北人智能装备科技有限公司信息系统等级保护二级建设项目

招标文件

2022 年 3 月

第一章 招标内容

现就 北人智能装备科技有限公司-信息系统等级保护二级建设项目 进行招标，欢迎贵单位参加投标。

序号	内　　容
1	项目名称：北人智能装备科技有限公司-信息系统等级保护二级建设项目 项目地址： 北京市大兴区科苑路 25 号
2	招标人名称：北人智能装备科技有限公司 招标人地址：北京市大兴区科苑路 25 号
3	资金落实情况：已落实
4	招标方式：公开招标 招标文件发布和获取：北人智能装备科技有限公司网站 www.beirenzn.com
5	投标书数量：正本四份。
6	现场勘察：2022 年 3 月 24 日 14：00 地址：北京市大兴区科苑路 25 号。 联系人：杨泰 13621089814
7	投标保证金：壹万元整。
8	投标文件的递交 投标文件递交截止时间：： 2022 年 4 月 6 日 13:30 投标文件递交地点：北人智能装备科技有限公司北京大兴科苑路 25 号
9	投标有效期：自投标截止之日起 120 天
10	开标时间： 2022 年 4 月 6 日 13:30 开标地点：北人智能装备科技有限公司北京大兴科苑路 25 号 开标形式：现场开标。
11	投标联系人： 周岚楠　　联系电话：80206089

第二章 投标须知

1、投标人资格

1.1 投标人应是在中华人民共和国境内注册、具有独立法人资格的企业。

1.2 投标人注册资金不低于【1000】万元人民币并实缴到位，投标人应提交前述证明材料。（投标人注册资金如为外币，以开标当日中国人民银行公告汇率中间价为基准换算成人民币）

1.3 投标人须具备开据增值税专用发票的一般纳税人资格或小规模纳税人资格。

1.4 投标人应当具有：计算机信息系统集成及服务资质和信息安全管理体系认证、IT 服务管理体系认证。

1.5 投标人不得存在下列情形之一：

（1）不具有独立法人资格的附属机构（单位）；

（2）被责令停业的；

（3）被有关机关暂停或取消投标资格的；

（4）财产被接管、冻结，或企业处于停产、停业、歇业或破产状态的；

（5）法定代表人为同一人或者存在控股、管理关系或其控股股东或实际控制人为同一人的不同单位，不得同时参加本招标项目投标。

1.6 本项目不接受联合体投标。

2、招标文件

2.1 招标文件中已阐明了本项目的要求及招标程序。

2.1.1 招标人为本次招标所作的一切有效的书面通知、修改及补充，均为招标文件不可分割的部分。

2.2 投标人应详细阅读招标文件中所有须知、格式、条款及要求，应按招标文件要求提供全部资料，如提交的投标文件未对招标文件做出全面的响应，则将有可能导致投标文件被拒绝。

2.3 招标文件的解释和澄清应以书面形式(包括书面文字、传真等，下同)为主，以电子文档方式为辅。

2.4 招标文件的补充和修改。招标人对招标文件所作的任何补充和修改均以北人

智能装备科技有限公司网站公告形式通知所有投标人。（北人智能装备科技有限公司网站 www.beirenzn.com）

2.5 招标文件的解释权归招标人。

2.6 本标书版权属招标人所有，未经许可，不得引用；投标人必须对本项目的所有招标文件进行严格保密，不得以任何原因向第三方透露本招标书中所包含的信息，如类似情况发生，招标人将保留追究责任的权利。

2.7 招标人提供的所有资料和投标人提供的投标文件，只能用于本次投标，不得用于其他用途。

3、投标文件

3.1 投标文件的组成。

3.1.1 投标文件由下述部分组成：

3.1.1.1 公司营业执照复印件、相关资质证书（盖公章）。

3.1.1.2 投标报价表及分项报价表（格式见附件一）。

3.1.1.3 投标人法定代表人授权书（格式见附件二）。

3.1.1.4 投标人承诺函（格式见附件三）。

3.1.1.5 近三年类似项目的业绩（格式见附件四）。

3.1.1.6 投标人关于资格的声明函（格式见附件五）。

3.1.1.7 安全免责声明（格式见附件六）。

3.1.1.8 投标技术方案，至少包含以下内容：技术资料（功能、性能、技术特点等），配置清单，实施方案。

3.1.1.9 关键项目响应表（格式见附件七）；

3.1.1.10 项目实施方案：项目实施进度计划，保证措施、质量保证计划及保证措施、项目管理、项目验收、系统故障时的应急预案、与相关单位的协作衔接、培训等。

3.1.1.11 证明投标人业绩及实力的资料或说明，包括不限于：投标人资质、项目经理、产品资质、安全产品原厂商服务能力、测评机构资质（参照评标评分构成及第四章技术标准和要求）。

