常州市政府采购合同（合同编号）

项目名称：江苏省常州市中级人民法院信息化设备外包运行维护服务项目

项目编号：JSZC-320400-JZCG-C2024-0504

甲方：（买方）江苏省常州市中级人民法院

乙方：（卖方）中国电信股份有限公司常州分公司

甲、乙双方根据常州市政府采购中心江苏省常州市中级人民法院信息化设备外包运行维护服务项目竞争性磋商的结果，签署本合同。

一、合同内容

1.1 标的名称：江苏省常州市中级人民法院信息化设备外包运行维护服务项目

1.2 标的质量：见附件《分项报价表》

1.3 标的数量（规模）：见附件《分项报价表》

1.4 履行时间（期限）：一年（2025 年 1 月 1 日至 2025 年 12 月 31 日）

1.5 履行地点：江苏省常州市中级人民法院

1.6 履行方式：服务，详见附件《分项报价表》

二、合同金额

2.1 本合同金额为（大写）：壹佰柒拾柒万圆（1770000 元）人民币，其中：网络安全服务费为 620000 元，开具 6%的增值税发票；云集成服务费为 1150000 元，开具 6%的增值税发票。。

三、技术资料

3.1 乙方应按磋商文件规定的时间向甲方提供与合同标的有关的技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同标的或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付的合同标的的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

本项目不收取履约保证金。

6.1 乙方交纳人民币____/____元作为本合同的履约保证金。（不得超过合同金额的

5%）。供应商可以自主选择以支票、汇票、本票、保函（保险）等非现金形式交纳或提交，按照省市有关文件精神，鼓励优先采用电子履约保函（保险）形式。

6.2 合同履行结束后，甲方应及时退还交纳的履约保证金。

6.2.1 履约保证金退还方式：

6.2.2 履约保证金退还时间：

6.2.3 履约保证金退还条件：

6.2.4 履约保证金不予退还的情形：

七、合同转包或分包

7.1 乙方不得将合同标的转包给他人履行。

7.2 乙方不得将合同标的分包给他人履行。

7.3 乙方如有转包或未经甲方同意的分包行为，甲方有权解除合同。

八、合同款项支付

8.1 分期付款：合同签订并收到发票后 10 个工作日内，支付合同金额的 80%。服务结束、验收合格并收到发票后 10 个工作日内，支付合同金额的 20%。满足合同约定支付条件的，自收到发票后 10 个工作日内支付。

九、税费

9.1 本合同执行中相关的一切税费均由乙方负担。

十、项目验收

10.1 甲方依法组织履约验收工作。

10.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

10.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

10.4 如有必要，甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收书的参考资料。

10.5 甲方成立验收小组，按照采购合同的约定对乙方的履约情况进行验收。验收时，甲方按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，验收小组出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料存档备查。

10.6 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

十一、违约责任

11.1 甲方无正当理由拒绝接受乙方提供的合同标的的，甲方向乙方偿付拒绝接受合同价款总值 5%的违约金。

11.2 甲方无故逾期验收和办理合同款项支付手续的，甲方应按逾期付款总额千分之六每日向乙方支付违约金。

11.3 乙方逾期交付合同标的的，乙方应按逾期交付合同总额每日千分之六向甲方支付违约金，由甲方从待付合同款项中扣除。逾期超过约定日期 10 个工作日不能交付合同标的的，甲方可解除本合同。乙方因逾期交付合同标的或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同价款总额 5% 的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

11.4 乙方交付合同标的的标准不符合合同规定及磋商文件规定标准的，甲方有权拒绝接受合同标的，并可单方面解除合同。

十二、不可抗力事件处理

12.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响 期相同。

12.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

12.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十三、解决争议的方法

13.1 双方在签订、履行合同中所发生的一切争议，应通过友好协商解决。如协商不成，可提交常州仲裁委员会仲裁，仲裁裁决应为最终裁决，对双方均具有约束力。仲裁期间，合同无争议部分继续履行。

