# **附件6**

# **广东省应急指挥中心项目信息化工程商用密码应用安全性评估服务采购项目需求书**

# **第一部分 采购概述**

1、项目名称：广东省应急指挥中心项目信息化工程商用密码应用安全性评估服务采购项目

2、数量：1项。

3、服务需求：对广东省应急指挥中心项目信息化工程商用密码应用建设方案进行评估，出具《商用密码应用方案评估报告》，对项目进行商用密码应用安全性评估，并出具《商用密码应用安全性评估报告》保障项目密码应用安全；同时为建设单位相关商用密码软硬件设备设施的提供建设部署意见及指导，提升系统商用密码安全性能。报告具有客观性、准确性、整体性、系统性、可靠性。

4、合同履行期限：服务期为自合同签订之日起30日。

5、商用密码应用方案评估服务预算：298000.00元。

# **第二部分 服务需求**

**一、项目背景**

当前，网络安全已经成为国家安全的重要组成部分，没有网络安全就没有国家安全。近年来，网络空间安全事件频发。面对国内外越来越严峻的网络安全的形势，网络安全提升到国家战略高度，而密码技术又是与核技术、航天技术并称为国家三大“杀手锏”，因此国产密码应用推进提到新的日程。《密码法》《网络安全法》等法律法规明确要求，重要领域网络和信息系统，应当采用国产密码进行保护，做到同步规划、同步建设、同步运行、定期评估。

对重要领域重要信息系统开展密码应用安全性评估，是《中华人民共和国密码法》和中央有关文件的明确要求，是落实总体国家安全观和网络强国战略的具体行动，是深入推进重要领域密码应用的必然要求。开展商用密码应用安全性评估工作，不仅对规范密码应用具有重大意义，同时对维护网络和信息系统密码安全，切实保障网络安全，有效应对各类网络安全风险，也具有不可替代的重要作用。

**二、项目目标**

商用密码应用方案评估由国家密码管理局认定的密码应用安全性评估机构承担。按照GB/T 39786-2021《信息系统密码应用基本要求》及国家有关商用密码应用有关法律法规、政策标准的要求，对被测系统的商用密码应用方案进行评估，由评估机构给出整改建议，被测系统责任单位依照整改建议进行方案整改，并向评估机构反馈整改结果，直至整改通过，并出具《商用密码应用方案评估报告》。

三、**项目对象**

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **网络安全保护等级** |
| 1 | 应急指挥一张图 | 等保2.0三级 |
| 2 | 值守信息管理系统 | 等保2.0三级 |
| 3 | 应急指挥服务门户 | 等保2.0三级 |
| 4 | 统一集成服务门户 | 等保2.0三级 |
| 5 | 应急指挥数据专区子门户 | 等保2.0三级 |
| 6 | 应急指挥统一用户中心 | 等保2.0三级 |
| 7 | 数字政府”辅助决策系统（“粤治慧”平台-可视化服务系统） | 等保2.0三级 |
|  |  |  |

**四、**项目预算

商用密码应用方案评估服务预算为298000.00元。

**五、服务内容**

**（一）开展商用密码应用方案评估内容**

密码应用方案评估主要是依据系统定级情况，审查被测系统责任单位的密码应用方案是否涵盖了所有需采用密码保护的核心资产或敏感信息，已设计的密码保护措施是否均能达到相应等级的密码使用要求或规定。评估由国家密码管理局认定的密码应用安全性测评机构进行评估。

