



# 云南驰宏资源综合利用有限公司 (护网行动)网络安全加固及网络故障恢复服务比价公示函

尊敬的客户：

云南驰宏资源综合利用有限公司（以下简称“驰宏综合利用”）根据公司各类信息资产及业务系统安全需要，将在中国铜业有限公司阳光采购平台面向社会对公司护网行动服务项目进行公开比价，诚邀广大有合作意向的客户前来咨询并参与竞价，现将相关事宜公告如下：

## 一、项目内容：

（一）项目名称：驰宏综合利用(护网行动)网络安全加固及网络故障恢复服务。

## （二）项目要求

确保公司各类信息资产及业务系统的网络安全，全面排查重要网络与核心业务系统的互联网暴露面、系统脆弱性等安全隐患，通过专业化技术手段完善网络安全防护措施、提升系统技术防护能力，保障公司正常生产经营秩序，提升公司网络安全防护保障能力。满足《中华人民共和国网络安全法》等级保护 2.0 等相关法规要求,提供针对性的驻场维护服务。

## （三）项目范围

驰宏综合利用(护网行动)网络安全加固及网络故障恢复服务主要包含两部分内容，一为网络安全托管服务，主要包括对互联网核心资产及业务系统进行全面深入的风险隐患排查，对不满足合规性的基础网络、机房、信息系统及工控系统问题进行整改，提供 7\*24 小时“人机共智”的安全托管服务，及时提供策略检查及配合开展应急演练、互联网全量资产梳理、互联网安全检测、全资产脆弱性识别和管理、渗透测试、安全加固、AI 软件导致的资产横向攻击行为的检测和防护，统一端点安全管理系统的防护、人员安全引导系统（对互联网开放）、视频抓违章后期系统引入等全量核心资产的护网值守、应急响应服务及检查（检测、监测），发现问题及时处置（如处置问题需要额外物资与甲方另行沟通商定）；二为护网监测现场值守。

（四）服务期限：2 年。

## 二、报价人资质要求：

1.报价人须具有在中华人民共和国正式注册的独立法人，具有有效的营业执照（三证合一），证照须完整齐全；营业执照经营范围中应包含计算机软硬件的技术服务或者信息系统运行维护服务。



2.未列入中国铝业集团有限公司、中国铜业有限公司、云南驰宏锌锗股份有限公司现行合格承包商清单。

3.业绩要求：报价人须提供 2023 年至今至少完成过 1 个网络安全服务类似项目业绩（提供中选通知书或合同或业主证明材料）。

4、技术要求：提供专业的运行维护团队，维护平台需与原品牌防火墙及 EDR 等网络防护设备实现无缝对接，提供 7\*24 小时互联网安全监测并实时推送报告，提供原厂授权并加盖厂商公章。

5.信誉要求：根据《关于对失信被执行人实施联合惩戒的合作备忘录》及《关于在招投标活动中对失信被执行人实施联合惩戒的通知》精神，未被列入最高人民法院官网中“全国法院失信被执行人名单信息公布与查询”及“信用中国”的失信被执行人，并提供相关查询资料。

6.报价满足比选文件要求。

7.响应时间：提供 365\*24 小时维护服务，接到采购人通知后 2 小时内达到现场。

### 三、密封报价文件要求、递交时间及地点：

1.具体内容详见比选文件，比选文件详见附件一。

2.报价人需提供纸质版报价文件,及与其对应的电子版报价文件，且密封完好。

3.递交时间：2026 年 5 月 7 日 13:00 前，逾期无效。

4.递交地点：邮寄或现场投递至云南驰宏资源综合利用有限公司装备部（办公大楼二楼）。

若邮寄请在快递单上备注：驰宏综合利用(护网行动)网络安全加固及网络故障恢复服务报价文件）。

### 四、联系方式

比选人：云南驰宏资源综合利用有限公司

联系人：徐宗旺 联系电话：17806915335

驰宏锌锗纪委举报电话：0874-8966630

驰宏锌锗纪委举报邮箱：chxzjw@chxz.com

云南驰宏资源综合利用有限公司

2026 年 4 月 30 日



附件一

云南驰宏资源综合利用有限公司  
(护网行动)网络安全加固及网络故障恢复服务

# 比选文件

比选人：云南驰宏资源综合利用有限公司

2026年4月30日



# 目录

第一章 报价要求	5
第二章 比选办法	15
第三章 技术规格书	21
第四章 比选文件格式	29
一、报价函	29
二、法定代表人授权书	30
三、报价一览表	31
四、报价人基本情况表	32
五、拟投入项目人员汇总表	33
六、主要人员资历表	34
七、资格证明材料	35
八、质量承诺及保证措施	36
九、响应时间承诺和保证措施	37
十、网络及信息安全保障服务方案；	37
十一、服务要求及服务响应方案	37
十二、安全底线承诺书	38
十三、中铝集团比价自律公约	39



# 第一章 报价要求

驰宏综合利用(护网行动)网络安全加固及网络故障恢复服务现已具备条件，现邀请具备相应资质和能力的单位参加本项目密封报价。

## 一、项目内容：

(一) 项目名称：云南驰宏资源综合利用有限公司(护网行动)网络安全加固及网络故障恢复服务。

### (二) 项目要求

确保公司各类信息资产及业务系统的网络安全，全面排查重要网络与核心业务系统的互联网暴露面、系统脆弱性等安全隐患，通过专业化技术手段完善网络安全防护措施、提升系统技术防护能力，保障公司正常生产经营秩序，提升公司网络安全防护保障能力。满足《中华人民共和国网络安全法》等级保护 2.0 等相关法规要求，提供针对性的驻场维护服务。

### (三) 项目范围

驰宏综合利用(护网行动)网络安全加固及网络故障恢复服务主要包含两部分内容，一为网络安全托管服务，主要包括互联网核心资产及业务系统进行全面深入的风险隐患排查，对不满足合规性的基础网络、机房、信息系统及工控系统问题进行整改，提供 7\*24 小时“人机共智”的安全托管服务，及时提供策略检查及配合开展应急演练、互联网全量资产梳理、互联网安全检测、全资产脆弱性识别和管理、渗透测试、安全加固、AI 软件导致的资产横向攻击行为的检测和防护，统一端点安全管理系统的防护、人员安全引导系统（对互联网开放）、视频抓违章后期系统引入等全量核心资产的护网值守、应急响应服务及检查（检测、监测），发现问题及时处置（如处置问题需要额外物资与甲方另行沟通商定）；二为护网监测现场值守。

具体服务内容如下：



网络安全托管服务：			
序号	服务类别	服务内容	数量
1	策略检查及应急演练	<p>1、上线前策略检查：上线前安全专家对安全组件上的安全策略进行统一检查，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果</p> <p>2、完善应急预案：针对专网不同类别应用系统失陷，建立演习应急处置预案及操作手册。</p> <p>2、开展应急演练：结合应急预案，开展桌面推演和现场演练，检验应急流程、应急措施和协同处置的有效性。</p> <p>3、一键断网应急演练：开展一键断网应急演练，强化应急处置流程。</p> <p>4、人员安排：需安排专业工程师及网络安全专家至少 2 人现场共同完成，每半年一次</p>	2 次
2	互联网暴露面资产梳理	<p>1、梳理驰宏资源现有的全量互联网暴露面资产，包括近 400 台终端 IP、办公网、环保在线监测系统、视频监控网（全厂 1000 多个摄像头）、应援布控系统、供电系统、P2P 网络、MES(DCS)网络、语音通讯网、新材料厂计量专网等驰宏资源全量资产。</p> <p>2、通过利用资产测绘工具，排查互联网侧是否存在未记录在案的相关互联网暴露面资产。</p> <p>3、建立互联网资产台账，包括内外网 IP 地址、端口、域名等信息，明确资产归属和资产责任人。</p> <p>4、人员安排：需安排专业工程师及网络安全专家至少 2 人现场共同完成，每季度一次。</p>	4 次
3	互联网资产安全检测	<p>1、漏洞扫描：对驰宏资源 MES（DS）内网资产和公网映射进行漏洞扫描，发现操作系统、数据库、中间件、网络设备、网络安全设备中存在的安全漏洞，出具漏洞扫描分析报告和整改建议。</p> <p>2、渗透测试：对全量互联网资产开展深度渗透测</p>	4 次



