采购需求

一、概述

国家药品监督管理局医疗器械技术审评中心是国家药品监督管理局的直属事业单位，中心主要负责国产三类和进口二三类医疗器械注册的技术审评工作。

中心的核心业务系统包括医疗器械注册电子申报系统、医疗器械注册技术审评系统、中心门户网站、中心 OA 办公系统、标准体系文件管理系统等等。其中医疗器械注册电子申报系统包括面向企业的预约咨询、申请人之窗（事项申请、电子申报、事项查询、文书接收等）等服务。

中心 2014 年对中心整个机房网络安全进行强化建设，并通过了三级等级保护评估。2019 年中心上线电子申报系统，为保障电子申报资料的安全，进一步对中心网络安全、数据安全防护体系进行升级，并对中心门户网站（包含电子申报相关服务）进行三级等保认证，并按要求每年开展等保评估。

近些年，网络安全形势的日趋严峻，外部对器械审评中心的关键业务系统的数据窥觑已久，为保障中心网络持续安全，保障重大活动等时期对网络安全、网络稳定运行需求的即时支撑，中心拟采购网络安全监测及运维维护服务。

二、总体要求

1.服务周期：

本次招标采购的中心网络安全监测及运维维护服务期限一年，服务期至 2026 年 12 月 31 日，合同将在本项目中标通知书发出后 30 日内签订。

服务合同为年度合同。服务内容包括网络运维服务、网络安全监测服务、网络安全加固服务、网络安全运维服务、网络安全等保实施服务、服务器系统服务、服务器安全服务、桌面安全服务、网络或安全咨询服务、其它甲方安排的驻场服务等。

2.服务要求：

（1）要求有驻场服务人员 4 人以上，项目经理 1 人负责运维工作的整个管理，项目经理不得更换；项目支撑团队不少于 8 人，每周一次项目例会，项目经理、驻场人员及项目支撑团队必须参加；

（2）要求对合同涉及的网络设备进行定期巡检，对网络安全进行定时监测，及时发现可能存在的问题，并及时进行安全加固，完成周巡检报告；要求每月完成月汇总，半年汇总、年汇总，形成汇总材料；

（3）网络出现故障或安全风险的情况，工作日内，要求立即响应，2 小时内恢复网络系统正常使用；非工作日，要求 2 小时响应，4 小时内恢复网络系统正常使用；要求事后分析故障原因，形成故障分析报告；

（4）国家法定节假日、特殊时期等做好保障工作，制定紧急预案，提供应急响应服务，保障系统安全；

（5）重大活动、节日等重保期间必须有值班人员，攻防演练期间需配置专家团队现场保障；

（6）设备集成服务；

（7）安全相关制度、报告、文件的编制服务；

（8）项目甲方安排的其它服务任务。

3.人员要求：

（1）要求有一名资深项目经理，除项目经理外需要驻场服务人员 4 人以上，项目经理不得自行更换；

（2）项目经理：国家人力资源和社会保障部颁发的信息系统项目管理师（高级），硕士及以上学历，有 5 年以上项目管理相关工作经验，需要具备相关行业安全服务项目实施案例。工作态度认真，责任心强，工作踏实细心，有较强的理解能力和较流畅的语言表达能力和沟通能力；

（3）驻场工程师：必须安排高级工程师提供驻场服务，需有 3 年以上安全、网络、系统运维工作经验，驻场工程师需具备注册信息安全专业人员（CISP）、DCMM 数据管理师、ITSS 服务工程师认证证书、系统架构师、系统分析师等多方面资质能力，熟悉计算机网络软、硬件管理，网络设备操作。具有较强的学习能力，掌握信息系统故障排查方法，并能够现场解决用户的实际问题。

4.其它：

为保持服务的延续性，最大限度保障中心网络持续安全稳定运行，本次招标确认的服务商，可在当年预算落实后予以延续签订新一年度（累计不超过三个年度）服务合同，若由于中标人上一年度服务考评未达标或本次招标的服务发生重大变化或财政变化导致预算无法落实，则采购人有权不再签订合同。

