448-2019 信息安全技术信息系统安全等级保护测评要求》、《GB/T 25070-2019 信息安全技术网络安全等级保护安全设计技术要求》、《GBT28449-2018 信息安全技术 网络安全等级保护测评过程指南》、《GB/T 20984-2022 信息安全技术 信息安全风险评估方法》、《GB/T 22080-2008 信息技术安全技术信息安全管理体系要求》、《GB/T

22081-2008 信息技术安全技术信息安全管理实用规则》等标准的要求，对采购人需要进行测评的信息系统进行等级测评，出具符合国家网络安全等级保护格式要求的等级测评报告。测评范围为项目目标所涉及的机房基础设施、网络环境、主机层面、应用层、数据库层及相关安全辅助设备与管理制度。服务目标为项目目标最终通过公安部门及相关部门的等级保护检查要求。

测评内容应包括但不限于以下内容：

（1）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等五个方面的安全测评；

（2）安全管理测评：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等五个方面的安全测评；

（3）系统整体测评：从安全控制点间、区域间对单项测评结果进行分析和整体评价。

3）安全整改建设方案编制

安全整改建设方案应严格依据《信息安全等级保护管理办法》、《信息系统安全等级保护基本要求》、《信息系统安全保护实施指南》、《信息系统安全管理要求》、《信息系统通用安全技术要求》、《信息系统等级保护安全工程管理要求》、《信息系统等级保护安全设计技术要求》等标准规范要求制定《信息系统安全整改建设方案》，并在后续提供安全整改咨询服务，协助客户完善信息系统的安全防护措施，使系统达到等级保护相应级别的相关要求。

4）二次测评

完成信息系统安全整改后，对整改后的信息系统进行复测，出具正式的测评报告，送公安部门办理备案手续。

5）标准和规范

《中华人民共和国网络安全法》

《中华人民共和国计算机信息系统安全保护条例》国务院[1994]147 号

《关于加强信息安全保障工作的意见》中办发[2003]27 号

《关于信息等级保护工作的实施意见》（公通字 66 号）

《信息安全等级保护管理办法》公通字[2007]43 号

《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071 号）

《计算机信息系统安全保护等级划分准则》(GB17859-1999)

《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2019)

《信息安全技术 网络安全等级保护定级指南》(GB/T 22240-2020)

《信息安全技术 信息系统安全等级保护测评要求》(GB/T 28448-2019)

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术 信息安全等级保护 信息系统物理安全技术要求》(GB/T 21052-2007)

《信息安全技术 信息系统安全等级保护实施指南》

《信息安全技术 信息系统安全等级保护测评准则》

《信息安全技术 信息系统通用安全技术要求》(GB/T20271-2006)

《信息安全技术 网络基础安全技术要求》(GB/T20270-2006)

《信息安全技术 操作系统安全技术要求》(GB/T20272-2006)

《信息安全技术 数据库管理系统安全技术要求》(GB/T20273-2006)、

《信息安全技术 服务器技术要求》

《信息安全技术 终端计算机系统安全等级技术要求》(GA/T671-2006)

《信息安全技术 信息系统安全管理要求》(GB/T20269-2006)

《信息安全技术 信息系统安全工程管理要求》(GB/T20282-2006)

《信息技术信息安全管理实用规则》（GB/T 19716-2005 ）

《信息技术 安全技术 信息技术安全性评估准则》（GB/T 18336）

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

6）测评实施原则

在项目实施过程中必须满足以下原则：

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采购人的行为。

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等级保护的相关标准进行。

规范性原则：投标方的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

可控性原则：项目安排工作进度要跟上进度表的安排，保证工作的可控性。

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。

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

7）整体要求

（1）投标人应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

（2）投标人应详细描述测评人员的组成、资质及各自职责的划分。投标人应配置有测评资质的专业人员进行本次信息安全等级保护测评工作。

（3）投标人必须具备丰富的等级测评项目经验，参与项目的测评人员不少于3人；投标人应提供本项目的高级测评师的或NSATP-A 注册网络安全渗透评估专业人员证书；投标人应具有中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类一级）或质量管理体系认证证书(ISO9001)或软件企业证书。

（4）本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件（包括测试工具和报告编写工具）应符合国家相关要求，报告编写工具应取得中关村测评联盟授权，经招标人确认后由投标人提供并在信息系统等级保护测评中使用。

