**中山大学孙逸仙纪念医院临床检验信息管理系统（三级）**

**等保测评项目采购公告**

一、项目名称/采购编号

**（****中山大学孙逸仙纪念医院临床检验信息管理系统（三级）等保测评项目/2023WL-30）**

二、项目背景

为贯彻落实国家《中华人民共和国网络安全法》、《信息安全等级保护工作的实施意见》等相关文件要求以及自身信息系统的信息安全考虑，从全局的高度看待目前我院信息系统所面临的信息安全风险，切实提高我院网络与信息安全防护与管控能力，保障和促进我院的信息系统的安全。为此，本次采购我院临床检验信息管理系统（三级）提供网络安全等级保护测评服务，进一步推进等级保护工作和巩固前期我院在信息安全方面所做的工作成果，切实为我院的信息化建设做好信息安全基础保障。

三、项目需求

1、项目标的及最高限价

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 标的名称 | 服务期限 | 最高限价 |
| 1 | 中山大学孙逸仙纪念医院临床检验信息管理系统（三级）等保测评项目 | 1年 | 4.5万元 |

2、所有对本项目作出响应的供应商，都需要出具完全响应采购方“临床检验信息管理系统（三级）等保测评项目”所有项目需求的承诺函，并加盖公章，若未能全部响应或不出具承诺函，视为无效投标。

四、采购内容

**4.1、项目要求**

**4.1.1 “中山大学孙逸仙纪念医院临床检验信息管理系统（三级）等保测评项目”内容包括但不限于：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目服务内容 | 数量 | 单位 | 备注 |
| 1 | 网络安全等级保护测评服务 | 1 | 个 |  |

**4.1.2“中山大学孙逸仙纪念医院临床检验信息管理系统（三级）等保测评项目”服务内容和要求：**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | 等级 | 服务内容 |
| 1 | 临床检验信息管理系统 | 第三级 | 协助定级备案、等级保护差距测评、整改建议和指导、验收测评和报告编制 |

| 序号 | 服务类型 | 服务内容 |
| --- | --- | --- |
| 1 | 定级备案 | 对本次项目中信息系统情况进行调研，协助我院编写定级报告，办理等保备案。 |
| 2 | 差距测评实施过程及结果输出 | 实施过程：依据《信息安全技术 网络安全等级保护基本要求》实施等级测评，对物理机房、网络结构、服务器、信息系统等进行合规性检查，发现信息系統与安全保护等级要求之间的差距，并输出《信息系统安全问题清单》 |
| 3 | 漏洞扫描 | 1、定期使用专业的 Web 扫描工具，对本次项目中信息系统针对 WEB 服务进行强力攻击检测和缓冲区溢出检测等漏洞扫描；  2、根据漏洞扫描结果进行人工验证，用以验证工具扫描的漏洞结果的准确性，出具相应的《信息系统漏洞扫描报告》，提供安全加固建议； |
| 4 | 渗透测试 | 1、采用专业工具与人工的方法，通过模拟黑客可能使用的攻击方式和漏洞挖掘行为进行渗透测试，对目标信息系统的安全进行深入安全检测、评估。  2、根据漏洞扫描结果进行人工验证，用以验证工具扫描的漏洞结果的准确性，出具相应的《渗透测试报告》，提供安全加固建议； |
| 5 | 整改建议和指导 | 差距测评结束后，按照国家有关规定和标准规范要求，指导我院进行整改，以达到提高信息系统整体安全保护能力。 |
| 6 | 报告编制及提交 | 验收测评完成后，编写《网络安全等级保护等级测评报告》并将测评报告上传提交至国家网络安全等级保护主管部门，并通过国家信息安全等级保护主管部门的最终测评验收。 |

**4.2测评内容要求：**

为了保证我院的信息系统能够成功通过公安机关的备案与检查，差距测评应与验收测评采用完全一致的国家信息安全等级保护测评相关标准。具体测评内容要求如下：

信息系统安全等级保护测评应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，安全控制测评是信息系统整体安全测评的基础。

安全控制测评使用测评单元方式组织，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：安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个层面上的安全控制测评；安全管理测评包括：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的安全控制测评。

