技术、服务及其他要求

（注：本章的技术、服务及其他要求中，带“★”的要求为实质性要求。采购人、代理机构应当根据项目实际要求合理设定，并在第五章符合性审查中明确响应要求。）

3.1.采购内容

采购包 1：

采购包预算金额（元）：900,000.00

采购包最高限价（元）：900,000.00

序号	采购品目名称	标的名称	数量（计量单位）	标的金额（元）	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及强制采购节能产品	是否涉及优先采购节能产品	是否涉及优先采购环境标志产品
1	其他运行维护服务	公共管理服务平台提升建设项目	1.00（批）	900,000.00	软件和信息技术服务业	否	否	否	否	否

报价要求

采购包 1：

序号	报价内容	数量（计量单位）	最高限价	价款形式	报价说明
1	公共管理服务平台提升建设项目	1.00（批）	900,000.00	总价	无

★注：采购包涉及采购货物的，投标人响应产品应当明确品牌和规格型号并指向唯一产品，不能指向唯一产品的，应通过报价表唯一产品说明栏补充说明。

本项目涉及核心产品：

采购包 1：

序号	采购品目名称	标的名称	产品名称
不涉及			

注：涉及核心产品的，具体评审规定见第五章。

本项目涉及采购进口产品：

采购包 1：

序号	采购品目名称	标的名称	产品名称
不涉及			

★注：不涉及采购进口产品时，投标人不得提供进口产品进行响应；涉及采购进口产品时，如国产产品满足采购需求，也可提供国产产品进行响应。

本项目涉及强制采购节能产品：

采购包 1：

序号	采购品目名称	标的名称	产品名称
不涉及			

★注：响应产品属于《节能产品政府采购品目清单》中政府强制采购的产品，投标人应当提供由国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（http://cx.cnca.cn）的认证信息截图，否则作无效投标处理。具体要求详见第五章符合性审查表。

本项目涉及优先采购节能产品：

采购包 1：

序号	采购品目名称	标的名称	产品名称
不涉及			

注：响应产品属于《节能产品政府采购品目清单》中优先采购的产品，投标人提供由国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（http://cx.cnca.cn）的认证信息截图，可以享受优先采购政策。具体要求详见第五章规定。

本项目涉及优先采购环境标志产品：

采购包 1：

序号	采购品目名称	标的名称	产品名称
不涉及			

注：响应产品属于《环境标志产品政府采购品目清单》中的产品，投标人提供由国家确定的认证机构出具的、处于有效期之内的环境标志产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（http://cx.cnca.cn）的认证信息截图，可以享受优先采购政策。具体要求详见第五章规定。

3.2.技术要求

采购包 1：

标的名称：公共管理服务平台提升建设项目

<table>
<tr><th>序号</th><th>符号标识</th><th>技术要求名称</th><th colspan="5">技术参数与性能指标</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2"></td><td rowspan="2">公共管理</td><td>序号</td><td>名称</td><td>参数</td><td>数量</td><td>单位</td></tr>
<tr><td>1</td><td>防火墙</td><td>★1、三层吞吐量≥3G，应用层吞吐量≥1G，并发连接数≥100</td><td>1</td><td>台</td></tr>
</table>

		服务平台提升建设项目			W; 硬件参数:≥6 个千兆电网口，≥2 个千兆光网口，为防止设备关键信息泄露，设备禁止配置显示模块，配置 3 年 WEB 应用防护、IPS 特征库、僵尸网络与病毒防护库和 URL&应用识别库定期更新； ▲2、支持对 X-Forwarded-For 字段的检测功能，一旦检测到非法源 IP,系统将自动记录相关日志，并触发联动机制，对非法 IP 进行封锁处理；**（提供 IP 封锁功能截图证明）** 3、防火墙需具备静态路由和多播路由，支持 RIP、OSPF、BGP 等动态路由协议； ▲4、提供服务器漏洞防扫描功能，一旦检测到扫描行为，系统不仅会记录相关源 IP 的日志信息，还会自动触发联动机制，对涉事 IP 实施封锁措施；**（需提供 IP 封锁功能截图证明）** 5、具备文件过滤功能，可对视频文件、音频文件、图片文件、文本文件、可执行文件、驱动文件等类型文件进行安全过滤； 6、产品支持对不少于 10000 种应用的识别和控制；			

