等保测评服务公告

一、供应商资格要求

（一）具备《中华人民共和国政府采购法》第二十二条的相关规定：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）法律、行政法规规定的其他条件。

（二）其他类似效力要求

（1）本项目参加政府采购活动的供应商及现任法定代表人(非法人机构则为主要负责人)不得具有行贿犯罪记录；

（2）供应商在采购公告发布之日前未被列入“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站(www.ccgp.gov.cn)中任一网站的失信被执行人名单或重大税收违法案件当事人名单或政府采购严重违法失信行为记录名单；

（3）法定代表人授权书原件；

（4）供应商与其他供应商之间，单位负责人不为同一人而且不存在直接控股、管理关系。

（5）本项目不接受联合体响应。

（三）本项目的特定资格要求

具有公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书。

二、项目概况

1、项目背景

为了落实公安部、医疗行业信息系统安全等级保护等文件要求，进一步增强医院信息系统安全防护能力，确保医院信息系统安全稳定运行，特开展此次等级保护测评工作, 防止因系统安全事件引发安全事故依据《信息系统安全等级保护基本要求》（GB/T 22239-2008）、《信息安全等级保护管理办法》（公通字[2007]43号）和《中华人民共和国网络安全法》等标准规范，特开展此次等级保护测评工作。

2、项目目标

依据国家和行业信息安全的相关标准，全面了解和掌握医院信息系统现有安全状况，找出其与《信息系统安全等级保护基本要求》对应级别的差距，及时发现系统存在的安全问题，针对等级保护测评及德阳市旌阳区中医院信息系统安全评估中发现的各种安全风险，测评项目组提出适宜的安全整改建议，最终提交该系统等级保护测评报告。

三、服务内容及范围

1、等级保护测评服务内容：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 信息系统名称 | 定级 | 服务描述 |
| 1 | 肿瘤医院信息系统 | 三级 | 对肿瘤医院信息系统进行等级保护测评服务，出具测评报告。 |

参照《GBT22239-2019 网络安全等级保护基本要求》和《GB/T28448-2019 网络安全等级保护测评要求》等标准规范要求，开展信息系统等级保护测评及整改工作。测评及整改范围为项目目标所涉及的基础网络环境、主机层面、应用层、数据库层及相关安全辅助设备与管理制度。服务目标为项目目标最终通过公安部门及相关部门的等级保护检查要求。

2、标准和规范

《GB 17859—1999 计算机信息系统 安全等级保护划分准则》

《GBT 20269—2006 信息安全技术 信息系统安全管理要求》

《GBT 20271—2006 信息安全技术 网络系统安全通用技术要求》

《GBT 20272—2006 信息安全技术 操作系统安全技术要求》

《GBT 20273—2006 信息安全技术 数据库管理系统安全技术要求》

《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》

《GBT 22239—2019 信息安全技术 网络安全等级保护基本要求》

《GB/T25070—2019 信息安全技术 网络安全等级保护设计技术要求》

《GB/T28448—2019 信息安全技术 网络安全等级保护测评要求》

《信息安全等级保护备案实施细则》（公信安[2007]1360 号）

《GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南》

《[GB-T 28449-2018](http://www.baidu.com/link?url=jrwCn0k5g-pjfPjj8ssoA8Zc8cGAmY6uAgqr_NWkuGJBmWRWjx-u7Cavb-A5H84m1zuEktrJPPYlpQ6pW78BxcZXjkBvAEsg8de6Wgjswey" \t "https://www.baidu.com/_blank) 信息安全技术 网络安全等级保护测评过程指南》

《公通字[2007]43号 信息安全等级保护管理办法》

3、本项目实施方案设计与具体实施必须满足以下原则：

1. 保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标方的行为。
2. 标准性原则：测评方案的设计与实施应依据国家信息系统安全等级保护的相关标准进行。
3. 规范性原则：投标方的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。
4. 可控性原则：项目安排工作进度要跟上进度表的安排，保证工作的可控性。
5. 最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。
6. 整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

4、整体要求

1. 投标人应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。
2. 投标人应完成信息系统定级报告及定级材料的准备、整理，完成信息系统去公安机关的备案工作。
3. 投标人应详细描述测评人员的组成、资质。
4. 本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件由投标人推荐，经招标人确认后由投标人提供并在信息系统等级保护测评中使用。
5. 信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。
6. 投标人应提供本次信息系统安全等级保护整改的整体实施方案，包括项目时间安排、阶段性文档提交等，并负责实施整改。

5、专用工具要求

本项目涉及工程实施和验收测试所需的工具，由投标方负责提供。用于测评的工具主要包括服务器安全测评工具、网络设备安全测评工具、终端计算机安全测评工具、网站等应用系统安全测评工具等。在使用前，应对工具进行测评，如果需要则对工具进行软件或代码升级。

