第五章　采购需求

一、采购标的需实现的功能或者目标，以及为落实政府采购政策需满足的要求

(一)采购标的需实现的功能或者目标：

信息安全等级保护制度是国家信息安全保障工作的基本制度,开展信息安全等级保护工作不仅是加强国家信息安全保障工作的重要内容，也是一项事关国家安全、社会稳定的政治任务。卫生部印发《卫生行业信息安全等级保护工作的指导意见》的通知等文件的要求，提升北京朝阳医院信息安全保障能力，特开展此项目。

（二）为落实政府采购政策需满足的要求

1. 促进中小企业发展政策：根据《政府采购促进中小企业发展管理办法》规定，本项目采购服务由小型或微型企业承接的，投标人应出具招标文件要求的《中小企业声明函》给予证明，否则评标时不予认可。投标人应对提交的中小企业声明函的真实性负责，提交的中小企业声明函不真实的，应承担相应的法律责任。（注：依据《政府采购促进中小企业发展管理办法》规定享受扶持政策获得政府采购合同的小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。）
2. 监狱企业扶持政策：投标人如为监狱企业将视同为小型或微型企业，且所投产品为小型或微型企业生产的，应提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。投标人应对提交的属于监狱企业的证明文件的真实性负责，提交的监狱企业的证明文件不真实的，应承担相应的法律责任。
3. 促进残疾人就业政府采购政策：根据《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）规定，符合条件的残疾人福利性单位在参加本项目政府采购活动时，投标人应出具招标文件要求的《残疾人福利性单位声明函》，并对声明的真实性承担法律责任。中标、成交投标人为残疾人福利性单位的，采购代理机构将随中标结果同时公告其《残疾人

福利性单位声明函》，接受社会监督。残疾人福利性单位视同小型、微型企业。不重复享受政策。

4. 鼓励节能政策：投标人的投标产品属于财政部、发展改革委公布的“节能产品政府采购品目清单”范围的，投标人需提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书。国家确定的认证机构和节能产品获证产品信息可从市场监管总局组建的节能产品、环境标志产品认证结果信息发布平台或中国政府采购网（www.ccgp.gov.cn）建立的认证结果信息发布平台链接中查询下载。

5. 鼓励环保政策：投标人的投标产品属于财政部、生态环境部公布的“环境标志产品政府采购品目清单”范围的，投标人需提供国家确定的认证机构出具的、处于有效期之内的环境标志产品认证证书。国家确定的认证机构和环境标志产品获证产品信息可从市场监管总局组建的节能产品、环境标志产品认证结果信息发布平台或中国政府采购网（www.ccgp.gov.cn）建立的认证结果信息发布平台链接中查询下载。

二、采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

无

三、采购标的的数量、采购项目交付或者实施的时间和地点

（一）采购标的的数量

包号	品目号	标的名称	数量	是否接受进口产品
1	1-1	2024 年网络安全深化项目	1 项	否

（二）采购项目交付或者实施的时间和地点：

1、采购项目（标的）交付的时间：合同正式签订后的 30 天内。

2、采购项目（标的）交付的地点：北京市朝阳区工体南路 8 号、北京市石景山区京原路 5 号。

四、采购标的需满足的服务标准、期限、效率等要求

（一）采购标的需满足的服务标准、效率要求

供应商应完成北京朝阳医院三个三级系统的2024年度等级保护测评服务；

应提供一名网络安全驻场人员提供应急响应及驻场运维服务。

（二）采购标的需满足的服务期限要求

本次采购的网络安全服务期限：签到合同后一年

五、采购标的的验收标准

详见第六章“合同条款”

六、采购标的的其他技术、服务等要求

1、详细采购清单如下：

序号	设备名称	数量
1	等保测评服务	1
2	安全驻场服务	1
3	安全产品续保	1
4	石景山医院态势感知安全服务	1
5	跨网文件传输系统	1
6	出口防火墙	2