十四、合同生效及其它

14.1 合同经双方法定代表人或授权委托代表人签字并加盖单位公章后生效。

14.2 本合同未尽事宜，遵照《民法典》、《政府采购法》有关条文执行。

14.3 本合同正本一式五份，具有同等法律效力，甲方、乙方各执二份，财政监管部门执一份。

甲方：江苏省常州市中级人民法院

地址：常州市永宁北路 6 号

法定代表人或授权代表：

联系电话：

签订日期：　　年　　月　　日

乙方：中国电信股份有限公司常州分公司

地址：常州市和平北路 29

法定代表人或授权代表：

联系电话：

2025 年 01 月 09 日

附件：《分项报价表》

分项报价表

序号	服务名称	服务内容	单位	数量	单价	总价
1	桌面终端软硬件维护	1、服务内容 负责对采购人的 750 台台式电脑、168 台笔记本电脑、250 台激光打印机、7 套智慧诉讼服务中心自助服务终端及系统、4 套 24 小时法院自助设备、1 套中间柜及其他相关终端设备（以下简称桌面终端设备）的日常维护工作。内容包括： 1）提供对 PC 机 Windows、麒麟、统信等操作系统进行安装及相关的基础排错服务； 2）提供对 PC 机应用软件的安装服务（采购人提供应用软件介质）及常用办公系统软件的维护服务； 3）提供对 PC 机接入采购人内部网络的服务； 4）PC 系统数据迁移备份和恢复（采购人提供需备份的数据列表）； 5）提供瑞星网络防杀病毒软件的定期升级服务； 6）打印机、扫描仪等外设的安装（采购人提供驱动程序）服务； 7）对采购人新购置设备的安装调试，包括：升级内存、升级硬盘、安装打印机耗材等； 8）协助负责对采购人工作人员的网络应用操作培训； 9）负责协调相关的产品厂家共同解决采购人 PC 应用中出现的问题； 10）对智慧诉讼服务中心智能化设备（主要包含：诉讼服务自助终端、叫号系统、智能送达终端、辅助填单终端、案件查询终端等）、智能中间柜设备进行日常使用维护； 11）每月向采购人提交一份软硬件系统设备的运维报告，报告内容包括：软、硬件系统设备故障原因，解决方法，解决周期；网络防病毒软件升级，确保病毒特征库是最新的；提供相关的技术支持服务等。 2、服务要求 ★供应商至少选派 2 名固定的技术熟练的计算机维护人员常驻采购人现场服务，无特殊原因不能更换人员，驻场服务人员参照常州中院正常工作时间定点上下班，不得出现无故离岗、旷工等情况，在工作时间内，服从采购人管理人员的调遣；非工作日接到故障电话后 2 小时内到现场（紧急事件 1 小时到场）。本项目配备的桌面终端软硬件维护 2 名驻场运维人员与网络设备软硬件维护 1 名驻场运维人员、网络安全设备软硬件维护 1 名驻场运维人员不能重复。（供应商提供承诺函并加盖供应商公章） 供应商还需满足以下要求：	项	1	290000	290000

		1）签订保密协议，对采购人的所有电子信息负有保密责任。 2）对本项目内各个设备、系统进行每日巡检，发现问题及时处理，保证各设备、系统每日正常运行； 3）相关耗材用完时需及时进行更换； 4）对各设备、系统进行定期病毒检测杀毒、打补丁、系统更新等，保证各系统运行的安全及流畅性 5）驻场维护人员需经过相关产品厂家技术培训方可上岗，否则采购单位有权要求更换服务人员。 6）保密要求：本项目所有运维人员及相关人员应严格履行保密义务，接受采购单位的监督管理，对在本项目实施运维过程中所掌握的商业及工作秘密，包括业务数据、业务需求、文档资料、技术成果和客户信息等负有保密义务，未经授权，不得修改、泄露、利用、转让、销毁或许可他人使用。				
2	计算机打印机维保	1、服务内容 负责对采购人的750台台式电脑、168台笔记本电脑、250台激光打印机的日常维保工作。内容包括： 1）对采购人上述计算机、打印机中损坏的设备进行维修或送修服务，损坏设备的所有固有配件免费维修（不包括硒鼓、墨盒等耗材，耗材及配件升级需另行付费购买）（供应商提供承诺函并加盖供应商公章）； 2）每季度向采购人提交一份计算机、打印机维保报告。 2、服务要求 供应商接到报障电话后2小时内到现场（紧急事件1小时到场），48小时内完成故障设备的维修。（供应商提供承诺函并加盖供应商公章） 供应商还需满足以下要求： 1）签订保密协议，对采购人的所有电子信息负有保密责任。 2）保密要求：本项目所有维修人员及相关人员应严格履行保密义务，接受采购单位的监督管理，对在本项目实施运维过程中所掌握的商业及工作秘密，包括业务数据、业务需求、文档资料、技术成果和客户信息等负有保密义务，未经授权，不得修改、泄露、利用、转让、销毁或许可他人使用。	项	1	100000	100000
3	服务器软硬件维保	1、服务内容 负责对采购人100台服务器的日常运维和维修工作。内容包括： 1）提供对服务器操作系统进行安装及相关的基础排错服务； 2）提供对服务器接入采购人内部网络的服务； 3）服务器系统数据迁移备份和恢复（采购人提供需备份的数据列表）； 4）协调应用开发商共同解决采购人服务器应用中出现的问题，协助应用开发商制订业务系统级的优化方案； 5)每月对服务器进行一次全面巡检，检查服务器是否正常运行，是否有指示硬件故障报警；检查操作系统，通过查看系统日志等方式分析判断系统的运行状况；检查服务器卷组信息、文件	项	1	240000	240000

