

十. 分项报价表

投标单位名称:中安网脉(北京)技术股份有限公司

包号: 包 8



单位: 人民币 (元)

序号	项目实施服务内容		数量 及单位	金额	备注
一	设备采购				
1	互联网边界 负载均衡设备	<p>1、硬件参数: 内存$\geq 32\text{G}$, 冗余电源, ≥ 10 个千兆电口、≥ 4 个千兆光口 SFP、≥ 2 个万兆光口 SFP+(满配多模光模块)。</p> <p>2、性能参数: 4 层吞吐量$\geq 40\text{G}$, 四层并发连接数$\geq 3000\text{W}$, 4 层新建连接数 CPS$\geq 80\text{w}$, 7 层新建连接数 RPS$\geq 80\text{w}$。</p> <p>3、功能参数:</p> <p>(1) 设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能, 三种功能同时处于激活可使用状态, 无需额外购买相应授权。</p> <p>(2) 支持基于 URL 的链路调度功能, 支持 DNS 内网记录, 包含 A、AAAA、CNAME、MX 和 TXT 等类型, 可识别内网用户并对其 DNS 请求直接返回相应结果; 支持智能 DNS 解析功能, 实现外网用户访问内网业务系统的最优路径选择。</p> <p>(3) 支持链路负载, 能够分别基于链路监测、应用选路和 ISP 流量进行展示分析, 其中链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量; 应用选路展示基于应用分类选择相应链路的示意图、ISP 展示基于运营商分类选择链路的示意图。</p> <p>(4) 具备业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数。</p> <p>4、提供大于等于三年硬件质保和软件升级等服务。注: 信创国产设备</p>	1 台	116000	<p>品牌: 网御</p> <p>规格或型号: Leadsec-ADC-H G-5000</p> <p>生产厂家: 北京网御星云信息技术有限公司</p>

序号	项目实施服务内容		数量及单位	金额	备注
2	上网行为管理设备	<p>1、硬件参数：内存≥8G，硬盘≥1.5T，双电源，≥6个千兆电口、≥2个万兆光口 SFP+ (满配多模光模块)。</p> <p>2、性能参数：网络层吞吐量（大包）≥10Gb，带宽性能≥1Gb，每秒新建连接数≥14000，最大并发连接数≥500000。</p> <p>3、功能参数：</p> <p>(1)支持网关模式，支持 NAT、路由转发、DHCP、GRE、OSPF 等功能。支持网桥模式，以透明方式串接在网络中；支持电口 bypass；必须支持多路桥接功能，最多可支持 32 组网桥模式。</p> <p>(2)支持部署在 IPv6 环境中，设备接口及部署模式均支持 ipv6 配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持 IPv6。</p> <p>(3)内置应用识别规则库。</p> <p>(4)能同时连接多条外网线路，且支持多条线路流量复用和智能选择流速最快线路的技术。</p> <p>(5)支持设备首页功能界面可分析显示接入用户人数、终端类型、认证方式；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况。</p> <p>(6)支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持下钻设置线路流控策略。</p> <p>(7)支持同步钉钉平台或企业微信组织结构；支持钉钉平台或企业微信等第三方账号授权认证。</p> <p>(8)支持通过抑制 P2P 的上行流量来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。</p> <p>4、提供大于等于三年硬件质保、应用特征库和软件升级等服务。注：信创国产设备</p>	1 台	90000	<p>品牌：天融信</p> <p>规格或型号：TopACM</p> <p>生产厂家：北京网御星云信息技术有限公司</p>
3	WEB 应用防火墙	<p>1、硬件参数：交流冗余电源，≥6 千兆电口（支持 bypass），≥4 个千兆光口、≥4 个万兆光口，≥内存 32G (满配多模光模块)。</p> <p>2、性能参数：应用层吞吐量≥3Gbps。</p> <p>3、功能参数：</p> <p>(1)提供 TCP Flood 防护、HTTP Flood 防护、慢速攻击防护。</p>	1 台	110000	<p>品牌：天融信</p> <p>规格型号：TopWAF (FT-A) (万兆)</p> <p>生产厂家：北京</p>

