

第五章 采购需求

一、采购标的需实现的功能或者目标

本项目为北京急救中心采购网络安全运维服务，投标人需根据项目的采购、技术规格要求，采用满足要求的服务进行投标，服务必须满足项目采购主要技术规格要求，并保证能对选用服务进行很好的实施。

通过本项目的实施，贯彻落实国家网络安全等级保护政策、标准、等级保护相关工作要求；落实国家关于加强等级保护建设，保障重要数据安全和个人网络安全的政策要求，提高北京急救中心整体信息系统可用性、稳定性、安全性，提升安全综合防护能力和风险处置能力，降低信息系统网络安全风险。

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

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

《网络安全等级保护条例》

《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 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）

《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）

《网络安全技术 网络安全运维实施指南》（GB/T45940—2025）

关于印送《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》的函（公网安〔2020〕1960号）

《关于进一步做好网络安全等级保护有关工作的函》（公网安〔2025〕1001号）

《关于对网络安全等级保护有关工作事项进一步说明的函》（公网安〔2025〕1846号）

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	标的名称	数量	是否接受进口产品
1	网络安全运维服务	1 项	否

服务需求清单:

序号	服务名称	单位	数量	备注
1	脆弱性检测	/次	1	针对北京急救中心所有系统。
2	安全加固	/次	1	针对北京急救中心所有系统。
3	渗透测试	/IP/域名	7	针对北京急救中心指定系统。
4	安全威胁监测	/年	1	针对北京急救中心网络环境。服务期提供 7*24 小时服务。
5	风险评估	/次	1	针对北京急救中心指挥调度系统。
6	应急演练	/次	1	/
7	应急预案培训	/次	1	服务期内按需提供。
8	辅助应急预案制定	/次	1	/
9	应急响应	/年	1	服务期内按需提供。
10	安全培训	/批次	1	服务期内按需提供。
11	安全驻场	人/年	4	/
12	安全通告	/次	52	每周通告 1 次。
13	辅助测评	/次	1	针对北京急救中心指定系统。
14	安全巡检	/次	4	每季度进行一次巡检。
15	网络安全资产管理	/次	12	每月进行一次资产台账梳理。
16	应急指挥系统运维保障	/年	1	服务期内按需提供。
17	网站安全监测	/年	1	服务期提供 7*24 小时服务。

(二) 采购项目交付或者实施的时间和地点

1. 采购项目(标的)实施的时间: 合同签订服务期之后, 一年内完成安全服务相关工作。

2. 采购项目（标的）实施的地点：北京急救中心指定的地点。

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要求

1、投标人需要具有丰富的安全实施团队，保证整体项目实施的完整性、安全性、可靠性、保质保量的按时完成。须针对本次项目提供完整的实施进度计划，项目管理计划，要从项目组织架构管理、项目进度管理、质量保证管理等多方面确保项目成功实施。

2、投标人提供的产品或服务，须与本工程的相关单位进行积极主动的合作。中标人必须服从项目单位的统一协调，在实施方案设计、技术支持、运行维护等方面相互配合。

（二）采购标的需满足的服务期限要求

合同签订服务期之后，一年内完成安全服务相关工作

五、采购标的的验收标准：

需提交的验收文件资料包括但不限于：

项目验收申请表；

项目设计方案及工程过程文档；

项目建设合同和有关修改、调整情况的纪要文件；

项目的技术报告和工作总结报告；

项目建设的主要成果技术资料及过程文档。

六、采购标的的其他技术、服务等要求：

（一）详细安全服务技术需求

1、脆弱性检测

序号	指标项	指标规格
1	服务内容	需指派专业技术服务团队对北京急救中心所有系统，通过手工脆弱性检查和使用漏洞扫描工具进行全面深入的脆弱性检查。
#2	服务要求	投标人需具备有效的国家计算机网络应急技术处理协调中心颁发的国家信息安全漏洞共享平台（CNVD）支撑单位证书

		(需提供复印件并加盖投标人公章)
3	服务范围	北京急救中心所有系统。
4	服务期限	1 年。
5	服务频次	服务期内针对北京急救中心所有系统提供 1 次。
6	服务成果	《信息系统网络安全脆弱性检测及分析服务报告》。

2、安全加固

序号	指标项	指标规格
1	服务内容	在对北京急救中心数据和信息技术科机房涉及网络信息系统脆弱性检测的基础上提出并完善安全加固方案，经过北京急救中心数据和信息技术科批准后，由相应的信息系统承建单位实施安全加固操作，系统安全加固实施后由安全工程师审查加固实施情况，进行安全加固补遗工作，保障北京急救中心数据和信息技术科信息系统的安全运行，排除安全隐患。
2	服务范围	北京急救中心所有系统。
3	服务期限	1 年。
4	服务频次	服务期内针对北京急救中心所有系统提供 1 次。
5	服务成果	《信息系统网络安全加固服务报告》。

