服务需求

一、 项目概况

近年来，网络和数据安全对国家安全和发展的重要性日益凸显，特别是在当前复杂多变的安全形势下，加强网络和数据安全保障工作已成为迫切需求。本项目依据《中华人民共和国密码法》《商用密码管理条例》《关键信息基础设施安全保护条例》等相关法律法规，结合市大数据中心网络和数据安全工作要求，旨在为上海市大数据中心信息化服务第五分中心（以下简称“第五分中心”）提供全面的网络和数据安全的技术支持和保障。

本项目需采购符合条件的商用密码应用安全性测评服务，出具符合规范的《商用密码应用安全性评估报告》，并协助落实密码应用安全整改工作，提升第五中心各信息化服务团队业务数据、信息系统安全管控能力，确保第五中心管辖内的各类信息化应用和数据安全、可靠、稳定运行。

服务期限：合同签订之日起至 2026 年 11 月 30 日

服务地点：上海市大数据中心

采购金额（最高限价）：1608694 元

组织形式：集中采购

采购方式：竞争性磋商

面向企业类型：面向所有类型

是否接受联合体响应：否

二、 测评服务范围

第五中心 2026 年密码应用安全性评估范围覆盖分中心下属八个信息化服务团队（市人民政府办公厅团队、市委编制办团队、市政府外办团队、市政府合作交流办、市司法局团队、市机管局团队、市监狱管理局团队和第五分中心团队）共计 49 个所属系统商用密码应用安全性评估工作，清单如下：

序号	团队名称	系统名称
1	市人民政府办公厅	上海市人民政府办公厅政务信息资源应用系统
2	市委编制办	上海市机构编制网
3		上海市事业单位登记管理综合业务系统
4		上海市事业单位机构编制综合管理系统
5	市政府外办	上海外事网上行政服务中心
6		因公出国（境）综合管理信息系统
7	市政府合作交流办	合作交流服务大系统
8	市机管局	智慧机管局政务服务系统
9		市机管局“一网统管”大系统
10		市级机关集中办公点安全保卫信息化系统
11	市司法局	上海市法律援助服务系统
12		上海市司法局全面依法治市大系统
13		上海市司法局人民陪审员综合信息管理系统
14		上海市司法局认罪认罚系统

15		上海市司法局人民监督员信息管理系统
16		上海市司法局 12348 公共法律服务系统
17		上海市司法局司法考试服务平台管理系统
18		上海市司法局在线公证系统
19		上海市司法局智慧调解系统
20		上海市司法局仲裁信息管理系统
21		上海市司法局涉法涉诉信访案件管理系统
22		上海市司法行政门户网站
23		上海市司法局行政许可审批管理系统
24		上海市司法局基层司法行政管理系统
25		上海律师综合管理信息系统
26		上海市法律服务行业信用信息系统
27		“一典通用”上海城市法典应用系统
28		上海市司法局一网统管基础系统
29		司法鉴定统一管理系统
30		社区矫正一体化大系统
31		智慧戒毒大数据系统
32		上海城市法规全书应用系统
33		上海市司法局电子卷宗应用系统
34		行政复议体制改革信息化配套工程系统
35		上海市司法局一体化办公系统

36		上海市司法鉴定执法执业系统
37		上海市司法局法治宣传云平台
38		上海市司法局“互联网+监管”配套管理系统
39		上海市司法局刑事执行系统
40		上海市司法局智慧公证系统
41		上海市司法局音视频信息综合指挥调度系统
42	市监狱管理局	上海市监狱管理局警务管理与评估系统
43		上海市监狱管理局指挥中心应用管理系统
44		上海监狱场所安全风险预警系统
45		上海监狱工作数据综合应用系统
46		上海监狱罪犯管理业务应用系统
47		上海市监狱管理局系统协同办公系统
48	第五分中心	上海市一体化办公平台
49		上海市视频会议基础能力平台

三、 测评工作内容

3.1 服务内容概述

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、《信息安全技术 信息系统密码应用测评要求》（GB/T 43206-2023）、《信息系统密码应用测评过程指南》（GM/T 0116-2021）、

《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》等技术要求，逐一对信息系统进行密码应用的合规性、正确性、有效性进行安全性评估，通过商用密码应用安全性评估深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全奠定基础。

测评的内容包括但不限于以下内容：

1、安全技术测评：包括物理和环境安全、 网络和通信安全、 设备和计算安全、 应用和数据安全等四个方面的安全测评。

（1）物理和环境安全

测评类别	测评单元
安全技术测评-物理和环境安全	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

（2）网络和通信安全

测评类别	测评单元
安全技术测评-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

（3）设备和计算安全

测评类别	测评单元
安全技术测评-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

（4）应用和数据安全

测评类别	测评单元
安全技术测评-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

2、安全管理测评：包括安全管理（分为制度、人员、建设和应

急四个子模块）的安全测评。

（1）管理制度

测评类别	测评单元
安全管理测评-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

（2）人员管理

测评类别	测评单元
安全管理测评-人员管理度	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

（3）建设运行

测评类别	测评单元
安全管理测评-建设	制定密码应用方案

运行	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

（4）应急处置

测评类别	测评单元
安全管理测评-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

3.2 服务要求

（1）服务提供方应详细描述本次项目的整体实施方案，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、阶段性文档提交和验收标准等。