系统整体测评涉及到信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关。在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，分析评估安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性。

综合测评总结将在安全控制测评和系统整体测评两个方面的内容基础上进行，由此而获得信息系统对应安全等级保护级别的符合性结论。

**4.3项目交付成果包括：**

* 《信息系统安全等级保护备案证明》
* 《信息系统安全问题清单》
* 《网络安全等级保护等级测评报告》

**4.4人员要求**

投标方参与本项目的人员至少有3人，所有工程师必须取得网络安全等级测评师证书或信息安全等级测评师资质，在突发应急事件中能临时增加2名实施人员。

**4.5服务周期**

1、合同签订后30个工作日内成交供应商完成临床检验信息管理系统的差距测评工作，并提交《信息系统安全问题清单》及整改建议方案。

2、采购方在投标人完成《信息系统安全问题清单》之日算起60个工作日内完成信息安全整改后，成交供应商必须在30个工作日内完成相关信息系统验收测评和《网络安全等级保护等级测评报告》，并通过国家信息安全等级保护主管部门的最终测评验收。

**4.6服务方式**

**电话服务：**开通服务热线电话，并通过电话给采购人提供支持和帮助；

**远程服务：**开通网络交流服务，所有系统用户可以通过即时通讯方式与远程服务支持工程师进行交流，及时解决问题；

**现场服务：**远程服务无法解决问题时需要到场解决。

**4.7商务要求**

**技术支持服务：**一般性质的技术支持服务，例如电话、传真、E-MALL等方式提供技术咨询。

**远程支持**：对电话指导不能解决的问题，提供远程技术支持；如：QQ、其他远程工具。

**现场支持：**如果通过电话，远程等非现场的方式无法解决问题，需安排技术人员前往客户现场解决问题，提供上门支持。

**4.8付款方式说明**

合同生效后，成交人出具《网络安全等级保护等级测评报告》并提供给院方。采购人在收到成交人开具的等额有效正规发票后30日内采购人向成交人支付合同额的100%。

五、响应人资格要求

1、响应人必须为在中华人民共和国境内注册的,在经营范围内响应(如营业执照未记载经营范围，同时提供在全国企业信用信息公示系统查询的单位“登记信息”的打印页面）（加盖公章）。

2、本次采购允许分公司投标，须提供总公司营业执照及相关授权书。(响应人出具声明函)

3、单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一包号响应或者未划分包号的同一采购项目响应(响应人出具声明函) 。

4、在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）没有被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合规定条件的供应商(提供查询的打印页面并加盖公章）。

5、已登记报名并获取本次采购文件

六、评分标准

**评分总值最高为100分，评分分值（权重）分配如下：**

|  |  |  |  |
| --- | --- | --- | --- |
| 评分项目 | 技术服务评分 | 商务评分 | 价格评分 |
| 权重 | 30% | 50% | 20% |

