中山市小榄人民医院

2024年度网络与数据安全服务项目

招标采购需求书

采购人：中山市小榄人民医院

日期：2024年9月5日

1 总则

1.1 响应供应商报价应包括服务项目相关的全部费用，如咨询规划、方案设计、需求调研、系统集成、数据处理、测试评估、设备维护费用、税费、人员差旅费、保险费、培训和质保等。在项目实施过程中出现报价内容的任何遗漏，均由成交供应商负责相关费用，采购人将不再支付任何费用。

★1.2 响应供应商须对第 4 节《2024 年度网络与数据安全服务清单》逐行进行单项报价。

1.3 采购文件中凡有“★”标识的内容条款为关键条款，响应供应商必须对此作出回答并完全满足这些要求，不可以出现任何负偏离，对这些关键条款的任何负偏离将视为无效响应。加注“▲”的内容为重点评标项目，响应供应商必须对该标识项目按照要求进行真实应答描述。

★1.4 本项目不接受联合体投标，成交供应商不得以任何方式转包本项目。

★2.供应商资格要求：

响应供应商必须具备下列规定的条件，并提供相应的证明材料：

2.1 必须是具有独立承担民事责任能力的在中华人民共和国境内注册的企业法人或其他组织，具备相应的经营范围。分公司报名的，还需提供投标人及其总公司营业执照，若投标人及其总公司之间存在多级授权的，则一并提供中间授权公司营业执照。

2.2 有国家认可的 ISO9001 质量管理体系认证证书、ISO14001 环境管理体系认证证书、ISO4501 职业健康安全管理体系认证证书和 ISO27001 信息安全管理体系认证证书。

2.3 单位负责人为同一人或者存在直接控股、关联关系的不同投标人，不得参加同一项目下的招标活动。（提供承诺函）

2.4 有良好的信誉、健全的财务会计制度。（提供承诺函）

2.5 无重大违法记录或失信记录。（提供承诺函）

2.6 依法缴纳税收和社会保障资金。（提供承诺函）

2 采购内容

序号	名称	数量	限价
1	中山市小榄人民医院 2024 年度网络与数据安全服务项目	1	85 万元

3 项目概述

3.1 项目名称

中山市小榄人民医院 2024 年度网络与数据安全服务项目

3.2 项目背景

依据国家网络安全等级保护相关规范与标准的要求，中山市小榄人民医院必须对院内重要信息系统进行定级备案、测评分析、整改建设、验收测评。同时，为满足中山市卫健局发布的《中山市医疗卫生机构网络数据安全绩效考核指标明细表（100 分）》的具体要求，医院需要建立一个完整的、动态的、可靠的网络与数据安全保障体系。

3.3 项目目标

通过采购人网信安全现状的全面排查与隐患整改，为采购人建立一个完整的、动态的、可靠的网络与数据安全保障体系，有效保障其系统业务的正常开展，保护敏感数据信息的安全，保证信息系统的安全防护能力达到《信息安全技术信息系统安全等级保护基本要求》中的相关技术和管理要求，满足《中山市医疗卫生机构网络数据安全绩效考核指标明细表（100 分）》的绩效要求。

3.4 项目依据及标准

3.4.1政策/法律法规

- 《中华人民共和国网络安全法》
- 《中华人民共和国数据安全法》
- 《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）

- 《中共中央办公厅国务院办公厅转发<国家信息化领导小组关于加强信息处理安全保障工作的意见>的通知》（中办发[2003]27 号）
- 《关于印发<关于信息安全等级保护工作的实施意见>的通知》（公通字[2004]66 号文）
- 《关于印发<信息安全等级保护管理办法>的通知》（公通字[2007]43 号文）
- 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号文）
- 《国家网络与信息安全协调小组关于开展信息安全风险评估工作的意见》（国信办[2006]5 号）

3.4.2技术标准

- 《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）
- 《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）
- 《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）
- 《信息安全技术网络安全等级保护实施指南》（GB/T25058-2019
- 《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）
- 《计算机信息系统安全保护等级划分准则》（GB17859-1999）
- 《信息安全技术信息系统通用安全技术要求》（GB/T20271-2006）
- 《信息安全技术网络基础安全技术要求》（GB/T20270-2006）
- 《信息安全技术操作系统安全技术要求》（GB/T20272-2006）
- 《信息安全技术数据库管理系统安全技术要求》（GB/T20273-2006）
- 《信息安全技术服务器技术要求》（GB/T21028-2007）
- 《信息安全技术终端计算机系统安全等级技术要求》（GA/T671-2006）
- 《数据安全技术 数据分类分级规则》（GB/T 43697-2024）
- 《信息技术 数据加密保护要求》（GB/T 39786-2021）
- 《信息技术 数据备份与恢复》（GB/T 30285-2023）
- 《信息技术 数据处理 安全要求》（GB/T 35273-2022）
- 《信息技术 安全技术 远程办公 数据保护指南》（GB/T 35416-2021）

除上述规范以外，还遵循国家现行的相关标准和规范要求。

4　2024年度网络与数据安全服务清单

序号	类别	工作内容	服务频次	交付成果
1	等级保护测评服务	1、等保测评：依据国家网络安全法最新的要求，对采购人的HIS、PACS、LIS三个系统按照等级三级的最新标准进行等级保护测评，医院官网系统按照等级二级的最新标准进行等级保护测评，进行差距分析、验收测评，并出具符合公安机关要求的测评报告。 2、测评支撑服务：严格按照最新国家等级保护标准要求，提供等级保护测评现场支撑服务，包含但不限定测评前期沟通协调、新上线系统定级备案、专家评审、现场实施对接、整改加固支撑、验收及公安报备等工作。 3、按照等级保护最新要求和最新的中山市医疗卫生机构网络数据安全绩效考核指标，为采购人完善一套安全管理制度集。 4、公安报备：协助向公安监管部门提交测评报告，取得回执。	服务期内	《差距分析报告》 《等保测评报告》 《整改实施方案》 《管理制度集》 《整改实施过程清单》
2	漏洞扫描服务	对网络资产进行漏洞扫描，发现资产存在的漏洞并对漏洞修补提出解决意见，提供对资产进行系统加固，实现漏洞闭环管理，漏扫范围包含系统漏洞检测、web漏洞检测、数据库漏洞检测、配置合规检测、弱口令检测等，每季度一次	年度4次	《漏洞扫描报告》
3	渗透测试服务	对医院官网和三大系统(HIS、LIS、PACS系统)进行渗透测试，在对现有信息系统不造成损害的前提下，由具备高技能和高素质的安全服务人员发起，并模拟常见黑客所使用的测试手段对目标系统进行模拟入侵。	年度4次	《渗透测试报告》