三、项目内容

（一）网络运维服务内容

网络运行维护服务内容要求如下：

（1）网络线路的按要求铺设：

按中心日常工作的需要，调整或增设办公区域的网络端点，调整或铺设各楼层的局域网络，调整或增设办公区域的无线网络及无线节点。

机房网络的调整及铺设，楼层交换网络的调整及铺设，监控网络的调整及铺设等。

（2）网络设备的日常巡检及监控：

提供每月、每季度、节假日前等时间段的现场巡检服务，检查内容包括网络运行状态、错误告警、性能检查等，提供详细的巡检报告。每次服务必须提交服务报告单，包括服务内容、处理过程、时间等，并由中心签字认可；

每季度对中心的网络设备运行情况进行全面、系统的检查和评估，并出具详尽的检查、评估和分析报告；

每半年，根据网络系统运行的整体运行情况，提供服务总结报告，提出合理化建议。

（3）故障应急响应：

提供全年（包括法定节假日）5*8 小时不间断技术服务。设备发生问题或故障时，30 分钟内电话响应。技术人员在 8 小时内到达现场并解决问题，工程师到达现场后 6 小时内无法修复故障，需协调设备原厂工程师到场协助处理故障；当故障设备 12 小时无法修复时，组织故障设备的维保服务商须提供不低于原设备配置的备机，故障解决时间不能超过 24 小时

（4）设备升级服务：

统筹设备管理，及时组织补丁和微码升级，包括及时通报设备升级计划，制定详细和可操作的设备升级方案，在确保对设备支撑业务影响最小的情况下实施相应升级方案。

（5）原厂技术支持：

对于复杂的技术问题和故障，根据中心要求，积极协调原厂提供技术支持。为了保证各设备维保服务质量，要求每年度服务期内，对各维保设备按照所属生产厂家，开展原厂服务评估。

（6）日常技术支持：

针对附件中的所列维保设备，配合和支持用户方完成相关系统和设备的技术支持工作，包括：为相应设备和系统提供技术咨询和方案建议，协助用户方进行设备调试、系

统优化、配置变更、网络调整、资料和文档整理等。针对新增业务需求，协助进行相应技术系统的配置修改和测试等。

（7）运维服务流程管理：

根据网络、服务器、存储平台系统上述维保服务技术需求须为本项目建立一套科学、先进、良性运转的服务管理体系，制定专门的维护服务管理制度和工作流程，并建立保证制度和流程能够在维护服务工作中贯彻落实配套措施和文档（包括巡检计划、巡检报告、维护清单、故障报告、应急处置预案等）。

（8）技术人员驻场服务：

于本项目所网络运行服务涉及设备及工作较多，且承载的业务非常关键，为了确保服务质量，要求投标商提供至少 1 名网络服务工程师 5*8 驻场服务。要求驻场工程师人员固定，经验丰富、能够独立维护维保设备中主要设备；要求驻场工程师善于沟通，当现场发生设备故障时，及时通报中心用户，积极处理；当故障无法解决时，能及时协调二线服务资源或原厂技术资源。

（二）网络安全服务内容：

本服务内容主要包括：安全设备运行监测及安全保障服务、系统安全加固服务、系统风险评估服务、渗透测试服务、应急响应服务、等保咨询服务、驻场运维服务。

（1）网络设备维护服务：

对中心安全系统清单中的所有设备提供 1 年 7*24 小时运行监测和安全保障服务，包括监测设备运行、软件安全升级、技术支持响应等。

（2）安全加固服务

根据中心系统安全等级的指标和测评标准，每季度一次对网络设备、安全设备等制定加固方案，通过打补丁、修改安全配置、增加安全机制等方法，合理加强设备的安全性，以满足等级保护三级防护要求。

安全加固设备参见下表：

类型	数量	加固内容	工作频度
网络设备	60 台	安全策略配置优化、协助开展系统安全升级	每季度一次
安全设备	40 台	安全策略配置优化、协助开展系统安全升级	每季度一次

（3）安全配置服务

根据中心工作开展的需要，调整中心安全设备的配置策略，保障新业务加入、安全配置调整、重大事件支撑等服务。

（4）风险评估服务

每月一次对电子提交系统电子文档的安全、系统面临的威胁和脆弱性等进行分析，采用工具扫描、渗透测试等方式，并提交风险评估报告和整改建议。

（5）渗透测试

每月一次为中心信息系统提供渗透测试服务，包括审评系统、电子提交系统、OA系统、中心门户网站、公众号，以及新上线的应用系统。采用黑盒、灰盒测试方式对被测系统进行渗透测试工作，主要包括 SQL 注入、XSS（跨站脚本）、CRLF 注入、目录遍历、文件包含、输入验证、认证、逻辑错误、Google Hacking、密码保护区域猜测、字典攻击、特定的错误页面检测、脆弱权限的目录、危险的 HTTP 方法、信息泄露、stuct2漏洞、Cookie 欺骗、源代码泄露、恶意网络地址转移、http 响应头截断、备份文件遗留隐患等常见的攻击方法，对渗透测试过程中发现的问题协助客户进行整改，并于渗透测试完成后一周内提交《渗透测试报告》。