**服务评审表：**

|  |  |  |
| --- | --- | --- |
| **一、商务部分（满分30分）** | | |
| **评价指标** | **分项分值** | **评分标准** |
| 企业技术实力综合体现 | 20分 | （1）供应商具备《计算机信息系统安全服务等级证》二级或二级以上证书。  （2）供应商具备风险评估类网络安全服务机构评定证书。  需提供有效期内的相关证书文件，复印件加盖公章，每项各10分，合计20分，不提供者不得分。 |
| 相关业绩 10分  【注：该项材料需提供项目合同关键页的复印件】 | | 提供近3年的等级保护测评项目相似业绩，每个2分，最高10分。（需提供合同关键盖章页并加盖公章） |
| **二、技术服务部分（满分50分）** | | |
| 技术服务方案 | 20分 | 1. 针对本项目的服务方案整体设计合理，需求贴近实际，得20分；  2. 针对本项目的服务方案整体设计比较完善合理，需求较贴近实际，得15分；  3. 针对本项目的服务方案整体设计水平中等合理，与实际情况有一定偏差，得10分；  4. 针对本项目的服务方案整体设计不甚完善合理，与实际情况差距较大，得5分；  5. 不提供者不得分。 |
| 响应人参与本项目技术队伍能力情况 | 20分 | 一、项目负责人具备以下能力资质：   1. 具有网络安全等级测评师证书或信息安全等级测评师证书中级或以上； 2. 具有注册信息安全专业人员证书，注册信息安全工程师（即（CISP-CISE）证书） 3. 具有注册信息安全专业人员证书，注册渗透测试工程师（即（CISP-PTE）证书） 4. 具有信息安全保障人员风险管理方向专业级认证证书（即（CISAW）证书）； 5. 具有项目管理专业人员资格认证证书（即PMP证书）；   以上具备一个得2分，满分10分。（需同时提供有效期内相应资质证书复印件及近三个月内任意一个月的社保证明，并加盖投标人公章。）。  二、技术队伍人员能力资质：  1.具有网络安全人员能力认证证书（即CPAC证书）；  2.具有网络安全等级测评师证书或信息安全等级测评师证书；  3.具有重要信息系统安全等级保护培训证书（即CIIP-A证书）；  4.具备网络安全相关专业的助理工程师职称证书；  5.具有计算机、网络、信息安全相关专业的硕士学历。  1）同一人具有多个证书的，按高级别的计算。  2）以上具备一个得2分，满分10分。同时提供有效期内的相应资质证书复印件及近三个月内任意一个月的社保证明，并加盖投标人公章。 |
| 测评工具技术 | 10分 | 根据投标人对测评工具要求中带“▲”的重要指标响应程度进行评价，满足“▲”条款的得1分/项，最高得10分。  注：投标人须提供对带“▲”参数指标进行点对点响应，并按其中要求提供厂家的书面确认（盖原厂公章），否则视为负偏离。 |
| **三、价格部分（满分20分）** | | |
| 价格  得分 | 20分 | 投标报价得分 = (评标基准价/投标报价)×20  评标基准价为满足招标文件要求且投标报价最低的投标报价，其价格分为满分。 |
| 总分 | **100分** |  |

七、测评工具要求

1、本项目在实施过程中所使用到的专业安全服务工具由投标人提供，响应供应商必须保证所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件可用性和可靠性。由此产生的一切责任由响应供应商负完全责任。（此费用已包含在本项目报价中，采购人不在另付费用。）

2、为确保响应供应商开展信息系统安全测评的服务质量，响应供应商必须采用符合国家标准的漏洞扫描设备辅助完成测评工作，投标时提供设备原厂授权书并加盖公章，参数要求如下：

