**包9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网络安全等级保护测评服务，确保信息系统的安全、稳定、合规运行，以及数据安全和风险可控。

## **（二）技术商务要求**

### **技术要求**

##### 服务商应具有国家信息安全等级保护工作协调小组办公室颁发等保测评资质等相关要求，依据《信息系统安全等级保护基本要求》（GB/T 22239-2019)、《网络安全等级保护测评过程指南》(GB/T 28449-2018)等国家规范和行业规范对我单位信息系统的安全技术体系和安全管理体系进行网络安全等级保护测评，出具《网络安全等级保护测评报告》，并提出具有针对性的整改建议，指导系统通过等保测评，并为采购人提供咨询、培训、现场支撑等服务。

##### 1.1服务范围

服务范围内的信息系统如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **系统等级** | 服务内容 |
|  | 数据健康大脑 | 3 | 1.协助备案工作  2.协助通过网络安全等级保护测评 |
|  | 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

通过委托专业的网络安全等级保护测评服务机构，对服务范围内的系统进行等保测评；依据《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）、《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）等规范，对信息系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等进行合规性检查，分析信息系统与安全保护等级要求之间的差距，并根据信息系统及安全防护措施的现状提出具有针对性的整改意见，最终出具通过的《网络安全等级保护测评报告》，确保信息系统的安全运行。服务期内，测评机构须向采购单位提供以下服务。

###### 1.2.1等级保护培训咨询服务

1.2.1.1等级保护政策/标准咨询

随着国家信息安全等级保护的推进工作，信息安全等级保护政策、法律法规和标准体系也会相应的发布和更新，测评机构应针对本项目设立信息安全等级保护咨询平台，明确较为固定的咨询服务人员，并根据咨询要求提供正式的答复资料和文档。咨询内容包括但不限于信息安全等级保护国内外发展动态、等级保护政策、法律法规和标准体系咨询服务。

1.2.1.2信息系统等级变更咨询

在信息系统出现等级变更时，测评机构须协助采购单位对信息系统进行分析，明确信息系统边界和定级对象，对信息系统的子系统进行划分，确定信息系统以及子系统的安全等级。

1.2.1.3等级保护建设整改咨询

按照信息系统安全总体方案要求，测评机构须结合信息系统安全建设项目计划，根据信息安全等级保护相关标准和规定，对采购单位等级保护建设整改工作提供全面的安全方案的详细设计咨询，结合采购单位的实际情况，协助采购单位落实安全技术与管理措施，并根据预期实现的安全目标，全程提供在建安全设备和系统的测试、验收工作，指导建设方进行系统整改，满足等保测评要求。

1.2.1.4信息系统安全检查咨询

在采购单位开展信息系统安全检查时，全程提供咨询服务，包括检查范围、检查方法、检查结果分析以及整改措施制定等。

###### 1.2.2等级保护测评服务

依据《信息系统安全等级保护基本要求》（GB/T 22239-2019）、《网络安全等级保护测评过程指南》（GB/T 28449-2018），对采购单位信息系统的安全技术体系和安全管理体系等进行网络安全等级保护测评，出具《网络安全等级保护测评报告》，并提出具有针对性的整改建议。

1.2.2.1测评内容

1、对采购单位的信息系统进行摸底、分析和梳理，提出详细的等保测评方案，并协助采购单位完成系统定级备案。

2、对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

① 安全技术测评：包括物理安全、通信安全、主机系统安全、应用安全和数据备份及恢复等五个方面的安全测评；

② 安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

③ 对涉及云计算、物联网、移动互联、IPv6等新技术新应用的系统开展测评，应参照《信息系统安全等级保护基本要求》（GB/T 22239-2019）、《网络安全等级保护测评过程指南》（GB/T 28449-2018）相关标准实施补充指标测评。

3、完成测评工作后，提出整改建议；最后出具符合公安部门要求的信息系统安全保护等级测评报告，并在后期整改实施过程中提供全程咨询服务（服务期自各项目系统平台竣工验收之日起1年）。

1.2.2.2测评实施

信息安全测评项目过程需按照《信息系统安全等级保护测评过程指南》开展工作，等级测评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、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