（6）中心应急响应

中标人接到用户应急请求后，必须立即做出实质性响应。对于中心设备故障，必须在 1 小时内提出故障解决方案,2 小时内恢复设备正常运行。并于故障解决后 24 小时内，向用户单位提交故障处理报告。说明故障种类、故障原因、故障解决中使用的方法及故障损失等情况。

（7）安全运维驻场服务

安排至少一名驻场网络安全工程师，对中心整体网络及信息系统提供每日安全巡检、重大事件驻场保障、安全通告等服务，每月进行安全监测、安全评估，以便及时发现问题和解决问题，并为器审中心信息系统安全防护能力建设提供技术咨询。

（三）服务器安全服务内容：

(1)根据中心系统安全等级的指标和测评标准，每季度一次对服务器设备、操作系统、中间件、数据库系统等制定加固方案，通过打补丁、修改安全配置、增加安全机制等方法，合理加强服务器的安全性，以满足等级保护三级防护要求。安全加固设备或系统参见下表：

类型	数量	加固内容	工作频度

操作系统	65 台	系统补丁安装、安全策略配置、病毒库升级等	每季度一次
中间件	5 套	软件升级、安全策略配置	每季度一次
数据库	10 套	补丁更新、安全策略配置	每季度一次

(2)对中心服务器所搭载的操作系统、中间件、数据库的软件系统的运行维护，对系统进行重装、对数据进行备份管理、对中心新添加设备的上架、网络配置、系统安装等服务。

（3）驻场服务，投标人须安排至少 1 名系统工程师驻场提供服务。承担中心全部服务器设备（现有及新增）的设备上架、系统安装、网络配置、数据库及应用中间件安装、应用软件部署、巡检等服务。

（四）网络及服务器设备维保服务内容

负责采购人机房内及楼层间的网络、服务器及存储设备（电子申报系统相关服务器/存储设备、签章认证设备、电子文档管理设备除外，维保设备详见维保服务设备清单）提供维保服务。

（1）对采购人使用的服务器提供备品备件支持，要求有丰富现场经验驻场工程师提供驻场服务。常用备件更换时间小于 2 小时，特殊备件更换时间小于 4 小时。提供临时服务器并负责协同软件开发迁移业务保障业务正常运行，缩短停机时间。维修完成后向采购人出具备件更换清单、故障报告及相关日志进行审核。

（2）对采购人使用的内、外网备份系统提供备品备件支持。包括但不限于：对备份磁盘及磁带进行检查，定期清洗磁带库驱动器，对磁盘损坏及磁带黏连进行及时更换等，保障备份系统正常运行。

（3）对采购人使用的机房及楼层弱电井网络设备提供维保服务（不含网络及安全设备的策略库升级更新），一般故障维修更换处理时间小于 1 小时，特殊故障处理时间小于 4 小时并提供同型号、同配置备机，保障业务系统正常运行。

（五）桌面安全服务内容：

承担中心的全部桌面计算机、笔记本等终端设备安全运行维护服务，包括终端设备的病毒软件安装、安全监测、病毒查杀、安全问题排查等。

（六）值守、安全演练及重保服务内容：

（1）配合上级单位开展安全演练。

按照上级安全演练工作部署，组织开展安全演练预案、安全监测、攻击行为追踪等安全防护工作，组织中心各服务商开展安全演练防护。

（2）按要求开展安全值守

按照上级、重保及中心特殊时期（如应急产品审批）工作要求，开展安全/网络保障值守工作。

（3）按要求开展重大活动安全保障

重大活动前组织开展安全自查，发现存在的可能安全隐患，对发现的隐患组织安全加固。活动期间，开展安全值守，监测网络异常行为，进行及时跟踪和处置。活动后，开展保障工作回顾，总结形成保障工作报告。

