**湛汽集团信息系统及网络安全**

**等级保护项目（一期）询价文件**

**广东省湛江汽车运输集团有限公司**

**2021年3月**

目录

[第一章 询价书 1](#_Toc7908)

[第二章 采购需求 3](#_Toc24470)

[第三章 评标方法和标准 18](#_Toc5902)

[第四章 报价文件参考格式 23](#_Toc32748)

[第五章 合同格式 37](#_Toc25521)

[合同通用条款 37](#_Toc14515)

**第一章 询价书**

根据业务发展需要，广东省湛江汽车运输集团有限公司（以下简称询价人或采购人）计划进行“信息系统及网络安全等级保护项目（一期）”（以下简称“项目”），根据项目的需求，询价人决定通过询价采购的方式来建设本项目。

1. **项目基本情况**

项目编号：DJBH-2021

项目名称：信息系统及网络安全等级保护项目（一期）

预算金额（元）：**485000**

最高限价（如有）：**485000元**

采购需求：

1. 标的名称：信息系统及网络安全等级保护项目（一期）
2. 标的数量：1批
3. 简要技术需求或服务要求：
4. 项目编号:DJBH-2021
5. 标的内容一览表

|  |  |  |
| --- | --- | --- |
| 标的名称 | 数量 | 最高限价 |
| 信息系统及网络安全等级保护项目（一期） | 1项 | 485000元 |

1. 本项目只允许采购本国产品；
2. 简要技术要求：具体详见采购需求。
3. 其他：本项目不属于政府采购项目。
4. 合同履行期限：合同签订后60日历天内安装调试完毕并交付使用。
5. 本项目不接受联合体报价。报价人不能为失信被执行人。
6. 为保障本项目正常进行，报价人提交报价文件前需向询价人汇入保证金5万元。

汇入账户：广东省湛江汽车运输集团有限公司

汇入账号：2015 0203 0902 2102 721

1. 在询价人与中选人签订书面合同后 5个工作日内，询价人将向中选和未中选的报价人退还保证金。下列任一情况发生时，保证金将不予退还：
2. 报价人在提交报价文件截止后撤销报价文件的；
3. 中选后中选人放弃中选资格的；
4. 报价人在报价文件中提供虚假材料的；
5. 除因不可抗力或询价文件认可的情形以外，中选人不与询价人签订合同的或在签订合同时向询价人提出附加条件的；
6. 属于报价人相互串通报价的情形。

**第二章 采购需求**

1. **有关说明**
2. 报价人须对本项目的采购标的进行整体报价，任何只对本项目采购标的其中一部分内容、数量进行的报价都被视为无效报价。
3. 采购需求中标注“★”号条款为实质性条款，必须逐条进行响应，有任何一条负偏离的，将导致**无效报价**。
4. 采购需求中标注“▲”号条款为重要技术参数，但不作为无效报价条款。
5. **项目采购内容**

|  |  |  |  |
| --- | --- | --- | --- |
| **采购内容** | **数量** | **最高限价****（**人民币 元**）** | **交货期** |
| 信息系统及网络安全等级保护项目（一期） | 1项 | 485000 | 合同签订后60日历天内安装调试完毕并交付使用。 |

1. **采购设备清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **部署位置** | **产品名称** | **性能配置要求** | **数量** | **单位** | **产品作用** |
| 1 | 互联网出口区 | 下一代防火墙 | 采用专用多核硬件平台，网络处理能力≥8G，并发连接≥350万，每秒新建连接≥8万/秒， 标准2U机箱，双电源，配置不少于6个10/100/1000M自适应千兆电接口、12个千兆光口、2个USB口、1个RJ45 Console口，配置不低于60GB SSD固态硬盘容量；默认支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及URL分类管理、流控和IPSec VPN模块；报价中包括3年硬件维修及3年软件全功能模块升级服务。 | 1 | 台 | 部署在网络出口区边界，作为最基础的网络安全防护，安全域、边界防护、内网防护。防攻击防漏洞防木马防僵尸病毒等。 |
| 2 | 上网行为管理 | 标准1U机架式设备，专用硬件平台和安全操作系统，配置≥4个千兆光口、10个千兆电口、单电源。用户数无限制，适用于150M以内带宽接入网络。整机吞吐≥8Gbps, 含3年硬件维修及3年软件全功能模块升级服务。 | 1 | 台 | 部署在网络出口区，对单位员工上网行为进行管理和审计；满足“公安部82号令”要求上网行为记录保存6个月的要求；同时通过此设备可以管理员工接入互联网的权限，实现网络带宽资源的合理分配等。 |
| WAF防火墙 | 专业级WEB应用防火墙设备及专业性WEB应用防火墙资质，而非NGAF、NGFW、UTM设备及资质。1U上架设备， 不少于2个USB口、双电源、1个RJ-45 Console口、1个10/100/1000 Base-T带外管理口、1个10/100/1000 Base-T HA口、4个具备BYPASS功能的10/100/1000Base-T接口、1个网络接口扩展槽位，整机吞吐≥2Gbps，并发连接数≥200万，含3年硬件维修及3年软件全功能模块升级服务。 | 2 | 台 | 加强Web系统的Web安全防护能力，能够对Web系统的应用层攻击（如SQL注入和XSS攻击等）进行防护，企业网站的网页内容防篡改功能等。 |
| 3 | 安全管理区 | 日志审计系统 | 日志审计硬件平台，1U标准机架式，单电源，专用千兆硬件平台和安全操作系统，不少于6个千兆电口、1个管理口，2个USB接口、1TB存储容量。日志处理性能≥3000EPS，提供不少于30个审计对象授权许可；支持主机操作系统、网络设备、安全设备日志收集，查询，告警，审计，报表等功能，含3年硬件维修及3年软件全功能模块升级服务。 | 1 | 台 | 日志审计是最直接、最准确、最符合法律法规要求的审计手段。 |
| 4 | 数据库审计系统 | 审计一体机，1U上架专用设备，不少于6个电口（含1个管理口，1个HA口）、1个接口扩展槽、1个RJ45串口、2TB硬盘容量、1个CF卡插槽、单电源；每秒入库速度≥10000，含嵌入式审计软件1套；支持Oracle、SQL-Server、MySQL等数据库的审计；报价中含3年硬件维修及3年软件全功能模块升级服务。 | 1 | 台 | 产品可对数据库协议解析、事件关联分析为基础，可以精准识别数据库操作，满足等保应用安全、数据安全和审计的相关要求。 |
| 5 | 堡垒机 | 1U机架式软硬一体设备，专用硬件平台和安全操作系统，不少于6个千兆电口、1个console管理口、1TB硬盘容量、单电源，自带应用发布软件；实现对运维操作的集中管理、访问控制、单点登录以及操作审计等功能。不少于200路图形会话或不少于600路字符会话并发，提供不少于50个资产管理授权，用户数无限制，远程应用发布无限制，含3年硬件维修及3年软件全功能模块升级服务。 | 1 | 台 | 产品集账号、认证、授权、审计为一体的设计理念，实现对数据中心的网络设备、数据库、安全设备、主机系统、中间件等资源统一运维管理和审计，满足等保三级对运维、操作认证及审计的要求。 |