3、渗透测试

序号	指标项	指标规格
1	服务内容	对北京急救中心指定系统进行受控的、非破坏性的渗透测试，提前发现应用系统的隐患及漏洞，为加固整改提供技术依据，以切实保证信息系统安全。 提供的渗透测试服务方案须包括但不限于 1、渗透测试目标和内容； 2、渗透方法和流程； 3、渗透测试须采用国内外商业检测工具或自有检测工具。
2	服务范围	北京急救中心 7 个 IP/域名。
3	服务期限	1 年。

4	服务频次	服务期内针对北京急救中心 7 个 IP/域名提供 1 次。
5	服务成果	《北京急救中心渗透测试服务报告》。

4、安全威胁监测

序号	指标项	指标规格
1	服务内容	投标人使用 APT 监测工具，实时抓取分析用户网络中的流量，采取异常网络行为分析、入侵攻击检测和沙箱检测等多种技术手段，结合威胁情报利用，进行网络安全威胁监测；将各类引擎检测结果进行相互关联，以进一步提升威胁监测成果质量；通过威胁监测，为威胁取证和场景溯源提供必要支撑，让网络运营者真正看清风险、实现网络安全管理简单化、实战化。
2	#服务要求	投标人需具备有效的中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（需提供复印件并加盖投标人公章）
3	服务范围	北京急救中心机房本地网络环境。
4	服务期限	1 年。
5	服务频次	服务期内按需提供。
6	服务成果	《北京急救中心网络环境安全威胁监测服务报告》。

5、风险评估

序号	指标项	指标规格
1	服务内容	需从技术、管理和人员等多个方面，包括网络安全技术架构、网络/安全设备性能和策略、主机（包括操作系统和数据库）安全策略、信息系统安全机制和策略以及安全管理制度方面，查找受保护的信息系统和关键资产存在的脆弱性，分析其面临的威胁和安全措施的有效性，明确保护重点。从资产重要性、脆弱性严重程度和威胁发生频率等方面分析北京急救中心数据和信息技术科信息系统面临的风险，为后续信息系统安全加固以及整改提供客观数据，为建立信息安全保障体系提供决策依据。

2	服务范围	北京急救中心 120 指挥调度系统。
3	服务期限	1 年。
4	服务频次	服务期针对 120 指挥调度系统提供 1 次。
5	服务成果	《120 指挥调度系统风险评估报告》。

6、应急演练

序号	指标项	指标规格
1	服务内容	需根据前期制定的应急预案，结合北京急救中心数据和信息技术科信息系统存在的脆弱性和面临的威胁，制定应急预案演练工作计划，并模拟在北京急救中心数据和信息技术科信息系统及重要设备出现故障等紧急情况下，依据前期制定的应急预案进行处理，其中包括事件的发现、上报、处理等环节。通过演练，使相关方熟悉应急响应流程，提高对安全事件的响应能力；同时验证预案正确性和适用性，进行总结分析，并根据需要对应急预案进行修订。
2	服务范围	北京急救中心指定的系统范围。
3	服务期限	1 年。
4	服务频次	服务期间提供 1 次。
5	服务成果	根据《北京急救中心网络安全综合应急预案》开展一次演练工作。

7、应急预案培训

序号	指标项	指标规格
1	服务内容	需对北京急救中心系统相关的人员进行应急预案培训，可以使北京急救中心信息系统相关人员及时了解及掌握适当的应急措施，在安全事件发生时，采取适宜的应对措施，降低系统损失时间，降低事件影响。
2	服务范围	北京急救中心所有系统。
3	服务期限	1 年。
4	服务频次	服务期间提供 1 次。
5	服务成果	《北京急救中心网络安全综合应急预案》培训过程文档。

8、辅助应急预案制定

序号	指标项	指标规格
1	服务内容	需要根据北京急救中心数据和信息技术科信息系统及其承载信息的重要性，以及北京急救中心数据和信息技术科业务特点，结合国家和北京市信息安全保障政策要求，制定应急预案，建立应急响应组织以及预防、预警机制，针对信息系统特点和可能的突发性安全事件拟制规范的应急处理流程。
2	服务范围	北京急救中心所有系统。
3	服务期限	1 年。
4	服务频次	服务期间提供 1 次。
5	服务成果	《北京急救中心网络安全综合应急预案》。

