用户需求书

（一）项目概况

1.项目名称：儋州市公安局网上督察视频智能分析平台项目(第二次采购)

2.项目编号：HNZS-2024-004

3.采购预算：106369.23 元，本项目分 2 个包，分包情况如下：

标包编号	标包名称	采购预算(元)
HNZS-2024-004-2	B 包(工程监理)	56369.23
HNZS-2024-004-3	C 包(等保测评)	50000.00
注：1、同一投标人只允许参与其中一个包的投标，否则投标无效。 2、超出各包采购预算金额的投标文件按无效投标处理。		

4.合同履行期限：

B 包(工程监理)：本项目监理服务周期自签订合同之日起，至建设项目完成竣工验收。

C 包(等保测评)：采购人下达的测评通知后 90 个日历天内交付测评报告。

（二）技术商务要求

B 包(工程监理)：

技术要求

监理单位应按照建设目标和要求，遵循国家信息系统工程建设和监理的标准与规范，依据项目建设合同和用户需求，采用先进、科学和适合本工程特点的项目管理技巧和手段，对项目进行质量、成本、进度、变更的全面控制和监督，负责相关的合同管理、信息管理、信息安全管理，负责上述整个项目全过程监督协调，从而使本项目“按期保质、高效、节约”地完成。

(一)监理范围

信息化部分，重点对项目建设过程中系统集成、软件开发、测试、培训、试运行、装修、验收等全过程进行监督管理，从系统集成、软件开发两个方面梳理该项目建设的过程监理应如何通过切实有效方法、手段达到建设方所要求的深度、广度，最终实现工程监理的目标。实现对质量、进度、投资、变更的控制及合同管理和文档管理。当工程质量或工期出现问题或严重偏离计划时，应及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

(二)监理目标控制方案

以工程建设合同、监理委托合同、国家(GB/T19668.1-19668.6《信息化工程监理规范》及有关法规、技术规范与标准、项目建设单位需求为依据，通过专业的控制手段，协助建设单位全面地进行技术咨询和技术监督，对工程全过程进行监督、管理、指导、评价，并采取相应的组织措施、技术措施、经济措施和合同措施，确保建设行为合法、合理、

科学、经济，使建设进度、投资、质量达到建设合同规定的目标。
1、监理质量目标控制
监理质量目标控制是监理技术服务的核心所在，也是监理单位综合实力的最好反映，所以做好监理质量目标控制方案，确保本项目建设质量能达到建设单位要求的质量目标。确保本项目建设质量达到工程合同中规定的功能、技术参数等目标。确保工程建设中的设备和各个节点满足相关国家(GB/T19668.1-19668.6《信息化工程监理规范》或行业质量标准和技术标准，按照承建合同要求进行基于总体方案的细化设计、开发、部署、培训和运行；系统集成和软件开发过程涉及用户需求调研分析、概要设计、详细设计、系统实现、系统测试和系统运行等比较复杂、制约因素多的工作内容，应该成为质量控制的重点；深化设计方案的确定、开发平台选定，也要进行充分论证。
要求监理在整个工程实施过程中做好对工程质量的事前控制，事中监督和事后评估，以确保工程质量合格。
投标人应针对本项目建设中系统集成、软件开发、工程培训等提出工程监理的质量控制原则、方法、措施、工作流程和目标。
2、监理进度目标控制
确保本项目按合同规定的工期完工。
依据合同所约定的工期目标，在确保质量和安全的原则下，采用动态的控制方法，对进度进行主动控制，确保项目按规定的工期完工。
通过对本项目概要设计的分析、研究，提出针对本项目建设的、有代表性的信息工程监理进度控制的主要原则、方法、内容、措施、工作流程和目标。
3、监理投资目标控制
协助建设方控制本项目建设总投资在项目预算及审计范围内，减少项目建设中的额外开支。以项目建设方和承建单位实际签订的合同金额为准，确保项目费用控制在合同规定的范围内。
4、监理项目变更控制
协助用户对本项目的整体进行工期进度、投资、技术等方面进行变更管理、审核。以项目建设方和承建单位的可研、招投标文件，以及签订的合同建设内容为监理依据，确保项目实施控制在规定的范围内没有遗漏，如有则需进行变更流程。在项目建设中，合理减少项目变更，保护建设单位的经济利益。
(三)工程监理重点难点分析
投标人应根据本项目建设的特点，从实际出发分析本项目监理工作的重点、难点，并根据分析的结果制定相应的监理工作规划、对策和策略，以便日后有针对性的开展建设工程的监理服务工作。
1、项目组织及总体技术方案的质量控制
(1)协助审查项目承建方的合同及实施方案；
(2)在技术上、经济上、性能上和风险上进行分析和评估，为采购人提
供建议；

