**采购需求**

1. **采购项目情况**
	1. **项目基本情况**

1.项目名称：信息系统租用市级政务云资源\_

2.项目预算金额：886.3万元

3.采购包情况：

|  |  |  |  |
| --- | --- | --- | --- |
| 包号 | 标的名称 | 采购包预算金额（万元） | 数量 |
| 01 | 北京市科学技术委员会、中关村科技园区管理委员会综合事务中心2025年信息系统租用市级政务云资源采购项目 | 886.3 | 1 |

4.合同履行期限：12个月\_

5.本项目是否接受联合体投标：□是 ☑否。

1. **规范性引用文件**
	1. **国家及北京市有关政策**

1.《关键信息基础设施安全保护条例》（中华人民共和国国务院令第745号）

2.《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）

3.《政府采购需求管理办法》(财库〔2021〕22号)

4.《关于促进政府采购公平竞争优化营商环境的通知》（财库〔2019〕38号）

5.《关于进一步提高政府采购透明度和采购效率相关事项的通知》（财办库〔2023〕243号）

6.《工业和信息化部信息通信管理局关于督促互联网网络接入服务企业依法持证经营的通知》（工信管函〔2018〕84号）

7.《云计算服务安全评估办法》（国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部公告2019年2号）

8.《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文〔2014〕14号）

9.《基于云计算的电子政务公共平台顶层设计指南》

10.《北京市财政局关于印发<北京市政府采购负面清单>的通知》（京财采购〔2020〕1345号）

11.《关于印发<关于推进我市政务信息系统整合共享的实施方案>的通知》（京经信委发〔2017〕89号）

12.《北京市人民政府关于印发<北京市政务信息资源管理办法（试行）>的通知》（京政发〔2017〕37号）

13.《关于印发<北京市市级政务云管理办法>的通知》（京经信函〔2019〕150号）

14.《北京市政务网络和数据安全管理办法》（京经信发〔2023〕57号）

* 1. **国家相关标准**
1. 《国家电子政务外网安全接入平台技术规范》
2. 《信息技术—云计算—云服务质量评价指标》（GB/T 37738-2019）
3. 《信息技术—云计算—云服务计量指标》（GB/T 37735-2019）
4. 《信息技术—云计算—云服务采购指南》（GB/T 37734-2019）
5. 《信息技术—云计算—云存储系统服务接口功能》（GB/T 37732-2019）
6. 《信息技术—云计算—云资源监控通用要求》（GB/T 37736-2019）
7. 《信息技术—云计算—云平台间应用和数据迁移指南》（GB/T 37740-2019）
8. 《信息技术—云计算—云服务交付要求》（GB/T 37741-2019）
9. 《信息系统灾难恢复规范》（GB/T 20988-2007）
10. 《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）
11. 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
12. 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
13. 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）
14. 《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）
15. 《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）
16. 《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）
17. 《信息安全技术 政府网站云计算服务安全指南》（GB/T 38249—2019）
18. 《信息安全技术 云计算安全参考架构》（GB/T 35279—2017）
19. 《信息安全技术 云计算服务安全能力评估方法》GB/T 34942—2017
20. 《信息安全技术 云计算服务运行监管框架》（GB/T 37972—2019）
21. 《信息技术 云资源监控指标体系》（GB/T 37938-2019）
22. 《电子信息系统机房设计规范》（GB50174-2017）
23. 《数据中心电信基础设施标准》（ANSI/TIA-942）
24. 《综合布线系统工程设计规范》（GB 50311—2016）
25. 《云计算关键领域安全指南V4.0》
	1. **北京市相关标准**
26. 《政务云平台建设技术要求》（DB11/T 2169-2023）
27. 《北京市政务云安全技术规范 IaaS云计算平台分册》
28. 《北京市政务云安全技术规范 IaaS云计算平台安全监管接口分册》
29. 《北京市政务云安全技术规范 信息安全服务接口分册》
	1. **其他**
30. 《北京市市级行政事业单位云计算服务框架协议采购项目（2023 年度）》征集文件第四部分采购需求中技术要求
31. **项目背景**