6、安全管理要求

为做好全过程的安全保密工作，在等级保护测评前、中、后三个阶段都要做好安全保密工作。

* + 1. **A、等级保护测评前**

1. 对等级保护测评人员要进行安全保密教育，制定安全保密措施；
2. 签订安全保密协议。
   * 1. **B、等级保护测评中**
3. 对被测单位的性质、机房物理位置、网络与系统、应用与服务、资料与数据、人员与管理等方面的信息进行严格的安全保密管理；
4. 等级保护测评工具应经过严格测试和检验，确保不对被测评系统造成损失，工作结束后不驻留任何程序；
5. 对被测单位信息系统的信息资产、发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围；
6. 对测评设备、介质进行严格的保密管理；
7. 工作过程中对人员要实施封闭式集中管理；
8. 对进场人员遵守被测单位的相关管理规定。
   * 1. **C、等级保护测评后**
9. 认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏；
10. 现场工作结束后，按被测单位的要求及时还原系统，确保系统中不遗留任何代码或可执行程序；
11. 在其他风险测评任务或宣传材料中不涉及被测单位的秘密、敏感情况。

7、文档要求

文档或报告的编写应完整清晰、用词规范、简明扼要，指出的问题应明确合理、符合逻辑、且有证据，出具的结论应公正客观、实事求是，提出的建议应符合国家标准规范、富有建设性和可操作性。

8、测评公司综合实力要求

投标方应提供测评成员的技术背景资历资料、从事测评的经验、人力资源的组织方式、项目实施的管理方式、项目成员的角色和责任。

9、售后服务

投标方承诺能按要求实现本技术规范规定的所有条款及功能要求，配合完成相关政府部门的信息安全等级保护相关（登记、整改等）工作要求。

四、项目实施内容与要求

1、项目定级备案

投标方应梳理现有的信息系统，严格按照《GB/T 22240-2020信息安全技术 网络安全等级保护定级指南》的要求，对信息系统的级别进行划定。完成信息系统定级报告及定级材料的准备、整理，完成信息系统去公安机关的备案工作。

2、项目测评内容

根据国家等级保护相关标准《GBT22239-2019 网络安全等级保护基本要求》，对重要信息系统等级保护测评项目应包括以下内容：

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、安全管理中心等五个方面的安全测评；

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、安全运维管理等五个方面的安全测评。

服务内容：

1. 协助开展系统和重要信息系统的自查自评工作，对存在的风险隐患和安全问题及时提供有针对性的安全整改建议，保障整改措施的落实，完成重要信息系统的定级、备案等相关工作；
2. 依据《网络安全等级保护基本要求》，从安全技术和管理两个方面共十个层面对信息系统进行等级测评，出具等级测评报告；
3. 针对信息系统等保测评实施过程中发现的安全隐患和薄弱环节，提供安全建设整改和安全加固方面的咨询。
4. 提供安全服务，及时发现信息系统中存在安全隐患和威胁，进一步开展安全建设整改工作，及时、有效、正确的预防和阻止各种黑客攻击。职责清晰，能快速及时的帮助客户处理网站安全事件。

|  |  |  |
| --- | --- | --- |
| **项目** | **服务内容** | **工作描述** |
| 等级测评 | 项目准备及现场调研 | 协助对信息系统物理环境、网络、终端、数据、安全管理等进行调研。 |
| 信息系统定级、备案 | 疏理信息系统定级工作，完成信息系统定级报告及定级材料的准备；  整理、补充信息系统备案所有相关的文档，完成相应信息系统等级保护备案工作。 |
| 信息系统差距分析 | 对定级的信息系统，依照《网络安全等级保护基本要求》进行逐个对照，分析信息系统安全情况与等级保护基本要求的差距，完成信息系统等级保护差距分析报告。 |
| 等级保护安全整改 | 协助落实相关的等级保护建设整改工作，等级保护整改实施具体内容包括安全管理制度修订、安全技术整改、形成安全配置基线、辅助进行安全增强配置和调试工作、实施等保相关培训、安全风险管理工作落实等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。 |
| 等级保护测评 | 参照《GBT22239-2019 网络安全等级保护基本要求》和《GB/T28448-2019 网络安全等级保护测评要求》等标准规范要求，对信息系统开展信息系统等级保护测评工作。 |
| 成果 | 服务目标为：协助用户取得公安机关备案证明；通过公安部门的等级保护检查，输出《信息系统等级保护测评报告》。 |

3、测评要求

（1）安全物理环境

物理安全测评是对信息系统的机房和办公场所的物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等方面的安全状况。

（2）安全通信网络

网络安全测评是对信息系统的网络系统安全防护情况进行测评，包括网络结构安全、网络访问控制、网络安全审计、网络边界完整性测评、网络入侵防范、网络恶意代码防范、网络设备防护等方面的安全状况。