		<p>试，检验应用系统健壮性、访问控制有效性、安全设备敏感性。</p> <p>3、人员安排：需安排专业工程师及网络安全专家至少2人每季度一次现场完成+提供云端7*24小时资产监测服务</p>	
4	内网资产梳理	<p>1、梳理并及时发现驰宏资源全量包括IT资产及其动态变化，包括：域名（含子域）、IP、站点防护设备、主机操作系统、服务和端口、网站应用容器、应用服务组件等。</p> <p>2、持续服务过程中安全专家定期对资产进行存活性探测，当发现未存活资产或资产发生变更时，安全专家对变更信息确认与更新，确保深信服安全运营中心中资产信息的准确性和全面性。</p> <p>3、服务方式：需提供专业工程师及网络安全专家至少2人每季度一次梳理服务+云端7*24小时探测服务</p>	4次
5	脆弱性识别	<p>一、攻击路径分析服务，针对驰宏资源全量：</p> <p>1.检查是否根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段。</p> <p>2.检查是否将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；</p> <p>3.检查是否在网络各个边界处部署了访问控制技术措施，如部署网闸、防火墙或ACL等。</p> <p>4.检查是否应能够对非授权设备私自联到内部网络的行为进行检查，准确确定出位置，并对其进行有效阻断；</p> <p>5.检查是否部署终端管理软件或采取其它技术手段防止非法外联行为；</p> <p>6.检查是否在网络边界处部署恶意代码防范技术措施，是否启用了检测和阻断功能；</p> <p>7.检查在网络边界处是否有对网络攻击进行检测的相</p>	全年7*24小时



	<p>关措施；</p> <p>8. 访谈管理员并查看网络拓扑图，系统是否采用冗余技术设计网络拓扑结构；</p> <p>9. 访谈管理员并查看网络拓扑图，系统是否有主要网络设备、通信线路和数据处理系统的硬件冗余等；</p> <p>二、敏感信息排查服务，针对驰宏资源全量：</p> <p>1. 暗网情报监控：监控暗网中与客户相关的敏感数据泄露、名男文件泄露等情报，及时告警并协助处置。</p> <p>2. 代码泄露监控：覆盖主流国内外代码托管平台（如github、GitLab、BitBucket、码云等），为客户发现并阻断代码泄露风险。</p> <p>3. 敏感文件监控：监控主流网盘（如百度网盘、115网盘等）、文库（百度文库、道客巴巴等）等文件共享平台，帮助客户管控机密文件外泄风险。</p> <p>4. 资产失陷监控：依托深信服威胁情报能力，为客户提供互联网暴露资产隐患排查。</p> <p>5. 高危漏洞监控：依托专业漏洞团队收集最新爆出的高危漏洞信息（危害、影响范围、修复建议等）并及时预警。</p> <p>三、漏洞扫描服务</p> <p>1. 本地扫描：是指经过用户授权后，扫描人员达到用户工作现场，根据用户的扫描目标直接接入到用户的办公网络或业务网络中。这种扫描的好处就在于免去了扫描人员从外部绕过防火墙、入侵保护等安全设备的工作。一般用于检测内部服务器地址的威胁源或路径。</p> <p>2. 互联网扫描：与本地扫描相反，扫描人员无需到达客户下场，直接从互联网访问用户的某个接入到互联网的系统并进行扫描即可。这种扫描往往是应用于那些关注互联网开放服务的用户，主要用于检测互联网</p>	
--	---	--



		开放服务的威胁源或路径	
6	基线核查服务	<p>基线核查服务</p> <p>1.人工检查主要包括登录信息收集、配置安全分析和形成检查报告。其中配置安全分析是比较重要的环节，分析结果直接影响报告的准确性、权威性；</p> <p>2.自动化检查是借助深信服的基线核查系统（BVT）或专门开发的检查脚本来自动化完成部分工作。自动化工具主要自动化完成目标设备登录、设备配置检查和配置信息记录工作，此部分工作借助自动化工具是为了消除手工误操作的隐患，提高检查效率和精确度；</p> <p>服务方式：</p> <p>1、针对服务资产的系统漏洞和 Web 漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。</p> <p>2、漏洞修复优先级排序与通告：基于漏洞扫描结果、资产重要性及漏洞的威胁情报，对漏洞进行重要性排序，确定修复的优先级；并将最终结果通告给用户。</p> <p>3、漏洞可落地修复方案：对漏洞进行分析并输出可落地的修复方案，通过工单系统跟踪修复情况。</p> <p>4、漏洞复测与状态追踪：对修复的漏洞进行复测，及时更新漏洞工单的漏洞修复状态。</p> <p>5、弱口令分析与管理：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、</p>	每 2 个月一次 现场共同完成+ 云端 7*24 小时 监测服务



		<p>smtp、VNC、ftp、telnet、ssh、mysql、tomcat 等。针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测。并将检测发现的问题通过工单系统跟踪修复状态。”</p> <p>6、最新漏洞通告与排查：实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行通告与排查。通告信息中包含最新漏洞信息、服务资产受影响情况。</p> <p>7、最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，修复方案以及临时规避措施。</p> <p>8、最新漏洞复测与状态跟踪：由安全专家对该最新漏洞建立工单进行持续跟踪。</p> <p>9、人员安排：需提供专业工程师及网络安全专家至少 3 人每 2 个月一次现场共同完成+云端 7*24 小时监测服务</p>	
7	渗透测试服务	<p>1.现场与远程测试</p> <p>现场测试是指经过用户授权后，测试人员到达用户工作现场，根据用户的期望测试的目标直接接入到用户的办公网络甚至业务网络中。这种测试的好处就在于免去了测试人员从外部绕过防火墙、入侵保护等安全设备的工作。一般用于检测内部威胁源和路径。</p> <p>远程测试与现场测试相反，测试人员无需到达客户现场，直接从互联网访问用户的某个接入到互联网的系统并进行测试即可。这种测试往往是应用于那些关注门户站点的用户，主要用于检测外部威胁源和路径。</p> <p>2.黑盒白盒测试</p> <p>黑盒测试是指测试人员对除目标系统的 IP 或域名以外的信息一无所知的情况下对系统发起的测试工作，这种方式可以较好的模拟黑客行为，了解外部恶意用户可能对系统带来的威胁。</p>	6 次



		<p>白盒测试则是指测试人员通过用户授权获取了部分信息的情况下进行的测试，如：目标系统的帐号、配置甚至源代码。这种情况用户模拟并检测内部的恶意用户可能为系统带来的威胁。</p> <p>3.服务方式及人员安排：需提供专业工程师及网络安全专家至少 2 人每 2 个月一次远程做渗透测试，确保各种攻击源的应对办法</p>	
8	<p>安全设备巡检及安全加固</p>	<p>1.对云南驰宏资源综合利用有限公司安全设备（包括：深信服防火墙、深信服上网行为管理、深信服日志审计、思科核心交换机、汇聚交换机、迪讯信息网络核心服务器等）及各所属单位专线防火墙开展设备巡检。</p> <p>2.更新安全设备版本、规则库，确保安全设备的防护能力达到最优。</p> <p>3.对检测出的漏洞加固：针对互联网系统安全检测发现的风险，及时下发相关的责任人，监督、指导开展整改工作，对于风险较大且无法整改的系统，建议关停或采取访问限制措施。</p> <p>4.平台加固：对于设备巡检中发现的设备问题，及时组织设备厂商开展安全加固，且务必完成整改。</p> <p>5.服务方式及人员安排：需提供专业工程师及网络安全专家至少 2 人现场巡检及网络安全加固，每 2 个月一次。</p>	6 次