		系统、日志状态；检查内存、CPU、磁盘、网络等的使用情况，记录异常信息；分析判断服务器可能存在的故障隐患及原因，第一时间向采购人提出修复、改善建议；提供服务器系统软件咨询服务，包括系统升级扩容方案，系统软件运行过程中的各种技术问题等。 6）对采购人损坏的服务器进行维修或送修服务，损坏服务器的所有固有配件免费维修（配件升级需另行付费购买）（供应商提供承诺函并加盖供应商公章）； 7）每月向采购人提交一份服务器软硬件维保报告。 2、服务要求 供应商接到报障电话后2小时内到现场（紧急事件1小时到场），48小时内完成故障设备的维修。（供应商提供承诺函并加盖供应商公章） 供应商还需满足以下要求： 1）签订保密协议，对采购人的所有电子信息负有保密责任。 2）保密要求：本项目所有维修人员及相关人员应严格履行保密义务，接受采购单位的监督管理，对在本项目实施运维过程中所掌握的商业及工作秘密，包括业务数据、业务需求、文档资料、技术成果和客户信息等负有保密义务，未经授权，不得修改、泄露、利用、转让、销毁或许可他人使用。				
4	网络设备软硬件维护	1、常驻服务 ★供应商必须选派1名固定的技术熟练的计算机网络维护人员常驻采购人现场服务，无特殊原因不能更换人员，驻场服务人员参照常州中院正常工作时间定点上下班，不得出现无故离岗、旷工等情况，在工作时间内，服从采购人管理人员的调遣；非工作日接到故障电话后2小时内到现场（紧急事件1小时到场）。供应商须签订保密协议，对采购人的所有电子信息负有保密责任。本项目配备的网络设备软硬件维护1名驻场运维人员与桌面终端软硬件维护2名驻场运维人员、网络安全设备软硬件维护1名驻场运维人员不能重复。（供应商提供承诺函并加盖供应商公章） 2、基础设施运维管理：根据维保设备清单中列明的网络设备提供维护、技术支持服务和运维管理服务，通过对设备定期进行规范化的预防性维护，提高系统与设备的可靠性、稳定性及可使用率；对存在问题及突发故障提供及时有效的技术支持、完善的解决方案和事后防范机制，减低故障对生产的影响，使系统与设备保持或迅速恢复其良好的工作状态，消除产生故障的薄弱环节，使系统与设备更趋于稳定、安全、合理和高效；负责网络维护、解决网络故障，保证网络正常工作；优化采购人网络，使其始终保持高速的数据传输能力，排除不安全隐患。 3、资产数字化管理：加强信息化资产包括应用系统资产整理能力，实施数字化资产整理服务，将目前所有的软硬件资产、外围线路资源、拓扑结构、系统架构、端口、应用数据信息梳理	项	1	175000	175000

		清楚。对大量基础设施进行统一管理、统筹分配形成专有信息资产库，结合完整的信息化资产整理规范，综合查看所有（机房、机柜、设备等）的软硬件配置、工作配置文件、质保时间、维修记录、服务工单、日常维护记录、巡检记录、运维知识库等，并能提供各种安全便捷的方式查看相关资料（电脑终端、微信端等），从而提高基础设施安全运维效率，保障整体网络的安全平稳运行。供应商应能提供相关数字化运维管理系统工具软件，包含资产查询机房机柜设备等、机房巡检、设备巡检、日常事件管理、服务工单管理、移动端运维服务管理等功能模块。 4、信息化基础架构整体优化部署：结合采购人现有的所有业务应用系统、实际业务需求，需不断优化现有基础设施软硬件设备的运行模式，并根据业务系统实际运行情况提出安全优化部署建议，根据采购人相应实施方案对信息化基础设施进行部署，重点对现有核心网络设备、核心存储设备、虚拟化平台等进行安全性、功能性优化，在保障基础设施重要设备得到充分利用的前提下，进一步提高业务系统的稳定性、安全性，增强虚拟化平台及相关存储的性能及稳定性，保障网络基础架构的高可用性，避免业务中断，增加网络稳定性及可靠性，同时，还须配合采购人做好服务期内机房及弱电井内线路整理工作，保证物理线路也得到充分优化及保障，使采购人的信息化基础设施安全保障工作达到一个更高的标准。 5、通讯链路检查排障：网络的健康状况整体运行状态、各项硬件资源开销状况、链路健康状况如端到端时延变化、链路端口工作稳定性、链路负载百分比、部署路由策略情况下端到端选路变化、路由条目变化、管理权限用户的行为审计、设备软件配置变动审计、设备日志审计、安全事件审计等，需根据采购人要求定期提供各种机房、系统、设备对应的数字化巡检报告，积极配合下属单位进行网络构架调整和故障处理，减少网络变更的风险。 6、关键基础设施资源技术支持：采购人现有基础设施资源中深信服云桌面、深信服超融合等软硬件设备都是信息化基础设施安全运行中的重要关键设施，为了保障业务系统的稳定运行，供应商需要协助采购人在后续的安全运维服务、网络优化、系统优化过程中，与原厂工程师协同提供高效、可靠、安全的运维服务，保障采购人现有基础设施资源在根据业务系统不断调整优化的过程中，还可以稳定可靠的提供高质量的设备运行维护质保服务。 7、供应商每季度进行一次网络设备软硬件巡检，提供巡检报告，与采购方有关负责人员和技术人员研讨网络设备软硬件系统运行状况、全面检查系统的工作状态、对系统的运行环境进行评估、现场解答采购人技术人员的有关网络软硬件、网络规划等技术方面的问题。				