(3)协助审查项目建设方提交的组织实施方案和项目计划等相关文档；
(4)协助审查项目建设方的工程质量保证计划及质量控制体系；
(5)参与制定项目质量控制的关键节点及关键路径。
2、项目质量控制
(1)组织措施：建立质量管理系统，完善职责分工及有关质量监督制度，落实质量控制责任。
(2)系统集成质量控制：审核系统总集成方案，参与制定系统验收大纲，对系统进行总体验收。
(3)人员培训的质量控制：协助审查并确认培训计划，审定培训大纲；监督审查建设方实施其培训计划，并征求采购人的意见反馈；监督审查考核工作，评估培训效果；协助审核并确认培训总结报告。
(4)文档：资料的质量控制：监督审查承建方提供的软件开发、测试、部署相关文件的标准性和规范化，在各项目验收时，应监督项目承建方提交符合规定的成套资料，包括纸质版和电子版。对监理项目实施过程中的文档进行标准化、规范化管理，在监理项目验收时，应提交符合规定的监理项目的成套资料，包括印刷本和电子版。
3、进度协调控制
(1)组织措施。建立进度控制协调制度，落实进度控制责任。
(2)编制项目控制进度计划。编制项目总进度计划和网络图。按各子系统实际情况进行编制，包括系统建设开工、软件的编制、试运行等各方面内容,做到既要保证各子系统、各阶段目标的顺利实现，又要保证项目间、阶段间的衔接、统一和协调。
(3)审查各子系统承建方编制的工作进度计划。分析系统建设进度计划是否能满足合同工期及系统建设总进度计划的要求,特别要对照上阶段计划工程量完成情况进行审查,对为完成系统建设进度计划所采取的措施是否恰当，管理上有无缺陷进行审查。要根据承建方所能提供的人员及产品性能复核、人员安排是否满足要求等，分析判断计划是否能落实，审查承建方提出的进度计划能否落实。如发现未落实，应及时报告采购人，要求承建方采取应急措施满足系统建设的需求。
(4)系统建设进度的现场检查。随时或定期、全面地对进度计划的执行情况跟踪检查，发现问题及时采取有效措施加以解决。加强系统建设准备工作的检查，在工程项目或部分工序实施前，对情况进行检查，要加强检查设备、人员安排、各项措施的落实情况，确保准备工作符合要求，不影响后续工程的进行。
(5)进度计划的分析与调整。要保证建设进度与计划进度一致，经常对计划进度与实际进度进行比较分析，发现实际进度与计划进度不符时，即出现进度偏差时，首先分析原因，分析偏差对后续工作的影响程度，并及时通知建设方
采取措施，向承建方提出要求和修改计划的指令。
4、投资控制
(1)审查设计图纸和文件。审查承建方的施工组织设计和各项技术措施，深入了解设计意图，在保证系统建设质量和安全的前提下尽可能优化设计。

(2)严格督促承建方按合同实施，严格控制合同外项目的增加。协助采购人严格控制设计变更，制定设计变更增加工作量的报批制度；及时了解系统建设情况，协调好各方矛盾，减少索赔事件的发生。对发生的事件严格按合同及法律条款进行处理，认真进行索赔调解。

5、合同管理

合同管理是加快系统建设进度、降低系统建设造价、保证系统建设质量的有效途径之一。通过合同管理，可以督促承建方在各个阶段按照合同要求保证设备、人员的配备及投入，保证各阶段目标按合同实施，减少索赔事件，控制系统建设结算等。具体要求如下：