**（二）评估指标**

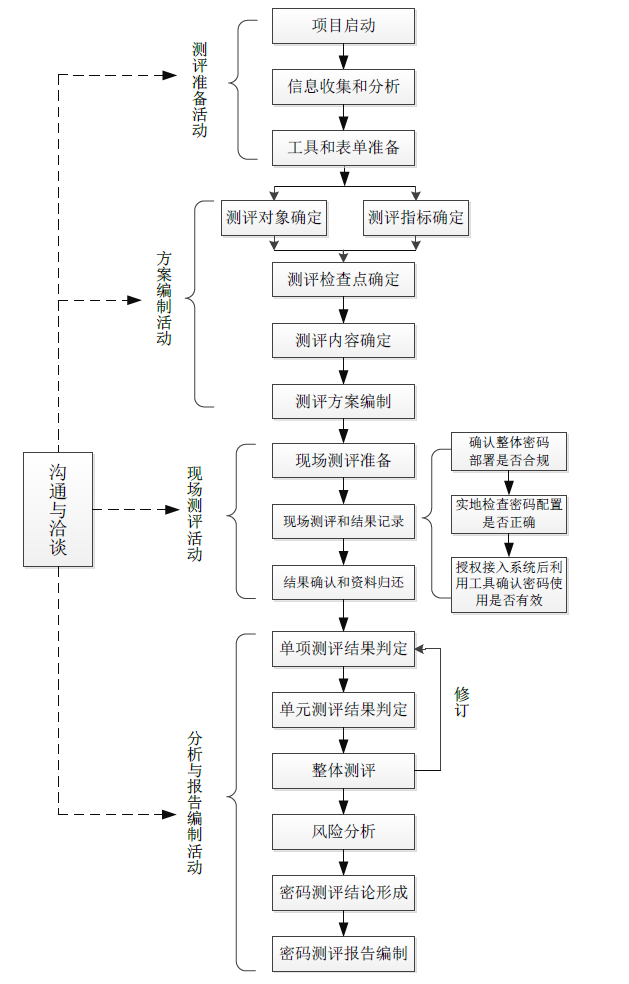
测评机构对被测系统的密码应用方案进行评估，对密码技术方案的正确性、密码技术对信息系统安全保护的有效性、密码产品选取的合规性等方面进行评估。对于没有通过评估的密码应用方案，由测评机构给出整改建议，被测系统责任单位依据方案不符合程度决定对设计方案进行修改完善或重新设计，并向测评机构反馈整改结果，直至整改通过，测评机构出具评估报告。

**评估依据**

|  |  |  |
| --- | --- | --- |
| 测评层面 | 测评单元 | 指标要求 |
| 物理和环境安全 | 身份鉴别 | 8.1a）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。 |
| 电子门禁记录数据存储完整性 | 8.1b）宜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。 |
| 视频监控记录数据存储完整性 | 8.1c）宜采用密码技术保证视频监控音像记录数据的存储完整性。 |
| 网络和通信安全 | 身份鉴别 | 8.2a)应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。 |
| 通信数据完整性 | 8.2b)宜采用密码技术保证通信过程中数据的完整性。 |
| 通信过程中重要数据的机密性 | 8.2c)应采用密码技术保证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 | 8.2d)宜采用密码技术保证网络边界访问控制信息的完整性。 |
| 安全接入认证 | 8.2e)可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。 |
| 设备和计算安全 | 身份鉴别 | 8.3a)应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。 |
| 远程管理通道安全 | 8.3b)远程管理设备时，应采用密码技术建立安全的信息传输通道。 |
| 系统资源访问控制信息完整性 | 8.3c)宜采用密码技术保证系统资源访问控制信息的完整性。 |
| 重要信息资源安全标记完整性 | 8.3d)宜采用密码技术保证设备中的重要信息资源安全标记的完整性。 |
| 日志记录完整性 | 8.3e)宜采用密码技术保证日志记录的完整性。 |
| 重要可执行程序完整性、重要可执行程序来源真实性 | 8.3f)宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。 |
| 应用和数据安全 | 身份鉴别 | 8.4a)应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。 |
| 访问控制信息完整性 | 8.4b)宜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。 |
| 重要信息资源安全标记完整性 | 8.4c)宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性； |
| 重要数据传输机密性 | 8.4d)应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。 |
| 重要数据存储机密性 | 8.4e)应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。 |
| 重要数据传输完整性 | 8.4f)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。 |
| 重要数据存储完整性 | 8.4 g) 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； |
| 不可否认性 | 8.4 h)在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。 |
| 管理制度 | 具备密码应用安全管理制度 | 8.5 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； |
| 密钥管理规则 | 8.5 b）应根据密码应用方案建立相应密钥管理规则； |
| 建立操作规程 | 8.5 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； |
| 定期修订安全管理制度 | 8.5 d）应定期对密码应用安全管理制度和操作规程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之处进行修订； |
| 明确管理制度发布流程 | 8.5 e）应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制； |
| 制度执行过程记录留存 | 8.5 f）应具有密码应用操作规程的相关执行记录并妥善保存。 |
| 人员管理 | 了解并遵守密码相关法律法规和密码管理制度 | 8.6 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； |
| 建立密码应用岗位责任制度 | 8.6 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：  1) 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；  2) 对关键岗位建立多人共管机制；  3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；  4) 相关设备与系统的管理和使用账号不得多人共用。 |
| 建立上岗人员培训制度 | 8.6 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； |
| 定期进行安全岗位人员考核 | 8.6 d) 应定期对密码应用安全岗位人员进行考核； |
| 建立关键岗位人员保密制度和调离制度 | 8.6 e) 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。 |
| 建设运行 | 制定密码应用方案 | 8.7 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； |
| 制定密钥安全管理策略 | 8.7 b）应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节密钥管理要求参照附录B； |
| 制定实施方案 | 8.7 c）应按照应用方案实施建设； |
| 投入运行前进行密码应用安全性评估 | 8.7 d）投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行； |
| 定期开展密码应用安全性评估及攻防对抗演习 | 8.7 e）在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。 |
| 应急处置 | 应急策略 | 8.8 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； |
| 事件处置 | 8.8 b）事件发生后，应及时向信息系统主管部门进行报告； |
| 向有关主管部门上报处置情况 | 8.8 c）事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。 |

