佛山市高明区人民医院
LIS 及 PACS 系统二级等保测评
采购需求说明

一、本项目报名方法

在本项目截止报名时间前，发送报名表（附件 2 佛山市高明区人民医院信息系统报名表）和本公告第三点所提及资料至电子邮箱 gm88882172@21cn.com，并通过电话 0757-88688809 或 88882172，与医院工作人员确认已在邮箱收到报名表为报名成功。

注意事件：1.报名截止时间以邮箱收到邮件时间为准；2.发送电子邮件后，务必要与医院工作人员联系、确认，否则可能因漏收邮件而导致报名不成功。

二、报名联系方式：

佛山市高明区人民医院信息科

采购咨询联系电话：0757-88688809　88882172

监督投诉联系电话 0757-88828698

电话接听时间为周一至周五早上 8 点至 12 点；下午 2 点半至 5 点半。

三、报名提交材料要求：

1、企业法人营业执照（副本）复印件。

2、税务登记证书（国、地税）复印件。

3、组织机构代码证复印件。

4、如已办理营业执照、税务登记证、组织机构代码证三证合一的企业，请提交加载法人和其他组织统一社会信用代码的营业执照复印件。

5、参会人如为法人代表，须提交报名单位法人代表证明书、法人代表第二代居民身份证复印件。参会代表如为授权代理人，须提交报名单位法人代表证明书、法人代表第二代居民身份证复印件、法人授权书及授权代理人第二代居民身份证复印件。未能通过核实的将会被取消报名资格。

7、报名单位应遵纪守法、诚信经营，近三年内（自招标公告发布之日起往前推三年）无违规违法行为或采购活动中无不良记录，报名单位须书面承诺。

四、报名其它要求：

1、参加采购单位必须响应本采购项目的全部内容和要求；预算报价包括本项目采购清单的所有内容，费用已包含一切预见或不可预见费用。

2、请严格按照本公告附件填写推介表，纸质和电子版推介表随参加投标人在投标当日自行携带入场提交。

3、本项目不接受联合体参与投标。

五、项目需求简介

本次服务对象为两个二级系统（PACS、LIS），由符合条件的第三方测评机构对我院的 2 个信息系统进行等级保护测评，另外，需对照二级安全等级保护标准完成我院 PACS 系统和 LIS 系统提供部分安

全服务。

六、性能需求

本次测评服务对象为 2 个二级系统（LIS 系统和 PACS 系统）。

序号	分类	详细描述	单位	数量
1	网络安全等级保护测评服务	邀请第三方网络安全等级保护测评机构对服务对象开展网络安全等级保护测评，出具安全等级保护测评报告，协助完成资料提交等。	个	2
2	信息安全加固服务	针对等级保护测评工作中发现的安全漏洞、安全隐患、不安全配置项，提供安全加固建议，并协助进行安全修复。	项	1
3	安全渗透测试服务	利用各种主流攻击技术对客户授权指定的系统做模拟攻击测试，提供渗透测试报告和改进建议。	项	1
4	安全应急演练服务	开展网络安全应急演练服务，演练结束后对本次演练效果进行评估及建议并形成报告。	次	1
5	网络安全扫描服务	对服务对象进行安全扫描，发现漏洞，提供扫描报告，并根据扫描报告给出漏洞整改或修复建议。	项	1
6	管理制度修订完善	根据等级保护二级要求，完善各项信息安全管理制度，通过对制度的补充、完善，形成一套可以满足信息安全等级保护二级要求，可以实际运用的管理制度文件。	次	1
7	网络安全咨询服务	根据日常工作中遇到的实际问题进行分析和探讨，结合安全发展趋势从安全技术和安全策略等方面，提供专业的安全建议。	项	1

1、网络安全等级保护测评服务

由具备资质的第三方测评机构按照等保 2.0 的相关要求对信息系统安全等级保护状况进行测试评估，包括安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求。

安全通用要求规定了不管等级保护对象形态如何必须满足的要求，评单元分

为安全技术测评和安全管理测评两大类，技术要求包括：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；管理要求包括：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

