桐梓县人民医院网络安全等级保护建设

需求公示

供应商资格条件：

（一）一般资格要求：

满足《中华人民共和国政府采购法》第二十二条规定：

1、具有独立承担民事责任的能力：提供法人或其他组织的营业执照等证明文件（复印件加盖供应商单位公章）；

2、具有良好的商业信誉和健全的财务会计制度：提供经合法审计机构出具的2023年度或2024年度财务审计报告，财务审计报告包括资产负债表、利润表、现金流量表及财务报表附注，财务审计报告应盖有会计师事务所单位章和注册会计师的执业专用章。新成立不足一年的企业（2024年08月01日起，以营业执照成立时间为准），可提供2025年01月起至响应文件递交截止时间任意一个月基本开户银行出具的资信证明文件（复印件加盖供应商单位公章）；

3、具有履行合同所必需的设备和专业技术能力：提供履行合同所必需的设备和专业技术能力的承诺函（承诺函格式自拟，加盖供应商单位公章）；

4、具有依法缴纳税收和社会保障资金的良好记录：提供依法缴纳税收（提供2025年01月01日至响应文件递交截止时间前任意一个月的纳税证明）和社会保障资金(提供2025年01月01日至响应文件递交截止时间前任意一个月的社会保障资金缴纳证明)的相关材料（复印件加盖供应商单位公章）；（注：无需缴纳税收的供应商须提供税务单位开具的无欠税证明）

5、参加本次政府采购活动前三年内，在经营活动中没有重大违法记录：提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明(格式文件详见响应文件格式)；

6、本项目 是 专门面向中小企业采购，若项目的承接企业是中小企业，请供应商按照《政府采购促进中小企业发展管理办法》(财库〔2020〕46 号）出具规定的《中小企业声明函》。声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。本项目所属行业为软件和信息技术服务业。

7、法律、行政法规规定的其他条件：

（1） 供应商须承诺：在“信用中国”网 站（www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn) 等渠道查询中未被列入失信被执行人名单、重大税收违法失信主体、政府采购严重违法失信行为记录名单中，如被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单中的供应商取消其竞标资格，并承担由此造成的一切法律责任及后果。

（2）根据《省发展改革委省法院省公共资源交易中心关于推进全省公共资源交易领域对法院失信被执行人实施信用联合惩戒的通知》黔发改财金(2020)421 号文件要求，采购人或代理机构在递交响应文件截止时间后现场根据贵州信用联合惩戒平台反馈信息，查询供应商是否属于法院失信被执行人，如被列入取消其投标资格。

（二）落实政府采购政策需满足的资格要求：

1、依据《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的相关要求，供应商不得为“信用中国”网站中列入失信被执行人和重大税收违法案件当事人名单的供应商，不得为中国政府采购网政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商。

2、根据《财政部关于进一步加大政府采购支持中小企业力度的通知》（财库[2022]19号）的规定，提高小微企业价格扣除比例。对未预留份额专门面向中小企业采购的采购项目，面向小微企业价格扣除比例按/%顶格执行（本项目是专门面向中小微企业采购，不再执行价格扣除）。

3、根据《关于促进残疾人就业政府采购政策的通知》（财库[2017]141号）文件规定，符合条件的残疾人福利性单位等同于小微企业在投标中享受同等优惠，但须提供《残疾人福利性单位声明函》。注：残疾人福利性单位属于小微企业的，不重复享受政策。

4、根据《司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）文件规定，在政府采购活动中，监狱企业视同小型、微型企业，享受同等政策，但不重复享受。但须提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

