2022年 0052

合同编号：JSHXS2204084CGN00

常州市人民检察院工作网安全防御设备（等保三级一期）项目系统集成合同

合同签订地：常州

甲方：江苏省常州市人民检察院
地址：常州市永宁北路 10 号
法定代表人/负责人：陈兴生

乙方：中电鸿信信息科技有限公司
地址：南京市玄武大道 699-1 号
法定代表人/负责人：刘永新

甲乙双方本着诚实信用、平等互利的原则，就甲方委托乙方承担[工作网安全防御设备（等保三级一期）]项目系统集成事宜，经协商一致，签订本合同。

第一条 合同内容

1.1 甲方委托乙方对[工作网安全防御设备（等保三级一期）]项目进行总体策划设计、开发、实施、服务及保障；乙方向甲方出具项目技术方案，并经甲方认可后进行实施、服务及保障。

1.2 乙方所提供的设备和服务必须符合国家有关标准和常采公[2022]0191 号采购招标文件和投标文件的要求。

1.3 系统集成所应达到的质量要求按项目技术方案执行，无项目技术方案的则按国家现行相关标准执行。

1.4 乙方提供本系统集成项目所需的硬件设备及相关材料，具体清单见本合同附件。如甲方提供的图纸（如有）与《硬件设备及相关材料清单》不符的，以《硬件设备及相关材料清单》为准。

1.5 项目的履行地点[常州]。

1.6 本系统集成项目合同金额为[968000]元（大写：[玖拾陆万捌仟圆整），其中安全设备费[796000]元（税率 13%），集成安全服务费[172000]元（税率 6%）。

1.7 工期：本合同生效且符合进场施工条件后[30]天内（以最晚时间为准）。因甲方原因造成乙方不能按期完成工作的，经甲方书面确认后，乙方工作期可以顺延，顺延的日期与甲方造成乙方不能正常工作的日期相等。

第二条 甲方职责

2.1 提供系统集成所需的工作场地及条件；

2.2 乙方提供的设备、材料到达甲方后，双方进行验收。验收合格的，设备、材料交由甲方负责保管和看护，若因保管和看护不当造成的损坏或短缺，由乙方负责修理或补足，但有关费用由甲方承担。若因此造成工期延误的，乙方不承担责任。

2.3 提供项目所需的各种资料、图纸、数据、表格或系统要求；

2.4 在项目期间做好必要的项目配合和协调工作；

2.5 在方案有变更时应尽早通知乙方，并做好书面记录。因此导致工期迟延的，乙方不承担责任；

2.6 在双方项目验收完毕前，甲方不得使用本合同项下的线路和设备，否则视为项目验收合格。

2.7 本项目中乙方所提供项目技术方案、系统或软件及相关技术等的知识产权属乙方或权利人所有，甲方仅享有使用权，且甲方保证只将其用于本项目。未经乙方书面许可，甲方不得泄露、提供给第三方或用作其他用途。否则，甲方应承担由此引发的一切责任。

第三条 乙方职责

3.1 设计并与甲方详细讨论方案，解答甲方对系统的相关咨询；

3.2 按照项目技术方案实施项目，保质、保量、按时完工；

3.3 负责提供本系统集成项目所需的硬件设备及相关材料（详见本合同附件），并提供相应的售后服务。根据项目需要，经甲方代表签证，乙方可使用代用材料或设备。因甲方原因使用时，由甲方承担发生的经济支出，因乙方原因使用时，由乙方承担费用。由于市场供应情况变化而造成材料或设备变更时，由甲乙双方协商解决。

3.4 竣工后提供详尽的技术文档。

第四条 项目管理

此项目乙方选派最优秀的项目管理人员进行项目管理，并服从甲方现场管理人员指挥。乙方接到甲方要求后[1]小时内派出现场代表到工地，协调项目施工，以确保项目的进度和质量。

第五条 验收

5.1 甲乙双方应在设备（材料）到场后的[1]个工作日内按照《硬件设备及相关材料清单》中约定的品牌、型号、规格对设备（材料）进行共同验收，验收合格的，甲方签字确认；甲方逾期不进行验收的，视为设备（材料）验收合格。

5.2 乙方提供竣工验收资料后[15]个工作日内，由甲方根据项目技术方案进行项目验收，无项目技术方案的则按国家现行相关标准验收，项目验收合格的，甲方签字确认。甲方逾期不进行验收的，视为项目验收合格。