1. **主要设备技术参数要求**

**（一）防火墙:**

1. ▲标准2U设备，双电源；实配≥6个10/100/1000M千兆电接口及12个千兆光接口，接口定义WAN和LAN无限制，吞吐≥8Gbps，并发连接数≥350万，每秒新建连接数≥8万/秒，配置不低于60GB SSD固态硬盘容量；提供入侵防御模块、防病毒模块、应用识别模块、VPN模块；提供3年IPS特征库、3年防病毒特征、3年应用识别及URL分类库等全功能模块升级服务，提供3年硬件维保服务。
2. ▲开通网络入侵防御功能，系统默认自带IPS规则库≥4000条。开通网络应用识别功能，系统默认自带应用识别≥1600种。开通网络防病毒功能，系统默认自带防病毒库≥1200万条；提供界面截图证明。
3. 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。
4. 支持基于硬件Hypervisor技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的CPU、内存、接口等资源。提供虚拟化防火墙CPU、内存、硬盘配置截图。
5. 支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每IP总连接数控制、每IP新建连接数控制。
6. ▲系统基于SQL注入、CC攻击检测、注入攻击的规则的防御方式，提供自主知识产权关于SQL注入漏洞检测方法及系统、检测和防御CC攻击的方法及装置、一种脚本注入攻击检测方法和系统证明文件。
7. 支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响；
8. 支持基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定；
9. 具备协议自动识别功能；支持自定义事件功能；
10. ▲具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的CVE漏洞发现数不低于1000个。提供自主挖掘CVE列表。
11. 支持静态路由、动态路由（RIP、OSPF、BGP4），基于入接口、源地址、目标地址、服务端口、应用类型的策略路由；
12. 支持通过ICMP、TCP、DNS、FDP、RADIUS、POP3、HTTP、HTTPS、UDP、LDAP、ORACLE、 MSSQL、MYSQL等十五种以上协议，实现对链路可用性的多重健康检查；
13. 可对exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip等常见的格式进行动态沙箱分析；可对rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做PE内嵌检测，并且能指出文件偏移位置； 提供相关界面截图。
14. 内置多种沙箱环境与应用环境，使用反沙箱、时光加速、机器学习等领先技术，确保恶意样本逃逸率大幅降低。
15. ▲支持多链路智能选路，根据业务对抖动、时延和带宽的要求，在多条不同链路上智能动态选路，通过自动重传技术，实现链路切换时无丢包，业务不掉线；提供相关界面截图；
16. 支持DNS透明代理功能，可将指定范围内的DNS请求自动重定向至管理员指定的DNS服务器，且支持多台DNS服务器的负载均衡；
17. 支持HA设备之间的会话自动同步，包括主主模式和主备模式，确保HA切换时业务不发生任何中断；
18. 支持整机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的TOP10统计展示、基于具体威胁事件/威胁类型的TOP10统计展示等，统计展示的时间周期包括1小时/1天/7天/30天；
19. 提供防火墙日志云端存储与分析服务，可将防火墙、NAT、系统和安全等日志一键上报至云端；
20. 支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能；
21. 支持源NAT、目的NAT、静态NAT，支持一对一、一对多和多对多等形式的NAT；
22. 产品具备计算机信息系统安全专用产品销售许可证-增强级；提供有效的资质证明复印件。
23. ▲为确保项目实施服务能力，所投产品厂商具备信息安全测评信息安全服务资质证书（安全工程类三级）。提供有效的资质证明复印件。
24. 产品具备IPv6 Ready logo Phrase 2认证；提供有效的资质证明复印件。
25. ▲为确保项目安全性、机密性，产品厂商必须具备涉密信息系统集成资质证书（甲级系统集成/软件开发运行维护）。需提供有效资质证明复印件。
26. ▲产品厂商为微软MAPP计划成员单位，第一时间获取漏洞信息，实现安全防御。需提供有效证明文件。
27. ▲所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（千兆EAL4+）（提供证书复印件以及中国信息安全测评中心产品测评网页截图并加盖厂商公章）。

**（二）上网行为管理：**

1. ▲多核架构设计，不允许采用X86架构，标准1U机架式设备，专用硬件平台和安全操作系统，配置≥4个千兆光口、10个千兆电口、单电源。用户数无限制，适用于150M以内带宽接入网络。整机吞吐≥8Gbps，提供3年硬件维修及3年软件全功能模块升级服务。
2. 支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备。
3. 支持静态路由、策略路由、动态路由、ISP路由；策略路由支持七元组策略；动态路由支持RIP、OSPF等；ISP路由支持运营商地址自定义；
4. 支持IPV6网络，可对IPV6网络进行审计、流量控制；
5. 支持服务器负载均衡，支持一个公网IP映射到内网多台服务器，服务器间支持连接和源地址hash,支持服务器健康检查；（提供WEB配置截图）
6. ▲提供WEB防护功能，可对防盗链、CSRF攻击、CC等攻击行为进行防护。（提供WEB配置截图）；
7. 支持主流P2P、IM、在线视频、网络游戏、网络炒股等应用识别；
8. 支持BYOD特征库，可识别IOS版和安卓版移动互联网软件如微博、微信等特征；
9. 可广泛识别恶意网站、违法网站，支持自定义URL过滤，并支持URL的模糊匹配；
10. ▲支持弱密码扫描功能，即时了解网内主机是否存在弱口令，内置弱口令库，并可自定义字典库。（提供WEB配置截图）；
11. 支持收集网站访问日志，记录用户所有访问网站行为；支持收集搜索引擎日志，记录用户的搜索内容；支持收集IM通讯软件日志，记录用户登陆、注销、收发消息、收发文件等行为；支持收集邮件日志，记录邮件发件人、收件人、主题、正文、附件等信息；
12. 支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息；
13. 应用特征数支持5000+；
14. 支持微信认证功能，使用微信连WiFi2.0接口，限制微信流量放通（pc和移动端，认证通过放通），支持基于http获取access\_token，支持微信内部浏览器http弹portal强制关注功能（定时检查用户是否关注公众号），提供web界面配置截图；
15. 可识别私接主机个数，并可制定策略分别设置私接终端类型个数为阀值进行封堵，支持自定义阻断时间，同时支持基于IP及IP段配置白名单；
16. ▲支持IPS功能，支持基于源、目的、规则集的入侵检测；支持针对WEB服务器防护，包括网页防爬虫、网页防篡改、HTTPS防护、DDOS攻击防护、WEB攻击过滤等。（提供WEB配置截图）；
17. 内网资产监控，可对终端风险级别、操作系统、浏览器类型、应用、杀毒软件等方面进行监控（提供WEB配置截图）；
18. ▲支持杀毒功能，可对HTTP、FTP、POP3、SNMP、IMAP协议的病毒进行查杀；支持ZIP、RAR等压缩文件的病毒查杀。压缩默认支持5层，最大20层（提供WEB配置截图）；
19. 支持用户（用户组）+应用（应用组）+时间等条件的组合进行多线路带宽管理；
20. 支持应用、用户流量统计，应用流量支持趋势图、饼状图呈现，可查看某一应用的流量趋势图和其Top流量用户；
21. 支持DNS透明代理；支持DNS负载均衡；支持DNS静态域名映射；支持DNS特定域名请求转发；
22. 针对设备系统健康检测功能，可以在某一时间段内逐级深入，并纂取任一时间内的详细信息，并可路转系统日志。
23. 设备具备公安部公共信息网络安全监察局颁发的《互联网公共上网服务场所信息安全管理系统》证书，并提供检测报告；
24. ▲产品厂商具备中国国家信息安全漏洞库（CNNVD）技术支撑单位一级，需提供有效证明文件。
25. 产品具备IPV6 Ready 证书；提供资质证明；
26. ▲为确保项目安全性、机密性，产品厂商必须具备涉密信息系统集成资质证书（甲级系统集成/软件开发运行维护）。需提供有效资质证明复印件。
27. ▲产品厂商为微软MAPP计划成员单位，第一时间获取漏洞信息，实现安全防御。需提供有效证明文件。