9、应急响应

序号	指标项	指标规格
1	服务内容	需要针对北京急救中心数据和信息技术科信息系统提供 7X24 小时技术支持，发生故障须 10 分钟响应，如果不能电话处理，需 2 小时内到达事故现场开展事件事故原因的记录、分析、排查、处置、防御以及恢复等一系列事件响应处置操作，尽快恢复系统的正常运行或采取必要的可控措施防止事态进一步发展，并在事后进一步分析原因，提供详细的事件响应报告。
2	服务范围	北京急救中心所有系统。
3	服务期限	1 年。
4	服务频次	服务期内按需提供。
5	服务成果	《应急响应服务报告》及应急响应服务过程文档。

10、安全培训

序号	指标项	指标规格
1	服务内容	需通过专业、全面的信息安全理论、信息安全实践等课程，全面提高相关人员的安全意识水平和安全技术能力，切实提高用户信息安全管理能力，保证业务系统安全稳定运行。

		1. 帮助北京急救中相关工作人员了解安全策略、掌握信息安全基础知识； 2. 帮助北京急救中相关工作人员熟悉各类安全产品的使用和管理； 3. 帮助北京急救中相关工作人员理解相应安全管理机制和应急保障工作流程等。
2	服务范围	北京急救中心数据和信息技术科相关人员。
3	#培训讲师要求	投标人提供的培训讲师需具备工业和信息化人才专业知识测评证书，提供证书复印件和本单位缴纳的社保证明（加盖投标人公章）。
4	服务期限	1 年。
5	服务频次	服务期内提供 1 次。
6	服务成果	《网络安全培训过程文档》。

11、安全驻场

序号	指标项	指标规格
1	服务内容	需提供 4 名专业工程师驻场，主要需完成北京急救中心所有网络安全设备的定期维护、运行调试以及所涉及相关信息资产设备维保、策略维护等运维工作，及时发现运维管理过程中存在的问题并按照管理制度流程进行处理，同时在驻场人员安全服务的过程中，定期编制信息系统安全运维报告月报等。 驻场人员需保障北京急救中心信息系统安全运行，对网络信息系统安全运行监控、配置信息系统安全访问策略、及时响应信息系统故障处置、排除网络信息系统安全隐患、重大信息安全事件的应急响应等服务内容，承担网络信息系统安全运行的现场技术保障。 安全驻场服务要求包括但不限于： 1、人员具有专业的安全运维知识和三年以上工作经验，会使用信息化工具做好运维管理工作；

		2、值守期间全天 5×8 小时工作制（同时手机需 7*24 小时待命）。 3、重大节假日及大型活动期间参与 7×24 小时值班； 4、每日做好详细安全值守记录工作。
2	服务范围	安全驻场的范围为北京急救中心所有信息系统。
3	服务期限	1 年。
4	#服务频次	服务期内工作频次为 4 人 1 年。
5	服务成果	《信息系统安全运维工作月度总结报告》《信息系统安全运维工作年度总结报告》

12、安全通告

序号	指标项	指标规格
1	服务内容	将搜集整理的漏洞信息、系统补丁信息、病毒信息等安全状态信息及时或定期有针对性地向指定部门或人员发布，并给出相应的解决方案，使北京急救中心能够及时预防和防御安全风险，降低损失和负面影响，确保北京急救中心数据和信息技术科机房信息系统安全稳定运行。需提供每周周报。
2	服务范围	安全通告的范围为北京急救中心重要信息系统。
3	服务期限	1 年。
4	#服务频次	服务期内工作频次为每周通告 1 次。
5	服务成果	《北京急救中心网络安全信息通告》。

13、辅助测评

序号	指标项	指标规格
1	服务内容	在测评机构在北京急救中心系统实施等级测评期间，投标人须委派安全咨询顾问提供全流程的测评辅助服务，包括测评前进行准备梳理、准备测评相关的管理制度、开展安全加固检查等工作，以及测评过程中配合测评机构进行配置检查和调研访谈等事项，从而确保等级测评工作的顺利开展。本次信息系统安全等级测评针对指定信息系统进行。测评内容分为单元测评与整体测评。单元测评包括技术控制测评、管理

		控制测评，涉及安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理 10 个方面。
2	服务范围	针对北京急救中心指定信息系统。
3	服务期限	1 年。
4	服务频次	1 年服务期内提供 1 次。
5	服务成果	《辅助测评服务过程文档》。

14、安全巡检

序号	指标项	指标规格
1	服务内容	需对服务器、安全设备等 IT 设施的健康状态进行检测，涉及设备自身硬件资源的使用情况、业务应用服务所占用的网络资源情况、端口服务开放情况的变更等内容，并实施必要的安全维护操作，具体内容包括：设备 CPU、内存状态、开放服务检测，日志审计，网站监控，系统故障检查、分析、排除和跟踪，定期更新安全设备登录用户名及口令，定期备份和维护安全设备配置，并做好版本管理，做好巡检记录，维护记录单，提交巡检报告。
2	服务范围	安全巡检的范围是北京急救中心重要信息系统。
3	服务期限	1 年。
4	服务频次	服务期内每个季度进行一次巡检。
5	服务成果	《北京急救中心重要信息系统安全巡检报告》。

