省粮食和应急物资综合管理信息平台及企业库点信息系统升级改造和运营（2025 年）项目商用密码应用安全性评估服务采购需求书

一、项目概况

1.1 项目名称

省粮食和应急物资综合管理信息平台及企业库点信息系统升级改造和运营（2025 年）项目商用密码应用安全性评估服务。

1.2 采购人

广东省粮食和物资储备局

1.3 项目总体目标

通过省粮食和应急物资综合管理信息平台及企业库点信息系统升级改造和运营（2025年）项目中的广东省粮食和应急物资综合管理信息平台开展商用密码应用安全性评估，优化信息安全的配置，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，保障信息系统安全运行。

1.4 服务地点

采购人指定地点。

二、项目预算

预算金额 8.00 万元。

三、服务期限

自合同签订之日起直至完成广东省粮食和应急物资综合管理信息平台商用密码应用安全性评估服务结束并出具测评报告为止。

四、服务内容

4.1 项目服务对象

序号	系统名称	等保级别	备注
1	广东省粮食和应急物资综合管理信息平台	三级	/

4.2 项目服务内容

4.2.1 商用密码应用安全性评估

4.2.2.1 测评目标

根据《中华人民共和国网络安全法》《商用密码管理条例》《商用密码应用安全性评估管理办法（试行）》以及国家关于网络安全等级保护和重要领域密码应用的有关要求，开展商用密码应用安全性评估，从总体要求、物理和环境、网络和通信、设备和计算、应用和数据、密钥管理、安全管理等方面开展评估。

测评机构最终输出信息系统的商用密码应用安全测评方案、信息系统的商用密码应用安全性评估报告及总体项目工作总结等，协助被测评单位将评估结果报广东省密码管理部门备案。

4.2.2.2 测评依据

1. 《广东省省级政务信息化项目商用密码应用工作指引》
2. 《商用密码应用安全性评估管理办法》
3. 《信息安全技术信息系统密码应用基本要求》
4. 《信息系统密码测评要求》（试行）