(1)以合同为依据，本着“实事求是、公正”的原则，合情合理地处理合同执行过程中的各种争议。

(2)分析、跟踪和检查合同执行情况，确保项目承建方按时履约。

(3)对合同的工期的延误和延期进行审核确认。

(4)对合同变更、索赔等事宜进行审核确认。

(5)根据合同约定，审核项目承建方的支付申请。

(6)建立合同目录、编码和档案。

(7)合同管理坚持标准化、程序化，如设计变更、延期、索赔、计量支付等应规定出固定格式和报表。合同价款的增减要有依据，合同外项目增加要严格审批制度。重大合同管理问题的处理，如大的变更、索赔、复杂的技术问题等，组成专门小组进行研究。不符合实际情况的合同条款及时向采购人报告，尽早处理，以免造成损失。

6、信息、工程文档管理

在项目管理过程中，为了实现对进度、质量、投资的有效控制，处理有关合同管理中的各种问题，监理方需要收集各种有用的信息。信息的来源主要包括采购人文件、设计图纸和文件、承建方的文件、建设现场的现场记录(或项目管理日志)、会议记录、验收情况及备忘录等等。其中项目管理日志是进行信息管理的一个最重要的方面。项目管理日志主要包括当天的工作项目和工作内容、投入的人力和设备运行情况、计划的完成情况及进度情况、停工和返工及窝工情况。信息管理主要措施要求如下：

(1)制定详细的信息收集、整理、汇总、分析、传递和利用制度，力求信息管理的标准化和制度化。由专人负责系统建设信息的收集、分类、整理储存及传递工作。信息传递以文字为主，统一编号，利用计算机进行管理，力求信息管理的高效、迅速、及时和准确，为系统建设提供及时有用的信息和决策依据。

(2)在项目实施过程中做好工程监理日记和工程大事记。

(3)做好双方合同、技术建设方案、测试文档、验收报告等各类往来文件的存档。

(4)建立必要的会议、例会制度，整理好会议纪要，并监督会议有关事项的执行情况。

(5)立足于建设现场，加强动态信息管理，对现场的信息进行详细记录和分析，做到以文字为基础，以数据说明问题。根据收集到的信息与合同进行比较，督促建设方的人员和设备到位，促使承包商按合同完成各项目标，从而实现对进度、质量、投资的控制。

(6)建立完整的各项报表制度，规范各种适合本项目的报表。定期将各种报表、信息分类

汇总，及时向采购人及有关各方报送。
(7)监理项目验收时，应提交符合规定的有关工程的成套资料，包括印刷本和电子版。
7、日常监理
(1)掌握监理范围内涉及的各种技术及相关标准；
(2)安排足够的监理人员，成立项目监理部，按工程需要派驻相应的专业人员进行项目现场监理，随时为采购人提供服务，总监理工程师必需专职于本项目；
(3)制定工程管理的组织机构方案并协助采购人组建相关机构，并提供相关培训；
(4)熟悉了解项目的业务需求，协助采购人对项目的目标、范围和功能进行界定，参与并协助项目的设计方案交底审核工作；
(5)建立健全科学合理的会议制度，并予以贯彻落实；
(6)建立健全科学合理的文档管理制度，制订开发过程中产生的各类文档制作、管理规范，并予以贯彻落实；
(7)与采购方一起制定评审机制，在工程实施全过程中随时关注隐患苗头，如发现将会导致工程失败的情况出现时，应及时启动评审机制，组织专家对工程实施情况进行评审，对评审不合格的，应向采购方提出终止合同意见。此外，还应组织定期评审(阶段性评审、里程碑评审、验收评审)，对评审结果为优的，提出奖励意见，评审不合格的，则向采购方提出处理意见。
(四)工程各阶段的监理规划、实施
投标人应对本项目从设计施工到项目竣工验收阶段制定一整套工程监理的工作流程，并叙述各阶段主要监理工作内容。
本项目监理工作主要分为设备/材料采购、开施工阶段、验收阶段、质保期阶段等。
1、设备/材料采购监理
建设项目由承包单位承担设备/材料采购任务，工程监理单位在设备/材料采购阶段监理工作主要有：
✧审核承包单位的设备采购计划和设备采购清单；
✧订货进货验证；
✧组织到货验收；
✧鉴定、设备移交等。
2、施工阶段监理
(1)开工前的监理
1)审核施工设计方案：开工前，由监理单位组织实施方案的审核，内容包括设计交底，了解需求、质量要求，依据设计招标文件，审核总体设计方案和有关的技术合同附件，以避免因设计失误造成实施的障碍；
2)审核实施方案的合法性、合理性、与设计方案的符合性；
3)审批施工组织设计：对施工单位的实施工作准备情况进行和监督；
4)审核施工进度计划：对施工单位的施工进度计划进行评估和审查；
5)审核实施人员：确认施工方提交的实施人员与实际工作人员的一致性，如有变更，则