5.3 如乙方提供的设备（材料）存在质量问题或项目验收不合格的，在乙方完成整改或返工后[15]个工作日内，甲方应按上述验收标准及方案进行验收，验收合格的，甲方签字确认；甲方逾期不进行验收的，视为验收合格。

5.5 本合同项下设备（材料）的所有权自甲方向乙方支付完项目验收款后转移至甲方。

六、付款方式：

6.1 甲乙双方银行账户信息和纳税人信息如下：

甲方信息如下：江苏省常州市人民检察院

开户行：[工行常州博爱路支行]

银行地址：[/]
户名：[江苏省常州市人民检察院]
账号：[110502132921950019 6]
纳税人识别号：[/]
地址：[常州市永宁北路 10 号]
电话：[0519-85336261]
乙方信息如下：中电鸿信信息科技有限公司
开户行：[中国建设银行股份有限公司南京湖北路支行]
银行地址：[/]
户名：[中电鸿信信息科技有限公司]
账号：[32001881436059000588]
纳税人识别号：[91320000668382125D]
地址：[南京市玄武大道 699-1 号]
电话：[18961235188]

6.2 甲方按以下方式向乙方支付合同价款。

签订合同后[7]个工作日内，甲方支付乙方合同总价的 40%；所有软硬件设备到货验收合格后[7]个工作日内，甲方支付乙方合同总价的 50%；项目通过终验后[7]个工作日内，甲方支付乙方合同总价的 5%；剩余款项质保期满后付清。

七、维护

7.1 本集成项目的质量保证期为叁年[自项目终验合格之日起算]，在此期间乙方提供免费维护，并承诺[15]分钟内响应，乙方故障受理热线为[4008280858]。但对于由于不可抗力，如火灾、水灾、台风、雷击、地震、战争、政府禁令等不能预见、不能完全避免并不能完全克服的客观情况或非乙方原因造成损害的，乙方提供收取材料成本的免人工费用的维护。

7.2 质保期满后，乙方提供有偿维护，收取成本（人工）费。

八、违约责任

8.1、乙方保证为甲方提供的设备、材料为正规渠道产品，若验收时发现存在质量问题的，乙方负责予以更换或退货；乙方保证项目的施工质量，若验收不合格的，乙方负责无偿整改或返工。

8.2 甲方若逾期不支付乙方合同款，每逾期一周，应向乙方支付合同总额的[千分之三]作为逾期违约金，不足一周按一周计。甲方支付逾期违约金，并不免除其支付合同款的义务。

8.3 若因乙方责任影响进度，每延迟一周，乙方按合同总额的[千分之三]向甲方支付逾期违约金，违约金累计不超过合同总价的[5]%；若因不可抗力、甲方原因或第三方原因影响进度，工期相应顺延，乙方不承担责任。

8.4 甲方不按合同约定履行自己的各项义务导致工期延误的，除乙方工期顺延外，每逾期一天，甲方应按合同总金额的[千分之三]向乙方支付逾期违约金。若导致合同无法履行的，甲方还应赔偿乙方因此而遭受的损失，包括但不限于因甲方违

约给乙方造成的停工、窝工等损失及其他因其违约导致乙方增加的经济支出和从应支付之日起计算的应付款项的利息等。

8.5 任何一方可在违约事项发生后[10]个工作日内，向对方发出要求索赔的通知，对方在接到索赔通知后[5]个工作日内给予答复，对方在[5]个工作日内未予答复，应视为该项索赔已经被接受。

第九条 法律适用和争议解决

9.1 本合同适用中华人民共和国法律。

9.2 所有因本合同引起的或与本合同有关的任何争议将通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可采取下述第[1]种争议解决方式：