5	网络安全设备软硬件维护	1、常驻服务 ★供应商必须选派 1 名固定的技术熟练的网络安全维护人员常驻采购人现场服务，无特殊原因不能更换人员，驻场服务人员参照采购人正常工作时间定点上下班，不得出现无故离岗、旷工等情况，在工作时间内，服从采购人管理人员的调遣；非工作日接到故障电话后 2 小时内到现场（紧急事件 1 小时到场）。供应商须签订保密协议，对采购人的所有电子信息负有保密责任。本项目配备的网络安全设备软硬件维护 1 名驻场运维人员与桌面终端软硬件维护 2 名驻场运维人员、网络设备软硬件维护 1 名驻场运维人员不能重复。（供应商提供承诺函并加盖供应商公章） 在整个服务期限内，每月向采购人提交一份网络安全系统运维报告。内容包括：网络安全系统的故障原因、解决方法、解决周期；对网络安全系统的升级与维护提供相关的技术支持服务等。 2、日常服务 全面检查、处理网络安全系统运行情况，检测潜在隐患，把故障消灭在未然之时。对网络安全设备及系统每个季度进行巡检服务。 3、紧急事件响应服务 如遇重大紧急故障处理等服务事项，供应商必须提供多人、快速的服务响应，并确保问题在 8 小时内找到妥善解决办法。 具体包括：1）大面积计算机瘫痪事件； 2）大面积病毒爆发，导致无法正常工作； 3）其他相关事件。 4、终端侦测与响应系统维保服务 1）提供原厂软件升级服务； 2）提供 7*24 小时的安全攻击事件分析/处置服务 3）每季度提供一次终端侦测与响应系统巡检，同时提供系统巡检报告。 5、网络安全态势感知系统维保服务 1）安全态势感知系统 供应商应提供目前采购人使用的 1 套深信服安全态势感知系统维保服务 1 年，同时享受 1 年的原厂质保，包括软硬件升级和运维。 2）技术支持服务 本次维保服务中，技术支持服务部分要求提供原厂的 7x24 小时的电话和远程调试服务，响应时间为 1 小时，通过电话指导、远程调试等方式确保采购人的技术问题能获得原厂技术专家直接的处理和跟踪，直至确保问题最终得到解决。 3）质保服务 本次维保服务中，产品质保部分要求提供原厂的硬件保修服务。发生故障时，2 小时内原厂技术人员需到达现场，现场修复故障设备或提供备件，4 小时内需恢复正常。如硬件故障无法现	项	1	320000	320000