要求叙述其原因；
6)审核《软件项目开发计划》。
(2)施工准备阶段的监理
1)审批开工申请，确定开工日期；
2)了解施工条件准备情况；
3)了解承建方实施前期的人员组织、施工设备到位情况；
4)编制各个子项目监理细则；
5)签发开工令。
(3)施工阶段的监理
1)审核软件开发各个阶段文件；
2)协助采购人组织软件开发阶段评审；
3)促使项目中所使用的产品和服务符合合同及国家相关法律法规和标准；
4)审核项目各个阶段进度计划；
5)督促、检查承建单位进度执行情况；
6)审查项目变更，提出监理意见；
7)审查承建单位阶段款支付申请，提出监理意见；
8)按周(月、旬)定期报告项目情况；
9)组织召开项目例会和专项会议。
(4)试运行阶段的监理
1)协助建设方确认项目进入试运行；
2)监查系统的调试和试运行情况，记录系统试运行数据；
3)进行试运行期系统测试，做出测试报告；
4)对试运行期间系统出现的质量问题进行记录，并责成有关单位解决。解决问题后，进行二次监测；
5)进行试运行时间核算；
6)协助建设方确认试运行通过。
3、验收阶段监理
(1)验收阶段
1)依照国家信息化管理细则，国家验收管理办法约定执行。
2)对承建单位在试运行阶段出现的问题的整改情况进行监督和复查；
3)监督检查承建单位作好用户培训工作，检查用户文档；
4)组织系统初步验收；
5)审查承建单位提交的竣工文档；
6)参与项目竣工验收；
7)竣工资料收集整理齐全并装订，签署验收报告；
8)审核项目结算；

9)审查承建单位阶段款支付申请，提出监理意见；
10)向建设单位提交监理工作总结；
11)将所有的监理材料汇总，编制监理业务手册，提交采购人；
12)系统验收完毕进入保修阶段的审核与签发移交证书。
(2)项目移交阶段
1)系统的设计方案、设计图纸和竣工资料的全部移交；
2)软件、材料等的验收文档核实；
3)施工文档的移交；
4)竣工文档的移交；
5)项目的整体移交。
4、质保期阶段监理
监理单位承诺依据委托监理合同约定的工程质量保修期规定的时间、范围和内容开展工作主要有：
(1)定期对项目进行回访，协助解决技术问题；
(2)对项目建设单位提出的质量缺陷进行检查和记录；
(3)对质量缺陷原因进行调查分析并确定责任归属；
(4)检查承建单位质保期履约情况，督促执行；
(5)审查承建单位阶段款支付申请，提出监理意见。
投标人应根据上述监理工作内容(但不局限于上述内容)，分别制定详细的监理工作流程，使本项目的监理工作流程化、制度化。
(五)监理工作要求
1、监理工作制度要求
根据本项目的特色，本项目要求以现场监理为主要方式进行，在施工现场主要监理人员必须具备所从事监理业务的专业技术和类似系统经验，并具有丰富的项目管理经验。监理工作必须由具有相应资质和职称的人员来担任。本次监理项目实行总监理工程师负责制，在整个项目建设期间，总监理工程师必须保证有三分之一工作日以上的时间到甲方现场，且必须在建设期间全程常驻至少一名监理工程师在甲方现场。监理公司应建立项目监理小组，负责整个项目的全程监理工作，本项目必须配备不少于3名的现场专业工程师。监理人员的确定和变更，须事先经业主方同意。监理人员必须奉公守法，具有高度的责任心。
2、监理项目组织要求
工程监理组织形式应根据工程项目的特点、工程项目承包模式、业主委托的任务以及监理单位自身情况而确定，结构形式的选择应考虑有利于项目合同管理、有利于目标控控制、有利于决策指挥、有利于信息沟通。
要求投标人在报价方案中要明确工程监理的各项运作，包括监理人员的相关资料、职能分配、监理组织的构成及工作流程、各项监理工作的相关负责人等。
3、监理信息管理要求