为贯彻落实北京市《北京市市级政务云管理办法》要求，我委于2021年底将全部信息系统迁入北京市级政务云，依托北京市级政务云平台为系统提供基础环境支撑，提升系统应用的安全稳定性、互联互通功能，以更好地为业务系统运行提供保障。截至目前，业务系统运行稳定。

持续租用市级政务云服务，完成已入云业务系统架构优化，提升系统可用性、可靠性、稳定性和安全性。根据系统安全等级评测要求，部署安全保障服务，提升各业务系统安全防护水平。并在此过程中对业务系统运行环境进行持续优化与改造，充分优化系统整体健壮性，提高系统可靠性。保障信息系统的日常稳定运行，开展政务云服务租赁。

1. **技术参数要求**
	1. **政务云基础服务**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **服务类别** | **服务子类** | **服务项** | **计价单位** | **报价单位** | **数量** | **期限** |
| **计算服务** | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1 CPU | 元/月 | 1251 | 12 |
| 内存 | 1 GB | 元/月 | 3849 | 12 |
| x86物理服务器租用服务 | x86 物理服务器配置2：4 路12 核（主频≥2.0Ghz），128G内存，2 块600G SAS 硬盘，2 个HBA 卡，2 个万兆端口 | 1 台 | 元/月 | 11 | 12 |
| 内存-32GB内存 | 1条 | 元/月 | 44 | 12 |
| 硬盘配置2-600GB SAS | 1块 | 元/月 | 75 | 12 |
| **存储服务** | 普通性能存储 | 普通存储（单盘技术指标:单盘IOPS 1000-3000 ） | 1 GB | 元/月 | 163436 | 12 |
| 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） | 1 GB | 元/月 | 163436 | 12 |
| 本地备份服务 | 本地备份服务 | 1GB | 元/月 | 163436 | 12 |
| **网络服务** | 互联网链路服务 | 互联网链路带宽 | 1 Mb | 元/月 | 900 | 12 |
| 互联网IP地址租用服务、并提供备案服务 | 1 IP | 元/月 | 16 | 12 |
| 主机负载均衡服务 | 主机负载均衡服务 | 1 IP（内网） | 元/月 | 16 | 12 |
| 远程接入服务 | 远程接入服务 | 1账号 | 元/月 | 48 | 12 |
| VPN服务 | SSL VPN接入 | 1套 | 元/月 | 48 | 12 |
| SSL证书服务 | 提供SSL 证书服务 | 1域名 | 元/月 | 6 | 12 |
| WAF防护 | web应用防火墙服务 | 1 IP（互联网） | 元/月 | 16 | 12 |

* 1. **政务云扩展服务**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **服务类别** | **服务子类** | **服务项** | **计价单位** | **报价单位** | **数量** | **期限** |
| 安全服务 | 主机杀毒服务 | 主机杀毒服务 | 1 台 | 元/月 | 199 | 12 |
| 云端抗DDOS服务 | 云端抗DDOS 服务  | 1 站点 | 元/月 | 6 | 12 |
| 主机防护 | 主机防护 | 1 台 | 元/月 | 199 | 12 |
| 主机日志分析 | 主机日志分析 | 1 台 | 元/月 | 199 | 12 |
| 数据库审计服务 | 数据库审计服务 | 1 套 | 元/月 | 4 | 12 |
| 其他服务 | 短信服务 | 提供短信服务 | 1条 | 元/月 | 799288 | 1 |
| 提供系统国密浏览器、ssl VPN等密码服务 | 提供系统国密浏览器、ssl VPN、强身份认证服务、加解密等密码服务 | 1套 | 元/月 | 2 | 12 |
| 单位端电子缴款书服务 | 通过单位端电子缴款书服务平台向甲方提供单位端电子缴款书服务及相关技术支持服务 | 1套 | 元/月 | 1 | 12 |