（5）信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。

8）专用工具要求

本项目涉及工程实施和验收测试所需的工具，由投标方负责提供。用于测评的工具主要包括服务器安全测评工具、网络设备安全测评工具、终端计算机安全测评工具、网站等应用系统安全测评工具等。在使用前，应对工具进行测评，如果需要则对工具进行软件或代码升级。

9）安全管理要求

为做好全过程的安全保密工作，在等级保护测评前、中、后三个阶段都要做好安全保密工作。

(1)等级保护测评前

1）对等级保护测评人员要进行安全保密教育，制定安全保密措施；

2）签订安全保密协议。

(2)等级保护测评中

1）对被测单位的性质、机房物理位置、网络与系统、应用与服务、资料与数据、人员与管理等方面的信息进行严格的安全保密管理；

2）等级保护测评工具应经过严格测试和检验，确保不对被测评系统造成损失，工作结束后不驻留任何程序；

3）对被测单位信息系统的信息资产、发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围；

4）对测评设备、介质进行严格的保密管理；

5）工作过程中对人员要实施封闭式集中管理；

6）对进场人员遵守被测单位的相关管理规定。

(3)等级保护测评后

1）认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏；

2）现场工作结束后，按被测单位的要求及时还原系统，确保系统中不遗留任何代码或可执行程序；

3）在其他风险测评任务或宣传材料中不涉及被测单位的秘密、敏感情况。

10）售后服务

项目验收后免费提供一年的安全服务，包括网站安全防护、漏洞修复、网络优化、配置加固、安全建设方案编写、安全管理制度完善、安全培训等安全咨询服务。

2、第三级系统测评内容

1）安全物理环境

测评对象主要为主机房，涉及工作单元 10 个，具体如下表：

序号	工作单元名称	测评指标

1	物理位置选择	a）机房场地应选择在具有防震、防风和防雨等能力的建筑内。
		b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
2	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
3	防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识。
		b）应将通信线缆铺设在隐蔽安全处。
		c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。
4	防雷击	a）应将各类机柜、设施和设备等通过接地系统安全接地。
		b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
5	防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。
		b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
		c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
6	防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
		b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
		c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
7	防静电	a）应采用防静电地板或地面并采用必要的接地防静电措施。
		b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
8	温湿度控制	a）应设置温、湿度自动询节设施，使机房温、湿度的变化在设备运行所允许的范围之内。
9	电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备。
		b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
		c）应设置冗余或并行的电力电缆线路为计算机系统供电。
10	电磁防护	a）电源线和通信线缆应隔离铺设，避免互相干扰。
		b）应对关键设备实施电磁屏蔽。

2）安全通信网络

测评对象主要为网络互联设备、网络安全设备以及网络拓扑结构等三大类，具体为：路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件，信息系统的整体网络拓扑结构，提供可信验证的设备或组件、提供集中审计功能的系统；涉及工作单元 3 个，具体如下表：

序号	工作单元名称	测评指标
	网络架构	a) 应保证网络设备的业务处理能力满足业务高峰期需要。
		b) 应保证网络各个部分的带宽满足业务高峰期需要。
		c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
		d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可 靠的技术隔离手段。
		e)应提供通信线路板、关健网络设备和关键计算设备的硬件冗余，保证系统的可用性。
	通信传输	a)应采用校验技术或密码技术保证通信过程中数据的完整性
		b)应采用密码技术保证通信过程中数据的保密性
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配登参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到 破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

3）安全区域边界

测评对象主要为：网闸、防火墙、路由器、交换机和无线接入网关设备、抗 ATP 攻击系统、网络回溯系统、抗 DDOS 攻击系统、入侵保护系统、入侵检测系统、防病毒网关和 UTM、综合安全审计系统、提供可信验证的设备或组件、提供集中审计功能的系统。涉及工作单元 6 个，具体如下表：

序号	工作单元名称	测评指标
1	边界防护	a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
		b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制。
		c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制。
		d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

2	访问控制	a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
		b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。
		c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许／拒绝数据包进出。
		d）应能根据会话状态信息为进出数据流提供明确的允许／拒绝访问的能力。
		e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
3	入侵防范	a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
		b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。
		c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。
		d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重 入侵事件时应提供报警。
4	恶意代码和垃圾邮件防范	a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级 和更新。
		b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级 和更新。
5	安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行 为和重要安全事件进行审计。
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
		d）应能对远程访问的用户行为、访问物联网的用户行为等单独进行行为审计和数据分析
6	可信验证	可信验证 可基于可信针对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将其验证结果形成审计记录并送至安全管理中心。