9	安全应急响应服务（网络攻击导致断网的网络恢复服务及常日网络安全核心设备故障的网络恢复服务）	<p>提供现场团队+原厂团队现场应急响应服务</p> <p>一、针对病毒攻击后的网络故障恢复服务 包括：对驰宏资源利用公司的主机安全数据进行分析、全方位监测发现的威胁和异常进行快速响应和处置，并针对安全事件进行深入调查和原因分析；同时输出事件响应处理报告，帮助速响应正确应对攻击入侵事件，降低安全事件带来的损失。</p> <p>服务方式：需提供专业的服务团队及网络安全专家现场服务，云端后台网络安全团队远程辅助</p>	60天
		<p>二、针对核心设备的日常网络故障恢复服务 服务方式：提供现场2小时应急响应服务能力。突发事件联络员全天候值班，安全服务管理职能部门负责人、与应急相关的其他部门负责人应急服务团队主管，取消休假，处于随时待命状态。</p> <p>2.服务方式：提供现场服务+云端后台网络安全团队远程辅助，所提供人员需具备网络专业技术水平至少2年以上维护经验，管理人员至少8年以上管理经验</p>	60天
10	护网监测值守	<p>一、网站安全监测：</p> <p>1.利用网站安全监测平台，对互联网系统开展7*24小时安全监测，包括可用性监测、网站篡改、挂马、黑链、敏感信息泄露等。</p> <p>二、互联网安全监测</p> <p>1.云端值守人员开展7*24小时互联网安全监测，及时发现、分析互联网侧的各类攻击事件，并开展处置。</p> <p>2、现场值守人员开展7*24小时互联网安全监测，及时发现、分析互联网侧的各类攻击事件，并开展处置。</p> <p>三、应急响应 针对突发安全事件，值守人员及时开展应急处置</p> <p>四、MSS重保值守</p>	全年7*24小时



		<p>以保障风险管控效果为目标，以 7*24h 持续在线守护为主线，以【资产、脆弱性、威胁、事件】四个核心安全风险要素为抓手，提升组织安全风险管控能力和安全工作效果，提供持续、有效、省心、便捷的网络安全运行维护服务。</p> <p>五、重大节假日重保值守</p> <p>重大节假日期间除“7*24 小时 MSS 值守外”的网络安全保障服务，MSS 处理不了的，提供专业人员至少 1 人现场解决，云端 7*24 小时监测服务</p> <p>六、服务方式及人员安排：</p> <p>针对驰宏资源的资产及业务系统进行网络安全保障服务及网络安全应急管理服务，以保障网络安全“持续有效”为目标，提供安全运营中心和网络安全专家服务团队，采用有效协同的“人机共智”模式，提供全天 7*24 小时实时网络安全监测、网络应急管理服务，发现问题第一时间应急处置，并时实发送处置报告</p>	
11	安全保障总结	<p>护网监测：安全专家每周总结阶段性安全运营情况并输出《日报、周报、月报、半年度总结、全年总结》报告，并向我单位定期总结汇报。</p> <p>安全运营年度汇报：安全专家总结年度安全运营情况并输出《年度总结报告》发送给我单位负责人进行总结汇报。</p> <p>用户 Portal：可视化 portal 支持随时查看服务范围内业务资产安全状态。支持在线展示所有脆弱性、威胁、事件工单的处置进程和结果支持用户在线对服务 SLA 进行查阅和监督。</p> <p>三、服务交付物</p> <p>《首次安全威胁分析报告》《漏洞举证报告》、《漏洞清单》、《应急响应报告》、《事件处置报告》、《威胁情报》、《安全运营周报》、《安全运营月报》、《半年度总结汇报》、《年度总结汇报》</p>	1 项



护网行动现场值守：			
序号	服务类别	服务内容	数量
1	护网值守（现场值守）	<p>一、护网期间网站安全监测：</p> <p>1.利用网站安全监测平台，对互联网系统开展 7*24 小时安全监测，包括可用性监测、网站篡改、挂马、黑链、敏感信息泄露等。</p> <p>2.护网期间分派 2 人现场值守，值守人员进行人工拨测，拨测周期为每两小时一次。</p> <p>二、互联网安全监测</p> <p>1.云端值守人员开展 7*24 小时互联网安全监测，及时发现、分析互联网侧的各类攻击事件，并开展处置。</p> <p>2.现场值守人员开展 7*24 小时互联网安全监测，及时发现、分析互联网侧的各类攻击事件，并开展处置</p> <p>三、服务方式及人员安排：需提供专业工程师及网络安全专家至少 2 人现场监测及值守</p>	60 天

（四）服务要求：

1、报价人所报服务需满足资产数量不少于 10 个（资产指服务器主机或虚拟机主机数）。

2、服务需结合安全工具发现的资产信息，对服务范围内的资产进行全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP 地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），建立资产台账，当资产发生变更时，安全专家对变更信息确认与更新。

3、需提供专业安全服务工程师采用专业安全工具，针对系统与 web 应用进行漏洞扫描、基线配置核查扫描、失陷主机分析、潜伏威胁分析等安全评估措施，综合评估安全现状。

4、需提供客观的修复优先级处置方案，不能以脆弱性危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度。（提供相关功能截图并加盖厂商公章）。

5、需对发现的脆弱性建立状态总览机制，持续跟踪脆弱性情况，清晰直观地展示脆弱性的修复情况，遗留情况以及脆弱性对比情况，使得采购方可做到脆弱性的可视、可管、可控。

6、需实时监测网络安全状态，对攻击事件生成工单，及时进行分析与预警。攻击事件包含



境外黑客攻击事件、暴力破解攻击事件、持续攻击事件（提供相关功能截图并加盖厂商公章，  
示当前安全事件的处置状态）。

7、基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置。

8、支持面向采购方的安全态势展示，展示出当前采购方遭受的威胁事件信息以及脆弱性信息统计，并支持服务专家按照资产类别、威胁类型进行定制化筛选查看，能直观感受到采购方当前的风险态势情况。

9、提供的服务平台支持面向采购方的安全报告与交付物管理，可生成、导出、下载各类安全报告，包括但不限于《安全服务值守日报》、《特殊时期值守报告》、《安全运营周报》、《安全运营月报》。（提供相关功能截图并加盖厂商公章）。

10、服务平台支持可导出报告，支持按照自定义模块进行导出，可自定义模块必须包括但不限于事件管理、攻击威胁（外部攻击趋势、TOP5 攻击 IP 等）、脆弱性管理（漏洞、弱密码）。

11、服务提供的服务平台支持的安全检测规则应超过 1000 个，且覆盖内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等。

12、支持服务厂商与单位现有防火墙、终端杀毒等安全设备进行联动，并每月对采购方的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平。采购方云端服务平台应当具备丰富的策略检查工具（要求不少于 40 种策略检查的工具），支持排查安全设备防护策略配置的合理性。（提供对接承诺函）

（五）服务期限：2 年。

## 二、报价人资质要求：

1. 报价人须具有在中华人民共和国正式注册的独立法人，具有有效的营业执照（三证合一），证照须完整齐全；营业执照经营范围中应包含计算机软硬件的技术服务或者信息系统运行维护服务。