（1）将该争议提交[项目履行地]仲裁委员会，按照申请仲裁时该会的仲裁规则进行仲裁。仲裁裁决是终局的，对双方均有约束力。仲裁费用由败诉方承担。

（2）向乙方所在地有管辖权的人民法院起诉。

9.3 仲裁或诉讼进行过程中，双方将继续履行本合同未涉仲裁或诉讼的其它部分。

第十条 合同生效及其他

10.1本合同自双方签字盖章之日起生效。

10.2本合同一式[7]份，甲乙双方各执[3]份，1份交常州市政府采购中心存档备案，具有同等法律效力。

10.3任何一方未经另一方同意，不得向任何第三方透露本合同的签订及其内容。乙方向其关联公司透露的，不在此限。

10.4任何与本合同相关但未在本合同中明确规定的事项将由双方另行友好协商解决。对本合同做出的任何修改和补充应为书面形式，由双方签字盖章后成为本合同不可分割的部分。本合同与其补充合同或补充协议冲突时，以补充合同或补充协议为准。

10.5未得到对方的书面许可，一方均不得以广告或在公共场合使用或摹仿对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写，任何一方均不得声称对对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写拥有所有权。

10.6本合同的任何内容不应被视为或解释为双方之间具有合资、合伙、代理关系。

10.7本合同替代此前双方所有关于本合同事项的口头或书面的纪要、备忘录、合同和协议。

10.8双方因履行本合同或与本合同有关的一切通知都必须按照本合同中的地址，以书面信函形式或双方确认的传真或类似的通讯方式进行。采用信函形式的应使用挂号信或者具有良好信誉的特快专递送达。如使用传真或类似的通讯方式，通知日期即为通讯发出日期，如使用挂号信件或特快专递，通知日期即为邮件寄出日期并以邮戳为准。

合同编号：JSHXS2204084CGN00

甲方：江苏省常州市人民检察院
地　址：常州市永宁北路 10 号
联系人：陈兴生
电　话：0519-85336261
传　真：
邮　编：

乙方：中电鸿信信息科技有限公司
地　址：南京市玄武大道 699-1 号
联系人：董科
电　话：18961235188
传　真：
邮　编：

9.9 附件为本合同不可分割的部分。若附件与合同正文有任何冲突，以合同正文为准。

本合同附件为：

附件：硬件设备及相关材料清单

甲方：江苏省常州市人民检察院
法定代表人/负责人
或授权代表(签字)：

年　月　日

乙方：中电鸿信信息科技有限公司
法定代表人/负责人
或授权代表(签字)：

年　月　日 2022.10.25

附件：硬件设备及相关材料清单

序号	分项名称	品牌商标	规格型号	技术参数	数量	单位	投标价格	
							单价	合价
1	核心交换机	H3C	S7506X-S-MF	业务插槽数≥6 整机交换容量≥76Tbps，整机包转发率≥8640Mpps（如官网指标出现两个值，以最小值为准） 冗余主控、冗余模块化电源 支持标准和扩展 ACL，支持基于 VLAN 的 ACL，支持 Ingress/Egress ACL 支持层次化 QoS（H-QoS），支持三级队列调度，支持队列调度机制，包括 SP、WRR、SP+WRR、WFQ，支持拥塞避免机制，包括 Tail-Drop、WRED 支持 CPU 保护技术，支持 VRRP，支持热补丁，支持硬件 BFD 支持 MAC Tracert，支持 Graceful Restart for OSPF/BGP/IS-IS 以太网支持千兆电口，千兆光口，万兆光口、万兆电口，25G 端口、40G 端口。 支持 RIPng、OSPFv3、BGP4+、IS-ISv6 协议，支持 IPv6 策略路由 支持 DHCPv6 功能、IPv6 portal 功能、IPv6 管理功能 支持基于 IPv6 的 VXLAN 二三层互通 支持创建、删除虚拟交换机，将虚拟化系统虚拟成多台交换机实现用户表项叠加，支持物理设备虚拟化实现负载分担，提供工信部权威第三方测试报告。 支持安全业务插卡，包含防火墙、负载均衡、应用控制网关、IPS、SSL VPN 等独立板卡，并提供官网选配信息证明。 支持 Telemetry 流量可视化功能。 支持融合无线 AC 功能，无需独立的 AC 业务板卡，即支持无线 AP 管理功能。 支持通过 Python/NETCONF/TCL 等对网络自动化编排，实现 DevOps 自动化运维。 内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级，提供工信部权威第三方测试报告。 支持 L3 VPN，支持 VLL，支持 VLPS，支持 MCE。	1	台	180000	180000