| **指标项** | **指标要求** | | | |
| --- | --- | --- | --- | --- |
| **资**  **质** | 设备原厂商为国家网络与信息安全信息通报中心技术支持单位；  设备原厂商具有中国信息安全认证中心颁发的信息安全应急处理服务资质（一级）；  设备原厂商具有信息安全服务资质证书（安全工程类）；  ▲设备原厂商为国家信息安全漏洞库共享平台（CNVD）漏洞报送成员单位；  ▲设备原厂商为中国国家信息安全漏洞库（CNNVD）一级技术支撑单位；  设备原厂商具有信息安全等级保护安全建设服务机构能力评估合格证书；  设备原厂商通过严格质量管理体系认证并获得证书；  设备原厂商通过严格环境管理体系认证并获得证书；  设备原厂商产品开发、生产、服务等管理体系符合信息安全管理体系要求。 | | | |
|  | 任务管理 | | 支持手动创建重要信息系统检查、行业主管部门检查、备案单位检查、网站检查、自定义检查任务。 | |
| 支持检查任务并行检查及并行检查结果合并。 | |
| 支持任务的打开、另存为、修改、删除、关闭。 | |
| 支持与等级保护监察平台数据的上报和下发。 | |
| 检查任务 | | 检查范围：支持行业主管部门、备案单位、重要信息系统、网站四类检查对象的检查范围。支持基本情况、定级备案检查范围。 | |
| 检查内容：支持系统定级情况、岗位设置情况、安全审计情况检查内容。 | |
| 检查要点：支持检查对象检查内容具体检查指标项进行检查。 | |
| 检查结果录入类型：  单项判定：支持判定未检、不适用、0分、1分、2分、3分、4分、5分。  检查结果录入：支持录入检查结果记录。 | |
| 针对每个检查要点应提供相应的检查方法，检查结果判定依据相关检查知识，以便引导进行现场检查。 | |
| ▲支持对检查过程中具体检查对象（例如：主机、网络设备）进行调整功能，要求可以选择已有的检查对象或录入新的检查对象。 | |
| 支持将任务导出成检查模板，检查人员能够根据被检查单位情况，灵活分配各自的检查任务，支持导出检查表单提前让被检查单位人员对应进行自查，检查人员经现场检查核对无误之后，可以直接将检查表单数据导入到工具箱中。 | |
| 检查层面、检查内容、检查指标项支持保存为模板，模板可导入、导出。 | |
| 支持检查工具检查结果信息的展现功能。 | |
| 支持导出、导入检查项。 | |
| 支持手动填写测评概述，概述内容包括测评目的、测评依据、测评方法、测评结论、整体测评结果汇总。 | |
| 数据汇总 | | ▲支持一键导入功能，将检查工具集、检测结果自动导入到工具箱。 | |
| 支持手动导入工具检查结果到工具箱及关联任务检查对象。 | |
| 支持工具检查结果自动关联知识库。 | |
| 检查结果导出 | | 应采用国家商用密码管理办公室指定认可的国产商用密码算法对检查数据进行加密后导出，以确保检查数据的保密性。 | |
| 导出的检查结果应按照指定的接口规范导出。 | |
| 支持自动生成不同类型检查任务的检查报告，检查报告应包含不符合项的风险描述信息和安全评分。 | |
| 兼容性 | | 支持与工具箱监察管理系统数据的上报和下发。 | |
| **监察指标库升级维护** | 指标库要求 | | 监察指标库包含：控制点和要求项。 | |
| 指标库升级维护 | | 提供监察知识库升级功能，可以对监察知识库进行手动更新。 | |
| 应提供升级检测和提醒功能。 | |
| 监察知识库升级应有日志记录。 | |
| **监**  **察**  **知**  **识**  **库**  **升**  **级**  **维**  **护** | 知识库要求 | | 知识库内容必须覆盖所有检查指标。 | |
| 知识库内容应包含检查指标的检查方法、检查结果判定依据和不符合项的风险提示。 | |
| 知识库可以依据网络安全的标准和分析模型，对检查工具的检查结果进行自动分析，给出相应的检查结果记录。 | |
| ▲知识库可以针对不同类型的检查任务，对检查结果进行自动分析和安全评分，自动生成相应的检查结果记录。 | |
| 知识库内容应描述正确，并具有明确的引导作用。 | |
| ▲知识库升级维护 | | 知识库内容必须覆盖所有检查指标。 | |
| 知识库内容应包含检查指标的检查方法、检查结果判定依据和不符合项的风险提示。 | |
| 知识库可以依据网络安全的标准和分析模型，对检查工具的检查结果进行自动分析，给出相应的检查结果记录。 | |
| **工**  **具**  **管**  **理** | 升级管理 | | 技术支持网站应提供检查工具升级提示功能，当检查工具有更新时，采购人可以进行检查工具的升级操作。 | |
| 检查工具升级操作应在工具箱留有日志记录。 | |
| 结果管理 | | 应提供结果分析，依据内置知识库自动对工具检查结果进行分析，自动判别相应检查指标的检查结果。 | |
| 结果导入操作应留有日志记录。 | |
| 风险提示 | | 所有检查工具启动时，默认都会进行风险提示，支持通过配置是否下次启用风险提示。 | |
| **系**  **统**  **管**  **理** | 配置管理 | | 配置管理应对工具箱监察管理系统参数进行配置:  支持系统最大登录次数设置；  支持锁定用户时间设置；  支持软件自动锁定功能；  支持口令强度策略设置。 | |
| 用户管理 | | 支持对采购人账户进行管理，支持管理员、操作员、审计员角色账户增加、口令修改；  支持对账户新增、修改、删除；  内置角色默认权限；  ▲支持用户密码找回功能。 | |