（三）本项目的特定资格要求：无

服务内容

一、网络安全系统及设备技术要求

序号	名称	技术要求	数量
1	网络边界防火墙	1.网络吞吐性能≥4Gbps；每秒新建连接数≥3 万；最大并发连接数≥100 万；SSL VPN 最大并发用户数≥4000。具备不少于 3 年硬件质保、软件升级。 2.内存≥4GB；冗余电源；配置千兆电口≥8 个，万兆光口 SFP+≥2 个，配置 128G SSD 硬盘。 3.配置三年的防病毒特征库、IPS 特征库和 URL&应用识别库升级升级授权；支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 4.支持一对一、一对多和多对多等形式的 NAT。 5.支持网络病毒防护功能，预定义病毒库超过 100 万种，可识别异常病毒行为。（需提供产品功能截图证明） 6.支持不低于 1 万种 IPS 规则，同时支持在控制台界面通过攻击名称、危险等级、安全类型等条件查询 IPS 特征信息，支持用户自定义 IPS 规则。（需提供产品功能截图证明） 7.支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护、Smurf 攻击防护、Land 攻击防护、WinNuke 攻击防护等攻击类型。 8.可设置基于 IP 过滤条件设置黑名单，实现对特定报文进行快速过滤。 9.支持主机威胁统计和展示，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。 10.支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志。 11.支持与本地态势感知平台联动，将防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。（需提供产品功能截图证明及联动承诺函） 12.供应商出具对本项目售后服务不低于三年的《售后服务承诺函》（格式自拟）。	2 台
2	数据中心防火墙	1.产品网络层吞吐量≥20Gbps，应用层吞吐量≥8Gbps，最大七层并发连接数≥200 万，HTTP 新建连接数≥15 万，不少于 6 千兆电口+4 千兆光口+2 万兆光口 SFP+，128G SSD 硬盘。具备 3 年硬件质保、软件升级。 2.配置不少于 3 年的 防病毒特征库、IPS 特征库和 URL&应用库升级授权。 3.支持路由、透明、旁路、虚拟线模式等多种部署方式。 4.产品支持静态路由、策略路由和多播路由协议，并支持 BGP、RIP、OSPF 等动态路由协议；支持策略路由负载，基于服务、ISP 地址、	1 台

		应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法。 5.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；支持NAT会话保持，使相同源IP的数据包经过地址转换后为其转换的源IP地址相同。 6.产品支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke 等攻击类型。 7.支持防flood攻击功能，包括TCPflood、UDPflood、ICMPflood、HTTPflood、DNSflood等。（需提供产品功能截图证明） 8.支持不低于1万种IPS规则，同时支持在控制台界面通过攻击名称、危险等级、安全类型等条件查询IPS特征信息，支持用户自定义 IPS 规则。（需提供产品功能截图证明） 9.产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。 10.支持与本地态势感知平台联动，将防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。（需提供产品功能截图证明及联动承诺函） 11.供应商出具对本项目售后服务不低于三年的《售后服务承诺函》（格式自拟）。	
3	漏洞扫描系统	1.接口不少于6千兆电口+4千兆光口SFP，2个接口扩展插槽，内存大小≥8G，硬盘容量≥128GB SSD+ 1TB SATA，具备3年硬件质保、软件升级。 2.设备支持系统漏扫授权 IP 数≥1000，WEB 漏扫授权 URL 数≥200；性能指标：主机漏扫最大并发 IP 数≥300，WEB 漏扫最大并发 URL 数 ≥10。 3.支持同时开启全插件系统漏洞扫描、WEB 漏洞扫描、弱口令扫描、基线配置核查，扫描速度不低于1000ip/h。（需提供产品功能截图证明） 4.支持多种协议口令猜测，包括SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM、REDIS、SMTP等，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。（需提供产品功能截图证明） 5.支持全局风险统计功能，通过扇形图/条状图/标签/表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急 漏洞、风险资产清单等信息，并可查看详情。（需提供产品功能截图证明） 6.支持资产发现功能，可基于 IP 地址/IP 网段/IP 范围/URL 等方式进行资产发现扫描，支持 EXCEL 格式批量导入。 7.支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等。 8.产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描	1套

		和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表等；每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认。 9.供应商出具对本项目售后服务不低于三年的《售后服务承诺函》（格式自拟）。	
4	日志审计系统	1.配置不少于 6 千兆电口+2 千兆光口 SFP，配置单交流电源，可用存储量≥8TB，具备 3 年硬件质保、软件升级。 2.配置不少于 200 个主机审计许可授权，日志处理性能不少于 2500EPS。（需提供产品功能截图证明） 3.支持通过接入序列号控制接入设备的个数，主要支持网络设备、安全设备、操作系统、中间件、数据库等设备的日志接入，可以获取到设备的传输日志量，设备同步数据状态等信息；可供多台设备同时接入同步数据，并实时分析展示。 4.支持多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持日志进行定时刷新。 5.支持以标准 syslog 等形式接收第三方设备的日志并存储；支持 FTP、Webservice、JDBC 的日志数据拉取接入方式；支持通过 agent、wmi 接口采集 windows 日志；支持对常见安全设备日志范式解析。 6.支持正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。 7.支持展示关联事件类型分布 TOP、对象 IP 统计 TOP、事件等级分布、事件趋势、事件列表；点击查看日志可自动跳转到日志检索。 8.内置主机安全报表（linux、windows，最好兼容国产操作系统如：欧拉、麒麟等）、数据库安全报表、网络设备安全报表、应用安全报表五种；支持导出日报、周报、月报。（需提供产品功能截图证明） 9.支持在数据存储时进行阈值设置，包括存储时间不能少于 180 天、使用容量告警、剩余容量告警、删除方式等设置。 10.支持国密算法，保障日志完整性，可以有效防止日志篡改等攻击行为。 11.支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。 12.供应商出具对本项目售后服务不低于三年的《售后服务承诺函》（格式自拟）。	1 套
5	数据库审计系统	1.设备配置≥6 千兆电口，≥2 个万兆光口，单交流电源，硬盘容量≥4T；设备吞吐量≥2Gbps，数据库流量≥500Mb/s，SQL 处理性 能≥30000 条 SQL/s，日志检索性能≥500000 条/秒；具备	1 套