1. **采购目标**

本项目的总体目标是通过持续租用政务云平台计算服务、存储服务、网络服务、基础软件支撑服务、安全服务、其他服务（包含短信服务、密码服务和单位端电子缴款书服务）等。提供全年7×24小时运维保障，做好重大活动和节假日应急值守保障服务，对我委云上业务系统的运行环境进行持续优化，充分优化系统整体兼容性，提高系统可靠性；完成日常运维和安全运维服务工作配合我委做好网络安全及密码应用等相关工作，确保各信息系统在政务云环境中安全、稳定运行。

1. **服务内容与服务标准**
	1. **计算服务**
		1. **服务内容**

按照采购人的具体需求，提供云主机服务，包括：x86 平台云主机服务和x86 物理服务器租用服务，按需求对CPU及内存进行动态调整，实现合理的计算资源配置。在提供政务云主机的服务过程中做好与采购人和对应项目应用开发厂商的协调沟通工作。

* + 1. **服务标准**

1.2.1 云主机应实现物理机的全部功能，如具有CPU、存储、内存、网卡等资源，可以指定单独的IP地址等；

1.2.2 支持存储裸设备映射（RDM），可以将存储设备上的LUN直接映射给虚拟机使用，并且支持SCSI指令使用透传模式或者非透传模式；

1.2.3 应满足云主机之间、CPU之间隔离保护要求；

1.2.4 支持资源的动态调整，根据业务的负载情况实现业务系统虚拟机的动态扩展和回收；

1.2.5 支持在线进行虚拟化软件版本升级，不同版本之间可以相互兼容；

1.2.6 支持异构虚拟化能力，如KVM等多种虚拟化技术；

1.2.7 云主机出现故障时，支持自动重启或者迁移，保障业务连续性；

1.2.8 支持虚拟机热迁移，可在不同代CPU资源池中进行虚拟机热迁移；

1.2.9 云计算资源性能要求包括但不限于如下：

1.2.9.1 物理服务器CPU主频应不低于2.40GHz；

1.2.9.2 主机内存硬件配置不低于DDR4-2400MHz；

1.2.9.3 可用性不低于99.99%。

* 1. **存储服务**
		1. **服务内容**

按照采购人的具体需求，提供存储服务，包括：普通性能存储、高性能存储和本地备份服务，实现合理的存储资源配置。在提供政务云存储的服务过程中需做好采购人和对应项目应用开发厂商的协调沟通工作。

* + 1. **服务标准**

2.2.1 支持结构化数据、半结构化数据和非结构化数据等多种数据类型存储；

2.2.2 支持块存储、对象存储、文件存储等多种存储方法，满足数据备份、视频存储等不同应用场景使用要求；

2.2.3 支持存储资源扩展能力，例如：PB级扩展；

2.2.4 支持磁盘容错技术，如磁盘故障后节点的自动平衡和重构、硬盘故障 检测和处理、集群节点出现单盘故障时不影响业务运行等；

2.2.5 存储资源性能要求包括但不限于如下：

2.2.5.1 吞吐量：高性能存储系统的读写带宽应不低于1000MB/s,IOPS不低于20000;普通性能存储系统的读写带宽应不低于200MB/s，IOPS不低于1000。

2.2.5.2 支持高可靠性，可靠性不低于99.9999%%；

* 1. **备份服务**
		1. **服务内容**

投标人需具有本地数据级备份能力，并配合采购人完成数据级容灾演练及恢复等工作。

* + 1. **服务标准**

按照采购人的各个应用系统对资源的备份需求通过备份策略实现对用户数据（文件、操作系统、数据库）的本地备份（不包含备份存储空间费用），默认提供非结构化数据保护与文件备份保护。备份应满足如下要求:

