

佛山市高明区人民医院

核心系统信息安全等级保护测评服务需求说明

我核心信息系统为 HIS、LIS、PACS，安全等级保护分别拟定三级、二级、二级，根据《网络安全法》等法律法规需要进行等级保护测评。本次为请有资质的测评公司为我院提供这三个系统的测评服务。包括等级保护信息系统资产调研、现场差距测评，出具差距测评报告，督促我院完成等级保护差距整改，完成差距整改后及时跟进开展等级保护验收测评，出具验收测评报告，并协助提交公安机关，确定公安机关备案回执。

测评服务要求：由符合条件的第三方测评机构对我院的 3 个核心信息系统进行等级保护测评，并完成等保测评备案工作。

依据 GB/T22239《信息安全技术信息系统安全等级保护基本要求》以及《信息系统安全等级保护测评指南》的要求，对信息系统安全等级保护状况进行测试评估，包括两个方面的内容：一是安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，对安全控制测评的描述，使用测评单元方式组织。测评单元分为安全技术测评和安全管理测评两大类。安全技术测评包括：物理安全、网络安全、主机系统安全、应用安全和数据安全等五个层面上的安全控制测评；安全管理测评包括：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控制测评。

在等级保护测评过程中，应采用人工访谈、工具检测、登录系统检测、文档分析的方式分析信息系统在等级保护方面与标准要求的差距；为确保测评机构开展信息系统安全测评的质量以及提高自动化程度，在工具检测方面，测评机构采用测评工具辅助完成测评工作，利用测评工具，提高测评人员工作效率、测评客观公平、测评结果可管理分析汇总。

一、测评工具指标要求：

项目	指标
产品要求	产品须提供公安部的《计算机信息系统安全专用产品销售许可证》的复印件。
	产品须提供国家保密科技测评中心的《涉密信息系统产品检测证书》的复印件。
	若非投标人独立研发的产品，请提供产品原厂商对该项目的授权书原件。

产品性能	<p>1. 系统漏洞扫描（漏洞知识库大于 82000 条，支持无限个扫描对象范围），</p> <p>2. WEB 漏洞扫描（支持会话录制、漏洞验证、敏感关键字检测、网马和暗链检测、钓鱼网站检测，支持无限个扫描对象范围），</p> <p>3. 网站安全监控（含 WEB 漏洞检测、网站可用性检测、网页篡改检测、敏感关键字检测、网马和暗链检测、钓鱼网站检测等，支持 64 个网站），</p> <p>4. 数据库安全扫描（支持国产数据库、nosql 数据库等十五大类，支持无限个扫描对象范围），</p> <p>5. 安全基线核查（支持多种协议远程检测，也支持 Agent 本地检测，支持无限个扫描对象范围），</p> <p>6. 工控漏洞扫描加强版（支持无损的工控漏洞扫描技术，工控专有的漏洞知识库数量大于 2200 多条，支持无限个扫描对象范围），工控漏洞扫描（支持无限个扫描对象范围），</p> <p>7. 大数据漏洞扫描（支持无限个扫描对象范围），</p> <p>8. APP 漏洞扫描（支持无限个扫描对象范围），</p> <p>9. WiFi 安全检测（支持无限个扫描对象范围），</p> <p>10. Windows 安全加固（支持无限个扫描对象范围）。提供上述界面截图并加盖厂商公章。</p>	
等级保护测评报告	<p>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。</p> <p>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。</p> <p>★系统内置有等级保护测评合规库，测评内容应包括技术要求和管理要求两大类。其中技术类测评应包括对物理安全、网络安全、主机安全、应用安全和数据安全及备份恢复等方面的测评。管理类测评应包括安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等方面的测评。提供界面截图并加盖厂商公章。</p> <p>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。提供界面截图并加盖厂商公章。</p>	
一键智能扫描	支持一键扫描，只需要输入 IP、IP 网段、URL，系统会自动调用选中的扫描引擎，使用默认的扫描模板、扫描参数对目标系统进行漏洞扫描，简单方便。提供界面截图并加盖厂商公章。	
系统漏洞扫描模块	扫描对象	<p>Windows 系列：NT、2000、XP、2003、Win7、Win10、2008、2012、2016 等。</p> <p>Linux 系列：Amazon Linux、CentOS、Debian、Fedora、Red Hat、SuSE、Ubuntu 等。</p> <p>Unix 系列：AIX、FreeBSD、HP—UX、Solaris、Mac OS X 等。</p> <p>WEB 应用服务：IIS、Apache、Tomcat、Websphere、Weblogic、Nginx 等。</p> <p>应用软件：Microsoft Internet Explorer、Office、RealPlayer、Outlook、Adobe Flash 等。</p> <p>数据库：Oracle、Mysql、DB2、Informix、MSSQL、Sybase 等。</p> <p>网络设备：思科 Cisco、华为 HUAWEI、华三 H3C 等。</p> <p>安全设备：juniper 等。</p> <p>虚拟化平台：Vmware EXSi、Citrix XenServer、Microsoft Hyper-V</p>