3.1.2 投标人应仔细阅读并充分理解招标文件的全部内容，投标文件一经提交即

具有法律效力，视为投标人已经充分理解并完全确认招标文件的全部内容。

3.1.3 提交投标文件的截止时间前，投标人为本次投标所作的一切有效补充、修改文件，均被视为投标文件不可分割的部分。

3.2 投标文件的编制。

3.2.1 一般要求：

3.2.1.1 投标人应严格按照本次招标文件规定的格式和内容要求编制投标文件，逐项逐条地应答招标文件及所有附件和附表。

3.2.1.2 投标文件与招标文件若有差异之处，无论大小，均应给予说明。

3.2.2 投标文件的份数、签署、密封、标志：

3.2.2.1 投标文件正本四份打印装订成册；

3.2.2.2 除报价外投标文件须注明“不准提前启封”字样；密封处应加盖投标人公章。

3.2.2.3 报价（样式见附件一）四份，单独密封包装。

3.3 电报、电话、传真、电子邮件形式的投标概不接受。

3.4 投标文件的递交、修改与撤回。

3.4.1 投标文件递交：现场递交或邮寄递交

3.4.1.1 递交投标文件截止时间：2022 年 4 月 6 日 13:30

3.4.1.2 投标文件递交地点：北人智能装备科技有限公司北京大兴科苑路 25 号。

3.4.1.3 逾期递交或不符合规定的投标文件恕不接收。

3.4.2 投标文件的修改与撤回：

投标人可以在递交投标文件后,在规定的投标文件递交时间之前,以书面形式向招标单位递交修改或撤回其投标文件的通知。在规定的投标文件截止时间之后，不能更改投标文件。

投标人的修改或撤回通知，应按规定编制、密封、标志和递交。

3.5 投标文件的澄清。

评标委员会可要求投标人对其投标文件进行澄清,澄清和答复均应以书面或会议的形式进行。投标人需在投标文件中明确本项目授权代表的电话、手机、邮件和/或传真，作为投标人进行澄清的联系方式。

3.6 无效投标。发生下列情况之一者，视为无效投标：

3.6.1 投标文件未按规定要求密封和/或投标文件未按规定加盖公章和签字。

3.6.2 投标文件未按规定填写和/或投标文件内容与招标文件有严重背离。

3.6.3 投标报价表中漏项较多。

3.6.4 投标文件内容不全或字迹模糊辨认不清。

3.6.5 投标人不具备投标资格的。

3.6.6 由于投标人原因，投标文件在招标人要求提交投标文件的截止时间后送达的。

3.6.7 投标人在投标活动中实施损害招标人或者其他投标人合法权益的行为。

3.6.8 其他不符合招标文件要求的投标。

3.6 投标有效期。投标有效期自投标截止之日起 120 天。若中标，有效期延至协议终止日为止。

3.7 投标人承诺。

3.7.1 投标人承诺：本次招标过程中各阶段的全部文件，包括但不限于投标文件、澄清阶段的文件以及招标人与投标人双方确认的其他文件，均可作为最终双方签订协议的附件。

3.7.2 投标人须对投标文件中的应答做出郑重承诺。中标投标人如在合同执行中未履行上述承诺，招标人有权解除合同，投标人并应承担以此所引起的一切损失及责任。

4、开标

4.1 开标方式：现场开标。投标人携带身份证，授权书到开标地点参加开标。

4.2 开标时间：2022 年 4 月 6 日 13:30

4.3 开标地点：北人智能装备科技有限公司北京大兴科苑路 25 号

5、评标

5.1 招标人将根据招标项目的特点组建评标委员会，其成员由招标单位相关人员组成。

5.2 评标工作将遵循公开、公平、公正的原则，对所有投标文件的评审，都采用相同的程序和标准。

5.3 评标委员会经评审，认为所有投标都不符合招标文件要求的，可以否决所有投标。

5.4 评标对象为投标文件（及其有效的澄清及补充文件）。评标的依据为招标文件（及其有效的澄清及补充文件）。

5.5 招标人在评标时采用综合评分法对投标文件进行评审，具体评分构成如下：

序号	评审因素	分值	评分说明
A	**技术方面**	**35 分**	
1	技术方案	5	充分了解项目需求，针对本项目提出较好的建设思路和技术方案，评价为优得 5 分；较优得 4-2 分，一般得 0-1 分。
2	关键项目响应	25	以关键项目响应表为标准，响应符合全部要求，产品选型优良，功能性能能够完全满足要求，并且具有较好的稳定性和扩展性，得 25 分；出现非关键性项目负偏离，每出现 1 个扣 0.5 分，直至本项得 0 分；出现带★号关键项目负偏离的，本项得分得 0 分，4 项以上带★号关键项目负偏离的，投标做废处理。
3	项目实施方案	5	主要从项目实施进度计划及其保证措施、方案的科学合理性及对项目的质量保证计划及保证措施以及项目管理、项目验收、系统故障时的应急预案、与相关单位的协作衔接、培训等方面进行评定。评价为优得 5 分；较优得 4-2 分；一般得 0-1 分。
B	**商务方面**	**25 分**	
4	项目经理	6	投标人应提供项目经理在投标单位连续五年及以上的个人社保证明为 1 分，否则此项不得分。

			项目经理拥有信息系统项目管理师认证（证书复印件加盖公章）得1分；
			项目经理具有ITIL EXPERT证书、CISP信息安全服务证书、ITSS服务经理证书、高级工程师（每提供1个证书复印件得1分，最高得4分）。
5	产品资质	8	日志审计系统，具备TL9000电讯业质量管理体系认证证书、信息安全测评中心颁发证书的CISP培训机构证书，国家保密局颁发的涉及国家秘密的计算机信息系统集成资质证书（甲级）包含（系统集成、软件开发、运行维护），中国国家信息安全产品认证证书（增强级），每个得1分，最高得4分。
			数据库审计系统，具备TL9000电讯业质量管理体系认证证书、信息安全测评中心颁发证书的CISP培训机构证书，国家保密局颁发的涉及国家秘密的计算机信息系统集成资质证书（甲级）包含（系统集成、软件开发、运行维护），中国国家信息安全产品认证证书（增强级，每个得1分，最高得4分。
6	安全产品原厂商服务能力	2	项目主要产品（日志审计系统、数据库审计系统）的原厂商出具针对本项目的每个产品售后服务承诺函的，每提供一个得1分，以上主要产品全部出具的得2分。
7	测评机构资质	2	测评机构需要须具有国家网络安全等级保护工作协调小组办公室颁发的“网络安全等级保护测评机构推荐证书”得2分。
8	资质	5	**投标人提供的资质证明文件：**具有ITSS一级资质得（2分），具有