3.2.1 备份介质本身具备高可用性和冗余性。

3.2.2 备份方式包括完整备份、差异备份和增量备份。

3.2.3 支持Windows系列操作系统、Linux主流系统操作系统、主流数据库软件、主流中间件软件、结构化数据以及非结构化数据等备份对象。

3.2.4 投标人应提供对备份过程状态、备份结果提供运维监控保障服务，确保备份任务执行成功以及备份的数据完整性。

* 1. **网络服务**
		1. **服务内容**
			1. 互联网链路服务

提供互联网链路带宽服务、互联网 IP 地址租用服务，并提供相应的网络域名备案服务，配合应用开发厂商提供网络策略配置服务。

* + - 1. 主机负载均衡服务

提供主机负载均衡服务，通过云管理平台实现针每租户按需自动分配负载均衡服务的能力。

* + - 1. 远程接入服务

提供远程接入服务，每个账号结合身份验证接入堡垒机维护应用系统。

* + - 1. VPN服务

提供SSLVPN接入须实现Web接入，TCP接入，IP接入等多种方式，能够记录完整的用户访问日志；支持基于用户身份的管理，实现不同身份的用户拥有不同的命令执行权限，并且支持用户视图分级，对于不同级别的用户赋予不同的管理配置权限；可以根据请求报文的目的IP地址和目的端口号、源IP地址和源端口号进行过滤；采用通过商用密码产品认证的SSLVPN产品。

* + - 1. SSL证书服务

提供SSL（Secure Sockets Layer，安全套接字协议）证书服务，证书类型为组织验证证书 (OV SSL)，兼容当前主流桌面和移动端操作系统、邮件客户端软件，支持RSA算法和ECC算法；保证系统数据的SSL加密传输。

* + - 1. WAF防护服务

提供WAF防护服务，在政务云流量入口架设WAF（Web Application Firewall，网站应用级入侵防御系统）防护服务，保证用户网站对已知安全隐患进行防御。

* + 1. **服务标准**
			1. 云内骨干线路带宽不低于10Gb/s；
			2. 服务器业务带宽不低于1Gb/s；
			3. 平均可用性不低于99.9%。
	1. **基础软件支撑服务**
		1. **服务内容**

提供国产操作系统、开源操作系统、开源应用中间件、国产数据库管理系统、国产数据库读写分离集群软件、开源数据库等软件服务。

* + 1. **服务标准**
			1. 国产操作系统租用服务

提供国产操作系统的租用、安装、调优、排错、技术支持服务。

* + - 1. 开源操作系统租用服务

按照采购人的具体需求提供CentOS等开源操作系统租用服务，并在提供服务的过程中做好与采购人及对应信息系统建设及运维厂商的协调沟通对接工作。

* + - 1. 开源应用中间件租用服务

提供主流开源中间件租用服务，应支持Tomcat等中间件的各种版本，并提供中间件的安装部署和各种故障处理和日常维护。

* + - 1. 国产数据库管理系统租用服务

由云服务商提供主流国产商用数据库租用服务，应支持3种以上国产数据库单机、集群的主流版本，提供数据库的安装部署和各种故障处理及日常维护。

* + - 1. 国产数据库读写分离集群软件租用服务

提供国产数据库读写分离集群软件的租用、安装、调优、排错、技术支持服务。

* + - 1. 开源数据库租用服务

提供主流开源数据库服务，应支持MYSQL数据库的主流版本，提供数据库的安装部署和各种故障处理及配置优化，提供数据库日常维护。

* 1. **云环境保障服务**
		1. **服务内容**

安全是政务云的红线，应按照网络安全等级保护等要求建设安全技术防护体系和安全管理体系，建立应急处置体系，强化各领域平台安全管控，本项目安全服务主要内容包含：

* + - 1. 主机杀毒服务

提供主机杀毒服务，对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。

* + - 1. 云端抗DDOS（分布式拒绝服务攻击）服务

利用云端海量带宽资源，提供DDOS 防护服务，为云内应用系统抵御大流量分布式拒绝服务攻击。根据流量提供云端抗DDOS服务，避免业务遭受拒绝服务攻击。

* + - 1. 主机防护

按照采购人的具体需求，提供符合等保三级要求的主机权限管理及安全防护。

* + - 1. 主机日志分析

对主机系统日志进行采集分析处理，用于发现各种安全威胁、异常行为事件。主机系统日志应集中存储，且日志存储时间不低于6个月。

* + - 1. 数据库审计服务

提供数据库审计服务，每月对数据库操作行为进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。对用户访问数据库行为的记录、分析和汇报，生成合规报告以及事故追根溯源。在提供服务的过程中做好与业主方和对应项目的应用开发厂商的协调沟通。