4）安全计算环境

序号	工作单元名称	测评指标

1	身份鉴别	a)应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。
		b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。
		c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
		d)应采用口令、密码技术、生物技术等两种或两种以上组合术来实现。
2	访问控制	a)应对登陆的用户分配账户和权限
		b)应重命名或删除默认账户，修改默认账户的默认口令。
		c)应及时删除或停用多余的、过期的账户，避免共享账户的存在。
		d)应授予管理用户所需的最小权限，实现管理用户的权限分离。
		e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则
		f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。
		g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
3	安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。
		c)应对设计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等;
		d)应对审计进程进行保护，防止未经授权的中断
4	入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序。
		b)应关闭不需要的系统服务、默认共享和高危端口。
		c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行 限制。
		d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。
		e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
		f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

5	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病 毒行为，并将其有效阻断
6	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等 进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安 全管理中心。
7	数据完整性	a)应采用校验技术或密码技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个人信息等。
		b)应采用校验技术或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个人信息等。
8	数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限千鉴别数据、重 要业务数据和重要个人信息等。
		b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重 要业务数据和重要个人信息等。
9	数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能。
		b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
10	剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
		b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
11	个人信息保护	a)应仅采集和保存业务必需的用户个人信息。
		b)应禁止未授权访问和非法使用用户个人信息。

5）安全管理中心

序号	工作单元名称	测评指标
1	系统管理	a） 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理 操作，并对这些操作进行审计。
		b） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源 配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

2	审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计 操作，并对这些操作进行审计。
		b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全 审计策略对审计记录进行存储、管理和查询等。
3	安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理 操作，并对这些操作进行审计。
		b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体 进行统一安全标记，对主体进行授权，配置可信验证策略等。
4	集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。
		b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。
		c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。
		d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。
		e）应对安全策略，恶意代码，补了升级等安全相关事项进行集中管理
		f）应能对网络中发生的各类安全事件进行识别、报警和分析。

6）安全管理制度

序号	工作单元名称	测评指标
1	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、 原则和安全框架等。
2	管理制度	a)应对安全管理活动中的主要管理内容建立安全管理制度
		b)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。
		c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度 体系。
3	制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定。
		b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。

7）安全管理机构

序号	工作单元名称	测评指标
1	岗位设置	a） 应成立指导和网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。
		b） 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。
		c） 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
2	人员配备	a） 应配备一定数量的系统管理员、审计管理员和安全管理员等。
		b） 应配备专职安全管理员，不可兼任。
3	授权和审批	a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。
		b)应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。
		c） 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
4	沟通和合作	a） 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期 召开协调会议，共同协作处理网络安全问题。
		b） 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。
		c） 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等 信息。
5	审核和检查	a)应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等 情况。
		b)应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。
		c)应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

8）安全管理人员

序号	工作单元名称	测评指标
1	人员录用	a） 应指定或授权专门的部门或人员负责人员录用。
		b） 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。

		c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
2	人员离岗	a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提 供的软硬件设备。
		b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
3	安全意识教育和培训	a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒 措施。
		b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。
		c）应定期对不同岗位的人员进行技能考核
		d)应对安全教育和培训的情况和结果进行记录并归档保存。
4	外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登 记备案。
		b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、 分配权限，并登记备案。
		c）外部人员离场后应及时清除其所有的访问权限。
		d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和 泄露任何敏感信息。

9）安全建设管理

序号	工作单元名称	测评指标
	定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。
		b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。
		c）应保证定级结果经过相关部门的批准。
		d）应将备案材料报主管部门和公安机关备案。
	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。
		b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划 和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件
		c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性 进行论证和审定，经过批准后才能正式实施。
	产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定
		b）应确保密码产品与服务的采购和使用符合国家密码主管部门的要求。