**（三）日志审计系统**

1. ▲1U标准机架式，单电源，专用千兆硬件平台和安全操作系统，不少于6个千兆电口、1个管理口、2个USB接口、1TB存储容量。日志处理性能≥3000EPS，提供不少于30个审计对象授权许可，含3年硬件维修及3年软件全功能模块升级服务。
2. 能对网络设备、安全设备和系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计；
3. 无需另外安装软件组件，审计中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFPT、NetBIOS、OPSEC等多种方式完成日志收集功能；
4. 针对文本格式的日志采集，支持本地文件、Windows共享和FTP、SFTP获取四种采集方式；
5. 系统支持以资产树的形式显示不同资产区域之间的关系；系统支持以列表的形式显示某个管理区域中的所有资产清单；
6. 工作台为用户提供了一个从用户自身业务需要出发使用本系统的快速入口。用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为不同角色的用户建立不同维度的仪表板；
7. ▲无需另外安装软件组件，审计中心即可实现新增Oracle数据库自身日志的采集任务、新增SQL Server数据库自身日志的采集任务新增Apache服务器日志的采集任务、新增Lotus Domino的日志采集任务；新增Checkpoint的日志采集任务；分别提供截图证明；
8. 系统必须具备日志范式化功能，实现对异构日志格式的统一化；
9. ▲内置Cisco PIX和交换机的事件编码知识库；内置Windows、Linux、Solaris、AIX操作系统的事件ID知识库；内置Oracle、SQL Server、MySQL、Informix、DB2数据库的事件编码知识库；分别提供截图证明；
10. 日志采集器支持以SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC等多种方式完成日志收集；
11. 系统可以统计不同采集器和不同安全域下的设备个数并以饼状图展示，统计采集器或安全域中事件量Top10以柱状图展示，配以统计列表；
12. 实时显示日志内容包括：接收时间、事件类型、事件名称、报警级别、来源IP、目的IP、设备类型、设备来源IP等；
13. ▲系统提供海量日志关联分析方法能力，提供国家第三方权威机构颁发的技术证明文件；
14. 提供内置报表模板；支持按照天、月度、季度、年度等时间周期生成报表；支持在报表中以柱状图、曲线图、饼状图方式统计安全报警情况；
15. ▲威胁情报，系统支持通过导入或者主动自动抓取的方式获取外部相关威胁情报信息，并能将这些威胁情报用于关联分析；提供截图证明。；
16. 产品须获得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》日志分析-行标三级；提供有效的资质证明复印件；
17. ▲为确保项目安全性、机密性，产品厂商必须具备涉密信息系统集成资质证书（甲级系统集成/软件开发运行维护）。需提供有效资质证明复印件；
18. ▲产品厂商具备《信息安全服务资质（一级信息系统安全运维服务）》，需提供有效证明文件。
19. ▲产品厂商为微软MAPP计划成员单位，第一时间获取漏洞信息，实现安全防御。需提供有效证明文件。

**（四）数据库审计系统**

1. ▲1U上架专用设备，不少于6个电口（含1个管理口，1个HA口）、1个接口扩展槽、1个RJ45串口、2TB硬盘容量、1个CF卡插槽、单电源；每秒入库速度≥10000，含嵌入式审计软件1套；提供3年硬件维修及3年软件全功能模块升级服务。
2. 支持旁路部署方式，无须在被审计系统上安装软件，对原有网络不造成影响，审计产品的故障不影响被审计系统的正常运行；
3. 支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache数据库审计。
4. 支持对Oracle数据库状态的自动监控，可监控会话数、连接进程、CPU和内存占用率等信息；支持国产数据库人大金仓、达梦、南大通用、神通数据库的审计； 支持MongoDB数据库的审计； 支持对针对数据库的XSS攻击、SQL注入攻击行为进行审计（提供功能界面截图）。
5. 支持访问数据库的源主机名、源主机用户、SQL操作响应时间、数据库操作成功、失败的审计；支持数据库操作类、表、视图、索引、触发器、存储过程、游标、事物等各种对象的SQL操作审计；
6. 支持数据库存储过程自动获取及内容审计；
7. 支持Telnet协议的审计、FTP协议的审计能够审计用户名、操作命令、命令响应时间、返回码等；
8. 支持RDP协议审计，可审计关键的键盘输入，记录会话过程；支持SSH协议审计，能够审计用户名、操作命令、命令响应时间、返回码；
9. ▲支持自动方式建立web访问和SQL访问之间的对应关系，生成访问行为模型库（提供功能界面截图）。
10. 支持中间件环境下的SQL语句关联到HTTP操作，HTTP操作关联到HTTP-ID，实现中间件环境下的审计追溯。；
11. ▲数据库操作行为基线包括数据库账号、操作类型（SQL模板）等行为特征，安全威胁检测等。提供第三方权威机构关于检测数据库是否遭到跨站脚本攻击的方法证明文件；
12. 可审计记录FTP、邮件、HTTP等方式传输的文件（包括文本、Word、Excel等格式），并对传输的文件内容中包含关键字的行为进行告警；
13. 系统应自带不少于100个缺省的审计规则库，方便用户选择使用；
14. 支持数据库操作的命令级阻断，可阻断单个操作，但会话保持。
15. 支持按照风险级别进行告警，告警方式支持界面告警、Syslog告警、SNMP trap告警、短信告警、邮件告警。
16. ▲为确保项目质量，所投产品是主流厂商产品，并且近三年(2017年-2019年)年市场占有率前三，提供2017年或2018年或2019年权威机构盖章的数据引用证明文件（如：IDC、CCID、Frost & Sullivan等权威机构）。
17. 支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多IP登录、上下班操作量对比异常、操作响应时间超时等信息；
18. 支持按每天、每周、每月、时刻生成报表，并且生成Word、PDF、xls、HTML格式的报表；
19. 数据库访问日志，支持按数据库名、数据库表名、字段值、数据库登陆账号、数据库操作命令、SQL语句关键字、数据库返回码、SQL响应时间、数据库返回行数作为查询和统计条件。；
20. 产品具有《计算机信息系统安全专用产品销售许可证》（增强级）。需提供有效资质证明复印件；
21. ▲为确保项目安全性、机密性，产品厂商必须具备涉密信息系统集成资质证书（甲级系统集成/软件开发运行维护）。需提供有效资质证明复印件；
22. ▲为确保项目实施服务能力，所投产品厂商具备信息安全测评信息安全服务资质证书（安全工程类三级）。提供有效的资质证明复印件。
23. ▲产品厂商为微软MAPP计划成员单位，第一时间获取漏洞信息，实现安全防御。需提供有效证明文件。

