

惠州市政务服务和数据管理局数字政府集约运营服务（2025年）项目-网络安全等级保护测评及商用密码应用评估服务 自行采购需求文件

一、采购项目概况

（一）采购项目名称

惠州市政务服务和数据管理局数字政府集约运营服务（2025年）项目-网络安全等级保护测评及商用密码应用评估服务

（二）项目基本情况

为落实《中华人民共和国网络安全法》《中华人民共和国密码法》要求，开展政务信息系统网络安全等级保护测评及商用密码应用安全性评估服务，保障数字政府平台安全合规运行。

（三）采购人：惠州市政务服务和数据管理局

（四）项目负责人/联系电话：杨子骁/0752-2898772

（五）采购方式：自行采购

（六）服务地点：惠州市政务服务和数据管理局

（七）中标（成交）供应商确定方式

本项目中标（成交）供应商的数量设置为1名。

评审小组将按评标总得分由高到低的排名顺序，每项采购包推荐第一名投标人为中标候选人，其次者可根据需要预设为替补候选人（1名）。

每项采购包需满足开标条件的数量设置不少于3家，开标前的投标人数量或经评审小组对投标文件进行资格性、符合性审查少于此要求的，将予以废标。

二、项目预算

本项目总预算为36.65万元，最终以合同签订金额为准。

三、服务期限

自合同签订之日起，至完成所有测评（评估）服务结束为止。

四、供应商资格条件

（一）资质要求：具备《中华人民共和国政府采购法》第二十二条规定的条件

- 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.法律和行政法规规定的其他条件。

采购人可以根据采购项目的特殊要求，规定供应商的特定条件，但不得以不合理的条件对供应商实行差别待遇或者歧视待遇。

（二）特定资格要求

- 1.投标人未被列入信用中国网（www.creditchina.gov.cn）“记录失信被执行人或重大税收违法失信主体或政府采购严

重违法失信行为记录”名单；不处于中国政府采购网

（www.ccgp.gov.cn）“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。

2.单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得同时参加本采购项目（或采购包）投标（响应）。投标人未参加本项目的除前期整体设计、规范编制或者项目管理、监理、检测等服务以外的其他采购活动。投标人必须符合法律、行政法规规定的其他条件。

3.投标人需具有《网络安全等级测评与检测评估机构服务认证证书》，且投标人需在网络安全等级保护网

（<https://www.djbh.net/>）的“网络安全等级保护测评机构服务认证获证机构名录”当中。在国家密码管理局商用密码应用安全性评估试点机构目录中或有商用密码检测机构资质申请受理回执证明。

4.本项目不接受联合体投标。

五、采购内容和要求

（一）采购清单

采购包预算金额：366500 元

序号	名称	数量	计量单位	最高限价（元）	备注
1	网络安全等级保护测评服务	1	项	132000	具体服务以合同约

2	商用密码应用安全性评估服务	1	项	234500	定为准。
合计：				366500	

(二) 网络安全等级保护测评服务

1. 测评系统清单

序号	系统名称 (项目管理平台上名称)	项目名称 (本次项目子项目名称)	系统属性		等保		备注
			是否上云	部署位置	首次/复评	级别	
1	XC 云环境	XC 云环境运维服务	/	电信机房	复评	三级	硬件
2	密码资源池管理平台	密码资源池管理平台运维服务	是	政务外网	首次	三级	软件
3	惠州市电子政务邮件系统	惠州市电子政务邮件系统运维服务	是	政务外网 / 互联网	复评	二级	软件
4	惠州市工程建设项目	惠州市工程建设项目	是	政务外网	复评	三级	软件

	目审批管 理系统	目审批管 理系统运 维服务					
--	-------------	---------------------	--	--	--	--	--

2.测评服务内容

中标人提供服务时，需自带综合漏洞扫描、Web 应用漏洞、渗透测试、模糊测试等专用测试工具，以实现本项目服务内容和目标。中标人在每次服务后需提交测试报告等服务成果物。

中标人按照国家网络安全等级保护相关政策文件要求，为所负责测评的应用系统提供等级保护测评服务，对系统进行定级备案和等级保护测评工作，掌握公共信息化系统安全防护和保障体系的现状，并编制《信息系统安全等级保护测评报告》，协助用户单位确保系统达到国家等级保护基本要求，并符合用户单位信息安全制度与规范的要求。

