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**

本项目为采购人购买北京协和医院网络信息安全服务。

**（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，本项目服务为小型或微型企业提供的，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，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、成交供应商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** | **品目名称** | **数量** |
| 1 | 1-1 | 网络信息安全保障服务 | 1项 |

**（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：合同签订之日起1年。
2. 采购项目（标的）交付的地点：中国医学科学院北京协和医院指定地点

**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**

详见七、采购标的需满足的质量、安全、技术规格、物理特性等要求

**（二）采购标的需满足的服务期限要求**

本项目服务期限为自合同签订之日起1年。

**五、采购标的的验收标准**

符合采购人的验收标准。

**六、采购标的的其他技术、服务等要求**

投标人需提供整体技术方案、项目实施与组织进度管理方案、项目人员安排方案

**七、采购标的需满足的质量、安全、技术规格、物理特性等要求：**

# 1、项目背景

近年来采购人信息系统应用规模日益扩大，随着互联网应用的增多，面临的网络安全风险也日益严峻。

国卫办规划函[2017]820号《国家卫计委办公厅关于全民健康网络与信息安全情况的通报》提出：“随着国际网络空间博弈越发激烈，针对关键信息基础设施和政府部门的网络攻击事件频发，网络安全环境更加复杂。卫生行业信息涉及社会全人群、生命全周期，安全形势更加严峻”“可参考其他行业的做法，选择安全工作经验丰富、技术实力较强、符合资质要求的企事业单位参与安全建设”

为提升网络信息安全，拟通过选择性外包、非核心工作服务外包方式，选择安全工作经验丰富、技术实力较强、符合资质要求的企事业单位参与医院安全建设，加强网络和数据安全日常管理，提升网络安全风险感知、分析、处置能力，提高重大事件和应急响应保障力量。

# 2、服务内容

**2.1工作时间**

按采购人工作时间进行考勤，特殊时期服从采购人工作安排。

**2.2服务内容**

根据北京协和医院网络信息安全服务项目要求和工作内容，按照北京协和医院网络信息安全主管领导要求明确工作计划和工作安排，提供针对性的管控方案和建议，持续开展监控、分析、应急响应、风险评估、安全整改等工作，落实并完善相关制度和基线要求，持续提升北京协和医院网络和数据安全防护和运营水平。

服务期限：合同签订之日起1年。

**2.3服务交付物**

协助北京协和医院提升安全保障能力。落实相关领域安全专项职责，提升软件、终端、网络和服务器、私有云相关IT运维团队的安全意识和安全能力，确保已发现的安全风险能够得到整改；处理网络安全事件，形成专项报告，交付文档包括但不限于：

|  |  |  |
| --- | --- | --- |
| 序号 | 主要交付内容 | 备注 |
| 1 | 《北京协和医院网络安全设备资产清单》 | 每月 |
| 2 | 《北京协和医院信息系统资产核查报告》 | 每季度 |
| 3 | 《北京协和医院网络安全工作周报》 | 每周 |
| 4 | 《北京协和医院X月XX安全事件专项报告》 | 发生时 |

# 3、其他技术、服务等要求

**3.1.安全保障服务**

**1）安全监控服务**

|  |  |
| --- | --- |
| 服务项 | 具体工作内容 |
| 网络安全监控 | 网络安全风险监测，负责管理全院安全监测类设备和系统，包括但不限于态势感知系统、入侵检测系统、蜜罐、主机安全等系统。 |
| 网络安全风险分析，具备安全事件风险分析判定能力，掌握各类安全事件特征，能准确判断安全事件真实性和攻击结果。 |
| 网络安全风险处置和上报，具备常见安全事件处置能力，输出分析报告见并按照安全事件响应机制完成上报流程。 |
| 态势感知类平台的运行维护工作，含设备日常维护、故障排查、资产管理、关联规则创建和优化工作。 |
| 网络安全监控工具 | 提供态势感知软件（包含资产安全管理、网络流量监测、安全大数据分析、安全事件联动、可视化功能）、漏洞管理平台等网络安全监控工具，根据现场环境进行定制开发，部署期不超过2个月，服务期间不单独支付费用。 |
| IT生产安全监控 | 医院IT生产安全监控系统运行维护，设备和服务运行状况监控，安全运行告警事件工单闭环管理，监控资产台账维护、告警规则优化调整。 |
| 管理制度和标准 | 根据法律法规标准同步修订北京协和医院信息安全管理相关的制度和规范文件，完善现有信息安全制度体系以及配套的制度文件； |
| 驻场人员要求 | 驻场安全运营工程师一名，本科及以上学历，3年以上相关工作经验。提供毕业证书等证明材料。  若出现驻场人员无法解决的问题，投标人应提供更多二线资源以保证完成项目目标，采购人不单独支付费用。 |