序号	项目实施服务内容		数量及单位	金额	备注
		<p>(2)支持识别 HTTP 报文常见的编码和编码攻击: URL 解码、Base64 解码、HTML 解码、JSON 解析、XML 解析、PHP 反序列解析、UTF-8 解码等。</p> <p>(3)支持 XML 攻击防护,对以 XML 格式传输和存储的数据进行解码检测识别,支持导入 Schema 文件和 WSDL 文件对上传的 xml 文件进行格式校验,防止攻击者恶意提交 XML 文件,支持外部实体、垃圾字符填充等 XML 注入攻击防护。</p> <p>(4)支持爬虫、扫描器等自动化工具的安全检测,能选择多种爬虫防护规则,并按照配置实例进行相应的动作。</p> <p>(5)同一域名/站点的 SSL 模块需同时支持国际标准 https 证书及国密证书,降低国密改造难度。</p> <p>(6)支持扫描防护,攻击者通常会利用各种工具扫描网站,探测网站漏洞,给网站的安全带来极大隐患,WAF 可以通过识别扫描工具的数据特征值,阻断扫描工具的探测,支持基于请求量统计和应答分布统计等算法对扫描行为进行分析并防护。</p> <p>(7)支持 ARP 欺骗防护。</p> <p>4、提供大于等于三年硬件质保、WEB 应用特征库、软件升级等服务。注:信创国产设备</p>			天融信网络安全技术有限公司
4	漏洞扫描设备	<p>1、硬件参数:交流冗余电源,≥6*电口,≥4*千兆光口,≥4T 硬盘。默认提供 1 路扫描端口授权,提供系统漏洞扫描、提供 Web 应用扫描模块(满配多模光模块)。</p> <p>2、性能参数:最大并发主机数≥60,最大并发任务数≥10。授权可扫描 1000 个 IP 地址或域名。</p> <p>3、功能参数:</p> <p>(1)支持检测的漏洞数大于 300000 条,兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准。</p> <p>(2)支持高级数据分析,可对同一 IP 的两次扫描结果进行风险对比分析,并可在线查看同一 IP 的多次历史扫描结果。</p> <p>(3)支持对扫描出的漏洞提供取证性质的验证并输出报告,直观展示漏洞利用过程和危害性。</p> <p>(4)支持漏洞验证扫描任务,包括系统漏洞验证扫描、Web 漏洞验证扫描。</p> <p>(5)具备单独口令猜测扫描任务,支持多种口令猜测方式,允许外挂用户提供的用户名字典、密码字典和用户密码组合字典。</p>	1 台	110000	<p>品牌: 天融信</p> <p>规格型号: TopScanner 7000 (FT-B20)</p> <p>生产厂家: 北京天融信网络安全技术有限公司</p>