			ITSS 二级资质得（1 分）；具有 ISO14001 环境管理体系认证证书（1 分）；具有质量管理体系认证（1 分）；
9	投标人业绩	2	提供 2019 年 1 月 1 日-2021 年 12 月 31 日期间成功实施的 100 万以上投标人直签客户同类案例（网络安全），须提供项目合同复印件，包括但不限于：合同首尾页、合同金额、项目内容、双方签字页，提供 3 个案例得 2 分，每少提供一个案例扣 1 分；
C	**价格方面**	**40 分**	
10	报价得分	40	投标报价部分评分计算方法如下： 有效报价的最低者为评标基准价，评标基准价得 40 分。 每比评标基准价高 10000 元，扣 0.5 分，以此类推。（其中 5000（含）-10000 元扣 0.5 分，不足 5000 元的扣 0 分）
D	**总分**	**100 分**	**D=A+B+C**

6、中标结果通知与授予合同

6.1 招标人不对评标过程和中标结果进行解释，不退还投标文件。

6.2 招标人以电子邮件形式或电话通知中标结果。

6.3 中标人在接到中标通知后，在规定的时间内与招标人签订合同。

6.4 招标人终止招标的，应当及时发布公告，或者以书面形式通知投标人。招标人已收取投标保证金的应予退还。

7、程序规则与保密

7.1 从投标截止日期到签署协议时止，有关投标文件的审查、澄清、评议以及有

关签署协议的意向等一切情况均不得透露给投标人或与上述工作无关的单位和个人。

7.2参与评标的人员应严格遵守中华人民共和国招标投标法以及其它有关保密的法律、法规和规定，严格自律。

7.3 投标人申报的关于资质、业绩等的文件和材料必须真实准确，不得弄虚作假。

7.4 投标人不得串通作弊。

7.5 投标人不得以任何形式打听或搜集评标机密，不得以任何形式干扰评标或授标工作。

7.6 投标人若违反上述任何要求，其投标将视为废标。

8、 投标保证金

8.1 投标保证金：拟投标人在投标截止前，需缴纳壹万元的投标保证金。

8.2 投标保证金应采用人民币，以电汇的形式缴纳。

（接受投标保证金的账户：

账户名称：北人智能装备科技有限公司

账号：0200268209024575495

开户银行：工行北京大兴经济开发区支行）

8.3 凡没有缴纳投标保证金的投标将被拒绝。

8.4 中标人的投标保证金作为服务质量保证金，按合同约定退还。

8.5 未中标的投标保证金将在定标后 30 天内退还（不计利息）。

8.6 下列情况发生时，投标保证金将被没收；如下述（2）表述的情况发生时，招标单位将同时保留追究该投标人的法律责任。

（1）投标人在规定的投标有效期内撤回投标。

（2）投标人在被通知中标后，拒绝签订合同。

第三章 合同条款及格式

合　　同　　书

项目名称：北人智能装备科技有限公司-信息系统等级保护二级建设项目

甲方：北人智能装备科技有限公司

乙方：_____

乙方为甲方完成信息系统安全等级保护 2 级的备案测评进行的系统整改，经甲乙双方根据《中华人民共和国民法典》等相关法律法规的规定，经平等协商达成合同如下：

一、 定义

除非另有特别解释或说明，在本合同及与本合同相关的，双方另行签署的其他文件（包括但不限于本合同的附件）中，下述词语均依如下定义进行解释：

1、“项目”指 北人智能装备科技有限公司-信息系统等级保护二级建设 项目。

2、“合同”指甲乙双方签署的，与本项目相关的合同、附件、附录和其他一切文件。

3、“附件”是指与本合同的订立、履行有关的，经甲乙双方认可的，对本合同约定的内容进行细化、补充、修改、变更的文件、图纸、音像制品等资料。

4、“合同标的”指合同标的列表中所规定的硬件、软件、安装材料、备件及专用器具、文件资料及软件开发、技术服务等内容。

5、“货物”指根据合同规定乙方向甲方提供的硬件、软件、安装材料、备件及专用器具、文件资料。

6、“服务”指根据合同规定乙方向甲方提供的软件开发服务或者其他技术服务。

7、“检验”指甲方收到货物后，按照本合同约定的标准对合同货物进行的检测与查验。

8、“初验报告”指若甲方收到货物后由合同双方签署的到货检验合格确认书，即初验合格证书。

9、“终验报告”指本合同标的安装调试完成并上线试运行【 】日后由合同双方签署的终验合格证书。

10、“技术资料”指安装、调试、使用、维修合同货物所应具备的产品使用说明书和 / 或使用指南、操作手册、维修指南、服务手册、电路图、产品演示等文件及音像资料和/或

软件开发的相关技术文件。

11、“保修期”指本合同货物初验合格之日起，乙方以自担费用方式保证合同货物正常运行的时期，及本合同软件开发完成之日起，乙方以自担费用方式保证合同软件正常运行的时期。

12、“第三人”是指本合同双方以外的任何中国境内、外的自然人、法人或其他经济组织。

13、“法律、法规”是指由中国有关部门制定的法律、行政法规、地方性法规、规章及其他规范性文件以及经全国人民代表大会常务委员会批准的中国缔结、参加的国际条（公）约的有关规定。