		3年硬件质保、软件升级。 2.采用B/S管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务。 3.支持主流数据库：Oracle、SQLserver、MySQL、DB2、MariaDB、SyBase、Informix、PostgreSQL、TeraData、Cache、HANA 等；支持国产数据库：达梦（DM6、DM7）、人大金仓（Kingbase）、南大通用（GBase8a）、神通（Oscar）等。（需提供产品功能截图证明） 4.支持非关系型数据库：Redis、MongoDB、Hive、HBaseJavaAPI、kafka、ElasticSearchHttp、ElasticSearchJavaAPI 等。 5.支持日志模糊化处理，保护访问数据安全，防止数据二次泄密。 6.支持审计访问数据库的时间，源/目的IP，源/目的端口，源/目的mac，资源账号，数据库名，规则名称，表名，命令，SQL语句、级别，响应时间、错误码，影响行数，连接方式，客户端程序名，模式名，客户端用户，SQL执行结果。（需提供产品功能截图证明） 7.支持基于网络流量的资产发现功能，能够发现数据库表和资源账号，其中数据库表的自动发现支持表名、数据库名、发现次数和发现日期，资源账号自动发现支持在线天数、首次发现日期、末次发现日期。 8.支持监控已添加的 Agent 的运行情况，包括：编号、名称、部署位置、监控的 IP、操作系统类型、占用的 CPU 资源、占用的内存资源、运行状态。（需提供产品功能截图证明） 9.支持对针对数据库的SQL注入、CVE高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。 10.供应商出具对本项目售后服务不低于三年的《售后服务承诺函》（格式自拟）。	
6	终端安全管理系统	1.产品以纯软件交付，包含管理控制中心软件及终端客户端软件；PC授权不少于550套、服务器授权不少于150套；具备不少于3年软件及病毒库升级服务。 2.具备多维度的态势展示，内容至少包括威胁告警统计、攻击阶段统计、威胁等级统计、漏洞信息 Top、终端威胁告警 Top、敏感信息 Top、敏感终端 Top、最新告警事件、威胁态势评分等信息。（需提供产品功能截图证明） 3.具备对全网终端资产进行统一管理和资产画像能力：可提供智能化分析，实现单个终端与全网终端的风险解读，直观展示终端资产的综合健康状态，并为用户提供合理的优化策略与处置建议。 4.具备资产清点能力，至少包括数据库、中间件、环境变量、内核模块、共享目录、Web 应用、Web 站点、安装包、证书等资产信息。 5.具备资产运维和资产发现能力：可对终端资产进行关闭、重启、	1套

