

南京医药应急物资储备管理项目配套网络设备采购项目

招标文件

招标单位：南京医药股份有限公司

项目名称：南京医药应急物资储备管理项目配套网络设备采购项目

编制单位：南京医药股份有限公司

编制日期：2020年12月

目 录

第一章 投标须知.....	3
一、总 则.....	4
二、投标文件的编制.....	5
三、开 标.....	6
四、评 标.....	6
第二章 招标具体内容和要求.....	8
第三章 投标文件格式.....	13
第一部分：投标函及投标函附录.....	13
第二部分：投标报价书.....	16
第三部分：资格证明文件.....	16

第一章 投标须知

项目名称	南京医药应急物资储备管理项目配套网络设备采购项目		
建设地点	南京医药机房（江苏省南京市内）		
联系人	蒋一飞	联系电话	025-84552675
招标方式	公开招标与邀请招标相结合		
项目目标	确保项目采购设备质量并按期完成安装调试工作		
项目主要内容	南京医药应急物资储备及云计算基础设施设备采购项目配套网络设备（网络（日志）审计设备、数据库审计设备、堡垒机（运维安全审计））的采购及配套安装调试工作。		
工期	中标通知书发出后 20 个日历日内完成		
质保期	提供三年的免费原厂质保。		
投标有效期	投标截止日后 <u>60</u> 日内有效		
投标文件份数	壹套正本贰套副本		
投标文件递交	递交地点：南京市宁双路 19 号云密城 A 幢 9 楼会议室 投标截止时间： <u>2020 年 12 月 28 日 14 时</u>		
开 标	时间：同投标截止时间 地点：同投标文件递交地点		
评标办法	由招标方组织的评标小组根据招标方的评标管理流程进行，采用经评审的最低投标价法确定中标单位。		
最高限价	人民币肆拾陆万元整（RMB460000 元）		
中标单位 合同签订	与本项目实际实施单位江苏中健之康信息技术有限公司（招标人全资子公司）签订合同。		

一、总 则

（一）项目概况

1、项目实施基本情况：南京医药应急物资储备及云计算基础设施设备采购项目配套网络设备（网络（日志）审计设备、数据库审计设备、堡垒机（运维安全审计））的采购及配套安装调试工作。

2、项目资金来源及落实情况自筹。

3、投标费用：投标人应承担其编制投标文件与递交投标文件所涉及的一切费用。不管投标结果如何，招标人对上述费用不负任何责任。

4、投标方须提供的资格证明资料：

（1）企业营业执照（开标时必须提供有效复印件加盖公章）；

（2）法人代表资格证明书或法人授权委托书（开标时必须出示原件及被委托人身份证原件）；

（3）所投品牌的经销资格证明材料（经销授权或代理商证明等均可，复印件加盖公章）；

（4）不少于一项 2017 年 11 月以来所投品牌同类设备的销售业绩（提供合同复印件加盖公章，合同金额不低于本次最高限价）；

（5）其他证明材料；

（二）投标

1、投标资格

投标单位应提供符合招标单位要求的资质文件，以证明其符合投标合格条件，具有被授予合同的资格和履行合同的能力。具体要求：

（1）投标人应提供所投品牌的经销资格证明材料（经销授权或代理商证明等均可，复印件加盖公章）；

（2）投标人注册资本不低于人民币 100 万元。

（3）投标人应提供不少于一项 2018 年 12 月以来所投品牌同类设备的销售业绩（提供合同复印件加盖公章，合同金额不低于本次最高限价）。

2、投标人工作范围

投标人须完成下列项目：按招标文件的要求提供货物采购及安装调试服务，并对所投标货物按招标方要求提供服务及质保。

3、投标需要注意的其它事项

投标人在收到本文件后，可自行与我公司联系安排踏勘工作，投标人应了解一切可能影响投标报价的因素，对自行获取资料信息的正确性负全责，因此所需费用自行承担。一旦中标，中标人不可以以不完全了解现场情况为由提出额外的补偿，费用增加等要求。