**（五）堡垒机**

1. ▲1U机架式软硬一体设备，专用硬件平台和安全操作系统，不少于6个千兆电口、1个console管理口、硬盘容量1TB、单电源，不少于200路图形会话或不少于600路字符会话并发，自带应用发布软件；提供不少于50个资产管理授权，用户数无限制，远程应用发布无限制，提供3年硬件维修及3年软件全功能模块升级服务。
2. 物理旁路，逻辑串联模式，不影响正常业务流量，并支持双机热备；
3. 数据库协议：支持Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、TeraData等数据库类型；
4. 支持web页面防跳转功能，进行http/https访问过程中，运维人员仅允许访问授权地址。提供界面截图证明；
5. 支持通过堡垒机web页面内嵌SSH、FTP、TELNET运维工具访问目标资源；
6. 系统级账号三权分立，系统级账号包括：系统账号管理员，系统审计员，系统管理员；业务管理员以业务管理权限范围实现不同业务管理员权限的完全隔离，可设置业务管理员可管理的用户组和资源组范围；
7. ▲支持用户忘记登录密码时，可通过邮件或短信方式获取验证码，验证通过后重置登录密码，提供界面截图证明并加盖厂商公章；
8. 对违规或高危操作的指令（黑名单）进行日志提醒、忽略命令、阻断会话或二次审批；
9. 从账号密码代填自动登录，使用人员不必知道服务器账号及密码（包括http/https访问的账号密码代填）支持基于角色管理的安全审计功能；
10. 针对SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计；记录会话时间、命令执行时间、会话协议、服务端IP、服务器端口、客户端IP、客户端端口、操作命令、返回信息、运维用户账号、审批用户账号、资源账号等信息；
11. ▲自动改密支持Linux、Unix、Windows（采用RPC方式）、AIX以及Oracle、SqlServer、PostgreSQL、MySql、DB2、Informix 、SYBASE的内置自身账号密码。提供界面截图证明；
12. 实时监控当前连接发生的所有会话信息和阻断功能；实时监控审计系统CPU、内存、磁盘的使用情况；记录审计系统自身的管理操作，保障审计系统自身安全；
13. ▲为确保项目质量，所投产品是主流厂商产品，并且近三年(2017年或2018年或2019年)市场占有率前三，提供权威机构盖章的数据引用证明文件。；
14. 随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并严格遵守密码强度设置；
15. 支持Oracle、postgresql、sybase、mysql、sqlserver数据库下行返回行数和oracle数据库变量绑定；
16. 支持按设备、系统账号、计划开始时间、改密周期等信息配置改密计划，到期自动执行；
17. DP图形操作过程中键盘输入操作记录和鼠标点击行为记录；支持开启或关闭键盘输入审计功能；支持RDP窗口标题审计，并支持窗口标题内容检索定位回放；支持对剪贴板拷贝文件行为和文本信息内容的记录。；
18. RDP协议支持windows服务端开启安全层SSL加密，加密级别符合FIPS标准，允许运行使用网络级别身份验证的远程桌面的计算机连接。提供界面截图证明；
19. 支持客户端菜单模式访问：用户可通过字符菜单（TELNET、SSH协议）或图形菜单（RDP、VNC协议）方式选择目标服务器并进行访问；
20. 支持数据备份；系统配置的导入、导出功能；配置和数据备份自动导出到FTP服务器；
21. 产品具备涉密信息系统产品检测证书。需提供有效资质证明复印件；
22. 产品具备计算机信息系统安全专用产品销售许可证。需提供有效资质证明复印件。；
23. ▲为确保项目安全性、机密性，产品厂商必须具备涉密信息系统集成资质证书（甲级系统集成/软件开发运行维护）。需提供有效资质证明复印件；
24. ▲产品厂商具备工业信息安全测试评估机构能力认证证书（二级）；提供有效的资质证明复印件。
25. ▲产品厂商为微软MAPP计划成员单位，第一时间获取漏洞信息，实现安全防御。需提供有效证明文件。