（2）服务提供方应详细描述实施人员的组成、资质及各自职责的划分。服务提供方应配置有经验的技术人员进行本次项目实施。

（3）本次项目实施过程中所使用到的各种工具软件由服务提供方推荐，经采购人确认后由服务提供方提供并在项目中使用。在响应文件中应详细描述所使用的安全技术工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。

（4）本次项目实施过程中所使用到的测评工具，应包括自主密码专用检测工具、漏洞扫描工具等获得许可的检测工具，对系统数据进行分析，并以分析结果辅证评估报告。

（5）安全技术工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由服务提供方推荐，经采购人确认后由服务提供方提供并在项目中使用。

（6）项目实施需要的运行环境（如场地、网络环境等）由采购人提供，服务提供方应详细描述需要的运行环境的具体要求。

3.3 服务计划

根据测评对象性质制定项目实施计划，6 月底应完成总体服务内容的 60%，9 月底应完成总体服务内容的 90%，10 月底应完成总体服务内容的 100%。

四、 测评工作目标

1、深刻理解本项目实施的背景，同时密切结合该项目的实际情况，提供针对性的项目实施方案，以便充分保障本项目按期完成；

2、项目的实施方案需包括项目背景之细述、结合该项目实际情况的具体测评实施方案和具体测评进度安排、各分项质量目标及保证措施以及本标书要求的其他应写入项目实施方案的内容；

3、项目测评工作中，出具每个系统的《问题汇总及整改意见表》等过程文件，以便配合业主督促项目实施运维商进行问题整改，在运维商完成整改后，再进行复核测评；

4、测评工作全部完成后，所有测评都将提供最终测评报告。

五、 服务需求

按照第五中心 2026 年商用密码应用安全性评估工作要求，按照实施范围完成信息系统密码应用安全性评估服务，出具符合规范的《商用密码应用安全性评估报告》，提供密码应用技术支撑并协助第

五中心各信息化服务团队开展密码应用安全整改工作。

服务方式：远程与现场相结合的方式。

服务交付物：《密码应用安全性评估差距分析及密码应用建议》、《商用密码应用安全性评估报告》、《密码应用安全性评估服务年度总结报告》。

六、 服务质量考核要求

服务质量的考核结果将作为确认甲方需支付的最终合同总价的依据之一。就甲方需支付的最终合同总价，服务质量考核结果为优秀和良好的按成交金额的 100%支付，服务质量考核结果为一般的按合同条款执行。

1、根据项目要求在项目验收前完成相关商用密码应用安全性评估服务工作。

2、服务提供方应根据第一分中心商用密码应用安全性评估项目需求，制定详细商用密码应用安全性评估工作计划和方案。

3、商用密码应用安全性评估项目服务响应率=100%。

4、文档完整度和准确率大于 95%。

七、 验收要求

测评服务工作期限终止时，服务提供方应当以书面形式向采购方提交服务总结报告及其他测评服务相关资料。采购方在收到服务

提供方提交的相关资料后10个工作日内，对服务提供方的工作进行验收。如属于服务提供方原因致使安全服务未能通过验收的，服务提供方应当在15个工作日内进行整改，并自行承担相关商用密码应用安全性评估相关费用，再次接受采购方的验收，直至符合约定要求。

八、 应急服务

1、服务提供方坚持主动预防、迅速高效的原则，紧密结合实际情况，精心编制并持续完善应急预案。

2、服务提供方必须提供7*24小时全天候应急响应服务。

3、中心安全事件应急响应等级分为Ⅳ级、Ⅲ级、Ⅱ级、Ⅰ级，分别对应一般、较大、重大和特别重大安全事件。中心安全事件分级原则详见附件一。

当：

a、发生Ⅰ级（特别重大）故障后0.5小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应2小时内到达用户现场；

b、发生Ⅱ级（重大）故障后0.5小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应3小时内到达用户现场；

c、发生Ⅲ级（较大）故障后1小时内无法通过电话或远程支持

服务排除故障，如采购人要求提供现场支持，服务提供方应 3 小时内到达用户现场；

d、发生Ⅳ级（一般）故障后 1 小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应 4 小时内到达用户现场。

4、如发生故障，服务提供方应严格按照制定的应急预案中故障处理流程实施故障排除操作。

5、当故障排除操作全部完成后，服务提供方应向采购人提交运维故障报告，经采购单位验证通过后签字确认并归档保存，同时组织更新相关文档。

6、如遇有重大事件（包括汛期、节假日、政治军事活动等），服务提供方应科学编制安全保障方案，并根据采购人需要提供现场保障服务。

九、 服务组织和人员要求

选派在项目服务方面富有经验的团队人员负责项目的密码测评，项目团队应配置对应的人员，团队应至少配备项目负责人 1 人，项目经理 1 人，测评人员 5 人，保密和档案管理员 1 人，具体人员要求如下表所示：