		场解决，由中标单位寄回故障设备，原厂收到故障设备后 20 个工作日（如遇节假日则顺延）内将维修好的硬件设备或部件送还到采购人。 4）软件升级 本次维保服务中，软件升级部分要求提供硬件设备同等功能软件版本更新、升级，以及该软件版本配套的文档资料、用户手册。升级后采购人将享有新版本软件的使用权利。 5）现场服务 本次维保服务中，现场部分要求提供原厂的现场产品技术使用支持、问题处理服务。 6）巡检服务 本次维保服务中，巡检服务部分要求提供原厂的巡检服务，原厂专业技术人员每个季度上门对产品功能及现场环境进行全面的检测分析，如有重大使用隐患，在分析后，给出后期产品稳定性及应用功能优化建议报告。 6、云桌面系统管理（深信服） 云桌面服务器故障维护（文件备份，恢复等）；瘦客户端故障维护（包括系统安装，系统还原，系统更新，常用软件安装）。 7、数据备份与恢复 每周配合采购人对云桌面备份数据的准确性、完整性进行检查，故障发生后可通过备份数据及时恢复，保证数据不丢失。 8、安全检查服务 每季度针对常州全市法院整体网络安全策略和设备等进行巡检，发现存在的问题并提出建议，并协助采购人进行加固。 9、主机防护安全巡检 用户权限与访问控制策略是否安全；是否及时更新操作系统补丁程序；系统日志管理是否完备，对现有对主机系统进行日志分析审计。 10、系统运行安全巡检 是否指定系统运行值班操作人员；是否提供常见和简便的操作命令手册；是否对运行值班过程中所有现象、操作过程等信息进行记录；是否有信息系统运行应急预案。 11、防病毒安全巡检 安装防病毒软件覆盖率是否达到 100%；是否对关键服务器实时查、杀毒，对用户端定期进行查、杀毒，并备有查、杀记录；是否有专责人员负责严重病毒的通告及病毒库及时更新；是否限制从网上随意下载软件；外来设备（硬盘、U 盘等）使用前是否进行杀毒处理等。				
6	网络安全服务	为准确识别信息安全各种风险和威胁，规避或减少信息安全事件造成的不良影响和损失，供应商应提供以下网络安全服务。供应商须根据信息安全风险级别，运用科学方法和手段，系统地分析网络和信息系统所面临的威胁及其脆弱性，评估安全事件一旦发生可能造成的危害程度，提出针对性的信息安全解决	项	1	180000	180000

		方案和加固建议，为网络、软硬件系统的安全与稳定运行提供有力的保障。 供应商须通过专业的安全服务和管理，及时协助信息安全管理人员发现和处理服务范围内的设备及系统安全事故，提供有针对性的安全咨询及安全规划方案，最大限度保障网络和信息安全。 1、应用系统漏洞扫描及安全渗透测试服务 检测范围：采购人所有互联网 IP 地址，检测频率：每半月一次。 采用主动防护的手段，每半月对采购人所有外网 IP 地址通过工具和人工检测的方式进行漏洞扫描，查找脆弱性风险，并提交《信息系统安全弱点评估报告及信息安全风险整改方案》。通过真实模拟黑客使用的工具、分析方法来进行实际的漏洞发现和利用的安全测试方法，并配合系统开发商做好漏洞整改、复测工作。 2、安全检查服务 检查频率：在服务期内根据采购人需求动态响应。 服务期内提供重要信息系统版本升级和功能增加及新系统上线前的安全测试服务，加强上线发布流程中安全测试环节的检测力度。（供应商提供承诺函并加盖供应商公章） 通过 web 扫描、漏洞扫描、漏洞验证等手段，对业务系统上线前进行脆弱性评估，识别业务系统安全脆弱性风险，基于安全评估结果分析系统安全风险和威胁，给出针对性的风险处理方案和整改建议。（服务所使用的扫描设备供应商自行提供，供应商提供承诺函并加盖供应商公章） 对采购人电脑病毒及安全隐患进行逐一排查；按照“涉密信息不上网，上网信息不涉密”的原则，对采购人计算机进行分类管理，严格实行内外网分离；及时更新杀毒软件和相应的系统办公软件，采取相应技术手段加强计算机的安全防范；定期开展计算机检查活动，做到“谁主管谁负责、谁运行谁负责、谁使用谁负责”。 3、安全巡检服务 巡检范围：采购人的 100 台服务器，巡检频率：每月一次。 对网络、操作系统的安全状况进行检查，以发现存在的安全漏洞和隐患，如：系统是否感染了计算机病毒、操作系统是否存在漏洞、主机或网络是否遭受过入侵攻击等。 1）病毒传播途径检查：管理员账户的口令是否设置为强口令，防止病毒、黑客通过猜口令的方式进行远程登录和入侵；服务器和客户端是否打开了共享目录。因为很多病毒通过共享方式传播，所以，应尽量关闭共享目录。 2）操作系统漏洞检查：操作系统是否已打上最新的补丁程序。 3）安全产品使用状况巡检：检查用户所使用的安全产品的部署和运行情况，检查网络节点上是否都已经安装防病毒产品。过滤策略设置是否合理、有效，是否设置了对病毒邮件、垃圾邮				