（三）招标文件的组成

1、招标文件包括本文件及所有投标截止日前发出的修改澄清通知。

2、投标人应认真审阅招标文件所有的内容，如果投标人的投标文件不能实质性地响应招标文件要求，责任由投标人自负。

3、本招标文件所指的实质性要求和条件是工期、质量、投标有效期、投标报价等。

二、投标文件的编制

（四）投标文件的要求

1、投标人应当对招标文件提出的实质性要求和条件做出一一响应，投标文件的组成应包括本文件的要求。

2、投标人应当使用投标文件中所提供的文件格式填写，如不够用时，投标人可按同样格式自行编制和添补。

（五）投标文件的份数和签署

1、投标人必须编制一份投标文件“正本”和前附表所要求份数的“副本”，并明确标明“正本”和“副本”。投标文件正本和副本如有不一致之处，以正本为准。

2、投标文件正本与副本均应使用不能擦去的墨水书写或打印，由投标人加盖公章和法定代表人或法定代表人委托的代理人印鉴或签字。

3、全套投标文件应无涂改和行间插字，除非这些删改是根据招标人的指示进行的，或者是投标人造成的必须修改的错误。修改处应由投标文件签署人加盖印鉴。

三、开 标

(六) 开标

1、开标由招标人主持，邀请所有投标人参加。

2、开标时，由投标人推选的代表检查投标文件的密封情况，投标文件未按照招标文件的要求予以密封的，将作为无效投标文件，退回投标人。经确认无误后，由工作人员当众拆封，宣读投标人名称、投标价格和其他招标人认为有必要的内容。

3、招标人在招标文件要求提交投标文件的截止时间前收到的所有投标文件，开标时都将当众予以拆封、宣读、记录。

4、唱标顺序按各投标人送达投标文件时间先后的逆顺序进行。

5、投标文件有下列情形之一的，招标人不予受理：

(1) 逾期送达的或者未送达指定地点的；

(2) 未按招标文件要求密封的。

(3) 投标人名称或组织结构与资格预审或报名时不一致的；

(4) 法定代表人或其委托人未到场或到场无法提供有效证明；

(5) 投标文件有下列情形之一的，由评标委员会初审后按废标处理：

①无单位盖章并无法定代表人或法定代表人授权的代理人签字或盖章的；

②未按规定的格式填写，内容不全或关键字迹模糊、无法辨认的；

③投标人递交两份或多份内容不同的投标文件，或在一份投标文件中对同一招标项目报有两个或多个报价，且未声明哪一个有效，按招标文件规定提交备选投标方案的除外；

四、评 标

(七) 评标

1、评标工作

评标工作在南京医药股份有限公司有关规定组建的评标小组组织下进行。

2、本工程采用下列第(1)种方式进行评标。

(1) 经评审的最低投标价法：是指在投标文件能够满足招标文件实质性要求的投标人中，评审出投标价格最低的投标人，但投标价格低于其企业成本的除外。

(2) 综合评估法：是指对投标文件提出的项目质量、实施期限、投标价格、实施组织设计或者实施方案、投标人及项目经理业绩等，能否最大限度地满足招标文件中规定的各项要求和评价标准进行评审和比较，择优选定中标单位。

3. 具体评审

(1) 由评标小组对各投标人递交的标书进行符合性审查，通过符合性审查的投标人报价为有效投标，该报价作为投标人第一轮报价；

(2) 评标小组对各投标人标书进行详细评审，并就各投标人标书存在的偏差进行质询；

(3) 各投标人对标书存在的问题进行纠偏后，按第一轮有效报价（指通过资格审查，且没有重大偏离或废标的投标单位）由低到高的排序，选择排序前3的单位进行第二轮报价；未进入第二轮报价的单位其第一轮报价即为其最终报价；如第一轮报价有效报价单位只有3家的，则全部进入第二轮报价；

(4) 第二轮报价后，如出现合理最低报价为1家单位，则报价结束；如出现两家或以上单位合理报价一致且为最低报价情况，则这些单位再进行下轮报价，直至出现最低报价为一家单位；以上二轮或多轮报价结束，招标人均当众宣读。

