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

保障业务系统的稳定运行，以风险管理为导向强化我单位信息安全保障体系，健全各项安全保护措施，提升我单位网络信息安全防护水平。根据国家相关政策规范、标准指南等文件，为药监局政务云上业务系统建立和完善信息安全保障体系，通过提供安全巡检、脆弱性检测、渗透测试、日志收集与分析、安全加固、安全值守、特殊时期值守服务、应急保障服务体系、安全通告、安全管理制度修订、安全咨询服务、主机杀毒服务、数据库审计服务、漏洞扫描、本地数据备份、数据库加密、可信验证服务、东西向策略梳理和防护服务、基础软件租用等服务，增强系统安全防护能力、隐患检测能力、应急响应能力和系统恢复能力，保障2023年药监局政务云上业务系统稳定安全运行。

（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，本项目供应商为小型或微型企业且所投产品为小型或微型企业生产的，供应商和产品制造商应出具采购文件要求的《中小企业声明函》给予证明，否则评审时不予认可。供应商和产品制造商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。

2. 监狱企业扶持政策：供应商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。供应商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. 节能环保政策：投标产品中如有财政部和国家发展和改革委员会公布的最新“节能产品政府采购品目清单”或财政部和生态环境部公布的最新“环境标志产品政府采购品目清单”中产品的，应提供相关证明文件。

4. 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，供应商应出具采购文件要求的《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/成交结果同时公告其《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。

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；

按照北京市药品监督管理局的要求，提供安全技术保障服务和常态化安全服务工作。具体安全服务内容包括：基础软件租用、安全巡检、脆弱性检测、渗透测试、日志收集与分析、安全加固、现场安全值守、特殊时期值守服务、应急保障服务体系、安全通告、安全管理制度修订、安全咨询服务等保运行维护服务、主机杀毒服务、数据库审计服务、漏洞扫描、本地数据备份、数据库加密、可信验证服务、东西向策略梳理和防护服务等服务。

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	包内容	数量	实施时间	实施地点
1	政务云安全运维服务	1项	合同签订之日起12个月	北京

（二）采购项目交付或者实施的时间和地点

1. 服务期：合同签订之日起12个月。

2. 服务地点：北京市药品监督管理局指定地点。

3. 支付方式：自本合同签订生效之日起，2023年7月底前甲方支付乙方本合同50%的服务费款项，本合同到期前3个月内支付剩余款项，乙方开具同期等额发票。

四、采购标的需满足的服务标准、期限、效率、验收标准、其他技术、服务等要求：

1. 概述

1.1 项目背景

自2012年开始，我市陆续开展电子政务云的试点工作，北京市药品监督管理局（以下简称“市药监局”）信息系统已迁移部署至市级政务云。为确保市药监局主要信息系统安全、可靠地运行，并最大限度地确保信息的机密性、完整性、可用性、可控性，避免各种潜在的威胁，必须借助专业的安全服务来加强信息系统的安全建设，保障市药监局政务云上信息系统安全稳定运行。由于信息安全的复杂性、全面性、动态性和主动性等特性，对安全专业技术人员提出了非常高的要求，安全运维需要引入专业安全服务商为市药监局提供信息安全专业服务，切实提高信息安全管理能力。

1.2 项目目标

保障业务系统的稳定运行，以风险管理为导向强化我单位信息安全保障体系，健全各项安全保护措施，提升我单位网络信息安全防护水平。根据国家相关政策规范、标准指南等文件，为药监局政务云上业务系统建立和完善信息安全保障体系，通过提供安全巡检、脆弱性检测、渗透测试、日志收集与分析、安全加固、安全值守、特殊时期值守服务、应急保障服务体系、安全通告、安全管理制度修订、安全咨询服务、主机杀毒服务、数据库审计服务、漏洞扫描、本地数据备份、数据库加密、可信验证服务、东西向策略梳理和防护服务、基础软件租用等服务，增强系统安全防护能力、隐患检测能力、应急响应能力和系统恢复能力，保障2023年药监局政务云上业务系统稳定安全运行。

1.3 项目周期

服务期限：自本项目合同签订之日起12个月。

1.4 项目原则

为实现我局年度信息系统安全运维服务项目的总体目标，结合我局信息体系建设的实际情况和未来发展需求，运维过程必须遵循以下原则：

- **安全保密原则**

执行国家《保密法》及有关保密的法律法规，服务过程中凡是涉及到的任何药监局信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害药监局利益。

- **最小影响原则**

要尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著

影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应对风险进行说明。

- **规范性原则**

应由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

- **可控性原则**

实施信息系统安全服务的工具、方法和过程要在双方认可的范围之内，保证药监局对于服务过程的可控性。

- **质量保障原则**

应特别重视项目质量管理，项目的实施将严格按照项目实施方案和流程进行，并由项目协调小组从中监督、控制项目的进度和质量。

2. 项目现状

截至2022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和基于AI的防疫物资识别分配系统等21个系统已迁移部署到北京市政务云。拓扑图如图1所示，业务系统列表如下。

