**一、采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物或服务名称 | 数量 | 单位 |
| 1 | 2023年北京市城市管理委员会政务云租用项目-北京市能源运行综合监测等系统 | 1 | 项 |

**二、项目背景**

**1、项目背景**

北京市城市管理委员会是负责北京市城市管理、城乡环境建设的综合协调和市容环境卫生管理、能源日常运行管理、相关市政公用事业管理的市政府组成部门。本次项目采购单位为北京市城市运行管理事务中心，北京市城市运行管理事务中心是北京市城市管理委员会的直属事业单位，承担本市城市管理“一网统管”相关平台建设、运行和数据信息管理等具体工作；负责城市运行智能感知体系建设、城市运行态势与数据监测、分析、预警等事务性工作，承担能源运行、户外广告以及安全生产、应急值守、“接诉即办”等城市运行领域的事务性工作。按照城市运行一网统管的要求，实行集约化建设，以构建安全稳定高效的信息化基础环境。运用物联网、云计算、大数据等信息技术，加强信息资源共享开放，不断提高网络安全防护水平，提升应急响应、事件快速处置能力，加强安全监控，确保信息系统安全稳定运行。

**2、信息系统清单**

|  |  |
| --- | --- |
| **序号** | **信息系统名称** |
| 1 | 北京市能源运行综合监测系统 |
| 2 | 北京市网格化城市管理系统（包括北京市城市管理信息平台、网格化城市管理联机分析系统、北京市信息化城市管理互动服务平台、市级网格化城市管理案件公开系统、城市管理案件统计分析数据库系统5个子系统） |
| 3 | 城市运行监测平台 |
| 4 | 北京市城市运行调度指挥平台 |

**三、技术参数要求**

**1、云资源租用清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 政务云资源-云计算服务清单 | | | | |
| 服务类别 | 服务子类 | 服务项 | 单位 | 数量 |
| 计算服务 | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1 CPU | 442 |
| 内存 | 1 GB | 1184 |
| x86物理服务器租用服务 | x86 物理服务器配置：2 路12 核（主频≥2.0Ghz），64G内存，2 块600G SAS 硬盘,2 个HBA 卡，2 个万兆端口 | 1台 | 4 |
| 存储服务 | 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） | 1 GB | 127144 |
| 普通存储 | 普通存储（单盘技术指标: 单盘 IOPS 1000-3000 ） | 1 GB | 36864 |
| 静态存储 | 大容量、高可靠的数据存储服务，具备PB级线性扩展能力 | 1 TB | 32 |
| 本地备份服务 | 通过备份策略实现文件、操作系统、数据库的本地备份 | 1GB | 81400 |
| 网络服务 | 互联网链路服务 | 互联网链路带宽 | 1 Mb | 200 |
| 互联网IP地址租用服务、并提供备案服务 | 1 IP | 4 |
| 远程接入服务 | 每个账号结合身份验证通过VPN远程接入堡垒机进行维护 | 1账号 | 15 |
| VPN服务 | SSL VPN接入 | 1套 | 11 |
| WAF防护 | 在网站前端架设WAF防护服务，保证用户网站对已知安全隐患进行防护，实时升级漏洞补丁，配置防护策略，可起到前端防护作用 | 1 IP（互联网） | 4 |
| SSL证书 | 由受信任的数字证书颁发机构CA，在验证服务器身份后颁发，实现服务器身份验证和数据传输加密功能 | SSL证书 | 1 |
| 云主机深度监控服务 | 特定云主机深度监控及运维保障服务（7\*24小时值守） | 7\*24小时深度监测云主机资源、硬件设备监控、云平台层应急处置等内容 | 1主机 | 52 |
| 政务云资源-扩展服务清单 | | | | |
| 服务类别 | 服务子类 | 服务项 | 单位 | 数量 |
| 基础软件支撑服务 | 商用操作系统套餐 | Windows Server套餐：Windows Server租用、安装及维护 | 1个主机 | 34 |
| 开源操作系统套餐 | 提供开源操作系统安装和维护服务 | 1个主机 | 18 |
| 安全监测及防护服务 | 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 台 | 52 |
| 主机防护 | 提供符合等保三级要求的主机权限管理及安全防护 | 1 台 | 52 |
| 主机漏洞扫描 | 为用户提供针对主机层面的安全扫描服务，并反馈相关结果 | 1 台 | 104 |
| 主机安全加固 | 针对漏扫或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞 | 1 台 | 104 |
| 网页防篡改服务 | 通过防篡改软件对用户页面进行实时防护，减少用户页面被恶意篡改的可能性 | 1 监控点 | 4 |
| 主机日志分析 | 针对操作系统进行日志收集，并且进行分析，并将结果反馈给用户，用于了解主机安全情况及资源使用情况 | 1 台 | 52 |
| 数据库审计服务 | 在不影响数据库系统自身性能的前提下，实现对数据库的监控和保护，及时地发现网络上针对数据库的违规操作行为并进行记录、报警，有效地弥补现有应用业务系统在数据库安全使用上的不足，为数据库系统的安全运行提供有力保障 | 1套 | 14 |
| 云端APT防护服务 | 精准发现网络中针对云上主机与服务器的已知高级网络攻击和未知的新型网络攻击的入侵行为，结合威胁情报对事件进行分析、研判和回溯，全面检测和分析网络威胁状况，创建全面纵深的安全防御体系，预警APT攻击行为 | 1套 | 1 |
| 网站安全防护服务 | 网站安全防护专业版：EB入侵防御、流量保险、访问过滤、自动登录交易保护、虚拟补丁、0day防御，漏洞扫描、专家服务 | 1个 | 4 |
| 个性化服务 | 数据库加密和防护服务（控制中心） | 实现对数据库的指定列、关键字段进行加密，保证敏感数据在存储层为密文存储，防止数据库数据以明文形式暴露，以实现存储层的安全 | 1个控制中心 | 1 |
| 数据库加密和防护服务（引擎端） | 1个数据库实例 | 3 |