4	安全支撑服务	协助完成上级主管或公安部门相关检查技术支撑工作和协助采购人组织好应急处置队伍	按需	《安全支撑服务报告》
5	安全巡检服务	1、对相关系统的内、外网进行资产情报的搜集，梳理出资产的 IP、端口信息、应用指纹信息等资产详情，提升资产管理能力。 2、对服务器、数据库、中间件、网络设备、安全设备、业务应用系统开展安全巡检工作，发现其存在的网络异常情况、配置缺陷以及风险漏洞，提出整改建议并对各个网络设备、安全设备和系统配置优化，进行漏洞处理，对信息系统软件层面的漏洞进行技术指导，协助厂商进行整改。	年度 4 次	《安全巡检报告》 《资产台账表》
6	应急响应及演练服务	1、应急响应:针对采购人出现的网络安全事件，提供安全应急响应支撑服务,协助对包括勒索病毒、网络攻击等安全事件，进行事件分析、攻击溯源、系统恢复等应急处置工作。 2、应急演练:按照应急演练的要求，结合采购人的需求，在服务期内提供两次安全应急演练服务，当发生安全事件时提供应急响应服务，且针对采购人实际情况提供应急预案材料。	一年	《安全事件应急响应处置报告》 《应急演练预案》 《应急演练计划方案》 《应急演练报告》 《应急过程材料等》
7	攻防演练安全保障支撑	攻防演练期间建立应急响应小组，对网站入侵、拒绝服务攻击、大规模病毒爆发、主机或网站异常事件等紧急安全问题提供全天候现场或者远程技术支持，控制事态发展，无条件提供各类安全技术人员和调动各类资源,确保及时处置安全事件。	按需	《重保值守日报》 《重保值守总结报告》

8	安全咨询服务	对安全体系设计等给予技术支持，提供管理体系、技术体系、运行体系的安全咨询服务。	年度一次	《X安全体系设计方案》
9	暴露面梳理服务	根据采购人需求,定期开展医院互联网资产暴露面的梳理工作,协助采购人收敛医院不必要对外开放的服务及端口,并开展互联网暴露面的风险识别工作。	按需	《互联网暴露面资产梳理报告》 《互联网侧漏洞扫描报告》
10	远程威胁检测与响应运营服务	1、以7*24小时持续在线守护为主线、以“资产、脆弱性、威胁、事件"四个核心安全风险要素为抓手，提供常态化7*24小时的远程监测分析服务，及时排查高危的漏洞和存在的安全隐患。 2、对内外网威胁封堵：精准研判外网威胁告警，封堵外网攻击IP地址及内网病毒传播、跳板攻击。	一年	《安全事件监测周报》 《安全事件监测月报》 《资产风险漏洞管理跟踪报告》
11	风险评估服务	根据风险评估标准及要求，对采购人HIS、LIS、PACS三个业务系统和医院官网等对外的业务系统进行系统风险评估工作,输出相关业务系统的风险评估报告。	年度一次	《风险评估报告》
12	零信任系统	采购人规格要求至少等于或高于以下功能要求： 管理平台:支持采用软硬件一体部署或云化部署 功能要求：支持包括接入安全检查、IAM权限控制、用户行为日志审计、精细粒度访问控双因子认证、终端行为管理、终端信任评分等，用户连接并发数≥50个（支持快速扩容）。 **质保要求：含3年功能授权及3年维保服务。**	一套	《实施方案》 《试运行报告》 《设备拓扑》 《培训记录》 《验收报告》 《使用手册》
13	政务网边界防火墙	采购人规格要求至少等于或高于以下功能要求： 硬件规格：1、软硬件一体产品；2、标准机架式、 电源规格：1+1冗余电源；内存≥8 GB；硬盘≥	一台	《实施方案》 《试运行报告》

		2 TB；3、网络吞吐性能≥6Gbps；4、每秒新建连接数（TCP）≥5 万；5、最大并发连接数（TCP）≥300 万。 功能要求：支持包括防病毒模块、IPS 入侵检测模块、上网行为管理模块、Web 安全防护模块、SSL VPN 等增强特性授权。 **质保要求：含 3 年功能授权及 3 年维保服务。**		《设备拓扑》 《培训记录》 《验收报告》 《使用手册》
14	3 台清华永新 TN-SG5000-E680 防火墙维保服务	1、日常适应性维护服务（提供 7*24*4 小时级别服务，7*24*4 是指每周 7 天,每天 24 小时，电话响应,包含法定节假日，如需要成交供应商工程师到现场的在接到采购人电话通知后最快 2 小时内到达故障设备现场，最迟不得超过 4 小时）； 2、在维护期内根据采购人要求，须确保维护设备功能完整，具备高级威胁防护许可，包括但不限于：一般更新、入侵防御、反病毒、突发防护等特征库的实时更新。 3、对于以上服务条款的内容，成交供应商需提供工程师到现场或通过远程的方式执行维护服务;电话响应时效为 0.5 小时内，若通过电话不能解决问题的,在 4 小时内到安排维护工程师达用户现场； 4、维修方能提供具有比较成熟的备件库运作管理机制，在维护周期内，如采购人需要成交供应商提供备件支持时,成交供应商能提供及时的服务支撑；	一年	《运行报告》
备注：主要内容及要求详见附件《项目需求内容及要求》				

5 采购项目需求内容及要求

5.1 安全服务类

5.1.1等级保护测评服务

在项目服务期内，依据国家网络安全法最新的要求，对采购人的HIS、PACS、LIS三个系统按照等级三级的最新标准进行等级保护测评，医院官网系统按照等级二级的最新标准进行等级保护测评，出具符合公安机关要求的测评报告。