序号	项目实施服务内容		数量 及单位	金额	备注
		<p>(6)支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息。</p> <p>(7)支持扫描国产操作系统、应用及软件的安全漏洞，如欧拉、统信、麒麟、达梦、南大通用、人大金仓等。</p> <p>(8)支持实现显示扫描结果，包括扫描进度、主机存活数、预计扫描时间、漏洞风险信息等等。</p> <p>4、提供大于等于三年硬件质保、系统规则库、WEB 应用规则库、软件升级等服务。注：信创国产设备</p>			
5	流量探针设备	<p>1、硬件参数：交流冗余电源，CPU 核数不少于4 核，内存不低于4G，≥6 个千兆电口、≥6 个千兆光口、≥2 个万兆光口，≥4T 硬盘(满配多模光模块)；</p> <p>2、性能参数：应用层性能≥1.8G，攻击特征库数量≥8500，病毒特征库数量≥600W、支持的应用协议识别数量≥6000、WEB 攻击特征库≥3500；</p> <p>3、功能参数：</p> <p>(1)设备需对流量一次性完成入侵威胁检测、防病毒检测、应用识别检测、URL 信誉检测、WEB 攻击检测、威胁情报匹配检测；设备不仅能够识别 P2P、IM、流媒体、网络社区、游戏等常见网络协议，而且能够对协议流量里的漏洞、恶意软件利用、传输文件等进行检测，给出风险级别判定结果。</p> <p>(2)支持自定义应用审计规则；支持主动对网络中特定网段进行端口扫描。</p> <p>4、提供大于等于三年硬件质保和软件升级服务。注：信创国产设备</p>	1 台	112000	<p>品牌：天融信</p> <p>规格型号：TopTVD</p> <p>生产厂家：北京天融信网络安全技术有限公司</p>
6	日志审计设备	<p>1、硬件参数：千兆电口≥6 个，千兆光口≥4 个，硬盘≥10T；内存≥16G；交流冗余电源(满配多模光模块)。</p> <p>2、性能参数：日志处理能力≥1000 条/秒，审计授权≥200。</p> <p>3、功能参数：</p> <p>(1)支持华三、华为、天融信、启明星辰、绿盟、深信服、迪普等国内外主流厂商的安全设备；</p> <p>(2)支持主流的路由器、交换机、负载均衡等网络设备；</p> <p>(3)包括但不限于支持 Windows、Window server、Linux、Unix、银河麒麟、统信、凝思、华为欧拉、中科红旗等操作系统；</p>	1 台	120000	<p>品牌：深信服</p> <p>规格或型号：SIP-Logger-L2100</p> <p>生产厂家：深信服科技股份有限公司</p>

序号	项目实施服务内容		数量及单位	金额	备注
		(4)包括但不限于支持 MySQL、Oracle、SQLServer、人大金仓、达梦、神州通用等数据库； (5)支持基于 TCP 和 UDP 的 syslog 协议、kafka、snmp trap、ftp、wmi 等采集协议格式的模式解析； (6)支持从不同类型系统采集到的日志进行分析； (7)支持将采集到的日志进行归并；支持资产自动识别；支持日志查询。 4、提供大于等于三年硬件质保和软件升级服务。注：信创国产设备			
7	数据库审计设备（核心产品）	1、硬件参数：交流冗余电源、≥6*GE 电口、≥4*SPF+光口，≥4T 硬盘，≥1 个管理口（满配多模光模块），数据库授权≥50。 2、性能参数：网络层吞吐量≥3500Mbit/秒，SQL 语句处理能力≥20000 条/秒。 3、功能参数： (1)支持达梦、人大金仓等国产数据库审计。 (2)支持 Oracle、SQLServer、MySQL、DB2 等国际主流数据库审计。 (3)支持在 IPV4、IPV6 环境中部署，支持所有数据库 IPV4、IPV6 协议的审计。 (4)支持根据不同的安全级别采用不同的响应方式，包括记录、告警等。 (5)支持精细化日志查询。 (6)支持实时展示当前活跃会话详情信息。包括：会话开始时间、持续时长、访问来源 IP、目标服务端 IP、数据库协议类型、数据库账户等。 (7)支持报表预览，查看报表统计结果。 4、提供大于等于三年硬件质保和软件升级服务。注：信创国产设备	1 台	110000	品牌： 天融信 规格型号： TA-DB (HG-B20) 生产厂家： 北京天融信网络安全技术有限公司
8	TAP 镜像交换机	1、硬件参数：实配≥24 个千兆电接口，≥8 个 10G 光接口，≥8 个万兆多模光模块；配置冗余可插拔双电源，冗余可插拔双风扇。 2、性能参数：采用国芯设备，交换容量≥2.0Tbps，包转发率≥500Mpps； 3、功能参数： (1)支持集群或堆叠多虚一技术；支持 Telemetry GRPC 可视化；支持 iNQA 流量监控技术；支持纵向虚拟化功能，支持一键配置下发、批量配置下发；支持全端口 256bit MACSEC 加密。 (2)支持流镜像，支持 N:M 端口镜像，支持本地和远程端口镜像，支持 ERSPAN。	1 台	14000	品牌： 华三 规格型号： H3C S5590-28T8XC-EI 生产厂家： 新华三技术有限公司