**六、评估流程**

商用密码应用安全性评估过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。双方之间的沟通与洽谈贯穿整个密码应用安全性评估过程。测评工作流程如下图所示。



**七、项目成果**

1.《商用密码应用方案评估报告》（每个系统各10份）并按要求汇编成册，并协助委托方将评估结果报密码管理主管部门备案。

**八、组织管理要求**

（一）服务人员

项目组人员需通过国家密码管理局商用密码检测中心或国家商用密码应用安全性评估人员测评能力考核小组组织的商用密码应用安全性评估人员测评能力考核。

1. 工期要求

按照客户要求完成测评（测试、安评等）工作。

1. 验收要求

最终输出省应急指挥中心项目信息化建设工程《商用密码应用方案评估报告》，并经委托方审核通过，并由商用密码主管部门备案通过。

**九、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 。

9.1资格项要求

投标人应是列入《国家密码管理局公告（第42号）》商用密码应用安全性评估试点机构目录的单位。

9.2综合评分法

9.2.1评分权值

总分为100分，评分分值分配如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **评分项目** | **技术评分** | **商务评分** | **价格评分** |
| 分值 | 50 分 | 40 分 | 10 分 |

9.2.2**商务评分表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评审内容** | **分数** | **评分细则** |
| **1** | **投标人**  **资质** | **20** | 1.具有中国合格评定国家认可委员会颁发的CNAS检验机构认可证书（未被撤销认可或暂停认可），认可的能力范围同时包括信息安全风险评估、网络安全等级保护测评、商用密码应用安全性评估（能力范围以CNAS官网查询截图为准，且需同时包括上述全部内容）。  2.具有中国合格评定国家认可委员会颁发的CNAS实验室认可证书（未被撤销认可或暂停认可）。  3.具有中国国家认证认可监督管理委员会颁发的检验检测机构资质认定证书（CMA）（未被撤销认可或暂停认可）。  4.承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构（以国家认监委、工业和信息化部、公安部、国家互联网信息办公室联合发文公告为准）。  5.具有中国国家认证认可监督管理委员会颁发的国家嵌入式软件产品质量检验检测中心资质认定授权证书。  同时具备以上5个资质证书得20分，少一个扣4分，扣完为止。  （以上资质证书须在有效期内，且未被暂停或撤销，提供各项资质证书的复印件并加盖公章，否则不得分） |
| **2** | 项目组人员资质（项目经理除外） | **16** | 投标人项目组人员通过国家密码管理局商用密码检测中心或国家商用密码应用安全性评估人员测评能力考核小组组织的商用密码应用安全性评估人员测评能力考核（分数在60分以上）：  通过考核人数≥12人得10分，少于12人得0分；考核成绩80分（含）以上每人得1分，最高得6分；  本项目最高16分。  需提供以上人员在本单位任职的相关证明材料（如：加盖政府有关部门印章的2023年连续3个月的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单，否则不得分） |
| **3** | 项目案例 | **4** | 投标人提供自2020年至今类似业绩，每提供1个有效类似业绩得0.5分.  本项最高得4分。要求提供加盖公章的合同关键页复印件。 |