5.1.1.1 系统定级备案服务要求

成交供应商需协助采购人完成采购人系统的定级备案工作，包括定级备案过程中的资产梳理、文档整理、材料编制及递交工作等事项，保证后续等级保护测评工作的顺利开展。

5.1.1.2 等级保护测评服务要求

成交供应商需委托具有资质的测评机构，根据《网络安全等级保护基本要求》等标准开展信息系统等级保护符合性测评，衡量采购人信息系统的安全保护管理措施和技术措施是否符合等级保护三级的相关要求，是否具备相应的安全保护能力。差距测评完成后，测评机构出具《差距问题清单》，罗列采购人系统存在的不符合问题项。

协助采购人根据《差距问题清单》完成相应整改后，测评机构针对采购人系统进行验收测试，验收测评完成后，测评机构出具《网络安全等级保护测评报告》，评估确认采购人系统是否满足等级保护三级相关要求。

5.1.1.3 管理制度修订要求

成交供应商需按照最新法律法规及《差距问题清单》要求对采购人的管理制度更新及修订，对应急预案进行修订优化，提供满足法律法规及相关规范要求的管理制度，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，所提供的网络安全管理制度需满足等级保护三级相关要求。

5.1.1.4 整改加固要求

成交供应商需提供技术支持协助采购人开展整改加固工作，对《差距问题清单》中存在的不符合问题项逐一进行整改加固，使其满足等保三级相关要求，整

改范围包括主机、数据库、应用系统、网络设备、安全设备等。整改完成后，成交供应商需提交相应的整改证明材料提交给测评机构做审核。

5.1.1.5 安全保密要求

成交供应商应当提供与采购人的保密协议草拟本，并在中标后与采购人签署保密协议，对于安全服务所获取的相关信息进行严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据、信息进行任何侵害采购人信息系统的行为。

5.1.1.6 服务人员要求

现场测评开展时，成交供应商必须安排中级或以上的安全工程师（有CISP或CISSP证书）到现场协助采购人完成测评工作，以及后续的整改实施，根据系统遗留隐患和不符合项的整改工作量，成交供应商安排的安全工程师驻场在医院的时间为到服务期结束。投标人应提供项目组成员姓名、学历、相关资质、在本项目中的职责及以前参与过的项目情况说明等。

成交供应商须保证队伍稳定，并由采购人项目负责人审核，审核通过后才能参与实施工作；经确认的技术团队，未经采购人项目负责人同意，不得更换技术人员；成交供应商必须遵守采购人内部各项规章制度和内部操作规程，履行保密义务，签署保密协议，未经批准不得以任何理由泄露任何保密信息和内部资料；技术团队应具备有利于开展实施工作的工具（包括软件和硬件）。

5.1.1.7 服务技术要求

成交供应商需提供详细的整体服务方案，包括技术方案和实施方案。技术方案包括整体流程、技术方法和服务方案设计等；实施方案包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等。

服务实施过程中所使用到的其他各种工具软件由成交供应商自行提供，漏洞扫描检测至少使用一款商用扫描系统。成交供应商须承诺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成交供应商负完全责任。

▲为了保障服务质量，成交供应商需提供相应的服务工具**（出具原厂授权书）**，包括但不限于以下工具：

1）漏洞扫描工具（含配置核查工具模块）

1、支持通过多种维度对漏洞进行检索，包括：CVE ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息；

2、可扩展支持等级保护配置核查；

3、支持与堡垒机联动，可从堡垒机获取目标设备密码进行配置核查，全程自动化，防止密码外泄；

4、可导出EXCEL格式，方便筛选分析。

▲成交供应商需承诺，在投标文件中承诺提供的工具系统必须在中国网络安全审查技术与认证中心通过认证的产品，并提供查询证明。采购人有权在中标后、项目实施前，进行现场工具检测，与招标文件不符合虚假者，采购人有权将按废标处理，并永久列入采购黑名单（承诺函格式自拟）。

▲成交供应商需提供信息系统等级测评项目的管理工具给采购人使用，以便采购人积累与利用服务成果。管理工具能够方便地保存和使用前一项所要求的各类技术文档，展示政策法规、管理规范、记录表单、操作规程和清单协议等五大类文件类型，针对于文档内容，可依据关键词，内容进行全局检索，支持PDF，Word，Excel等多种格式检索，提升合规操作易用性;具备等保自检功能，能够辅助采购人人员自主测评，提升测评效率和通过率；能够对发现的风险，测评问题进行记录，整改，闭环管理;能够展示当前全局合规状态，合规建设程度情况，自动化提炼管理关键词;能够从实际业务场景出发提供自检自查服务，从线上执行，自动计算得分，检查留痕;内置提供常用和典型的安全检查指标要求，方便采购人自行维护更新;提供安全培训课件和培训文档资料统一管理的功能**（提供产品截图、原厂授权及销售许可证）。**

▲为了确保顺利通过管理制度要求，成交供应商需提供安全管理制度管理工具，以信息系统的角度，以保障系统业务正常运行为出发点，将系统的信息安全管理状况与等级保护管理要求进行深入的差距分析，深入分析现有的系统管理体系和信息安全管理制度，从各个方面协助建立与信息系统安全技术和安全运行相适应的完善的符合系统业务特点的信息安全管理体系。提供的管理工具满足如下功能指标**（提供产品截图、原厂授权及销售许可证）：**

1）制度管理：支持以等保要求的类型对安全制度进行分类，须包含以下类

型：政策法规、管理规范、记录表单、操作规程、清单协议，为规范化的安全制度管理奠定基础。

2）制度台账：支持对各个类型的系统台账管理，并能所涉及到的纪要、记录等内容上传后存档管理。

▲成交供应商需为采购人提供安全等保安全支撑服务，包含等保二级、等保三级的技术支撑，提供针对等保迎检、安全合规迎检工作支撑服务，需为本次服务的提供一套安全迎检合规系统，部署在本地环境，提供态势大屏呈现，资产管理、制度管理、漏洞风险管理、等保系统备案管理、等保系统测评项目管理、安全培训管理、安全应急演练管理、安全迎检管理，合规知识库管理等工作（**提供产品截图、原厂授权及销售许可证**）。