**2、基础安全保障服务清单**

基础安全保障服务是云服务商应具备的云平台层安全保障能力，使用单位无需购买即可享受服务，具体服务内容如下表：

|  |  |  |
| --- | --- | --- |
| **服务类别** | **服务目录** | **服务项** |
| 安全管理服务 | 运维人员管理 | 7x24小时运维人员管理、安全登记 |
| 机房运维管理 | 机房设备管理、安全控制 |
| 应急演练 | 协助使用单位进行安全应急演练 |
| 安全技术  服务 | 物理访问控制 | 机房进出控制、监控等 |
| 机房三防服务 | 机房防火、防盗、防雷电 |
| 设备访问审计 | 设备访问记录、日志统计、安全事件 |
| 出口流量监测 | 出口流量控制、检测，并且可观测数据，互联网网络行为审计 |
| 本地抗DDoS防护 | 云平台整体提供总带宽为20Gb的抗DDoS防护 |
| 防火墙安全防护 | 出口安全 |
| 防入侵监测IPS | 防入侵监测 |
| 远程接入服务 | 免费提供1个远程登录堡垒机的运维账号 |
| 租户隔离 | 租户虚拟化层隔离 |
| 租户内部访问控制 | 租户内部访问权限控制，用户可以自由分配 |
| 云主机监控 | 提供云上资源的基本监控，包括CPU、内存使用率等 |
| 角色权限管理 | 提供通过代入角色实现获取操作权限 |
| 监控平台接入服务 | 可提供租户管辖内的云资源监控数据接口调用 |

**四、项目服务内容概述**

**1、项目基本信息**

项目名称：2023年北京市城市管理委员会政务云租用项目-北京市能源运行综合监测等系统

项目预算金额：590.35万元，其中包括政务云租用云计算服务预算：385.14万元，政务云租用扩展服务预算：205.21万元。

**2、项目目标**

为北京市城市管理委员会已入云的北京市能源运行综合监测等系统提供政务云租用服务，通过配置北京市政务云的计算服务、存储服务、网络服务、云主机深度监控服务等各类服务，满足云上信息系统的基础运行环境需求。同时，通过开展基础软件支撑服务、安全监测及防护服务、个性化服务等服务，完成信息系统的日常运维和安全运维服务工作，确保系统在云上安全、稳定地运行。

**3、政务云服务内容概述**

政务云租用服务包括计算服务、存储服务、网络服务、云主机深度监控服务、基础软件支撑服务、安全监测及防护服务和个性化服务等。

**（1）计算服务**

为北京市城市管理委员会部署在政务云平台中的信息系统提供x86平台云主机服务和x86物理服务器租用服务。

**（2）存储服务**

选择普通存储存放备份数据，选择高性能存储存放业务数据。其中，高性能存储用于解决数据中心存储单点故障导致业务停顿和数据丢失的问题；普通存储采用分布式文件系统通过数据保护技术将数据保存在不同节点中解决数据中心存储单点故障导致业务停顿和数据丢失的问题。

本地备份服务：根据应用系统的具体需求，配合采购人制定系统级备份、应用级备份和数据备份方案。备份可实现对用户数据（文件、操作系统、数据库）的本地备份，默认提供非结构化数据保护、Windows/Linux/Unix操作系统备份保护及对应平台的数据库、文件备份保护。