(5) 评标小组对各投标人的二轮（或多轮）报价的进行合理性评判，并按二轮（或多轮）合理报价由低到高推荐中标候选人。

第二章 招标具体内容和要求

一、本次采购设备基本参数及数量需求

序号	名称	参数	数量	功能
1	网络（日志）审计设备	不少于4个千兆电口，4个SFP接口，1个管理口，2个USB接口，存储空间不少于2TB，内存不少于8G，审计对象授权不少于250个。	1	通过对网络数据的采集、分析、识别，实时动态监测通信内容、网络行为和网络流量，发现和捕获各种敏感信息、违规行为，实时报警响应，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全事件的准确定位，为整体网络安全策略的制定提供权威可靠的支持。对安全设备、网络设备、主机设备、应用系统、中间件等的日志采集，发现潜在风险，对安全问题进行定位、追踪、取证，确保企业网络及业务的顺畅运行。
2	数据库审计设备	不少于6个千兆电口，1个扩展插槽，1个管理口，2个USB接口，不少于2TB硬盘，无限数据库审计授权。	1	对数据库操作行为进行记录分析，精确审计各种SQL语句，并通过可视化查询、完整回溯等特点，在数据库发生异常操作之后，迅速定位。
3	堡垒机（运维安全审计）	不少于6个千兆电口，2个SFP插槽，不少于4TB硬盘，1个管理口，双电源，不少于500个被管资源数授权，最大可管理设备数≥500台。	1	通过远程访问权限的事前控制与访问全过程的监控记录（录屏追踪），进行运维人员的安全审计，降低人为误操作安全风险，保障信息资产的安全运行和数据的安全使用。

注：上表所列需求设备，为我公司本次采购所需的最低配置要求，参与单位可自行选择不低于以上配置要求的设备参与本项目。

二、设备详细功能及技术指标要求

下列表中为本次采购设备的详细技术要求，投标人在投标时应编制技术偏离表，对上表所列技术要求逐一回复是否满足，为保证项目的充分竞争性，下列表中所有要求提供的证书均非唯一指定，投标人可提供类似证书及相关说明，经评委评审认可后同样有效。

（一）网络（日志）审计

序号	类别	功能及技术描述
1	设备基本要求	标准1U或2U机架尺寸，含交流单电源模块，≥2个USB接口，≥1个RJ45串口，≥1个GE管理口，≥4个GE电口（内置电口Bypass），≥4个SFP光口，检测能力≥600Mbps。提供3年质保服务。

2	审计功能	支持扩展通过扫描指定网站，分析检测网页是否被挂马，并实时告警响应记录。
		支持 HTTP 网页浏览及关键字搜索审计：记录用户网站访问行为包括源 IP 地址、目的 IP 地址、访问时间、URL、网页浏览时间等，并提供网页还原功能。
		支持电子邮件审计：支持 SMTP、POP3、WEBMAIL 等协议，支持基于邮箱地址、邮件主题、邮件内容、附件名的关键字审计功能；
		支持扩展无线热点发现功能，能够实时、自动发现办公网络内的无线热点，记录无线热点访问网络时所使用的 IP 地址、认证用户等信息。提供界面截图证明
		支持移动应用审计，能够识别通过移动热点所访问的移动类应用，例如 IM 类、社交类、网购类、影音类、资讯类等应用，并记录 IP 地址、应用名称、访问时间等信息；
		支持基于论坛主题、发帖内容的关键字审计功能；支持基于用户/用户组、时间、关键字等多种组合审计策略，可记录源 IP 地址、目的 IP 地址、发帖论坛、发帖人、主题、发帖时间、发帖内容等，并提供内容还原功能。
		支持文件传输审计：支持 HTTP、FTP 协议，支持基于用户/用户组、时间、关键字等多种组合审计策略，用户可自定义下载文件类型，对文件上传、下载类型进行审计，可记录日志包括源 IP 地址、目的 IP 地址、时间、传输文件名等。提供界面截图证明
3	日志审计	可对 P2P 下载、在线视频、网络游戏、炒股软件等行为进行审计，支持基于 IP 地址、用户组、时间、协议等组合审计策略，记录日志包括源 IP 地址、目的 IP 地址、时间、应用名称等。提供界面截图证明
		针对接入外网的终端用户，系统提供增强的身份认证功能，支持标准的 radius 和 LDAP 接口，及第三方认证平台，实现更灵活、更安全的认证控制。提供界面截图证明
		系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等
4	系统管理	系统支持的数据采集方式包括但不限于 SYSLOG、RSYSLOG、SNMP Trap、FTP、ODBC、JDBC、Net flow、WMI、二进制数据、专用 Agent 等方式采集日志
		系统支持采集的设备厂家包括但不限于：NSFOCUS(绿盟科技)、Venustech(启明星辰)、Topsec(天融信)、DBAPPSecurit(安恒)、SANGFOR(深信服)、Hillstone(山石网科)、东软、瑞星、金山、网康、360 网神、Dptech(迪普)、艾科网信、Imperva、Juniper(瞻博网络)、F5、Symantec(赛门铁克)、Deep Security(趋势科技)、MaAfee(迈克菲)、Fortinet(飞塔)、Windows、Linux/Unix、Cisco(思科)、HUAWEI(华为)、H3C(华三)、中兴、Apache、nginx、IIS、WebLogic、Vmware、Kvm、Xen、OpenStack、Hyper-V、华为 FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind 等
5	产品资质	支持用户身份信息智能关联技术，可将用户各种身份信息与其终端 IP 地址进行智能关联形成用户身份信息库，从而提高事件定位的精确度。提供界面截图证明 支持 IPV6 审计日志和报表，提供界面截图证明 支持历史版本回滚功能，系统内建历史版本库，可保留最近升级的两个历史版本，并支持回滚到任一历史版本，提高了产品升级过程的可靠性。
		产品需具有公安部《计算机信息系统安全专用产品销售许可证》网络安全审计类（增强级），提供有效证书的复印件。 产品需具有中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》（增强级），提供有效证书的复印件。 产品需具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》（EAL3+），提供有效证书的复印件。