* + 1. **服务标准**

投标人所投云平台具备完备的安全防护体系和安全防护设备，具有成熟的安全运维方案，应保证各业务应用系统的支撑环境，包括但不限于服务器、网络、存储以及相关物理环境，应能满足不低于网络安全等级保护（GB/T22239-2019）第三级要求，并积极配合采购人根据各业务系统具体等保需求，开展相应等保评估、检查、整改等工作。

投标人需利用监控系统或人工对机房环境、硬件设备及应用系统的运行情况进行7\*24小时的不间断巡检监控，及时发现安全隐患，通知相关人员及时处理，并形成监控报告。

投标人承担云平台数据防篡改、防丢失的安全责任。业务数据未经采购人同意，不得离开云机房。投标人未经允许不得对云平台上的任何数据进行非法截取、加工、分析处理或提供给第三方机构。投标人在未经过用户邮件、书面材料确认前提下，不能查看、修改、拷贝用户业务系统文件和数据；各业务系统、数据归属于采购人，投标人无权支配。

投标人需保证安全技术服务能力不低于所承载的信息系统的最高级别，并通过GB/T22239相应等级的测评；通过商用密码应用安全性评估，商用密码应用安全性评估参考GB/T39786-2021中相应等级规定。

* 1. **其他服务**
		1. **服务内容**

本项目的其他服务内容包含短信服务、国密浏览器、SSL VPN和单位端电子缴款书服务。

* + 1. **服务标准**
			1. 短信服务

提供云上系统短信接口服务。

* + - 1. 国密浏览器、SSL VPN等密码服务

提供使用国密算法的浏览器：针对现有三级系统，配合SSL VPN，按照租户授权的方式，在云平台与云平台管理员、租户之间建立安全通信通道。

提供SSL VPN：针对现有三级系统，配套安全浏览器、移动终端密码模块等，在云平台与云平台管理员、用户之间建立安全通道，并提供接入认证相关功能。

* + - 1. 单位端电子缴款书服务

提供通过单位端电子缴款书服务平台向甲方提供单位端电子缴款书服务及相关技术支持服务。

* 1. **运维服务**
		1. **服务内容**
			1. 服务规范

投标人须严格按照《北京市市级政务云管理办法》和采购人制定的管理办法、流程及其他汇报制度、应急制度、文档管理、资产管理、基线管理、人员管理、培训与考试、知识库管理、安全管理等相关制度，开展标准化运维工作。

* + - 1. 服务方式

1.投标人需利用监控系统或人工对机房环境、硬件设备及应用系统的运行情况进行全年7×24小时的不间断巡检监控，及时发现安全隐患，通知相关人员及时处理，并形成监控报告。

2.投标人负责设立技术支持热线，并安排专人值守，为运维工作提供全年7×24小时热线支持服务。投标人针对采购人要求的云平台运维服务相关内容，需指定专业技术能力较强的工程师，根据采购人要求配合开展相关维护服务。

3.投标人建立服务团队，团队至少3人，其中至少1名驻场人员提供工作日5×8现场服务，支撑云平台运维服务相关内容；团队成员确需调换的，需经市科委、中关村管委会综合中心同意。

4.投标人应提供全年7×24小时云资源使用情况监控服务，发生云资源使用率过高情况时应及时通知采购人及相应系统运维服务商。每周和每月提供政务云服务报告，其中周报主要报告主要云资源调整及使用情况，针对各信息系统云效率进行统计；月报对当月政务云服务情况进行总结，包括各类云资源调整、使用及服务情况，以及日常维护、应急值守、故障处置等情况。