**2）专项保障服务**

|  |  |
| --- | --- |
| 服务项 | 具体工作内容 |
| 资产配置核查 | 每季度对服务器、存储、网络设备、客户端、应用系统等IT资产进行资产梳理和安全配置核查，形成核查报告。 |
| 应用及数据安全专项保障 | 对接应用和数据相关工作，开展应用系统和数据识别和梳理工作，含现有系统和新上系统，明确安全保护对象。开展安全专项保障工作，负责信息系统等级保护管理工作、业务安全建设、应用数据相关安全产品的运营工作,包括但不限于数据防泄漏、数据脱敏、数据库审计等系统。   * + 根据GB∕T 22240-2020 《信息安全技术 网络安全等级保护定级指南》要求，结合北京协和医院实际情况，对应用系统和数据进行重要性分级，协助制定不同安全级别系统的不同保护策略。   + 根据等级保护和风险评估要求，基于医院相关策略文档，落实《北京协和医院网络安全制度汇编》要求   + 开展应用及数据相关的安全检查及复查工作，及时发现应用系统存在的安全隐患，排除数据泄露风险，提出整改建议并促进持续改进；   + 落实“网络安全三同步”要求，完成新入网的应用系统上线材料审查、安全责任书签署等工作；   + 开展重要信息系统和数据安全检查，及时发现安全隐患，并提出整改建议； |
| 网络及边界安全专项保障 | 对接系统后台运维工作，明确网络层面的安全保护对象，开展医院网络整体架构的安全保障工作，负责网关类安全设备及相关安全产品的运维管理工作，包括但不限于防火墙、IPS、WAF等。   * + 落实“网络安全三同步”要求，对新入网的网络设备进行配置核查；   + 网络设备专项检查内容包括但不限于：对操作系统、数据库、网络设备进行安全风险检查，排查高危漏洞并提出整改建议；对网络设备、安全设备的身份权限、访问控制、安全审计、边界保护、入侵防范、设备防护等进行手工配置核查，督促安全整改。 |
| 计算环境安全专项保障 | 对接桌面运维工作，审计并保障相关工作符合安全要求，配合安全风险分析人员进行现场终端检查抽查，负责终端安全管理、服务器安全管理、网络准入系统等相关产品的运维管理工作。   * + 开展服务器安全加固工作，及时发现服务器存在的安全隐患，提出整改建议并促进持续改进；   + 开展终端相关安全检查及复查工作，包括终端安全准入、防病毒等，及时发现终端存在的安全隐患，提出整改建议并促进持续改进；   + 终端审计与取证：及时发现失陷主机，保持并维护现场，进行恶意样本提取形成分析证据。   + 终端专项检查：包括但不限于工作用手机终端、PDA、笔记本电脑、医疗设备、医护工作站电脑、打印机等。   + 终端和服务器专项检查内容包括：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。并提出整改建议并形成专报，并保障相关工作符合安全要求并能够持续改进； |
| 制度完善 | 根据法律法规标准同步修订北京协和医院网络安全管理相关的制度和规范文件，协助医院信息中心完善标准操作流程，提出合理化建议，形成良好的PDCA循环。 |
| 信息系统项目建设 | 全过程参与北京协和医院信息系统项目建设，在规划、设计中给出专业建议，对不符合安全要求的建设过程及时提出整改意见。 |
| 整改追踪 | 逐项落实《北京协和医院安全整改通知》和历次安全检查中发现的问题，督促相关技术人员进行整改，对整改进度进行追踪，对超出整改时限的，按照院方要求落实关停措施。对整改效果负有最终责任。 |
| 安全项目建设 | 协助开展网络安全建设项目，配合网络安全相关新产品、新技术的探索与实践。 |
| 漏洞消控 | 协助渗透测试人员进行全网漏洞扫描、配置检查等；协助相关软硬件厂商进行安全整改，必要时配合进行安全配置操作，确保排除安全风险。 |
| 二线支持 | 投标人拥有技术能力较强的二线技术支持团队，至少需要5-7人，具有丰富的网络安全实战攻防能力，作为主力队员参与过国家级攻防演习活动，拥有渗透测试、APP检测能力、源代码审计能力等，具备CISP-PTS（渗透测试专家）、CISP-IRS（应急响应专家）、等级保护高级测评师等主流网络安全相关高级认证证书。 |
| 发生应急事件或重大活动期间，二线人员应按采购人要求提供现场支持服务，累计不少于20人/天。 |
| 远程保障服务 | 围绕资产、漏洞、威胁、事件，提供7\*24小时远程保障服务，协助医院构筑不间断的安全运营能力。 |
| 驻场人员要求 | 安全保障工程师（网络&边界防护方向）一名，本科及以上学历，6年以上相关工作经验，具备CISP、PMP证书。  安全保障工程师（应用&数据方向）一名，本科及以上学历，3年以上相关工作经验。具备CISP证书。  安全保障工程师（服务器&终端方向）一名，本科及以上学历，3年以上相关工作经验。  以上需提供毕业证书等证明材料。  若出现驻场人员无法解决的问题，投标人应提供更多二线资源以保证完成项目目标，采购人不单独支付费用。 |
| 驻场人员中项目经理应具备3年以上项目管理经验，提供劳动合同。 |

