**包**10**采购需求**

## （一）项目概况

对“海南智慧健康岛建设工程项目”包1至包6的相关软件系统进行商用密码应用安全性评估服务，确保信息系统中商用密码的应用符合规范、安全有效，保障数据和业务安全。

## **（二）技术商务要求**

根据《GB/T 39786-2021信息系统密码应用基本要求》《商用密码应用安全性评估管理办法》等，对本项目进行密评工作，通过密评工作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水平奠定基础，推动国产密码应用工作的进一步落实。同时，也指导评估对象的信息安全保障体系建设，增强密码安全管理意识，促进安全管理水平的提高。

### （1）技术要求

##### 1.1服务清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **系统等级** | 服务内容 |
|  | 数据健康大脑 | 3 | 1.商用密码应用安全性评估  2.协助备案工作 |
|  | 健康服务全岛通 | 3 |
|  | 三医联动智慧行 | 3 |
|  | 公共卫生医防融 | 3 |
|  | 行业治理防风险 | 3 |
|  | 数字健康创新引擎 | 3 |

##### 1.2服务内容

密码应用安全性评估过程包括但不限于以下测评活动：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。

按照商用密码应用安全性分类分级评估的要求，依据《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）要求及信息系统等级保护定级情况，进行评估，评估过程活动包括但不限于测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动，评估内容包括但不限于以下内容：

|  |  |  |  |
| --- | --- | --- | --- |
| **测评单元** | | | **测评指标** |
| 技术  要求 | 物理和环境安全 | 身份鉴别 | 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； |
| 电子门禁记录数据存储完整性 | b）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 | c）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 | a）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 | b) 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 | c) 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 | d) 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 | e) 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 | a) 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 | b) 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 | c) 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 | d) 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 | e) 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 | f) 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 | a) 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 | b) 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 | c) 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 | d) 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 | e) 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 | f) 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 | 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 | 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  要求 | 管理  制度 | 具备密码应用安全管理制度 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任；  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 | 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 | 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 | 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 | 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 | 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，各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录A； |
| 制定实施方案 | 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 | 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 | 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 | 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 | 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 | 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。 |

##### 1.3交付成果

测评单位交付成果和报告包括但不限于：

1、密码应用安全评估测评方案；

2、密码应用安全性评估报告；

3、密码应用安全性评估问题清单及整改建议；

4、整体性的汇总报告；

5、测评过程材料，包括调研表、技术测评记录、会议纪要等。

##### 1.4交付成果要求

按照本项目建设内容开展商用密码应用安全性评估并分别交付相应的商用密码应用安全性评估报告（包括原件扫描电子件）,评估报告应至少符合下列4点要求：

1、标准化：项目验收最关键的指标，应确保评估过程符合最新的国家标准规范；

2、系统稳定性：在评估过程中应确保软硬件环境的稳定性、运行正常；

3、系统文档：验收文档是否齐全、规范、准确、详细；

4、系统可操作性：交付成果清晰、通俗易懂。

##### 1.5验收要求

测评单位应根据整体工作计划和安排完成服务工作，交付商用密码应用安全性评估报告，协助建设单位向密码管理部门完成备案工作，确保本项目（主体建设）通过组织的竣工验收。

### （2）商务要求

##### 2.1采购标的所属行业

本次采购标的所属行业为软件和信息技术服务业。

##### 2.2服务期限

自合同签订之日起，采购人下达通知书后开始实施，投标人应当在60天内完成商用密码安全性评估并交付服务成果。

##### 2.3实施地点

采购人指定地点（海南省内）。

##### 2.4支付方式（以实际签订合同为准）

1.本合同签订后，采购人待省财政资金下达后，采购人凭测评单位开具的正式有效增值税普通发票在3个工作日内向测评单位支付合同金额的30%预付款。

2.本项目初验合格,待省财政资金下达后,且采购人确认测评单位提供的商用密码应用安全性评估及服务成果符合要求，采购人在收到测评单位开具的增值税普通发票之日起3个工作日内,向测评单位支付合同总金额的40% 。

3.本项目通过整体竣工验收,且采购人确认测评单位提供的商用密码应用安全性评估及服务成果符合要求，待省财政资金下达后，采购人在收到测评单位开具的增值税普通发票之日起3个工作日内,向测评单位支付合同总金额的30%。

注：测评单位每次申请付款应提供付款申请书、符合采购人要求的等额发票及采购人报账所必须的相关材料。测评单位申请付款时，如测评单位提供的材料不完整、不真实，采购人有权暂缓付款而不视为违约。

##### 2.5其它相关要求

###### 2.5.1项目组人员要求

1、测评单位须根据项目特点和实际情况，提出项目团队配置方案，包括团队成员、组织架构和分组分工等，满足项目实施建设的需要。

2、项目团队成员应不少于1名项目经理、4名项目团队人员，所有人员必须属于测试单位在册员工**（提供社保缴纳证明为认定依据或出具承诺函）**，并提供相应人员相关简历信息**（包含所学专业、学历等证明材料），相关证明须加盖投标人公章。**合同签订后根据采购人实际需要派驻相关资历人员驻场开展服务。

3、合同签订后根据采购人实际需要派驻相关资历人员驻场开展服务直至项目验收，驻场地点由采购人指定。如实际提供的项目团队与投标提供的团队名单材料不符，将视为虚假应标。若采购人认为项目经理或团队成员能力与工作所要求的能力不相称而提出更换时，测评单位必须予以更换，人员更换不得影响测评成果交付时间；测评单位单方面更换项目经理或团队成员必须经采购单位书面同意，否则按违约处理直至合同终止。

4、项目团队实施中提供7×8小时咨询服务。项目验收后提供1年的跟踪咨询服务，自项目验收通过之日起计算。在实施单位提出服务请求时，项目团队应在30分钟内响应，在24个小时内提供解决方案。

###### 2.5.2工作要求

1、提供详细的项目实施方案和计划进度说明书；

2、项目实施完成后提供可靠的后期技术服务工作；

3、严格按照双方确定的计划进度保质保量完成工作；

4、规范项目实施过程中的文档管理；

5、提供必要的增值服务：配合省信息化主管部门开展本项目电子政务工程项目绩效评价考核、跟踪监督及项目档案事后监督等工作。

6、在本项目竣工验收阶段，对信息化主管部门及专家提出的涉及本项目软件系统整改意见的，评估单位应积极配合就整改后的应用系统进行再次评估，并出具最终评估报告，确保项目质量。

###### 2.5.3安全保密要求

要求测评单位制定服务密码应用安全性评估制度，确定项目保密责任人，同时要求测评单位：

1、按照国家和海南省有关保密规定，与测评单位签订保密协议，参与测评或评估的工作人员签订保密承诺函；

2、严格履行保密职责，按照保密规定开展测评工作。

###### 2.5.4服务要求

测评单位需根据测评结果，应针对性的提出整改建议方案。整改建议方案应具有可操作性，符合采购单位实际情况，且能够切实解决问题。对于现状测评过程中发现的问题，测评机构应先出具问题汇总报告，并出具成果文件。

整改建议方案应明确设计依据、整改内容、整改建议、基于系统现状指导进行系统整改。在整改实施过程中，测评机构应全力支持，负责技术把关、整改验收以及其他咨询工作。