投标人应制定有关本项目信息管理流程，规范各方文档并负责整理记录归档业主单位与承建单位来往的文件、合同、协议及会议记录等各种文档，并定期以监理月(周/季)报形式提交业主。包括下列监理工作：

(1)做好监理日记及工程大事记；

(2)做好合同批复等各类往来文件的批复和存档；

(3)做好项目协调会、技术专题会等各项会议纪要；

(4)管理好实施期间的各类、各方技术文档；

(5)做好项目周报；

(6)做好监理建议书、监理通知书存档；

(7)阶段性项目总结。

投标人应针对项目特点，制定相应的信息分类表、信息流程图、信息管理表格、信息管理工作流程与措施，同时要求采用先进的项目信息管理软件对项目信息进行综合管理。

4、监理合同管理要求

本项目建设过程中会与承建单位签订合同或协议，投标人应该针对项目特点制定合同从草案到签署的管理工作流程与措施，规范合同管理，并在具体项目合同执行时进行下列监理工作：

(1)跟踪检查合同的执行情况，确保承建单位按时履约；

(2)对合同工期的延误和延期进行审核确认；

(3)对合同变更、索赔等事宜进行审核确认；

(4)对合同终止进行审核确认；

(5)根据合同约定，审核承建单位提交的支付申请，签发付款凭证；

(6)要求对项目合同进行合理的管理，以完善整个项目建设的过程。

四、监理服务准则

遵照国家GB/T19668.1-19668.6《信息化工程监理规范》，以“守法、诚信、公正、科学”的准则执业，维护建设方与承建方的合法权益。具体应做到：

(1)执行有关项目建设的法律、法规、规范、标准和制度，履行监理合同规定的义务和职责。

(2)不收受被监理单位的任何礼金。

(3)不泄漏所监理项目各方认为需要保密的事项。

(4)遵守国家的法律和政府的有关条例、规定和办法等。

(5)坚持公正的立场，独立、公正地处理有关各方的争议。

(6)坚持科学的态度和实事求是的原则。

(7)在坚持按监理合同的规定向建设单位提供技术服务的同时，帮助被监理者完成起担负的建设任务。

(8)不泄漏所监理的项目需保密的事项。

五、监理依据

(1)国家GB/T19668.1-19668.6《信息化工程监理规范》和国家有关信息系统项目建设和

监理管理规范；
(2)建设单位与承建单位签订的承包工程合同
(3)建设单位与监理单位签订的委托监理合同
(4)本工程招标书、招标过程文件、各中标单位的投标书
(5)国家有关合同、招投标、政府采购的法律法规
(6)部颁、地方政府的信息工程、信息工程监理的管理办法和规定
(7)建设工程和信息工程相关的国家、行业标准和规范
(8)建设工程和信息工程技术监督、工程验收规范
(9)与工程相关的技术资料
(10)其他与本项目适用的法律、法规和标准
(11)国家、地方及行业相关的技术标准
六、安全保密要求
本项目要求投标人制定一整套工程监理安全保密制度，确定工程保密责任人，同时要求投标人：
(1)按照国家、省、市的有关法规文件规定，要求监理履行保密责任，并与建设单位签订保密协议；
(2)监理单位各级组织严格履行保密职责；
(3)按照公司内部保密规定开展监理工作。
七、监理验收要求
审核监理方应提交的各类监理文档和最终监理总结报告，综合评估监理方在系统开发进度、质量把关、重难点问题解决、项目投资等方面的监理情况。只有文档齐全，系统开发工作中没有出现重大质量事故才予验收。
本监理工作的最终验收由主管部门组织，项目通过验收即为验收通过。
八、其它要求
总监理工程师、总监理工程师代表及专业监理工程师均需对应行业标准要求设定。
投标人须提供详尽的监理技术方案，包括但不限于施工组织部署、项目管理目标、施工准备、进度控制、质量管理、验收方法等内容。
（2）商务要求
1.预算金额:56369.23 元(超出本包采购预算(最高限价)的投标报价，按无效投标处理；)
2.监理服务地点：海南省儋州市
3.合同履行期限：本项目监理服务周期自签订合同之日起，至建设项目完成竣工验收。
4、支付方式
（1）合同签订后 5 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同款的 30%(预付款)；
（2）项目通过初验后 5 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同款的 50%；
（3）项目通过终验后 5 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同款

