

一、项目概述

依据《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)、《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号)、《关于信息安全等级保护工作的实施意见》(公通字[2004]66 号)、《信息安全等级保护管理办法》(公通字[2007]43 号)、《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护定级指南》、《计算机信息系统安全保护等级划分准则》等相关规定和标准,对采购人网络安全和信息系统提供配套服务。

配套服务包括网络安全等级保护测评、商用密码应用安全性评估、软件测试服务、网络安全服务等。涉及业务系统包含 10 个二级业务系统,2 个三级业务系统。

本项目分为三包。第一包:网络安全等级保护测评及商用密码应用安全性评估。第二包:软件测试服务。第三包:网络安全服务

二、项目内容及范围

1. 第一包:网络安全等级保护测评及商用密码应用安全性评估。涉及 10 个二级业务系统和 2 个三级业务系统。

序号	业务系统名称	数量	网络安全等级保护测评	商用密码应用安全性评估
1	二级业务系统	10 个	√	×
2	三级业务系统	2 个	√	√

2. 第二包:软件测试服务。涉及 12 个业务系统。

序号	业务系统名称	数量	软件测试服务
1	二级业务系统	10 个	√
2	三级业务系统	2 个	√

3. 第三包:网络安全服务。包含网络安全服务 1 年。

三、第一包:网络安全等级保护测评及商用密码应用安全性评估

1. 总体要求

依据《中华人民共和国网络安全法》、《内蒙古自治区计算机信息系统安全保护办法》等法律法规,按照《GB / T 22239-2019 网络安全等级保护基本要求》等国家及行业标准完成网络安全等级保护测评、商用密码应用安全性评估等工作。

网络安全等级保护测评、商用密码应用安全性评估检出的问题，投标人提出整改建议，由采购人责成内部或相关承建厂商落实整改。整改期间，投标人进行不限次数的测评、评估。

2. 网络安全等级保护测评

(1) 测评技术主要标准

《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》。

(2) 测评项要求

依据国家标准，三级系统测评项目不少于 211 项，二级系统测评项目不少于 135 项，本次对 12 个业务系统进行单次测评，其中二级业务系统 10 个，三级业务系统 2 个，投标方应具备在测评工作中有关电子数据分析、鉴定、取证的能力。

① 测评内容：

安全要求
<input checked="" type="checkbox"/> 安全通用要求

安全要求	安全分类
<input checked="" type="checkbox"/> 安全通用要求	<input checked="" type="checkbox"/> 安全物理环境 <input checked="" type="checkbox"/> 安全通信网络 <input checked="" type="checkbox"/> 安全区域边界 <input checked="" type="checkbox"/> 安全计算环境 <input checked="" type="checkbox"/> 安全管理中心 <input checked="" type="checkbox"/> 安全管理制度 <input checked="" type="checkbox"/> 安全管理机构 <input checked="" type="checkbox"/> 安全管理人员 <input checked="" type="checkbox"/> 安全建设管理 <input checked="" type="checkbox"/> 安全运维管理

② 三级系统测评指标

安全通用要求-安全物理环境	
测评控制点名称	三级测评点

物理位置选择	2
物理访问控制	1
防盗窃和防破坏	3
防雷击	2
防火	3
防水和防潮	3
防静电	2
温湿度控制	1
电力供应	3
电磁防护	2
合计	22

安全通用要求-安全通信网络	
测评组件名称	三级测评点
网络架构	5
通信传输	2
可信验证	1
合计	8

安全通用要求-安全区域边界	
测评组件名称	三级测评点
边界防护	4
访问控制	5
入侵防范	4
恶意代码和垃圾邮件防范	2
安全审计	4
可信验证	1
合计	20