5.1.1.8 服务成果物要求

本项服务的交付成果包含但不限于以下文档：

- 《中山市小榄人民医院 XX 系统差距分析报告》
- 《中山市小榄人民医院 XX 系统等级保护测评报告》
- 《中山市小榄人民医院 XX 系统整改实施方案》
- 《中山市小榄人民医院管理制度集》
- 《整改实施过程清单》

5.1.2漏洞扫描服务

项目服务器内，成交供应商需对采购人网络资产进行漏洞扫描，发现资产存在的漏洞并对漏洞修补提出解决意见和协助修补，提供对资产进行系统加固，实现漏洞闭环管理，漏扫范围包含系统漏洞检测、web 漏洞检测、数据库漏洞检测、配置合规检测、弱口令检测等，每季度一次。

5.1.2.1 服务成果要求

本项服务的交付成果包含但不限于以下文档：

- 《漏洞扫描报告》

5.1.3渗透测评服务

项目服务期内，成交供应商需对采购人医院官网和三大系统（HIS、LIS、PACS系统）进行渗透测试，通过模拟真实攻击来发现采购人信息系统中存在的安全漏洞和弱点，服务频率为一年四次。

5.1.3.1 渗透测试要求

模拟黑客攻击手段对目标系统进行探测攻击，从而发现黑客入侵信息系统的潜在可能途径。

渗透测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透、B/S 或 C/S 应用程序测试、社会工程等。

测试范围必须包括以下内容：

- Web 安全：Web 安全测试范围包括 SQL 注入、XSS、XXE、CSRF、RFI、上传漏洞、信息泄露、远程命令执行、反序列化漏洞等。
- 业务逻辑安全：业务逻辑安全测试范围包括用户或口令枚举、弱口令测试、平行/垂直越权、未授权访问、验证缺陷、业务逻辑限制缺陷等。
- 中间件安全：中间件安全测试范围包括配置缺陷、中间件弱口令、反序列化漏洞、代码执行漏洞等。
- 服务器安全：服务器安全测试范围包括域传送漏洞、弱口令漏洞、未授权访问漏洞、脚本密码检查、本地提权漏洞、应用防护软硬件缺陷等。

5.1.3.2 服务成果要求

- 《XX 系统渗透测试报告》

5.1.4安全支撑服务

服务器内，成交供应商需按需协助完成上级主管或公安部门相关检查的技术支撑工作，协助采购人组织好应急处置队伍。

5.1.4.1 服务成果要求

- 《XX 系统渗透测试报告》

5.1.5安全巡检服务

服务期内，成交供应商需定期对采购人院内系统、设备等做安全巡检，包括：

- 对相关系统的内、外网进行资产情报的搜集，梳理出资产的IP、端口信息、应用指纹信息等资产详情，提升资产管理能力。
- 对服务器、数据库、中间件、网络设备、安全设备、业务应用系统开展安全巡检工作，发现其存在的网络异常情况、配置缺陷以及风险漏洞，提出整改建议并对各个网络设备、安全设备和系统配置优化，进行漏洞处理，对信息系统软件层面的漏洞进行技术指导，协助厂商进行整改。

5.1.5.1 服务成果要求

- 《安全巡检报告》
- 《资产台账表》

5.1.6应急响应及演练服务

服务期内，成交供应商需针对采购人出现的网络安全事件，提供安全应急响应支撑服务，协助对包括勒索病毒、网络攻击等安全事件，进行事件分析、攻击溯源、系统恢复等应急处置工作；此外，成交供应商需提供两次安全应急演练服务，检验采购人应急响应流程的有效性和实用性。

5.1.6.1 应急响应要求

在项目服务期内，服务提供商提供信息安全事件应急响应救援服务。应急响应内容主要包括：病毒暴发、黑客攻击、网络大范围瘫痪、应用系统瘫痪及其他严重影响业务运行的事件。响应要求如下：

1．对于病毒暴发和黑客攻击现象发生时、在十分钟内响应，提供远程诊断技术支持，远程无法解决的，2小时内赶到现场，解决故障恢复正常或提出可行的临时解决措施。

2．出现网络大范围瘫痪、应用系统瘫痪及其他严重影响业务运行的事件时、应立即派具有相关应急经验的工程师2小时内上门协助处理，若指定时间内未能解决故障，应提供事件处理的临时解决方案。

3．在应急响应结束3天内，需提供本次应急解决处理方案和安全防护建议，针对事件中的问题协助采购人进行安全加固。

5.1.6.2 应急演练要求

信息安全应急管理体系是指导及提升应急响应工作的重要支撑。由于信息安全的动态变化，成交供应商需根据安全态势的发展，协助采购人优化与完善应急响应体系。

成交供应商需协助采购人完成现有信息安全应急管理体系文件的年度修编，确保采购人网络安全应急总预案满足安全监控部门以及行业主管机构在信息安全及安全预案方面的整体性要求，同时确保采购人网络安全预案能够应对最新的安全攻击技术、最新出现的安全事件，具有较强的实时性。

成交供应商需协助采购人开展应急演练工作。通过应急演练，完善应急流程与操作，提升采购人对重大安全事件的应急处置能力。

5.1.6.3 服务成果要求

- 《中山市小榄人民医院安全事件应急响应处置报告》
- 《中山市小榄人民医院应急演练预案》
- 《中山市小榄人民医院应急演练计划方案》
- 《中山市小榄人民医院应急演练报告》
- 《中山市小榄人民医院应急过程材料等》

5.1.7攻防演练安全保障支撑服务

服务期内，成交供应商需在采购人攻防演练期间建立应急响应小组，对网站入侵、拒绝服务攻击、大规模病毒爆发、主机或网站异常事件等紧急安全问题提供全天候现场或者远程技术支持，控制事态发展，无条件提供各类安全技术人员和调动各类资源，确保及时处置安全事件。