的 20%；

C 包(等保测评)：

技术要求

(一)项目需求

根据等级保护测评的工作要求，测评范围覆盖安全管理中心、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个层面。

具体服务内容包括：

(1)协助业主单位进行信息系统的信息安全等级定级和备案工作。

(2)差距测评，至少包括：

安全技术测评。包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的安全测评。

安全管理测评。包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维五个方面的安全测评。

形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计(测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果)；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果制定《系统等级保护测评问题汇总及整改意见报告》，列出被测信息系统中存在的主要问题及整改意见。

(3)协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。

(4)等级测评，至少包括：

按照等级保护相关标准对系统从安全技术、安全管理等方面进行等级测评工作。

编制测评报告，制定并提交《网络安全等级测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求。

(二)服务内容指标

分类	子类	基本要求
安全物理环境	物理位置选择	a)机房场地应选择在具有防震、防风和防雨等能力的建筑内； b)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a)应将设备或主要部件进行固定，并设置明显的不易除去的标识； b)应将通信线缆铺设在隐蔽安全处。
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。

	防火	a)机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
	防水和防潮	a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透;b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
	电力供应	a)应在机房供电线路上配置稳压器和过电压防护设备； b)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
安全通信网络	网络架构	a)应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； b)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
	通信传输	应采用校验技术保证通信过程中数据的完整性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全区域边界	边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

	访问控制	a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
	入侵防范	应在关键网络节点处监视网络攻击行为。
	恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
	安全审计	a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计;b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c)应对审计记录进行保护,定期备份,避免受到未预期的删除、修改或覆盖等。
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证,并在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心。
安全计算环境	身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； c)当进行远程管理时,应采取必要措施防止鉴别信息在网络传输过程中被窃听。
	访问控制	a)应对登录的用户分配账户和权限； b)应重命名或删除默认账户，修改默认账户的默认口令;c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；

		d)应授予管理用户所需的最小权限，实现管理用户的权限分离。
	安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序； b)应关闭不需要的系统服务、默认共享和高危端口； c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
	恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
	数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。
	数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能； b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
	剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

	个人信息保护	a)应仅采集和保存业务必需的用户个人信息； b)应禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计;b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
	审计管理	a)应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； b)应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
	管理制度	a)应对安全管理活动中的主要管理内容建立安全管理制度;b)应对管理人员或操作人员执行的日常管理操作建立操作规程。
	制定和发布	a)应指定或授权专门的部门或人员负责安全管理制度的制定； b)安全管理制度应通过正式、有效的方式发布，并进行版本控制。
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
安全管理机构	岗位设置	a)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； b)应设立系统管理员、审计管理员和安全管理员等岗位，
		并定义部门及各个工作岗位的职责。
	人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。

	授权和审批	a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； b)应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。
	沟通和合作	a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
安全管理人员	人员录用	a)应指定或授权专门的部门或人员负责人员录用； b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查。
	人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
	安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。
	外部人员访问管理	应在外部人员物理访问受控区域前先提出书面申请批准后由专人全程陪同，并登记备案； b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案； c)外部人员离场后应及时清除其所有的访问权限。