				支持 IEEE 802.1ae 介质访问控制安全技术。 ★实配双主控，双 1400W 电源，千兆电口≥48，千兆光口≥48，万兆光口≥20，三年质保，要求与现有核心交换机进行双机虚拟化。				
2	防火墙（万兆）	深信服	FW-2000-X210（万兆）V2.0	★产品应用多核并行处理架构，并采用国产处理器和国产操作系统。 性能参数：网络层吞吐量≥39Gbps，应用层吞吐量≥9Gbps，并发连接数≥4000 万，新建连接数（CPS）≥23 万。 ▲硬件参数：规格：2U，内存大小≥16G，硬盘容量≥128GB SSD，电源：冗余电源，接口≥6 千兆电口+4 千兆光口 SFP+4 万兆光口 SFP+。含 4 个万兆多模光模块。 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；支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 支持僵尸网络检测功能，防止失陷主机威胁内网扩散，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“僵尸网络检测”的相关证书。 具备至少对 ARP Flood、ICMP Flood、SYN Flood、DNS Flood、UDP Flood 等泛洪类攻击防护的能力，并支持 IP 地址扫描和端口扫描攻击防护；支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御。 具备识别与阻断，外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“漏洞防扫描”的相关证书。 ▲产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护，产品支持≥7200 种特征规则数量。 支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等等检测和防护 ▲产品具备 Web 应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含 SQL 注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL	2	台	175000	350000

				后门攻击、跨站请求伪造、目录遍历攻击、WEB 整站系统漏洞等应用层攻击行为，安全特征规则≥3320 种。（提供产品功能截图证明） 产品支持对多重压缩文件的病毒检测能力，支持不小于 12 层压缩文件病毒检测与处置。 支持主备、主主两种模式 ▲产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括 DNS 解析、ARP 探测和 PING 方式。				
3	运维安全管理系统（堡垒机）	天融信	TopSAG（ZX-A）V3	▲采用国产 CPU，主频不低于 2.0GHz，4 核 ▲2U 机箱，千兆电口≥6 个，千兆光口≥4 个，内存 16GB，硬盘 1TB。2 个可插拔的扩展槽，标配模块化双电源。 100 个主机/设备许可；用户数不限制； 采用物理旁路部署，不改变现有网络结构 支持用户的增删改查、锁定、激活，进行用户全生命周期管理，支持用户批量导入和导出 采用三员管理，支持系统管理员、安全审计员和安全操作员，并且三员之间权限相互制约 用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP 认证、RADIUS 认证、USBKEY 认证、OTP、短信认证等身份认证方式；支持可知因素和不可知因素的双因素认证。 支持中标麒麟、银河麒麟、Windows 等操作系统，支持网络设备、安全设备、数据库等的资产管理 支持修改管理协议默认端口（提供产品功能截图证明） 支持资产的批量导入导出（提供产品功能截图证明） 支持资产组的增删改查 支持资产账号手动添加，支持账号的批量导入导出 自动对 Windows、Linux 等设备进行账号改密，改密支持手动和定期任务，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成（提供产品功能截图	1	台	108000	108000

				证明） 支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权 支持会话、指令、剪切板上下行、文件上传下载的约束行为； 支持用户会话超时退出；支持用户密码连续鉴权失败锁定，到期自动解锁；支持用户强密码策略，密码长度 8 位以上，包含字母、数字、特殊字符等；支持对用户登录 IP 地址、MAC 地址、时间的限定 支持对运维时间、运维地址、运维操作指令的限定，触发策略后进行告警 支持管理员自定义幽灵账号开启和关闭 支持自动发现运维人员运维过程中创建的后门账号行为，并以列表方式向设备管理员展示托管设备中所有的后门账号信息。 设备访问支持最新的 html5 技术，在同一 WEB 窗口页签中，无需 JAVA 应用插件或调用本地应用客户端，即可实现对目标设备的快速运维； 支持 SecureCRT、XShell、WinSCP 等客户端直接连接堡垒机进行代理运维目标资产 支持对用户和管理员的认证登录、操作和配置管理进行日志记录 支持对 Windows、VNC 等图形界面的运维操作进行录屏审计，支持图形和字符协议的视频回放 支持对图形和字符协议的操作进行文本记录，如鼠标操作、文本内容操作等，Linux 命令操作等（提供产品功能截图证明） 支持对在线会话的实时监控和即时阻断，避免违规操作 支持全文审计检索。可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯。 报表针从会话、指令等多个维度进行统计； 系统内置丰富报表统计模板：协议运维排名、资产运维次数 top10、资产运维趋势 top10、用户运维趋势 top10、协议运维趋势、用户运维次数 top10、指令分布 top10、top10 指令资产分布、指令用户分布 top10、指令资产账号分布、指令排名、指令				