2. 未列入中国铝业集团有限公司、中国铜业有限公司、云南驰宏锌锗股份有限公司现行的不合格承包商清单。

3. 业绩要求：报价人须提供 2023 年至今至少完成过 1 个网络安全服务类似项目业绩（提供中选通知书或合同或业主证明材料）。

4. 技术要求：提供专业的运行维护团队，维护平台需与原品牌防火墙及 EDR 等网络防护设



备实现无缝对接，提供 7\*24 小时互联网安全监测并实时推送报告，提供原厂承诺并加盖原厂公章。

5.信誉要求：根据《关于对失信被执行人实施联合惩戒的合作备忘录》及《关于在招投标活动中对失信被执行人实施联合惩戒的通知》精神，未被列入最高人民法院官网中“全国法院失信被执行人名单信息公布与查询”及“信用中国”的失信被执行人，并提供相关查询资料。

6.报价满足比选文件要求。

7.响应时间：提供 365\*24 小时维护服务，接到采购人通知后 4 小时内达到现场。

### 三、报价文件递交时间及地点：

1.递交时间：2026 年 5 月 7 日 13:00 前，逾期无效。

2.递交地点：驰宏综合利用装备部。

### 四、联系方式：

比选人：驰宏综合利用

联系人：徐宗旺 联系电话：17806915335

驰宏锌锗纪委举报电话：0874-8966630

驰宏锌锗纪委举报邮箱：chxzjw@chxz.com



## 第二章 比选办法

本次比选程序及选择成交单位的办法按以下内容执行。

### 1、评选机构

1.1 本办法参照《中华人民共和国比价投标法》，《中华人民共和国比价投标法实施条例》，七部委 12 号令《评选委员会和评选方法暂行规定》，《云南驰宏锌锗股份有限公司维修维护服务业务建设招投标管理实施细则》的有关规定制订。

1.2 比选人依法组建评选委员会，评选委员会成员人数为 5 人及以上单数。

### 2、比选纪律

2.1 评选委员会的成员应严格自律，自觉接受有关部门的监督。

2.2 比选过程中，评选委员会成员不得擅离职守，影响比选程序正常进行。

2.3 评选委员会的成员不得与报价人、其他利害关系人私下接触，不得向报价人、其他利害关系人泄露对报价文件的评审、比较，中选候选人的推荐以及与评审有关的其它情况。

2.4 比选过程中，不允许任何人把报价文件及其汇总材料带出评审会场，完成评选后所有材料如数交还。

2.5 比选过程中，非评选委员会的成员/工作人员不得随意进入比选会场。

2.6 与会人员违反上述规定对比选造成不良影响的，后果由责任者承担。

### 3、有下列情形之一的，不得担任评选委员会成员：

（一）报价人或者报价人主要负责人的近亲属；

（二）与报价人有经济利益关系，可能影响对比选公正评审的；

（三）曾因在比价、评选以及其他与比价报价有关活动中从事违法行为而受过行政处罚或刑事处罚的。

评选委员会成员有前款规定情形之一的，应当主动提出回避。

### 4、比选原则及纪律

4.1 比选遵循“客观、公正、科学、择优”的原则。

4.2 只对报价文件进行评选，报价文件以外的资料信息（除询标相关资料外）不作为评选的依据和参考。

4.3 评选委员会如有需询问、澄清问题时，由专职联络员负责联系报价人到场。



## 5、比价程序

### 5.1 响应性评审

条款号		评审因素	评审标准
5.1.1	响应性 评审标 准	营业执照及资质证书	报价人须具有在中华人民共和国正式注册的独立法人，具有有效的营业执照（三证合一），证照须完整齐全。营业执照经营范围中包含计算机软硬件的技术服务或者信息系统运行维护服务。
		承包商准入	未列入中国铝业集团有限公司、中国铜业有限公司、云南驰宏锌锗股份有限公司现行的不合格承包商清单。
		业绩要求	报价人须提供 2023 年至今完成过至少 1 个网络安全服务类似项目业绩（提供中选通知书或合同或业主证明材料）
		技术要求	提供专业的运行维护团队，维护平台需与原品牌防火墙及 EDR 等网络防护设备实现无缝对接，提供 7*24 小时互联网安全监测并实时推送报告，提供原厂授权并加盖厂商公章
		信誉要求	根据《关于对失信被执行人实施联合惩戒的合作备忘录》及《关于在招投标活动中对失信被执行人实施联合惩戒的通知》精神，未被列入最高人民法院官网中“全国法院失信被执行人名单信息公布与查询”及“信用中国”的失信被执行人，并提供相关查询资料。
		比选报价	比选报价满足比选文件。
		响应时间	提供 7*24 小时维护服务，接到采购人通知后 4 小时内达到现场。

注：对未通过响应性评审的报价人比价小组应通过相关的决议或在评选报告中说明情况。如果评选委员会根据本办法的规定否决不合格报价或者界定为废标后，有效报价人不足三个，评选委员会认为仍具备竞争性的，可进入下一阶段的评选。

### 5.2.综合评审

5.2.1 评选定标原则：本项目采用综合评分法进行评选，定标将依据评选委员会递交的推荐中选候选人顺序及其他规定确定中选人。



### 5.2.2 评选办法：

评选委员会根据拟定的评选办法对报价文件提出的质量承诺及保证措施、服务承诺和保证措施、报价人及企业业绩等及能否最大限度满足比选文件中规定的各项要求进行评定和打分，择优选定中选单位，具体评分办法如下：

总分（满分 100 分）=商务部分得分（满分 40 分）+技术部分得分（满分 60 分）。

#### 1)商务部分（满分 40 分）

此部分满分 40 分，按照以下原则进行计算分数：

本项目对报价人比选报价进行评分，比选报价与评选基准价相比，等于评选基准价时得 30 分（基准分）；比选报价每比评选基准价高 0.1 万元在基准分基础上扣 1 分、低 0.1 万元在基准分基础上加 1 分，不足 0.1 万元的部分按 0.1 万元计算，分数加满或扣完为止。评选指标价按以下公式计算：

公式三：（适用于当比选报价个数  $n \geq 3$  范围时）

$$P = \frac{t_1 + t_2 + \dots + t_n}{n}$$

其中：

- ①  $t_1$ 、 $t_2$ 、... $t_n$  指比选报价；
- ②  $n$  指报价个数。
- ③  $P$  评选基准价。

#### 2)技术部分（满分 60 分）

##### 质量承诺及保证措施评审评分（10 分）

第一个档次（8-10】分：质量承诺满足比选文件，能提供“信息安全质量管理体系认证证书”、质量保证措施严格按比选文件要求的施工技术规范、标准编制且针对性好的；

第二个档次（5-8】分：质量承诺满足比选文件，质量保证措施达到比选文件要求的施工技术规范、标准但针对性一般的；

第三个档次（3-5】分：质量承诺满足比选文件，质量保证措施基本达到比选文件要求的施工技术规范、标准但明显缺乏针对性的；

第四个档次（1-3】分：质量承诺满足比选文件，质量保证措施基本达到比选文件要求的施工技术规范、标准但有重大缺陷或错漏的；

对质量无承诺或质量承诺不满足比选文件的不得分。

##### 故障应急处置方案评审评分（15 分）



第一个档次（12-15】分：故障应急处置方案满足比选文件要求，保证措施合理且有针对性的；

第二个档次（10-12】分：故障应急处置方案满足比选文件要求，保证措施合理但针对性一般的；

第三个档次（5-10】分：故障应急处置方案满足比选文件要求，保证措施基本合理；

第四个档次（1-5】分：故障应急处置方案满足比选文件要求，但保证措施存在问题；

### 网络及信息安全保障服务方案评审评分（15分）

第一个档次（12-15】分：报价人针对项目网络及信息安全保障措施完善、具有丰富的信息安全服务经验、针对性强；

第二个档次（10-12】分：具有较好的网络及信息安全服务能力，有一定的信息安全服务经验，能基本满足用户信息安全维护需求；

第三个档次（5-10】分：具有一定的网络及信息安全服务能力，信息安全服务经验一般；

第四个档次（1-5】分：网络及信息安全服务能力一般，信息安全服务经验有所欠缺；

无网络及信息安全保障服务方案的不得分。

### 服务要求及服务响应程度评审评分（20分）

根据服务要求及服务响应方案进行评分。

1、报价人所提供的技术服务及服务内容完全满足或优于比选文件要求的得满分；

2、服务方案内容一般，且每缺一项服务要求及服务内容的截图部份不满足或未提供截图证明的，每项扣2分，扣完为止。

#### 5.2.3 定标

根据评选办法，对通过响应性评审的报价人分别就报价文件的技术部分、商务部分进行打分。根据报价人综合得分高低，排出第一中选候选人，并依次排出中选单位候选人第二、三名。