**（六）WAF防火墙：**

1. ▲专业级WEB应用防火墙设备及专业性WEB应用防火墙资质，而非NGAF、NGFW、UTM设备及资质。1U上架设备，不少于2个USB口、双电源、1个RJ-45 Console口、1个10/100/1000 Base-T带外管理口、1个10/100/1000 Base-T HA口、4个具备BYPASS功能的10/100/1000Base-T接口，整机吞吐≥2Gbps，并发连接数≥200万，提供3年硬件维修及3年软件全功能模块升级服务。
2. 支持透明、代理模式、旁路部署、单臂部署、策略路由部署，支持NAT环境下的用户识别能力。
3. ▲具备SQL注入攻击、XSS攻击、WEB恶意扫描防护的检测与防御能力、企业网站的网页内容防篡改功能，提供自主知识产权关于SQL注入攻击检测方法及系统证明文件。
4. 具备HTTPS加解密攻击流量的检测及防护功能，具备HTTP协议详细字段分析能力同时支持自学习功能
5. 具备暴力扫描防护功能，防止暴力破解网站，支持跨站脚本攻击的检测，提供自主知识产权关于跨站脚本攻击的检测方法证明文件。
6. 具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截；
7. 具备XML DoS检测与防御能力
8. 具备SYN Flood/UDP Flood/ICMP Flood攻击检测与防御能力
9. 支持Cookie信息防篡改功能，至少包括Cookie签名、Cookie自学习、Cookie加密等属性设置。
10. 具备客户端访问控制功能，预防恶意客户端进行访问频率的多层次恶意访问。
11. 支持网站盗链行为检测与防御。
12. 支持Web服务器操作系统指纹信息返回保护；支持Web服务器信息返回保护。；支持HTTP错误页面信息返回保护；支持银行卡信息返回保护；应支持身份证信息返回保护；应支持文件上传下载控制功能
13. ▲应具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响；提供界面截图证明。
14. 支持获取Web安全事件的原始攻击信息，提供自主知识产权关于 SQL解析及匹配的方法和系统证明文件。
15. 具备慢速攻击防护功能，有效防护Slow headers方式、Slow body方式、Slow read方式等慢速攻击；
16. 应具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑；提供界面截图证明。
17. ▲为确保项目质量，所投产品是主流厂商产品，所投产品2017-2019年必须连续3年市场占有率前三，提供证明文件。
18. 具备Web环境感知功能，自动识别被保护服务器操作系统、服务器类型、语言、中间件；
19. 产品具备计算机信息系统安全专用产品销售许可证（增强级）；提供资质证明。
20. 产品连续6年具备WEB应用防火墙认证证书；提供资质证明。
21. ▲产品有入围2019年Gartner魔力象限；提供证明文件。
22. ▲为确保项目安全性、机密性，产品厂商必须具备涉密信息系统集成资质证书（甲级系统集成/软件开发运行维护）。需提供有效资质证明复印件；
23. ▲产品厂商为微软MAPP计划成员单位，第一时间获取漏洞信息，实现安全防御。需提供有效证明文件。
24. ▲Web应用防火墙，硬件WAF，满足两台服务器（一主一冷备）的防护，对于网站的“读、写”权限进行封锁，实时监控网页状态和网络状态，一旦发生网络中断网页防篡改自动锁定页面，当发现篡改行为时第一时间还原网页内容，保障网页真实性。
25. **设备要求**
26. 货物为原制造商制造的全新产品，整机无污染，无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可依常规安全合法使用。
27. 货物为原厂商未启封全新包装，具出厂合格证，序列号、包装箱号与出厂批号一致，并可追索查阅。
28. 有关键主机设备的用户手册、保修手册、有关单证资料及配备件、随机工具等，使用操作及安全须知等重要资料应附有中文说明。
29. 报价人所投设备的性能指标，按照报价时厂家公开公布的实际性能指标参数如实填写。如报价文件有不如实填写的，到货验收时将导致整台设备被用户拒收和索赔，由此引起的所有损失由中选人负责。
30. 对于影响设备正常工作的必要组成部分，无论在技术规范中指出与否，报价人都应在报价文件中明确列出。
31. 本项目要求中所出现的工艺、材料、参数仅为方便描述而没有限制性，报价人可以在其提供的文件资料中选用替代标准，但这些替代标准应优于或相当于本用户需求书的标准。
32. ★其他要求：本项目必须按网络安全等级二级的标准进行设计及实施**（提供承诺函）**。
33. **质保期及售后服务**
34. 质量保证期（简称“质保期”）为三年，质保期自货物最终验收合格之日起算，质保期内中选人对所供货物实行包修、包换、包退、包维护保养，期满后可同时提供终身有偿维修保养服务。
35. 对采购人的服务通知，中选人在接报后1小时内响应，4小时内到达现场，48小时内处理完毕。若在48小时内仍未能有效解决，中选人须免费提供同档次的设备予采购人临时使用。
36. 中选人需提供7×24小时响应服务。
37. 中选人对设备提供终生维修服务，质保修期外只收取零部件配件费和维修费用，并享有优惠购买零配件待遇。
38. 中选人需对采购人所购买软件提供服务期内定期升级版本服务。
39. **安装与调试**
40. 中选人必须依照询价文件的要求和报价文件的承诺，将设备、系统安装并调试至正常运行的最佳状态。
41. 合同设备安装
42. 中选人负责合同设备的安装，一切费用由中选人负责。
43. 中选人安装时须对各安装场地内的其他设备、设施有良好保护措施。
44. 技术培训方案：根据采购人需求，负责采购人人员的免费教育培训。免费对设备操作人员和维修人员进行操作要领、维修保养常等内容进行培训，培训时间不低于3个工作日，使操作人员和维修保养人员达到独立操作程度；培训资料有中选人提供。
45. **采购项目交付或者实施的时间和地点**
46. 交付或实施的时间：合同签订后60日历天内安装调试完毕并交付使用。
47. 交付或实施的地点：广东省湛江市
48. **交付验收标准依次序对照适用标准**
49. 符合中华人民共和国国家安全质量标准、环保标准或行业标准；
50. 符合询价文件和响应承诺中采购人认可的合理最佳配置、参数及各项要求；
51. 货物来源国官方标准。
52. **设备验收要求**
53. 设备验收在采购人和中选人双方共同参与下按国家有关的规定、规范进行；
54. 验收时如发现所交付的设备有短装、次品、损坏或其它不符合本合同规定之情形者，采购人应作出详尽的现场记录，或由采购人、中选人双方签署备忘录。此现场记录或备忘录可用作补充、缺失和更换损坏部件的有效证据。因此产生的有关费用由中选人承担；
55. 如果合同设备运输和安装过程中因事故造成货物短缺、损坏，中选人应及时安排补货、换货， 以保证合同设备安装的成功完成。换货的相关费用由中选人承担；
56. 中选人保证合同项下提供的设备不侵犯任何第三方的专利、商标或版权。否则，中选人须承担 对第三方的专利或版权的侵权责任并承担因此而发生的所有费用。
57. **培训要求**
58. 在设备安装和调试完成后，中选人应提供培训服务，提供专业技术人员对采购人科室使用设备人员和相关管理人员进行一周培训，并保证两名以上操作人员熟练掌握操作技术为止。
59. 中选人需制定详细的培训内容和培训计划。
60. 如遇设备升级更新，中选人需及时提供更新操作指导。
61. **付款及结算方式**
62. 合同款支付：
63. 合同签订生效且采购人接到中选人通知和发票凭证资料后20日向中选人支付合同总价的30%。
64. 全部合同货物到达交货地点，并安装调试后10日历日内，凭验收合格单或验收合格报告，采购人在收到发票后20日内向中选人支付合同总价的60%。
65. 采购人在验收合格满一年收到发票后20日内向中选人支付合同总价的10%质保金。
66. 每次按合同支付款项前，中选人应向采购人提供与支付金额相符的合法有效完整的完税发票及凭证资料，且收款方、出具发票方、合同乙方均必须与中选人名称一致。
67. 违约责任：采购人逾期支付合同款项的，除应当支付合同款项外，还应当每日按合同总价的0.3‰向中选人偿付违约金，但因中选人自身原因导致无法及时支付的除外。
68. 付款方式：采用电汇形式。