		c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品 名单
	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制。
		b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则
		c）应制定代码编写安全规范，要求开发人员参照规范编写代码
		d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制
		e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码 进行检测
		f)应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制
		g)应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查
	外包软件开发	a）应在软件交付前检测软件其中可能存在的恶意代码
		b）应保证开发单位提供软件设计文档和使用指南
		c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道
	工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理
		b）应制定安全工程实施方案控制工程实施过程
		c）应通过第三方工程监理控制项目的实施过程
	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告
		b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用 安全性测试相关内容
	系统交付	a)应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点
		b）应对负责运行维护的技术人员进行相应的技能培训
		c）应提供建设过程文档和运行维护文档
	等级测评	a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改
		b）应在发生重大变更或级别发生变化时进行等级测评
		c）应确保测评机构的选择符合同家有关规定
	服务供应商管理	a）应确保服务供应商的选择符合国家的有关规定
		b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全 相关义务

		c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制

10）安全运维管理

序号	工作单元名称	测评指标
	环境管理	a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理。
		b)应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理作出规定。
		c)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等
	资产管理	a)应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容
		b)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。
		c)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理
	介质管理	a)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储介质专人管理，并根据存档介质的目录清单定期盘点。
		b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录
	设备维护管理	a)应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理
		b)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等
		c)信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密
		d)含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
	漏洞和风险管理	a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
		b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

	网络和系统安全管理	a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和 权限。
		b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行 控制。
		c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新等方面做出规定
		d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置
		e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等 内容
		f)应指定专门的部门或人员对 H 志、监测和报警数据等进行分析、统计，及时发现可疑 行为。
		g)应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数， 操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。
		h)应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不 可更改的审计日志，操作结束后应删除工具中的敏感数据。
		i)应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。
		j)应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为
	恶意代码防范管理	a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等
		b） 应定期验证防范恶意代码攻击的技术措施的有效性。
	配置管理	a） 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组 件的版本和补丁信息、各个设备或软件组件的配置参数等
		b） 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基 本配置信息库。
	密码管理	a） 应遵循密码相关的国家标准和行业标准
		b）应使用国家密码管理主管部门认证核准的密码技术和产品
	变更管理	a)应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方 可实施。
		b)应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。
		c)应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

	备份与恢复管理	a)应识别需要定期备份的重要业务信息、系统数据及软件系统等。
		b)应规定备份信息的备份方式、备份频度、存储介质、保存期等。
		c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、 备份程序和恢复程序等。
	安全事件处置	a)应及时向安全管理部门报告所发现的安全弱点和可疑事件。
		b)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程， 规定安全事件的现场处理、事件报告和后期恢复的管理职责等。
		c)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录 处理过程，总结经验教训。
		d)对造成系统中断和造成信息泄露的重大安全事件采用不同的处理程序和报告程序。
	应急预案管理	a)应规定统 一 的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。
		b)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容
		c)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。
		d) 应定期对原有的应急预案重新评估，修订完善
	外包运维管理	a)应确保外包运维服务商的选择符合国家的有关规定。
		b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。
		c)应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展 安全运维工作的能力，并将能力要求在签订的协议中明确。
		d)应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感 信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

3、测评风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责信息安全测评过程中的安全保密管理工作，对测评活动、测评人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

安全测评工作中可能出现的安全风险点，按照检测对象周密制定测评方法，根据被测评对象的不同采取相应的风险控制手段。不限于以下方法：

1）操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

2）操作时间控制

对测评直接影响系统工作时，尽可能避开敏感时期。

3）人员与数据管理

必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测评单位之间应签署长期保密协议，测评人员与被测评单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

4）制定应急预案

根据测评范围界定的系统情况，在实施前制定应急预案。

5）关键业务系统风险控制

对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、测评和简单测试的方式进行。

6）优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

7）数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止测评过程中对设备与主机的损伤影响业务系统的正常运行。

8）厂商协作

厂商需要提供各应用系统的名称、版本、协议、开发语言、进程名和相应的端口号等信息，在测评之前，由三方共同分析测评对业务可能造成的风险，分析可能存在的问题。在测评过程中尽量规避这些风险。