9.2.3**技术评分表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评审内容** | **分数** | **评分细则** |
| **1** | **项目实施方案** | **6** | 依据各投标人项目实施方案内容进行评审。  内容全面，测评服务流程清晰，完全满足并优于采购需求，得6分；内容较全面，测评服务流程较清晰，完全满足采购需求，得4分；内容不够全面，测评服务流程不够清晰，不能完全满足采购需求，得2分；未提供得0分。 |
| **2** | **6** | 依据各投标人提交的测试模板、结果报告模板等测试过程文档模板进行评审。  模板内容完整、可操作性强，完全满足并优于采购需求，得6分；模板内容较完整、可操作性较强，完全满足采购需求，得4分；模板内容不够完整、可操作性不太强，不能完全满足采购需求，得2分；未提供得0分。 |
| **3** | **6** | 依据各投标人项目实施方案中进度控制相关内容进行评审。  实施计划进度内容非常详细，安排非常科学合理，完全满足并优于采购需求，得6分；实施计划进度内容较详细，安排较科学合理，完全满足采购需求，得4分；实施计划进度内容不够详细，安排不够科学合理，不能完全满足采购需求，得2分；未提供得0分。 |
| **4** | 项目经理资质 | **18** | 派驻本项目的项目经理具备以下资质：  1.具备硕士研究生或以上学历；  2.通过国家密码管理局商用密码检测中心的商用密码应用安全性评估人员测评能力考核成绩80分或以上；  3.PMP项目管理专业人士资格认证；  4.(ISC)2注册信息系统安全认证专家（CISSP）证书；  5.工信部和人社部共同颁发的信息系统项目管理师证书；  6.获得由中国密码学会商用密码应用安全性评估联合委员会颁发的优秀密评工作人员荣誉证书；  同时具备以上6个资质证书得18分，少一个扣3分，扣完为止。  需提供项目经理在本单位任职的相关证明材料（如：加盖政府有关部门印章的2023年连续3个月的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单。）复印件，否则不得分。 |
| **5** | 安全测评能力 | **8** | 自2017年起，曾取得了国家信息安全漏洞共享平台（CNVD）原创漏洞证明。  1.原创漏洞证明超过5个的，得8分，少一个扣1.6分，扣完为止；  提供加盖投标人公章的证书复印件 |
| **6** | 安全测评工具 | **6** | 具有以下安全测评工具：  1.长矛深度安全检测系统；  2.Nessus及Nexpose 漏扫管理系统工具  3.Fortify  4.ICSSCAN NX3-S  5.Canvas  6.Achilles  同时具备以上6个工具得6分，少一个扣一分，扣完为止。需提供安全测评工具加盖投标人公章的采购合同复印件。 |

## 9.2.4 价格分计算

|  |
| --- |
| 计算价格评分：价格分统一采用低价优先法计算，各有效投标人的评标价（指投标报价经算术修正和落实政府采购政策需进行的价格扣除后的价格）中，取最低价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算： |
| 价格评分=（评标基准价／评标价）×10分 |