等级保护测评的主要服务内容包括：

(1) 确定测评方案

中标人应对信息系统开展前期调研，确定测评范围，并搜集信息，确定测评方案。

(2) 协助自查

中标人应依据国家有关信息系统安全等级保护要求，利用专业的安全测评设备和软件（专业安全扫描器、漏洞测试工具等）从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机

构、安全管理人员、安全建设管理、安全系统运维等方面对目标信息系统进行安全需求测评分析，确定信息系统安全建设整改需求，提交整改建议。

①协助自查方式

中标人所采用的等级保护测评方法至少包括人员访谈、文档检查和系统测试三类：

人员访谈：通过与信息系统有关人员进行交流、讨论等活动，获取证据以证明信息系统安全保护措施是否有效的一种方法。

文档检查：通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全保护措施是否有效的一种方法。

系统测试：依照相关标准与法律法规实施测评，使用等级保护检查工具作为主要的系统检查、信息收集、分析工具，同时结合其他专业脆弱性安全扫描工具、安全配置核查工具的扫描分析结果作为参考。将该阶段搜集的数据信息录入系统测评核查表，以供后期分析。配置核查扫描提供每个扫描任务的日志文件报告，方便后期进行行为审计。

②协助自查内容

中标人依据《网络安全等级保护基本要求》，从技术和管理方面等 10 个类别的单元测评内容对所测系统进行协助自查。

3.安全开展测评

(1) 安全技术测评

安全技术测评包括以下几个层面：

①安全物理环境。通过访谈、文档审查和实地察看的方式测评信息系统的物理安全保障情况。主要涉及对象为机房及相关配套设施。

②安全通信网络。通过访谈、配置检查和工具测试的方式测评信息系统的网络安全保障情况。主要涉及对象为网络互联设备、网络安全设备和网络拓扑结构等三大类对象。

③安全区域边界。通过访谈、配置检查和工具测试的方式测评信息系统的网络边界安全保障情况。重点测评的包括各边界防火墙，交换机等。

④安全计算环境。通过访谈、配置检查和工具测试的方式测评信息系统的操作系统、数据库等保障情况。

⑤安全管理中心。通过访谈、配置检查的方式测评信息系统的安全管理中心保障情况，主要涉及对象为纳入测评范围的安全管理中心等。

（2）安全管理测评

①安全管理制度。通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其他人员、各类管理制度、各类操作规程文件等对象。

②安全管理机构。通过访谈和检查的形式评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。

③安全管理人员。通过访谈和检查的形式评测机构人员

安全控制方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。

④安全建设管理。通过访谈和检查的形式评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。

⑤安全系统运维。通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。

（3）整体测评分析

中标人依据等级保护标准要求，进行技术和管理方面等10个类别的单元测评，完成对各个指标项的符合性评估后，需要对信息系统的安全情况进行总体评估。主要从层面内安全、层面间安全、区域间安全、系统结构安全进行整体评估，总结关键风险点。

中标人应单独出具单台主机的详细漏洞描述和解决建议作为后期整改依据。

（4）系统安全整改建议分析

中标人依据系统测评结果，针对不符合项、系统漏洞和系统风险点，提出安全整改建议，并形成安全整改方案。

（5）协助完成信息系统整改

中标人提供整改建议，协助采购人完成信息系统信息安全整改，达到国家规定的信息安全要求。

（6）开展验收测评

中标人对信息系统进行验收测评，按照公安部制定的网络安全等级测评报告格式编制等级测评报告，并协助采购人向公安机关提交符合要求的验收测评报告，完成测评备案及验收工作。

4.服务要求

中标人按相关政策文件要求完成测评后，根据测评类型提供现场测评记录、问题汇总清单（含整改建议）、等级保护测评报告、备案回执（具体文档名称以采购人确认为准），相关管理部门有对应要求的，中标人应当按照相关要求提供服务。

（1）测评问题单及现场测评记录

中标人按相关要求完成《现场测评记录》及编制《等级保护测评问题清单》，其中问题清单的格式与采购人协商制定，内容包括问题存在的系统、问题分类、问题详细描述、风险等级、问题整改方法等。