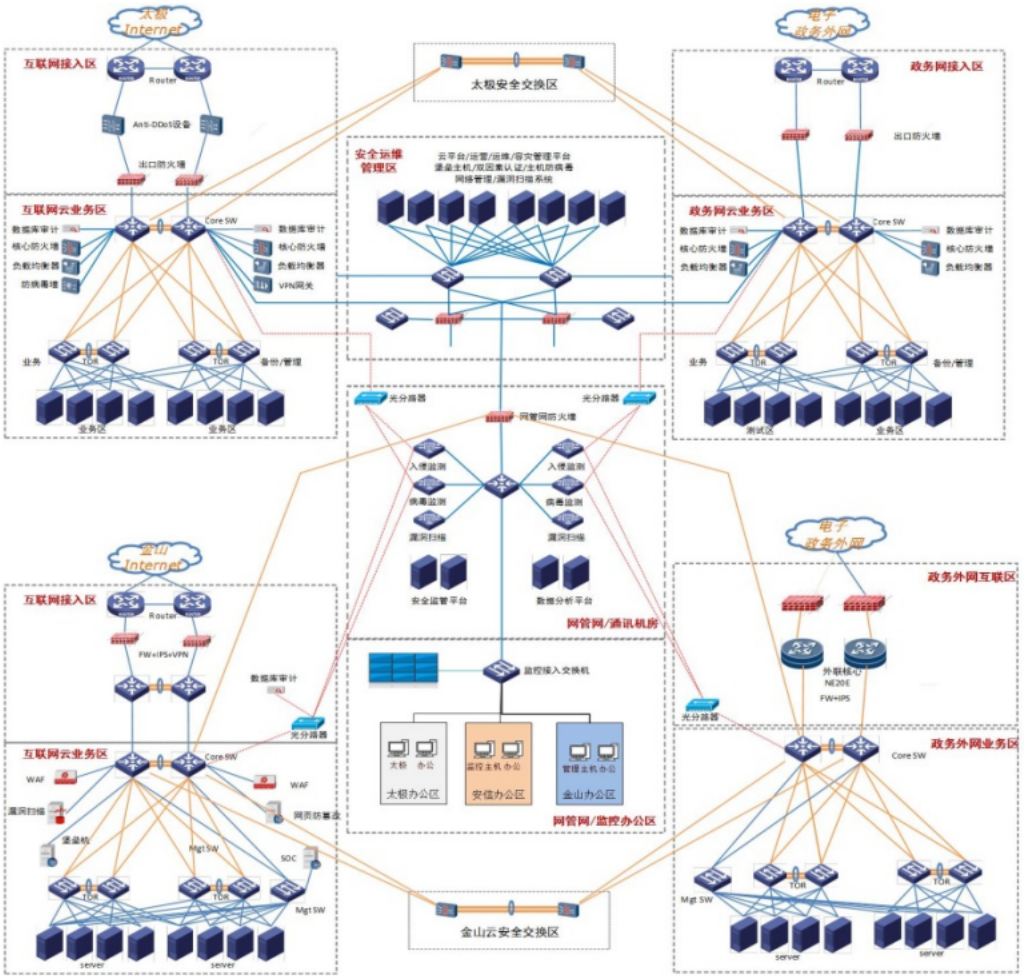

图 1 市级政务云拓扑图

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	食品药品安全监管研判与应急指挥系统
12	食品药品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	基于 AI 的防疫物资识别分配系统
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	公务仓管理系统
18	移动执法系统
19	办公自动化系统
20	食品药品安全信用信息系统
21	疫苗等高风险品种智慧生产监管系统

3. 服务内容和要求

按照北京市药品监督管理局的要求，提供安全技术保障服务和常态化安全服务工作。具体安全服务内容包括：基础软件租用、安全巡检、脆弱性检测、渗透测试、日志收集与分析、安全加固、现场安全值守、特殊时期值守服务、应急保障服务体系、安全通告、安全管理制度修订、安全咨询服务、等保运行维护服务、主机杀毒服务、数据库审计服务、漏洞扫描、本地数据备份、数据库加密、可信验证服务、东西向策略梳理和防护服务等服务。

（1）针对北京市药品监督管理局在北京市市级政务云平台上所有系统（云上系统参照采购需求）。具体服务内容如下：

服务名称		服务范围（表格中为截至 2022 年底数据，2023 年具体开展以实际为准）	服务期限
基础软件租用及安全服务		操作系统 127 个，约 127 个主机	合同期内
		开源数据库，约 5 个云主机	
安全技术保障	主机杀毒服务	入云系统，约 127 个云主机	
	主机防护服务	入云系统，约 127 个云主机	
	主机安全加固服务	入云系统，约 127 个云主机	
	主机漏洞扫描服务	入云系统，约 127 个云主机	
	数据库审计服务	入云业务系统的数据库	
	本地数据备份服务	入云业务系统，约 35290GB	

	数据库加密服务	入云业务系统的数据库	
	东西向策略梳理和防护服务	政务外网和互联网 vpc	
	数据库防火墙	入云业务系统的数据库	
	数据库漏扫	入云业务系统的数据库	
	互联网应用级入侵检测和防御服务	入云的互联网业务系统	
	可信验证	入云系统的云主机	
	日志收集与分析	入云系统的云主机	
	渗透测试	入云互联网系统的 IP	

（2）针对在北京市市级政务云平台上的业务系统，开展常态化安全服务，服务内容如下：

服务名称		服务范围	服务频率	服务期限
应急保障服务	应急预案服务	针对药监局在北京市市级政务云平台上业务系统展开	服务期内开展 1 次	合同期内
	应急演练服务	针对药监局在北京市市级政务云平台上业务系统展开	服务期内开展 2 次	
	应急响应服务	针对药监局在北京市市级政务云平台上业务系统展开	服务期内开展 2 次	
安全通告		针对药监局在北京市市级政务云平台上业务系统展开	服务期内开展 52 次	
安全管理制度修订		针对药监局在北京市市级政务云平台上业务系统展开	服务期内开展 1 次	
安全巡检		针对药监局在北京市市级政务云平台上业务系统展开	服务期内开展 12 次	合同期内
脆弱性检测		针对药监局在北京市市级政务云平台上业务系统展开	服务期内开展 2 次	合同期内