		<p>等。</p> <p>云平台：VCenter、OpenStack、Eucalyptus 等。</p> <p>大数据：Hadoop、Spark、HBase、Hive 等。</p> <p>视频监控系统：海康（Hikvision）、大华（Dahua）、Axis（安迅士）、D-Link（友讯）等。</p> <p>工业控制系统：西门子 SIMATIC、施耐德 Schneider、通用电气 GE、艾默生 Emerson、霍尼韦尔 Falcon、研华等。</p>
	扫描技术	支持智能服务识别、授权登录扫描、安全优化扫描等。
	扫描策略	▲支持 25 种以上的默认扫描策略，分别针对不同的扫描对象，如 Windows、Linux、Unix、数据库、WEB 应用服务、网络设备、虚拟化平台、云平台、大数据、视频监控系统、工控系统等。提供界面截图并加盖厂商公章。
	系统漏洞知识库	<p>▲系统漏洞知识库的检测脚本大于82000多条，所有的检测脚本都能够产品中随机进行浏览和多维度检索。提供界面截图并加盖厂商公章。</p> <p>系统漏洞知识库兼容CVE、CNCVE、CNNVD、CNVD、CVSS、Bugtraq等主流标准。</p>
空间资产管理模块	资产类别	包括：操作系统、网站、数据库、中间件、网络设备、安全设备、虚拟化设备等。
	资产探测	支持主动探测资产的操作系统类型、开启的端口等，智能识别端口对应的服务以及软件版本等。
	资产权重	支持资产的权重设置，可以对资产进行赋值。
	资产管理	▲支持将资产信息批量导入到资产树，可在资产树上直接指定资产开展扫描任务，也可以查看该资产相关详细信息。提供界面截图并加盖厂商公章。
	资产报告	支持将资产导出，生成资产报告，报告内容包括：资产组、资产名、IP 地址、MAC 地址、端口、主机名、操作系统、负责人、地区等信息。提供界面截图并加盖厂商公章。
	分组管理	支持资产信息设置，包括资产名、所属组、负责人、所在地等。
	工控管理	▲支持工控系统信息设置，包括设备类型（PLC、RTU、DCS、数据采集模块、继电保护装置、DTU 等），厂商（abb、siemens、schneider_electric、ge、advantech 等），设备型号，设备版本，物理地址等信息。提供界面截图并加盖厂商公章。
	网站管理	▲支持 WEB 网站信息设置，包括网站名、URL、负责人、所在地、操作系统、页面类型、数据库类型、WEB 认证、客户端证书、COOKIE 配置、URL 提取规则等。提供界面截图并加盖厂商公章。
网站安全监控模块	网络拓扑图	支持自动生成网络拓扑图，资产类型包括：机房、云、交换机、路由器、防火墙、负载均衡、服务器、客户机等。还可以进行添加、修改、删除，并查看各资产的详细信息。提供界面截图并加盖厂商公章。
	网站监控内容	▲支持WEB漏洞检测、网站可用性检测、网页篡改检测、敏感关键字检测、网马和暗链检测、钓鱼网站检测等。提供界面截图并加盖厂商公章。
	WEB 漏洞检测	支持OWASP TOP 10漏洞检测，支持SQL注入、XSS跨站脚本、命令执