（2）等级保护测评报告

中标人按要求完成现场测评工作以后，根据被评估单位整改情况对整改结果进行确认，并根据最终的测评结果完成报告编制，并提交采购人审查。

5.项目管理要求

中标人不得以任何理由（不可抗力除外）拒绝提供服务。

①文档管理要求

投标人应在项目完成时，将本项目所有文档、资料汇集

成册交付给采购人，所有文件要求用中文书写或有完整的中文注释。验收后，投标人按国家、省以及采购人档案管理要求，向采购人提供装订成册的纸质文档至少 1 套，电子文档 1 套。

② 资产权属

中标人为委托项目任务提供的所有资料及工作成果归采购人所有。中标人不得使用或者授权他人使用本合同项下的成果及相关信息，否则相关收益归采购人所有，中标人应另向采购人承担侵权责任，并赔偿采购人全部损失。

中标人应保证委托项目任务的知识产权等相关权利均为其所有，否则因侵犯第三人的知识产权或其他相关权利而造成采购人的损失，包括但不限于采购人因此垫付任何费用，采购人有权要求中标人全部承担。

③ 保密要求

中标人应签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。

中标人不得以竞争为目的，或出于私利，或为第三人牟利而擅自保存、披露、使用采购人商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露采购人的商业秘密和党政机关保密信息。中标人在从事委托项目任务时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或中标人

内部与该项目无关的任何人员。

中标人对于工作期间知悉用户单位的商业秘密和党政机关保密信息（包括业务信息在内）或工作过程中接触到的政府机关文件（包括内部发文、各类通知及会议记录等）的内容，同样承担保密责任，严禁将政府机关内部会议、谈话内容泄露给无关人员；不得翻阅与工作无关的文件和资料。

严禁泄露在工作中接触到的政府机关科技研究、发明、装备器材及其技术资料和政府工作信息。

6.验收要求

（1）验收交付物

本项目验收材料应包括但不限于以下（名称暂定，最终以采购人确定的实际服务过程产生交付物名称为准）：

- ① 《信息系统等级保护备案证》及备案回执；
- ② 《等级保护定级报告》；
- ③ 《现场测评记录》；
- ④ 《等级保护测评问题单》；
- ⑤ 《信息系统等保整改建议》。

（2）验收标准

按照双方签订的技术协议完成双方约定的工作内容。

中标人提交成果必须符合采购人相关信息安全标准和管理办法。中标人必须完成项目要求的所有工作内容。

（3）验收方法

如双方认为项目已具备验收条件，中标人向采购人提出验收申请，采购人在接到中标人验收申请后组织对中标人提交的资料进行审核，确认中标人提交资料符合采购人信息化

项目验收标准后，由采购人组织相关人员对中标人第三方测评服务工作进行最终验收评审。

(三) 商用密码应用安全性评估服务（含商用密码应用方案评估服务）

1. 评估系统清单

序号	系统名称（项目管理平台上名称）	项目名称（本次项目子项目名称）	系统属性		密评		备注
			是否上云	部署位置	首次/复评	级别	
1	惠州市电子政务协同办公云平台	惠州市电子政务协同办公云平台运维服务	是	政务外网	复评	三级	软件
2	XC云环境	XC云环境运维服务	/	电信机房	复评	三级	硬件
3	密码资源池管理平台	密码资源池管理平台运维服务	是	政务外网/互联网	复评	三级	软件

4	惠州市 电子政 务邮 件系 统	惠州市电 子政务邮 件系统运 维服务	是	政务 外网/ 互联 网	首次	二 级	软 件
---	-----------------------------	-----------------------------	---	----------------------	----	--------	--------

2.评估服务内容

中标人严格按照《信息系统密码应用基本要求》(GB/T39786-2021)，对信息系统的总体要求，包括密码算法、密码技术、密码产品和密码服务进行测评；对信息系统的密码技术应用要求，包括物理和环境安全、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进行测评。中标人对所负责评估的系统提供商用密码应用安全性评估服务（含密码应用方案评估），最终输出被评估系统密码应用方案评估报告、商用密码应用安全性评估报告（含整改建议），满足商用密码应用安全性评估工作的验收要求，并协助采购人在测评结束后 30 个工作日内完成在密码管理部门的报告备案工作。具体内容包括：