（六）商用密码应用安全性评估服务

1、遵循的标准和规范

《中华人民共和国密码法》

《关于请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》

《政务信息系统密码应用与安全性评估工作指南》

《商用密码管理条例》

《GB/T 39786-2021 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过程指南》

《信息系统密码应用测评要求》

《信息系统密码应用高风险判定指引》

2、服务内容

根据相关文件及标准要求，对采购人重要信息系统进行商用密码应用安全性评估及相关服务，具体服务内容如下：

序号	项目名称	服务内容	具体要求
1	商用密码应用安全性评估服务项目	总体规划	协助甲方对重要信息系统面临的安全风险和风险控制需求进行分析，明确密码应用需求，根据各系统的网络安全保护等级，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，协助采购人和集成单位编制《政务信息系统密码应用方案》，完成重要信息系统密码应用需求和建设方案。
2		密码应用评审	乙方对编制的《政务信息系统密码应用方案》进行商用密码应用安全性评估（以下简称“密评”），乙方完成密码应用方案评审，输出《政务信息系统密码应用方案评估报告》的报告。
3		安全建设咨询	建设阶段涉及密码应用方案调整优化的，投标人需再次对调整后的密码应用方案进行评估。系统建设期间，投标人提供建设咨询服务，指导集成方完成安全建设。建设完成后，投标人对系统开展上线前的密评工作，确保系统满足国家相关标准。并提交符合格式要求的《商用密码应用安全性评估报告》
4		运行阶段密评	系统运行阶段，投标人定期对系统开展密评，提交符合格式要求的《商用密码应用安全性评估报告》的方案。

3、服务要求

总体规划

投标人协助采购人对重要信息系统面临的安全风险和风险控制需求进行分析，协助完成密码应用需求调研，根据各系统的网络安全保护等级，依据 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》，完成物理和环境、网络和通信、应用和数据、设备和计算、应用和数据以及安全管理风险分析和密码应用需求分析，根据分析结果确定密码应用需求，协助采购人和集成单位编制《政务信息系统密码应用方案》，完成重要信息系统密码应用需求和建设方案。

密码应用评审

在系统规划阶段，投标人负责对编制的《政务信息系统密码应用方案》进行密评。在对政务信息系统的密码应用方案进行密评时，需依据《基本要求》等标准要求，分析密码应用方案是否对信息系统中需要保护的资产、数据提供了体系化、完备、适用的密码保障措施。若信息系统密码应用方案中存在不适用指标,需对不适用指标及其论证材料进行评估，审核不适用的具体原因的合理性，并审核是否存在可满足安全要求并达到等效控制的其他替代性风险控制措施。提交符合格式要求的《密码应用方案密码应用安全性评估报告》。

安全建设咨询

信息系统建设期间，投标人提供建设咨询服务，指导采购人和集成方完成安全建设，提供安全咨询服务，确保集成单位按照《政务信息系统密码应用方案》开展建设，建设完成后，投标人对系统开展上线前的密评工作，确保系统满足国家相关标准。并提交符合格式要求的《商用密码应用安全性评估报告》。

运行阶段密评

信息系统运行阶段，投标人每年对等保第三级及以上的政务信息系统开展密评，并与网络安全等级测评等工作同步开展。密评完成后，提交符合格式要求的《商用密码应用安全性评估报告》。主要评估内容如下：

1、物理和环境安全

物理和环境安全应包括：身份鉴别、电子门禁记录数据完整性、视频记录数据完整性、硬件密码模块实现等工作单元。

2、网络和通信安全

网络和通信安全应包括：身份鉴别、访问控制信息完整性、通信数据完整性、通信数据机密性、集中管理通道安全、硬件密码模块实现等工作单元。

3、设备和计算安全

设备和计算安全应包括：身份鉴别、远程管理身份鉴别信息机密性、访问控制信息完整性、敏感标记完整性、重要程序文件完整性、日志记录完整性、硬件密码模块实现等工作单元。

4、应用和数据安全

应用和数据安全应包括身份鉴别、访问控制、数据传输安全、数据存储安全、日志记录完整性、重要应用程序的加载和卸载、抗抵赖、硬件密码模块实现等工作单元。

5、密钥管理

密钥管理应包括密钥生成、密钥存储、密钥分发、密钥导入与导出、密钥使用、密钥备份与恢复、密钥归档、密钥销毁等工作单元。

6、安全管理

安全管理应包括制度、人员、建设、应急等工作单元。

评估实施原则

在项目实施过程中必须满足以下原则：

保密原则：对评估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人的行为。

标准性原则：评估方案的设计与实施应依据国家相关标准进行。

规范性原则：投标人对工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

可控性原则：项目安排工作进度要跟上进度表的安排，保证工作的可控性。

最小影响原则：评估工作应尽可能小的影响系统和网络，并在可控范围内；评估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。