	测	行、目录遍历、上传漏洞等检测。	
		支持输入Cookie信息，进行登录扫描。支持会话录制功能。提供界面截图并加盖厂商公章。	
	网站可用性检测	支持检测网站是否可用，检测 DNS 解析时间，检测连接服务器时间，检测服务器响应时间，检测域名劫持等。	
	网页篡改检测	支持白名单设置，图片 MD5 比较，页面标题比较，删除链接提醒，新链接提醒，页面相似度阈值设置等。	
		支持定位到篡改的页面源码位置，高亮显示。提供界面截图并加盖厂商公章。	
	敏感关键字检测	支持自定义敏感关键字，基于分词的语义分析。	
		支持身份证信息、银行卡等个人敏感信息识别，支持图片文字识别。提供界面截图并加盖厂商公章。	
数据库安全扫描模块	网马和暗链检测	支持网马、暗链动态检测。 支持 Activex 识别。	
	钓鱼网站检测	支持钓鱼网站检测。	
	扫描对象	支持关系型数据库：Oracle、Mysql、Sqlserver、Sybase、DB2、Informix、Postgresql。	
		▲支持国产数据库：人大金仓 Kingbase、达梦 dameng、南大通用 GBase。提供界面截图并加盖厂商公章。	
		▲支持 nosql 数据库：MongoDb、Redis、CouchDb、Memcache。提供界面截图并加盖厂商公章。	
	扫描技术	支持非授权扫描，只需要配置目标数据库的 IP 地址、数据库类型和端口号。	
		支持授权扫描，需要配置目标数据库的 IP 地址、数据库类型、端口号，以及高权限用户名和密码等认证信息。	
		▲能够通过对数据库对象、二进制文件等进行对比，从而发现数据库中潜藏的木马。提供界面截图并加盖厂商公章。	
工控漏洞扫描模块	认证授权	▲支持选择相应的数据库类型，包括主流的数据库、国产数据库和 nosql 数据库，可以输入相应的端口号、用户名、密码等。并支持认证授权的测试验证功能，确保认证授权的正确性和可用性。提供界面截图并加盖厂商公章。	
	数据库漏洞知识库	▲数据库漏洞知识库的扫描策略大于2000多条，所有的检测脚本都能够在产品中随机进行浏览和多维度检索。提供界面截图并加盖厂商公章。	
		▲数据库漏洞知识库兼容 CVE、CNCVE、CNNVD、CNVD 等主流标准。提供界面截图并加盖厂商公章。	
		数据库漏洞知识库根据漏洞类型分为：SQL 注入漏洞、权限绕过漏洞、缓冲区溢出漏洞、访问控制漏洞、拒绝服务漏洞、不安全配置等。	
		▲数据库配置基线方面的漏洞有：用户帐号、密码策略、日志配置、权限控制、版本补丁等。提供界面截图并加盖厂商公章。	
	扫描对象	支持专有的工控系统	包括：abb、siemens（西门子）、schneider_electric（施耐德）、ge（通用电气）、rockwellautomation（罗克韦尔）、honeywell（霍尼韦尔）、beckhoff（德国倍