（3）针对北京市市级政务云平台上的业务系统，开展有需性安全服务，服务内容如下：

代码审计	按需开展	服务期内提供 2 个	合同期内

3.1服务提供清单

本次项目服务范围、服务周期清单：

项目	序号	服务名称	服务范围	单位	数量	服务期限
基础软件租用	1	操作系统租用（含windows server、Linux等）	约35个云主机	套	35	12个月
			约92个云主机	套	92	12个月
	2	开源数据库租用	约5个云主机	个	5	12个月
安全技术保障	1	主机杀毒服务	约127个云主机	台	127	12个月
	2	主机防护服务	约127个云主机	台	127	12个月
	3	主机安全加固服务	约127个云主机	台	127	12个月
	4	主机漏洞扫描	约127个云主机	台	127	12个月
	5	数据库审计服务	入云系统的数据库	个	36	12个月
	6	本地数据备份服务	入云业务系统的数据	GB	35290	12个月
	7	数据库加密服务	入云系统的数据库	个	36	12个月
	8	东西向策略梳理和防护服务	-	个	4	12个月
	9	数据库防火墙服务	入云系统的数据库	个	36	12个月
	10	数据库漏扫服务	入云系统的数据库	个	36	12个月
	11	互联网应用入侵检测和防御服务	-	个	9	12个月
	12	可信验证	入云业务系统的云主机	个	56	12个月
	13	日志收集与分析服务	入云业务系统的云主机	个	21	12个月
	14	渗透测试	入云业务系统的IP	个	21	12个月
常态化安全服务	15	应急预案	针对药监局在北京市市级政务云平台上业务系统展开	次	1	12个月
		应急响应	针对药监局在北京市市级政务云平台上业务系统展开	次	2	12个月
		应急演练	针对药监局在北京市市级政务云平台上业务系统展开	项	2	12个月
	16	安全通告	针对药监局在北京市市级政务云平台上业务系统展开	次	52	12个月
	17	管理制度修订	针对药监局在北京市市级政务云平台上业务系统展开	次	1	12个月
	18	安全巡检	针对药监局在北京市市级政务	次	12	12个月

			云平台上业务系统展开			
	19	脆弱性检测	针对药监局在北京市市级政务云平台上业务系统展开	次	2	12 个月
	20	代码审计	按需开展	个		12 个月

3.2基础软件租用及安全服务

3.2.1 操作系统套餐租用及安全服务

服务内容：根据北京市药品监督管理局信息系统现状和需求，提供信息系统在北京市市级政务云平台上正常运行所需要的操作系统 Windows Server、Linux 等套餐租用服务。包括租用、安装及维护，根据漏洞扫描结果或等级测试要求对操作系统进行安全加固。

服务范围：针对 127 台云主机展开。

3.2.2 开源数据库租用及安全服务

服务内容：供应商需按照市药监局的要求，提供开源一年租用服务，并协助安装和调试数据库，并提供对数据库的维护服务。

服务范围：针对 5 台云主机展开。

3.3安全技术保障

3.3.1 主机杀毒服务

服务内容：针对云主机提供恶意代码检测和拦截服务，及时发现和拦截各种恶意代码、病毒木马等，并有效阻断。

服务方式：采用适配云环境的防病毒软件，对虚拟机环境进行有效的病毒防护和查杀。

服务范围：针对 127 台云主机展开。

服务成果（包括但不仅限于）：针对 127 台云主机服务期内提供 2 份《主机杀毒服务报告》（每半年一份）。

3.3.2 主机防护服务

服务内容：针对信息系统主机提供防护服务。

服务方式：采用适配云环境的主机防护软件，对虚拟云主机进行有效的防护。

服务范围：针对 127 台云主机展开。

服务成果（包括但不仅限于）：针对 127 台云主机服务期内提供 2 份《主机防护服务报告》（每半年一份）。

3.3.3 主机安全加固

服务内容：通过技术手段对入云业务系统进行安全策略加强、调优，加强网络、系统和设备抵御攻击和威胁的能力。

服务方式：通过人工服务的方式对云主机进行安全加固。

服务范围：针对 127 台云主机展开。

服务频次：127 台云主机服务期内提供 2 次。

服务成果（包括但不仅限于）：针对 127 台云主机服务期内提供 2 份《主机安全加固服务报告》（每半年一份）。

3.3.4 主机漏洞扫描

服务内容：供应商应根据现有云主机的情况，通过对云主机进行漏洞扫描，分析业务系统所存在的风险隐患。

服务方式：采用适配云环境的主机漏洞扫描软件，通过与人工服务相结合的方式对云主机进行漏洞扫描。

服务范围：针对 127 台云主机展开。

服务频次：127 台云主机服务期内提供 2 次。

服务成果（包括但不仅限于）：针对 127 台云主机服务期内提供 2 份《主机漏洞扫描服务报告》（每半年一份）。

3.3.5 数据库审计服务

服务内容：对数据库系统的操作行为和访问行为进行分析和审计，及时发现高危操作行为和访问行为，并进行预警。

服务方式：在虚拟机部署数据库审计系统，通过虚拟网络旁路监听或代理实现数据库审计。

数据库审计系统指标要求：

指标项	指标要求
部署方式	旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计（不需要提供 DBA 账号和任何数据库账户，不需要创建任何数据库账户）。
	支持在目标数据库 服务器主机上安装 agent 解决云环境、虚拟化环境内部流量