（七）等级保护及商密年审实施服务内容：

(1)等级保护及商密评估年审实施

每年组织对中心认定为三级等保的系统开展等级保护测评和商密评估，对中心新件业务系统组织实施等保评定及备案。

实施内容包括联系等保测评、商密评估、等保备案单位，按照测评、备案要求准备相关资料及文档，协调被评定系统服务商按测评要求配合等级测评和商密评估等工作。

编制符合等级保护要求的安全制度文档，涵盖安全组织、安全建设和安全运维等方面的各种制度、流程、表格、技术标准和规范等。

(2) 等级保护及商密整改

根据三级系统测评、商密测评要求，对测评中发现的问题进行整改组织实施，包括对网络安全进行整改、对相关制度文档预案进行修订、组织相关系统承建商对系统进行安全整改。

（八）安全咨询服务内容：

根据中心安全工作需要，配合甲方做好相关安全报告编制、上级安全调研表单填制、安全形势评估、安全发展规划等服务内容。

投标人须派驻 1 人以上驻场，承担相关文档的编制工作。

（九）分中心网络安全保障服务

负责医疗器械技术审评检查长三角分中心、大湾区分中心安全指导工作，协同分中心信息化服务商保障分中心与国家器审中心的网络连接安全和国家器审中心系统应用安全。

（1）制定国家器审中心与分中的安全保障方案，提出分中心的安全管理要求，并指导分中心按管理要求保障共同的网络安全。

（2）监测分中心与国家器审中心的专线网络连接、管理连接安全策略，及时发现安全风险并进行防范。

（3）对分中心网络接入或网络升级等安全状态变更时，配合分中心对其网络安全进行评估，确保网络持续安全可靠。

（十）甲方安排的其它服务内容：

驻场人员需全职承担甲方的工作任务，驻场人员应服从甲方调度，完成甲方安排的其它工作内容。

四、中心业务系统及设备清单

医疗器械技术审评中心核心业务是接收国家药品监督管理局转交的进口器械及国产三类器械的技术审评工作，中心自成立以来逐步建设了技术审评业务管理信息系统、办公自动化系统等内部管理信息化系统，详细系统清单如下表所示：

业务系统清单：

业务系统	网络区域	概述
业务审评系统	内网	linux、oracle、普元 EOS 开发平台、普元工作流、smartBI 报表
10 版业务审评系统	内网	linux、oracle、was、JAVA
03 版业务审评系统	内网	windows、domino notes
OA 办公自动化系统	内网	linux、oracle、JAVA
知识库管理系统	内网	linux、oracle、普元 EOS 开发平台
预约咨询管理系统（管理端）	内网	linux、oracle、普元 EOS 开发平台
数据整理系统	内网	linux、oracle、普元 EOS 开发平台
中心网站	外网	linux、oracle、JAVA
审评进度查询	外网	linux、oracle、JAVA
预约咨询	外网	linux、oracle、JAVA
公众号服务平台	外网	linux、oracle、JAVA
邮件服务	互联网	第三方服务
知网服务	互联网	第三方服务
电子申报系统	内网、互联网	linux、oracle、普元 EOS 开发平台

维保服务设备清单：

网络设备	描述	数量
路由器	互联网出口，1 台备份	2
防火墙	天融信数通	1
防火墙	国家局专网	1
IPS 防入侵	国家局专网	1
路由器	国家局专网	1
接入交换机	国家局专网	1
核心交换机	互联网	2
接入交换机		16
审评系统负载均衡		1
服务器		
内网数据库服务器	RH5885V3	2
DI 数据同步+杰表打印服务器	RH2288V3	1
备份服务器	RH2288V3	1
云课堂服务器	RH2288V3	1
体系文件库+临床试验数据库	RH2288HV5	1
OA 服务器	RH2288HV5	2
中软老审评服务器	DL580G7	2
虚拟化 DNS 服务器	RH2288HV5	1
审评测试服务器	RH2288HV5	1
网站服务器	DL380G7	1
微信公众号	DL380G7	2
短信平台	DL380G7	1
数据整理服务器	DL380G7	1
网站测试服务器	DL380G7	1
外网数据交换服务器（RTS）	DL380G7	1
远程管理服务器	RH2288HV5	1
中软老审评存储	MSA2000	1
存储光纤交换机		1