5.投标人须每季度提出云资源调整建议，其中的云资源占用率较大的重点项目需按月提出调整建议。

* + - 1. 安全及保密要求

投标人须严格遵守采购人的相关网络安全规定，不得擅自修改采购人数据及其他信息或透漏给第三方。

* + - 1. 响应的及时性

1.投标人应能提供高效的云资源及环境维护服务，有效防范系统风险，保证全年7×24小时电话畅通，发生故障应在15分钟内响应；在系统发生除宕机外的其他故障问题时，协调人员在1小时内到达运维现场提供服务。

2.对于虚拟CPU、内存、存储等云主机资源和网络策略的调整，自提出明确需求至完成调整时间不超过4小时，重点保障时期云主机资源调整时间不超过2小时。针对重点保障时期的重要信息系统（根据采购人相关要求确定）的云主机，投标人应按采购人要求进行实时监控，超过预警阈值时主动上调云资源，并第一时间通知采购人进行相应操作，确保系统平稳运行。

3.投标人应具备故障快速响应、定位和恢复能力，入云系统发生故障时，应在30分钟内响应，响应后故障定位排除时限不超过30分钟，其中重要信息系统故障响应后的定位排除时限不超过10分钟，整体需在4个小时之内使系统恢复正常，故障处理完毕后需提供相关系统故障报告。

4.政务云出现故障时，平均响应时间小于等于15分钟，平均故障恢复时间小于等于30分钟。出现故障时应第一时间通知采购人，并及时反馈处置结果，故障结束后应提交相应的应急处置报告。

* + - 1. 重点保障要求

投标人应具备完善的系统服务保障体系，配备足够的技术人员，在重大节假日、重大活动及业务高峰期内加大运维保障力度，保证期间系统平稳运行。重保阶段的重要系统保障满足需要的900MB带宽独享，提供多运营商、多链路的带宽服务，并可灵活调整。

* + 1. **服务标准**

8.2.1 为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求投标人根据业务周期性特点，加大运维保障力度，保证在业务高峰期内系统平稳运行。

8.2.2 重点保障时期重要信息系统云主机资源调整时间不超过1小时，针对重点保障时期的重要信息系统重要云主机，投标人应按采购人要求进行实时监控，超过预警阈值时主动上调云资源，并第一时间通知采购人进行相应操作，确保系统平稳运行。

8.2.3按照国家、北京市相关规定和信息安全技术标准及规范要求,落实安全保障措施,通过信息安全测评机构的测评和政务云安全审查。

8.2.4 除不可抗力或计划内维护作业造成的政务云服务中断外,政务云实行24小时不间断运行。

* 1. **迁移服务**
		1. **服务内容**

投标人需提供整体的业务上云迁移服务，应支持X86云主机迁移、X86物理主机迁移、单机数据库迁移、高可用数据库迁移等迁移场景。提供信创环境迁移服务。负责需求调研、架构规划设计、应用迁移部署等工作。

* + 1. **服务标准**

本项目涉及的业务系统为采购人在用的生产系统，目前在北京市政务云上平稳运行，因此业务连续性是首要的保障需求。迁移服务具体要求如下：

9.2.1 投标人需编制业务连续性服务方案。

9.2.2 本项目如涉及系统迁移，在连续性服务方案中需提供确实可行的迁移部署服务子方案，迁移部署服务子方案应包括（但不限于）迁移部署流程（包含但不限于应用、虚拟机和数据类迁移）、业务系统部署迁移方案。迁移部署服务子方案应明确需要采购人配合的具体工作内容及时长，针对系统迁移过程中容易造成业务系统中断的环节，包含但不限于互联网及政务外网IP变更割接、业务数据同步及切换上线、应急回退方案等，进行风险评估，提出详细解决方案。

9.2.3 本项目如涉及系统迁移，为保障业务系统的连续性，投标人应承诺自中标之日起，积极与原服务商对接，在5个工作日内，完成系统迁移平滑过渡，且因此产生的各项费用（包括但不限于测试阶段的云资源费用，系统开发商对业务系统的部署、调试费用等），应包含在投标人的报价中，提供“承诺函”并加盖投标人公章。