2、与朝阳医院现有产品关联：

朝阳医院现有网络安全感知系统（本部）产品	品牌：奇安信网神 型号：TSS10000-GM
朝阳医院现有终端安全管理系统（本部）产品	品牌：奇安信网神 型号：奇安信网神终端安全管理系统
朝阳医院现有堡垒机（石景山院区）产品	品牌:奇安信网神 型号:C6100-BH-TF10
朝阳医院现有态势感知平台（石景山院区）产品	品牌:深信服 态势感知:SIP-1000-B400 探针：STA-100-B420

1. 等保测评服务

（1）背景

信息安全等级保护制度是国家信息安全保障工作的基本制度,开展信息安全等级保护工作不仅是加强国家信息安全保障工作的重要内容，也是一项事关国家安全、社会稳定的政治任务。卫生部印发《卫生行业信息安全等级保护工作的指导意见》的通知等文件的要求，提升北京朝阳医院信息安全保障能力，特开展此项目。

（2）服务目标

2.1 完成北京朝阳医院“HIS 系统”、“互联网医院系统”和“集成平台”三个三级系统的安全基础调研和等级保护差距分析工作。

2.2 完成北京朝阳医院三个三级系统的等级保护方案设计。

2.3 完成北京朝阳医院三个三级系统的 2024 年度等级保护测评工作，并出具《系统安全等级测评报告》。

（3）服务内容及要求

3.1 安全调研及等保差距分析服务

安全服务商针对确定范围内的三个三级系统进行安全调查，并完成三个三级系统等级保护的差距情况调查和差距分析。

调研分为信息安全管理部分和信息安全技术部分。其中信息安全管理部分至少包括制度体系、安全组织、人员安全、系统建设安全管理、系统运维安全管理五个部分。技术部分至少包括物理环境与设备安全、网络安全、主机安全、数据安全和备份恢复。

调研完成后提交《差距分析报告》，说明目前的安全状态和所存在的差距。其中差距至少包括与等级保护要求的差距。

3.2 信息安全等级保护方案设计

在完成三个三级系统安全基础调研、差距分析、风险评估的基础上，依照等级保护和风险评估的要求，结合医院实际情况，进行安全保障体系基本框架和等级保护方案的设计工作。并协助北京朝阳医院组织专家对方案、北京朝阳医院信息系统安全等级定级等进行评审。

信息安全体系基本框架和等级保护方案的设计至少包括信息安全技术体系和信息安全管理体系两大部分。其中信息安全技术体系部分至少包括物理环境与设备安全设计、网络安全设计、主机安全设计、应用安全设计、数据安全与备份恢复设计，应用系统程序开发安全规范设计。信息安全管理体系部分至少包括信息安全制度体系、安全组织、人员安全、系统建设安全管理和系统运维安全管理。信息安全体系设计方案需要依据医院的实际情况进行合理的安全能力配置，防止出现安全能力空白、能力配置不足或者能力误配的情况。

编写信息安全体系文档，包括技术体系文档和管理体系的文档。文档需要通过相关等级保护主管部门和单位及等级保护专家的评审。

3.3 等级保护测评

在项目完成系统整改、上线前检测、安全加固等工作，进入试运行阶段，安全服务商应协助用户单位通过专业安全测评机构对系统的等级保护测评，并出具测评报告。

3.4 其他服务及培训

安全服务商应协助医院进行安全规划与安全事故的调查，参与安全评审，提供预防性的安全建议，并为我医院接受监管部门信息系统安全方面的检查提供必要的技术支持和建议。安全服务商应无偿作为我医院的技术支持单位。

2. 安全驻场服务

（1）应急响应服务

1.1 服务范围

应急响应服务范围通常为客户现场发生信息破坏事件（篡改、泄露、窃取、丢失等）、大规模病毒事件、网站漏洞事件等信息安全事件时，由投标方提供应急响应专家协助处置现场突发安全事件。其中，应急响应事件服务范围具体包括以下内容：勒索病毒、挖矿木马、蠕虫病毒、APT 事件、网站挂马、网站暗链、网站篡改、漏洞事件、数据泄露以及其他安全事件。