14、**合同文件**

下列文件构成本合同的组成部分，应当认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

a.本合同书

b.中标通知书

c.合同条款

d.投标文件(含澄清文件)

e.招标文件其他内容

二、 合同标的

乙方向甲方出售列表中所列货物及相关服务。

序号	设备名称	数量	单位
1	日志审计系统	1	台
2	数据库审计系统	1	台
3	服务器防护系统	1	套

4	等保测评服务	1	套
5	机房环境整改	1	项

三、 合同价格

1、 本合同总金额为人民币大写【】（¥【】）（合同总金额已含各项税费）。

其中软硬件产品金额为人民币大写【】（¥【】），税率为 13%；

服务工作金额为人民币大写【】（¥【】），税率为 6%；

其余____工作金额为人民币大写【】（¥【】），税率为___%；

整体工作内容详细报价见附件一《分项报价表》

2、 本合同项下详细工作说明见附件二《工作说明书》

四、 支付和结算方式

1、 双方因本合同发生的一切费用均以人民币结算及支付。

2、 乙方的账户名称、开户银行及账号以本合同提供的为准。

乙方：户　名:_____
开户行:_____
账　号:_____

3、 甲方的开票信息：

名称：北人智能装备科技有限公司，

纳税人识别号：91110115MA00FJRM2E，

地址、电话：北京市大兴区经济开发区科苑路 25 号 5 幢 1 层 108 80206018

开户行及账号：工行北京大兴经济开发区支行 0200268209024575495

4、 付款方式： 分期付款

1)合同签订后 7 个工作日内甲方以_____结算方式向乙方支付货物和服务价款的_35_%

为预付款即人民币_____元整（小写：_____）。

2）乙方将合同货物全部运抵交货地点并经甲方核对无误，双方签署到货报告。完成各项整改及系统评测报告，等级保护整改工作完成后进行最终验收，终验完成后付款：合同货物安装调试完成且服务工作完成后取得等级保护最终测评报告符合度达标，双方签署终验报告后 7 个工作日内甲方以_____结算方式向乙方支付货物和服务价款的__60_%即人民币元整（小写：_____）。

3）服务完成 2 年后，甲方以_____结算方式向乙方支付货物和服务价款的__5_%即人民币_____元整（小写：_____）。

4）乙方在收到甲方付款同时，应向甲方开具相应金额的增值税专用发票。

5）乙方向甲方开具的发票不作为甲方已经完成付款的凭证，甲方相应款项到达乙方指定账户视为完成相应的付款义务。

五、交货及服务期限

1、 交货方式 ：现场交货

货物应运至甲方指定地点，并卸至甲方指定位置，经甲方核对无误后当日，双方签署初验报告。若到货后三个工作日内因甲方原因未能签署初验报告，视为初验报告已签署。初验报告一式两份，甲方和乙方各执一份。由于甲方原因,导致货物不能放至甲方指定位置时应由甲方负责另行提供暂时存放地点直至厂商装机完毕 。

2、 交货日期：合同签订后【30】工作日内到甲方指定地点。

3、 交货（安装、调试、服务）地点 ：大兴区科苑路 25 号。甲方应在乙方发货前通知乙方发货地点。

4、 乙方应于合同签订之日起【4】个月内完成本项目。

六、包装和标记

1、 乙方交付的所有合同货物应具有适于运输的坚固包装，并且乙方应根据合同货物的不同特性和要求采取防潮、防雨、防锈、防震、防腐等保护措施，以确保合同货物安全无损地送达交货地点。

七、货物和服务的标准

1、 乙方应保证提供给甲方的合同货物是货物生产厂商原造的并完全符合原厂质量、性能和规格的要求。

2、 乙方应保证所提供的货物经正确安装、合理操作和维护保养在其使用寿命期内具有的性能。

3、 乙方承诺提供给甲方的合同货物质量应符合中华人民共和国标准及相应的技术规范要求。乙方承诺向甲方提供的服务应符合中华人民共和国标准和本合同附件的要求。乙方承诺完成本合同后，甲方能够达到信息系统等级保护 2 级的要求，完成等级保护 2 级的备案和测评。

4、 甲方对合同货物的数量、规格和质量的检验，应依据第七条第 3 款约定的质量标准进行。采用现场交货方式的，检验在交货地点进行。

5、 开箱检验时双方应派员参加，并签署开箱验收记录，以此作为双方确定责任的依据。

6、 若检验时发现货物数量不足、规格与合同要求不符或开箱时虽然货物外包装完好无损，但箱内货物短缺或损伤，双方应签署书面形式证明，乙方应根据该证明及时补足或更换。

7、 合同货物安装调试完成且软件开发完成后进入试运行期间，在经过【 】天试运行期后，双方组织验收，签署最终验收报告。在试运行期间，乙方应保证货物正常运行，若在此期间货物发生故障，试运行期间应从故障排除之日重新计算。

8、 乙方提供的机房整改服务中的内容，应当符合相关标准，能够满足等级保护 2 级的要求。

八、技术服务和保修责任

1、 乙方对合同货物的质量保修期为到货合格之日起【 】个月。本合同项下为服务工作保修期为本合同服务工作最终验收合格之日起【 】个月。

2、 乙方承诺在合同货物的质量保修期内免费为甲方提供合同货物的技术指导和维修服务，技术指导的包括但不限于：微信、电话、上门等方式。乙方提供热线支持服务的时间是：【7*24 小时】。