		件和带有关键字的内容得过滤或拦截规则等。检查防火墙运行是否正常，访问控制规则设置是否合理。 4、安全应急演练支撑服务 每年开展一次网络安全应急演练，包括演练方案制定、演练环境部署、演练技术支撑、演练工具提供、演练报告编写等内容，进一步提高我单位信息安全突发事件处置能力，帮助建立科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全。 5、安全通报服务 响应频率：服务期内动态响应。 服务内容：通过特定方式向采购人提供安全通告列表，实时提供最新出现的安全漏洞和安全升级通告。对于影响力范围广、破坏大的计算机病毒提供具体的检测和修复办法。 6、安全周活动配合 配合采购人在办公大楼门口或者食堂门口集中布设展板，国家网络安全宣传周期间向本单位工作人员宣传网络安全相关法规，接受咨询网络安全相关问题。 7、应急响应服务 响应频率：服务期内动态响应，服务周期：一年。 服务内容（包括但不限于）： （1）对设备提供现场安全维护服务，经维护发现设备故障或损坏时，及时向采购人技术人员详细说明故障原因及损坏程度，并提供最佳的解决方案，协助采购人将有关设备恢复到原来的运行状态； （2）提供对意外事故的处理； （3）提供对非法入侵的处理和调查恢复； （4）提供对网络攻击的应急防护； （5）提供应急响应服务的同时，进行数据备份，确保数据的安全存放，并在故障排除后将数据恢复到原有状态； 服务要求： （1）为采购人信息安全突发事件提供 7×24 小时技术支持； （2）为采购人的信息安全咨询提供 5×24 小时专人电话服务； （3）对于突发的网络安全事故，中标方技术人员需在 2 小时内到达现场； （4）每次维护均要有记录，年末提供年度汇总报告。 8、安全培训、管理制度建立和落实 培训周期：每年不少于 2 次 以安全检查为契机，从宣传教育入手，组织大家学习网络安全及保密知识，使大家充分认识到计算机网络泄密的严重危害和加强网络安全管理工作的重要意义，强化网络风险防范意识，掌握基本的安全防范措施，充分发挥信息系统的服务作用。加强网络安全管理，建立网络安全管理制度，强化风险意识，进一步提高常州市中级人民法院网络的安全防护等级和水平。 信息安全意识：在项目实施亦始或期间，向采购人提供针对一				

		般人员的信息安全意识培训，目的在于让所有与信息安全相关的人员都了解信息安全管理基本要领，理解信息安全策略，知道信息安全问题所在，掌握应对和解决问题的基本方法和途径。 信息安全管理基础：除了基本意识，向采购人项目实施相关人员提供以 ISO 27000 为主的信息安全管理基础培训，通过概要性的介绍，帮助大家掌握 ISO 27000 标准的精髓，理解自身角色和责任，了解信息安全体系建设、风险评估方法，从而在项目实施过程中起到应有的作用。 信息安全综合技能培训：让采购人信息安全管理体系能够长期稳定地运行下去，向相关人员提供信息安全操作技能的培训，目的在于提高其运营信息安全体系的技术能力，掌握处理问题的思路和方法。通过案例教学方法说明安全问题的处理、漏洞修补等。 专业人员资质认证培训：向采购人从事信息安全技术和管理工作的专业人员提供权威的资质认证培训，包括 CISSP 国际认证以及 ISO 27000 审核员资质等。 安全标准与法规培训：安全标准培训（如 ISO 15408，ISO 27000，ISO 13335，SSE-CMM 等）和国内外相关安全法律规范培训。 9、系统安全加固服务 依据安全评估和安全渗透结果，和采购人共同制定系统加固实施方案，依据方案实施加固，并输出完整的系统加固实施记录。 10、咨询服务 安全规划设计：基于组织的业务需求，规划出组织的安全建设蓝图；近景规划，中期规划以及远景规划，使得组织可以依据规划中的时间计划表以及规划内容来指导组织后续的安全建设。 安全集成方案设计：以采购人具体安全需求为出发点，从网络结构或应用系统等方面，设计集成的安全解决方案，并公平推荐有竞争力的安全产品。 安全应用方案设计：根据采购人目前网络结构以及应用情况，对于采购人新上线项目提出合理化安全建议。				
7	重要时期安全保障服务	在重大节日、重要活动前，根据采购人的安排，对照上级法院和信息安全主管单位关于强化网络安全防范工作的具体要求，供应商应作为信息安全技术支撑单位对采购人及各基层法院网络安全情况开展全面梳理排查，对重要系统和网站进行安全检查和技术检测，逐条对照，查漏补缺，及时排查网络安全隐患。同时应及时形成重要时期安全保障服务报告，承担后期的复测工作，以安全检查活动来提高直属单位以及下属单位的信息安全意识。	项	1	120000	120000
8	UPS 维保	1、供应商工程师至少每季度巡检一次（采购人指定时间）。 2、实行“7×24”服务方针，提供每周七天、每天 24 小时服务响应，专人配备手机为采购人保持不间断热线服务。 3、维修响应时间：接到采购人维修申请后保证在规定时间内（4	项	1	50000	50000