1.2 服务内容

服务内容：建立网络安全应急响应体系，及时响应网络全突发事件，确保在15 分钟内响应，2 小时内到达问题现场，4 小时以内处置安全事件。在应急响应完成后，及时总结网络安全事件原因，提出预防和改进建议，并出具应急响应报告。

1.3 服务频率：一年一次。

（2）驻场运维服务

2.1 人员要求

2.1.1 通用基本技能：

2.1.1.1 基础数据库 SQL，备份操作。

2.1.1.2 基础 Windows、Linux 操作系统安装及配置。

2.1.1.3 基础路由器、交换机、防火墙、网闸设备的配置。

2.1.1.4 掌握安全产品在安全能力实现方面的基本原理。

2.1.2 终端专业技能:

2.1.2.1 终端基本的物理故障、系统故障、软件故障排查思路。

2.1.2.2 EPP、EDR 安全产品中的功能和作用。

2.1.2.3 掌握终端杀毒、监控、调试、取证工具的使用。

2.1.2.4 掌握终端杀毒监控、调试、取证工具，排查终端具体故障的方法。

2.1.3 网络专业技能：

2.1.3.1 网络设备的故障排查思路。

2.1.3.2 网络准入、IPS、IDS、WAF、SOC 安全产品的功能和作用。

2.1.3.3 掌握常用流量抓取工具的使用方法。

2.1.3.4 掌握流量分析来排查网路故障的方法。

2.1.4 人员水平要求:驻场运维人员要求至少有 3 年以上工作经验。驻场工程师同时具备 ISO27001、ITIL、CISP 等专业认证证书，需要提供证书复印件并加盖公章。

2.2 服务要求

应具备维护团队，提供驻场服务、7*24 应急响应及技术支持服务，并提供不少于 1 人的常驻场服务人员进行 5*8 运维服务。服务经理负责带领运维团队管理驻地运维工作，需根据 IT 技术发展态势和信息化运维服务体系标准化的需要，提出具有战略性、前瞻性的业务咨询报告和运维评估报告，协助医院不断提高信息化安全工作的效率和质量。

