# 网络安全等级保护建设项目比选公告

致: 各友好单位

我司现有网络安全等级保护建设项目，特邀请参加本项目的询价采购，请在规定日期前报送参选文件，具体要求如下:

一、项目名称: 网络安全等级保护建设

二、采购单位: 重庆天原化工有限公司

三、工作内容: 建设网络安全等级保护二级。于 2025 年 6 月 30 日前完成相应安装调试并交付使用。具体数量、技术指标和商务指标详见《报价要求》《技术指标》

四、报价文件编制要求: 详见《报价要求》《技术指标》

五、确定服务商方式: 按照质量和服务满足询价文件要求且报价最低(不含税价格)的原则来确定服务商。

六、报价依据及风险: 总报价(含税及专票)最高限价 35 万元并应结合市场价考虑，对报价过高、不合理的报价或超出询价人支付能力的报价，询价人有权否决全部报价，询价人不作任何补偿，请报价人注意风险。

七、请于 2025 年 5 月 23 日前将响应文件纸质版密封后由顺丰、邮政、京东邮寄或现场递交方式送至重庆市涪陵区白涛化工园区重庆天原化工有限公司办公室。逾期提交响应文件的，视为放弃。

八、联系人: 罗意志(电话: 02364689628)

重庆天原化工有限公司

2025 年 5 月 19 日

# 网络安全等级保护建设项目报价要求

**一、资格要求:**

1.报价人须是在中华人民共和国境内注册的具有承担民事责任能力的企业,提供营业执照复印件一份(加盖鲜章)。

2.报价人所提供的产品应当是具备计算机软件著作权登记证书以及网络安全专用产品安全检测证书。

3.报价人如为代理商应当提供除“资格要求”第二条列明的文件外,需另行提供设备制造商的授权文件(格式自拟制造商加盖鲜章)。

4.报价人所提供的主要产品堡垒机、日志审计、服务器安全管控系统应为同一品牌厂商的产品。

**二、主要要求:**

1.提供符合《技术指标》内产品并负责安装，系统施工安装期间需要遵守询价人相应安全生产管理规定。

2.设计、施工过程需遵守安装相关规范。

**三、合同主要条款及付款条件:**

1. 报价人于合同签订后 30 天内自行运输设备到货并按相应规范完成建设及调试投用(含相应文件移交)。

2.报价人确保建设内容通过等保保护二级建设要求并获得等保保护二级相关认定证书。

3.在询价人验收通过并获得等保保护二级认定证书文件后于 45 天内支付 95%相应合同款项，质保期 3 年后支付剩余 5%合同款项。支付方式为银行承兑或电汇。

4.上述内容以最终签订的合同文件为准。

**四、报价文件编制要求:**

1. 报价人报列的项目及价格为完成本项目所涉所有内容,询价人不另行支付相应费用。

2.报价人不少于《技术指标》所列明的产品及数量进行报价（需列出不含税价和含税价），辅材、人工等均自行测算填报。

3.报价人应当对报价文件封面、正文、侧面加盖鲜章。

**五、现场查勘:**

1.如需现场查勘，请不晚于 2025.5.19 日前报名，拟于 2025.5.20 日组织现场查勘。

# 技术指标

| 序号 | 名称 | 技术规格 | 单位 | 数量 |
|---|---|---|---|---|
| 1 | 堡垒机 | 1. 标准型机架设备，内存≥8GB，硬盘≥2TB，千兆光口≥2 个，满足国产化硬件要求，并提供不少于 50 点的资产授权，授权时间不得低于 3 年。<br>2. 支持协议类型：RDP、VNC、X11、Telnet、SSH、FTP、SFTP、Oracle：PLSQL、TOAD、SQLPLUS、SQLDEVELOPER；Informix：DBACCESS；Mysql：MYSQLFRONT、HIDESQL；SQL Server：SQLserver（2000-2012）；Sybase：SCVIEW4；DB2：DB2CMD、DB2QUEST、navicat、Dbeaver、HTTP、HTTPS。<br>3. 所有图形化应用在实际操作环境中均可以正常使用且可自由调整应用的窗口大小，做到无缝发布，拖拽窗口应自然流畅，无卡顿现象，像是在本地运行应用程序一样。<br>4. 支持通过 Web 运维方式运维，支持 Web 运维显示用户名水印。<br>5. 通过 ssh-keygen 产生公钥和私钥密码对，上传堡垒机，可实现免密码登录服务器。<br>6. 默认规定用户登录后，只能在其目录下进行操作，不能随意跳转至其他目录进行操作，也可通过开关打开限制。<br>7. 支持命令记录：字符终端命令记录、图形终端键盘操作记录、数据库运维 SQL 命令、图形标题栏识别（OCR）<br>8. 运维回放：WEB 在线回放完整会话；字符终端操作会话支持倍速播放；图形操作会话支持拖拉定位播放；支持暂停、停止、重新播放等播放控制操作。 | 台 | 1 |
| 2 | 日志审计 | 1. 标准型机架设备，内存≥32GB，硬盘≥12TB，千兆光口≥4 个，事件综合处理性能≥9000EPS，满足国产化硬件要求，并提供不少于 200 点的数据源接入授权授权，授权时间不得低于 3 年。<br>2. 支持内置多种日志源类型开箱即用，默认可接入各类硬件设备和应用系统，包含但不限于主机、防火墙、IPS/IDS、WAF、网络设备、安全设备、数据库、应用系统、中间件、存储。设备、虚拟化设备、机房设备等多种设备和系统的日志接入方式。云平台支持 AWS 数据通过 S3 直接采集。<br>3. 支持业内通用标准数据获取方式，包括 Syslog、SFTP、文件、Kafka、HDFS、DB2、Mysql、Oracle、Sqlserver、Postgrel、SNMP、Netflow、WMI、ES、AWS 等。<br>4. 支持手动资产添加，可定义资产名称、IP、MAC、 | 台 | 1 |