**4、绩效考核**

投标人应遵守医院各项规章制度，以诚信的态度，尽最大努力，为采购人提供优质服务。

如果采购人认为投标人提供的服务人员在工作中未完成工作量或因工作疏忽造成采购人损失，采购人有权从应支付给投标人的费用中扣除相应的款项。如：处理安全事件时造成可用性次生事故、督促安全整改不力等，出现一次扣合同金额的2%，以后每出现一次，在上一次扣款额度上，增扣合同金额的1%。

如果采购人认为投标人提供的服务人员在工作中未尽到应有的注意义务或无法胜任工作，采购人有权要求投标人更换。投标人有责任在一周内提供合适的候选人供采购人挑选并上岗工作，变更后人员资质不应低于变更前的人员。若不能达到以上要求，每发生一人次，应扣除合同金额的2%。

投标人应尽力保障驻场人员的稳定性。因投标人原因（包括员工离职）造成驻场人员变更的，投标人应提前30天提出书面离职申请，并在一周内提供合适的候选人供采购人挑选并上岗工作，变更后人员资质不应低于变更前的人员。若不能达到以上要求，普通驻场人员每变更一人次，应扣除合同金额的2%，驻场项目经理每变更一次扣除合同金额的5%。

采购人可根据具体工作要求对投标人人员进行月度或季度考核，甲乙双方应按月度以月报的形式对考核结果确认。若考核结果为不合格，应限期整改，整改后仍不合格的，采购人有权从应支付给投标人的费用中扣除相应的款项。

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**

本项目为采购人购买北京协和医院网络信息安全服务。

**（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，本项目服务为小型或微型企业提供的，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，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、成交供应商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** | **品目名称** | **数量** |
| 2 | 2-1 | 网络信息安全风险分析服务 | 1项 |

**（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：合同签订之日起1年。
2. 采购项目（标的）交付的地点：中国医学科学院北京协和医院指定地点

**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**

详见七、采购标的需满足的质量、安全、技术规格、物理特性等要求

**（二）采购标的需满足的服务期限要求**

本项目服务期限为自合同签订之日起1年。

**五、采购标的的验收标准**

符合采购人的验收标准。

**六、采购标的的其他技术、服务等要求**

投标人需提供整体技术方案、项目实施与组织进度管理方案、项目人员安排方案

**七、采购标的需满足的质量、安全、技术规格、物理特性等要求：**

# 1、项目背景

近年来采购人信息系统应用规模日益扩大，随着互联网应用的增多，面临的网络安全风险也日益严峻。

国卫办规划函[2017]820号《国家卫计委办公厅关于全民健康网络与信息安全情况的通报》提出：“随着国际网络空间博弈越发激烈，针对关键信息基础设施和政府部门的网络攻击事件频发，网络安全环境更加复杂。卫生行业信息涉及社会全人群、生命全周期，安全形势更加严峻”“可参考其他行业的做法，选择安全工作经验丰富、技术实力较强、符合资质要求的企事业单位参与安全建设”

为提升网络信息安全，拟通过选择性外包、非核心工作服务外包方式，选择安全工作经验丰富、技术实力较强、符合资质要求的企事业单位参与医院安全建设，加强网络和数据安全日常管理，提升网络安全风险感知、分析、处置能力，提高重大事件和应急响应保障力量。