				趋势、风险指令次数、风险指令 top10 等多种类型报表模板。 支持 HTTPS 方式和 Console 方式进行管理 支持管理口与业务口分离（提供产品功能截图证明） 支持将本机日志、告警日志通过 SYSLOG、邮箱等进行外发和告警 支持配置数据和审计数据的备份、自动清理，支持备份数据通过 FTP 方式远程备份 支持配置时间同步服务器，进行时间自动校对，保障审计的有效性和准确性				
4	日志审计	天融信	TA-LOG （FT-A20）V3	▲产品采用国产处理器和国产操作系统，主频不低于 2.0GHz，64 核 ▲2U 机架式设备，千兆电口≥2 个，万兆光口≥2 个（含 2 个万兆多模光模块）； 采集处理峰值≥20000EPS，日志源数量≥100。 支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等。 支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；（提供产品功能截图证明） 支持对每个日志源设置过滤条件规则，自动过滤无用日志； 支持日志转发给第三方系统平台，支持设置多个日志转发 IP 地址，支持转发格式化日志或仅转发原始日志； 支持 IPv6/IPv4 双栈环境部署，对 IPv6/IPv4 日志源的日志进行高速采集； 支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储、网络存储； 支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数；（提供产品功能截图证明） 支持 IPv6 日志的全量存储；（提供产品功能截图证明） 支持为不同类型日志设置不同的查询条件和显示条件；（提供产品功能截图证明） 支持原始日志全文检索；查询结果可将归一化日志和原始日志同屏对比显示； 支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析； 支持多种运维管理工具，可对日志源进行 HTTP、HTTPS、SSH、SCP、SFTP、FTP、MYSQL、ORACLE、SQLSERVER 等操作。（提供产品功能截图证明） 支持首页展示当日告警情况统计；支持展示当日最新告警 TOP10、TOP30 和 TOP50；	1	台	108000	108000

				内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别。 支持安全告警概况、安全告警趋势的统一展示，实时告警可根据级别、规则类型等进行分类； 支持实时告警展示，可根据告警规则、告警级别两个维度进行实时告警监视，并可对刷新事件间隔进行设定；（提供产品功能截图证明） 支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备 IP、源 IP、目的 IP 等方式快速检索安全事件告警，检索结果支持 Excel 等格式导出； 支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析； 支持在告警事件查询界面直接显示触发告警的关联日志，也支持点击跳转到日志查询界面。 支持告警抑制规则设定，防止报警信息短时间内大量发送。 系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应；（提供产品功能截图证明） 支持自定义统计日志数据形成报表，支持统计分析报表以 PDF、word、execl、html 等方式导出；支持实时报表、计划报表。 支持手动添加日志源，管理员可以对日志源进行查看、批量修改、添加、编辑、删除以及启\禁用的操作； 支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息；（提供产品功能截图证明） 系统内置常见安全事件关联分析规则； 系统内置多种维度的数据在线分析模型，在数据查询结果界面直接对查询结果数据进行多维度在线数据分析，分析结果实时展示，分析模型包括但不限于树图、散点图、关系图、折线图、时序图、柱状图等。 支持用户按角色管理，支持三权分立； 支持将日志源管理权限分配给不同的操作管理员，不同用户管理不同日志源的日				