3、 在合同货物保修期届满后，乙方保证继续为甲方提供维修服务，甲方应按乙方提供的优惠价格向乙方支付相关费用。

九、违约责任

1、 迟延交付的违约责任

如果乙方未按照合同规定的要求交付合同货物和提供服务，每逾期一周，乙方应按照逾期未交付金额的百分之零点五计算，向甲方支付逾期交付违约金。

2、 延期付款的违约责任

如甲方无正当理由未按照合同约定时间或金额支付合同价款，每逾期一周，甲方应按照逾期应付未付金额的百分之零点五计算，向乙方支付逾期付款违约金。

3、 乙方因任何原因未按本合同约定履行本合同，均视为违约，乙方应按照本合同全部价款的 20%向甲方支付违约金。给甲方造成损失的，乙方应承担全部赔偿责任。

4、 其它约定：因甲方装机条件不具备导致乙方不能按合同规定期限完成装机，乙方不负有违约责任。

十、不可抗力

1、 不可抗力指下列事件：战争、动乱、瘟疫、严重火灾、洪水、地震、风暴或其他自然灾害，以及本合同各方不可预见、不可防止并不能避免或克服的一切其他事件。

2、 任何一方因不可抗力不能履行本合同规定的全部或部分义务，该方应尽快通以书面形式向另一方提供详细情况报告及不可抗力对履行本合同的影响程度的说明。

3、 发生不可抗力事件，任何一方均不对因不可抗力无法履行或迟延履行本合同义务而使另一方蒙受的任何损失承担责任。但遭受不可抗力影响的一方有责任尽可能及时采取适当或必要措施减少或消除不可抗力的影响。遭受不可抗力影响的一方对因未尽本项责任而造成的相关损失承担责任。

十一、联系方式

1、 合同双方发出与本合同有关的通知或回复，应以专人送递、传真或特快专递方式发出；

如果以专人送递或特快专递发送，以送达至对方的住所地或通讯联络地为送达；如果以传真方式发送，发件人在收到传真报告后视为送达。

2、 合同双方发出的与本合同有关的通知或回复均应发至以下通讯地址，付款或收款应使用以下账号，一方变更通讯地址或账号，应自变更之日起三个工作日内，将变更后的地址通知对方。变更方不履行通知义务的，应对此造成的一切后果承担法律责任。

甲方：　　联系人：

地址：　　电话：

乙方：　　联系人

地址：　　电话

3、 上述发出通知、回复的费用由发出一方承担。

十二、保密条款和知识产权条款

1、 任何一方对其获知的本合同及附件中其他各方的商业秘密和国家秘密负有保密义务。

2、 除非法律、法规另有规定或得到本合同另一方的书面许可，任何一方不得向第三人泄露前款规定的商业秘密和国家秘密。保密期限至上述商业秘密和国家秘密为公开信息时。

3、 双方同意，甲方委托乙方开发的软件产品的知识产权、著作权归属甲、乙双方共有。

十三、合同的解释和法律适用

1、 任何一方对本合同及其附件的解释均应遵循诚实信用原则,依照本合同签订时有效的中国法律、法规以及通常的理解进行。

2、 本合同标题仅供查阅方便，并非对本合同的诠释或解释；本合同中以日表述的时间期限均指自然日。

3、 对本合同的任何解释均应以书面作出。

4、 本合同及附件的订立、效力、解释、履行、争议的解决等适用本合同签订时有效的中华人民共和国法律、法规的有关规定。

十四、合同的终止

1、 本合同因下列原因而终止：

1) 本合同正常履行完毕；

2) 合同双方协议终止本合同的履行；

3) 不可抗力事件导致本合同无法履行或履行不必要；

4) 任何一方行使解除权，解除本合同。

2、 对本合同终止有过错的一方应赔偿另一方因合同终止而受到的损失。对合同终止双方均无过错的，则各自承担所受到的损失。

十五、权利的保留

1、 任何一方没有行使其权利或没有就违约方的违约行为采取任何行动，不应被视为是对其权利的放弃或对追究另一方违约责任权利的放弃。任何一方放弃针对违约方的某种权利，或放弃追究违约方的某种责任，不应视为对其他权利或追究其他责任的放弃。

2、 如果本合同部分条款依据现行有关法律、法规被确认为无效或无法履行，且该部分无效或无法履行的条款不影响本合同其他条款效力的，本合同其他条款继续有效；同时，合同双方应根据现行有关法律、法规对该部分无效或无法履行的条款进行调整，使其依法成为有效条款，并尽量符合本合同所体现的原则和精神。

3、 在本合同履行期间，因中国法律、法规、政策的变化致使本合同的部分条款相冲突、无效或失去可强制执行效力时，双方同意合作尽快修改本合同中相冲突或无效或失去强制执行效力的有关条款。

十六、争议的解决

1、 合同双方应通过友好协商解决因解释、执行本合同所发生的和本合同有关的一切争议。

如果经协商不能达成协议，则双方同意在甲方所在地有管辖权人民法院即北京市大兴区人民法院提起诉讼。

十七、合同的补充、修改和变更

1、 双方协商一致，可以对本合同进行补充、修改或变更。

2、 对本合同的任何补充、修改或变更必须以书面形式进行。

3、 双方签订的补充协议以及修改或变更的条款与本合同具有同等法律效力。

十八、合同的生效

1、 本合同经双方法定代表人（负责人）或授权代表签字并加盖单位公章或合同章后生效。

十九、其它约定事项

1、 本合同未尽事宜，双方协商解决。

2、 本合同中的附件均为本合同不可分割的部分，与本合同具有相同的法律效力。

3、 本合同一式四份，甲乙双方各两份，每份具有同等法律效力。

以下无正文

甲方：　　乙方：

单位名称（公章或合同章）　　单位名称（公章或合同章）

法定代表人或授权代表法定代表人或授权代表：

签约日期：年　月　日　　签约日期：　年　月　日

本合同附件：
一、《分项报价表》
二、《工作说明书》

第四章 技术标准和要求

1.项目概述

1.1 项目背景

为了保障北人智能网站和 OA 系统的安全、稳定、持续运行，同时根据业务系统存储信息及影响范围进行调研判断，OA 和网站应至少满足等保二级系统评测要求，因此需要对北人智能机房物理环境、网络环境和安全系统进行整改。