### 5.3 对报价文件澄清

必要时，评选小组可要求报价人对报价文件中的疑问和问题进行澄清，报价人应在规定的时间以书面形式予以澄清或答复。书面澄清或答复须经法定代表人或授权代表签字，澄清和答



复将作为报价文件的组成部分。澄清问题不允许超出要求的范围或修改报价文件的实质性内容。

#### 5.4 中选标准

本次比选采用综合评估法，在进行商务和技术评估的基础上，依据本项目的特点，由评选小组对各报价人进行综合评估和评价。根据各评选小组成员打分情况汇总计算各报价人最终综合评估得分，评选小组按照各报价人最终综合评估得分从高到低进行排序推荐中选候选人。

#### 5.5 评选结果报告

评选小组完成比选后，全体成员要在书面报告上签字，对评审结论有不同意见的可书面阐述不同意见和理由。评选小组成员拒绝在评选结果报告上签字且不陈述其不同意见和理由的，可视为同意评审结论。评选小组将对此做出书面说明并记录在案。

向比选人提交书面评选结果报告后，评选小组即告解散。

### 6、定标

6.1 比选人根据评选小组的书面评选结果报告确定中选人。

6.2 中选人收到成交通知书后根据要求的时间、地点与业主签合同。

### 7、报价文件的密封与标记

7.1 报价人须将报价文件的正本和副本密封，并在封袋上标明“正本”或“副本”；正本和副本如有不一致之处，以正本为准，所有封袋的齐缝处必须密封、盖章（若不密封、盖章，报价文件可视为废标）。

7.2 所有封袋上写明报价人的名称。

7.3 若报价人未将报价文件按上述规定进行密封和标记，造成遗失，失密等情况，采购人将不承担与此有关的责任。

7.4 报价文件正本份数 1 份，副本份数为 1 份，共 2 份。

7.5 报价人需提供与纸质版对应的电子版报价文件，且密封完好。



## 第三章 技术规格书

### 一、技术标准和要求

1. 本次服务业务中报价人所提供的材料、设备、服务须达到现行中华人民共和国以及省、自治区、直辖市或行业的维护服务业务建设标准和规范的要求，符合《中华人民共和国网络安全法》、满足第二级系统网络安全等级保护相关技术要求。
2. 本业务项目安全、文明、施工及社会环境的保护应按中华人民共和国以及省、市、自治区、直辖市或行业、当地政府以及采购人有关规定执行。
3. 除满足上述标准和规范要求外，还必须满足国家其他相关强制性标准和规范的要求。
4. 对接触到采购人的信息化数据进行保密。

### 二、服务内容

云南驰宏资源综合利用有限公司(护网行动)网络安全加固及网络故障恢复服务。

### 三、服务范围

对驰宏综合利用互联网核心资产及业务系统进行全面深入的风险隐患排查，对不满足合规性的基础网络、机房、信息系统及工控系统问题进行整改，以 7\*24 小时“人机共智”的安全托管服务，及时提供策略检查及配合开展应急演练、互联网全量资产梳理、互联网安全检测、全资产脆弱性识别和管理、渗透测试、安全加固、护网监测、AI 软件导致的资产横向攻击行为的检测和防护，统一端点安全管理系统的防护、人员安全引导系统（对互联网开放）、视频抓违章后期系统引入等的全量核心资产的护网现场值守、应急响应服务及检查（检测、监测），发现问题及时处置（如处置问题需要额外物资与甲方另行沟通商定）。

具体服务内容如下：



网络安全托管服务：			
序号	服务类别	服务内容	数量
1	策略检查及应急演练	<p>1、上线前策略检查：上线前安全专家对安全组件上的安全策略进行统一检查，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果</p> <p>2、完善应急预案：针对专网不同类别应用系统失陷，建立演习应急处置预案及操作手册。</p> <p>2、开展应急演练：结合应急预案，开展桌面推演和现场演练，检验应急流程、应急措施和协同处置的有效性。</p> <p>3、一键断网应急演练：开展一键断网应急演练，强化应急处置流程。</p> <p>4、人员安排：需安排专业工程师及网络安全专家至少 2 人现场共同完成，每半年一次</p>	2 次
2	互联网暴露面资产梳理	<p>1、梳理驰宏资源现有的全量互联网暴露面资产，包括近 400 台终端 IP、办公网、环保在线监测系统、视频监控网（全厂 1000 多个摄像头）、应援布控系统、供电系统、P2P 网络、MES(DCS)网络、语音通讯网、新材料厂计量专网等驰宏资源全量资产。</p> <p>2、通过利用资产测绘工具，排查互联网侧是否存在未记录在案的相关互联网暴露面资产。</p> <p>3、建立互联网资产台账，包括内外网 IP 地址、端口、域名等信息，明确资产归属和资产责任人。</p> <p>4、人员安排：需安排专业工程师及网络安全专家至少 2 人现场共同完成，每季度一次。</p>	4 次
3	互联网资产安全检测	<p>4、漏洞扫描：对驰宏资源 MES（DS）内网资产和公网映射进行漏洞扫描，发现操作系统、数据库、中间件、网络设备、网络安全设备中存在的安全漏洞，出具漏洞扫描分析报告和整改建议。</p> <p>5、渗透测试：对全量互联网资产开展深度渗透测</p>	4 次



		<p>试，检验应用系统健壮性、访问控制有效性、安全设备敏感性。</p> <p>6、人员安排：需安排专业工程师及网络安全专家至少2人每季度一次现场完成+提供云端7*24小时资产监测服务</p>	
4	内网资产梳理	<p>1、梳理并及时发现驰宏资源全量包括IT资产及其动态变化，包括：域名（含子域）、IP、站点防护设备、主机操作系统、服务和端口、网站应用容器、应用服务组件等。</p> <p>2、持续服务过程中安全专家定期对资产进行存活性探测，当发现未存活资产或资产发生变更时，安全专家对变更信息确认与更新，确保深信服安全运营中心中资产信息的准确性和全面性。</p> <p>3、服务方式：需提供专业工程师及网络安全专家至少2人每季度一次梳理服务+云端7*24小时探测服务</p>	4次
5	脆弱性识别	<p>一、攻击路径分析服务，针对驰宏资源全量：</p> <p>1.检查是否根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段。</p> <p>2.检查是否将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；</p> <p>3.检查是否在网络各个边界处部署了访问控制技术措施，如部署网闸、防火墙或ACL等。</p> <p>4.检查是否应能够对非授权设备私自联到内部网络的行为进行检查，准确确定出位置，并对其进行有效阻断；</p> <p>5.检查是否部署终端管理软件或采取其它技术手段防止非法外联行为；</p> <p>6.检查是否在网络边界处部署恶意代码防范技术措施，是否启用了检测和阻断功能；</p> <p>7.检查在网络边界处是否有对网络攻击进行检测的相</p>	全年7*24小时