- 加强组织：成交供应商需成立专门的网络安全保障工作小组，明确责任分工，确保各项工作落到实处。
- 完善预案：针对可能出现的网络安全事件，制定应急预案，明确应急处置流程和措施。
- 全面排查网络安全薄弱环节：对信息系统和网站进行全面的安全检查，及时发现和修复安全隐患。
- 加强监测：利用技术手段，对网络进行实时监测，以便于发现和应对可能的网络安全威胁。
- 落实值班值守制度：在重要时期，安排人员值班，确保网络安全事件能够得到及时处置。

5.1.7.1 服务成果要求

- 《重保值守日报》
- 《重保值守总结报告》

5.1.8安全咨询服务

成交供应商需对采购人安全体系设计等给予技术支持，提供管理体系、技术体系、运行体系的安全咨询服务。

5.1.8.1 服务成果要求

- 《XX 安全体系设计方案》

5.1.9暴露面梳理服务

成交供应商应根据采购人需求，定期开展采购人互联网资产暴露面的梳理工作，协助采购人收敛医院不必要对外开放的服务及端口，并开展互联网暴露面的风险识别工作。

5.1.9.1 服务成果要求

- 《互联网暴露面资产梳理报告》
- 《互联网侧漏洞扫描报告》

5.1.10 威胁检测与响应运营服务要求

以7*24小时持续在线守护为主线、以“资产、脆弱性、威胁、事件"四个核心安全风险要素为抓手，提供常态化7*24小时的远程监测分析服务的及时高危的漏洞和存在的安全隐患。同时对内外网威胁封堵：精准研判外网威胁告警，封堵外网攻击IP地址及内网病毒传播、跳板攻击。

成交供应商需提供7*24小时远程威胁检测与响应运营服务，通过部署在采购人本地的远程威胁检测与响应运营平台，并联动云端的线上监管运营服务，实时监测和发现采购人网络中的安全威胁，以自动化+人工介入的形式分析和处置安全事件，开展实战化与常态化安全运营。

本项服务提供的具体服务项，包括但不限于以下内容：

- 攻击面监测：探测互联网上潜在的未知资产，不必要开放的资产，并自动验证互联网资产是否存在可利用漏洞、弱口令；
- 资产梳理：以主动探测和被动探测的方式，对网站、服务器、终端资产自动化梳理；
- 网站监测：对网站的“漏洞、篡改、黑链、敏感文件、敏感词、网马监测、可用性、域名劫持”等7个维度开展实时监测；
- 威胁诱捕：在不改变单位的网络架构前提下（包括：不做镜像流量、不做牵引流量等），通过旁路部署，在“DMZ区”、“服务器区”、“终端区”分别生成仿真业务系统；
- 漏洞屏蔽：通过主机Agent，快速屏蔽各类漏洞扫描攻击；
- 威胁处置：在判断事件类型可能为安全事件，技术人员通过现场或非现场等方式进行信息收集工作，详细了解掌握事件发生的始终、现状、可能的影响，对事件进行详细分析，提供事件处理建议，并协助采购人解决事件。

5.1.10.1 服务成果物要求

- 《安全事件监测月报》
- 《资产风险漏洞管理跟踪报告》

5.1.11 风险评估服务

根据风险评估标准及要求，对采购人HIS、LIS、PACS三个业务系统和官网对外的业务系统进行系统风险评估工作，输出相关业务系统的风险评估报告。

根据《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》要求，从风险管理的角度分析采购人指定的核心系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成危害程度，提出有针对性地抵御威胁的防护对策和整改措施；为防范和化解信息安全风险，在考虑控制成本与风险平衡的前提下选择合适控制方式将风险控制在可接受的水平，从而最大限度地为保障信息安全提供科学依据。安全风险评估服务内容包含基础环境安全评估、安全管理评估两个方面，一年一次。

5.1.11.1 服务成果要求

- 《XX系统网络安全风险评估报告》

5.1.12 3 台清华永新 TN-SG5000-E680 防火墙维保

服务期内，成交供应商需为采购人院内 3 台清华永新 TN-SG5000-E680 防火墙提供维护，具体要求如下：

- 日常适应性维护服务（提供 7*24*4 小时级别服务，7*24*4 是指每周 7 天，每天 24 小时，电话响应,包含法定节假日，如需要成交供应商工程师到现场的在接到采购人电话通知后最快 2 小时内到达故障设备现场，最迟不得超过 4 小时）；
- 在维护期内根据采购人要求，须确保维护设备功能完整，具备高级威胁防护许可，包括但不限于：一般更新、入侵防御、反病毒、突发防护等特征库的实时更新。
- 对于以上服务条款的内容，成交供应商需提供工程师到现场或通过远程的方式执行维护服务;电话响应时效为 0.5 小时内，若通过电话不能解决问题的，在 4 小时内到安排维护工程师达用户现场；
- 成交供应商能提供具有比较成熟的备件库运作管理机制，在维护周期内，如采购人需要成交供应商提供备件支持时，成交供应商能提供及时的服务支撑；

5.1.12.1 服务成果要求

- 《运行报告》

5.2 安全设备类

5.2.1零信任系统

实现对用户的本地或远程接入的安全管理和审计，具体要求如下：

序号	指标项	技术指标
1.	硬件配置	CPU≥16 核、内存≥64G DDR4、硬盘≥1T SSD、双口千兆电口以上，双电源支持冗余模式，三年软件升级和硬件保修服务
2.	部署方式	支持硬件/软件部署模式,软件部署可根据采购人提供的服务器进行搭建，也支持在 VMware、Citrix、Microsoft 等厂商的虚拟服务器中搭建
3.	架构设计及授权	C/S 架构设计,专有通信协议,国密算法加密传输,安全性高,避免 B/S 架构频繁的补丁修复。
4.		▲具备高可用架构设计，确保系统容错安全；支持≥50 管理员用户，≥500 IP 永久授权许可。
5.	实施与维保服务要求	★实施服务要求：原厂认证工程师现场咨询，安装，配置服务。 维保服务要求：原厂三年维保服务，包含软件升级和硬件保修，远程技术支持，7*24 小时电话支持，邮件支持服务**（请提供原厂授权函）**
6.	用户管理	支持对各个角色的运维人员创建实名制账号，在以后的日常运维工作中运维人员只需记住一个账号，无需记住多个业务系统服务器账号和密码，同时避免了业务系统账号信息的丢失和泄露的安全隐患；
7.		支持账号与有效 IP 地址或者 IP 地址段绑定策略；
8.		支持账号密码复杂度要求策略、可设置账号登录失败次数，达到失败次数锁定账号功能，并可设置账号解锁时间策略。
9.	认证	双因子认证 App 令牌、支持自有 OTP 认证方式（提供由厂商