序号	服务内容	服务内容子项	工作内容
1	需求沟通确认	需求沟通调研和确认工作实施要求	对安全评估的组织实施流程、风险管控效果、时间节点、交付成果、评估方式等基础信息进行沟通核实，确认服务需求和

			工作要求
2	基础材料搜集整理和现场沟通采集	按照评估准备实施要求，搜集整理必要素材	通过远程或现场会议方式与业务研发、运维部门技术团队和保障团队沟通评估所需基础素材、文档等必要信息
3	密码应用方案评估	密码应用方案评估	对委托方制定的密码应用方案（升级改造方案）进行评估，出具《密码应用方案评估意见》
4	指导整改	制定整改建议，明确具体措施、效果要求	根据《密码应用方案评估意见》，结合密码应用法律法规、政策标准及风险管控要求，提出评估意见和整改建议，指导系统集成商对被测系统按照《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）进行整改
5	验收评估	对整改完成	对整改完成后的系统，按

		后的系统进行评估	照《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）及评估通过的密码应用方案进行评估，给出最终评估结论。
--	--	----------	---

中标人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》（每个系统一份，具体文档名称以采购人确认为准）。

3.服务要求

中标人按相关政策文件要求完成测评后，根据测评类型提供现场测评记录、问题汇总清单（含整改建议）、密码应用方案评估意见、信息系统密码应用安全性评估报告（具体文档名称以采购人确认为准），相关管理部门有对应要求的，中标人应当按照相关要求提供服务。

（1）测评问题单及现场测评记录

中标人按相关要求完成《现场测评记录》及编制《等级保护测评问题清单》，其中问题清单的格式与采购人协商制定，内容包括问题存在的系统、问题分类、问题详细描述、风险等级、问题整改方法等。

（2）商用密码应用安全性评估报告

中标人按要求完成现场测评工作以后，根据被评估单位整改情况对整改结果进行确认，并根据最终的测评结果完成报告编制，并提交采购人审查。

4.项目管理要求

中标人不得以任何理由（不可抗力除外）拒绝提供服务。

①文档管理要求

投标人应在项目完成时，将本项目所有文档、资料汇集册交付给采购人，所有文件要求用中文书写或有完整的中文注释。验收后，投标人按国家、省以及采购人档案管理要求，向采购人提供装订成册的纸质文档至少 1 套，电子文档 1 套。

②资产权属

中标人为委托项目任务提供的所有资料及工作成果归采购人所有。中标人不得使用或者授权他人使用本合同项下的成果及相关信息，否则相关收益归采购人所有，中标人应另向采购人承担侵权责任，并赔偿采购人全部损失。

中标人应保证委托项目任务的知识产权等相关权利均为其所有，否则因侵犯第三人的知识产权或其他相关权利而造成采购人的损失，包括但不限于采购人因此垫付任何费用，采购人有权要求中标人全部承担。

③保密要求

中标人应签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。

中标人不得以竞争为目的，或出于私利，或为第三人牟利而擅自保存、披露、使用采购人商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人

披露采购人的商业秘密和党政机关保密信息。中标人在从事委托项目任务时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或中标人内部与该项目无关的任何人员。

中标人对于工作期间知悉用户单位的商业秘密和党政机关保密信息（包括业务信息在内）或工作过程中接触到的政府机关文件（包括内部发文、各类通知及会议记录等）的内容，同样承担保密责任，严禁将政府机关内部会议、谈话内容泄露给无关人员；不得翻阅与工作无关的文件和资料。

严禁泄露在工作中接触到的政府机关科技研究、发明、装备器材及其技术资料和政府工作信息。

5.验收要求

（1）验收交付物

本项目验收材料应包括但不限于以下（名称暂定，最终以采购人确定的实际服务过程产生交付物名称为准）：

- ① 《商用密码应用方案评估报告》；
- ② 《商用密码应用安全性评估报告》；
- ③ 《系统安全测评整改建议》。

（2）验收标准

按照双方签订的技术协议完成双方约定的工作内容。

中标人提交成果必须符合采购人相关信息安全标准和管理办法。中标人必须完成项目要求的所有工作内容。

（3）验收方法

如双方认为项目已具备验收条件，中标人向采购人提出

验收申请，采购人在接到中标人验收申请后组织对中标人提交的资料进行审核，确认中标人提交资料符合采购人信息化项目验收标准后，由采购人组织相关人员对中标人第三方测评服务工作进行最终验收评审。