1. **运维团队要求**

服务期内，投标人须设有7×24小时电话响应服务、具备运维团队，提供售后服务保障。团队成员应明确职责，架构清晰，岗位设置合理，且具备与本项目相关的项目经验。

投标人须提供项目经理1人、技术负责人1人以及相应实施人员，项目团队人员8人（含项目经理和技术负责人）及以上。为本项目提供服务。要求如下：

项目经理具备5年及以上类似工作经验，且具有信息系统项目管理师（高级）证书或高级职称等同类证书。

技术负责人具备5年及以上类似工作经验，且具有CISP（注册信息安全专业人员）等同类证书。

团队成员（除项目经理和技术负责人之外）具有CISP等同类证书。

项目技术负责人应是专职负责人，在服务期内不可更换。项目成员如有变化，需提前一个月通知采购人。

1. **商务要求**
	1. **服务地点**

北京市政务云机房及采购人办公地现场。

* 1. **服务期限**

自合同签订之日起12个月。

* 1. **服务费用及支付方式**

1标的费用共计人民币小写：886.3万元。

2合同签订后20个工作日内投标人向采购人提供合同金额80%的增值税普通发票，采购人收到发票后向投标人支付合同金额的80%。

3年底前，投标人向采购人提交已完成工作的总结报告和服务成果，提供合同金额20%的增值税普通发票，采购人确认工作成果并收到发票后向投标人支付合同尾款。

4投标人应在每次付款前向采购人交付等额的法定正规发票。发票应符合开具时国家法律法规及政策对发票类型、税种、税率的相关要求。所开具的发票不符合约定的，采购人有权延期付款，且无需承担违约责任。

* 1. **验收服务标准**
		1. **服务绩效指标**

（1）云服务全年整体可用性≥99.9%；

（2）故障响应率100%；

（3）应急响应时间≤5分钟（重大事件1分钟内响应）；

* + 1. **项目验收要求**

（1）投标人所提供的北京市市级政务云基础资源服务应遵循客观、科学、合理的原则，符合《北京市市级政务云管理办法》的相关标准及要求。

（2）投标人所提供资源应满足采购文件规定的要求。保证合同期内系统安全稳定运行，不因硬件故障导致服务中断4小时及以上。

（3）服务期满后10个工作日开始对合同项目进行验收，投标人应当在采购人指定的验收日前向采购人提交验收报告。验收报告的内容包括但不限于，合同规定的各项服务清单，各系统设备运行情况。

（4）服务期届满，投标人按照采购人要求完成所有项目，各项记录、报告等文档齐全，无任何系统遗留问题，并通过由采购人组织的专家验收评审，方可通过验收。

1. **其他相关要求**
	1. **知识产权和保密要求**

投标人应确保本项目所提交成果无知识产权纠纷，项目成果的知识产权属于项目委托方。

在签订和履行合同过程中从采购人处获知的技术和商业秘密，无论在合同期限内还是合同终止后，均应遵守国家有关版权、专利、商标等知识产权方面的法律规定，尊重需求方的知识产权，对所知悉的采购人的技术秘密和商业秘密负有保密责任。未经采购人事先书面授权，不得以任何方式向任何其他组织或个人泄露、转让、许可使用、交换、赠与或与任何其他组织或个人共同使用或不正当使用（依据国家或上级部门指示所做的赠送除外）。违反本条规定给对方造成损失的，违约方应负相关的法律责任。

* 1. **售后服务及培训要求**

投标人提供全年7×24技术支持，为采购人提供咨询服务。保证系统全年7×24小时不间断稳定运行，系统故障时间不能超过4小时（经上级领导及直属单位或主管部门批准的系统停机维护时间除外）。

投标人应提供云服务操作手册，并为采购人提供必要的使用培训。

投标人提供的政务云平台需通过网络安全等级保护三级测评和网信办云计算服务安全评估。