	无法镜像场景下数据库的审计（不需要提供DBA账号和任何数据库账户，不需要创建任何数据库账户），审计平台可以实时监控agent CPU使用率、内存使用率、传输包个数。
	agent参数支持自定义，支持IP(IPv4\IPv6)、CPU占用率、内存占用率、本地缓存大小、端口等灵活配置。
	支持审计平台WEB界面管理插件，支持插件的配置、唤醒、挂起、中断、升级，审计平台支持远程安装、卸载、下载。
协议支持	支持Oracle、SQL Server、Db2、Informix、PostgreSQL、Sybase ASE、Sybase IQ、MySQL、MongoDB、SAP HANA、MariaDB、Percona等主流数据库。
	支持Hive、HBase、Sentry、Impala、HDFS、ES(Elasticsearch)、GP(Greenplum)、Redis等大数据平台的审计。
	支持Teradata、Cache、人大金仓、达梦、神通、南大通用、华为Guass等数据库审计。
	支持华为Guass DB 100、Guass DB 200数据库。
	支持SSH或者KVM登录Oracle、MySQL、SQL Server数据库服务器后，直接执行的SQL操作的审计，不依赖于数据库自身审计功能。
审计功能智能发现	支持跨语句、跨多包的绑定变量名及绑定变量值的审计；支持对超长SQL操作语句审计，可以正常记录单条长度小于等于2M个字节的SQL语句内容。
	支持访问来源信息：客户端IP、端口、数据库名称、数据库用户、OS用户、访问工具、主机名称、MAC地址。
	支持应用身份信息：应用客户端IP、端口、应用用户名、应用URL标识、应用URL模板、URL、URL地址参数、URL消息体参数；支持数据库主机信息：数据库IP、端口、数据库名、服务名（实例）。
	支持SQL语句信息：SQL标识、操作类型（DDL、DML、DCL等）、影响行数、响应时间、语句捕获时间、执行结果（DB应答码、应答错误信息）、受影响对象、SQL语句、SQL语句模板、SQL参数、结果集；支持数据库单向\双向审计。
	支持数据库告警功能，支持对根据IP、账号、客户端工具名、时间等定制规则进行告警。
	支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址等信息，并且自动添加到审计范围，无需用户提供网段、数据库地址等信息。
结果集审计	支持按照策略进行结果集审计，可以指定敏感表审计结果集。
	支持通过返回行数和内容大小控制返回结果集大小，降低系统开销。
	支持基于结果集的关键字检索。
安全审计	内置安全特征库规则，如SQL注入、缓冲区溢出、权限提升、数据泄露、拒绝服务、访问操作系统、改密码、Bypass FGAC、修改FGAC、审计、游标注入、访问敏感组件、创建外部JOB、恶意代码、非系统用户执行命令等常规漏洞。
	应具备漏洞攻击规则库，漏洞攻击规则应至少包括：漏洞名称、CVE标识、CNNVD、漏洞类型、影响范围等内容。
	支持识别口令猜解攻击，以及在同一个会话里，相同IP、数据库用户的频次攻击告警。
审计策略	可自定义审计策略。审计策略至少支持20个条件，规则各条件之间支持与或非

	逻辑关系。
	结果集审计支持全局开启，也支持按照具体策略进行结果集审计开启的功能。
	告警数量需支持最大告警数量限制，超过告警阈值之后便不告警。
审计查询	支持基于时间、IP 地址、数据库服务器 IP 地址、用户名、数据库操作命令、数据库表名，执行结果，应用用户、数据库服务（实例）名、报文关键字等多种丰富的查询检索条件；支持应用层关联审计查询和关联分析。
	支持不同审计账户，各自查看不同的数据库审计内容，要求：A 账户不能看到 B 账户的数据库审计记录，B 账户不能看到 A 账户的数据库审计记录，安全管理员可以看到所有的审计记录。
	支持将常用的查询条件保存成固定查询模板，方便后续快速查询。
	支持对查询结果中可能存在的敏感数据进行掩码处理，防止敏感数据泄露。
	支持对查询结果以 CSV 文件格式导出到本地。
	在同一套审计系统内可创建子账号，并对不同的子账号授予不同的数据库审计记录的查询检索权限，确保子账号之间彼此数据不可见，避免数据交叉泄露。
	支持 SQL 语句自定义业务化语言翻译。
统计报表	系统提供不少于 40 个报表模型，分别基于全库、数据库组和单库维度进行展现。
	支持合规性报表，如 PCI、等级保护、SOX 法案等专项报表展现。
	支持专项报表展现，针对风险、性能、访问源、账户等信息做专项报表展现。
	支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式，基于总体概况、性能、会话、语句、风险多层面展现报表。
	支持按日、周、月等时间周期生成报表。
	支持报表数据后台定期预生成，保障报表数据展现速度。
	支持将报表按指定的时间推送至指定管理员的邮箱。
	报表支持以 Word、PDF、HTML 等格保存到本地。
会话分析	支持会话级检索和详情展现：包括在线的并发会话、活跃会话、失败登录会话等提供专项的分析界面。
	支持失败登录会话查询和统计：包括客户 IP、数据库用户、操作系统用户、工具或应用、数据库应答码、失败原因和失败次数等信息。
	访问源分析：可展现不同数据库节点的访问源统计、分析状态。
对象统计	以操作类型为维度，统计表级别对象被访问次数，可生成行为轨迹图； 并可通过对象的访问次数，下钻追溯到该表对象下所有的访问语句详情，以及该表对象访问来源。
统计信息环比	获取同一数据库不同时间段及不同数据库同一时间段的 SQL 语句量和会话量的对比统计数据以及变化趋势。
行为建模	可基于单个数据库建立学习期，默认学习期内行为可信认，学习期结束后，产生的数据标记为新型对象、新型语句模板
数据管理	日志备份与恢复管理，支持审计日志数据的备份与恢复，支持自动备份，备份数据可以选择**高性能或高压缩比**，支持的备份服务器类型至少包含 FTP、SFTP、NFS 方式，备份记录可以查询。

