采购需求

1. 概述

1.1 项目背景

北京市药品监督管理局(简称市药监局)主要负责本市药品(含中药、民族药)、医疗器械和化妆品安全监督管理等各项工作，核心包括药品、医疗器械、化妆品的产品备案注册、企业准入、全生命周期监管等，构建了行政审批、专业监管、公众服务等19个业务应用系统，面向公众、从业企业、监管部门提供数据、信息化支撑等服务。

《网络安全法》2017年6月1日起实施，网络安全法明确提出“建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。”。2022年9月，国家网信办公开征求网络安全法修订意见，启动网络安全法修订工作，拟进一步加强完善网络安全立法体系。

《数据安全法》2021年9月1日起施行，数据安全法提出“各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。国家建立数据分类分级保护制度，各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。”等诸多法规要求。就行业主管部门数据安全管理职责、数据分类分级管理要求、数据安全保护义务等提出了明确要求。

市药监局做为药品、医疗器械、化妆品行业主管部门，构建了一些列面向公众、相对人、监管人员的信息化系统，系统的网络安全保障工作、行业数据的保护责任重大。

为进一步提升市药监局网络安全性，提升重点时期网络安全的保障水平，落实数据安全保护义务，我局在既有的网络安全保护设备、设施、防护工具的基础

上，通过第三方外包服务的方式，对我局网络安全体系进行滚动评估、提出优化方案、持续指导网络安全优化升级并对安全体系进行迭代、提供重点时期专业团队 7*24 小时保障、提供外部网络安全的不间断监测和预警、持续保障网络安全，同时协助我局对数据全生命周期安全进行管理。全面落实“实战化、体系化、常态和”和“动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控”的“三化六防”措施，深化建设整改、检查检测、检测预警、应急处置等体系化安全工作管理，构建“打防管控”一体化的网络安全综合防御体系，不断提升网络安全整体防护能力和技术对抗能力，切实保障保障我局网络安全、数据安全。

1.2 项目目标

支撑我局对网络安全体系进行全面管理，包括网络架构、网络安全制度、网络安全工作开展等，保障我局网络安全有体系、有计划、有序合规开展。

指导并协助完成我局数据分类分级，并对数据分类分级进行持续管理，协助定期对信息系统数据安全性合规性进行评估并指导进行优化，确保我局数据安全。

重保时期，全面监测网络攻击和社会攻击行为，分析攻击方法、溯源攻击路径，形成防护报告，确保攻击监测无遗漏、攻击行为全掌握，攻防演练考评合格、无重大安全事故。

1.3 项目周期

服务期限：自本项目合同签订之日起 12 个月。

2. 项目现状

截至 2023 年底，北京市药品监督管理局有行政许可系统、北京药店数据管理系统等在运行的 19 个系统全部部署在北京市政务云。拓扑图如图 1 所示，业务系统列表如下。另有药品全生命周期档案管理系统、药品追溯监管系统一期建设中。

业务系统清单如下：

序号	系统名称
1	行政许可系统
2	监督检查系统
3	执法案件系统
4	互联网监测系统

5	电子档案综合管理系统
6	风险监测评估与检验检测系统
7	认证审评系统
8	统计分析与决策支持系统
9	药品类数据管理系统
10	统一认证系统
11	安全监管研判与应急指挥系统
12	实验室管理与质量安全数据分析平台系统
13	北京药店数据管理系统
14	公共卫生应急物资保障信息平台
15	门户网站系统（对外服务平台）
16	药品物流在线实时追溯系统
17	办公自动化系统
18	食品药品安全信用信息系统
19	疫苗等高风险品种智慧生产监管系统

3.服务内容和要求

基于当前网络安全形势，结合公安部网络安全保护重点措施指导意见，为进一步保障北京市药品监督管理局网络和数据安全，在政务云安全保障体系的基础上，针对攻防演练、数据分类分级、数据安全要求，开展网络安全体系持续优化、数据全生命周期安全防护与管理、重点时期重要安全专职专业团队保障、外围7*24小时监测预警等服务。

3.1 网络安全体系技术支持

根据网络安全面临的形势变化，持续完善和调整网络技术架构、安全防护机制、安全策略、安全管理措施、技术防护措施、运行维护措施等，增强防护弹性和可持续性。具体包括：

- 指定专门的安全专家，就物理环境与通信网络、纵深防御的区域边界、计算环境、系统环境、业务系统、应用行为的安全可靠进行深度剖析，长期对口协助优化网络安全体系。
- 结合最新形势和各级安全要求，参与协助修订内部安全管理制度，并跟

踪统计制度执行情况。

- 挂图作战，按照“理论支撑技术、技术支撑时间”，有序规划年度安全计划，建立实战化、体系化、常态化的工作机制，并按计划统筹云服务安全、杀毒软件安全、日常安全监测等服务是否执行到位，协助统计服务频次、效能等，保障网络安全运行体系持续有效。
- 协助第二级以上信息系统等级保护管理，协助和指导按项目完成年度和专项等保测评。
- 指导信息系统按等级测评、安全检测、风险分析、事件分析、实战检验等发现的问题制定整改方案、路径，督促指导整改情况。
- 协助进行信息系统商用密码安全性评估统筹和评估工作。
- 定期梳理和更新供应链安全目录，梳理和维护企业、产品和人员清单，及时查找发现供应链安全风险隐患，采取措施指导消除隐患，闭环完善。
- 协助迎接上级和网安管理部门现场和远程检查。
- 提供驻场安全工程师 1 名（5*8 驻场，7*24 防护）。
- 提供远程专家不少于 3 名（行业领域顶尖安全专家，要求参与过北京市网信部门组织的攻击和防守、参与国家药监局护网行动）专门负责药监局安全体系和具体咨询。