						7、支持网站防篡改功能，可防止攻击者非授权修改网站目录文件； 8、产品内置不低于 8000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则； 9、产品支持病毒例外特征设置，根据文件 MD5 值和文件 URL 设置病毒白名单，不对白名单进行病毒查杀； 10、产品支持用户账号安全保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生； ▲11、产品支持勒索病毒检测与抵御，需提供针对勒索病毒攻击设置专项安全策略的相关功能截图；**（提供检测机构出具关于“勒索病毒”的相关证书证明功能有效性）** 12、产品支持安全策略有效性分析功能，能够分析出策略冲突、策略冗余、权限放通过大、无效			

						策略等，给运维人员提供优化建议； 13、产品支持 https 解密功能，支持 TCP 代理和 SSL 代理； 14、产品支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间； 15、产品支持联动防御实现对 APT 攻击的检测与阻断； 16、产品支持对不同用户和应用的流量进行带宽的差异化管控； 17、产品支持 SNMP V1/V2/V3/Trap 等标准网络管理协议； 18、产品支持管理员三权分立功能，根据管理员权限分为安全管理员、安全审计员、系统管理员三种角色； ▲19、产品支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改；**（需提供具有 CMA 标识的第三方检测报告）** ▲20、产品支持与本次提供的终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理，支持检测到某主机有僵木蠕毒的 C2 通信时，手动或自动化将			

					恶意域名信息下发到终端安全软件做 C2 通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离；**（需提供联动终端安全软件功能截图证明）**			
			2	终端安全软件	★1、配置≥100 PC 授权许可，≥3 服务器授权许可,产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；同时也支持硬件管理平台交付，三年升级服务。采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能； ▲2、提供勒索病毒的整体防护体系入口，该入口能够直观地展示最近七天内的勒索病毒防护成效。具体数据包括成功处置的勒索病毒数量、有效阻止的勒索病毒行为次数、及时防御的未知进程操作次数以及成功拦截的暴力破解攻击次数。通过这些详实的数据，可以全面了解防护体系的运行状况和效果；**（需提供功能截图证明）**	1	套	

						3、支持基于系统内置弱密码字典和自定义弱密码字典的检查功能，弱密码检测支持至少包括SSH、RDP、MySQL、Tomcat、Redis等应用类型，可按照空密码、自定义弱密码、密码长度小于8、字符种类小于3等常见弱密码类型进行分类查看； 4、支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描，及时发现尚未纳入管控的终端； ▲5、支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴；**（需提供功能截图证明）** 6、支持配置不同的权限角色，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限，并配置可管辖的终端范围，支持管理员账号限制IP登录；支持管理员账号采用双因素认证； ▲7、支持禁止黑客工具启动，至少包含：xuetr、ProcessHacker、PCHunter、Mimikatz工具的			

						自启动，防止黑客攻击；**（需提供功能截图证明）** 8、具备针对最新未知的文件，使用 IOC 特征（文件 hash、dns、url、ip 等）的技术，进行云端查询。云端的安全中心，使用大数据分析平台，基于多维威胁情报、云端沙箱技术、多引擎扩展的检测技术等，秒级响应未知文件的检测结果，构架公有云云查体系； 9、支持开启 agent 自动降级机制，可设置主机资源如 CPU 利用率、剩余内存、等待任务长度、磁盘列队长度达到的阈值，当任意资源达到阈值持续一段时间后，agent 会进入降级状态，当资源占用恢复到正常值时，agent 自动恢复为在线状态； ▲10、支持勒索可疑行为的检测功能，利用先进的行为 AI 技术，能够精准识别并告警勒索信、命令行操作、修改文件等多种高风险、高频率的勒索病毒投放场景，并自动采取拦截措施，确保系统安全；**（需提供功能截图证明）** ▲11、支持基于异常行为 AI 的			