5. 《商用密码应用安全性评估测评过程指南》（试行）

6. 《商用密码应用安全性评估测评作业指导书》（试行）

7. GB/T 15843.3-2016《信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制》

8. GM/T 0001.1-2012 祖冲之序列密码算法 第 1 部分：算法描述

9. GM/T 0001.2-2012 祖冲之序列密码算法 第 2 部分：基于祖冲之算法的机密性算法

10. GM/T 0001.3-2012 祖冲之序列密码算法 第 3 部分：基于祖冲之算法的完整性算法

11. GM/T 0002-2012 SM4 分组密码算法

12. GM/T 0003.1-2012 SM2 椭圆曲线公钥密码算法 第 1 部分：总则

13. GM/T 0003.1-2012 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法

14. GM/T 0003.3-2012 SM2 椭圆曲线公钥密码算法 第 3 部分：密钥交换协议

15. GM/T 0003.4-2012 SM2 椭圆曲线公钥密码算法 第 4 部分：公钥加密算法

16. GM/T 0003.5-2012 SM2 椭圆曲线公钥密码算法 第 5 部分：参数定义

17. GM/T 0004-2012 SM3 密码杂凑算法

18. GM/T 0005-2012 随机性检测规范

19. GM/T 0006-2012 密码应用标识规范

20. GM/T 0008-2012 安全芯片密码检测准则

21. GM/T 0009-2012 SM2 密码算法使用规范

22. GM/T 0010-2012 SM2 密码算法加密签名消息语法规范

23. GM/T 0011-2012　　可信计算 可信密码支撑平台功能与接口规范

24. GM/T 0012-2012　　可信计算 可信密码模块接口规范

25. GM/T 0013-2012　　可信计算 可信密码模块接口符合性测试规范

26. GM/T 0014-2012　　数字证书认证系统密码协议规范

27. GM/T 0015-2012　　基于 SM2 密码算法的数字证书格式规范

28. GM/T 0016-2012　　智能密码钥匙密码应用接口规范

29. GM/T 0017-2012　　智能密码钥匙密码应用接口数据格式规范

30. GM/T 0018-2012　　密码设备应用接口规范

31. GM/T 0019-2012　　通用密码服务接口规范

32. GM/T 0020-2012　　证书应用综合服务接口规范

33. GM/T 0021-2012　　动态口令密码应用技术规范

34. GM/T 0022-2014　　IPSec VPN 技术规范

35. GM/T 0023-2014　　IPSec VPN 网关产品规范

36. GM/T 0024-2014　　SSL VPN 技术规范

37. GM/T 0025-2014　　SSL VPN 网关产品规范

38. GM/T 0026-2014　　安全认证网关产品规范

39. GM/T 0027-2014　　智能密码钥匙技术规范

40. GM/T 0028-2014　　密码模块安全技术要求

41. GM/T 0029-2014　　签名验签服务器技术规范

42. GM/T 0030-2014　　服务器密码机技术规范

43. GM/T 0031-2014　　安全电子签章密码技术规范

44. GM/T 0032-2014　　基于角色的授权管理与访问控制技术规范

45. GM/T 0033-2014　　时间戳接口规范

46. GM/T 0034-2014　　基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范

47. GM/T 0035.1-2014　　射频识别系统密码应用技术要求 第 1 部分：密码安全保护框架及安全级别

48. GM/T 0035.2-2014　　射频识别系统密码应用技术要求 第 2 部分：电子标签芯片密码应用技术要求

49. GM/T 0035.3-2014　　射频识别系统密码应用技术要求 第 3 部分：读写器密码应用技术要求

50. GM/T 0035.4-2014　　射频识别系统密码应用技术要求 第 4 部分：电子标签与读写器通信密码应用技术要求

51. GM/T 0035.5-2014　　射频识别系统密码应用技术要求 第 5 部分：密钥管理技术要求

52. GBT39786-2014　　采用非接触卡的门禁系统密码应用技术指南

53. GM/T 0037-2014　　证书认证系统检测规范

54. GM/T 0038-2014　　证书认证密钥管理系统检测规范

55. GM/T 0039-2015　　密码模块安全检测要求

56. GM/T 0040-2015　　射频识别标签模块密码检测准则

57. GM/T 0041-2015　　智能 IC 卡密码检测规范

58. GM/T 0042-2015　　三元对等密码安全协议测试规范

59. GM/T 0043-2015　　数字证书互操作检测规范

60. GM/T 0044-2016　　SM9 标识密码算法

61. GM/T 0045-2016　　金融数据密码机技术规范

4.2.2.3 测评内容

（1） 总体测评

测评对象：系统使用的密码算法、密码技术、密码产品及密码服务。测评内容如表 2 所示。

表 2 总体测评内容

测评单元	测评指标	测评方法	测评方式	预期结果
密码算法合规性检查	a）信息系统中使用的密码算法应当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。	1)访谈密码管理员，查看技术文档，并实际查看密码系统，了解系统使用的算法名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件）。	访谈、文档审查和实地查看或配置检查	1）明确了系统使用的算法名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件）。 2）系统使用的密码算法以国家标准或行业标准形式发布，或具有国家密码管理部门同意其使用的证明文件。
		2）核查密码算法是否以国家标准或行业标准形式发布，或取得国家密码管理部门同意其使用的证明文件。	文档审查和实地查看或配置检查	
密码技术合规性检查	b）信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。	核查系统所使用的密码技术是否以国家标准或行业标准形式发布。	访谈、文档审查和实地查看或配置检查	1）系统所使用的密码技术以国家标准或行业标准形式发布。
密码产品合	c）信息系统中使用的密码产品与密码模块应通过国家密码管理部	核查系统所采用的相关密码产品和密码模块是否获得国家密码管理部门颁发的密码产品型号证书，或国家密码管理部门认可的	访谈、文档审查和实地查看或配置检	1）系统所采用的密码产品和密码模块获得了国家密码管理部门颁发的密码产品型号证书（或具有国家密码管理部门认可的商用