15、网络安全资产管理

序号	指标项	指标规格
1	服务内容	对北京市急救中心物理机房所具有的各信息系统、支撑软硬件、信息系统终端的资产进行管理，包括资产的品牌型号、功能用途、安全密码等方面。
2	服务范围	北京急救中心物理机房内所有硬件、软件。
3	服务期限	1 年。

4	服务频次	服务期内每个月进行一次巡检。
5	服务成果	《北京急救中心网络安全资产管理台账》

16、应急指挥系统运维保障

序号	指标项	指标规格
1	#服务内容	需针对北京急救中心应急指挥系统（包括 120 专网会议、卫生应急会议、保密会议以及腾讯会议等）做系统运维保障，包括系统管理维护服务和现场会议保障服务等。其中，系统管理维护服务包括：预防性巡检、软硬件故障修复、系统升级与优化等；现场会议保障服务包括：会议调试服务、会议召开服务、会场保障服务等。需提供承诺并加盖投标人公章。
2	服务范围	北京急救中心应急指挥系统。
3	服务期限	1 年。
4	服务频次	服务期内按需提供。
5	服务成果	《北京急救中心应急指挥系统运维保障过程文档》

17、网站安全监测

序号	指标项	指标规格
1	#服务内容	需通过专业的工具及人工分析对北京急救中心指定系统进行 7x24 小时安全运行监控，能及时发现系统的安全隐患和问题，第一时间通过电话、短信、邮件等方式通报相关人员，协助解决系统的安全问题。监测内容包括但不限于：远程网站漏洞扫描、远程网页木马监测、网页敏感内容监测、网站可用性监测、网页篡改监测。 投标人须提供监控工具的证明材料；须至少采用一种自主研发的监控工具（提供计算机软件著作权登记证书并加盖投标人公章）
2	服务范围	北京急救中心 OA 办公系统、北京急救中心门户网站、互联网支付平台。
3	服务期限	1 年。
4	服务频次	服务期提供 7*24 小时服务。

5	服务成果	《北京急救中心网站安全监测报告》
---	------	------------------

（二）项目实施需求

1、项目工期要求

本项目服务期限为一年，在本项目合同签订服务期之后，一年内完成安全服务相关工作及交付相应服务成果。

2、组织管理要求

要求给出切实可行的项目实施方案，方案中要包含项目管理控制措施、风险管理、进度管理、变更管理、沟通管理、文档管理、质量管理等内容；

在项目实施的全过程中，采购人有对项目进度、质量进行监督控制的职责和权利，投标人应全面配合，定期向采购人提交项目进展情况报告。

3、项目实施团队要求

投标人应有专门的技术部门并指定固定技术力量用于本项目的实施，主要实施人员要保持稳定，除离职外一般不得随意更换，确需要更换要报采购人批准，人员变更需提前一个月申请，更换后的人员需同等或优于更换人员。

投标人应按照项目的需求建立完善的组织结构和职责分工，进行相关的项目管控和随时调整项目实施方向。针对本项目成立专门的项目组成员不少于 6 人，确保人力、物力的投入，项目组成员角色包含项目经理、项目技术专家和项目实施人员三类：项目经理，主持编制项目实施规划，负责项目组与用户沟通，保证项目进度质量；项目技术专家，针对项目实施过程中的技术难题，提出解决方案；项目实施人员，负责整个项目的具体实施工作，包括驻场人员和其他服务实施人员。项目组成员必须稳定，项目实施的主要技术成员在项目终验前如果退出或更换，需要征得采购人同意。

项目经理需具有 5 年以上安全集成或服务项目实施经验，并具有类似运维服务的项目经历。项目技术专家需具有 10 年以上相关安全工作经验。项目驻场人员需具有 3 年以上相关工作经验。并提供项目组人员相关资格证明文件复印。

4、技术支持及服务需求

投标人应针对本项目提供详细的技术支持及服务方案、包括服务方式、响应时间、服务热线、服务保障措施等内容，投标人需具备完善的服务体系。

在服务实施过程中，投标人需成立专门技术队伍，投标人需提供 7*24 小时热线电话服务响应；如电话不能解决用户发起的问题请求，需提供现场排除及解决软

硬件故障的服务，在接到用户故障报告后响应时间不超过 1 小时，如电话不能解决问题，需 2 个小时内赶到用户现场进行问题分析和处理。驻场人员值守期间需为 5×8 小时工作制（同时手机需 7*24 小时待命），重大节假日及大型活动期间参与 7×24 小时值班。