	<p>关措施；</p> <p>8. 访谈管理员并查看网络拓扑图，系统是否采用冗余技术设计网络拓扑结构；</p> <p>9. 访谈管理员并查看网络拓扑图，系统是否有主要网络设备、通信线路和数据处理系统的硬件冗余等；</p> <p>二、敏感信息排查服务，针对驰宏资源全量：</p> <p>1. 暗网情报监控：监控暗网中与客户相关的敏感数据泄露、名男文件泄露等情报，及时告警并协助处置。</p> <p>2. 代码泄露监控：覆盖主流国内外代码托管平台（如github、GitLab、BitBucket、码云等），为客户发现并阻断代码泄露风险。</p> <p>3. 敏感文件监控：监控主流网盘（如百度网盘、115网盘等）、文库（百度文库、道客巴巴等）等文件共享平台，帮助客户管控机密文件外泄风险。</p> <p>4. 资产失陷监控：依托深信服威胁情报能力，为客户提供互联网暴露资产隐患排查。</p> <p>5. 高危漏洞监控：依托专业漏洞团队收集最新爆出的高危漏洞信息（危害、影响范围、修复建议等）并及时预警。</p> <p>三、漏洞扫描服务</p> <p>1. 本地扫描：是指经过用户授权后，扫描人员达到用户工作现场，根据用户的扫描目标直接接入到用户的办公网络或业务网络中。这种扫描的好处就在于免去了扫描人员从外部绕过防火墙、入侵保护等安全设备的工作。一般用于检测内部服务器地址的威胁源或路径。</p> <p>2. 互联网扫描：与本地扫描相反，扫描人员无需到达客户下场，直接从互联网访问用户的某个接入到互联网的系统并进行扫描即可。这种扫描往往是应用于那些关注互联网开放服务的用户，主要用于检测互联网</p>	
--	---	--



		<p>开放服务的威胁源或路径</p>	
<p>6</p>	<p>基线核查服务</p>	<p>基线核查服务</p> <p>1.人工检查主要包括登录信息收集、配置安全分析和形成检查报告。其中配置安全分析是比较重要的环节，分析结果直接影响报告的准确性、权威性；</p> <p>2.自动化检查是借助深信服的基线核查系统（BVT）或专门开发的检查脚本来自动化完成部分工作。自动化工具主要自动化完成目标设备登录、设备配置检查和配置信息记录工作，此部分工作借助自动化工具是为了消除手工误操作的隐患，提高检查效率和精确度；</p> <p>服务方式：</p> <p>1、针对服务资产的系统漏洞和 Web 漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。</p> <p>2、漏洞修复优先级排序与通告：基于漏洞扫描结果、资产重要性及漏洞的威胁情报，对漏洞进行重要性排序，确定修复的优先级；并将最终结果通告给用户。</p> <p>3、漏洞可落地修复方案：对漏洞进行分析并输出可落地的修复方案，通过工单系统跟踪修复情况。</p> <p>4、漏洞复测与状态追踪：对修复的漏洞进行复测，及时更新漏洞工单的漏洞修复状态。</p> <p>5、弱口令分析与管理：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、</p>	<p>每 2 个月一次 现场共同完成+ 云端 7*24 小时 监测服务</p>



		<p>smtp、VNC、ftp、telnet、ssh、mysql、tomcat 等。针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测。并将检测发现的问题通过工单系统跟踪修复状态。”</p> <p>6、最新漏洞通告与排查：实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行通告与排查。通告信息中包含最新漏洞信息、服务资产受影响情况。</p> <p>7、最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，修复方案以及临时规避措施。</p> <p>8、最新漏洞复测与状态跟踪：由安全专家对该最新漏洞建立工单进行持续跟踪。</p> <p>9、人员安排：需提供专业工程师及网络安全专家至少 3 人每 2 个月一次现场共同完成+云端 7*24 小时监测服务</p>	
7	渗透测试服务	<p>1.现场与远程测试</p> <p>现场测试是指经过用户授权后，测试人员到达用户工作现场，根据用户的期望测试的目标直接接入到用户的办公网络甚至业务网络中。这种测试的好处就在于免去了测试人员从外部绕过防火墙、入侵保护等安全设备的工作。一般用于检测内部威胁源和路径。</p> <p>远程测试与现场测试相反，测试人员无需到达客户现场，直接从互联网访问用户的某个接入到互联网的系统并进行测试即可。这种测试往往是应用于那些关注门户站点的用户，主要用于检测外部威胁源和路径。</p> <p>2.黑盒白盒测试</p> <p>黑盒测试是指测试人员对除目标系统的 IP 或域名以外的信息一无所知的情况下对系统发起的测试工作，这种方式可以较好的模拟黑客行为，了解外部恶意用户可能对系统带来的威胁。</p>	6 次



		<p>白盒测试则是指测试人员通过用户授权获取了部分信息的情况下进行的测试，如：目标系统的帐号、配置甚至源代码。这种情况用户模拟并检测内部的恶意用户可能为系统带来的威胁。</p> <p>3.服务方式及人员安排：需提供专业工程师及网络安全专家至少 2 人每 2 个月一次远程做渗透测试，确保各种攻击源的应对办法</p>	
8	<p>安全设备巡检及安全加固</p>	<p>1.对云南驰宏资源综合利用有限公司安全设备（包括：深信服防火墙、深信服上网行为管理、深信服日志审计、思科核心交换机、汇聚交换机、迪讯信息网络核心服务器等）及各所属单位专线防火墙开展设备巡检。</p> <p>2.更新安全设备版本、规则库，确保安全设备的防护能力达到最优。</p> <p>3.对检测出的漏洞加固：针对互联网系统安全检测发现的风险，及时下发相关的责任人，监督、指导开展整改工作，对于风险较大且无法整改的系统，建议关停或采取访问限制措施。</p> <p>4.平台加固：对于设备巡检中发现的设备问题，及时组织设备厂商开展安全加固，且务必完成整改。</p> <p>5.服务方式及人员安排：需提供专业工程师及网络安全专家至少 2 人现场巡检及网络安全加固，每 2 个月一次。</p>	6 次



9	安全应急响应服务（网络攻击导致断网的网络恢复服务及常日网络安全核心设备故障的网络恢复服务）	<p>提供现场团队+原厂团队现场应急响应服务</p> <p>一、针对病毒攻击后的网络故障恢复服务 包括：对驰宏资源利用公司的主机安全数据进行分析、全方位监测发现的威胁和异常进行快速响应和处置，并针对安全事件进行深入调查和原因分析；同时输出事件响应处理报告，帮助速响应正确应对攻击入侵事件，降低安全事件带来的损失。</p> <p>服务方式：需提供专业的服务团队及网络安全专家现场服务，云端后台网络安全团队远程辅助</p>	60天
		<p>二、针对核心设备的日常网络故障恢复服务 服务方式：提供现场2小时应急响应服务能力。突发事件联络员全天候值班，安全服务管理职能部门负责人、与应急相关的其他部门负责人应急服务团队主管，取消休假，处于随时待命状态。</p> <p>2.服务方式：提供现场服务+云端后台网络安全团队远程辅助，所提供人员需具备网络专业技术水平至少2年以上维护经验，管理人员至少8年以上管理经验</p>	60天
10	护网监测值守	<p>一、网站安全监测：</p> <p>1.利用网站安全监测平台，对互联网系统开展7*24小时安全监测，包括可用性监测、网站篡改、挂马、黑链、敏感信息泄露等。</p> <p>二、互联网安全监测</p> <p>1.云端值守人员开展7*24小时互联网安全监测，及时发现、分析互联网侧的各类攻击事件，并开展处置。</p> <p>2、现场值守人员开展7*24小时互联网安全监测，及时发现、分析互联网侧的各类攻击事件，并开展处置。</p> <p>三、应急响应 针对突发安全事件，值守人员及时开展应急处置</p> <p>四、MSS重保值守</p>	全年7*24小时