| 日志管理 | | 可查看操作日期、操作用户、操作对象日志记录。 | |
| 提供日志筛选功能。 | |
| 提供日志导出备份功能。 | |
| 系统升级 | | 应提供升级功能，升级操作应简单。 | |
| 技术支持网站应提供升级提示功能。 | |
| 设备厂商应定期发布离线升级包，支持手动导入升级。 | |
| 升级操作应留存日志记录。 | |
| 工具箱监察管理系统具有登录尝试失败锁定功能。 | |
| 访问控制 | | 应依据安全策略严格控制用户文件，数据表重要信息资源的操作。 | |
| 应确保不提供已注销用户的任何信息，包括鉴别信息。 | |
| 安全审计 | | 指标库、知识库、监察工具升级操作。 | |
| 用户登录和注销事件。 | |
| 数据导入、导出事件。 | |
| 通信安全 | | 应采取措施确保导入和导出数据的完整性。 | |
| U盘安全检查工具向工具箱提交的检查结果数据的完整性。 | |
| 数据安全 | | 采用国家商用密码管理办公室指定认可的国产商用密码算法对以下数据进行加密。 | |
| **等级保护工具箱配备U盘安全检查工具集** | | | | |
| Windows  主  机  安  全  配  置  检  查  工  具 | | ▲支持检查主机系统配置信息，包括：计算机名、用户名、操作系统、版本、内存大小、磁盘大小、系统路径、共享目录；  支持检查USB接入设备信息；  支持检查Internet Explorer、Chrome、Firefox等浏览器上网记录、Cookie记录；  支持检查主机硬件信息，包括：CPU信息、主板信息、内存信息、显卡信息、硬盘信息、网卡信息；  支持检查主机开机自启动项程序；  查看主机上已经启动的可能有风险的服务程序，包括：如Task Scheduler、Print Spooler、Remote Registry等服务；  支持检查账户安全策略信息，包含口令长度、复杂度、定期更换、登录失败、锁定次数等；  对系统账户进行检查，可智能识别系统影子账户（隐藏账户）；  查看系统是否开启系统审核、系统登录事件、审核账户登录事件等安全审计策略；  运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；  支持在线更新、离线升级。 | | |
| 主  机  病  毒  检  查  工  具 | | 支持对操作系统的关键机制，如系统服务、内存、注册表、启动进程；检测操作系统的安全模型，包括访问控制、特权和审计；反馈系统安全配置、文件访问，驱动、引导系统深度进行检查；  检查流氓软件、蠕虫病毒、其它恶意程序等；  支持快速扫描、全盘扫描、自定义目录扫描；  运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；  支持在线更新、离线升级。 | | |
| 主  机  木  马  检  查  工  具 | | 支持检查系统中的木马程序、Rootkit、间谍程序等；  提取操作系统的关键机制，如系统服务、内存、注册表、启动进程；检测操作系统的安全模型，包括访问控制、特权和审计；反馈系统安全配置、文件访问，驱动、引导等系统深度信息；  支持快速扫描、全盘扫描、自定义目录扫描；  运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；  支持在线更新、离线升级。 | | |
| 网站  恶意  代码  检查  工具 | | 支持asp、asa、cer、jsp、jspx、php等文件格式检查；  支持自定义文件后缀格式；  支持异性、变异WEBSHELL后门代码检查；  支持关键恶意特征码定位；  支持快速扫描、全盘扫描、自定义路径扫描；  支持自定义扫描策略、可扩充恶意特征码；  支持自定义文件大小扫描；  运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；  支持在线更新、离线升级。 | | |
| **等级保护工具箱配备在线检查工具集** | | | | |
| Linux  主  机  安  全  配  置  检  查  工  具 | | 支持检查主机系统配置信息，包括：计算机名、用户名、操作系统、版本、内存等；  支持检查系统安全补丁升级情况；  支持检查不必要的服务和端口（如TELNET、SSH、SNMP、HTTP等）；  支持检查账户安全策略信息，包含口令长度、复杂度、定期更换、登录失败、锁定次数等；  支持SNMP、SSH服务、版本信息检查；  支持检查安全审计配置情况、包含事件类型；  支持检查屏幕保护恢复时间；  支持RedHat、Ubuntu、Debian、Fedora、Suse、Centos操作系统类型；  支持在线更新、离线升级。 | | |
| 网  络  及  安  全  设  备  配  置  检  查  工  具 | | 支持对华三、思科、华为路由器、交换机通用系列网络设备安全分析检查；  支持对天融信、网神、启明星辰、网御星云、Juniper防火墙通用系列设置安全分析检查；  支持检查账户安全策略信息，包含口令长度、复杂度、定期更换、登录失败、锁定次数等；  支持检查安全审计策略，包含事件类型、SYSLOG服务器；  支持检查不必要的服务和端口（如TELNET、FTP、SNMP、HTTP、Sendmail）；  支持SNMP、SSH服务、版本信息检查；  运行环境支持Windows XP、 Windows7、 Windows Server 2003、Windows Server 2008等操作系统类型；  支持在线更新、离线升级。 | | |