2.3 服务内容

2.3.1 资产配置核查：每季度对服务器、存储、网络设备、客户端、软件等 IT 资产的配置信息进行核查。

2.3.2 终端安全加固：

2.3.2.1 终端安全加固包括：账户策略、补丁策略、安全设置、关闭服务及端口、磁盘分区、网络共享、非法外联、敏感文件、U 盘记录等。

2.3.2.2 及时发现终端存在的安全隐患，提出整改建议并持续改进。

2.3.3 网络服务器保障：

2.3.3.1 开展网络设备和重要服务器的安全检查工作，及时发现网络设备和重要服务器存在的安全隐患，提出整改建议并持续改进。

2.3.3.2 落实“网络安全三同步”要求，对新入网的服务器进行配置核查。

2.3.4 日常运维工作：

2.3.4.1 对安全设备运行进行监控和维护，定期巡检。

2.3.4.2 对终端、网络、应用系统等出现故障及时进行排查工作。

2.3.4.3 对安全设备产生的高、中风险告警进行分析。

2.3.4.4 协助医院通过每年的等级保护安全测评。

2.3.4.5 对突发安全事件进行应急响应。

2.4 输出文档

驻场运维人员需编写及形成的文档具体有：

《故障排除流程报告文档》

《运维周报总结》

《运维月报总结》

《现状安全系统潜在风险及漏洞报告》

《周期性巡检报告》

《安全设备配置、策略整改优化文档》

3. 安全产品续保

（1）网络安全感知系统（本部）产品续保

序号	重要程度	指标项	规格要求	证明材料要求
1		升级要求	针对朝阳医院现有网络安全感知系统 1 年维保服务，服务包含：①1 年系统硬件维保；②1 年规则库和威胁情报升级服务。	否
2	#	威胁感知	应支持以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产	是
3			应支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行攻击带外分析。	否
4			应用安全的细分维度应支持但不限于：WEB 安全、数据库安全、中间件安全、邮件安全系统安全的细分维度应支持但不限于：暴力破解、弱口令、未授权访问、挖矿行为	否
5		威胁情报	应支持基于威胁情报的威胁检测，检测类型支持但不限于 APT 事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报	否
6	#	非常规访问分析	应支持可疑代理分析：能够发现包括但不限于 socks、http、reDuh、Regeory Tunnel、Tunna 等代理类型	是
7			应支持内部资产主机外联分析，能展示资产 ip、外联 ip、外联地域、端口、协议、时间等详细信息，且能自定义源 ip 白名单	否

8	#	策略管理	应支持策略定义，可根据工作流进行处置动作定义，且能根据告警类型、攻击结果、威胁类别进行联动策略定义	是
9	#	联动处置	支持与朝阳医院现有终端安全管理系统进行联动，发现威胁事件后支持与控制中心进行指令下发执行终端隔离和扫描操作。提供系统原厂联动适配承诺函，并加盖系统原厂公章。	是
10	#	原厂售后服务要求	需提供采购方现有网络安全感知系统原厂售后服务承诺。	是

（2）堡垒机（石景山院区）产品续保

序号	重要性	指标项	指标要求	证明材料要求
1		升级要求	针对朝阳医院现有的一台堡垒机设备采购1年软硬件维保服务，包含但不限于：系统版本升级，远程电话、邮件等技术支持，以及紧急问题上门技术支持等服务内容	否
2	#	多因子认证	应支持多因子认证，方式包括手机令牌、手机短信、动态令牌、国密USBKey、指纹识别等多因子认证方式	是
3		用户管理	系统应内置部门管理员、策略管理员、审计管理员、运维员等角色，并支持按模块和功能自定义角色权限，便于管理，用于复杂的业务场景需求；支持角色权限细粒度划分，包括新建部门、安全配置、网络配置、HA配置、端口配置、外发配置、认证配置、工单配置、告警配置、系统风格等权限划分	否
4		协议支持	应支持的运维协议包含但不限于SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin、DM、Redis、PostgreSQL等	否
5		访问控制	支持同时以用户、用户组、账户、账户组为核心要素，来设置多对多的资源访问授权，用户组和账户组内的新增成员可自动继承授权关系	否

6		运维任务	应支持将执行命令、执行脚本和传输文件传操作灵活组合成运维任务，运维任务支持手动执行、定时执行和周期执行	否
7	#	实施监控	应支持对实时会话进行无延时的实时监控和切断	是
8		系统报表	系统应支持内置多种系统报表模板，应支持按用户控制、用户与资源操作、用户源IP数、用户登录方式、异常登录、会话控制、用户状态等维度进行统计，支持按日、周、月为周期，自动生成Word、HTML、Excel和PDF格式的报表	否
9		在线升级	应支持在线升级，系统应支持自动检查并下载最新版本升级包，用户可手动一键升级	否
10	#	原厂售后服务要求	需提供采购方现有堡垒机产品原厂售后服务承诺。	是

（3）态势感知平台（石景山院区）产品续保

序号	重要性	指标项	指标要求	证明材料要求
1		升级要求	针对朝阳医院现有的一套态势感知设备采购1年软硬件维保服务，包含但不限于：系统版本升级，远程电话、邮件等技术支持，以及紧急问题上门技术支持等服务内容。	否
2		规则库升级	态势感知平台及探针需具备最新威胁防御能力，能够自动识别勒索病毒、挖矿病毒等网络病毒并及时给出告警及处置建议。漏洞库、规则库、安全情报库等具备实时更新能力并能够自动更新到最新。	否
3	#	原厂售后服务要求	需提供采购方现有态势感知产品原厂售后服务承诺。	是