	管理	盖章确认的产品界面截图证明）
10.		支持多种认证方式，支持第三方 OTP，支持本地用户、LDAP、AD、Radius 和 OTP 认证用户自由组合实现双因子
11.	控制管理	支持管理员对应用工具设置剪贴板功能（拷进、拷出）的权限分配，支持针对应用工具磁盘映射管理控制。（提供由厂商盖章确认的产品界面截图证明）
12.		从操作层面控制操作者的权限，可以细化限制到每个运维人员所能管理访问的业务系统资源，限制每个运维人员所使用的运维工具/ 协议/ 客户端/端口,以及限制用什么账号登录系统业务资源;
13.		基于资源或者设备的授权管理，自然人账号及资源设备授权清晰明了， 将所有数据保存在控制管理服务器数据库中，管理员可以实时管理自己权限范围的资源设备;
14.		支持针对 Telnet、SSH 设置命令黑白名单（精确匹配/模糊匹配），用户无法成功运行黑名单中的命令，并支持将用户执行过黑名单中命令内容发送告警邮件给管理员。
15.	应用管理	支持针对不同的运维人员提供运维人员习惯的管理工具，而并不需要运维人员去适应运维系统提供的模板化基于协议的工具，满足不同个性化的需求。
16.		可以实现对终端类，窗口类应用，远程桌面，浏览器，虚拟客户端、客户定制的客户端程序等进行集中管理，集中授权，支持用户和密码代填功能，实现一键式自动登录: 终端类应用（TerminalApp）Telnet、Rlogin、Putty、SSH、Openssh 和 SecureCRT 等 远程桌面类应用 windows RDP、PC Anywhere、VNC、RealVNC、TightVNC、UltraVNC 和 VNCViewer 等 窗口类应用（WindowsApp）Windows Explorer、Vmware vsphereclient、WinScp、Filezilla、Xwindows、Xmanager、Xmin、Xwindows、Xterm、Oracle TOAD、SQL Client 等

		支持开发工具 eclipse 发布 虚拟客户端应用 Citrix ICA 、RemoteApp、xencenter、vmware vplayer、microsoft hyper-v 浏览器类应用 Internet Explorer、FireFox、Google Chrome 和 http/https URL 支持自定义客户端应用 支持 Citrix Xenapp 应用发布 （提供由厂商盖章确认的产品界面截图证明）
17.	资源管理	可以对数据中心、业务系统、操作系统和设备类型等信息进行自定义设置，用户登录管理资源一目了然。支持根据客户部门功能性质的不同支持创建无限制的分支类别，超强的细粒度，使资源以更加简单的方式呈现给运维管理人员。
18.		系统支持对不同被管理设备的运维端口或协议当前是否正常可用的监测机制即健康检查
19.	端口管理	支持一个账号使用不同端口管理授权方式，如 Telnet 协议使用 admin 账号登录，端口 23 为管理端口，2223 端口为监控端口等等。对于协议/ 客户端可使用非著名端口进行配置访问，避免了资源设备的安全漏洞，加固了资源设备安全。
20.	工具管理	支持一个资源有多种不同运维工具管理的模式。如：支持带内 RDP 管理方式，支持带外浏览器管理方式，同时也支持虚拟应用管理方式，多种方式可以同时存在和运行；
21.	审批机制	支持手动或者自动管理审批流程（提供由厂商盖章确认的产品界面截图证明）
22.	单点登录	1. 支持终端类用户名及密码的代填：SecureCRT、Openssh、Xshell、Putty、Telnet 等程序，不受程序类型限制。支持二次及更多代填次数功能。 2. 支持对窗口类用户名及密码的代填：Filezilla、PCAnywhere、SQLClient、PLSQL、OracleClient 等，不受程序类型限制。

		3. 支持对远程桌面类用户名及密码的代填 ：RealVNC、TightVNC、Windows RDP、VNCviewer 等，不受程序类型限制。 4. 支持对虚拟客户端用户名及密码代填：Citrix ICA、Windows RemoteApp、VMware vsphere/vcenter/vmplayer。 5. 支持各类 B/S 架构系统用户名及密码的代填。 6. 应支持在主帐号登录完成后,只能够访问已被授权的被管资源。 7. 支持自助式用户和密码代填，无需管理员参与设置。 8. 支持 SAP 客户端用户、密码和 IP 地址代填 9. 支持 Navicat 工具基于 oracle、mysql 管理用户和密码代填 10. 支持客户端针对应用实现自助式用户和密码代填 （提供由厂商盖章确认的产品界面截图证明）
23.	▲改密功能	1. 支持针对操作系统改密：操作系统，包括：Windows/AD 系列、UNIX/Linux 系列、AIX 系列、HPUX、COSLinux、SCO 系列、麒麟 linux、银河 linux、中标 linux、RedHat 系列、Centos 系列、Tru64、NonStop、ESX、Citrix Server、OVMS 等等； 2. 网络设备改密：网络设备，包括：CISCO、HUAWEI、H3C、迈普、Juniper、中兴、锐捷、神州数码、D-LINK、联想等等； 3. 安全设备改密：安全设备，包括：天融信、绿盟科技、山石网科、中科网威、飞塔、启明星辰、网神、锐捷网络、迪普科技、安恒、网御星云、paloalto、东软、网康、梭子鱼、CheckPoint 等等； 4. 数据库改密:数据库,包括:Oracle、MSSQL、DB2、informix、Sybase、Mysql 和 Any ODBC 修改密码的方式； 5. Web 应用改密：Web 应用，包括：静态网页和动态网页密码修改，如：OA、SAP、Mail、ERP、SAP 等等，针对 WebLogic Web 改密；