# 2、服务内容

**2.1工作时间**

按采购人工作时间进行考勤，特殊时期服从采购人工作安排。

**2.2服务内容**

根据北京协和医院网络信息安全服务项目要求和工作内容，按照北京协和医院网络信息安全主管领导要求明确工作计划和工作安排，提供针对性的管控方案和建议，持续开展渗透测试、代码审计检测等工作，持续提升北京协和医院安全风险分析和处置能力。

服务期限：1年。

**2.3服务交付物**

交付文档包括但不限于：

|  |  |  |
| --- | --- | --- |
| 序号 | 主要交付内容 | 备注 |
| 1 | 《北京协和医院渗透测试报告》 | 每半年 |
| 2 | 《北京协和医院安全整改通知书》 | 每月 |
| 3 | 《北京协和医院XX系统源代码审计报告》 | 发生时 |

# 3、其他技术、服务等要求

**3.1.安全风险分析服务**

|  |  |
| --- | --- |
| 服务项 | 具体工作内容 |
| 渗透测试服务 | 以攻击方视角发现信息系统存在的问题，每半年进行一次全面的渗透测试检查，并按资产清单出具报告。  覆盖信息系统对应的所有服务器存储、网络设备、安全设备。涵盖本年度新上线系统。 |
| 模拟真实攻击方法，可远程与现场检测相结合，但不得使用破坏性攻击手段。 |
| 服务内容包含初测、复测、整改协助。  初测是指渗透人员在不同的位置（比如从内网、从外网等位置）利用各种手段对某个特定网络进行测试，以期发现和挖掘系统中存在的漏洞。  复测是指渗透人员对以往被测系统测出的漏洞进行二次测试，记录系统的修复情况，并将此业务系统进行交叉测试，更全面的发现系统的问题。  整改协助是指导帮助应用系统厂商工程师完成漏洞整改任务，包括整改报告的解读、线上回答应用系统工程师问题等。 |
| 现场服务累计不少于50人/天。 |
| 代码审计服务 | 针对本年度新上线系统开展代码审计工作，出具《北京协和医院XX系统源代码审计报告》 |
| 风险处置建议 | 利用多渠道收集安全威胁情报、漏洞信息，对新出现的安全威胁及安全事件进行分析、研判，协助开展院内排查，结合排查情况给出安全建议并协助修复漏洞。 |
| 人员能力要求 | 1）项目经理需具有10年以上工作经验，并具有CISSP、CISP、CCSK、PMP等资质证书，同时满足以上资质，且项目经理需具备医疗领域安全服务经验并提供证明。  2）项目组需配备技术专家1名，作为主力队员参加过国家级攻防演练活动。（需提供相关证明）  3）项目组配备其他人员需具备CISP资质证书,且需具备医疗领域安全服务相关经验并提供证明。 |
| 投标人从2019年至今在公安部组织的网络攻防演习中获得过“最佳攻击团队”或者“优秀攻击队伍”奖，从2019年1月1日至今在国内网络安全赛事（强网杯、网鼎杯等国家级赛事）中获奖。提供证明材料。 |
| 事件通报处置 | 对于国家卫生健康委员会、公安网安、网信部门等相关组织下发的网络安全类通报文件，协助进行深度分析，识别可能影响的范围及严重程度，提出安全加固建议并协助加固。 |
| 根据渗透测试结果整理《北京协和医院网络安全整改通知书》。 |

**4、绩效考核**

投标人应遵守医院各项规章制度，以诚信的态度，尽最大努力，为采购人提供优质服务。

如果采购人认为投标人提供的服务人员在工作中未完成工作量或因工作疏忽造成采购人损失，采购人有权从应支付给投标人的费用中扣除相应的款项。如：未能及时发现潜在APT攻击导致网络安全事件、漏查安全漏洞被行业主管部门或安全执法部门通报等，出现一次扣合同金额的2%，以后每出现一次，在上一次扣款额度上，增扣合同金额的1%。

如果采购人认为投标人提供的服务人员在工作中未尽到应有的注意义务或无法胜任工作，采购人有权要求投标人更换。投标人有责任在一周内提供合适的候选人供采购人挑选并上岗工作，变更后人员资质不应低于变更前的人员。若不能达到以上要求，每发生一人次，应扣除合同金额的2%。

采购人可根据具体工作要求对投标人人员进行月度或季度考核，甲乙双方应按月度以月报的形式对考核结果确认。若考核结果为不合格，应限期整改，整改后仍不合格的，采购人有权从应支付给投标人的费用中扣除相应的款项。