整体性原则：评估的范围和内容应当整体全面，包括密码应用于安全性评估等相关要求涉及的各个层面。

整体要求

（1）投标人应详细描述本次商用密码应用安全性评估整体实施方案，包括项目概

述、密评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

（2）投标人应详细描述测评人员的组成、资质及各自职责的划分。投标人应配置有测评资质的专业人员进行本次商用密码评估工作。

（3）投标人必须具备项目经验，参与项目的测评人员不少于 5 人；

（4）商用密码应用安全性评估需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。

专用工具要求

商用密码应用安全性评估工具须包含算法验证工具、随机数检测工具、协议分析工具和漏洞扫描工具等。在使用前应对工具进行检测。

安全管理要求

为做好全过程的安全保密工作，在商用密码应用安全性评估前、中、后三个阶段都要做好安全保密工作。

1、评估前

（1）对实施人员要进行安全保密教育，制定安全保密措施；

（2）签订安全保密协议。

2、评估中

（1）对被评估单位的性质、机房物理位置、网络与系统、应用与服务、资料与数据、人员与管理等方面的信息进行严格的安全保密管理；

（2）评估工具应经过严格测试和检验，确保不对被评估系统造成损失，工作结束后不驻留任何程序；

（3）对被测单位信息系统的信息资产、发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围；

（4）对评估设备、介质进行严格的保密管理；

（5）工作过程中对人员要实施封闭式集中管理；

（6）对进场人员遵守被测单位的相关管理规定。

3、评估后

（1）认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏；

（2）现场工作结束后，按被测单位的要求及时还原系统，确保系统中不遗留任何代码或可执行程序；

（3）在其他风险测评任务或宣传材料中不涉及被测单位的秘密、敏感情况。

风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在评估过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责商用密码应用安全性评估过程中的安全保密管理工作，对评估活动、评估人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

对评估工作中可能出现的安全风险点，按照检测对象制定评估方法，根据被评估对象的不同采取相应的风险控制手段。不限于以下方法：

1、操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

2、操作时间控制

对评估直接影响系统工作时，尽可能避开敏感时期。

3、人员与数据管理

必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。评估与被评估单位之间应签署保密协议，按国家有关要求做好保密工作。

4、制定应急预案

根据评估范围界定的系统情况，在实施前制定应急预案。

5、关键业务系统风险控制

对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用评估工具，采用访谈、测评和简单测试的方式进行。

6、优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

7、数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止评估过程中对设备与主机的损伤影响业务系统的正常运行。

8、厂商协作

按需提供各应用系统的名称、版本、协议、开发语言、进程名和相应的端口号等信息，在评估之前，由三方共同分析评估对业务可能造成的风险，分析可能存在的问题。

技术标准

物理和环境安全

主要涉及物理与环境安全：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方面评估。

测评单元	控制点	测评指标	应用要求
物理和环境安全	身份鉴别	7.1 a）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；	宜
	电子门禁记录数据存储完整性	7.1 b）可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；	可

网络和通信安全

主要涉及网络和通信安全：身份鉴别、通信数据完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完整性、安全接入认证方面评估。

测评单元	控制点	测评指标	应用要求
网络和通信安全	身份鉴别	7.2 a）宜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；	宜
	通信数据完整性	7.2 b）可采用密码技术保证通信过程中数据的完整性；	可
	通信过程中重要数据的机密性	7.2 c）宜采用密码技术保证通信过程中重要数据的机密性；	宜
	网络边界访问控制信息的完整性	7.2 d）可采用密码技术保证网络边界访问控制信息的完整性；	可

设备和计算安全

主要涉及设备和计算安全：身份鉴别、远程管理通道安全、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方面评估。

测评单元	控制点	测评指标	应用要求
设备和计算安全	身份鉴别	7.3 a）宜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；	宜
	系统资源访问控制信息完整性	7.3 b）可采用密码技术保证系统资源访问控制信息的完整性；	可
	日志记录完整性	7.3 c）可采用密码技术保证日志记录的完整性；	可

应用和数据安全

主要涉及应用和数据安全：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、不可否认性方面评估。

测评单元	控制点	测评指标	应用要求
应用和数据安全	身份鉴别	7.4 a）宜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实性；	宜
	访问控制信息完整性	7.4 b）可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；	可
	重要数据传输机密性	7.4 c）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机密性；	宜
		7.4 d）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机密性；	宜
		7.4 e）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；	宜
		7.4 f）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；	宜