	支持 KAFKA、SYSLOG 方式进行审计数据外送； KAFKA 外送审计数据内容包括：客户端 IP、客户端端口、客户端 MAC、数据库用户名、数据库实例名等会话信息，SQL 语句参数、SQL 捕获时间、结果集、语句模板、SQL 语句等语句详细信息。
IP 别名管理	支持客户端 IP 别名设置，针对不同客户端 IP 自定义别名展现。
分组管理	支持 IP 地址、数据库用户、时间、对象、应用用户分组，并且分组对象可以直接在规则中引用。
运维管理	审计设备 WEB 界面提供自动诊断功能，可以自动收集实例级参数、策略中心参数、操作系统参数、应用中间件参数。
告警管理	系统告警内容支持网卡异常、分区超限、异常关机、CPU 超限、内存超限、会话超限、包数超限、SQL 数超限、agent 异常等
	风险告警内容支持触发规则风险内容，并支持根据风险等级高、中、低进行告警通知。
	告警方式包括：邮件、短信、SYSLOG、SNMP、企业微信、审计系统前台界面；支持短信平台对接，发起告警操作。
系统管理	支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色，并且可以新建不同用户，分配不同数据库权限和不同的菜单管理权限。
	系统支持 LDAP/AD 域对接，支持 AD 域用户关联审计系统用户，通过 AD 域账户统一登录审计系统。
	具有自身安全审计功能，可以对审计系统的所有用户操作进行审计记录。

服务范围：针对入云业务系统数据库展开。

服务成果（包括但不仅限于）：针对入云业务系统服务期内提供 2 份《数据库审计服务报告》，每半年一份。

3.3.6 本地数据备份服务

服务内容：针对入云系统数据库提供本地数据备份和恢复服务，并提供备份策略配置和维护服务。

服务方式：通过在虚拟机中部署数据备份系统来实现。

数据备份系统指标要求：

指标项	指标要求
备份功能要求	支持 Windows、Linux 及 Unix 操作系统下的文件、操作系统、数据库、应用等在线备份；
	支持不同平台下 Oracle10G 11G 版本、Oracle RAC、SQL Server、MySQL5.6 等国外数据库备份及恢复；
	支持人大金仓 V7、达梦、南大通用 GBase、神通等国产数据库备份及恢复功能
	提供远程灾备功能，采用对等多主控模式，各主控能独立工作；支持断点续传、双向缓冲、流量控制、传输时间段限制、压缩、加密等有效的广域网数据备份技术，减少网络通信流量，提高数据传输的稳定性和高效性；并可实现一对一、

	一对多、多对一、多对多的远程备份容灾方式。
	支持打包备份功能、备份任务自动拆分处理功能，可针对细碎文件进行有效的备份处理，并支持对各种数据库进行脚本备份功能；
管理功能	简洁的图形化管理能力，提供中文管理界面； 允许用户可自行规划、划分、分配磁盘 LUN 组及修改配置

服务范围：针对入云业务系统数据库展开。

服务成果（包括但不仅限于）：针对入云业务系统服务期内提供 1 份《本地数据备份服务报告》。

3.3.7 数据库加密服务

服务内容：加强用户数据的安全防护，防止数据信息泄露，防止非法入侵敏感数据，防止内部人员数据窃取和违规数据访问等，建立数据库的纵深防御体系，保证用户应用系统数据安全；以数据库访问控制为基础，以攻击防护和敏感数据保护为核心，梳理敏感数据，对 SQL 协议进行解析，对非法操作和命令进行拦截和报警。

服务方式：通过在虚拟机上部署数据库加密与访问控制系统来实现。

服务范围：针对入云业务系统云主机数据库展开。

服务成果（包括但不仅限于）：针对入云业务系统服务期内提供 1 份《数据库加密服务报告》。

3.3.8 东西向策略梳理和防护服务

服务内容：实现 VPC 内部安全域之间的隔离和访问控制。针对东西向安全策略进行梳理，并提供政务云东西向的网络区域隔离防护。实现用户 VPC 内部不同安全域之间访问控制，在不同安全域之间实现基于应用特征、行为和关联信息的应用识别和访问控制策略，满足等级保护关于划分安全域和边界防护的要求。

服务范围：2 个 VPC。

服务成果（包括但不仅限于）：服务期内提供 2 份《东西向策略梳理和防护服务报告》（每半年一份）。

3.3.9 数据库防火墙服务

服务内容：有效抵御并消除由于数据库漏洞导致的安全问题，保护核心数据安全。

服务方式：通过在虚拟机上部署数据库防火墙系统来实现。

数据库防火墙系统指标要求：

指标项	指标参数
数据库兼容性	支持 Oracle、mySQL、SQL Server、DB2、Sybase、informix 等主流数据库协议的解析
	支持 postgreSQL、Cache、Teradata、HANA 等专业数据库协议的解析
	支持达梦、人大金仓、南大通用、神舟通用等国产数据库协议的解析
	支持主流大数据平台数据库的解析，包括 Redis、MongoDB、Hive、Kafka、ES 等
部署模式	支持直路串联、代理网关和旁路路由部署模式，并均支持数据风险操作阻断。
	支持虚拟化部署。
防护策略	支持内置针对 Oracle、mySQL、SQL Server、DB2、达梦等各数据库特征的默认防护策略
	支持内置默认的刷库、拖库、撞库的防护策略
	支持 PLSQL 超级白名单防护策略，支持基于各类型数据库的 SQL 白名单策略控制防护，超级白名单规则不少于 100 条。
	支持自定义规则策略配置及管理，可对预设条件进行阻断。预设条件至少包括访问的时间、执行时长、访问次数、访问客户端 IP、客户端操作系统主机名、MAC 地址、客户端操作系统用户名、数据库用户名、数据库实例、表、列、存储过程等、操作类型：DML、DDL、DCL、SQL 语句、SQL 字符串、SQL 语句、返回行数、敏感数据状态、关联表个数、响应状态等
	支持 SQL 注入特征识别，支持基于 CVE 的 SQL 注入漏洞检测，支持根据内部 SQL 注入特征库进行识别并有效阻断，支持 SQLMap 注入检测。
	支持虚拟补丁防护，内置多种数据库漏洞补丁，支持特征方式的缓冲区溢出检测规则以及其它漏洞检测规则，对外来攻击进行识别并有效阻断支持，Oracle 数据库漏洞数量不低于 500 个。
智能学习	支持基于机器学习技术对用户行为进行学习并生成基线规则，支持基线规则策略与其它防护策略同时生效。支持特征值大小控制。支持特征模型持续更新、手动修改、例外加入等操作。
	支持对基线学习内容的特征展示和修改，特征内容至少包括数据库用户、源 IP、目标数据库 、源应用程序、主机名、系统用户名、表与操作、查询组、特权操作等。
	支持偏离基线的行为检测，包括未授权的源 IP 特征、偏离基线的主机特征、操作系统用户特征、源应用程序特征、数据库用户特征、数据库 Schema 特征、表/操作访问特征、查询特征等。支持对于上述基线偏离行为进行风险级别和应对动作设置，应对动作支持操作 t 行为阻断并实时告警。
日志查询	支持日志内容能够详尽的显示访问行为发生的具体特征，包括数据库名称、操作类型、数据库用户、操作对象、数据库 IP、客户端 IP、数据库 MAC 地址、客户端 MAC 地址、主机名、系统用户名、源应用程序、客户端端口、捕获时间、执行时长、响应状态、动作、记录方式、风险等级、匹配策略、SQL 内容、SQL 结果、SQL 模式、日志 ID、数据敏感度、返回行数等
	支持根据日志具体特征、策略、风险等级、时间等进行条件检索，支持对实时防护数据和历史数据进行监控与查询，并支持结果导出，支持 PDF、