序号	项目实施服务内容		数量及单位	金额	备注
		(3)提供 TAP 功能，支持基于端口 N:M 复制。 4、提供大于等于三年硬件质保和软件升级服务。注：信创国产设备			
9	网闸	1、硬件参数：配置冗余电源，内网≥8 个千兆光口，≥4 个万兆光口，外网≥8 个千兆光口，≥4 个万兆光口(满配多模光模块)； 2、性能参数：网络吞吐量≥10Gbps，系统整体时延<5ms，并发连接数≥100W； 3、功能参数： (1)支持代理、路由、透明工作模式，管理员可依据实际网络状况进行相应的部署。 (2)支持图形化拖拽方式策略编排、支持模版导入导出策略配置等多种策略配置方式，用户凭借实际应用系统部署位置即可通过拖拽元素来编排复杂的业务流程与数据流向策略，实现快速配置。 (3)支持 HTTP、HTTPS 服务访问；支持 POP3、IMAP、SMTP 邮件服务访问；支持 FTPS、SMB 文件服务访问；支持 SIP、RTSP 等主流视频传输及控制协议。 (4)支持对病毒检测，异常时进行阻断、记录日志等动作。 (5)支持 HTTP、HTTPS 服务访问；支持 POP3、IMAP、SMTP 邮件服务访问；支持 FTPS、SMB 文件服务访问；支持 SIP、RTSP 等主流视频传输及控制协议。 4、提供大于等于三年硬件质保和软件升级服务。注：信创国产设备	1 台	140000	品牌： 天融信 规格型号： TopRules (FT-A 10) 生产厂家： 北京天融信网络安全技术有限公司
10	入侵防御设备	1、硬件参数：内存≥16G，硬盘≥1T，冗余电源，≥6 个千兆电口、≥4 个千兆光口、≥2 个万兆光口(满配多模光模块)。 2、性能参数：网络层吞吐量≥20G，IPS 吞吐量≥2G，并发连接数≥800 万，HTTP 新建连接数≥16 万。 3、功能参数： (1)支持路由模式、透明模式、旁路镜像模式等多种部署方式。 (2)支持链路连通性检查功能。 (3)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。 (4)支持 NAT44、NAT64、NAT66 地址转换方式。支持双机模式部署。支持 NAT 穿透技术 ALG，支持 FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323 等协议。 (5)支持异常数据包攻击防御。 (6)支持对压缩病毒文件进行检测和拦截。	1 台	112000	品牌： 深信服 规格或型号： NIPS-2000-L22 02 生产厂家： 深信服科技股份有限公司