4. 石景山医院态势感知安全服务

序号	重要性	指标项	指标要求	证明材料要求
1		首次安全评估	暴露面梳理：投标方应使用安全工具对招标方服务资产开展互联网暴露面探测，以	否

			梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。 提供服务工具具备以上暴露面梳理能力的证明截图；	
2		脆弱性管理	针对服务范围内资产扫描到的高危可利用漏洞，投标方应当为招标方做好每一个高危可利用漏洞的防护工作，包括但不限于为招标方提供漏洞修复方案和安全设备防护策略，以及帮助招标方配置防护规则，保证招标方不因此出现重大事件和损失； 提供服务平台具备高危可利用漏洞防护规则的证明，并且支持对扫描到的高危可利用漏洞能够自动匹配漏洞防护规则；	否
3		威胁管理	为了保证安全监测的准确率和服务质量，投标方应当支持为招标方自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求； 提供投标方服务平台支持为用户自定义配置安全规则的截图；	否
4		7*24H的服务团队	为了保障服务质量和加强投标方与招标方的沟通，投标方应当承诺为招标方配置一名经验丰富的安全专家作为专属服务经理，并且实时响应投标方咨询的网络安全相关问题；	否
5			投标方应当为招标方提供 7*24 小时的安全守护，不论是白天、黑夜、节假日投标方都应该能做到 7*24H 在线服务，并且在节假日期间应当每日为招标方提供《节假日值守总结》 投标方应当向招标方承诺，不论白天、黑夜、节假日投标方都能为招标方提供 7*24H 在线服务，并且在节假日期间能为招标方提供每日的《节假日值守报告》	否
6		安全巡检	应承诺提供合同期间集中安全检测、日常巡检每个月不少于一次	否
7		安全报告	合同签订之日起应承诺每个月应根据甲方的网络与信息等情况出具相应的报告，若有突发的安全事件，应随时出响应的安全报告。	否

5、跨网文件交换系统（1 套）

序	重要性	指标项	指标要求	证明材料

号				要求
1		基础架构要求	系统服务端应支持部署在 Linux 操作系统，应支持国产服务器和国产操作系统，应支持物理机和虚拟机部署。终端用户应支持使用通用浏览器访问，不限桌面操作系统平台。	否
2		用户和权限管理	应支持按树状结构管理多级组织架构和用户账号。	否
3	#		应支持 LDAP/AD 用户集成，应支持用户账号自动同步和统一身份认证。	是
4	#		应支持分级管理和三员分离管理模式，应支持超级管理员、分级管理员、系统管理员、安全保密员、安全审计员等多种平台管理和安全管理角色。	是
5		工作空间管理	系统应支持创建多个逻辑独立的工作空间，用于面向不同的网域、部门、项目等，各自独立开展文件管理和安全管控，提供具备经 CNAS 认可的实验室出具的功能检测报告；	否
6			各工作空间应支持独立配置文件存储位置、总体存储容量、个人存储容量、归档路径、归档容量、归档加密和压缩等存储参数。	否
7			应支持开启或关闭网盘、文件邮、收集箱、中转站等应用功能，并配置有效期、文件限制、提取次数、通知等各项具体应用功能参数。	否
8	#		应支持工作空间管理员开启或接受与其他工作空间之间的文件投递策略，未经许可，不同工作空间之间不能够进行文件交换。提供经CNAS认可的实验室出具的功能检测报告；	是
9	#	用户文件管理	用户在具备权限的工作空间内应支持拥有个人文件存储空间，用户可管理文件目录结构，上传、下载、移动、删除个人文件。	是
10	#	跨网文件摆渡	系统应支持以跨网中转站形式提供独立的跨网文件摆渡功能和区域，终端用户可在安全规则控制下，自主进行跨网文件摆渡，无需系统管理员协助。跨网中转站独立于个人存储空间，不同用户的中转站相互隔离。	是
11			应支持每次跨网文件摆渡产生一个文件批	否