		<p>以保障风险管控效果为目标，以 7*24h 持续在线守护为主线，以【资产、脆弱性、威胁、事件】四个核心安全风险要素为抓手，提升组织安全风险管控能力和安全工作效果，提供持续、有效、省心、便捷的网络安全运行维护服务。</p> <p>五、重大节假日重保值守</p> <p>重大节假日期间除“7*24 小时 MSS 值守外”的网络安全保障服务，MSS 处理不了的，提供专业人员至少 1 人现场解决，云端 7*24 小时监测服务</p> <p>六、服务方式及人员安排：</p> <p>针对驰宏资源的资产及业务系统进行网络安全保障服务及网络安全应急管理服务，以保障网络安全“持续有效”为目标，提供安全运营中心和网络安全专家服务团队，采用有效协同的“人机共智”模式，提供全天 7*24 小时实时网络安全监测、网络应急管理服务，发现问题第一时间应急处置，并时实发送处置报告</p>	
11	安全保障总结	<p>护网监测：安全专家每周总结阶段性安全运营情况并输出《日报、周报、月报、半年度总结、全年总结》报告，并向我单位定期总结汇报。</p> <p>安全运营年度汇报：安全专家总结年度安全运营情况并输出《年度总结报告》发送给我单位负责人进行总结汇报。</p> <p>用户 Portal：可视化 portal 支持随时查看服务范围内业务资产安全状态。支持在线展示所有脆弱性、威胁、事件工单的处置进程和结果支持用户在线对服务 SLA 进行查阅和监督。</p> <p>三、服务交付物</p> <p>《首次安全威胁分析报告》《漏洞举证报告》、《漏洞清单》、《应急响应报告》、《事件处置报告》、《威胁情报》、《安全运营周报》、《安全运营月报》、《半年度总结汇报》、《年度总结汇报》</p>	1 项



护网行动现场值守：			
序号	服务类别	服务内容	数量
1	护网值守（现场值守）	<p>一、护网期间网站安全监测：</p> <p>1.利用网站安全监测平台，对互联网系统开展 7*24 小时安全监测，包括可用性监测、网站篡改、挂马、黑链、敏感信息泄露等。</p> <p>2.护网期间分派 2 人现场值守，值守人员进行人工拨测，拨测周期为每两小时一次。</p> <p>二、互联网安全监测</p> <p>1.云端值守人员开展 7*24 小时互联网安全监测，及时发现、分析互联网侧的各类攻击事件，并开展处置。</p> <p>2.现场值守人员开展 7*24 小时互联网安全监测，及时发现、分析互联网侧的各类攻击事件，并开展处置</p> <p>三、服务方式及人员安排：需提供专业工程师及网络安全专家至少 2 人现场监测及值守</p>	60 天

#### 四、质量要求

服务质量必须符合驰宏综合利用(护网行动)网络安全加固及网络故障恢复服务要求，提供相应的维护成果及报告，满足《中华人民共和国网络安全法》、第二级系统网络安全等级保护相关技术要求，必须通过驰宏综合利用使用部门、管理部门的一次性验收合格。

#### 五、报价要求

报价说明：报价单位按照比选控制价进行下浮报价（保留小数点后一位）。

#### 六、安全要求

按照驰宏综合利用相关安全环保职业卫生管控制度、第二级系统网络安全等级保护相关技术要求、《中华人民共和国网络安全法》在合同中进行明确约定。



## 第四章 比选文件格式

### 一、报价函

（采购单位名称）：

我方全面研究了“（项目名称）”比选文件及相关技术文件，决定参加贵单位组织的本项目比选报价。我方授权（受托人姓名、职务、身份证号码）代表我方（报价单位的名称）全权处理本项目报价的有关事宜。

- 1.我方自愿按照“（项目名称）”比选文件及相关技术文件规定的各项要求向比选人提供所需维修维护服务业务服务。
- 2.一旦我方中选，我方将严格履行合同规定的责任和义务。
- 3.我方为本项目提交的报价文件正本 1 份，副本 1 份。
- 4.我方愿意提供贵公司可能另外要求的与比价谈判有关的文件资料，并保证我方已提供和将要提供的文件资料是真实、准确的。
- 5.我方完全理解比选人不一定将合同授予最低报价的报价人的行为。

报价人名称：\_\_\_\_\_（盖章）

法定代表人或授权代表（签字或盖章）：\_\_\_\_\_

通讯地址：\_\_\_\_\_

邮政编码：\_\_\_\_\_

联系电话：\_\_\_\_\_

传 真：\_\_\_\_\_

日 期：\_\_\_\_\_



## 二、法定代表人授权书

(采购单位名称)：

本授权声明：(报价人名称) (法定代表人姓名：\_\_\_\_\_、 职务：\_\_\_\_\_ ) 授权 (被授权人姓名) (职务：\_\_\_\_\_ ) 为 我方“\_\_\_\_\_”项目 (编号) 报价活动的合法代表，以我方名义 全权处理该项目有关比价报价、签订合同以及执行合同等一切事宜。

特此声明。

法定代表人签字或盖章：\_\_\_\_\_

法定代表人身份证号码：\_\_\_\_\_

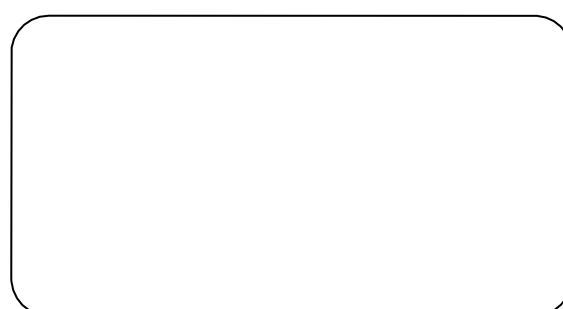
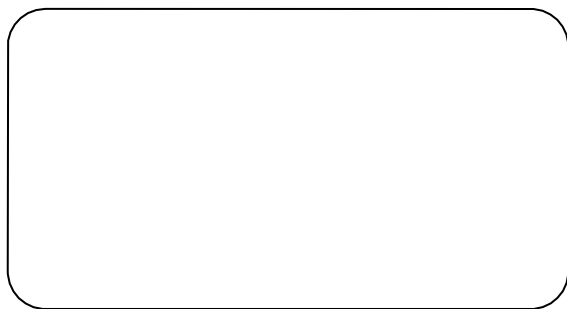
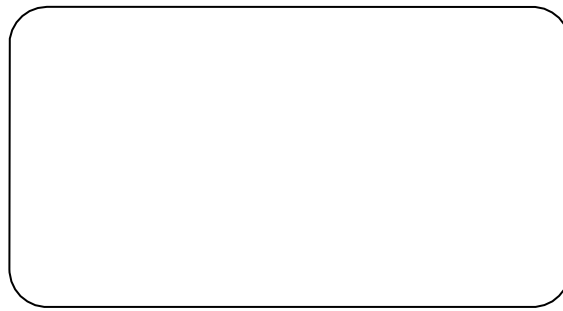
授权代表签字或盖章：\_\_\_\_\_

授权代表身份证号码：\_\_\_\_\_

报价人名称：\_\_\_\_\_ (盖公章)

日 期：\_\_\_\_\_

注：附法定代表人及授权代表二代身份证复印件 (正、反两面)





### 三、报价一览表

项目名称：云南驰宏资源综合利用有限公司(护网行动)网络安全加固及网络故障恢复服务

序号	项 目	比选控制价	报价
1	护网行动服务	<u>28</u> 万元	<u>    </u> 万元
2	响应时间	提供 <u>365*24</u> 小时持续在线监测运维服务，接到采购人通知后 <u>4</u> 小时内达到现场。	提供 <u>    </u> 小时持续在线监测运维服务，接到采购人通知后 <u>    </u> 小时内达到现场。
3	其他承诺	(自拟)	