6	厂商资质	<p>厂商具有中国信息安全测评中心颁发的《国家信息安全测评信息安全服务资质证书（安全工程类三级）》，提供有效证书的复印件</p> <p>厂商应通过 ISO 20000-1:2011 标准认证，且认证范围至少包含向外部客户提供整体安全解决方案，安全软件的设计、开发和运行维护，硬件的运行维护，安全相关的 SaaS 及运营服务等，提供有效证书的复印件；</p> <p>厂商是微软 MAPP 项目合作伙伴，可以在微软每月发布安全更新之前获得漏洞信息，为客户提供更及时有效的保护，提供微软官方网站截图证明</p> <p>厂商具有中国信息安全测评中心颁发的《国家信息安全测评信息安全服务资质证书（安全开发类二级）》</p>
---	------	--

(二) 数据库审计

序号	类别	功能与技术描述
1	设备基本要求	标准 1U 或 2U 机架式设备，含单交流电源，≥1 个 RJ45 串口，≥1 个 GE 管理口，≥2 个 USB 接口，≥6 个 GE 电口，≥1 个扩展槽位，硬盘≥2T，SQL 处理性能≥5000 条/秒，入库语句量≥3000 条/秒。提供 3 年质保服务。
2	数据库类型	支持主流数据库：Oracle、SQL Server、MySQL、DB2、Sybase、PostgreSQL、Informix、DM、Oscar、Kingbase、Gbase、Hbase、MongoDB、HIVE、Redis、Cache，提供界面截图证明。
3	部署方式	<p>支持在目标数据库安装 Agent 解决无法通过旁路镜像获取流量的场景，如同服务器部署数据库和应用系统、云环境、虚拟化环境场景下数据库的审计，提供界面截图证明。</p> <p>支持在 IPV6 环境中部署，且支持所有数据库 IPV6 协议的审计，提供界面截图证明。</p>
4	审计内容	<p>审计内容：支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小；</p> <p>审计要素：执行人 who：审计到前端的应用用户、数据库用户名、主机名称、操作系统用户等；执行内容 what：具体的操作，访问的数据库、表、列、字段、包、存储过程、函数、视图；执行时间 when：每个操作发生的具体时间，操作时间、登录时间等；执行地点 where：操作的来源和目的，包括 IP 地址、MAC 地址、用户名、端口号、数据库类型；</p> <p>支持 ssh、telnet、nfs、smb、ftp、http 等运维协议的审计，提供界面截图证明。</p> <p>支持 MySQL 数据库的 SSL/TSL 加密链路审计，提供界面截图证明。</p>
5	入侵检测能力	<p>支持扩展对基于数据库漏洞进行攻击行为监测和告警，支持 200 个以上的数据库漏洞攻击规则库</p> <p>高危操作：对超过特定行数阈值的批量数据修改、删除，或全表 Update、Delete 等行为进行监测</p>
6	告警能力	根据风险操作、SQL 注入、漏洞攻击检测、语句管理等模块定义告警规则
7	阻断能力	对于高风险操作所在的会话，支持旁路阻断功能，避免更大的危害，提供界面截图证明。
8	审计结果展现与查询	<p>操作记录的信息：审计结果中包括：告警级别、事件发生时间、客户端 IP、目标数据库 IP、操作类型、客户端 MAC 地址、客户端端口号、返回状态、结果信息、客户端执行命令等详细信息内容。</p> <p>对审计结果集敏感内容可进行屏蔽，提供界面截图证明。</p> <p>对详细信息中的 SQL 语句能进行客户化翻译，提供界面截图证明。</p>
9	报表统计分析	<p>风险分析：根据风险语句、sql 注入、漏洞攻击、风险操作等维度以时间维度统计数据库分析信息。支持规则命中查询、支持风险查询。</p> <p>语句分析：基于 SQL 语句的操作类型统计，支持失败 sql 统计、Top sql 统计；支持针对新型语句、语句审计模板检索。</p>