测评单元	测评指标	测评方法	测评方式	预期结果
规性检查	门核准。	商用密码测评机构出具的合格检测报告。	查	密码测评机构出具的合格检测报告）。
密码服务合规性检查	d）信息系统中使用的密码服务应通过国家密码管理部门许可。	核查系统所采用的相关密码服务是否获得国家密码管理部门颁发的密码服务许可证。	访谈、文档审查和实地查看或配置检查	1）系统所采用的相关密码服务获得了国家密码管理部门颁发的密码服务许可证。

（2） 单元测评

本任务主要是将单项测评结果进行汇总，分别统计不同测评对象的单项测评结果，从而判定单元测评结果，并以表格的形式逐一列出。输入：测评报告的单元测评的结果记录部分，测评作业指导书（参考《商用密码应用安全性评估测评作业指导书（试行）》）任务描述：

按层面分别汇总不同测评对象对应测评指标的单项测评结果情况，包括测评多少项，符合要求的多少项等内容，一般以表格形式列出。测评对象在某个测评指标的单元测评结果判别原则如下：

测评指标包含的所有测评项的单项测评结果均为符合，则该测评对象对应该测评指标的单元测评结果为符合。

测评指标包含的所有测评项的单项测评结果均为不符合，则该测评对象对应该测评指标的单元测评结果为不符合。

测评指标包含的所有测评项均为不适用项，则该测评对象对应该测评指标的单元测评结果为不适用。

测评指标包含的所有测评项的单项测评结果不全为符合或不符合，则该测评对象对应该测评指标的单元测评结果为部分符合或不符合。输出/产品： 测评报告的单元测评的结果汇总部分。

测评单元			测评指标
总体要求	密码算法		5.1 信息系统中使用的密码算法应当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。
	密码技术		5.2 信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。
	密码产品		5.3 信息系统中使用的密码产品与密码模块应通过国家密码管理部门核准。
	密码服务		5.4 信息系统中使用的密码服务应通过国家密码管理部门许可。
密码技术应用要求	物理和环境安全	身份鉴别	7.1.4 a）应使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性。
		电子门禁记录数据完整性	7.1.4 b）应使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性。
		视频记录数据完整性	7.1.4 c）应使用密码技术的完整性功能来保证视频监控音像记录的完整性。
	网络和通信安全	身份鉴别	7.2.4 a）应在通信前基于密码技术对通信双方进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性。
		访问控制信息完整性	7.2.4 b)应使用密码技术的完整性功能来保证网络边界和系统资源访问控制信息的完整性。
		通信数据完整性	7.2.4 c)应采用密码技术保证通信过程中数据的完整性。
		通信数据机密性	7.2.4 d)应采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性。
		集中管理通道安全	7.2.4 e)应采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。
	设备和计	身份鉴别	7.3.4 a)应使用密码技术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。

测评单元			测评指标
	算安全	远程管理身份鉴别信息机密性	7.3.4 b)在远程管理时，应使用密码技术的机密性服务来实现鉴别信息的防窃听。
		访问控制信息完整性	7.3.4 c)应使用密码技术的完整性功能来保证系统资源访问控制信息的完整性。
		敏感标记的完整性	7.3.4 d)应使用密码技术的完整性功能来保证重要信息资源敏感标记的完整性。
		重要程序或文件完整性	7.3.4 e)应采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护。
		日志记录完整性	7.3.4 f)应使用密码技术的完整性功能来对日志记录进行完整性保护。
	应用和数据安全	身份鉴别	7.4.4 a)应使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性。
		访问控制信息和敏感标记完整性	7.4.4 b)应使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性。
		数据传输机密性	7.4.4 c)应采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等。
		数据存储机密性	7.4.4 d)应采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息、重要可执行程序等。
		数据传输完整性	7.4.4 e)应采用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用户信息等。
		数据存储完整性	7.4.4 f)应采用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