安全通用要求-安全计算环境	
测评组件名称	三级测评点
身份鉴别	4
访问控制	7

安全审计	4
入侵防范	6
恶意代码防范	1
可信验证	1
数据完整性	2
数据保密性	2
数据备份恢复	3
剩余信息保护	2
个人信息保护	2
合计	34

安全通用要求-安全管理中心	
测评组件名称	三级测评点
系统管理	2
审计管理	2
安全管理	2
集中管控	6
合计	12

安全通用要求-安全管理制度	
测评组件名称	三级测评点
安全策略	1
管理制度	3
制定和发布	2
评审和修订	1
合计	7

安全通用要求-安全管理机构	
测评组件名称	三级测评点
岗位设置	3
人员配备	2
授权和审批	3
沟通和合作	3

审核和检查	3
合计	14

安全通用要求-安全管理人员	
测评组件名称	三级测评点
人员录用	3
人员离岗	2
安全意识教育和培训	3
外部人员访问管理	4
合计	12

安全通用要求- 安全建设管理	
测评组件名称	三级测评点
定级和备案	4
安全方案设计	3
产品采购和使用	3
自行软件开发	7
外包软件开发	3
工程实施	3
测试验收	2
系统交付	3
等级测评	3
服务供应商选择	3
合计	34

安全通用要求- 安全运维管理	
测评组件名称	三级测评点
环境管理	3
资产管理	3
介质管理	2
设备维护管理	4
漏洞和风险管理	2
网络和系统安全管理	10

恶意代码防范管理	2
配置管理	2
密码管理	2
变更管理	3
备份与恢复管理	3
安全事件处置	4
应急预案管理	4
外包运维管理	4
合计	48

③ 二级系统测评指标

安全通用要求-安全物理环境	
测评控制点名称	二级测评点
物理位置选择	2
物理访问控制	1
防盗窃和防破坏	2
防雷击	1
防火	2
防水和防潮	2
防静电	1
温湿度控制	1
电力供应	2
电磁防护	1
合计	15

安全通用要求-安全通信网络	
测评组件名称	二级测评点
网络架构	2
通信传输	1
可信验证	1
合计	4

安全通用要求-安全区域边界	
测评组件名称	二级测评点

边界防护	1
访问控制	4
入侵防范	1
恶意代码和垃圾邮件防范	1
安全审计	3
可信验证	1
合计	11

安全通用要求-安全计算环境	
测评组件名称	二级测评点
身份鉴别	3
访问控制	4
安全审计	3
入侵防范	5
恶意代码防范	1
可信验证	1
数据完整性	1
数据备份恢复	2
剩余信息保护	1
个人信息保护	2
合计	23

安全通用要求-安全管理中心	
测评组件名称	二级测评点
系统管理	2
审计管理	2
合计	4

安全通用要求- 安全管理制度	
测评组件名称	二级测评点
安全策略	1
管理制度	2
制定和发布	2

评审和修订	1
合计	6

安全通用要求- 安全管理机构	
测评组件名称	二级测评点
岗位设置	2
人员配备	1
授权和审批	2
沟通和合作	3
审核和检查	1
合计	9

安全通用要求-安全管理人员	
测评组件名称	二级测评点
人员录用	2
人员离岗	1
安全意识教育和培训	1
外部人员访问管理	3
合计	7

安全通用要求- 安全建设管理	
测评组件名称	二级测评点
定级和备案	4
安全方案设计	3
产品采购和使用	2
自行软件开发	2
外包软件开发	2
工程实施	2
测试验收	2
系统交付	3
等级测评	3
服务供应商选择	2
合计	25

安全通用要求- 安全运维管理	
测评组件名称	二级测评点
环境管理	3
资产管理	1
介质管理	2
设备维护管理	2
漏洞和风险管理	1
网络和系统安全管理	5
恶意代码防范管理	3
配置管理	1
密码管理	2
变更管理	1
备份与恢复管理	3
安全事件处置	3
应急预案管理	2
外包运维管理	2
合计	31

3. 商用密码应用安全性评估

依据的主要标准：GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》、《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化规则》