10	产品资质	产品需具备公安部销售许可证，且须为增强级，提供有效证书的复印件。 产品需具备国家信息安全测评信息技术产品安全测评证书，且须为 EAL3+ 及以上，提供有效证书的复印件。 产品需具备 IPv6 Ready Logo 认证证书，提供有效证书的复印件。
11	厂商资质	厂商具有中国信息安全测评中心颁发的《国家信息安全测评信息安全服务资质证书（安全工程类三级）》，提供有效证书的复印件 厂商应通过 ISO 20000-1:2011 标准认证，且认证范围至少包含向外部客户提供整体安全解决方案，安全软件的设计、开发和运行维护，硬件的运行维护，安全相关的 SaaS 及运营服务等，提供有效证书的复印件； 厂商是微软 MAPP 项目合作伙伴，可以在微软每月发布安全更新之前获得漏洞信息，为客户提供更及时有效的保护，提供微软官方网站截图证明 厂商具有中国信息安全测评中心颁发的《国家信息安全测评信息安全服务资质证书（安全开发类二级）》

(三) 堡垒机

序号	类别	功能与技术描述
1	设备基本要求	标准 1U 或 2U 机架式结构，1 个 console 口，2 个 USB 口；6 个千兆电口，2 个 SFP 插槽，2 个可扩展插槽；16G 内存，4T 存储空间，双电源；不少于 500 个主机/设备许可，用户数不限制；提供 3 年质保服务。
2	系统配置架构要求	采用物理旁路模式部署，不影响网络结构。支持运维审计日志集中管理运维审计系统分布式部署方式。 支持堡垒机集群模式部署，添加一台或多台协议代理服务器，分担堡垒机主服务器性能压力，便于提高整体性能；支持集群设备多节点数据实时同步。
3	组织结构	不限级数的进行分层分级分类管理，支持从 AD 域抽取 OU，方便快捷建立组织结构，支持从 AD 域抽取 OU，方便快捷建立组织结构，帐号支持从 AD 域内抽取，方便快捷建立主帐号。提供界面截图证明。
4	资源管理	支持柱形图方式查看系统中不同资源所占总数。 支持 unix 资源、网络资源、windows 资源、数据库资源、C/S 资源、B/S 资源、中间件资源、大型机资源等。 支持 SSH、TELNET、FTP、SFTP、VNC、XWINDOW、WINDOWS 文件共享等协议。
5	用户权限管控要求	系统默认自带三权分立用户，系统管理员、运维管理员和审计管理员权限相互制约。
6	授权管理	支持自定义角色。角色可按照组节点进行定义，从而实现分层分级管理模式。角色权限可以针对组织结构、用户、资源、授权关系和审计等自由结合。 资源授权模式基于岗位授权，岗位上绑定资源账号，这样授权可迁移、授权粒度更细；并可针对岗位设置相关安全策略。提供界面截图证明
7	审计管理	支持对 RDP 实时会话的锁定和解锁，并可以在锁定解锁时发送即时通讯消息。发现危险操作可立即进行锁定操作。提供界面截图证明 RDP 审计策略支持关键帧，帧间隔，录像文件压缩比等设置，以缩小录像文件大小。提供界面截图证明。 RDP 审计策略支持审计录像的画质选择，至少支持真彩，仿真彩，灰度三种画质选择。
8	流程管理	支持将重要的资源设置为登录审批，登录访问是需提交工单申请，审批人同意才可登录。 支持授权审批功能，即针对不属于自己岗位的资源，需要临时运维操作进行临时申请审批，申请中包含需要临时登录的资源，账号，登录时间范围等信息。 支持将高危命令设置为执行需审批策略，当指定资源执行高危命令时，需要审批通过后，命令才能执行生效。