注：此“开标一览表”，报价人应放在报价文件封面后第一页。

报价人名称：\_\_\_\_\_（盖章）

法定代表人或授权代表（签字或盖章）：\_\_\_\_\_

报价日期：\_\_\_\_\_



## 附件一

## 驰宏综合利用(护网行动)网络安全加固及网络故障恢复服务

序号	名称	服务内容	单位	数量	控制价 含税 6%	备注
1	网络安全 托管服务	互联网核心资产及业务系统进行全面深入的风险隐患排查，对不满足合规性的基础网络、机房、信息系统及工控系统问题整改，提供 7*24 小时“人机共智”的安全托管服务，及时提供策略检查及配合开展应急演练、互联网全量资产梳理、互联网安全检测、全资产脆弱性识别和管理、渗透测试、安全加固、AI 软件导致的资产横向攻击行为的检测和防护，统一端点安全管理系统的防护、人员安全引导系统（对互联网开放）、视频抓违章后期系统引入等全量核心资产的护网值守、应急响应服务及检查（检测、监测）	套	1	180000 元	
2	护网行动 现场值守	护网值守（现场值守）	天	1	1600 元	60 天

## 四、报价人基本情况表



报价人名称						
注册地址				邮政编码		
联系方式	联系人			电话		
	传真			网址		
组织结构						
法定代表人	姓名		技术职称		电话	
技术负责人	姓名		技术职称		电话	
成立时间			员工总人数：			
企业资质等级			其中	项目经理		
营业执照号				高级职称人员		
注册资金				中级职称人员		
开户银行				初级职称人员		
账号				技工		
经营范围						
备注						

注：此表后附报价人相关资料（如开户许可证、2022年至今任意一年财务审计报告、近半年社保及税务缴款凭证）

报价人名称：\_\_\_\_\_（盖章）

法定代表人或授权代表（签字或盖章）：\_\_\_\_\_

报价日期：\_\_\_\_\_





## 六、主要人员资历表

注：附证明材料（复印件）

一般情况					
姓名		性别		年龄	
执业资格 (或职称)		在本项目中 拟职		专业	
学历					
经历					
时间	负责过的主要项目	该项目中任职		备注	
获奖情况					

报价人：\_\_\_\_\_（盖公章）

法定代表人或授权代表：\_\_\_\_\_（签字或盖章）

日期：\_\_\_\_年\_\_月\_\_日



## 七、资格证明材料

- 1、营业执照副本（复印件加盖公章）；
- 2、资质证书副本（复印件加盖公章）；
- 3、业绩要求（2021年至今完成过至少 1 个网络安全服务类似项目业绩）（提供中选通知书或合同或业主证明材料）；
- 4、技术要求：提供专业的运行维护团队，维护平台需与原品牌防火墙及 EDR 等网络防护设备实现无缝对接，提供 7\*24 小时互联网安全监测并实时推送报告，提供原厂承诺并加盖厂商公章。
- 5、信誉要求：根据《关于对失信被执行人实施联合惩戒的合作备忘录》及《关于在比选活动中对失信被执行人实施联合惩戒的通知》精神，未被列入最高人民法院官网中“全国法院失信被执行人名单信息公布与查询”及“信用中国”的失信被执行人，并提供相关查询资料；
- 6、其它需附材料依次装订在此部分。



## 八、质量承诺及保证措施

包括但不限于以下内容：

- 1、质量承诺及保证措施；
- 2、故障应急预案；
- 3、其它。

(格式自拟)



## 九、响应时间承诺和保证措施

(格式自拟)

## 十、网络及信息安全保障服务方案；

(格式自拟)

## 十一、服务要求及服务响应方案

(格式自拟)



## 十二、安全底线承诺书

云南驰宏资源综合利用有限公司：

按照贵单位关于承包商安全生产风险管控的相关要求，我单位在承担（项目名称：）服务中，严格遵守并执行以下安全底线：

序号	类别	安全底线要求
1	资质证照	具备符合要求的资质证照；营业执照等要齐全且保证在合同期内有效。
2	安全管理机构和人员	设立相应的安全管理机构或配备合格的安全管理人员。
3	安全管理制度	严格执行国家现行安全规程、依法建立和落实安全生产管理制度和岗位安全操作规程。安全生产管理制度包括：安全生产责任制度，安全教育培训制度，安全检查制度，危险源辨识及风险控制管理制度，安全生产费用投入管理制度、职业健康管理制度，劳动防护用品管理制度，事故应急救援管理制度，安全档案管理制度，安全奖惩管理制度，危险作业分级管理制度，隐患排查治理制度等。遵守甲方安全生产管理制度。
4	安全教育培训	按规定对所有从业人员进行相关安全教育培训，经考试合格，方可上岗。现场主要负责人（项目经理）、安全管理人员、特种作业人员必须持证上岗；所有人员（含变更人员）均需在甲方备案，更换项目经理需征得甲方同意。
5	设备设施	必须使用符合国家、行业标准的设备设施及工器具。
6	隐患排查	建立健全安全生产检查制度，定期进行安全检查，及时消除事故隐患。
7	安全投入	保证用于配备劳动防护用品、进行安全生产教育和培训等必要的安全生产投入。
8	工伤保险	为从业人员按时足额缴纳工伤保险。
9	职业健康管理	依法对接触职业危害因素的人员进行职业健康体检，并建立健全职业健康监护档案。
10	应急管理	建立应急救援预案，配备应急救援器材，定期对人员进行应急培训并组织演练。
11	劳动防护	依法为从业人员配备符合国家标准或者行业标准且与承揽项目相适应的劳动防护用品，并监督、教育从业人员正确佩戴和使用。
12	现场管理	严格遵守中国铝业公司企业标准《施工现场安全底线标准（试行）》（QB CHINALCO-HSE-06-2017）。

特此承诺！

承诺单位：\_\_\_\_\_（盖章）

年 月 日

## 十三、中铝集团比价自律公约



比价项目：\_\_\_\_\_

### 报价人自律守则

- 1.依法从事报价和其他交易活动，诚实守信，自觉接受监督。
- 2.参与项目报价遵循法定或比选文件规定的资质、业绩或许可条件。不伪造从业人员资质证书、业绩情况、财务状况、信用状况、报价人授权委托书等相关资信文件和印章参与报价。
- 3.不挂靠其它企业、不超越本企业资质等级许可的业务范围或以任何形式借用其他企业的名义参与报价。
- 4.不通过联合比选人或比价代理人设置有利条款等方式干预比选文件编制。
- 5.按照比选文件要求编制报价文件、缴纳保证金等，不违背国家有关价格规定或低于成本价报价。遵守法律、法规和比选文件规定的比选程序，不隐瞒真实情况、弄虚作假、骗取报价和中选资格。
- 6.坚决抵制事先约定中选者、互相约定抬高或压低报价等串标、围标违法报价行为。不以宴请、提供礼品、行贿等方式贿赂比选人、比价代理人或评选专家。
- 7.严格按照比选文件和报价文件约定的条款，及中选条件签订合同协议，不签订“阴阳合同”，不将中选项目违法转包和违规分包。
- 8.依法履行合同约定，确保质量、进度，不得擅自变更、增减合同标的物及款项，做好项目的后续服务工作。
- 9.对违法和不公正行为投诉时，保证投诉内容及相应证明材料



的真实合法。

本人参加本项目比价报价相关工作，自愿签署本公约，共同承诺自觉履行和遵守公约的各项规定，坚持守法、守信，维护比价报价活动秩序。

报价单位名称: \_\_\_\_\_

法定代表人或授权代表签字: \_\_\_\_\_

日期: \_\_\_\_\_