1.2 项目内容

根据北人智能装备科技有限公司 OA、网站系统目前实际情况，综合考虑现有的机房基础环境及安全防护措施，与《信息安全技术网络安全等级保护基本要求》间存在的差异，整改机房基础环境及信息系统中存在的薄弱环节，提高业务系统的安全防护水平,完善安全管理制度体系。投标人应当帮助招标人完成备案。

结合国家相关政策文件精神和等级划分的原则,国有企业内部信息系统构筑至少应达到二级或以上防护要求，因此 OA、网站系统拟定为等保第二级，所以需要对信息系统及现有机房环境进行符合相应安全保护等级的安全整改措施,具体包括以下方面：

1. 系统中部署部署综合安全审计设备（日志审计系统、数据库审计系统），对网络边界、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；
2. 服务器安全防护软件，为服务器提供安全保护的软件。提供检测和杀灭木马、病毒，保护网络安全，增强服务器的安全性。避免配置风险，底层驱动保护
3. 等保测评服务，为 OA 和网站系统提供差距分析、整改方案、协助甲方完成定级备案、差距分析、网络安全架构整改、安全制度整改和漏洞扫描等工作，完成测评报告编写工作，出具测评报告。
4. 机房环境：对现有网络布线进行整理，线路的标记、核对、巡线、标签；

机房环境进行调整、不限于吊顶、隔断、地板、墙面。配电、照明系统和制冷系统、门禁系统和动环监控系统等。满足现场办公和网络安全相关要求。

5. 提供满足等级保护 2 级要求的阿里云服务器所须安全组件选型。

1.3 项目集成服务要求

本项目等级保护安全测评服务，协助用户完成测评系统的备案、现场测评和整改等服务，取得等保测评报告。

本项目集成服务包括软硬件设备的安装、联调、配合现有网络优化和安全配置提供升级和系统终验工作。

本项目涉及网络安全系统集成测试，是一项复杂的系统工程，对建设标准要求高，要求建设单位具备相应的能力。

1.4 项目工期和建设要求

本项目要求自合同签订开始，机房整改与设备到货安装在 45 天内完成、测评工作（以拿到测评报告为准）在 120 天内完成，进行正式验收。

2. 技术和服务要求

本项目技术和服务方面要求如下：

2.1 项目采购产品列表

序号	设备名称	数量	单位
1	日志审计系统	1	台
2	数据库审计系统	1	台
3	服务器防护系统	1	套
4	等保测评服务	1	套
5	机房环境整改	1	项

2.2 项目采购产品技术要求

1. 日志审计系统

类别	功能及技术描述
性能要求	★1U 机架式设备，不少于 6 个千兆电口，存储容量不少于 4TB。支持 50 个日志源授权。包含日志收集、存储、查询、统计分析等功能。综合采集处理均值 5000EPS。
数据采集	★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；
数据存储	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；
数据查询	支持为不同类型日志设置不同的查询条件和显示条件；
数据查询	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；
告警管理	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；
日志源管理	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；
系统管理	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。
系统管理	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；
《计算机信息系统安全专用产品销售许可证》	★所提供的产品检验报告须符合《信息安全技术 日志分析产品安全技术要求 GA/T 911-2019》检验规范，增强级；
IT 产品信息安全认证证书	★所提供的产品获得中国信息安全认证中心颁发的《IT 产品信息安全认证证书》，需符合《日志采集与分析产品安全技术要求》，并提供完整的检测报告复印件；
IPv6 Ready Logo 认证	★所提供的产品获得全球 IPv6 论坛 IPv6 Ready Logo 委员会颁发的 IPv6 Ready Logo 认证证书；
计算机软件著作权登记证书	★所提供的产品获得国家版权局计算机软件著作权登记证书
TL9000 认证	TL9000 电讯业质量管理体系认证
安全开发二级及以上	中国信息安全测评中心颁发的《安全开发资质认证二级及以上》
CISP 培训机构	信息安全测评中心颁发证书的 CISP 培训机构
涉甲级资质	国家保密局颁发的涉及国家秘密的计算机信息系统集成资质证书（甲级）包含（系统集成、软件开发、运行维护）