					实时监测，实现文件秒级动态备份，发生勒索事件时，支持自动删除原始文件夹中被加密的文件夹并隔离文件；支持文件恢复密码保护，用户下发文件恢复操作时需要经过认证校验，确保文件恢复操作的合法性；**（需提供功能截图证明）**			
			3	日志分析管理系统	★1、产品不少于 6 个千兆 SFP 口，2 个万兆 SFP+口， 2U 机箱，配置不少于 50 个日志接入授权，日志处理性能不少于 2500EPS； 2、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于 800 种日志对象的日志数据采集； 3、支持主动与被动相结合的数据采集模式，可以通过部署 Agent 进行日志数据的实时采集，还兼容多种采集方式，如 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、SFTP、文件/文件夹读取以及 Kafka 等，以满足不同场景下的日志收集需求，确保数据的全面性和准确性； 4、支持以可视化的方式，通过正则、分隔符、JSON、XML 等灵	1	台	

						活手段自定义规则解析，以覆盖更多种类的日志格式。同时支持对解析结果字段进行新增、合并、映射等操作，以弥补内置解析规则可能无法覆盖的日志类型，从而满足更广泛的日志处理需求； 5、支持自动识别并采集设备信息，同时在设备出现异常时能够自动触发告警机制。为了方便用户及时获取告警信息，支持将设备异常告警以邮件形式发送给用户，或者通过调用第三方接口实现告警信息的推送； ▲6、支持使用 TLS 加密方式进行日志传输，以确保数据安全性。同时支持对日志传输状态和最近同步时间进行监控，方便实时了解传输情况。提供统计功能，能够计算每个日志源今日的传输量以及总传输量，帮助更好地管理日志数据；**（需提供功能供截图证明）** 7、支持日志文件备份到外置存储节点，支持 ISCSI 存储方式，并可查看外置存储容量、状态等信息； 8、支持用户根据自定义的过滤			

					条件进行检索，包括模糊 IP、多个 IP、IP 地址段、应用、协议、MAC 地址等字段的精准检索。在检索过程中，至少支持 AND、OR、NOT 三种运算符，以满足用户复杂的查询需求，提升检索的灵活性和准确性； 9、支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括 base64、Unicode、GBK、HEX、UTF-8 等； 10、支持自定义首页卡片，支持实时监控系统日志传输量和日志留存的合规情况； 11、持采用 SM3 国密算法，以确保日志数据的完整性和安全性。通过该算法能够有效防范日志篡改等攻击行为，保障数据的真实性和可信度； ▲12、支持利用 POC 测试工具实现一键式数据生成，从而便捷地验证日志数据采集的准确性与完整性，有效预防设备部署后因采集失效而未能及时发现的潜在风险，确保日志数据的稳定可靠；**（需提供功能供截图证明）**			
				4	运维安全管理系统	★1、默认含 50 个资源授权（可扩展到 150 个），提供运维人员	1	台	

						单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能，并满足等级保护三级建设要求； 2、物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构，系统各模块支持以 B/S 方式管理，采用 https 加密方式访问； 3、支持通过协议前置机进行协议扩展，至少支持扩展 KVM、Vmware、数据库、http/https、CS 应用等； 4、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入； 5、支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期； ▲6、用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、短信认证（移动云 mas)、AD 域/LADP 认证、Radius 认证等认证方式；并支持各种认证方式和静			

					态口令组合认证；（提供功能截图证明） 7、支持对用户指定限制登录 IP、登录时间段（可循环，如每周一到周五 9：00-17：00 时）等规则，以确保可信用户登陆系统； 8、支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度必须符合密码策略要求； 9、全面支持 IPV6，设备自身可以配置 IPV6 地址供客户端访问，并且支持目标设备配置 IPV6 地址实现单点登陆和审计。			
				5	云计算产品	1、产品规格： CPU：≥C86 架构 HG7360 处理器（核数≥24 核，主频≥2.2GHz）；内存：≥128G 内存，4 根 32G DDR4，≥16 根内存插槽；存储：配置≥8 盘位，系统盘≥480G SSD×2（RAID_1）； 缓存加速盘≥480G SSD×2；数据盘≥4T 7,2K SATA×2；阵列卡：配置 SAS_HBA 卡，支持 RAID 0/1/1 0；PCIE 扩展：最大可支持 6 个 PCIe 扩展插槽；网口：配置≥2 个千兆电口，≥ 2 个万兆光口（含光模块）；电源：≥550W（1+1）	1	台	