		小时内到达现场）上门服务。 4、UPS 巡检服务：供应商应提供以下 UPS 巡检服务： （1）UPS 机房环境的检查及维护 1）检查 UPS 机房环境： a. 温度检测 b. 湿度检测 c. 通风检测 d. 清洁工作 2）机房配电系统检测 a. 配线紧固及老化情况检测 b. 面板各显示表及指示灯检测校准 （2）UPS 系统物理检查及维护 1）检查 UPS 外部清洁 a. 外壳清洁 b. 风机工作情况有无异响及清洁 2）检查 UPS 内部清洁 a. 电路板及显示屏清洁 b. 电路板连线接插件及配线端子清洁 c. 连接线紧固，检查是否过热及老化情况及清洁 d. 检查功率元件及清洁 e. 检查开关、继电器、接触器及清洁 f. 检查交直流电容是否漏液、变形及清洁 g. 检查风机工作情况有无异响并加油清洁 h. 检查变压器工作情况有无异响及清洁 3）电池系统清洁 a. 电池环境清洁 b. 电池表面清洁 （3）UPS 系统运行参数检查及维护 1）UPS 输入输出电压（各相）检测； 2）UPS 输入输出电流（各相）检测； 3）直流充电电压电流（浮充和均充）检测； 4）整流器锁相及启动情况； 5）逆变器锁相及启动情况； 6）旁路锁相及启动情况； 7）所有面板测量值检测。 （4）电池系统检查及维护 1）电池组总体外观检查，是否有漏液、变形现象； 2）检查直流接线紧固情况； 3）在线测试各个单节电池容量，数据记录； 4）电池放电实验，放电时间根据实际放电速率决定，放电 30%的额定容量。 （5）现场解答采购人使用过程中问题 和采购人沟通在实际使用过程中发生的问题，作出合理解答和处理意见并记录在案，如果现场处理不了则承诺在一定的时限				

		内向采购人做出处理意见。				
9	精密空调维保	1、供应商工程师至少每季度巡检一次（采购人指定时间）。 2、实行“7×24”服务方针，提供每周七天、每天 24 小时服务响应，专人配备手机为采购人保持不间断热线服务。 3、维修响应时间：接到采购人维修申请后保证在规定时间内（4 小时内到达现场）上门服务。 4、 空调巡检服务：供应商应提供以下空调巡检服务： （1）制冷系统 1）压缩机的维护：检查压缩机润滑、吸排气压力，压缩机电机性能是否完好； 2）检查制冷系统管路压力是否达到设定值，否则找出原因进行维修； 3）检查室外机的运行情况，如室外机灰尘堵塞应清洗，并指导甲方操作维护人员做好日常清洗保养工作。 （2）电气系统： 1)对电气柜进行检查，重点检查交流接触器电气特性是否完好； 2）检查风机电机、加热器、加湿器静态阻值及绝缘性能； 3）检查冷凝器电气箱内调速器及冷凝风机是否完好； 4）校正高、低压保护器是否与设定值相符； （3）风道系统： 1）检查风机皮带及皮带轮的运行情况，如有误差应调校； 2）检查空气过滤网情况，如有通风不畅应更换。	项	1	30000	30000
10	安防监控设备维保	保障安防监控系统正常工作，充分满足采购人对日常服务及应急故障处理的需求。服务期内，维修配件包含硬盘录像机配件、摄像机、摄像机电源、摄像机支架、摄像机交换机、光纤收发器等硬件设备。故障设备如在厂商免费保修期限及范围内，则由供应商提供送修服务或协助采购人联系厂商进行保修；故障设备如超出厂商免费保修期限及范围，供应商应免费维修；故障设备如非正常损坏或超出保修范围，供应商应提供优惠价格方便采购人选择购买。 1、服务范围 系统设备的定期升级、巡检、故障修复及发现损坏设备，更换无法修复的设备，对不能立即排除故障，提供备用设备减小停用时间。提供对安防监控系统设备的每季度一次定期巡检及常规维护服务，对于巡检过程中发现的各类问题，及时提供有效的解决办法，确保系统的高可用性。 2、服务响应时间要求 从服务需求提出，即电话申请服务后开始计时：紧急问题要求供应商承诺工程师在接到问题报告后 15 分钟之内提供电话响应或在线支持服务，并于 1 小时内到达现场，并于 4 小时内修复。 3、项目管理要求	项	1	115000	115000