2. 数据库审计系统

类别	功能及技术描述
性能要求	★1U 机箱， 不少于 6 个千兆电口，不少于 1TB 存储空间，单电源；审计能力 100Mbps，SQL 处理数 1000 条/秒。含 3 应用识别库。
数据库类型	★支持 Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata 等数据库系统
	支持 Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis 等国际主流数据库系统
	支持 KingBase、DaMeng、Oscar、GBase、Inspur_KDB、Highgo、GaussDB 等国内主流数据库系统
主流业务协议审计	★支持 HTTP、Telnet、FTP、SMTP、IMAP、POP3 的审计
主流业务协议审计查询	HTTP 协议支持按 HTTP 访问域、URL、请求类型、请求文件、Cookie、返回码等 34 个分项作为查询和统计的条件
	Telnet 协议支持按 telnet 命令、返回信息等 20 个分项作为查询和统计的条件
	FTP 协议支持按 ftp 命令、传输文件信息、ftp 用户名、密码等 23 个分项作为查询和统计条件
	邮件协议支持按邮件主题、附件、发送 ip 等 24 个分项作为查询和统计的条件
数据库监控	支持依据数据库实例监控各个数据的数据库类型、活跃会话数、总会话数、负载等信息
	支持依据数据库实例监控各个数据库的连接池、缓冲区、表空间、死锁、CPU、内存、硬盘等信息，可自定义告警阈值进行健康评估
	支持自定义时间条件进行各个数据库的会话趋势、SQL 操作趋势、安全趋势、访问源趋势的图表展示
	支持自定义审计精确到秒级的流入流出总流量趋势、总体新建与并发会话数趋势、总体资源占用率趋势
SQL 操作统计	支持各类 SQL 操作数量以及占比情况
应用流量监听	支持审计各个应用协议的流量大小和数据包数量，并以图表形式进行排名；
	支持自定义时间查看各个协议审计的流量趋势图，直观展示应用流量的监听情况
设备运行状态	支持首页直观展示数据库审计系统的运行情况，比如并发连接数、每秒新建连接速率、版本号、运行时间以及 CPU、内存、硬盘等资源占用情况

数据库攻击行为审计	★支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为，利用漏洞攻击等行为进行审计，并进行实时报警
SQL 错误统计	多个维度展示错误占比及趋势，从源 IP 维度以柱状图展示 SQL 错误数（TOP10）
SQL 错误分析	以列表形式给出出错原因、出错信息以及解决办法
SQL 效率分析	★以饼图展示正常 SQL 与慢 SQL 占比情况、TOP10 慢 SQL 的详细分析：TOP 排名信息、事件 ID、数据库名、目的 ip、协议类型、源 ip、sql 响应时间、操作类型、具体 sql 语句等要素
会话回放	支持会话回放功能,并至少支持 0.5 倍速、1 倍速、1.5 倍速、2 倍速、4 倍速五级播放速度调节
翻译功能	实现对 SQL 语句报警内容自定义成中文自然语言的描述功能，便于非技术人员理解报警内容；
数据查询	支持基于数据库时间、源/目的 IP、数据库名、应用协议、数据库表名、字段值、预处理 SQL、SQL 关键词、数据库返回码、SQL 响应时间、数据库操作类型、影响行数等条件的审计查询。
	边查询边统计机制，页面采用异步加载技术，保障查询和统计效率
	查询方式支持精确查询与模糊查询两种模式，并支持自定义保存当前查询条件，为后续查询提高便捷
复杂 SQL 审计能力	支持超长 SQL 语句审计，至少不低于 2M
	支持嵌套 SQL 语句的审计
	准确审计绑定变量的 SQL 语句
	有效分割、准确审计主流数据库协议的多 SQL 语句
版本回滚	支持历史版本回退功能，系统内建历史版本库不少于 3 个
操作系统	安全操作系统采用冗余设计，可在设备命令行启动过程中选择主备系统
云检测	支持云检测，可对本单位部署的同一品牌的多台审计或者多类型安全设备（版本号、序列号、型号、运行时长、CPU 和内存占用、并发和新建连接数、设备流量等）进行远程统一检测，保障各设备的安全稳定运行
系统抓包	支持抓包工具（可配置抓包个数、源和目的 IP、协议等）、系统巡检、网络诊断、规则库升级
一键巡检	支持系统本身主要运行功能服务模块的运行状态巡检，保证系统安全稳定运行
配置与策略	支持系统配置文件和系统策略的密文导入导出，不可设置为明文
安全浏览器管理	支持红莲花、密信等安全浏览器登录管理设备，该类浏览器支持国密算法 SM2/SM3/SM4，安全性非常高
系统登录连接数设置	支持 webui/ssh/telnet 方式登录系统的最大连接数设置
日志外发	支持 Syslog、SNMP、kafka 等方式外发日志

磁盘管理	支持手动、自动方式的磁盘清理，可根据剩余空间、保存时限等条件灵活设置，磁盘空间占用情况的检查频率可灵活设置：10min、30min、1h、3h、6h、24h 等时长 ），支持存储外发。
告警级别	支持告警级别划分，至少分为七类，例如：紧急、警告、一般等级别，以便运维人员作出不同响应
报表模板	支持等保、萨班斯法案报表模板以及自定义报表，可以按日、周、月等周期自动生成报表
《计算机信息系统安全专用产品销售许可证》	★《计算机信息系统安全专用产品销售许可证》，证书类别必须为：数据库安全审计类（增强级）
IPV6 认证中心证书	★所提供的产品获得全球 IPv6 论坛 IPv6 Ready Logo 委员会颁发的 IPv6 Ready Logo 认证证书；
信息技术产品安全测评证书	信息技术产品安全测评证书，级别：EAL3+
中国国家信息安全产品认证证书	中国国家信息安全产品认证证书，增强级
TL9000 认证	TL9000 电讯业质量管理体系认证
安全开发二级及以上	中国信息安全测评中心颁发的《安全开发资质认证二级及以上》
CISP 培训机构	信息安全测评中心颁发证书的 CISP 培训机构
涉甲级资质	国家保密局颁发的涉及国家秘密的计算机信息系统集成资质证书（甲级）包含（系统集成、软件开发、运行维护）