| 弱  口  令  检  查  工  具 | | 应用服务支持类型：SSH、SMB、TELNET、FTP、RDP、SQL Server、Oracle、MySQL、POP3等协议应用程序弱口令检查；  支持自定义账户、口令字典；  支持自定义应用协议TCP端口；  内置常见弱口令字典（如口令为：123456、88888888、12345等）；  支持本地、远程主机及多协议同时检查；  运行环境支持Windows XP、Windows7、Windows Server 2003、Windows Server 2008等操作系统类型；  支持在线更新、离线更新。 | | |
| 数  据  库  安  全  检  查  工  具 | | 支持IPV6地址检查；  支持对数据库弱点、不安全配置、安全策略、补丁升级、弱口令安全检查；  支持主流Oracle、SQL Server、DB2、Informix、MySQL、Sybase数据库类型；  支持授权扫描，使用具有DBA权限的数据库用户，执行选定的安全策略实现对目标数据库检查；  非授权扫描,采购人在没有授权的情况下（即：不需要数据库用户名、密码），根据选定的安全策略对目标数据库进行的检测；  策略自定义,提供扫描策略可自定义模式，操作者可以灵活选择默认策略的同时也可以自定义添加策略；  支持在线更新、离线升级。 | | |
| 网  站  安  全  检  查  工  具 | | 支持WEB 2.0，支持各类JavaScript脚本解析；  支持WAP站点扫描；  支持FLASH解析；  支持基于HTTPS应用系统的扫描；  支持实时存储扫描项目文件、断点续扫；  支持ERP等复杂的Web应用系统扫描；  支持易通、织梦、、Discuz、Ecshop、易思、方欣、大汉、科讯、通达OA、PHPCMS、PHP168、PHPCMS2008、phpcms v9、SHOPEX、SiteServer CMS、TRS、 Nginx代码执行、Spring代码执行、亿邮邮件系统命令执行等国内、国外知名WEB应用程序漏洞扫描；  支持JSP、CGI、ASP、.NET等类型动态页面；  支持IP地址、域名地址、批量网站扫描；  支持无人值守模式下的全自动扫描；  支持HTTP 1.0和1.1标准的Web应用系统；  支持Oracle、SQL Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Access、Ingres等后台数据库类型；  支持对SQL注入、XSS跨站脚本、伪造跨站点请求、网页木马、隐藏字段、表单绕过、AJAX注入、弱配置、敏感信息泄漏、HI－JACK攻击、弱口令、Xpath注入、LDAP注入、框架注入、操作系统命令注入、Flash源代码泄漏、Flash跨域攻击、Cookies注入、敏感文件、第三方软件、其他各类CGI等漏洞进行扫描；  支持在线更新、离线升级。 | | |
| 系  统  漏  洞  检  查  工  具 | | 支持对Microsoft Windows XP/2003/Vista/2008/7、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD等操作系统进行漏洞扫描；  支持对Web、FTP、电子邮件等应用系统以及Office、Apache等常用软件进行漏洞扫描；  支持对网络设备进行漏洞扫描；  支持多种扫描策略，包括常规完全扫描、高强度完全扫描、高强度扫描、中强度扫描、低强度扫描、Windows主机扫描、类Unix主机扫描等扫描策略，方便采购人快速选择；  支持自动统计总体漏洞数量、统计不同操作系统类型的主机数量、统计所有开发端口、可用帐户、列出每一个漏洞所存在的主机、详细描述与修补建议。漏洞详细描述包括：漏洞名称、详述、修补方案、CVE/Bugtraq/CNCVE/CNNVD编号、CVSS评分等；  支持在线、离线更新；  支持导出Word、PDF常见格式报表。 | | |
| 运行安全 | | 不得改变检查对象当前配置； | | |
| 不影响检查对象正常运行； | | |
| 不影响检查对象所属网络正常运行； | | |
| 不在检查对象中遗留痕迹。 | | |
| 数据安全 | | 存储安全 | | U盘检查工具应对所有检查数据采用国产加密算法进行加密，防止监察数据被非法读取。 |
| 痕迹安全 | | U盘检查工具应对所有检查数据采取痕迹消除措施，以防止信息泄露。 |
| **安全性** | | 支持等级保护检查过程的采购人信息的安全保护，所有数据以加密方式存储传输。 | | |
| U盘自身具有病毒、木马程序免疫功能，防止病毒、木马程序感染U盘内文件。 | | |
| ▲**报表中心** | | 支持生成信息系统检查任务报告、行业主管部门检查任务报告、备案单位任务报告、网站安全检查任务报告、自建检查任务报告；  支持检查任务汇总、预览；  支持对信息系统检查任务检查结果进行得分汇总，并以饼形图的方式进行展示；  支持生成等保测评报告、工具检测类型报表，等保测评报告采用最新的测评报告2015模板；  支持WORD、HTML格式报表导出；  支持下载自查表。 | | |
| **辅助**  **功能** | | ▲工具箱监察管理系统和U盘安全检查工具应提供软件截图工具，便于实时保存系统关键界面信息。 | | |