评估指标要求：依据标准，三级系统评估指标不少于 41 项，本次对 2 个三级业务系统进行评估。详细评估指标如下：

（1）物理和环境安全

评估指标
身份鉴别
电子门禁记录数据存储完整性
视频监控记录数据存储完整性

（2）网络和通信安全

评估指标
身份鉴别

通信数据完整性
通信过程中重要数据的机密性
网络边界访问控制信息的完整性
安全接入认证

(3) 设备和计算安全

评估指标
身份鉴别
远程管理通道安全
系统资源访问控制信息完整性
重要信息资源安全标记完整性
日志记录完整性
重要可执行程序完整性、重要可执行程序来源真实性

(4) 应用和数据安全

评估指标
身份鉴别
访问控制信息完整性
重要信息资源安全标记完整性
重要数据传输机密性
重要数据存储机密性
重要数据传输完整性
重要数据存储完整性
不可否认性

(5) 管理制度

评估指标
具备密码应用安全管理制度
密钥管理规则
建立操作规程
定期修订安全管理制度
明确管理制度发布流程
制度执行过程记录留存

(6) 人员管理

评估指标

了解并遵守密码相关法律法规和密码管理制度
建立密码应用岗位责任制度
建立上岗人员培训制度
定期进行安全岗位人员考核
建立关键岗位人员保密制度和调离制度

(7) 建设运行

评估指标
制定密码应用方案
制定密钥安全管理策略
制定实施方案
投入运行前进行密码应用安全性评估
定期开展密码应用安全性评估及攻防对抗演习

(8) 应急处置

评估指标
应急策略
事件处置
向有关主管部门上报处置情况

4. 项目实施周期

依据采购人 12 个信息系统的建设进度，按照网络安全等级保护测评、商用密码应用安全性评估规定的时间节点展开测评、评估工作。服务周期从合同签订之日起，至采购人 12 个信息系统需要配套网络安全等级保护测评、商用密码应用安全性评估的项目验收结束。

5. 培训

(1) 针对网络安全管理部门的培训：

通过全面学习商用密码、等级保护以及网络安全相关的政策、法规、理论知识及应用技能，充分认识了网络安全工作的重要意义，进一步提升了网络安全意识，明确了行业网络安全的主要任务，为下一步扎实推进网络安全等级保护、商用密码应用安全等做好相关工作，推动医院信息化建设打下了坚实的基础。培训方式为实战演练和集中培训，不少于 1 次，培训地点为采购人办公现场。

(2) 针对院领导及中层干部的培训：

主要内容为网络安全管理政策及应对策略，网络安全管理制度的制订和落实。培训方式为集中培训，不少于 1 次。培训地点为采购人办公现场。

(3) 针对全员的培训：

要内容为日常生活中需要注意的网络安全问题，日常工作中的网络安全防护及网络安全现状分析及容易忽视的安全问题。培训方式为集中培训，不少于 1 次。培训地点为采购人办公现场。

6. 验收要求

(1) 网络安全等级保护测评：须提供各应用系统的备案证书、测评报告、测评证书。

(2) 商用密码应用安全性评估：须提供评估报告。

(3) 分别对单个业务系统进行网络安全等级保护测评、商用密码应用安全性评估验收。出具了正式的网络安全等级保护测评、商用密码应用安全性评估报告，即为单个业务系统的网络安全等级保护测评、商用密码应用安全性评估验收通过。

7. 其它

项目实施期间要求不少于 15 人的现场实施人员。

四、第二包：软件测试服务

1. 总体要求

按照《GB / T 22239-2019 网络安全等级保护基本要求》、《系统与软件工程 系统与软件质量要求和评价（SQuaRE）》（GB/T 25000-2016）等国家及行业标准完成软件测试与评估服务。

软件测试服务检出的问题，投标人提出整改建议，由采购人责成医院内部或相关承建厂商落实整改。整改期间，投标人进行不限次数的复测，不再另外增加费用。

2. 基础要求

本次软件测试对 10 个二级业务系统，2 个三级业务系统：产品说明、用户文档集，功能性、性能效率、兼容性、易用性、可靠性、信息安全性、维护性、可移植性八大特性进行检验检测，须依据各系统的需求文档、用户手册、招标文