1、测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。

详细要求见下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工作内容** | **工作详细任务** | **输出成果** |
| 1 | 项目启动 | 1.组建测评项目组 | 向用户提交 《项目计划书》 《提供资料清单》 |
| 2.编制《项目计划书》 |
| 3.确定采购单位应提供的资料 |
| 2 | 信息收集分析 | 定级报告及整改方案分析 | 《系统基本情况分析报告》 |
| 1.整理调查表单 |
| 2.发放调查表单给采购单位 |
| 3.协助采购单位填写调查表 |
| 4.收回调查结果 |
| 5.分析调查结查 |
| 3 | 工具和表单准备 | 1. 测评机构应在测评开始前完成测评工作所需的测评工具的准备，并及时完成测评工具调试 | 测评工具清单、《现场测评授权书》 《测评结果记录表》 《文档交接单》 |
| 2.模拟被测系统搭建测评环境 |
| 3.模拟测评 |
| 4.准备打印表单 |

2、测评方案编制活动

测评方案编制活动包括测评对象确认、测评指标确定、工具测试点确定、测试内容确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工作内容** | **工作详细任务** | **输出成果** |
| 1 | 测评对象确认 | 识别被测系统等级  识别被测系统的整体结构  识别被测系统的边界  识别被测系统的网络区域  识别被测系统的重要节点和业务应用  确定测评对象 | 《测评方案》的测评对象部分 |
| 2 | 测评指标确定 | 识别被测系统业务信息和系统服务安全保护等级 | 《测评方案》的测评指标部分 |
| 选择对应等级的ASG三类安全要求作为测评指标 |
| 就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标 |
| 3 | 工具测试点确定 | 确定工具测试的测评对象  选择测试路径  确定测试工具的接入点 | 《测评方案》的测试工具接入点部分 |
| 4 | 测试内容确定 | 识别每个测评对象的测评指标 | 《测评方案》的单项测评实施和系统测评实施部分 |
| 识别每个测评对象对应的每个测试指标的测试方法 |
| 5 | 测评指导书开发 | 从已有的测评指导书中选择与测评对象对应的手册 | 《测评方案》的测评实施手册部分 |
| 针对没有现成测评指导书的测评对象，开发新的测评指导书 |
| 6 | 测评方案编制 | 描述测评项目基本情况和工作依据 | 向用户提交 《测评方案》 |
| 描述被测系统的整体结构、边界和网络区域 |
| 描述被测系统的重要节点和业务应用 |
| 描述测评指标 |
| 描述测评对象 |
| 描述测评内容和方法 |

3、现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工作内容** | **工作详细任务** | **输出成果** |
| 1 | 现场测评准备 | 现场测评授权书签署 | 会议记录、确认的授权委托书、更新后的测评计划和测评方案 |
| 召开现场测评启动会 |
| 双方确认测评方案 |
| 双方确认配合人员、环境等资源 |
| 确认信息系统已经备份 |
| 测评方案、结构记录表格等资料更新 |
| 2 | 现场测评和结构记录 | 依据测评指导书实施测评 | 访谈结果：技术安全和管理安全测评的测评结果记录或录音 文档审查结果： 管理安全测评的测评结果记录 配置检查结果： 技术安全测评的网络、主机、应用测评结果记录表格 工具测试结果： 技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 实地查看结果： 技术安全测评的物理安全和管理安全测评结果记录 测评结果确认： 现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件 |
| 记录测评获取的证据、资料等信息 |
| 汇总测评记录，如果需要，实施补充测评 |
| 3 | 结果确认和资料归还 | 召开现场测评结束会 |
| 测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可 |
| 测评人员归还借阅的各种资料 |

4、报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动详细要求见下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工作内容** | **工作详细任务** | **工作依据** |
| 1 | 单项测评结果判定 | 分析测评项所对抗威胁的存在情况 | 等级测评报告的单项测评结果部分 |
| 分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较 |
| 综合判定单个测评项的测评结果 |
| 2 | 单元测评结果判定 | 汇总每个测评对象在每个测评单元的单项测评结果 | 等级测评报告的单项测评结果汇总分析部分 |
| 判定每个测评对象的单元测评结果 |
| 3 | 整体测评 | 分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况 | 等级测评报告的系统整体测评分析部分 |
| 分析被测系统整体结构的安全性对结果的影响情况 |
| 4 | 系统安全保障评估 | 综合单项测评和整体测评结果，计算修正后的安全控制点得分和层面得分，并根据得分情况对被测系统的安全保障情况进行整体评价 | 等级测评报告的系统安全保障评估部分 |
| 5 | 风险分析 | 整体测评后的单项测评结果再次汇总 | 等级测评报告的风险分析部分 |
| 分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性 |
| 分析威胁利用安全问题后造成的影响程度 |
| 为被测系统面临的风险进行赋值 |
| 评价风险分析结果 |
| 6 | 等级测评结论形成 | 统计再次汇总后的单项测评结果为部分符合和不符合项的项数 | 等级测评报告的等级测评结论部分 |
| 形成等级测评结论 |
| 7 | 测评报告编制 | 概述测评项目情况 | 等级测评报告 提交用户 |
| 描述被测系统情况 |
| 描述测评范围和方法 |
| 描述整体测评情况 |
| 汇总测评结果 |
| 描述风险情况 |
| 给出等级测评结论和整改建议 |