（四）商务要求：

1.项目启动时间：服务合同签订后，5个工作日内启动服务。

2.投标有效期：从提交投标文件的截止之日起90日历天。

3.采购资金支付期次如下：

（1）启动服务合同签订并启动服务后，在收到发票之后10个工作日内完成支付至合同总金额中的30%；

（2）在等保测评、密评服务方案通过评审备案后且收到乙方提供的合法有效等额增值税发票起10个工作日内，支付合同总价的50%；

（3）在项目通过验收后且收到乙方提供的合法有效等额增值税发票起10个工作日内，支付合同总价的20%。

4.验收依据：

依据本服务项目的合同及双方补充协议、备忘录、项目任务委托书等文件。

5.验收要求：

符合以下条件后，中标人应及时申请交付确认：

基于中标人提交的测评服务方案，采购人完成方案评估备案，项目材料齐全。

因财政资金未能及时拨付到位导致采购人无法按时支

付相应价款给中标人，中标人表示谅解，采购人不承担因款项延期拨付给中标人造成的各类损失（如利息、连带责任等），不得由此追究采购人的违约责任。

六、评审方法

拟采用以下第 1 种评审方法：

- 1.综合评分法；
- 2.最低价法；
- 3.其他。

评审因素	评审标准	
分值构成	价格部分 10.0 分 商务部分 30.0 分 技术部分 60.0 分	
价格部分	投标报价得分（10.0 分）	各有效投标供应商的评标价中，取最低者作为基准价，各有效投标供应商的价格评分统一按照下列公式计算：价格评分 = (基准价 ÷ 评标价) × 10
商务部分	资质情况（3.0 分）	在投标文件中提供国家认证认可监督管理部门批准设立的认证机构颁发并在有效期内认证证书： 1、具有质量管理体系认证证书 ISO9001 证书，得 1 分； 2、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（风险评估二级）或

		<p>CCRC 信息安全服务资质认证证书(信息安全风险评估一级)，得 1 分；</p> <p>3、具有中国信息安全测评中心颁发的国家信息安全漏洞库 (CNNVD) 技术支撑单位等级证书，得 1 分。</p> <p>需提供相关证明材料复印件并加盖应答人公章，未按要求提供的不得分。</p>
	<p>同类项目业绩经验 (6.0 分)</p>	<p>投标人需提供 2022 年 1 月 1 日以来承接同类项目相关业绩，每提供一项得 2 分，最高得 6 分。投标人需提供中标通知书或合同关键页等相关扫描件证明材料。(合同关键页包括：合同封面或首页、服务内容页及双方签章页；加盖供应商公章) 作为评审依据，无提供或提供不全或提供的证明材料不清晰明确，评委无法辨认的，则不得分。</p>
	<p>项目负责人 (5.0 分)</p>	<p>投标人拟投入本项目的项目负责人 1 名，具有：</p> <p>1、具备商用密码应用安全性评估从业人员考核合格证书，得 1 分。</p> <p>2、具备网络安全等级保护测评师证书 (高级)，得 1 分。</p> <p>3、具备重要信息系统安全等级保护培训证</p>

		<p>书（CIIP-T），得1分。</p> <p>4、具备信息安全保障人员认证证书 CISA W 风险管理(专业级)，得1分。</p> <p>5、具备注册信息安全专业人员证书(CISP)，得1分。</p> <p>注：需同时提供项目负责人在投标单位缴纳社保证明复印件以及相关有效资质证书复印件，不提供不得分。要求为2025年1月至今任意1个月社保证明文件复印件及以上要求的对应证书复印件才能得分。</p>
	<p>技术负责人 (6.0分)</p>	<p>投标人拟投入本项目的技术负责人1名，具备以下情况：</p> <p>1、具备商用密码应用安全性评估从业人员考核合格证书，得2分。</p> <p>2、具备网络安全等级保护测评师证书（中级及以上），得2分。</p> <p>3、具备信息安全保障人员认证证书 CISA W 安全运维(专业级)，得2分。</p> <p>每提供一项得2分，本项最高得6分。</p> <p>注：需同时提供技术负责人在投标单位缴纳社保证明复印件以及相关有效资质证书复印件，不提供不得分。要求为2025年1月</p>