件、投标文件、合同等需求文件制定测试方案及制定测试计划，完成上述系统检验检测，协助提出应用系统整改意见，最终须出具加盖 CMA 标识具有法律效力的软件检测报告，并提供加盖检测章的原始记录原件。

3. 内容要求

(1) 产品说明：

以文体的方式对产品进行详细表述，具有真实性、科学性、条理性、通俗性、实用性。

(2) 用户文档集：

产品使用的全部信息，包括用户可调用的所有功能，所有边界值，具有完备性、正确性、一致性、易理解性。

(3) 功能性：

根据项目建设要求，测试系统是否按照招标文件及需求规格说明书的规定提供全部功能；系统功能模块应全部挂接；所有的功能模块均正确实现；业务操作流程应该符合系统设计文件的要求；软件数据共享，达到集成要求，程序是否能适当地接收输入数据而产生正确的输出信息，并保持外部信息（如数据库或文件）的完整性；投标方根据需求规格说明书和用户手册，将功能点转换为功能测试需求，根据需求编写测试用例，保证所有功能点必须被测试用例覆盖。用例设计上兼顾正常业务逻辑和异常业务逻辑。

(4) 性能效率：

使用测试工具，测试系统是否满足用户的性能需求，系统是否能够达到预期的系统响应时间以及业务处理时间，满足业务需求。监控平台数据库、中间件、应用服务器使用情况，分析数据库、中间件、服务器性能对软件运行效率的影响，提出优化建议。

系统上线前后性能测试及数据库调优，测试系统功能模块的稳定性，以应对大并发量的访问以找到目前系统的瓶颈、估算当前系统的最大并发业务处理能力，对系统整体进行性能测试与优化建议，验证稳定性和可靠性。识别系统性能瓶颈，给出优化建议。

(5) 兼容性：

在不同硬件厂商的不同硬件配置、软件系统环境下能够正常运行，并达到一

致效果。软件能稳定地工作在若干个操作系统中，而不会出现意外的退出。

（6）易用性

易安装性、用户界面的友好性、易学习性、易操作性、联机帮助丰富性。

（7）可靠性：

软件可靠性与软件本身的缺陷数量息息相关，因此结合功能测试寻找软件缺陷，可以提高软件系统可靠性，主要是系统的错误屏蔽、数据校验能力和其他与功能相关的可靠性指标。

（8）信息安全：

对于用户权限限制、用户密码封闭性、数据备份与恢复手段、留痕功能等系统安全性的测试可以结合功能测试完成。对于安全方面，验证系统是否采用正确的安全保障方法即可以了解系统安全性。

（9）维护性：

当试图诊断缺陷或失效的原因，或标识需要修改的部分时，维护者或用户的工作量应较小，耗费资源应较少。

（10）可移植性：

软件对特定硬件、特定操作系统、特定数据库系统、特定支撑软件或其特定版本的依赖程度，软件可移植、跨平台使用的能力。考察软件与其他常用应用程序的兼容性。软件应具有一定程度的开放性，在保证系统和数据安全的前提下，能够方便地与其他系统应用软件实现数据交换和共享。

4. 实施管理要求

（1）应成立项目管理组织，严格遵守采购人项目管控相关规章制度的要求。在项目实施各个阶段，按照采购单位相关要求提交文档，并配合其工作。

（2）投标方应基于成熟的项目管理方法论，制订完善的项目管理制度、流程，合理划分项目管理的阶段，借助工程工具，在项目实施过程中对项目进行规范化管理，确保项目实施进度和实施质量。

（3）投标方应提供项目管理方案，至少覆盖进度管理、范围管理、风险管理、需求管理、质量管理、资源管理、时间管理、沟通管理等。

（4）投标方应根据项目管理的需要，提供和使用项目管理工具。如采购人要求使用的，必须使用采购人提供的项目管理工具。

（5）提供项目管理工具的，应保证采购人免费使用该管理工具，如涉及版权纠纷，后果由投标方承担。

（6）各阶段产出物采用特殊格式的，投标方需提供相应的打开、编译、运行、修改、打印等工具，并确保采购人无限制的使用；不受版权和知识产权限制，采购人不对工具额外付费。