**第三章 评标方法和标准**

1. **说明：**
2. 报价人必须严格按照《符合性审查表》的评审内容的要求如实提供证明材料并应加盖报价人公章，若报价人不满足《符合性审查表》中任何情形之一的，则其报价无效。
3. 本项目资格性、符合性审查内容详见《符合性审查表》。
4. 技术、商务评分：采购人组织的评审小组各成员分值的算术平均值（四舍五入后，小数点后保留两位有效数）。
5. 报价人应如实提交《综合评分表》要求提交的相关各类证明、资料等并应加盖报价人公章，报价人如未按要求提交的，该项评分为零分。

符合性审查表

**项目名称：**信息系统及网络安全等级保护项目（一期）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 报价单位评审内容 |  |  |  |  |  |
| 1 | 报价文件中有有效的法定代表人证明书原件，或由委托代理人签署的报价文件中有法定代表人授权书原件； |  |  |  |  |  |
| 2 | 报价人报价与用户需求书要求一致； |  |  |  |  |  |
| 3 | 报价按要求报价； |  |  |  |  |  |
| 4 | 报价文件按规定的格式填写，主要内容齐全，关键字迹清晰、容易辨认； |  |  |  |  |  |
| 5 | 报价总报价不超过报价限价48.5万元。 |  |  |  |  |  |
| 6 | 报价文件中没有建设单位无法接受的条件。 |  |  |  |  |  |
|  | 结论 |  |  |  |  |  |

注：1.凡符合以上各项条件，结论为有效，否则就为无效。

2.如对本表中某种情形的评审意见不一致时，以评审小组过半数成员的意见作为评审组对该情形的认定结论。

 **评委签名： 日期**

综合评分表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **评审因素** | **评分细则** | **分值****（分）** | **权重****（%）** |
| **一** | **技术商务部分（合计40分）** |
|  | 货物技术参数和性能指标 | 根据报价人所投设备对《第二章采购需求》“四、主要设备技术参数要求”中带“▲”号技术参数指标的响应情况进行打分，完全满足或正偏离询价文件要求得20分，每负偏离或不满足一条扣0.5分，扣完为止。备注：1、按照《第二章采购需求》“四、主要设备技术参数要求的要求提供相应证明文件，否则不得分。2、凡是标有序号的指标项即为一项单独的条款，无论是否隶属于上一级编号。 | 20分 | 20% |
|  | 系统整体设计方案 | 根据报价人提供的系统整体设计方案情况进行打分：方案完善、可靠、先进性、适用性、易维护性强，得10分；方案较完善、可靠、但先进性、适用性、易维护性一般，得7分；方案不够完善、可靠、先进性、适用性、易维护性一般，得4分；方案不够完善、可靠、先进性、适用性、易维护性差，得1分；未提供方案的不得分。 | 5分 | 5% |
|  | 供货实施方案 | 根据报价人的项目供货实施方案（包括人员安排，安全文明施工措施、工期安排、设备安装、调试、验收计划等）情况进行打分：方案具体，人员5人以上，可行性高的，得5分；方案比较具体，人员4-5人，可行性比较高的，得4分；方案比较具体，人员3人，但可行性一般的，得3分；方案具体程度一般，人员2人，可行性一般的，得2分；方案不够具体，人员1人，可行性较差，得1分；未提供方案的不得分。(本项人员需提供近半年社保证明。) | 5分 | 5% |
|  | 售后服务方案 | 根据报价人售后服务方案（包括售后服务流程、服务响应时效、技术支持、售后服务承诺等）进行评分：方案全面、具体、合理性高，得5分；方案较全面、较具体、合理性较高，得4分；方案较全面、较具体、合理性一般，得3分；方案不全面、不具体、合理性差，得1分；未提供方案不得分。 | 5分 | 5% |
|  | 设备制造厂商实力 | 报价人所投产品原厂商具有信息安全测评信息安全服务资质证书（安全工程类三级），需提供有效资质证明复印件，得1分；报价人所投产品原厂商具有涉密信息系统集成资质证书（甲级系统集成/软件开发运行维护）。需提供有效资质证明复印件，得1分；报价人所投产品原厂商具有《信息安全服务资质（一级信息系统安全运维服务）》；提供有效的资质证明复印件，得1分；报价人所投产品原厂商具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的CNNVD漏洞发现数不低于30个。提供自主挖掘CNNVD证书证明，得1分；报价人所投产品原厂商具有工业信息安全测试评估机构能力认证证书（二级）；提供有效的资质证明复印件，得1分； | 5分 | 5% |
| 二 | **价格部分（合计60分）** |
|  | 报价人报价 | 价格分应当采用低价优先法计算，即满足询价文件要求且报价价格最低的报价为评标基准价，其价格分为满分。其他报价人的价格分统一按照下列公式计算：报价人报价得分=(评标基准价／报价人报价)×100×权重备注：1. 因落实采购政策进行价格调整的，以调整后的价格计算评标基准价和报价,详见《价格扣除》。
2. 报价人报价得分四舍五入后，小数点后保留两位有效数。
 | 60分 | 60% |
| **合计** | **100分** | **100%** |

**第四章 报价文件参考格式**

**法定代表人证明书**

同志，现任我单位 职务，为法定代表人，特此证明。

有效日期： 签发日期：

单位： （公章）

附：代表人性别：\_\_\_\_\_\_年龄：\_\_\_\_\_\_身份证号码：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

营业执照号码：

法定代表人身份证复印件

**法人授权委托证明书**

致：广东省湛江汽车运输集团有限公司

本授权委托证明书宣告：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（报价人名称）\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（职务）\_\_\_\_\_\_\_\_\_\_（法定人代表姓名）合法地代表我单位，授权\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（职务）\_\_\_\_\_\_\_\_\_\_（姓名）为我单位代理人，该代理人有权在湛汽集团信息系统及网络安全等级保护项目（一期）报价活动中，以我单位的名义签署报价书，与贵司协商、签订合同协议书以及一切与此有关的事项。

代理人无转委权

报价人：（盖章）

法定代表人：（签字或印鉴）

授权代理人：（签字或印鉴）

日 期： 年 月 日

代理人身份证复印件

开标一览表(报价表)

项目名称：信息系统及网络安全等级保护项目（一期）

|  |  |  |  |
| --- | --- | --- | --- |
| **采购内容** | **数量** | **报价人报价****（人民币 元）** | **交货期** |
| 信息系统及网络安全等级保护项目（一期） | 1项 | 小写：大写： 增值税专用发票税率： % | 合同签订后 60 日历天内安装调试完毕并交付使用 |

报价人名称（单位盖公章）：

法定代表人或报价人授权代表（签名或盖个人名章）：

日期：

**说明：**

1. 中文大写金额用汉字，如壹、贰、叁、肆、伍、陆、柒、捌、玖、拾、佰、仟、万、亿、元、角、分、零、整（正）等。
2. 除询价文件另有规定外，报价文件内不得含有任何对本报价进行价格折扣的说明或资料，否则为无效报价。
3. 报价人报价的小数点后保留2位有效数。