序号	项目实施服务内容		数量 及单位	金额	备注
		(7)支持杀毒白名单设置。 (8)支持僵尸主机检测功能。 4、提供大于等于三年硬件质保、入侵防护特征库、软件升级等服务。注：信创国产设备			
11	WEB 应用防火墙	1、硬件参数：交流冗余电源,≥6 千兆电口 (支持 bypass), ≥4 个千兆光口、≥4 个万兆光口, ≥内存 32G(满配多模光模块)。 2、性能参数：应用层吞吐量≥3Gbps。 3、功能参数： (1)提供 TCP Flood 防护、HTTP Flood 防护、慢速攻击防护。 (2)支持识别 HTTP 报文常见的编码和编码攻击：URL 解码、Base64 解码、HTML 解码、JSON 解析、XML 解析、PHP 反序列解析、UTF-8 解码等。 (3)支持 XML 攻击防护，对以 XML 格式传输和存储的数据进行解码检测识别，支持导入 Schema 文件和 WSDL 文件对上传的 xml 文件进行格式校验，防止攻击者恶意提交 XML 文件，支持外部实体、垃圾字符填充等 XML 注入攻击防护。 (4)支持爬虫、扫描器等自动化工具的安全检测，能选择多种爬虫防护规则，并按照配置实例进行相应的动作。 (5)同一域名/站点的 SSL 模块需同时支持国际标准 https 证书及国密证书，降低国密改造难度。 (6)支持扫描防护，攻击者通常会利用各种工具扫描网站，探测网站漏洞，给网站的安全带来极大隐患，WAF 可以通过识别扫描工具的数据特征值，阻断扫描工具的探测，支持基于请求量统计和应答分布统计等算法对扫描行为进行分析并防护。 (7)支持 ARP 欺骗防护。 4、提供大于等于三年硬件质保、WEB 应用特征库、软件升级等服务。注：信创国产设备	1 台	110000	品牌： 天融信 规格型号： TopWAF (FT-A) (万兆) 生产厂家： 北京天融信网络安全技术有限公司
12	流量控制设备	1、硬件参数：≥6 千兆电口、≥6 个千兆光口 (满配多模光模块)，含不低于 6 条线路接入授权，冗余双电源。 2、性能参数：设备整机吞吐≥10Gb，IPSEC VPN 加密性能≥200M。 3、功能参数： (1)支持基于用户组、位置、终端类型、URL 类型配置流量管控策略，支持基于 IP 或用	1 台	91000	品牌： 网御 规格或型号： LeadsecACM-NS 1200 生产厂家： 北京

序号	项目实施服务内容		数量 及单位	金额	备注
		户名灵活配置流控单位。 (2)能够实时看到各级流控通道的状态。 (3)支持根据百分比或数值设置通道带宽，并支持设置各通道的优先级。 4、提供大于等于三年硬件质保和软件升级服务。注：信创国产设备			网御星云信息技术有限公司
13	其他要求	1.需根据所购设备网络环境和现状提供详细的设备接入融合方案和网络及安全优化方案，确保原有网络内系统、安全设备及各类业务稳定运行。 2.提供接入和优化构架相关材料，包括但不限于网络拓扑图、路由等网络运行配置清单、设备连接图、业务连接图、资产清单等。对上架设备做好标签归类等服务。 3.服务期内按要求提供设备巡检方案，并根据国家档案整理标准对产出相关文档资料进行归档整理和电子化。 4.提供服务相关承诺函，承诺函内容包括：①合同签订日起15个自然日内完成设备到货，设备到货后30个自然日内完成构架整改和设备上架工作，在设备上架并经甲方确认后开始计算特征库、病毒库等功能性服务开始时间，同时应提供所购设备采购单位对设备功能的永久使用权。②故障响应：若出现故障时，甲方通知乙方后，乙方需于30分钟内响应，于4小时内到达现场进行故障的排查处理，若涉及设备或硬件更换，乙方即需按应急处置方案恢复业务正常运行，并于10个工作日内完成备品备件的到货及替换。③提供针对甲方相关人员的培训，培训内容包括向所购设备的基本操作、日常维护、故障排查等。	1 项	0	
二	网络安全服务采购				
1	网络安全日常运维及安全监控服务	通过日常安全监控、事件分析、安全预警、事件处理以及应急响应，为青海省生态环境厅信息中心各业务系统、重大安全事件提供全天候的现场值守服务、安全保障服务和安全设备监测服务，便于用户随时查询每日各系统的运行情况和安全状况，掌控自身系统的安全风险。安全月度报告不低于12份，安全周报合不低于50份，安全值守报告不低于50份。	1 项	40000	
2	安全设备巡检服务	定期对安全设备开展月度和年度巡检工作，根据巡检结果及时产出安全巡检报告，针对发现的问题，提供解决方案，完成整改等。	1 项	30000	