测评单元			测评指标
			数据、重要视频数据和重要用户信息、重要可执行程序等。
		日志记录完整性	7.4.4 g)应使用密码技术的完整性功能来实现对日志记录完整性的保护。
		重要应用程序的加载和卸载	7.4.4 h)应采用密码技术对重要应用程序的加载和卸载进行安全控制。
密钥管理	生成		8.4 a)密钥生成使用的随机数应符合 GM/T 0005 要求，密钥应在符合 GM/T 0028 的密码模块中产生；密钥应在密码模块内部产生，不得以明文方式出现在密码模块之外；应具备检查和剔除弱密钥的能力。
	存储		8.4 b) 密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在符合 GM/T 0028 的二级及以上密码模块中。
	分发		8.4 c)密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。
	导入与导出		8.4 d)应采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。
	使用		8.4 e) 密钥应明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；密钥泄露时，应停止使用，并启动相应的应急处理和响应措施。应按照密钥更换周期要求更换密钥；应采取有效的安全措施，保证密钥更换时的安全性。
	备份与恢复		8.4 f)应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。
	归档		8.4 g)应采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。

测评单元			测评指标
	销毁		8.4 h)应具有在紧急情况下销毁密钥的措施。
安全管理	制度	制定密码安全管理制度	9.1.3 a)应制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度应包括密码建设、运维、人员、设备、密钥等密码管理相关内容。
		定期修订安全管理制度	9.1.3 b)应定期对密码管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
		明确管理制度发布流程	9.1.3 c)应明确相关管理制度发布流程。
	人员	了解并遵守密码相关法律法规	9.2.3 a)应了解并遵守商用密码相关法律法规。
		正确使用密码相关产品	9.2.3 b)应能够正确使用商用密码产品。
		建立岗位责任制度	9.2.3 c) 应根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责应建立多人共管制度，互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用。
		建立人员考核制度	9.2.3 d) 应建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度。
		建立人员培训制度	9.2.3 e)应建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训。
		建立关键岗位人员保密制度和调离制	9.2.3 f)应建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。

测评单元			测评指标
		度	
	实施	规划	9.3.1.3 信息系统规划阶段，责任单位应依据密码相关标准，制定密码应用方案，组织专家进行评审，评审意见作为项目规划立项的重要材料。通过专家审定后的方案应作为建设、验收和测评的重要依据。
		建设-制定实施方案	9.3.2.3 a) 应按照国家相关标准，制定实施方案，方案内容应包括但不少于信息系统概述、安全需求分析、密码系统设计方案、密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、密码系统安全管理与维护策略、密码系统实施计划等。
		建设-选用合规密码产品和密码服务	9.3.2.3 b)应选用经国家密码管理部门核准的密码产品、许可的密码服务。
		运行-评估后方能运行	9.3.3.3 a)信息系统投入运行前，应经商用密码应用安全性测评机构进行安全性评估，评估通过方可投入正式运行。
		运行-每年评估和整改	9.3.3.3 b)信息系统投入运行后，责任单位每年应委托商用密码应用安全性测评机构开展密码应用安全性评估，并根据评估意见进行整改；有重大安全隐患的，应停止系统运行，制定整改方案，整改完成并通过评估后方可投入运行。
	应急	应急预案	9.4.3 a)制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置。
		事件处置	9.4.3 b)事件发生后，应及时向信息系统的上级主管部门进行报告。
		向有关主管部门上报处置情况	9.4.3 c)事件处置完成后，应及时向同级的密码主管部门报告事件发生情况及处置情况。

4.3 项目交付成果

4.3.2 商用密码应用安全性评估

序号	系统名称	等保级别	交付内容
1	广东省粮食和应急物资综合管理信息平台	三级	《广东省粮食和应急物资综合管理信息平台系统》商用密码应用安全性评估报告

五、服务要求

5.1 技术要求

5.1.1 总体技术要求

为保障广东省粮食和应急物资综合管理信息平台的运行安全，密码应用符合国家的相关标准，系统建设完成后需要按照相关的要求进行商用密码的测评，保证各项改造符合商用密码的应用安全要求。