		6. 目录服务器改密:目录服务器,包括:Windows AD、SunOne、Novel、UNIX NIS、FreeIPA、 OpenLDAP、FreeLDAP 等等,针对 FreeIPA; 7. 中间件改密：中间件，包括：Jboss、Tomcat、WebLogic、WebSphere 以及包括部署修改集群密码等等，针对 Tomcat 与 Mysql 改密集成和传递; 8. KVM 带外管理改密:KVM,包括:HMC、HPiLO、ALOM、Raritan、DRAC 等等; 9. 服务类型改密：服务（service）类型，包括：COM+ Application、Windows Service、Windows ScheduledTasks、IIS AppPools、IIS Anonymous、Database String、INI File、Text File、Web File、Windows Registry、XML File 等等。 10. 支持自定义平台特权账号密码修改。 （提供由厂商盖章确认的产品界面截图证明）
24.	数据安全	系统支持简便的备份功能，自定义需要备份的内容，例如用户、应用程序、被管理设备、授权关系。可方便的进行系统恢复，保证整个系统的安全、稳定的为运维人员提供服务。
25.	▲审计功能	1. 支持图形和键盘输入信息审计; 2. 支持程序应用、网站访问、电子邮件、即时通讯及文件访问的分类图形审计; 3. 支持多种接入方式，操作审计无盲点（本地操作、Citrix ICA、Microsoft RDP 等）; 4. 支持按照用户操作行为审计; 5. 支持可选择用户或用户组方式审计(选择或者排除方式); 6. 支持多种服务器虚拟化平台：包括 Citrix XenServer、VMWare ESX、Microsoft Hyper-V; 7. 支持审计视频大小调整; 8. 用户可根据具体的用户名、时间、IP 地址等查询、定位操作日志;

		9．支持图形标题关键字查询； 10．支持键盘输入信息关键字查询，支持通过检索输入信息可定位到相应的图形审计日志。 11．具有检索功能的图形审计。（可以检索到用户在某段时间中做的具体内容，准确定位，避免图形审计回放需要从头到尾查看） （提供由厂商盖章确认的产品界面截图证明）

5.2.1.1 成果物要求

- 《零信任系统实施方案》
- 《零信任系统试运行报告》
- 《零信任系统设备拓扑》
- 《零信任系统培训记录》
- 《零信任系统验收报告》
- 《零信任系统使用手册》

5.2.2政务网边界防火墙

防火墙设备部署于政务网边界同时对接多套外部网络,功能要求至少等于或高于以下要求：

序号	指标项	技术指标
1	基本要求	标准1U设备,单电源；至少提供10个千兆电口、4个千兆SFP插槽、2个USB接口、1个RJ45 Console口、1块64G SSD硬盘；
2	性能要求	系统吞吐量≥8Gbps,IPS吞吐量≥5Gbps,防病毒吞吐量≥3Gbps,应用层吞吐量≥6Gbps；最大并发连接数≥400万，每秒新建连接数≥5万，SSL VPN用户数≥200，IPSec VPN隧道数≥20000；
3	操作系统	▲支持多系统（≥3个）引导，可在WEB界面上直接配置启动顺序，除恢复系统之外，还可在WEB界面完整备份当前系统，可导入导出配置各类文件，提供相关功能截图；
4		▲采用安全网关节能技术，设备通过了RoHS认证，提供相关证明文件
5		系统采用多核多线程并行操作系统和加速操作系统，提供软件著作权登记证书
6	网络适应性	▲支持透明、路由、混合等多种工作模式，具备基于桥的二层交换式防火墙包过滤能力，提供国家第三方机构（如：中国信息安全测评中心、公安部信息安全产品检测中心、国家知识产权局、中国网络安全审查技术与认证中心、国家版权局等国家权威机构）出具的相关证明文件；
7		支持针对策略中的源、目的地址进行新建、并发限制，可以针对单IP(或地址范围)进行新建、并发控制；
8		支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路
9		支持数据防泄密功能，可针对SMTP协议主题、正文的敏感信息检测，支持对HTTP协议POST数据的消息体的敏感信息检测，支持对FTP协议上传下载文件内容的敏感信息检测；
10	安全防	▲支持一体化安全策略配置,可通过一条策略实现用户认证、IPS、

	护功能	AV、URL 过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能，提供具有 CMA 或 CNAS 认证的第三方检测报告；
11		支持漏洞扫描功能，支持后门、文件共享、系统补丁、IE 漏洞等主动式扫描；
12		系统缺省含不少于 200 个 SSL VPN 授权，设备具备基于 SSL 协议的远程安全接入能力；
13	入侵防护	支持入侵场景保留，可记录入侵行为相关的网络数据报文，报文可保存至 U 盘或某台内网服务器；
14		内置入侵防御特征库，特征规则数量不少于 7000 条，特征库可按分组进行管理，可自定义入侵攻击和应用软件的特征，提供截图证明；
15		支持 HTTP 类攻击重定向功能，能够把 HTTP 协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析；
16		▲采用业界领先的入侵检测技术，提供国家第三方机构出具的加快旁路入侵检测的方法的技术证明文件；
17	防病毒	支持基于策略的病毒扫描与防护，可针对不同的源目 IP 地址、源 MAC 地址、服务、时间、安全域、用户等，采用不同的病毒防护策略，提供截图证明；
18		支持配置多个不同的防病毒引擎，提高病毒检测效率
19		支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个接口、多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境；
20		支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性；
21	抗拒绝服务攻击	▲支持专业的 DNSflood 攻击防护，具有高级的基于聚类限速、聚类分析、重传检测等多种高级防护算法，提供具有 CMA 或 CNAS 认证的第三方检测报告；
22		支持专业的 HTTP Flood 攻击防护，可以实现 get 和 post 的攻击