			福)、beldenhirschmann(美国百通赫思曼)、moxa(摩莎)、omron(欧姆龙)、pheonixcontact-software(菲尼克斯)、koyo(日本光洋)、mitsubishi(三菱)、advantech(研华)等。
		支持传统的IT系统	包括:windows、centos、redhat、debian、ubuntu、freebsd、symantec、cisco等。
	扫描技术	远程无损扫描技术	▲支持采用低发包率、非漏洞触发的远程指纹探测技术,远程检测出目标工控系统的设备型号和相关漏洞。提供界面截图并加盖厂商公章。
		本地漏洞库比对技术	▲支持在系统平台上直接手动输入工控系统相关的设备型号,通过离线比对工控漏洞库获得目标工控系统的漏洞信息。提供界面截图并加盖厂商公章。
	漏洞知识库	兼容标准	工控漏洞知识库兼容CVE、CNNVD、CNVD等主流标准。提供界面截图并加盖厂商公章。
		工控漏洞库	▲工控专有的漏洞知识库数量大于2200多条,所有的漏洞信息都可以在系统中随机进行浏览和多维度检索。提供界面截图并加盖厂商公章。
工控漏洞扫描模块	▲支持检测SCADA、DCS、PLC等控制系统存在的安全风险。提供界面截图并加盖厂商公章。		
	支持检测ModbusTCP、S7等协议存在的安全风险。		
	支持远程、非接触式为工业控制系统进行安全漏洞检测。包括西门子SIMATIC、施耐德Schneider、通用电气GE、艾默生Emerson、霍尼韦尔Falcon、研华等工控设备。		
	▲工控漏洞知识库所有的检测脚本都能够在产品中随机进行浏览和多维度检索。提供界面截图并加盖厂商公章。		
	工控漏洞知识库兼容CVE、CNCVE、CNNVD、CNVD、CVSS、Bugtraq等主流标准。提供界面截图并加盖厂商公章。		
大数据漏洞扫描模块	▲支持对主流大数据组件进行漏洞扫描和安全配置合规性检查,包括Hadoop、Spark、Hbase、Solr、ES等。		
	大数据漏洞知识库所有的检测脚本都能够在产品中随机进行浏览和多维度检索。		
	大数据漏洞知识库兼容CVE、CNCVE、CNNVD、CNVD、CVSS、Bugtraq等主流标准。		
APK漏洞扫描模块	▲支持检测APK中存在的组件安全、配置安全、数据安全和恶意行为等安全风险。提供界面截图并加盖厂商公章。		
	▲支持检测的内容包括:允许程序读写系统设置、允许程序访问GPS位置、允许程序发送SMS短信、允许程序拨打电话、允许程序读取底层系统日志文件、加载本地库等。提供界面截图并加盖厂商公章。		
	支持直接拖入APK文件,支持上传APK文件。		
	支持获得APP相关信息:包括版本、sdk版本、证书、md5、sha1、sha256等。		
WiFi安全检测模块	▲支持识别接入点和WiFi信道,支持WiFi的弱密码检测。提供界面截图并加盖厂商公章。		
	支持搜索出无线WIFI的SSID、硬件厂商、MAC地址等信息。		
	支持搜索出无线WIFI隐藏SSID。		
	支持获取各无线节点所连接的客户端相应的MAC地址等信息。		