序号	项目实施服务内容		数量 及单位	金额	备注
3	应急响应和重大安全事件处置服务	针对客户网络系统等的安全需求，为客户提供安全应急响应服务，提供专业、快速反应的紧急事件响应队伍，帮助业务系统所属单位在遇到网络安全的突发事件时能够迅速、准确地发现并解决问题，将损失降低到最小。对于突发的安全事件在最短时间内做到应急响应，了解安全事件的基本现象，判断安全事件的原因，进行故障和事件的处理，并针对安全事件形成的破坏做出灾难恢复，在必要的情况下，协助客户网络系统进行入侵追踪和犯罪取证。同时提供相应支撑验证验证材料。	1 项	10000	
4	重大保障支持服务	切实提高信息安全保障能力，进一步提升网络安全防护水平。支撑做好中央、省级和省厅要求的重大节日和各类网络攻防演习及上级领导检查期间提供信息安全保障服务工作，包括制定应急或演练方案，开展演习及节假日期间网络安全值守，重要防护值守工作日志量不低于实际值守天数。同时提供相应支撑验证验证材料。	1 项	5000	
5	网络安全策略监控梳理优化	定期梳理防火墙策略，实时动态保障防火墙策略为最有效状态，严防死守保护系统安全；定期结合青海省生态环境厅信息中心实际需求与现状进行安全防护策略调研与分析，并及时、合理、有效地更新安全防护策略，使其发挥业务最优化、安全最大化原则。 1. 安全防护设备策略优化 结合省生态环境厅实际需求与现状开展网络安全设备防护策略优化服务，对外网边界防火墙、专网上联防火墙、专网下联防火墙、专网边界防火墙等网络安全设备更新安全防护策略。 2. 流量分析与处置 通过网络流量分析软件，确定数据包类型特征，并核对防火墙上配置的访问控制策略，清理无效、错误策略，限制或过滤来自于攻击源、不可靠的流量。 对现有主机设备的安全现状（包括补丁，权限，安全特性等）进行了解，包括：是否存在的安全漏洞，这些安全漏洞是否严重，系统配置是否满足安全要求等。 检查系统是否有被攻击或入侵，主要包括对操作系统或应用系统、数据库的审计，确认系统是否被非授权用户获得权限或系统被非正常使用。 对安全系统进行专业的检查，看是否得到了正确的使用，以及相关的事件是否对系统有影响，审计的对象包括：防火墙，防病毒，入侵检测等安全设备。 以上同时提供相应支撑验证验证材料。	1 项	5000	