管理制度

主要涉及密码管理制度：具备密码应用安全管理制度、密钥管理规则、建立操作规程、定期修订安全管理制度、明确管理制度发布流程、制度执行过程记录留存方面评估。

测评单元	控制点	测评指标	应用要求

管理制度	具备密码应用安全管理制度	7.5 a）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制度；	应
	密钥管理规则	7.5 b）应根据密码应用方案建立相应密钥管理规则；	应
	建立操作规程	7.5 c）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；	应

人员管理

主要涉及密码人员管理：了解并遵守密码相关法律法规和密码管理制度、建立密码应用岗位责任制度、建立上岗人员培训制度、定期进行安全岗位人员考核、建立关键岗位人员保密制度和调离制度方面评估。

测评单元	控制点	测评指标	应用要求
人员管理	了解并遵守密码相关法律法规和密码管理制度	7.6 a）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；	应
	建立密码应用岗位责任制度	7.6 b）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；	应
	建立上岗人员培训制度	7.6 c）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；	应
	建立关键岗位人员保密制度和调离制度	7.6 d）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。	应

建设运行

主要涉及密码建设运行：制定密码应用方案、制定密钥安全管理策略、制定实施方案、投入运行前进行密码应用安全性评估、定期开展密码应用安全性评估及攻防对抗演习方面评估。

测评单元	控制点	测评指标	应用要求
建设运行	制定密码应用方案	7.7 a）应依据密码相关标准和密码应用需求，制定密码应用方案；	应

	制定密钥安全管理策略	7.7 b）应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节安全管理要求参照附录 B；	应
	制定实施方案	7.7 c）应按照应用方案实施建设；	应
	投入运行前进行密码应用安全性评估	7.7 d）投入运行前宜进行密码应用安全性评估。	宜

应急处置

主要涉及密码应急处置：应急策略、事件处置、向有关主管部门上报处置情况方面评估。

测评单元	控制点	测评指标	应用要求
应急处置	应急策略	7.8 a）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；	应

五、验收标准要求

1、项目管理单位负责整理相应的项目建设档案和技术资料。负责进行单位工程验收和竣工综合验收中的项管验收，并出具验收报告。项管单位对出具的验收报告负责，接受使用单位和采购人的监督，一旦发现项管单位失职或不规范，将按合同违约进行处罚。

2、项目管理单位提出书面验收意见，并对其提出的意见负责。协助使用单位进行使用单位验收、采购人组织的专家验收及第三方正式验收。测评单位对其出具的各项测评报告负责。

3、本项目服务期届满后，服务范围内待审计项目通过审计部门的复核及决算视为验收合格。

附件：联合体协议

联合体协议书

中德华建（北京）国际工程技术有限公司(甲公司名称)以下简称甲方

湖北星野科技发展有限公司(乙公司名称)以下简称乙方

中德华建（北京）国际工程技术有限公司(甲公司名称)、湖北星野科技发展有限公司（乙公司名称)自愿组成联合体，参加武汉市东西湖区大数据中心东西湖区城市运行管理平台建设项目主项目公开招标采购项目投标，不再单独参加或者与其他供应商另外组成联合体参加本项目的采购活动。现就有关事宜订立协议如下：

1、甲方为联合体主体，乙方为联合体成员。

2、联合体将严格按照招标文件的各项要求办理投标事宜，投标文件中的所有承诺均代表了联合体各成员，联合体各成员共同承担相应的法律责任。

3、联合体分工原则：

甲方承担项目采购合同金额的58%，负责的工作为：项目管理服务、深化设计服务、跟踪审计服务；

乙方承担项目采购合同金额的42%，负责的工作为：第三方检测服务、网络安全等级保护测评服务、商用密码应用安全性评估服务。

4、若中标，联合体成员共同与采购人签订采购合同（本协议应作为采购合同的组成部分），就采购合同约定的事项对采购人承担连带责任，联合体主体负主要责任。

5、其他：甲方代表联合体各方对其投标文件盖章及签字，甲方所盖章签署的文件联合体各方均认可。

6、本协议书自签署之日起生效，若未中标，自本次投标有效期结束后自行失效；若中标，自合同书规定的期限之后自行失效。

7、本协议书正本一式两份，联合体成员各执壹份；副本一式四份，联合体成员各执壹份。

甲方（公章）：中德华建（北京）国际工程技术有限公司

法定代表人：

2023年08月14日

乙方（公章）：湖北星野科技发展有限公司

法定代表人：

2023年08月14日