数据备份策略与频率：虚拟机每周备份1次，备份文件保留1个月，保留2份副本。数据库文件每天增量备份，每周全量备份，备份文件保留1个月，保留2份副本。

**（3）网络服务**

云平台按照等级保护三级要求进行建设，且所有设备全部冗余，可避免一台设备宕机造成的单点故障。云平台分为互联网区和政务外网区，两区之间逻辑隔离，采用防火墙实现数据交换，并建立安全监管平台来保障政务云平台的安全，其中，互联网采用双链路，政务外网网络带宽不低于1千兆。

网络服务内容包括：提供链路带宽服务及互联网IP地址租用服务，并提供相应的网络域名备案服务，按照管理部门要求，配合系统应用厂商提供网络策略配置服务；提供主机负载均衡服务，实现主机应用集群的负载均衡；提供远程接入服务，每个账号结合身份验证通过VPN远程接入堡垒机维护应用系统；提供SSL证书服务，由受信任的数字证书颁发机构CA，在验证服务器身份后颁发，实现服务器身份验证和数据传输加密功能；提供WAF防护服务，能够针对Web应用提供安全防护。

**（4）云主机深度监控服务**

根据信息安全等级保护计算环境中“与计算环境安全”的要求，需要对计算机设备进行云主机深度监控。深度监控内容包括但不限于：系统情况监控、计算资源监控、网络状态监控、集中告警监控、Top性能监控、安全事件服务、应急处置服务。对资产进行梳理采集，以及资产的变更统计分析。

**（5）基础软件支持服务**

提供主机的商用操作系统、开源操作系统的安装及维护服务。

**（6）主机杀毒服务**

按照采购人的有关管理规定及应用系统需求，对主机进行定期的病毒查杀，针对主机提供恶意代码检测和拦截服务，及时发现、拦截、阻断各种恶意代码、病毒木马等。提供集中控制杀毒软件，对主机性能无影响。

**（7）主机防护** 按照采购人的有关管理规定及应用系统需求，对主机进行多方面的安全防护，对入侵行为进行检测及防护，包含网页后门、反弹 shell、异常账号、日志删除、异常登录、异常进程、命令篡改行为。提供安全策略进行安全防护，包括暴力破解防护、扫描防护、病毒防护、 IP 黑白名单、端口安全、访问控制、进行行为控制、进程白名单。

**（8）主机漏洞扫描和加固服务**

按照采购人的有关管理规定及应用系统需求，提供全部在用主机漏洞扫描和加固服务，以发现主机高危端口、操作系统、数据库、中间件等层面存在的安全漏洞，并完成操作系统层（含）以下的安全加固，同时配合应用系统主责部门进行系统安全加固。

**（9）网页防篡改服务**

投标人需根据采购人的需求，提供网页防篡改服务，对互联网应用的动态页面和静态页面的篡改行为进行检测和防护，防止对目录中的网页、电子文档、图片等类型的文件进行非法篡改和破坏。

**（10）主机日志分析**

针对操作系统进行日志收集，并且进行分析，并将结果反馈给用户，用于了解主机安全情况及资源使用情况，日志需保存6个月。

**（11）数据库审计服务**

投标人需根据采购人的需求，为数据库实例提供数据库审计服务，以网络旁路的方式工作于数据库主机所在的网络，对访问数据库服务器的行为进行全方位审计。数据库审计在不影响数据库系统自身性能的前提下，对数据库的操作实现跟踪记录、定位，实现对数据库的监控和保护，及时地发现网络上针对数据库的违规操作行为并进行记录、报警为数据库系统的安全运行提供有力保障。

**（12）云端APT防护服务**

投标人通过对流量进行深度解析，发现流量中的恶意攻击，提供全面检测和预警的能力，可分析网络威胁状况，对安全事件进行分析、研判和回溯。

**（13）网站安全防护**

按照采购人的有关管理规定及应用系统需求，在互联网应用网站前端架设防护服务，保证用户网站对已知安全隐患进行防护，实时升级漏洞补丁，配置防护策略，可起到前端防护作用。

**（14）数据库加密及防护服务（控制中心和引擎端）**

投标人需根据采购人的需求，对数据库实例进行数据库加密。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；实现对数据库的指定列、关键字段进行加密，保证敏感数据在存储层为密文存储，防止数据库数据以明文形式暴露，以实现存储层的安全加固。

**五、云平台安全能力要求**

投标人需提供标准云平台的安全管理服务和安全技术服务，包括但不限于云平台7\*24小时监控、机房运维管理、应急演练、物理访问控制、机房三防、租户隔离、角色权限管理等。

投标人所投云平台应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/T 22239-2019）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。**投标人管辖范围内的硬件、软件及支撑环境资源，至少达到业务系统的最高安全等级要求。