3.2 数据全生命周期安全防护支持

协助强化数据安全保护，提供数据安全专家，按照《数据安全法》相关要求，专门对口协助和指导实施数据安全分类分级管理、数据安全验证和日常数据安全防护等技术保障，对数据收集阶段、存储阶段、使用和加工阶段、数据传输阶段、共享公开阶段、数据销毁阶段进行细化管理，切实落实各阶段数据安全保护措施。主要内容：

- 协助梳理数据分类分级标准，开展分类分级试点实施。
- 评估信息系统评估数据安全合规性。在对数据采集、加工、分类、处置、存储、删除的全生命周期，进行技术鉴别和记录，确保符合数据管理相关法律法规和监管要求。
- 数据共享和开放安全技术支持。在从事数据共享和开放活动中，全程指导信息系统进行安全管理，对敏感数据进行加密或脱敏传输。对数据传输日志进行管理，定期对数据共享和开放传输行为进行审计，提升安全

性。

- 进行数据加密和备份技术支持。按照《数据管理法》《密码法》等相关要求，指导信息系统开展数据加密，定期组织开展数据备份和恢复演练。
- 定期巡查数据库中的数据安全状况，优化数据安全策略。

3.3 重点时期重要安全保障支持

在法定节假日，国家、北京市开展的安全攻防演练、护网、重大活动时期（约1个月，加上前期准备和后期处置，安全人员保障时间约2个月。），进行驻场支持，协助进行网络安全防守，强化我局特殊时期网络安全防护能力。主要内容：

- 法定节假日期间，实施7*24小时重点保障。每日2小时一次，监测信息系统状态，互联网出口数据流量，定时汇报安全状态，发现攻击第一时间拦截处置并报告，响应上级有关节假日重点安全保障技术支持等。
- 攻防演练、重保期间，按照不少于三个特殊保障团队的分工进行驻场技术支持。共驻场安全专家不少于6人，后台专家团队支撑不少12个人，协同分工值守。重点进行IP地址封堵、攻击拦截、攻击溯源、邮件临时安全管控、社攻风险排查等技术工作。同时，通过技术监测工具，发现内部地址风险行为，封堵内部攻击路径，追踪攻击IP等。（重保时期驻场专家要求：三个专家团队应分别由不同参与过北京市和国家部委历年护网行动、攻防演练红蓝单位人员组成，有6年以上网络安全工作经验。）

3.4　7*24小时安全监测及预警（态势感知）

落实网络安全实施监测措施，聘请第三方态势感知专业团队，部署行业顶尖安全产品，对我局全部公网（政务外网）IP地址，开展全年无休日常监测，标记异常流量、访问、攻击、挂马暗链等，第一时间提供攻击溯源和分析报告。

3.5 特征库升级和维保服务

针对以下设备提供维保服务和特征库升级服务：1个web应用防火墙、2个IPS、2个防病毒网关、2个漏扫、2个网页防篡改、2个上网行为管理。

4.项目服务要求

- 服务时间要求

项目服务周期一年，项目服务启动后，应在两周内完成服务实施方案的制定，做好进度和任务安排。项目服务周期内，每季度总结服务报告，年度服务结束后开展服务总结和评价。

➢ 质量控制要求

为保证项目进度与质量，在项目的每一阶段，都需要编制相应的文档（包括文件资料和项目过程中填写的各种图表）。这些文档和计算机程序以及数据在一起，成为项目管理中不可缺少的部分。在项目实施期间，不能影响系统的正常应用。

在项目实施工作中，项目管理人员应对项目过程进行管理。管理过程从获取项目的需求开始，需求一旦确定，管理人员应当制定实施项目的计划，如制定按时完成任务的时间表、在整个项目中使用的质量控制措施等；在计划付诸实施后，管理人员应履行对实施过程的控制，调查、分析和解决发现的问题，问题及具体的解决办法都应写成文档，管理人员应在约定的阶段对项目进展写成报告；当每一阶段任务完成后，管理人员应对交付成果进行检查和评价，保证交付成果和计划的完整性和一致性。管理文档是记录项目过程各类管理信息的文档，主要包括：质量控制计划、项目周报、会议记录等。

➢ 保密要求

项目启动阶段服务方应依据项目服务方案开展项目管理措施、提供相应的组织保证、质量保证、安全保密保证，已保证项目按期保质安全的完成。

服务方要严格遵守国家《保密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，相关人员恪守职业道德，服从药监局的管理，严格遵守药监局的保密规定和工作制度，并承担相应的保密责任。

所有参与本项目的服务人员，都必须签订《保密承诺书》。投标人负责对《保密承诺书》归档保管，接受药监局检查。投标人要对承诺履行情况负有监督责任，一经发现违反承诺情况，要及时向药监局报告。

➢ 人员要求

项目团队人员不少于 10 人，项目经理应具备高级项目经理和数据安全工程师资质；数据安全工程师不少于 4 人，信息安全工程师不少于 2 人，网络工程师不少于 2 人。

服务团队人员应严格遵守药监局的各项规章制度和管理规定，爱岗敬业，不得擅离职守或做与工作无关的事情，能够与客户进行很好的沟通，具有很强的工

作责任心和客户服务意识。

项目服务人员需保持稳定性，在本项目服务结束前，参加本项目的人员变动必须取得市药监局的同意。

5.项目验收

项目服务结束后15日内，服务方提供纸质和电子版的项目验收文档。验收文档包括项目管理过程文档、相关服务交付物等。我局根据验收文档及项目服务过程开展服务评价，服务评价合格的项目通过验收。