	EXCEL、WORD 等文件格式。
	支持日志会话回放功能，还原用户的访问行为
风险告警	支持以数据源和时间（年、月、日、时、分）的方式进行告警日志汇总显示和告警日志查询，支持以折线图的形式显示攻击趋势和访问来源趋势。
	支持自定义告警的风险等级策略，包括低风险、中风险、高风险、致命四个等级
	支持根据客户不同业务情况对告警信息进行自定义处理，包括加入基线、加入 SQL 注入例外、禁用 SQL 注入规则、阻断攻击、通过攻击
统计报表	支持视图、服务器分析、来源分析、数据访问模式、特权操作、其他视图、基于时间的分析等报表类型的添加和删除操作。支持针对各类型报表进行详细内容的自定义配置。
	支持报表自动生成和自动发送，并可生成定时和周期报表任务。
可靠稳定性	支持软件 byPass，设备运行时软件层面出现异常，自动透传数据库访问流量，防止单点故障。
系统管理	支持三权分立，内置系统管理员、安全管理员、审计管理员，以满足合规要求。支持角色创建，支持针对某些功能页面进行授权。
	支持对系统的 CPU、内存、磁盘、磁盘读写情况、网络流量、访问情况、事件统计、攻击记录、告警列表、引擎列表进行实时监控
	支持系统配置+审计日志的全量备份 支持的备份方式：手工备份、定时自动备份、自动远程备份； 支持手工方式还原和备份文件手工、自动方式清理
	支持系统时间手工、自动与 NTP 服务器同步，保证审计日志时间准确性。
	支持用户登录安全设置，包括登录次数、超限锁定时间、用户会话超时等；支持导出文件密码设定。
	支持告警配置及多种告警发送方式，至少包括 FTP、Email、syslog、SNMP。
	支持页面方式进行系统升级和配置导入导出功能。
	支持系统能够自动对审计进程、解析进程、存储进程、检索进程进行诊断分析，方便用户排除故障。
	支持磁盘使用率监控，当磁盘使用率达到预定的阈值时，页面弹框提示管理员，同时系统停止记录日志或者覆盖以前的记录；支持磁盘使用率超限时，自动清理历史业务数据文件。
	支持系统恢复出厂设置，支持页面关机和重启。

服务范围：针对云上业务系统数据库展开。

服务成果（包括但不仅限于）：针对入云业务系统服务期内提供 1 份《数据库防火墙服务报告》。

3.3.10 数据库漏扫服务

服务内容：能够精准检测数据库中存在的各种漏洞问题，包括 SQL 注入漏洞、权限绕过漏洞等，在数据库受到危害之前为管理员提供专业、有效的安全分析和修补建议。

服务范围：针对云上的业务系统云主机数据库展开。

服务频次：入云业务系统云主机服务期内提供 4 次。

服务成果（包括但不仅限于）：针对入云业务系统服务期内提供 4 份《数据库漏扫服务报告》（每季度一份）。

3.3.11 互联网应用级入侵检测和防御服务

服务内容：通过互联网应用级入侵检测和防御服务，对互联网应用系统进行事前、事中和事后的全周期防护。

服务方式：通过在互联网应用虚拟机上部署互联网应用级入侵检测和防御系统来实现。

互联网应用级入侵检测和防御系统指标要求：

指标项	指标要求
Web 防护功能	需支持对 Web 相关应用协议进行自定义功能，并提供详细协议分析变量，具备协议识别与分析能力、网络层访问控制能力和 Web 防护能力。
	需支持 HTTP 协议验证、支持常规入侵攻击防护、恶意爬行程序防护、SQL 注入攻击类防护、跨站点脚本攻击防护、命令注入类攻击防护、命令执行类攻击防护、弱密码类攻击防护、文件上传类攻击防护、文件下载类攻击防护、信息泄露类攻击防护和中间件通用漏洞防护功能。
	需支持 CC 攻击防护功能，基于来源 IP、 Rerferer、特定 URL 攻击防护。
	需支持 ASCII、Unicode 编码及各种混淆编码的还原功能
安全设置	需支持基于 IP、端口号的保护列表设置功能；
	需支持对 HTTP 请求方式设置功能，报头各字段长度限制、URL 关键字过滤、后缀名过滤、web 服务器返回代码及返回内容设置。
	需支持智能黑名单设置功能，特定 IP 在攻击行为达到系统设定的阈值，则系统会自动把该 IP 添加至“黑名单”
	需支持内置策略组、策略自定义组合设置功能，可选策略≥10 条。
管理功能	需支持 B/S 管理功能，通过 Web 浏览器对进行远程管理；
	需支持导入升级包的方式一键升级功能
	需支持三员管理功能，并满足管理员自定义。
报表功能	需支持拦截统计、网络接口流量统计等类型的报表统计功能。
	需支持按事件类型、保护网站的 IP、时间等条件进行报表查询功能
	需支持根据月、周、日、时对网站安全状态进行动态安全评估功能，并以分数形式体现给客户。
日志系统	需支持日志审计功能，包括不仅限于系统日志、审计日志和安全防护日志。
	需支持日志查询功能。包括不仅限于基于时间、IP、危害类别、请求方法等。