**投标人所投云平台通过中央网信办云计算服务安全评估。**

**投标人所投云平台应具备商用密码服务能力，并通过商用密码应用安全性评估。**

**投标人提供的网站安全防护能力包括但不限于：Web攻击防护能力、DDoS攻击防护能力、CC攻击防护能力、高防DNS、爬虫攻击防护能力、敏感词过滤、CDN加速缓存、双协议栈（支持IPv4、IPv6双协议并存）、攻击告警等。**

**六、运维保障服务**

**1、服务规范**

投标人须严格按照政务云管理单位和采购单位制定的管理办法、流程、应急制度、文档管理、资产管理、基线管理、人员管理与培训、知识库管理、安全管理等相关制度，规范地开展标准化的运维服务工作。

**2、运维要求**

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。

投标人负责设立技术支持热线，并安排专人值守，为运维工作提供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、安全及保密要求**

投标人须严格遵守采购人的相关信息安全规定，不得利用系统维护服务时的便利对采购人数据及其他信息擅自修改或透漏给第三方。

**4、响应及时性要求**

投标人应当提供高效的系统监控服务，有效防范系统风险，负责人7\*24小时电话畅通，在系统发生故障时，投标人应在5分钟内响应，在30分钟之内处理故障，如需要运维人员现场处置的，应能协调人力资源在1小时内到达运维现场提供服务。

**5、重点保障要求**

为保障五一、十一、春节、两会等重要时期以及业务高峰期内的系统平稳运行，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。

**6、应急保障和风险防控措施**

投标人应具备相应的应急预案与风险防控措施,在云平台运行维护期间，出现应急情况和风险状况时，按照预案处置,快速解决问题。

**七、服务团队要求**

投标人须根据项目要求安排具备相应资质和经验的专业人员从事本项目工作，提供服务团队，须确保项目实施队伍的稳定，提供本地化服务。投标人需提供项目团队组织架构、成员名单、成员职责，保证担任重要岗位的人员具备相应专业资质。

**八、业务连续性要求**

1、本项目如涉及系统迁移，投标人需编制业务连续性服务方案。投标人以迁移时间窗口与进度要求为总约束，合理规划，科学组织。迁移部署服务子方案应包括（但不限于）政务云资源配置、应用迁移、数据迁移、测试验证、业务割接、风险评估、迁移期间安全保障、迁移期间应急保障、迁移期间运维保障等内容。

2、本项目如涉及系统迁移，针对已经运行在政务云平台上的应用系统，为确保迁移过程中数据不丢失、系统业务不中断，投标人负责与原政务云平台的服务商进行主动对接，投标人需承诺系统迁移涉及的所有费用（包括但不限于中标人迁移测试阶段的云资源费用，第三方对业务系统的部署、调试费用等）由投标人承担。

**九、售后服务**

投标人应成立专门的技术支持和售后服务小组，提供完善周到的本地化服务，具有7\*24小时的维护支持能力以及优先服务级别。投标人应提供具体的技术支持和售后服务方案。

自租用期始至服务期止，需向采购人提供以下两方面内容，其它内容可自愿提供。

1、定期向采购人提供月度服务报告。

2、至少提前一天通知即将进行的，与采购人系统运行相关的安全事件、项目施工、功能或者性能调整工作。

**十、服务时间及地点（服务期限）**

1、本项目服务期限：12个月。

2、服务地点：采购人指定地点。

**十一、验收服务要求**

**1、验收标准**

投标人提供的服务质量符合国家或相关行业标准，并满足合同约定的要求。

**2、验收方式**

在服务期满后20 个工作日内，投标人向采购人提交验收材料后，由采购人组织验收工作。验收材料包括但不限于合同规定的各项服务清单等。验收不合格的，投标人应当在15 日内进行调整，并重新提交验收

**十二、付款方式**

本项目分2次支付项目款：

1、签订合同后采购人向投标人支付合同总金额的60%；

2、投标人提供本协议项下的全部服务内容并经采购人最终验收合格后，采购人向投标人支付合同总金额的40%。

**十三、技术指标要求**

1、云平台运行技术指标应符合国家法规、标准，云平台可用性不低于99.99%，数据可靠性不低于 99.9999%。

2、云平台具备高可用和动态迁移功能，发生物理设备故障后，虚拟机可以自动迁移到其他可用资源上运行，确保业务系统不受物理设备故障影响。

3、云平台支持对虚拟机CPU、内存、存储、带宽进行实时监控，并支持自定义告警规则。

4、云平台提供备份/快照功能，能对云平台中的物理和虚拟服务器进行备份，防止存储故障导致数据丢失。

5、云管平台支持图形化管理，支持自动生成资源使用的数据报表。

6、云平台应具备为计算单元提供授时时钟源的能力。