安全建设管理	定级和备案	a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； c)应保证定级结果经过相关部门的批准； d)应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	a)应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； b)应根据保护对象的安全保护等级进行安全方案设计； c)应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。
	产品采购和使用	a)应确保网络安全产品采购和使用符合国家的有关规定;b)应确保密码产品与服务的采购和使用符合国家密码管理 主管部门的要求。
	自行软件开发	a)应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； b)应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。
	外包软件开发	a)应在软件交付前检测其中可能存在的恶意代码； b)应保证开发单位提供软件设计文档和使用指南。
	工程实施	a)应指定或授权专门的部门或人员负责工程实施过程的管理； b)应制定安全工程实施方案控制工程实施过程。
	测试验收	a)应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； b)应进行上线前的安全性测试，并出具安全测试报告。
	系统交付	a)应制定交付清单，并根据交付清单对所交接的设备、软

		件和文档等进行清点； b)应对负责运行维护的技术人员进行相应的技能培训； c)应提供建设过程文档和运行维护文档。
	等级测评	a)应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； b)应在发生重大变更或级别发生变化时进行等级测评； c)应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a)应确保服务供应商的选择符合国家的有关规定； b)应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
安全运维管理	环境管理	a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； b)应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；c)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
	介质管理	应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理	a)应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理； b)应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。

分类	子类	基本要求
	漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
	网络和系统安全管理	a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定； d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
	恶意代码防范管理	a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； b)应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等； c)应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
	配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
	密码管理	a)应遵循密码相关国家标准和行业标准;b)应使用国家密码管理主管部门认证核准的密码技术和产品。
	变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。
	备份与恢复	a)应识别需要定期备份的重要业务信息、系统数据及软件

分类	子类	基本要求
	管理	系统等； b)应规定备份信息的备份方式、备份频度、存储介质、保存期等； c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
	安全事件处置	a)应及时向安全管理部门报告所发现的安全弱点和可疑事件； b)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等； c)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。
	应急预案管理	a)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； b)应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。
	外包运维管理	a)应确保外包运维服务商的选择符合国家的有关规定； b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

(三)完成项目所需提交的文档清单

在本项目完成后，服务方须提供以下文档资料：

- 《信息系统安全问题汇总及整改建议》
- 《网络安全等级保护等级测评报告》及过程资料

(四)技术标准和规范

- 《中华人民共和国计算机信息系统安全保护条例》(国务院令 147 号)
- 《信息安全等级保护管理办法》
- 《计算机信息系统安全保护等级划分准则》(GB17859-1999)

●《信息安全技术网络安全等级保护定级指南》(GB/T22240-2020)●《信息安全技术网络安全等级保护基本要求》(GB/T22239-2019)
●《信息安全技术网络安全等级保护测评要求》(GB/T28448-2019)
●《信息安全技术网络安全等级保护测评过程指南》(GB/T28449-2018)
●《信息安全风险评估规范》(GB/T20984-2007)
(五)安全要求
成交供应商在项目实施过程中，必须遵守以下技术原则：
1 保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购方的行为，否则采购方有权追究供应商的责任。
2 标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。
3 规范性原则：供应商的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制，测评出具的报告须符合公安部颁布的《网络安全等级测评报告模板》。
4 可控性原则：等保测评服务的进度要按照招标文件的要求，保证采购方对于测评工作的可控性。
5 整体性原则：等保测评服务的范围和内容应当整体全面，包括国家等级保护相关要求测评要求涉及的各个层面。
6 安全性原则：等保测评服务工作应不得影响系统和网络的正常运行；测评工作不得对现有信息系统的正常运行、业务的正常开展产生任何影响。
7.测评机构资质及人员要求：
从事信息系统检测评估相关工作人员无违法记录。
工作人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。
测评期间需遵守被测单位相关管理规定，禁止利用测评工作从事危害被测单位利益、安全的活动。
商务要求
1、采购预算:50000.00 元(超出本包采购预算(最高限价)的投标报价,按无效投标处理;)
2、合同履行期限：采购人下达的测评通知后 90 个日历天内交付测评报告。
3、付款方式：
(1)签订合同后 5 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同总额的 70%款项;
(2)甲方在收到乙方提交的《信息系统安全等级保护测评报告》和《信息系统安全整改设计方案》后，甲方凭乙方开具的正式有效发票在 5 个工作日内向乙方支付剩余合同总额的 30%款项。