	需支持日志管理功能，包括不仅限于日志导出、导入、删除；
系统监控	需支持显示网络接口状态、引擎状态、系统 CPU 及内存使用率等功能；
高可用性	需支持主从部署模式、双机配置自动同步、心跳同步；需支持串联部署和旁路部署；需支持防护模式的切换、安全系数更改和双向检测。
	需支持内置 bypass 模块，发生故障直接切换到 bypass 模式

服务范围：针对互联网应用展开。

服务成果（包括但不仅限于）：针对互联网应用服务期内提供 4 份《互联网应用级入侵检测和防御服务报告》每季度一次。

3.3.12 可信验证

服务内容：针对虚拟机操作系统引导程序、系统程序、重要配置参数和应用程序进行可信验证，并在应用程序关键执行环节进行动态可信验证，从保障主机操作系统安全的角度出发，以可信计算为基础、访问控制为核心，构建主动防御体系，从源头上保证云主机安全，提供虚拟机操作系统内核级加固、强身份鉴别、重要数据资源保护、网络访问控制等安全机制。

服务方式：通过在虚拟机上部署主机可信验证系统进行交付。

主机可信验证系统指标要求：

指标项	指标要求
部署方式	需支持云环境下软件部署，支持主流云架构。
	需支持单机部署和集群部署
	需支持 Windows、Linux 主流系统部署
可信度量	需支持软件白名单，不在白名单的程序将拒绝执行
	需支持在终端软件安装时可自动采集本地执行程序形成白名单,以后需通过管理中心下发白名单策略。
	需支持根据可信计算机制，将可信程序添加到信任列表，为可信度量提供度量依据。
	需支持静态度量机制，对软件程序启动时进行完整性度量，在度量结果和预期值一致的前提下，该程序才允许运行，否则拒绝运行。
	需支持动态度量机制，对进程、模块、文件系统等操作系统运行中的关键数据进行监控
访问控制	需支持自主访问控制，控制终端中用户和进程对目录、文件的访问和操作，防止其他用户对自己的客体进行攻击
	需支持强制访问控制，支持对重要主体及客体的安全标记，控制主体对于客

	体的访问权限，实施强制访问控制，严格控制用户行为。主体包括用户、进程等，客体包括文件、进程和设备等
策略管理	需支持对接入终端的策略、资源的统一管理以及审计的统计与分析功能；
	需支持一个终端或一组终端进行策略的管理。
	需支持策略备份功能，包括手动备份和定时备份；
	需支持策略备份还原功能；
系统管理	需支持终端的注册、注销功能
	需支持三权分立管理模式，将管理员划分系统管理员、安全管理员、安全审计员；
	需支持受控终端 CPU、内存资源、开放端口、当前运行进程的使用情况展示。
	需支持运维模式和调试模式；
	需支持证书管理，包括管理平台、软件库、终端证书；
软件管理	需支持软件自保护功能，终端软件安全运行、使用，防止非法篡改或停止。
	需支持可靠的软件采集和验证，将 Windows 和 Linux 平台的软件统一纳入软件库进行运维管理。
	需支持最小化安装原则，根据不同节点的业务需求，主动推送相关应用软件。
	需支持应用软件版本控制，可灵活应用相同软件的不同版本，其他版本禁止安装，降低软件版本带来的安全风险。
	需支持支持远程推送安装，支持自动化静默安装。
日志审计	需支持日志采集功能，包括用户登录、主体访问客体、配置更改，数据上传、终端管理等
	需支持终端审计、 软件库和管理平台自身审计的展示、查询
设备升级	需支持终端批量升级功能

服务范围：针对入云业务系统的云主机展开。

服务成果（包括但不仅限于）：针对入云业务系统服务期内提供 1 份《可信验证服务报告》。

3.3.13 日志收集与分析服务

服务内容：通过日志收集与分析的方式，对业务系统访问日志和运行日志进行数据分析，发现安全风险和入侵行为，当存在安全问题时，提出相关内容并给出解决建议。

服务范围：针对云上的业务系统云主机展开。

服务频次：入云业务系统云主机服务期内提供 2 次。

服务成果（包括但不仅限于）：针对业务系统服务期内提供2份《日志收集与分析服务报告》（每半年一份）。

3.3.14 渗透测试服务

服务内容：从攻击者的角度去分析目标所存在的安全隐患以及脆弱性，以全面了解和掌握应用系统所面临的安全威胁和存在的风险。采用专业测试工具针对云上业务系统环境主机、网络设备、应用系统等进行受控的、非破坏性的渗透测试，通过模拟黑客对目标系统进行渗透测试，对系统的任何弱点、技术缺陷或漏洞进行主动分析，评估系统抗攻击能力，全面了解和掌握应用系统所面临的安全威胁和存在的风险，为开展安全加固及优化建设提供依据，并指导实施调优及加固工作，以切实保证信息系统安全。