角色	主要职责	人数	人员要求	驻场要求
项目负责人	项目计划的部署，组织会议制定整个项目计划。项目过程中的协调组织，项目过程中的风险控制。对测评过程中遇到的各类技术问题进行决策。	1人	密码学或计算机相关专业硕士以上学历，信息安全相关专业的高级职称，具备5年及以上密码应用测评工作经验。	不驻场
项目经理	负责项目实施过程中测评技术管理工作。参与项目计划的实施，测评过程中的协调组织，保障整个测评任务的完成。	1人	具备4年及以上密码应用测评工作经验。	不驻场
测评人员	负责项目实施过程中技术应用的测评工作	4人	具备3年及以上密码应用测评工作经验。	不驻场
保密和档案管理员	负责对各类档案的接收，分类，编目，编制等系统管理。做好文件，资料，档案的	1人	具备3年及以上密码应用测评工作经验。	不驻场

	保密保管工作。			

人员要求具体如下：

➢ 密码测评人员要求：需要 3 年及以上信息系统商用密码应用安全性评估工作经验；了解各类密码测评操作平台和软件工具，有独立判断网络和系统问题的能力。

➢ 有应急事项发生时，人员 2 小时内到达现场。

十、 供应商综合能力要求

供应商具有 ISO 9001 质量管理体系认证证书、ISO 27001 信息安全管理体系认证的优先考虑。

十一、 密码测评工具和模拟测评环境要求

11.1 测评工具要求

本次项目实施过程中所使用到的测评工具，应包括具有自主知识产权或计算机软件著作权的密码检测工具（详细描述所使用工具的型号、功能、使用的方式和对环境和平台的要求以及使用可能对系统造成的风险等），对系统数据进行分析，并以分析结果辅证评估报告。

检测工具包括但不限于以下几类：

1、密码算法验证工具，包括国密算法 SM2、SM3、SM4，常见的国际通用算法 AES、DES、RSA 等的验证；

2、随机数随机性检测工具；

3、数字证书检测工具，包括数字证书的格式的合规性验证、数字证书的证书链的检验等；

4、网络协议分析工具；包括但不限于 SSL 协议、IPSec 协议；包括主动协议分析工具和被动分析工具。

11.2 模拟测评环境要求

服务提供方具有密码测评模拟验证环境的能力及相关设备，包括但不限于以下的密码设备：

1、SSL VPN：支持国密算法；具有商用密码产品认证证书，用于搭建 SSL VPN 网络，模拟 SSL VPN 通信信道的测评。

2、IPSec VPN：支持国密算法；具有商用密码产品认证证书，用于搭建 IPSec VPN 网络，模拟 IPSec VPN 通信信道的测评。

3、服务器密码机：支持国密算法；具有商用密码产品认证证书，用于实现重要数据的加解密和完整性保护，模拟重要数据加解密和完整性保护的测评。

十二、 项目的变更、解除和终止

如果服务提供方丧失履约能力、发生资不抵债或进入破产程序，采购单位可在任何时候以书面形式通知服务提供方终止本项目的执行而不给予服务提供方补偿。该终止本项目将不损害或影响采购单位已经采取或将要采取任何行动或补救措施的权利。

如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照公平、合理的原则共同协商修改本项目对应的合同的相关条款。

十三、 保密责任

项目过程中不出现任何泄密事件和安全事故，在合同期内或合同终止后，未征得有建设单位同意，不得泄露与本项目及本合同业务有关的保密资料。

（1）测评单位因为本项目提供测评服务而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、电子文件、访谈记录、现场实测数据、建设单位相关工作程序等）以及因为本项目提供测评服务而形成的数据、信息和任何形式的工作成果，属于建设单位所有，均是建设单位要求保密的信息。除法律法规另有规定外，未经建设单位书面同意，测评单位不得对外泄露建设单位要求保密的信息，不得用于其他用途，否则测评单位需承担由此引起的法律责任和经济损失，包括但不限于直接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

（2） 测评单位应采取必要的有效措施保证其参与本项目的人员（包括测评单位聘用的人员、借调的人员、在测评单位实习的人员）无论是在职或离职后，以及测评单位的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若测评单位参与

本项目的人员或测评单位合作方违反本条规定，测评单位应承担连带责任。

（3）保密期限自测评单位知悉保密信息起始至保密信息被合法公开之日止。

（4）除法律法规另有规定外，测评单位（含测评单位参与本项目的人员）未经建设单位书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本合同有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。

（5） 在本项目合同无效、终止或解除之后，合同各方在本合同中的保密义务并不随之终止，各方仍需依据本合同的保密规定履行保密义务。