						冗余电源； 2、一套云平台支持同时提供虚拟机、LXC 容器和 Docker 容器服务，实现虚拟机和容器的统一调度和管理； 3、支持通过文件夹对虚拟机进行分组，不同类型的虚拟机实现逻辑分组管理，文件夹深度可达 5 层；支持对分组虚拟机批量进行关闭、启动、重启、删除、迁移操作； 4、虚拟机支持多种启动方式，包括硬盘启动、虚拟光驱启动和网络启动，可依次设置设备第一启动顺序、第二启动顺序和第三启动顺序； ▲5、 支持创建虚拟机时，同时创建云硬盘，系统自动进行云硬盘的格式化和目录挂载操作，无需手动进入操作系统后台操作；（需提供具有 CMA 标识的检测报告复印件） 6、支持虚拟机和云硬盘的回收站功能，统一管理被删除的虚拟机和云硬盘，防止因误删除导致数据丢失。支持设置回收站文件保存周期，超期的文件将被自动删除，支持批量销毁或还原虚拟			

						机和云硬盘； ▲7、支持在不中断已有业务的情况下，对数据中心内部各类已有服务器设备进行监控纳管，包括 X86 服务器、ARM 服务器、存储服务器、专有智能设备。支持通过 IPMI 协议对纳管的存量服务器进行远程开关机、远程监控等，管理员或租户可对纳管的服务器进行资产分配，分配给不同的租户或用户进行管理，并支持资产回收；（需提供具有 CMA 标识的检测报告复印件） 8、支持 iSCSI、NFS、CIFS、FTP、HTTP、HDFS、S3、Swift 等，支持 CSI 接口 支持多副本和 EC 纠删码保护机制，最大可选择 6 副本，允许用户设置副本数量为 1～6 副本； 9、支持一套系统同时接入多种类型的存储后端，包括本地存储、分布式存储 ceph 和集中式存储，其中集中式存储支持多种存储方式接入，包括 LVM 逻辑卷接入、iSCSI 网络接入和 FC 网络接入，支持可视化存储拓扑展示，支持对系统可用存储资源空间进行展示，包括物理磁盘空			

					间、逻辑已用空间、当前使用空间和总体剩余空间等； 10、支持无代理跨物理主机的虚拟机 USB 映射，需要使用 USB KEY 时，无需在虚拟机上安装客户端插件，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的 USB 资源+HBA 卡，支持 RAID 0/1/10； 11、PCIE 扩展：支持≥6 个 PCIE 扩展插槽；网口：板载≥2 个千兆电口。支持选配 10GbE、25GbE SFP+等多种网络接口； 其他接口：≥1 个 RJ45 管理接口，后置≥2 个 USB 3.0 接口，前置≥2 个 USB2.0 接口，≥1 个 VGA 接口；电源：标配 550W（1+1）冗余电源。			
				6	综合安防平台	1、综合安防管理平台，支持统一管理视频监控、一卡通、车辆管控、报警检测、综合管控等应用，实现安防系统的智能化应用及统一集成化管理； 2、 最大支持监控点管理容量≥100000 路，最大支持用户≥10000 个，支持并发在线用户≥1000 个； 3、支持用户密码有效时间段进	1	套	

						行设置管理，支持用户 IP 绑定，指定IP地址用户才能登陆平台；支持 BS、CS 客户端以及 IOS、Android 移动端应用； 4、支持自动在 1/4/6/7/9/16/24 画面分隔模式间进行监控点轮巡预览，轮巡时间可设置，支持全屏显示，预览画面支持监控点信息、语音对讲、开关声音、云台与镜头控制、抓图、多图抓拍等； 5、支持门禁设备接入、管理和控制，支持门禁权限配置和下发，支持卡（含身份证）、人脸、指纹、卡密码等凭证单独或组合使用的认证方式； ▲6、支持业务应用组件化，各组件独立运行维护、独立安装或卸载，支持部署组件（服务）到服务器集群，支持集群管理，支持系统分布式、负载均衡等技术，支持多级架构进行系统平台规模扩展，支持开放 API 接口给第三方系统对接；（需提供具有 CMA 标识的检测报告复印件） ▲7、支持根据用户使用习惯自定义配置快捷功能入口，支持首页投放大屏展示，支持不少于最			