9	单点登录	运维人员可将经常访问的资源添加到收藏夹，根据自己的登录习惯，更加便捷的定位需要访问的资源。
		支持一键批量登录选中的资源，简化工作量。
		支持将登录配置保存为默认后，可以一键快速登录目标资源。
10	产品资质	产品需具有信息系统安全专用产品销售许可证，提供有效证书的复印件
11	厂商资质	厂商具有 ISO9001 认证，提供有效证书的复印件；厂商具有 CMMI5 认证，提供有效证书的复印件； 厂商具有获得国家互联网应急中心颁发的《网络安全应急服务支撑单位-国家级》，提供有效证书的复印件；

三、交货、培训、售后服务要求：

1. 交货时间为合同签订后 20 个日历日内必须安装调试完毕。
2. 中标人设备到达安装现场，应提前通知招标人，安装前开箱查验由中标人会同招标方及有关人员根据有关清单进行验收，并按照招标人方需求安装相应的操作系统及软件。
3. 安装开始前，中标人应委派项目负责人与招标人代表根据所提供的设备、材料装箱清单共同对设备进行开箱验收，进行确认。一旦清单与采购要求不符或发现缺损、不实，中标人须立即予以更换，有关费用及可能造成的损失全部由中标人承担。
4. 设备安装调试完成，按招标人要求提供系统安装、数据库实施安装、数据迁移等各项服务。在实施过程中如发现系统不兼容或硬件参数与招标参数有偏离，中标人无法正常实施本项目，招标人有权中止合同，并对中标人做出相应处罚。
5. 中标人须提供现场技术培训，要求为使其掌握设备使用技巧、常见故障排除等知识。

四、拟签合同主要条款

本合同无预付款；合同签订完成后 7 日内付合同价 20% 的预付款；全部采购设备到场安装调试完成，并经甲方验收合格后 7 日内，向乙方支付至合同价的 90%；项目整体竣工验收合格使用六个月后，无质量问题，7 日内向乙方支付至合同价的 100%。

项目安装调试完成每延迟一天，罚款 2000 元，延期达到 5 天，甲方有权取消合同，且乙方还需承担由此对甲方造成的一切损失。

第三章投标文件格式

第一部分：投标函及投标函附录

投 标 函

招标人：南京医药股份有限公司

1、根据已收到的南京医药应急物资储备管理项目配套网络设备采购项目的招标文件，我单位经考察和研究上述项目招标文件的投标须知、合同条件和其他有关文件后，我方愿以人民币_____元的总价，按上述合同条件和招标文件的要求条件承包上述项目的实施。

2、一旦我方收到本项目中标通知书，我方保证在__个日历日内按招标文件要求完成设备供货及安装调试服务，并提供__年的免费原厂质保。

3、如果我方中标，将派出_____（姓名）作为本工程的项目负责人。

4、我方接受招标文件中的要求条件。

5、我方同意所递交的投标文件在“投标须知”前附表规定的投标有效期内有效，在此期间内我方的投标有可能中标，我方将受此约束。

6、除非另外达成协议并生效，你方的中标通知书和本投标文件将构成约束我们双方的合同。

投标人：（盖章）

单位地址：

法定代表人或委托代理人：（盖章或签字）

日期： 年 月 日

法定代表人资格证明书

(本格式仅作为参考格式)

单位名称：

地址：

姓名：

性别：

年龄：

职务：

系 的法定代表人。

特此证明。

投标人：（盖章）

日期：年 月 日

授权委托书

本授权委托书声明：我(姓名)系(投标人名称)的法定代表人，现授权委托(单位名称)的(姓名)为我公司代理人，参加(招标人)的项目的投标活动。代理人在投标、开标、评标、合同谈判过程中所签署的一切文件和处理与之有关的一切事务，我均予以承认。

代理人无转委托。特此委托。

代理人： 性别： 身份证号：

年龄： 单位： 职务：

投标人：（盖章）

受托人：（签字或盖章）

法定代表人：（签字或盖章）

日期： 年 月 日

第二部分：投标报价书

投标报价表

序号	设备名	品牌及具体型号	配置描述	数量	单位	单价 (元)	小计 (元)
1	网络 (日志) 审计设备			1			
2	数据库审计设备			1			
3	堡垒机 (运维安全审计)			1			

第三部分：资格证明文件

投标人自行准备，包括但不限于招标文件要求的全部资格证明资料。