序号	项目实施服务内容		数量及单位	金额	备注
6	安全漏洞扫描评估及整改加固服务	提供漏洞扫描服务，每月通过专业评估工具以本地扫描或远程扫描的方式对评估范围内的系统和网络（包含私有云平台）和设备进行安全扫描，从专网和外网两个角度来查找区络服务器主机、WEB 应用系统等安全对像目标存在的安全风险、漏洞和威胁，产出漏洞扫描报告。提供漏洞闭环管理服务，以工单形式进行漏洞排查验证、漏洞修复核验、漏洞闭环跟踪，提供最优安全漏洞解决建议，通过邮件等方式通知相应责任人进行漏洞处置，协助开展漏洞修补、加固、防护等网络安全服务。	1 项	15000	
7	弱口令扫描与整改服务	提供弱口令扫描服务，每月通过专业评估工具以本地扫描或远程扫描的方式对评估范围内的系统和网络（含私有云平台）进行安全扫描，从内网和外网两个角度来查找含私有云平台的安全对像目标存在的弱口令，同时产出弱口令扫描报告。	1 项	10000	
8	安全配置核查评估及整改加固服务	严格参照等保、青海省生态环境厅信息中心的各种设备安全配置规范要求从网络设备、业务系统、中间件、数据库、防火墙、应用（包含私有云平台）等方面着手，每月执行一次配置核查服务，提供配置核查结果和报告、对比分析报告和安全加固建议；对入网前设备进行完整、有效、科学、缜密的安全配置评估与加固指导，全程保障设备的顺利、安全、合规地上线；在日常运维中，提供临时性的配置核查工作，输出配置核查报告以及安全修复加固建议并指导修复加固。同时提供相应支撑验证材料。	1 项	15000	
9	网络安全应急演练及应急处置支持服务	切实提高应急处理能力，进一步提升网络安全防护水平。负责组织单位应急演练实施及网络安全事件应急处置等，每年不少于两次，同时提供相应支撑验证材料。	1 项	10000	
10	信息安全迎检保障和培训服务	配合做好网络安全各类检查自查支撑协助和资料打印等工作，满足上级单位对信息安全要求各类指标，圆满协助客户完成上级单位检查；按照客户要求对客户单位网络使用人员进行网络安全规范使用及网络安全防护培训。同时提供相应支撑验证材料。	1 项	5000	
11	网络安全管理制度完善	完善现有网络安全管理制度，建立一套以安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等五方面安全需求为主的网络安全管理制度体系。网络安全管理制度满足信息系统运行要求、遵守相关规程，实施等级保护及风险管理确保网络安全实现持续改进。同时提供相应支撑验证材料。	1 项	10000	
12	市州网络安全技术支持	按照甲方要求为青海省各市州环境局提供网络安全评估、网络安全整改建议、应急响应等技术支持服务。该服务形式以远程支持为主，特定情况下乙方需前往市州现场支持。	1 项	5000	

序号	项目实施服务内容		数量及单位	金额	备注
	服务	在甲方要求的情况下为市州生态环境局提供渗透测试和漏洞扫描服务。以上同时提供相应支撑验证材料。			
13	商密测评	按照甲方要求对重点信息系统提供商用密码应用安全性评估服务。	1 项	100000	
14	省厅防火墙病毒库授权提供和病毒库升级服务	按照甲方要求提供省厅 8 台防火墙病毒库授权 1 年，1 台防火墙病毒库、IPS、URL 授权 1 年，用于省厅网络构架安全体系防护。并根据官网病毒库更新情况，及时做好省厅防火墙病毒库的更新工作。同时提供相应支撑验证材料。	1 项	100000	
15	文档交付	本次安全服务过程中，对各阶段工作的结果进行综合分析，实时提交可操作可执行的安全应急响应预案、安全整治方案、漏洞整改报告、整改通知联系单及综合分析报告等安全文档。同时配合开展重点信息系统安全档案的整理、归档等工作。包括《青海省生态环境厅信息中心漏洞扫描报告》、《青海省生态环境厅信息中心安全漏洞加固方案》、《青海省生态环境厅风险评估报告》、《青海省生态环境厅信息中心渗透测试报告》《青海省生态环境厅信息中心信息系统安全运行周报》、《青海省生态环境厅信息中心信息系统安全运行月报》、《青海省生态环境厅信息中心安全巡检报告》、《青海省生态环境厅安全事件应急响应报告》等相关文档。做好运维档案归档和整理，对项目产出文件等资料及时进行分类整理和档案入盒，并同步提交电子扫描文档。	1 项	5000	
其他承诺及需要说明的事项：1. 合同签订日起 15 个自然日内完成设备到货，设备到货后 30 个自然日内完成构架整改和设备上架工作，在设备上架并经甲方确认后开始计算特征库、病毒库等功能性服务开始时间，同时提供所购设备采购单位对设备功能的永久使用权。 2. 服务期：自合同签订之日起 1 年。					
投标总价		大写：壹佰陆拾万元整 小写：1600000 元			

注：本表应依照采购一览表中的服务内容逐项填写。须列出具体的服务项目名称、内容及费用清单。（此表可按服务内容自行调整表格或增加附页）

投标单位： 中安网脉（北京）技术股份有限公司 （公章）

法定代表人或委托代理人： 冉庆国 （签字或盖章）

2025年 4 月 1 日