（3）安全区域边界

安全区域边界是对信息系统的边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面的安全状况。

（4）安全计算环境

安全计算环境是对信息系统的身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等方面的安全状况。

（5）安全管理中心

安全管理中心是对信息系统的系统管理、审计管理、安全管理、集中管控进行测评。

（6）安全管理制度

安全管理制度测评是对信息系统的安全策略、管理制度、制定和发布、评审和修订等情况进行测评。

（7）安全管理机构

安全管理机构测评是对信息系统的岗位设置、人员配备、授权与审批、沟通和合作、审核和检查等情况进行测评。

（8）安全管理人员

人员安全管理测评是对信息系统相关内部人员的人员录用、人员离岗安全意识教育和培训、外部人员访问管理等情况进行测评。

（9）安全建设管理

系统建设管理测评是对信息系统建设过程中的、测试验收、系统交付、等级测评服务供应商管理等情况进行测评。

（10）安全运维管理

系统运维管理测评是对信息系统运行维护过程中的环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等情况进行测评。

4、测评风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责信息安全测评过程中的安全保密管理工作，对测评活动、测评人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

安全测评工作中可能出现的安全风险点，按照检测对象周密制定测评方法，根据被测评对象的不同采取相应的风险控制手段。不限于以下方法：

（1）操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

（2）操作时间控制

* + 1. 对测评直接影响系统工作时，尽可能避开敏感时期。

（3）人员与数据管理

* + 1. 必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测评单位之间应签署长期保密协议，测评人员与被测评单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

（4）制定应急预案

* + 1. 根据测评范围界定的系统情况，在实施前制定应急预案。

（5）关键业务系统风险控制

* + 1. 对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、测评和简单测试的方式进行。

（6）优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

（7）数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止测评过程中对设备与主机的损伤影响业务系统的正常运行。

* 1. 5、整改实施内容

投标方严格按照差距分析报告内容，落实相关的等级保护建设整改工作，等级保护整改实施具体内容包括安全管理制度修订、安全技术整改、形成安全配置基线、进行安全增强配置和调试工作、实施等保相关培训、安全风险管理工作落实等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。

* 1. 6、汇总项目材料并验收

投标方对整改后的内容进行最终确认，并汇总信息系统等级保护测评报告，完成公安机关的材料报备，取得信息系统备案证明。

投标方汇总等级保护测评阶段性文档（不限于定级备案材料、差距分析报告、整改实施方案、测评报告、备案证明等），保证通过评审及验收。

7、互联网资产服务

基于梳理好的互联网资产，提供一年不少于2次的检测服务，包含WEB漏洞、主机漏洞、安全事件、文件泄露、可用性、弱口令、高危服务等。供应商将检测结果形成纸质的检测报告，加盖供应商公章后递交给采购人。同时将梳理好的互联网资产根据算法自动评估出互联网资产风险值，在每次检测服务完成后，通过平台展示资产风险情况，提供风险值变化趋势分析及资产风险值TOP排名，服务单位可通过微信公众号进行安全事件、域名有效期、证书有效期的推送。（供应商提供推送服务的功能截图，加盖供应商公章。）

支持展示当前最新的检测结果中新增WEB/主机漏洞和本次被修复的WEB/主机漏洞、新增弱口令和本次被修复的弱口令；支持展示客户当前环境的主机中存在的高危端口服务的检测结果；支持展示用户安全事件发现的变化趋势。（提供此项功能性截图证明文件并加盖供应商公章）

8、渗透测试服务

（1）对测评的业务系统进行渗透测试，渗透测试应至少包括但不限于WEB 应用系统渗透、主机操作系统渗透、数据库系统渗透。

（2）渗透测试方法需模拟黑客入侵思路与技术手段，以人工渗透为主，工具为辅，工具包括但不局限于：信息收集工具、漏洞扫描工具、口令猜测工具、脚本测试工具等。

（3）渗透测试大项包括但不局限于：配置管理、身份鉴别、认证授权、会话管理、输入验证错误处理、业务逻辑等。

（4）渗透测试方法包括但不局限于：信息收集、端口扫描、公网登录口的口令猜测、远程溢出、本地溢出、脚本测试、目标系统权限获取等。

（5）渗透服务后需提交渗透测试报告，需对业务系统中存在的安全隐患以及专业的漏洞风险提供专业的处置建议，报告内容应包括但不限于：信息系统整体安全状况综述、具体发现的漏洞、漏洞产生的原理、漏洞危险程度、测试用例、修复建议等。

（6）所使用漏洞扫描工具支持检测的漏洞数大于300000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准。（须提供证明截图）

（7）所使用漏洞扫描工具支持对C/C++/Python/Java/Php/go等语言的代码解析，语言的词法、语法分析；内置缺陷模板和缺陷规则，并支持自定义。（须提供功能截图）

（8）供应商为本项目提供一名渗透测试技术人员，具有注册渗透测试工程师（CISP-PTE）、CNVD原创漏洞证明。（提供有效证书/证明材料复印件）