服务范围：针对云上的业务系统展开。

服务频次：入云业务系统云主机服务期内提供2次。

服务成果（包括但不仅限于）：针对入云业务系统服务期内提供2份《渗透测试报告》（每半年一份）。

3.4常态化安全服务

常态化安全服务包括应急保障服务、安全通告服务和安全管理制度修订服务。

3.4.1 应急保障服务

（1）应急预案修订与完善

服务内容：研究制定局内应急预案体系，内容将包含制定相应应急响应组织、预防、预警机制、事件定义分类、应急响应程序、事件上报处理机制、后期处理机制等内容，具体将分为综合预案、专题预案以及特定预案。在预案修订与完善的咨询服务过程中，将与局内相关人员保持紧密的沟通合作，以确保预案的科学性、指导性和合理性。

服务范围：针对药监局在政务云上业务系统展开。

服务频次：服务期内提供1次。

服务成果（包括但不仅限于）：服务期内提交1份《应急预案》（修订版）

（2）应急演练

服务内容：供应商应根据信息化主管部门要求，不定期地进行网络信息安全方面的应急演练，模拟实战对业务信息系统开展防御演练。

供应商应根据用户的安排每年至少进行 1 次网络信息安全应急演练。应急演练需模拟实际攻防环境，包括网络攻击、应用系统防御、病毒入侵等方面的内容。应急演练结束后供应商需对演练进行总结，以提高运维人员实际处理突发事件的能力。

服务范围：针对云上业务系统展开。

服务频次：服务期内提供 2 次。

服务成果（包括但不仅限于）：服务期内提交 2 份《应急演练报告》（每半年一份）。

（3）应急响应

服务内容:在信息系统发生安全事件时及时响应，执行应急响应流程，通过专家级技术支持和快速响应，及时抑制和消除用户信息系统安全事件，减少损失和负面影响，提高药监局信息系统业务连续性。

服务范围：针对云上业务系统展开。

服务频次：服务期内按需提供。

服务成果（包括但不仅限于）：服务期内提交 2 份《应急响应报告》（每半年一份）

3.4.2 安全通告

服务内容：供应商应组织专人定期搜集整理漏洞信息、系统补丁信息、病毒信息等安全状态信息，形成安全通告信息，并定期以电子邮件的方式发送给用户信息安全负责人，确保用户在第一时间内得到相关的安全态势信息。

服务范围：针对云上业务系统展开。

服务频次：每周 1 次，整个服务期共 52 次。

服务成果（包括但不仅限于）：服务期内提交 52 份《安全通告》。

3.4.3 安全管理制度修订

服务内容：基于用户实际信息化组织结构情况，参考信息安全等级保护管理要求，从安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运

维管理等方面修订和完善安全管理制度，健全相应的安全管理组织架构，明确相应岗位和职责，完善安全管理和操作流程。

服务范围：针对云上业务系统展开。

服务频次：服务期内提供 1 次。

服务成果（包括但不仅限于）：合同签订后 1 个月内提交 1 份《安全管理制度》，并组织实时修订。

3.4.4 安全巡检

服务内容：供应商应根据服务合同要求的安全巡检指标，定期对云上业务系统云主机操作系统、数据库、中间件性能、状态、策略进行安全巡检，分析历史状态或事件记录，可以发现系统数据库中隐藏的安全隐患，并及时落实补救措施，重点搜集分析当月日志信息，并做好巡检记录。

服务范围：针对云上业务系统展开。

服务频率：安全巡检工作频率为 1 次/月。

提交成果：服务期内提交 12 份《安全巡检报告》。

3.4.5 脆弱性检测

服务内容：供应商应针对北京市药品监督管理局信息系统云主机操作系统、数据库、中间件采用工具扫描和手工检测的方式进行脆弱性检测，检测存在的漏洞、补丁、端口开放情况等，并进行脆弱性分析。

服务范围：针对云上业务系统展开。

服务频率:服务期内提供 2 次。

提交成果:服务期内提交 2 份《脆弱性检测报告》（每半年一份）。

3.5有需性安全服务

代码审计：服务内容：源代码审计服务是通过对代码的检测，检查，识别发现代码中的安全漏洞，性能瓶颈，逻辑错误等问题，帮助开发人员在应用系统错误蔓延前发现问题。

服务范围：针对存在重大调整或新上线的业务系统

服务频次：按需开展，一年内最多 2 次。

服务成果（包括但不仅限于）:《源代码审计报告》

4.服务团队和人员要求

供应商必须向药监局提供拟派参加本项目的主要人员名单、项目组织结构以及各自职责的划分，并附上核心项目人员简历。所报项目组成员一旦确定，不得擅自更改。

供应商必须向药监局保证成交后服务人员的稳定性项目实施的主要成员，在本项目服务结束前，参加本项目的人员变动必须取得药监局同意。供应商必须保证其项目组人员严格按照工作实施方案实施。供应商核心人员包括：项目经理、安全专家、高级技术人员、关键岗位成员等。

成交供应商应组织项目团队完成本项目安全运维服务及其他工作，此外还需派驻驻场安全运维人员不少于1人，完成本项目中相关的组织沟通工作。

成交供应商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。

5.项目服务要求

确定成交供应商后，采购人与成交供应商签订服务合同。

（1）本项目服务时间要求

供应商须在合同结束前完成本项目所有服务内容，供应商要按照服务内容的要求，制定具体的实施方案，做好进度和任务安排。

（2）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。

（3）保密要求

供应商在响应文件中应针对本组织的项目管理措施、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的完成。

成交供应商要严格遵守国家《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》。供应商负责对《保密承诺书》归档保管，接受药监局检查。供应商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。

（4）其他要求

采购人将在成交后针对重要招标要求对成交供应商进行确认和检查，供应商不得虚假投标，否则药监局有权废除成交结果，并追究供应商责任和赔偿。

6. 项目验收

成交供应商最晚应在服务合同到期之后 15 天之内完成项目终验。提供纸质和电子版的项目验收文档。供应商应在项目验收时做好项目质量控制、成本控制、进度控制等管理，做好项目过程中各种文档的管理，如招响应文件、合同、会议纪要、验收报告等，在验收阶段提供验收报告。