报价分项报价表

项目名称：信息系统及网络安全等级保护项目（一期）

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 品牌 | 规格 | 型号 | 制造商（生产者） | 原产地 | 单位 | 数量 | 单价（人民币元） | 合计（人民币 元） | 备注 |
| 1 |  |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |  |  |  |  |  |
| **总计** | 小写：RMB大写： 增值税专用发票税率： % |

报价人名称（单位盖公章）：

法定代表人或报价人授权代表（签名或盖个人名章）

日期：

说明：

1、对于有配件、耗材、选件和特殊工具的货物，还应填报报价货物配件、耗材、选件表和备件及特殊工具清单，注明品牌、型号、产地、功能、单价等内容，该表格式由报价人自行设计。

2、报价人按照上述要求分类报价，其目的是便于评标，但在任何情况下并不限制采购人以任何条款签订合同的权利。

报价人资格声明函

**广东省湛江汽车运输集团有限公司：**

关于贵公司年月日发布 信息系统及网络安全等级保护项目（一期） 项目（项目编号：DJBH-2021）的采购公告，本单位愿意参加报价，并声明：

1. 本单位具备以下条件：
2. 具有履行合同所必需的设备和专业技术能力；
3. 本单位（如前三年内有名称变更的，含变更前名称）参加采购活动前三年内，在经营活动中没有重大违法记录（重大违法记录是指没有因违法经营受到刑事处罚或责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚）；
4. 法律、行政法规规定的其他条件。
5. 本单位及附属机构，并非受托为本项目同一合同项下或者其中分项目的前期工作提供设计、编制规范、进行管理等服务的供应商。
6. 本单位没有为采购项目同一合同项下提供整体设计、规范编制或者项目管理、监理、检测等服务。
7. 我方承诺如与本项目同一合同项下其他报价人的单位负责人为同一人或者存在直接控股、管理关系的情形，同意按报价无效处理。

本单位承诺在本次询价采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我单位承担。

特此声明！

**说明：**

1. 本声明函必须提供且内容不得擅自删改，否则视为无效报价。
2. 本声明函如有虚假或与事实不符的，作**无效报价**处理。

报价人名称（单位盖公章）：

单位地址：

日期：

报价函

**广东省湛江汽车运输集团有限公司**

我方确认收到贵方 信息系统及网络安全等级保护项目（一期）采购货物及相关服务的询价文件（项目编号：DJBH-2021）， (报价人名称、地址)。作为报价人已正式授权《法定代表人授权委托书》中的授权代表或法定代表人为我方签名代表，签名代表在此声明并同意：

1. 我们愿意遵守询价文件的各项规定，自愿参加报价，并已清楚询价文件的要求及有关文件规定，并严格按照询价文件的规定履行全部责任和义务。
2. 我们同意本报价文件的报价有效期从提交报价文件的截止之日起**90日历日内有效**。
3. 我们承诺从本项目报价截止时间起，本报价始终有效且不予撤销已递交的报价文件。
4. 我们已经详细地阅读并完全明白了全部询价文件及附件，包括澄清（如有）及参考文件，我们完全理解本询价文件的要求，我们同意放弃对询价提出不明或误解的一切权力。
5. 我们同意提供采购人要求的有关报价的一切数据或资料。
6. 我们理解采购人并无义务必须接受最低报价的报价或其它任何报价，完全理解采购人拒绝迟到的任何报价和最低报价的报价不是被授予中选的唯一条件。
7. 如果我们未对询价文件全部要求作出实质性响应，则完全同意并接受按无效报价处理。
8. 我们证明提交的一切文件，无论是原件还是复印件均为准确、真实、有效、完整的，绝无任何虚假、伪造或者夸大。我们在此郑重承诺：在本次询价采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。
9. 如果我们提供的声明或承诺不真实，则完全同意认定为我司提供虚假材料，并同意作相应处理。
10. 我们是依法注册的法人，在法律、财务及运作上完全独立于本项目采购人和用户单位（如有）。
11. 与本报价有关的一切正式信函请寄：地址

报价人名称（单位盖公章）：

法定代表人或报价人授权代表（签名或盖个人名章）

日期

备注：报价函中承诺的报价有效期应当不少于询价文件中载明的报价有效期，其他内容不得擅自删改，否则视为无效报价。

  采购需求条款响应一览表

说明：

1. 报价人必须对应询价文件条款逐条应答并按要求填写下表。
2. 报价人响应描述：报价人按响应货物/服务实际数据填写。
3. 报价人应按询价文件要求附相关证明文件，如有任何一项不响应或不满足的视为负偏离。
4. 偏离情况说明：报价人根据报价人实际情况填写“正偏离”“完全响应”或“负偏离”。

项目名称：信息系统及网络安全等级保护项目（一期）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 询价文件条款描述 | 报价人响应描述 | 偏离情况说明 | 查阅/证明文件指引 |
| **（一）标注“★”的实质性条款** |
|  | 六★其他要求：本项目必须按网络安全等级二级的标准进行设计及实施（提供承诺函）。 |  |  |  |
| **（二）标注“▲”的重要条款（主要设备技术参数要求中“▲”的条款）** |
|  |  |  |  |  |
|  |  |  |  |  |
| … |  |  |  |  |
| **（三）其他条款（主要设备技术参数要求中非“▲”的条款）** |
|  |  |  |  |  |
|  |  |  |  |  |
| … |  |  |  |  |
| **（四）其他条款** |
|  | 五、设备要求 |  |  |  |
| 2 | 七、质保期及售后服务 |  |  |  |
| 3 | 八、安装与调试 |  |  |  |
| 4 | 九、采购项目交付或者实施的时间和地点 |  |  |  |
| 5 | 十、交付验收标准依次序对照适用标准 |  |  |  |
| 6 | 十一、设备验收要求 |  |  |  |
| 7 | 十二、培训要求 |  |  |  |
| 8 | 十三、付款及结算方式 |  |  |  |

报价人名称（单位盖公章）：

日期：

承诺函

关于贵公司年月日发布信息系统及网络安全等级保护项目（一期）（项目编号：DJBH-2021）的采购公告，本公司（企业）愿意参加报价，并承诺：

如我司中选，我司将严格按照询价文件要求按网络安全等级二级的标准进行设计及实施本项目。

特此承诺！

报价人名称（单位盖公章）：

法定代表人或报价人授权代表（签名或盖章）：

日期：

技术服务方案

**主要内容应包括但不限于以下内容（格式自定）：**

1. 系统整体设计方案；
2. 供货实施方案；
3. 售后服务方案；
4. 须采购人配合事项；
5. 报价人认为对报价有利的其他资料。

报价人名称（单位盖公章）：

日期：

售后服务情况表

项目名称：信息系统及网络安全等级保护项目（一期）

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **报价人承诺** | **备注** |
| 1 | 保修期内售后服务情况(可用附页和宣传材料) | 生产厂商售后服务情况： |  |
| 报价人售后服务情况： |  |
| 2 | 保修期后售后服务 |  |  |
| 3 | 培训方案（可用附页） |  |  |