恶意代码检测	▲支持木马后门的离线检查，可以下载检查工具。提供界面截图并加盖厂商公章。
	▲支持网站恶意代码的离线检查，可以下载检查工具。提供界面截图并加盖厂商公章。
报表管理	支持将扫描结果以HTML、WORD、PDF、XML、XLSX等通用格式导出。
	扫描报告包含漏洞描述、漏洞详情、风险级别、加固建议等。
	▲支持扫描任务的合并功能，合并后的任务可统一出具报告，并保留合并前的任务及报告。提供界面截图并加盖厂商公章。
	支持扫描任务的对比分析功能，不仅可以灵活选择不同时间段的扫描任务进行对比分析，了解新增漏洞、减少漏洞的相关数据。还可以自动与上一次的扫描任务进行对比，自动获得新发现漏洞、已修复漏洞的相关数据。提供界面截图并加盖厂商公章。
	▲支持报告预览、报告导出、报告生成、报告查询与下载等。提供界面截图并加盖厂商公章。
系统管理	支持用户的增删改，默认用户有系统管理员admin、安全审计员audit、安全保密管理员secret，支持设置密码有效期、密码最短长度、用户登录最大错误次数、错误次数达上限后锁定时间。
	▲支持用户权限的分级管理。可以限定用户允许登陆IP地址范围，限定用户允许扫描IP地址范围及允许扫描的网站。提供界面截图并加盖厂商公章。
	支持角色的增删改，默认角色有系统管理员、安全审计员、安全保密管理员。
	▲支持在系统界面开启或关闭SSH服务、SNMP服务方便远程维护。支持将自身运行情况以SNMP发送至第三方安全管理中心等平台。支持将自身运行情况以SYSLOG发送至第三方安全管理中心等平台。提供界面截图并加盖厂商公章。
	支持设置预警邮件服务器，可以将漏洞扫描结果通过邮件发送给安全管理员。
	支持设置预警短信平台，包括阿里云短信、腾讯云短信、网易云信，可以将漏洞扫描结果通过短信发送给安全管理员，短信内容支持定制。提供界面截图并加盖厂商公章。
	支持日志的查询、删除、导出、导入，支持按用户名、操作事件、IP地址、开始时间、结束时间进行查询，支持设置最大存储空间。
	支持数据备份，可以对当前系统、数据进行备份，也可以上传备份文件进行恢复。提供界面截图并加盖厂商公章。
	支持配置网卡、重启、关机，可以查看CPU、内存、硬盘等占用情况，以及引擎版本、策略版本等信息。
大屏展示	▲提供诊断工具，包括ping、tracert、curl、摘要算法（MD5和SHA等）、编/解码、加/解密等。提供界面截图并加盖厂商公章。
	▲支持脆弱性分析大屏展示，通过大屏展示各类漏洞地理分布情况，资产统计，漏洞统计，最新漏洞、风险趋势等。提供界面截图并加盖厂商公章。
使用模式	采用B/S模式管理，通过浏览器就可以正常使用、维护，不需要再安装其它软件。提供界面截图并加盖厂商公章。
产品部署	支持单机部署，支持分布式部署。
	产品旁路接入网络，无需改变原有的网络架构。

二、公司技术团队及专业资质

本项目项目负责人能力情况	▲1、同时具备等级测评师证书、CISP 认证证书、IT 服务项目经理证书、ITIL Foundatior Examination 认证证书、计算机软件产品检验员、CISAW 认证证书
	2、发表过等级保护方向的论文
	3、网络安全类的获奖情况：省级或以上。
	（提供相关证明文件复印件加盖公章及近三个月在投标单位购买社保的证明文件复印件）
参与本项目技术队伍能力情况	1、具备有广东省信息网络安全专业技术人员继续教育证书 3 人或以上。
	▲2、具备 CISAW 认证证书 1 人或以上。
	▲3、具备 CISP 认证证书 1 人或以上。
	▲4、具备 IT 服务项目经理证书 1 人或以上。
	5、具备 ITIL Foundatior Examination 认证 1 人或以上。
	6、具备计算机软件产品检验员证书 1 人或以上。
	（提供相关证明文件复印件加盖公章及近三个月在投标单位购买社保的证明文件复印件）
公司资质	▲具备国家信息安全等级保护工作协调小组办公室颁发的《信息安全等级保护测评机构推荐证书》（提供证明文件，复印件加盖公章）
	获评全国网络安全等级保护测评机构先进单位（提供证明文件，复印件加盖公章）
	获得广东省公安厅金盾工程第三方检测机构验收资质（提供证明文件，复印件加盖公章）
	▲为广东省关键信息基础设施网络安全检查技术支持单位（提供证明文件，复印件加盖公章）
	▲具备计算机信息系统安全服务等级证（提供证明文件，复印件加盖公章）
	▲投标人具有信息网络安全应急响应服务平台的建设经验（提供证明文件，复印件加盖公章）
	▲投标人具有部委授权的全国性内网安全测评项目实施经验（提供证明文件，复印件加盖公章）
	▲投标人 2016 年以来具有网络安全服务类项目经验，以合同复印件为准。 等级保护测评服务项目（单个项目合同中的服务金额不少于 40 万元）， 其它信息安全服务项目（单个项目合同中的服务金额不少于 30 万元）， 关键信息基础设施服务类项目（单个项目合同中的服务金额不少于 40 万元）。

三、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%。

四、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。