		供应商应派遣一名对科技法庭比较熟悉的资深技术人员与采购人对接，负责本项目整体管理，统筹相关工作，项目监督与情况汇报，执行变更和应急情况管理，并根据实际状况调整供应商服务人员安排，以保证此服务项目的正常高效运作。 4、技术交流及培训 不定期向采购人的系统维护人员提供必须的服务技能培训，并对相关技术问题进行充分交流，以提高采购人维护人员的业务水平，保障系统科技法庭及安防设备的稳定健康运行。 5、提供设备清点排查及建档服务 在运维期间为采购人更新在用监控系统设备清单；同时按要求填制各项相关视频监控系统的巡检、养护、维修等记录文档。 6、提供特殊需求现场保障服务 在采购人有大要案件庭审或系统升级切换等特殊情况发生时，可提前与供应商确定安排专人提供现场值守，确保重要时刻系统稳定运行。				
11	电视电话会议设备维保	1、维保内容 维保内容包含视频会议设备维护、配套使用的会议发言设备维护、配套使用的音响设备维护、配套使用的显示设备维护。维保服务包含了服务期内硬件设备单次维修费用不高于500元的维修；如硬件设备单次维修费用超出500元，维修费由采购人承担。 维保服务内容如下： （1）确保维保范围内所有系统的正常运行，每季度对视频会议系统功能和稳定性进行检查，确保视频会议图像、声音清晰流畅，投影机、大屏等正常使用，处理故障隐患，确保各部分设备各项功能良好，能够正常运行，巡检完成后出具巡检报告。 （2）协助用户建立各种故障的恢复流程及应急措施。 （3）提供全年的现场会议保障工作。 2、服务标准 采购人通过电子邮件、7*24小时客户服务热线电话、网络等联系方式通知供应商需要现场会议保障服务时，供应商应立即安排专业工程师提前做好保障工作： （1）会前准备工作：供应商安排固定专业工程师提前一天上门到会议现场对采购人的系统进行全面的检测、调试（音响效果、话筒有无啸叫、会议摄像机的位置及图像调整到最佳状态、LED大屏或投影仪是否正常显示、上下级网络是否正常、协助采购人提前做好会标准备工作等），并协助采购人配合上级法院和基层法院调试会议系统设备且均符合会议要求，确保会场所有设备正常运行及与上下级法院达到互通互联； （2）会议当天：会议当天供应商工程师应提前3小时到达会议现场，再次对会议系统设备及网络进行多次检测及联调，使所有设备及网络保持在最佳状态；检测会标是否有错字漏字现象，话筒切换是否正常。	项	1	120000	120000

		（3）会议进行中：供应商工程师应一直在音控室随时待命，保障好会议中可能出现的突发状况，并及时解决，确保会议正常进行。 （4）会议结束：供应商工程师在会议结束、所有参会人员全部离场后，对所有设备逐一关机收到原存放设备处，并对临时线路进行拆除；配合保洁人员做好会场设备保洁工作，检查所有设备是否全部处于待机或者关机状态；关掉会场所有灯光和空调，锁门离开。 （5）会议保障结束：每次会议保障工作结束后，供应商针对此次会议中出现的情况及突发事件（如中控失灵，音响损坏），应出具相应的情况说明，并由采购人相关人员签字认可；如无突发事情，会议顺利结束，供应商也应出具相应的服务报告，并由采购人相关人员签字认可。供应商应做好每一次的维护工作记录，确保维护工作记录的准确性、完整性。 供应商应针对各系统的实际情况及具体需求，制订具体的维护标准和方案，包括故障恢复、灾难恢复、维护信息管理档案、紧急维护维修方案、备件提供等。供应商应对维修、维护记录建档；进行定期维护的，每次维护应提交维护检测报告，由采购人相关人员确认。 其他要求：如日常中设备有故障，供应商工程师应及时响应，响应到位 2 小时内对有关需求提出产生原因、具体解决方案、维修费用报价等书面报告。如需原厂检修方可确定的重大故障，供应商应在 12 小时内提供原厂报告及预算，属关键部件故障的，供应商及原厂应根据采购人的工作需要安排维修人员加班检修。				
12	LED 显示屏维保	LED 显示屏维护内容和标准如下： 1、电脑部分 1）系统程序 2）播放软件 3）电脑硬件 2、大屏部分 1）信号线路及接收卡、发送卡 2）电源线路、电源盒、电灯 3）大屏模组、箱体、结构 4）大屏内部防渗漏 注：大型设备（处理器及发送卡等）因无法维修需更换时，供应商按成本收取费用，不在免费维保范围内。 3、大屏钢结构防水、防锈、结构检查 1）主体钢结构节点检查 2）主题钢结构防腐检修 3）屏体外框防水检查、维护 4）屏体与建筑、屏面连接防水检查、维护 4、维修时间	项	1	30000	30000

		供应商应设置 24 小时售后服务热线，在接到报障后 4 小时到达现场、12 小时内解决故障（重大故障除外），保证显示系统正常可靠运行。				
总报价（人民币：元）						1770000