		锁屏、结束进程、断开网络、远程协助等操作，同时可通过 ARP、PING、NMAP 三种方式对非法接入的终端资产进行探测，发现未安装客户端的终端资产。（需提供产品功能截图证明） 6.对外设 USB 设备的读写功能进行管控。（需提供产品功能截图证明） 7.具备对端口、进程、网络、文件等多方面的管控能力，并具备剧本式的全网自动响应能力，可根据告警事件类型编排响应动作、响应时间等。产品需支持与同品牌防火墙设备深度联动实现应用准入控制，仅允许安装客户端且合规的终端访问受保护资源，对未装客户端用户提供浏览器友好引导自助安装，并对不合规终端实施访问阻断。 8.具备病毒查杀能力，可自行选择查杀效率、查杀位置、查杀引擎、处置方式等，并且应直观展示已处理和未处理的病毒数量，展示内容应至少包括已处理/未处理的全病毒数量、已处理/未处理的勒索病毒数量、已处理/未处理的挖矿病毒数量、已处理/未处理的蠕虫病毒数量；同时，针对 Windows 系统，产品应具备勒索病毒专项防护能力，包括勒索诱捕、文件保险箱、数据备份等，实时检测勒索病毒，防止勒索病毒入侵。（需提供产品功能截图证明） 9.需注意事项：采购人现用电脑多为 i5-10 代，内存 8G，Windows7 操作系统，投标人需保证软件安装后不影响业务系统正常使用。 10.供应商出具对本项目售后服务不低于三年的《售后服务承诺函》（格式自拟）。	
7	安全隔离与信息交换系统（双向网闸）	1.设备吞吐量≥500Mbps，最大并发连接数≥10 万；主机配置≥6 个千兆电口；具备 3 年硬件质保、软件升级。 2.采用“2+1”系统架构，即由两个主机系统和一个隔离交换模块组成；隔离交换模块基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为断开状态。 3.内、外网主机分别具备三系统，即系统 A、系统 B 和备份系统。支持在 WEB 界面上配置启动顺序，在 A 系统发生故障时，可以切换到 B 系统；支持将当前运行系统备份。（需提供产品功能截图证明） 4.支持文件交换容错和告警功能，交换出错能够自动重传，出现异常能够告警提示并记录日志。 5.支持 TCP 应用层数据单向传输的控制，保证 TCP 应用数据的 0 反馈，以满足二次防护对数据传输的安全性需求。 6.支持 URL 地址过滤，并可限制网页中的 Script 脚本、ActiveX 脚本、java applet 等。 7.内/外网主机系统分别具有独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等。 8.供应商出具对本项目售后服务不低于三年的《售后服务承诺函》（格式自拟）。	1 套

8	原有安全产品特征库升级服务	对医院现状所具有的安全产品（3 台防火墙、1 套上网行为管理、1 台网闸、1 套态势感知平台、1 台 VPN 设备）进行病毒特征库和产品软件提供不少于 3 年升级服务，升级的病毒特征库必须是最新版本。	/
9	设备安装调试、系统集成及售后等技术服务	1.根据等保系统建设需求提供所要的辅助材料，对整个等级保护系统的原有设备、新增设备按照标准整体安装调试、系统集成等服务，按照等级保护三级 2.0 建设标准实施，且配合好等级保护三级 2.0 测评工作。 2.项目实施中机房内不能任意断电和断网，如确需断电和断网，需在晚上 12 点后实施，且每次断电断网的时间不能超过 2 小时，断电断网后所产生的服务器和其他硬件设备及软件业务系统不能正常启动和运行，成交供应商需承担包括维修等费用在内的全部责任。 3.在等保测评时，成交供应商至少派遣具有资质的 2 名工程师现场全程配合测评机构整体测评，并提供测评所需的技术整改服务及按采购人要求配合资料编制服务。 4.项目实施完毕后，须按国家规定的项目建设规范资料要求提供项目实施整体过程资料、竣工资料、各产品使用手册、网络安全重要防控手册等全套资料。 5.提供不低于 3 年×7×24 小时线上、现场技术响应服务，当采购人提出技术服务需求时，10 分钟线上响应、2 小时现场响应，技术服务内容包含但不限于故障修复、设备维修、策略调整、设备重新部署等。 注：以上全部服务内容须提供《服务承诺函》并加盖投标人公章。	1 项

二、安全托管服务

2.1 本项目针对医院的核心系统设备进行安全托管服务，项目涉及的安全托管服务服务资产数≥20 个，设备质保期三年内免费安全托管，设备维保到期后再另行采购；

2.2 要求供应商对服务范围内的资产提供安全事件损失理赔承诺/网络安全保险服务，即在正常服务过程中因供应商的服务缺陷导致采购人服务范围内的资产遭受安全事件时，采购人有权要求供应商赔偿该事件直接造成的营业中断、数据恢复、第三者责任、应急响应、网络勒索损失，要求累计赔付金额不得低于 20 万元人民币。

2.3.安全托管服务技术要求

服务细项	内容及要求
资产盘点	按半年一次进行定期清点资产内容包含托管运营范围内资产的类型、支持操作系统、IP 地址、端口、位置、描述、资产管理人等信息清点。
互联网资产梳理	每季度提供 20 个 IP 或域名（含二级域名）的互联网资产梳理服务，服务内容包括：通过主动探测发现与梳理暴露于互联网侧的 IP、域名、