				志，互不干扰； 支持设置非法用户访问控制策略； 系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。 支持将常用 IP 地址或 IP 地址网段标记为自定义名称，在日志查询界面可以在 IP 列中对应悬浮显示自定义名称；				
5	链路检测	H3C	SWP-IMC7-IMP	国产品牌，与核心交换机同一品牌 支持自动发现网络中的所有网络设备，并在拓扑中显示出来支持拓扑图自定义修改，包括设备、链路等。 支持面板视图视图，设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态；并提供基于设备面板的设备、单板、端口配置功能。（提供产品功能截图证明） 接收 Syslog，完成基本格式的解析，并入库。提供 Syslog 特征分析及策略注册能力，支持基于统计规则进行聚合生成告警（Trap） 支持批量的设备配置备份和恢复。支持向导方式或者任务方式（周期性任务、一次性任务或立即任务）批量的备份、恢复完整的配置文件，也可以批量的下发配置片断。 支持设备配置集中管理：配置库包括配置文件和配置片断，配置内容可带有参数，在部署时根据设备的差异设置不同的值；配置文件可部署到设备的启动配置或者运行配置；配置片断只能部署到设备的运行配置； 实现网络 IP 地址自动扫描、统计、分配和管理，同时允许用户手工分配和管理 IP 地址，以达到更加灵活的分配管理。结合 IP 地址段的管理功能，将整个网络的 IP，划入各个不同的 IP 地址段，分别进行管理，并给出详细直观的 IP 分配情况统计图表，使管理员能清楚的了解和掌握整个网络的 IP 使用情况。（提供产品功能截图证明） 支持设备软件智能升级。支持网络运行设备的软件版本查询功能，支持先备份后升级，保证一旦升级失败后可以恢复到原有设备软件版本，支持对整个升级过程的可	1	套	50000	50000

				靠性检查，如设备软件版本和设备是否配套，flash 空间是否足够等，确保用户的整个升级操作万无一失。支持不间断业务的软件升级 ISSU。 新设备注册，告警注册，新性能指标注册，新 Syslog 解析注册，Mib 编译，第三方设备配置管理-CLI 下发，配置管理-配置备份、软件升级（使用 TCL/ Expect /Perl 模板自定制），第三方设备管理系统集成。 平台提供有网络基础管理视图、分级管理视图、快捷业务视图、桌面视图。视图切换方便。极大提高菜单易用性。创建操作员时可以指定有权限的视图和默认登录视图 投标产品厂商须具备 CMMI(软件能力成熟度模型集成)5 级或以上认证评估，并提供相应证书复印件。 网络设备管理 license≥100，要求能够对大楼原有网络设备进行管理，可以远程对网络设备端口进行 UP 和 DOWN 管理。				
6	漏洞扫描服务	定制	定制	对网络进行漏洞扫描工作，配合做好漏洞指导整改、复测工作。	6	次	2000	12000
7	等保三级测评费	定制	定制	委托具备资质的第三方信息安全等级测评机构（以下简称“测评机构”）对采购人的信息系统进行信息等级保护三级测评，按照信息安全等级保护制度建设要求提出安全整改建议形成《安全整改建议书》，待采购人根据《安全整改建议书》组织完成整改后，测评机构再依据依照《信息系统安全等级保护基本要求》（GB/T 22239-2019）进行复测，验证安全整改的结果，最终出具《信息系统安全等级测评报告》。	1	次	80000	80000
8	三年原厂升级服务（山石）	定制	定制	提供现有山石入侵防御系统（一台） 三年原厂升级服务	1	项	35000	35000
9	三年原厂升级服务（瑞星）	定制	定制	提供现有瑞星下一代网络版杀毒软件三年原厂升级服务	1	项	45000	45000
合　　计								968000

保密协议

甲方：常州市人民检察院
乙方：中电鸿信信息科技有限公司

为保守国家秘密，维护国家安全和利益，甲、乙双方签订保密协议如下：

一、甲方承担的保密责任：

负责对乙方施工人员进行保密宣传教育，使乙方知悉与其业务有关的保密规定。

二、乙方承担的保密责任：

乙方在维修过程中严格遵守下列保密守则：

1、不私自询问、查看、摄录、复制、存储、传播国家秘密。

2、维修过程中不得擅自将乙方设备接入甲方信息系统。

3、不得擅自更改甲方信息系统中的配置信息。

4、在实施过程中存储涉密信息设备时，需将存储过涉密信息的硬件或部件拆除，并交于甲方保管。

维保单位人员如违反本责任书的条款，甲方将根据国家保密法律法规进行处理，情节严重者转交常州市保密行政管理部门。

三、本责任书未尽事宜，按照国家保密法律法规以及涉密信息系统有关保密规定执行。

四、本责任书自签字之日起生效。责任书一式三份，甲方负责设备维保部门和保密管理部门（备案）各一份，乙方一份。

甲方
（盖章）
年 月 日

乙方
（盖章）
年 月 日