八、采购流程

1、响应人必须为在中华人民共和国境内注册的，具有独立法人资格的合法企业,在经营范围内响应(如营业执照未记载经营范围，同时提供在全国企业信用信息公示系统查询的单位“登记信息”的打印页面）（加盖公章）。

2、本次采购只接受独立法人响应，不接受任何形式联合体响应(响应人出具声明函)。

3、单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一包号响应或者未划分包号的同一采购项目响应(响应人出具声明函) 。

4、在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）没有被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合规定条件的供应商(提供查询的打印页面并加盖公章）。

5、已登记报名并获取本次采购文件(具体方式详见第五条)。

五、符合资格的响应人应当在2023年6月12日至2023年6月16日每天（节假日除外）9:00至11:30，14:30至17:00(北京时间) 到广州市越秀区沿江西路107号中山大学孙逸仙纪念医院岭南楼1A层智慧医院建设部登记报名并领取项目相关资料。

1、登记报名时，提供第四点中要求的证明文件；

2、资格审核通过后的供应商按上述要求以及采购方提供的用户需求相关资料写报价文件，并提供相关资质证明材料，在响应截止日期前将报价文件密封（一正五副），并注明报价供应商名称、联系人、联系电话盖公章后交至中山大学孙逸仙纪念医院岭南楼1A层智慧医院建设部；

3、符合要求的报价文件交由本项目采购委员会讨论，按院内采购、议价程序等相关规定，推荐成交候选单位；

4、将推荐的成交候选单位相关资料上报医院按程序审批，审批通过后，将结果挂网公示，公示期结束后与成交人签订合同。

六、开标时间、地点：

1、响应截止时间（北京时间）：2023年6月19日14时30分00秒(注14时30分开始受理纸质响应文件)

2、响应文件送达地点（响应地址）：中山大学孙逸仙纪念医院岭南楼1A层智慧医院建设部（广州市越秀区沿江西路107号）（纸质响应文件应由响应人授权代表亲自送达响应地址，采购方将不接受其他形式递交的响应文件）

3、开标时间（北京时间）：2023年6月19日15时00分00秒

4、开标地点：中山大学孙逸仙纪念医院岭南楼1A层智慧医院建设部（广州市沿江西路107号）

5、采购人联系方式

联系人：许先生

电话：020-81332305

联系地址：广州市沿江西路107号

邮编：510120

 中山大学孙逸仙纪念医院

2023年6月12日