		防护，且 get 防护算法支持 4 类；支持独立 url 处理动作；以上防护功能均可以基于聚类分析、可信度、回探等多种防御机制；
23		支持 WEB 界面下对攻击流量进行抓包分析，支持自定义抓包参数，至少包括数据报文长度、报文数量、抓包时间及采样频率等基本参数；
24	负载均衡	支持多种（≥10）服务器负载均衡算法，提供服务器负载均衡防火墙系统软件著作权登记证书；
25	反垃圾邮件	支持垃圾邮件智能学习，从已检测出的垃圾邮件内容中提取特征，增强后续对相似垃圾邮件的识别能力，
26		支持防邮件炸弹功能，即设置 POP3、SMTP 的连接频率；
27	WEB 安全	支持对 SQL 注入攻击、XSS 跨站脚本攻击、WEB 恶意扫描等 WEB 攻击行为进行防护；
28	安全管理	支持多个（≥3）Syslog 服务器，可自定义日志服务器端口和日志类型；
29	可靠性	支持端口联动，支持上下行端口组的联动，可实现单端口决定同组中的任意接口失效启动链路切换
30		具备网络安全设备及其组成实现高可用性的能力
31		支持集群模式部署，具备在集群模式下实现网络安全设备高可用性能力
32		▲符合 GB/T 17626.5-2008 和 YD/T993-1998 标准，通过了雷击型式试验和浪涌(冲击)抗扰度试验，提供国家第三方机构出具的检测报告；
33	实施与维保服务要求	★实施服务要求：原厂认证工程师现场咨询，安装，配置服务。 维保服务要求：原厂三年维保服务，包含软件升级和硬件保修，远程技术支持，7*24 小时电话支持，邮件支持服务**（请提供原厂授权函）**

5.2.2.1 成果物要求

- 《政务网边界防火墙实施方案》
- 《政务网边界防火墙试运行报告》
- 《政务网边界防火墙设备拓扑》
- 《政务网边界防火墙培训记录》
- 《政务网边界防火墙验收报告》
- 《政务网边界防火墙使用手册》

6 项目服务要求

6.1 技术服务团队要求

1）成交供应商应为本项目提供专业服务团队，该团队包括项目经理和至少四名技术人员。团队所有人员均具有不少于三年网络或信息安全从事经验（成交供应商应提供项目组成员姓名、学历、相关资质、在本项目中的职责及以前参与过的项目情况说明等。），同时，技术人员对采购人现有的安全设备型号具有一定的维护和实施经验，如：熟悉防火墙、堡垒机参数配置、性能优化调整等。

2）成交供应商须保证队伍稳定，并由采购人审核，审核通过后才能参与实施工作；经确认的技术团队，未经采购人同意，不得更换技术人员；成交供应商必须遵守采购人内部各项规章制度和内部操作规程，履行保密义务，签署保密协议，未经批准不得以任何理由泄露任何保密信息和内部资料；技术团队应具备有利于开展实施工作的工具（包括软件和硬件）。

6.2 安全服务技术要求

成交供应商需提供详细的整体服务方案，包括技术方案和实施方案。技术方案包括整体流程、技术方法和服务方案设计等；实施方案包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等。

服务实施过程中所使用到的其他各种工具软件由成交供应商推荐，系统安全维护的定期扫描服务至少使用一款商用扫描系统。成交供应商须承诺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成交供应商负完全责任。

6.3 文档管理要求

成交供应商须按照项目阶段，提供符合采购人文件管理及版本控制要求的项目文档，要求如下：

（1） 记录专门的档案；

（2） 详细记录系统环境、运行状况评估、故障问题报告等信息；

（3） 现场档案与资料的管理，后方档案与资料的管理；

（4） 档案报告交流。

6.4 项目管理要求

成交供应商须根据实际维护服务项目的状况，定期组织汇报与技术交流、紧急情况工作会议，要求如下：

双方技术人员定期（1 次/月）开会，就过去遇到问题情况作总结汇报和交流，确定下一步工作方案，以提高和改善服务质量，并根据需求对服务方案不断进行完善；发现潜在和细小问题，防患于未然；最新产品介绍与业界动态信息；其它用户的经验介绍及分享；举办年度研讨会，对一年的工作作出总结，并为下一年度的工作作出规划。

对于任何紧急情况，如有必要，应协调相关部门负责人、技术人员，无论何时，根据需要召开紧急会议，重点处理紧急问题，以保证重大故障得到及时解决。

6.5 项目服务周期

项目服务周期，自合同签订之日起一年。自签订合同之日起30天内完成零信任系统和政务网边界防火墙的安装调试服务。其他服务内容按第二章第2点《2024年度网络与数据安全服务清单》的要求在自签订合同之日起一年内完成。

6.6 项目售后要求

1）成交供应商应提供切实可行的售后服务方案

2）★成交供应商应提供 7×24 小时运维响应服务，在 10 分钟内响应，30 分钟内派出有能力的技术人员现场处理，同时提供远程和现场两类方式的安全支撑服务，**（需要提供投标人盖章的承诺函）**。

2）▲成交供应商应承诺，如中标后，在服务期内，成交供应商应安排至少一名同时具备以下资质和经验的项目经理：持有CISAW信息安全保障人员认证、CISP注册信息安全工程师等国内行业第三方权威资质认证；在中标后提供该项目经理资质证书及在投标单位近半年任意一个月的社保缴纳记录，应提供投标人盖章的承诺函。

6.7 项目验收要求

1、按照国家相关标准及规范进行验收。相关服务无国家标准时按地方相关

标准或行业规范进行验收。

2、在符合国家相关标准及规范的前提下，服务期满结束后，由成交供应商提起验收申请，15 个工作日内，经招标人同意并签字盖章确认后完成验收。

7 付款方式

合同签订后 15 个工作日内，成交供应商向采购人开具合同金额 30%款项的普通发票，采购人在收到发票后 15 个工作日内向成交供应商支付对应款项。

零信任系统、政务网边界防火墙完成安装正式上线运行后且完成 HIS、PACS、LIS、医院官网四个系统等级保护初测并出具问题清单后，成交供应商向采购人开具合同金额 40%款项的普通发票，采购人在收到发票后 15 个工作日内向成交供应商支付对应款项。

在所有服务项目均完成并通过最终验收后，成交供应商向采购人开具合同金额 30%款项的普通发票，采购人在收到发票后 15 个工作日内向成交供应商支付对应款项。