						近七日的用户活跃数统计，支持对系统中的分组、服务器、组件等统计概览、查看，支持统计服务器在线率及各服务器在线详情；（需提供具有 CMA 标识的检测报告复印件） ▲8、支持不同色彩展示运行告警状态，支持告警统计、概览、处理，支持告警记录查看、查询，支持告警单条、批量处理；支持系统最近 7 天每日告警数统计，支持评分量化系统监控指数，显示系统运行状态；（需提供具有 CMA 标识的检测报告复印件） ▲9、支持系统内各节点进行查看、增加、删除、修改，展示、查找；支持对系统内所有服务器进行监控，包括名称、IP 地址、状态、未处理告警数、CPU 使用率、内存使用率、磁盘容量、主机代理版等；支持对系统内所有组件信息进行监控，组件信息包含：组件名称、未处理告警数、所属服务器、最近操作时间、授权状态、维保期限、使用期限等；（需提供具有 CMA 标识的检测报告复印件） ▲10、支持对服务的参数配置进			

					行查询、查看、修改、下发，支持告警策略配置启用、查看、修改、设置，支持集群信息查看、添加、删除，支持授权查看管理、导入、移除授权文件；支持在线授权激活、离线授权激活；（需提供具有CMA标识的检测报告复印件） 11、支持查看视频设备、门禁设备、停车场出入口设备、可视对讲设备、梯控设备、报警设备、消防设备、安检设备、其他类型设备的设备接入的情况和在离线信息展示，支持查看监控点、门禁点、报警防区、IO通道等通道资源接入情况； 支持在预览监控点画面时进行一键上墙、 云台控制、语音对讲，支持视频画面叠加水印，包括视频预览、录像回放、即时回放、录像剪辑、手动录像和录像下载时叠加，支持录像回放和录像下载权限分离，支持为用户分配是否具有录像下载权限；			
				7	租赁费	★1、服务器托管及云服务器租用。	2	年	
				8	系统集成	★1、防火墙、云计算产品、综合安防平台等系统集成，智慧农	2	年	

					业平台使用运维。		
			9	网络专线	★1、提供农业农村局一条 150M 专线的租赁服务。	2	年
			10	其他	★1、种子农药包装押金收退终端平台运维。	2	年

3.3.服务要求

3.3.1.服务内容要求

采购包 1：

序号	符号标识	服务要求名称	服务要求内容
无			

3.3.2.商务要求

采购包 1：

序号	符号标识	商务要求名称	商务要求内容
1	★	服务期限	软硬件产品在合同签订后 30 日内交付。
2	★	服务地点	采购人指定地点。
3	★	验收、交付标准和方法	严格按照验收标准以投标文件技术参数及要求和相关行业标准为准，并按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205 号）等相关规定验收程序组织验收。
4	★	支付方式	分期付款
5	★	付款进	1、通过验收后，达到付款条件起 20 日内，支付合同总金

		度安排	额的 95.00% 2、满一年后，达到付款条件起 10 日内，支付合同总金额的 5.00%
6	★	违约责任与解决争议的方法	1.因货物的质量问题发生争议，由具有法定资格条件的质量技术监督机构进行质量鉴定。货物符合标准的，鉴定费由甲方承担；货物不符合质量标准的，鉴定费由乙方承担。 2.合同履行期间，若双方发生争议，双方本着友好合作的态度，对合同履行过程中发生的违约行为进行及时的协商解决或由有关部门调解解决，如不能协商解决可向合同签约地法院通过法律诉讼解决。

3.4.其他要求

采购包 1：

★1.质保期：2 年(其中防火墙和端点安全软件质保期为 3 年)。 ★2.本次招标含“智慧农业”大数据平台系统二级等保 1 次测评费用 。 3.投标人根据本项目实际情况制定详细的实施方案，方案包含但不限于:①项目实施概述；②实施方案；③施工进度表；④进度保证措施；⑤系统调试等。 4.投标人根据本项目实际情况制定详细的售后服务方案，方案包含但不限于:①免费售后服务呼叫中心；②现场服务支持能力；③售后巡检方案及培训方案 注:★为实质性要求，投标人必须响应。