报价人名称（单位盖公章）：

日期：

**第五章 合同格式**

**合同通用条款**

甲 方（采购人）：

电 话：

传 真：

住 所：

乙 方（中选人）：

电 话：

传 真：

住 所：

根据 信息系统及网络安全等级保护项目（一期） （项目编号：（DJBH-2021））的采购结果，按照《中华人民共和国政府采购法》及其实施条例、《中华人民共和国合同法》的规定，经双方协商，本着平等互利和诚实信用的原则，一致同意签订本合同如下。

1. **采购标的**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 商品名称 | 品牌、规格型号、配置（性能参数） | 产地 | 数量 | 单价(元) | 金额(元) |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 合计总额：￥ 元； 大写： 增值税专用发票税率： % |

合同总额包括乙方设计、安装、随机零配件、标配工具、运输保险、调试、培训、质保期服务、各项税费及合同实施过程中不可预见费用等项目相关的一切费用。

1. **合同金额**

合同金额为￥ 元；大写： 增值税专用发票税率： %

1. **设备要求**
2. 货物为原制造商制造的全新产品，整机无污染，无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可依常规安全合法使用。
3. 交付验收标准依次序对照适用标准为：①符合中华人民共和国国家安全质量标准、环保标准或行业标准；②符合询价文件和响应承诺中甲方认可的合理最佳配置、参数及各项要求；③货物来源国官方标准。
4. 进口产品必须具备原产地证明和商检局的检验证明及合法进货渠道证明（如适用）。
5. 货物为原厂商(制造商)未启封全新包装，具出厂合格证，序列号、包装箱号与出厂批号一致，并可追索查阅。
6. 乙方应将关键主机设备的用户手册、保修手册、有关单证资料及配备件、随机工具等交付给甲方，使用操作及安全须知等重要资料应附有中文说明。
7. **质量要求：**
8. 乙方须提供全新的货物（含零部件、配件等）表面无划伤、无碰撞痕迹，且权属清楚，不得侵害他人的知识产权。
9. 货物必须符合或优于国家（行业）标准，以及本项目询价文件的质量要求和技术指标与出厂标准。
10. 乙方须在本合同签订之日起 日内送交货物成品样品给甲方确认，在甲方出具样品确认书并封存成品样品外观尺寸后，乙方才能按样生产，并以此样品作为验收样品；每台货物上均应有产品质量检验合格标志。
11. 货物制造质量出现问题，乙方应负责三包（包修、包换、包退），费用由乙方负担，甲方有权到乙方生产场地检查货物质量和生产进度。
12. 货到现场后由于甲方保管不当造成的质量问题，乙方亦应负责修理，但费用由甲方负担。
13. **采购项目交付或者实施的时间和地点：**详见本次询价文件采购需求
14. **付款方式：**详见本次询价文件采购需求
15. **质保期及售后服务要求**
16. 本合同的质量保证期（简称“质保期”）为3年，质保期自货物最终验收合格之日起算，质保期内乙方对所供货物实行包修、包换、包退、包维护保养，期满后可同时提供终身 (免费/有偿) 维修保养服务。
17. 对甲方的服务通知，乙方在接报后1小时内响应，4小时内到达现场，48小时内处理完毕。若在48小时内仍未能有效解决，乙方须免费提供同档次的设备予甲方临时使用。
18. 3年质保期届满后，甲乙双方若签订安全维护服务合同，乙方同意收取的维护费不高于本合同总金额的8%，具体维护服务内容与标准以新签订的维护合同约定为准；或可根据甲方要求，将维护事项交给甲方提供的当地第三方公司代为维护，具体维护事项由乙方与第三方公司自行协议。
19. **安装与调试**

乙方必须依照询价文件的要求和报价文件的承诺，将设备、系统安装并调试至正常运行的最佳状态。

1. **验收标准**
2. 货物若有国家标准按照国家标准验收，若无国家标准按行业标准验收，为原制造商制造的全新产品，整机无污染，无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可依常规安全合法使用。
3. 货物为原厂商(制造商)未启封全新包装，具出厂合格证，序列号、包装箱号与出厂批号一致，并可追索查阅。所有随设备的附件必须齐全。
4. 乙方应将关键主机设备的用户手册、保修手册、有关单证资料及配备件、随机工具等交付给甲方，使用操作及安全须知等重要资料应附有中文说明。
5. 甲方组成验收小组按国家有关规定、规范进行验收，必要时邀请相关的专业人员或机构参与验收。因货物质量问题发生争议时，由本地质量技术监督部门鉴定。货物符合质量技术标准的，鉴定费由甲方承担；否则鉴定费由乙方承担。
6. **违约责任与赔偿损失**
7. 乙方交付的货物、工程/提供的服务不符合询价文件、报价文件或本合同规定的，甲方有权拒收，并且乙方须向甲方支付本合同总价5%的违约金。
8. 乙方未能按本合同规定的交货时间交付货物的/提供服务，从逾期之日起每日按本合同总价3‰的数额向甲方支付违约金；逾期15天以上（含15天）的，甲方有权终止合同，要求乙方支付违约金，并且给甲方造成的经济损失由乙方承担赔偿责任。
9. 甲方无正当理由拒收货物/接受服务，到期拒付货物/服务款项的，甲方向乙方偿付本合同总价的5%的违约金。甲方逾期付款，则每日按本合同总价的0.3‰向乙方偿付违约金。
10. 其它违约责任按《中华人民共和国合同法》处理。
11. **争议的解决**

合同执行过程中发生的任何争议，如双方不能通过友好协商解决，甲、乙双方一致同意向甲方所在地人民法院提起诉讼。

1. **不可抗力**

任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件结束后1日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并根据情况可部分或全部免于承担违约责任。

1. **税费**

在中国境内、外发生的与本合同执行有关的一切税费均由乙方负担。

1. **其它**
2. 本合同所有附件、询价文件、报价文件、中选通知书均为合同的有效组成部分，与本合同具有同等法律效力。
3. 在执行本合同的过程中，所有经双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分。
4. 如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。
5. 除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下的义务。
6. **合同生效**
7. 合同自甲乙双方法人代表或其授权代表签字盖章之日起生效。
8. 合同壹式份，其中甲乙双方各执份，采购代理机构执壹份。

甲方（盖章）： 乙方（盖章）：

代表： 代表：

签定地点：

签定日期： 年 月 日 签定日期： 年 月 日

开户名称：

银行账号：

开 户 行：