			次，支持多个文件、文件夹，每个批次可指定摆渡投递的目标网络和工作空间。	
12			应支持根据预先定义的安全策略和审核规则，跨网文件摆渡可以触发不同的审批流程，审批通过后，文件才能够进行网域之间或工作空间之间的物理转移。	否
13	#		跨网摆渡的文件在过期失效后，应支持根据预先配置的策略进行自动清理，以释放存储空间。	是
14		文件共享协作	工作空间内应支持创建和维护多个文件库，应支持分别配置每个文件库的存储路径、存储容量，可将用户、用户组或部门设定为文件库的授权用户范围，应支持为不同用户分配不同的文件库读写访问权限。	否
15			应支持对办公文档、图片等文件类型开启预览水印，用户在线预览文档时强制显示用户名、时间等水印覆盖，支持自定义水印内容	是
16	#	文件安全	接收者提取文件时，系统应支持自动对文件进行水印添加，水印包括但不限于文件被提取的时间，用户所属部门、手机号码、邮箱、姓名等,文件类型支持但不限于 doc，docx，pdf，xls，xlsx，ppt，pptx，wps，wpt，dot，dps，dpt，pot，pps，xlt，et，ett、jpg， bmp，gif，tif、html，	是
17	#	文件交换审核	应支持内置审批流程引擎，支持不限层级的审批流程，支持按用户或角色配置审批权限，支持会签、或签。	是
18			审核全过程应支持自动通知，告知发起人、审核人、抄送人最新审核动态和提醒处理。	否
19		安全保护机制	系统内置自研杀毒引擎，启用后可对用户上传文件自动进行病毒检测，病毒文件将被自动隔离	否
20			应支持管理员根据实际使情况，可对疑似病毒文件进行加白处理，加白以后，用户可正常投递该文件	否
21	#	断点续传	文件上传、下载和网间摆渡过程均应支持断点续传，异常中断恢复后，可自动接续已经传输的部分继续传输。	是
22		日志审计	系统应具备全平台级别的完整的日志记	否

			录，对用户登录行为、用户和组织修改、空间配置调整、应用功能配置调整、组件运行状态变化等动作均进行了全面记录，便于检索、审计和异常问题的定位排除。	
23	#	维保及售后服务承诺	提供三年软件系统升级维保服务，需提供原厂售后服务承诺	是

6、出口防火墙（2 台）

序号	重要性	指标项	指标要求	证明材料要求
1	★	接口要求	千兆电口≥12，万兆光口≥12；	否
2	#	硬件架构	设备形态 1U；采用多核架构；支持交流双电源；支持风扇可插拔（提供证明截图）；支持前后风道（提供证明截图）	是
3	★	性能要求	防火墙吞吐量≥40Gbps，最大并发连接数≥1200 万，每秒新建连接数≥40 万	否
4		策略管理	支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维。	否
5	#		支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议	是
6			支持与 firemon 对接，实现策略的命中，冗余分析及风险调优	否
7	#	入侵防御及病毒防护	系统预定义 IPS 签名数量≥8000，支持用户自定义签名规则，支持正则表达式，病毒库数量≥500W	是
8			支持基于场景进行策略入侵防御的模板定制。	否
9			支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。	否
10	#		支持恶意域名过滤，实现对 C&C 进行阻断。（提供功能截图）	是
11		负载均衡	针对多链路出口场景，支持智能 DNS 功能、透明 DNS 功能、动态 DNS 功能，支持会话保持，满足多链路的负载均衡	否
12			可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式	否

13		可靠性	支持 BFD 链路检测，支持 BFD 与 VRRP 联动实现双机快速切换，支持 BFD 与 OSPF 联动实现双机快速切换。	否
14			支持 HA 平滑升级，升级窗口中支持不同版本的软件形成双机热备	否
15		路由特性	全面支持 IPV4/IPV6 下的多种路由协议，如 RIP、OSPF、BGP、IS-IS、IPv6RD、ACL6 等。	否
16	★	实配	实配千兆电口≥12，万兆光口≥12，万兆多模光模块≥12 个，万兆单模光模块≥6 个；支持 IPSec 最大连接数为 15000 个，SSL VPN 并发用户数授权 100 个，威胁防护授权（IPS、AV、URL、云沙箱）≥3 年。	否