5.2 管理要求

5.2.1 服务人员

投标人须书面承诺，如在项目实际执行过程中发生项目经理不能按采购文件要求胜任相关工作的，采购人有权要求更换项目经理，投标人必须在两周内调整为符合采购文件要求且能胜任相关工作的项目经理并到位开展工作，否则采购人有权终止合同并报相关管理部门进行处理。

投标人承诺的项目经理和项目实施的主要人员未经用户同意不得调整；投标人如中途更换项目经理和主要技术人员，须书面向采购人提出申请，说明申请理由，经采购人书面同意方可调整团队人员，调入人员的资历和从业经验不低于调出人员，否则视为违约行为，采购人有权终止服务合同。

投标人应指派固定的团队为本项目提供专业服务，服务团队成员不得少于 3 人，其中：项目团队成员应具有国家密码管理局颁发的商用密码应用安全性评估

从业人员证书；。

5.2.2 进度要求

自签订合同起一年内完成所有服务内容。

5.2.3 组织实施要求

为使项目按质、按量、按时及有序实施，投标人应建立完善、稳定的项目团队、内部组织管理方式及管理机构、协调机制、技术基础，支撑保障要求及其他相关要求。在机制保障方面，成立组织实施小组和项目专家组的双轨制的组织模式。在项目日常管理和条件保障方面，从行政组织、后勤保障和支撑条件各方面创造良好的服务环境，确保项目的顺利实施。

5.2.4 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，并按国家、省以及采购人档案管理要求，向采购人提供相应的资料及服务报告。

5.2.5 质量保证要求

为保证本项目能按时高质的顺利完成，规避项目风险或将风险降至最低程度，投标人应建立项目质量管理体系，包括但不限于质量目标、质量指标、岗位责任、问题处理计划、质量评价、整改完善等内容，并建立奖惩制度。

5.2.6 保密要求

1．投标人应对因项目开展而知悉的保密信息应严格保守，保证不被披露或使用，包括故意或过失。

2．投标人不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用保密信息；除法律法规另有规定外，不得直接或间接地向无关人员泄露采购人的保密信息；不得向不承担保密义务的任何第三人披露采购人的保密信息。投标人在开展项目工作时，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投标人内部与该项目无关的任何人员。

3．投标人对于工作期间知悉采购人的保密信息（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。

4．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。

5.2.7 验收要求

1. 验收严格按国家和省现行的相关质量评定标准和服务验收规范、规程进行服务和验收，由采购人根据国家有关标准、合同及有关附件要求组织开展。

2. 验收标准：

（1）完成合同和根据采购文件所编写的响应文件中列举的全部工作内容。

（2）服务期间，投标人已按照合同、采购文件的要求和响应文件的服务承诺提供稳定、可靠、优质的服务，按要求提交如下文件并通过采购人和监理确认：

《广东省粮食和应急物资综合管理信息平台系统商用密码应用安全性评估报告》

（3）投标人按照国家和省有关档案管理规定完成商用密码应用安全性评估服务成果归档工作。

六、付款方式

分首期、尾款 2 个支付周期支付，实际支付以当年实际财政资金安排为准，具体支付方式如下：

(1) 首期支付

签订合同后 30 个工作日内，乙方书面提出支付申请函及与拟支付金额等额的符合甲方财务管理要求的相应发票，甲方确认后启动首期款支付流程，支付人民币_____元整（¥___元）（约占合同总金额的 60%）。

(2) 尾款支付

本项目经甲方最终验收通过后 30 个工作日内，乙方书面提出支付申请函及与拟支付金额等额的符合甲方财务管理要求的相应发票，甲方确认后启动尾款支付流程，支付人民币____元整（¥____元）（约占合同总金额的 40%）。