| | | | | |
|---|---|---|---|---|
| | | 是否重点资产、设备型号、设备厂商、设备类型、物理位置、组织机构、责任人信息、自定义信息等，也可以使用导入模板，导入资产信息。<br>5. 支持 SNMP v1/v2c/v3 协议采集其他设备信息，并可配置采集频率，并支持随时启停操作。<br>6. 支持自定义报表图形化结果展示，包括但不限于柱状图、折线图、区域图、环形图、明细表格、聚合表格、统计量、环比量等。<br>7. 支持等级保护工作电子流程化管理，按基础信息录入、定级、备案、差距分析、整改、测评、监督检查等流程化管理电子文档，并支持等保知识库管理功能。 | | |
| 3 | 服务器安全管控系统 | 1. 服务端控制中心支持多种部署环境，需满足国产化操作系统要求，支持 X86 架构的麒麟 V10SP1、UOS20 或 ARM 架构的麒麟 V10/UOS20 操作系统。<br>2. 提供 windows 服务器授权点数 6 个、国产操作系统服务器授权 26 个，授权时间不得少于 3 年。<br>3. 客户端支持多类型操作系统同台管理，包括但不限于 windows 服务器、麒麟 V10/麒麟 V10 SP1/统信 UOS 等操作系统。<br>4. 产品需支持多引擎查杀技术,至少包括云查杀引擎、大数据特征引擎、人工智能引擎、脚本引擎等 4 个引擎，客户端支持以图形化方式展示各个引擎的信息,以确保产品可适应不同环境。<br>5. 防病毒要具备自我学习的机制，提高隔离网环境下病毒查杀能力。支持基于机器学习的程序识别方法，通过对海量样本进行分析，得到识别恶意程序的模型，发现程序内在规律，对未发生的恶意程序进行预防。<br>6. 支持在服务端对客户端下发多种扫描指令，包括快速扫描、全盘扫描、强力扫描等；支持对客户端系统设置、常用软件、内存活跃程序、开机启动项以及系统关键位置进行扫描。支持设置扫描任务有效期。<br>7. 提供人性化的扫描控制策略，服务端可限制客户端暂停或停止扫描任务，可控制是否扫描网络映射驱动器，支持速度最快、性能最佳、自定义三种查杀模式。支持自定义设置病毒查杀时，占用的 CPU 使用百分比、和内存占用的最大值。<br>8. 支持查看当日内网整体终端勒索病毒、宏病毒、感染型病毒、挖坑病毒、远控木马、黑客工具进行分类统计，可根据周、月为单位生成防病毒报告；支持对内网病毒日志自动关联攻击团伙/家族功能，可以攻击团伙/家族维度查看内网终端感染情况；支持根据病毒日志对未处理的病毒，远程一键处置。 | 套 | 1 |
| 4 | 电脑端安全 | 依托全面 SaaS 架构，实现硬件、软件、数据、资产、 | 套 | 300 |

| | | | | |
|---|---|---|---|---|
| | 管理运维 | 上网、防勒索等全方位数字安全与管理服务。从管人员、管资产、管数据三大价值层面助力企业数字化管理提效，对人员身份及行为管理、软、硬资产兼管、数据全链路守护等实现了一体化综合统效。 | | |
| 5 | 等级保护测评服务 | 1. 在充分了解被测系统的实际情况下，根据 GB/T 22239-2019《网络安全等级保护基本要求》等技术标准选择测评指标，结合信息系统的构成特点，确定具体的测评对象，建立测评方案和测评指导书，通过访谈、检查和工具测试等方式判断该系统安全管理和安全技术的各个方面相对于测评指标的符合程度，并对系统的不足提出整改建议，帮助测评单位对系统进行安全测评。<br>2. 对指定的一个二级系统进行网络安全等级保护测评，完成定级备案工作，最后出具符合公安部门要求的等级保护对象安全保护等级测评报告。 | 套 | 1 |