（7）投标方应认真估算工作量，做好工作量冗余。终验前，投标方须无条件接受并按采购人要求完成各种项目变更，采购人不另行支付费用。

（8）投标方在项目实施过程中所需各种检测工具、项目管理工具等由投标方提供，其结果文档应不依赖于工具而具有可读性，采购人不对此额外付费。

5. 知识产权要求

本项目在进行过程中，所产生的所有与本项目相关的，无论以任何载体形式出现的工作成果，其知识产权均属于采购人所有。

投标方保证采购人及其用户在使用过程中不受到第三方关于侵犯专利权等知识产权的指控。任何第三方如果提出指控，投标方须与第三方交涉并承担可能发生的一切法律责任和费用。

6. 保密要求

投标方必须提供对本项目的保密承诺，保证对工程技术文件以及由采购方提供的所有内部资料、技术文档和信息予以保密；服务人员需签订服务保密协议。在服务工作中获取的业务信息，以及提供的所有文件都属于保密信息，未经同意，不得泄露、传播、发布、发表、传授、转让或者以其他任何方式使第三方知悉。

7. 业务系统专家评估要求

代表采购人，邀请相关专业、行业及管理方面业内专家，对采购人 12 个信息系统的运行情况和业务使用效果进行专家论证，论证内容以用户实际需求和现场要求为主，并出具专家评估意见书。

论证专家须为本项目和采购人信息化项目所涉及领域或行业（计算机技术、应用系统开发、医院或其业务管理等）的专业技术或业务管理人员，从业五年以上，为内蒙古自治区或各盟市级政府采购评审专家库成员。

8. 服务周期

依据采购人 12 个信息系统建设进度，按照软件测试规范规定的时间节点展开软件测试工作。服务周期从合同签订之日起，至采购人 12 个信息系统建设需要配套软件测试的项目验收结束。

9. 验收要求

- (1) 须提供软件测试报告、专家评估报告。
- (2) 分别对单个业务系统进行软件测试验收。出具了正式的软件测试报告和专家评估结论，即为单个业务系统的软件测试验收通过。

10. 其它

项目实施期间要求不少于 5 人的现场实施人员。

五、第三包：网络安全服务

1. 总体要求

依据《中华人民共和国网络安全法》、《GB / T 22239-2019 网络安全等级保护基本要求》等国家及行业标准完成网络安全服务与全院网络运维等工作。

为保障招标人能够顺利通过等保测评，避免招标人重复建设和浪费投资，投标人须出具的等保合规服务方案，方案须取得等保测评机构出具的网络安全方案等保合规认可书，该认可书包括但不限于：《等保合规服务方案认可书》及测评机构自身的《网络安全服务认证证书（等级保护测评服务认证）》、《检验机构认可证书》、《检验检测机构资质认定证书》。

2. 网络安全服务

安全服务要求：针对内外网开展如下服务内容，服务周期为一年，安全服务详细内容如下：

服务类别	服务名称	详细描述	开展周期
基础安全	定制安全通告	实时关注安全动态，为客户精心提供安全通告服务。该通告包括安全漏洞(补丁)通告、安全威胁通告、安全业界动态、恶意代码防范、紧急通告等多项内容。	每月提供 不少于 1 个