### **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天内完成等保测评服务并交付服务成果。

##### 2.3实施地点

采购人指定地点（海南省内）。

##### 2.4支付方式

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

2.本项目初验合格,且采购人确认测评机构提供的网络安全等级保护测评服务及服务成果符合要求，待省财政资金下达后，采购人在收到测评机构开具的增值税普通发票之日起3个工作日内,向测评机构支付合同总金额的40% 。

3.本项目通过整体竣工验收,且采购人确认测评机构提供的网络安全等级保护测评服务及服务成果符合要求，待省财政资金下达后，采购人在收到测评机构开具的增值税普通发票之日起3个工作日内,向测评机构支付合同总金额的30%。

注：测评机构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。测评机构申请付款时，如测评机构提供的材料不完整、不真实，采购人有权暂缓付款而不视为违约。

##### 2.5服务要求

###### 2.5.1项目组人员要求

1、测评机构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、测评机构项目团队成员应不少于1名项目经理、4名项目团队人员。项目经理负责项目现场实施，至少有3年以上等级保护测评工作经历和经验；团队成员至少有1年以上的等级保护测评工作经历和经验。所有人员必须属于测评机构在册员工（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），相关证明须加盖测评机构公章。**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、合同签订后必须派驻相关资历人员驻场开展服务。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。若采购单位认为项目负责人或者技术人员能力与工作所要求的能力不相称而提出更换时，测评机构必须予以更换，人员更换不得影响测评成果交付时间；测评机构单方面更换项目负责人或技术员（工程师）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。项目验收后提供不少于半年的跟踪咨询服务，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

测评机构须给出采购单位在进行调查和评估时所需要提供的信息列表，并经采购单位确认。采购单位有权利不提供信息列表以外的任何信息。

安全评估必须按照分层的原则，包括但不限于以下对象：物理环境、网络结构、网络服务、主机系统、数据、应用系统、安全系统、安全相关人员、处理流程、安全管理制度、安全策略等。

在评估前，将采购单位系统根据业务特性和安全要求划分成不同的区域，并确定安全保护等级。然后设计不同等级的安全评估标准指标，并经采购单位认可，以保证评估标准的适用性。测评机构须在投标文件中详细描述针对采购单位网络系统的分为不同等级的评估标准指标。

测评机构应详细描述安全调查和评估的组织方式，包括组成的人员及分工、评估的过程组织、实施时间安排、评估方式所遵循的标准等。测评机构需要描述调查和评估过程的步骤，每一步骤的具体内容、时间安排、详细实施过程、可能对网络及主机造成的影响等等。

安全调查和评估的过程中，测评机构如需采购单位配合，测评机构需要详细描述需要配合的内容。如需要采购单位协助完成各种表单，需要详细描述表单的名称、功能及主要表项等等，并由测评机构给出具体示例。采购单位有权利拒绝提供任何未事先提出的配合要求，由此产生的损失由测评机构负完全责任。

安全调查和评估过程中，如需使用安全工具，请详细描述所使用的安全工具（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等。所使用的安全工具必须具备公安部颁发的《计算机安全产品销售许可证》。

测评机构应向采购单位提供详细的评估的原始材料、各种表单及结果报告。

测评机构需要详细描述本次评估采用的评估方式及标准。

###### 2.5.3安全保密要求

要求测评机构制定等保测评服务安全保密制度，确定项目保密责任人，同时要求测评机构：

1、按照国家和海南省有关保密规定，与采购单位签订保密协议，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，按照保密规定开展等保测评工作。

###### 2.5.4交付成果和验收要求

1、测评机构交付成果和报告包括但不限于：

《网络安全等级保护测评报告》（结果为良或以上）

《网络安全等级保护安全整改建议方案》

信息系统定级相关文件和报告

测评过程材料，包括调研表、技术测评记录、会议纪要等。

2、项目验收要求

测评机构必须提供给采购单位详细的项目验收方案。成立由采购单位、测评机构以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

###### 2.5.5服务要求

测评机构需根据测评结果，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。