云计算拓展要求包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全建设管理。

移动互联网拓展要求包括：安全物理环境、安全区域边界、安全计算环境、安全建设管理。

物联网安全拓展要求包括：安全物理环境、安全区域边界、安全建设管理。

工业控制系统安全拓展要求包括：安全物理环境、网络通信网络、安全区域边界、安全计算环境。

2、信息安全加固服务

针对网络安全扫描服务和安全渗透测评服务过程中发现的系统漏洞、安全隐患和配置缺陷，结合单位实际情况，提供加固建议和方案，协助配合用户完成整改修复。

3、安全渗透测试服务

由安全工程师模拟黑客的行为模式，采用黑客的漏洞发现和利用技术，以及尽可能多的攻击方法，对目标应用系统的安全性进行深入分析，验证当前的安全防护措施，找出风险点，提供有价值的安全建议。渗透测试对象包括应用服务系统（WEB 系统）以及相关的其他系统。

渗透测试服务配套工具详细功能需求如下表：

序号	指标子项
1	支持网络地址自动快速扫描
2	支持资产集中管理
3	支持主机/应用识别服务
4	支持 appscan 检测结果文件导入
5	支持 AWVS 检测结果文件导入
6	支持 nessus 检测结果文件导入

序号	指标子项
7	支持 OWASP ZAP 检测结果文件导入
8	支持国产网络安全漏洞扫描产品检测结果文件导入
9	支持渗透测试结果 excel 文件导入
10	支持基于上述结果文件导入，自动化输出渗透测试报告
11	基于国密算法加密通道的中文管理界面。

4、安全应急演练服务

为了健全单位的运行应急机制，检验网络与信息安全综合应急预案和业务技术专项应急工作机制及有效性，验证相关组织和人员应对网络和信息安全突发事件的组织指挥能力和应急处置能力，满足突发情况下网络与信息系统运行保障和故障恢复的需要，确保信息系统安全畅通，提供安全应急演练，以不断提高各部门开展应急工作的水平和效率，发现预案的不足，进一步完善应急预案。

根据实际环境，提供专项应急演练方案，准备演练场景，以模拟演练的方式检验应急预案和应急流程是否完善，提高应急处理能力。

5、网络安全扫描服务

对所需评估的网络、信息系统进行安全扫描，采用专业安全扫描工具与人工检查相结合的方式，检测主机的安全策略实施现状，检测主机是否存在本地漏洞，对网站和应用系统进行安全扫描，发现漏洞，提供扫描报告，并根据扫描报告给出漏洞整改或修复建议，协助单位技术人员完善本地策略的实施。

专业安全扫描服务工具要求：

指标项	指标子项
产品功能	具备以下产品功能： (1) 系统漏洞扫描； (2) 网站漏洞监控； (3) 数据库漏洞扫描； (4) 基线配置核查； (5) 工控漏洞扫描； (6) 大数据漏洞扫描； (7) APP 漏洞扫描；

指标项	指标子项
	(8) Docker 漏洞扫描； (9) WIFI 安全检测。
等级保护专项功能	具备以下等保专项功能： (1) 支持新建等级保护测评任务，包括 SAG 等级、备案证明编号、被测单位、测评单位等信息。 (2) 支持设置等级保护测评信息，包括机房、网络设备、安全设备、服务器、终端、数据库、业务系统等，以及安全人员、安全文档、安全服务、访谈人员等。 (3) 内置有等保合规库，测评任务包含等保 2.0 任务。 (4) 支持将扫描结果与信息安全等级保护合规库进行关联分析，生成满足规范要求的等级保护测评报告。

6、管理制度修订完善

根据等级保护要求，完善各项信息安全管理制度，通过对制度的补充、完善，形成一套可以满足信息安全等级保护要求，并且可以实际运用的管理制度文件。

7、网络安全咨询服务

根据客户日常工作中遇到的实际问题进行分析和探讨，结合安全发展趋势从安全技术和安全策略等方面，向客户提供专业的安全建议。

七、付款方式要求

1.出具差距测评报告，后 30 天内，支付 20%。
2. 出具合规的验收测评报告，提交公安部门，在备案完成并取得备案回执后 30 天内付 80%。

八、项目执行期限

本项目如签订合同 8 个月后，仍未法完全履行项目全部内容，则合同自行中止。