	安全巡检服务	检查内容包括机房所有安全设备（系统）运行情况及审计日志分析、验证、重要服务器端口状况扫描、端口监听检查、用户列表检查、进程检查、病毒检查、系统木马检查等安全检查与分析工作。	每月 1 次
	安全漏洞评估	使用多厂商远程漏洞评估产品，检测网络设备、操作系统、数据库和应用服务中存在的安全漏洞，提供漏洞评估报告和修复建议。	每月 1 次
	安全配置评估	使用多厂商安全配置核查产品或人工方式，对系统网络设备、操作系统、数据库和应用服务器的配置进行安全检查，提供安全配置评估报告和改进建议。	每月 1 次
	安全加固支持	针对安全漏洞和安全配置评估中发现的安全漏洞和配置缺陷，提供加固意见和方案，配合客户完成配置修复。	每月 1 次
	恶意样本分析	人工方式检测操作系统和应用中是否存在恶意样本，分析样本的访问行为，评估对系统的影响，提供安全分析报告和清除方法。	发生此类事件时
	日志安全分析	对各类系统（IDS、WEB 服务器等）产生的日志进行数据分析，及时发现攻击事件和可疑行为，提供日志分析报告。	每月 1 次
	紧急响应	远程或现场方式及时响应和处理信息安全事件，协助客户降低影响，分析问题产生的原因，提供应急响应报告和改进建议。	发生安全事件时
应用安全	渗透测试	通过人工黑盒的测试方式，发现网络和业务系统中网络和系统存在的安全缺陷，提供渗透测试报告和改进建议。	每季度 1 次
安全预防	开放端口检查	通过扫描方式对互联网、内网、专网上客户开放的端口、服务进行检查，识别客户对外提供服务的真实情况。	每月 1 次
鉴定	电子数据司法鉴定服务	对甲方重要信息系统在发生各类情况（包括但不限于故障、纠纷、投诉等等）需要开展电子数据司法鉴定的有关事宜在服务期内不限次数开展司法鉴定工作并出具具备法律效力的司法鉴定报告。	发生网络安全问题时
检查	安全检查技术支持	按照甲方工作要求，安排专业技术人员携带必备安全检查工具与甲方开展面向甲方本单位、本行业的网络安全检查工作。	检查期间开展
重保	安全值守服务	在攻防演习及重要时期（法定节假日、重大会议活动等）期间，提供现场安全专家值守服务，实时监测、分析、研判、处置各类网络攻击，保障业务系统安全稳定运行。以“事前准备、事中保障（值守、监控、应急、处置）、事后总结（复盘、提升）”的思路来保障用户信息系统的安全。	重保期间开展

监测	威胁检测与全流量回溯（含功能化安全服务）	发现弱点扫描、命令执行、注入攻击、跨站脚本、信息泄露、邮件钓鱼等相关风险行为。用于满足等级保护-安全区域边界中恶意代码和垃圾邮件防范的要求，以及满足安全区域边界-入侵防范中“应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析”的高危风险要求。 部署三年全部特征库升级的全网安全监测与感知预警系统（态势感知）3套，包含新楼内网、新楼外网、旧楼外网；部署开通全部功能、具备三年全部特征库升级的网络流量检测与回溯系统1套，可处理不小于10G带宽流量，存储能力不少于128T，支持流量采集、数据存储、协议解析、资产分析、数据回溯、安全分析、高级攻击行为分析溯源等功能。	实时监测
----	----------------------	--	------

3. 服务周期

网络安全服务项目为合同签订之日起1年

4. 验收要求

（1）网络安全服务：须按每项服务周期要求，定期提供服务报告。

5. 其它

项目实施期间要求不少于3人的现场实施人员。

六、付款方式

1. 第一包：网络安全等级保护测评及商用密码应用安全性评估

从合同生效之日起，完成6个系统（5个二级系统、1个三级系统）的网络安全等级保护测评及1个三级系统的商用密码应用安全性评估后付款50%，项目整体验收合格后付款50%，完成的标志为出具了正式的网络安全等级保护测评、商用密码应用安全性评估报告。

2. 第二包：软件测试服务

从合同生效之日起，完成6个系统（5个二级系统、1个三级系统）的软件测试服务后付款50%，项目整体验收合格后付款50%，完成的标志为出具了正式的软件测试报告。

3. 第三包：网络安全服务

从合同生效之日起，每 6 个月结算一次，总共结算两次。