		至今任意 1 个月社保证明文件复印件及以上要求的对应证书复印件才能得分。
	项目团队成员 (8.0 分)	<p>对拟派出人员服务能力 (不少于 4 名, 不含项目负责人) 情况进行评价, 一人多证不可重复计分, 本项满分 8.0 分。</p> <p>具备商用密码应用安全性评估从业人员考核合格证书或网络安全等级保护测评师证书 (高级) 或信息安全工程师或信息系统项目管理师的, 每提供 1 种证书, 得 2 分, 每人最高得 2 分; 未提供的不得分。</p> <p>注: 投标文件提供项目组人员在本单位参保的证明材料, 要求为 2025 年 1 月至今任意 1 个月社保证明文件复印件及以上要求的对应证书复印件才能得分。</p>
	服务能力 (2.0 分)	<p>投标人承诺接到采购人通知后 1 小时内到达采购人指定地点提供服务的得 2 分; 投标人承诺接到采购人通知后 1 至 2 小时内到达采购人指定地点的得 1 分; 投标人承诺接到采购人通知后 2 小时以上到达采购人指定地点的得 0.5 分; 未提供承诺的不得分。(需提供单独承诺函加盖投标人公章)</p>
技术部分	等保测评技	方案应包含但不限于对项目的理解、服务内

<p>术方案(12.0分)</p>	<p>容、技术标准及规范、网络安全等级保护测评等内容。评标小组根据测评方案内容是否具体详细以及全面、合理性、与信息系统实际情况的贴合程度进行评分，满分 12 分。方案完全满足并优于采购需求，得 12 分；方案基本满足采购需求，得 9 分；方案不能完全满足采购需求，得 6 分；未提供不得分。</p>
<p>商用密码应用安全性评估服务方案(12.0分)</p>	<p>方案应包含但不限于对项目的理解、服务内容、技术标准及规范、商用密码应用方案评估及安全性评估等内容。评标小组根据测评方案内容是否具体详细以及全面、合理性、与信息系统实际情况的贴合程度进行评分，满分 12 分。方案完全满足并优于采购需求，得 12 分；方案基本满足采购需求，得 9 分；方案不能完全满足采购需求，得 6 分；未提供不得分。</p>
<p>重难点分析(10.0分)</p>	<p>投标人提供对项目服务保障措施及项目重点、难点分析、应对措施及建议。评标小组根据投标人对本项目服务保障能力、对项目的重点、难点分析是否准确合理，应对措施是否有效合理进行评分，满分 10 分。方案完全满足并优于采购需求，得 10 分；方案</p>

		基本满足采购需求，得 7 分；方案不能完全满足采购需求，得 5 分；未提供不得分。
	安全检测工具要求(10.0分)	<p>投标人需提供以下安全测评工具的软件著作证书。</p> <ol style="list-style-type: none"> 1.信息安全等保测评系统，得 2 分； 2.网络攻防演练与测试评估平台系统，得 2 分； 3.漏洞检测平台，得 2 分； 4.信息安全态势感知平台，得 2 分； 5.资产管理与威胁监测系统，得 2 分； <p>注：需提供软件著作权证书复印件并加盖公章，不提供不得分。</p>
	原创漏洞信息证明(10.0分)	<p>自 2020 年起获得国家信息安全漏洞共享平台（CNVD）或中国国家信息安全漏洞库（CNNVD）原创漏洞信息证明，每提供 1 份得 1 分，不提供不得分，最高得 10 分。</p> <p>注：需提供相关证明文件复印件，并加盖公章，不提供不得分。</p>
	售后服务方案（6.0分）	<p>根据投标人提供的售后服务方案,包括服务内容、服务体系应急预案、人员配备、响应时间、服务工作流程等进行综合评价满分 6 分。方案完全满足并优于采购需求，得 6</p>

		分；方案基本满足采购需求，得 4 分；方案不能完全满足采购需求，得 2 分；未提供不得分。
--	--	---