	操作系统、开放端口、服务、站点、中间件、应用、未授权访问等资产信息，并对资产指纹中存在的高危漏洞进行 POC 验证测试，发现存在的安全隐患，出具《资产梳理报告》并通过邮件方式发送。
脆弱性风险发现	按季度对托管范围内的资产进行系统安全风险脆弱性安全检测，提供 1 次 254 个 IP 地址的脆弱性风险数据分析评估。出具《脆弱性安全检测报告》。
弱口令监测	按季度基于流量探针评估弱口令对网络系统的安全风险，包括攻击者可能利用弱口令进行的攻击行为、对系统的影响范围和严重程度等。
安全威胁监测与分析	对 20 个资产内采集的安全数据进行通过告警降噪、关联分析、威胁建模等能力，利用专家经验及 AI 算法，对采集到的日志深入分析、捞捕，识别并监测潜在的网络攻击、安全入侵、异常行为等安全风险，7*24 小时远程安全威胁监测。通过微信服务群或电话方式进行安全威胁监测通告，以邮件方式按月周期发送运营报告。
安全事件快速响应处置	供通过日志与流量威胁分析监测，以发现可能的安全事件和异常情况；当检测到安全事件或异常情况时，立即进行分析研判，确定事件的性质、影响范围和严重程度。
	对事件进行详细记录和分析，通过图文方式进行系统性的描述，形成完整的事件报告，提交至用户，以便进行决策和改进，输出《事件分析与处置报告》。

第二节 商务要求

一、服务期及服务地点

服务期：3年。

服务地点：桐梓县人民医院（具体以采购人指定地点为准）。

二、验收标准、规范及方式

满足采购人及主管部门验收要求。

三、付款方式

签订合同后项目实施完成支付成交价的30%，整个等级保护系统的原有设备、新增设备按照标准整体安装调试、系统集成后支付成交价的30%，通过三级等保2.0测评后支付成交价的30%，剩余10%按照合同签订时间2年内系统运行正常一次性支付。

四、履约保证金

本项目不要求

五、磋商有效期

90日历天

六、其他要求

1、采购人保留对成交供应商响应文件复核的权利，成交供应商所提供的佐证材料若有不符，则成交人自行承担由此导致的与本项目有关的任何损失及法律责任。

2、在合同有效期内不受市场价格变化因素的影响调整价格，如果不能达成共识，可终止本项目续签。

3、供应商须承诺：

（1）供应商须承诺成交后：采购人对采购的系统运行服务质量进行全过程监督，成交供应商日常工作不到位、不达标、或有违约现象，将依据合同约定，做出相应的违约处理与处罚。

（2）供应商须承诺服务人员在岗履行工作职责期间，发生自身的人身伤害、伤亡，均由成交供应商负责处理并承担经济和道义上的责任，采购人不承担任何责任。

（3）供应商人须承诺成交后如违反国家相关法规，与服务人员发生纠纷，均由成交供应商负责调解与处理，采购人不承担责任。

本项目采用综合评分法进行评审。

无效标条款

供应商所提交的响应文件有下列情况之一的，按无效投标处理：

（1）递交的响应文件未在规定时间解密成功或未按采购文件要求签署、盖章的；

注：但不得因签章地方的当前页面签章位置偏移，作无效标依据。

（2）供应商不符合采购文件规定的资格要求的；

（3）项目接受联合体投标时，投标联合体未提交联合投标协议的；

（4）任何一轮报价经磋商小组认定低于成本价的；

（5）响应文件未对采购文件的实质性要求和条件作出响应的；

（6）响应文件中含义不明确、同类问题表述不一致或者有明显文件和计算错误的内容，经磋商小组认定影响响应文件响应的；

（7）投标报价超过采购文件规定的预算金额（最高限价）的；

（8）响应文件含有采购人不能接受的附加条件的；

（9）供应商有串通投标、弄虚作假、行贿等违法行为的；

（10）有下列情形之一的，视为供应商串通投标，其投标无效：

1.不同供应商的响应文件由同一单位或者个人编制；

2.不同供应商委托同一单位或者个人办理投标事宜；

3.不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；

4.不同供应商的响应文件异常一致或者投标报价呈规律性差异；

5.不同供应商的响应文件相互混装；

6.不同供应商的投标保证金从同一单位或者个人的账户转出。

（11）投标有效期不满足采购文件要求的；

（12）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，参加同一合同项下的政府采购活动的；

（13）违反政府采购法律法规，足以导致响应文件无效的情形。

注：不得因文件排序等非实质性的格式、形式问题限制和影响供应商投标（响应）。

废标条款

在项目采购中，出现下列情形之一的，应予废标：

1、出现影响采购公正的违法、违规行为的；

2、供应商的报价均超过了最高限价；

3、因重大变故，采购任务取消的；

4、国家法律法规规定的其它情形。

废标后，采购人和采购代理机构应当将废标理由通知所有供应商。