3. 服务器安全防护系统

类别	功能及技术描述
操作系统兼容性	支持windows/linux主流操作系统,包括但不限于以下的操作系统：Windows Server 2003 SP2（x86/x64）、Windows Server 2008（x86/x64）、Windows Server 2012、Windows Server 2016、Windows Server 2019；
	RedHat 4.3~RedHat 5.11（x86/x64）、RedHat 6.0~RedHat 6.7（x86/x64）、RedHat 7.0~RedHat 7.2 RedHat8.0 ；
	CentOS 4.3~CentOS 5.11（x86/x64）、CentOS 6.0~CentOS 6.10（x86/x64）、CentOS 7.0~CentOS 7.6、Centos8.0；
	Ubuntu10.0 以上；
	Suse 10~Suse 10 sp3、Suse 11~Suse 11 sp3、Suse12；中标麒麟、红旗 Redflag3~4；

产品安全机制	客户端具有反逆向、反调试功能、自保护功能，客户端和管理中心通信采用安全的加密机制
	支持自我防护技术，即使客户端被意外关闭，防护依然有效
风险发现	支持服务器系统级、数据库、中间件、应用级的弱口令、口令复用扫描，并可对扫描的结果进行修复验证，还可对口令风险的扫描任务进行设置，包括任务名称、目标服务器、扫描类型、扫描所用字典、执行周期等方式。
基线检查	支持 CIS、等级保护二级、三级检查，系统内置官方等保 2.0 的二级、三级基线模板，满足等保二级及等保三级要求，同时支持用户自定义基线检查任务。并支持基线检查结果的图形化统计，包括：合规率、问题项 TOP5、风险服务器 TOP5 等维度的统计，并可导出基线检查报告。
病毒查杀	采用主动的方式进行自动化病毒查杀，可支持 Bitdefender、ClamAV、Qowl 等多引擎技术识别并查杀最新病毒；可支持病毒文件自动隔离、自动删除、不处理三种方式。并可将病毒查杀的结果导出报告
威胁总览	支持统计并展示服务器的可疑威胁及告警信息，包括：可疑威胁事件统计、可疑威胁分布、可疑问些趋势，以及具体的威胁事件列表，并可对威胁事件进行研判，还可将威胁事件导出为 EXCEL 格式的报告
防恶意扫描	以攻击者视角、受害者视角展示恶意扫描的事件，包括：服务器名称、负责人、所属部门、操作地址、最近发生时间、受害 IP、攻击 IP 等信息，并可将事件加入黑名单或白名单，还可对受害的 IP 进行防端口扫描、屏蔽扫描器等设置
暴力破解检测	对暴力登录系统的账号和 IP 进行自动发现并上报暴力破解入侵事件，支持对 RDP、SSH、FTP 等服务的暴力破解行为进行检测拦截，支持设定暴力破解行为的请求范围、失败次数，针对暴力破解的 IP 支持设定锁定时长。
异常登陆监测	以违规登录、可疑登录的视角，对异常登录行为进行监控及告警，包括：登录账号、来源 IP、登录区域、服务器 IP、操作系统等，并可进行登陆规则的设置，以及告警设置
后门检测	支持对操作系统、文件、软件中存在的后门进行检测，包括：发现时间、后门名称、后门类型、风险等级、服务器名称、服务器 IP、操作系统等，并可进行隔离、删除、加白、下载等操作，并提供后门的详情信息

Webshell 检测	自动识别 web 服务目录，并实时进行 webshell 后门的扫描，包括：危险级别、文件路径、文件代销、文件 MD5、文件修改时间、webshell 发现时间、感染服务器等信息。
反弹 shell 检测	可实时发现反弹 shell 等危险的反链操作风险，包括：发起连接主机、服务器名称、服务器别名、AgentID、服务器 IP、操作系统等信息，并支持事件的上报和阻断。
性能监控	支持对服务器主机的 CPU 利用率、内存使用率、磁盘使用率进行监控，支持展示近 1 小时、近半天、近 1 天、近 7 天、近 1 个月、近 1 年的监控数据
	支持对自身 Agent 的 CPU 利用率、内存使用率进行监控，支持展示近 1 小时、近半天、近 1 天、近 7 天、近 1 个月、近 1 年的监控数据
	支持对当前的客户端性能、服务器主机性能监控数据进行导出
报表生成下载	支持各类日志、安全报表、资产报表、事件报表、功能状态报表的综合下载导出，并可根据实际情况对报表内容进行自定义导出
产品后台管理	支持展示客户端的安装时间、当前客户端版本、最新客户端版本、启动时间、结束时间、更新状态进行展示
	支持批量对客户端的版本进行更新
	支持离线安装、命令安装客户端，采用命令安装时支持设置代理地址、默认端口、安装路径、磁盘检测、是否允许覆盖安装等参数
账号管理	支持创建子账号，创建账号时支持配置其角色、上级账户、绑定服务器，支持添加归属人、手机号、邮箱、备注等附属信息
资质要求	产品拥有自主知识产权，具有国家版权局颁发的“计算机软件著作权登记证书”
	产品拥有公安部颁发的销售许可证

4. 等保测评服务

差距测评	依据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）及行业管理规范，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理层面对已定级的信息系统（被测对象）进行安全测评，分析所采取的安全保护措施与等级保护标准要求之间的差距，并出具初测初稿。

	依据《信息安全技术网络安全等级保护测评过程指南》(GB/T 28449-2018)及行业管理规范对已定级的信息系统（被测对象）进行漏洞扫描，并出具《安全漏洞扫描报告》。每个信息系统的漏洞扫描均包含一次初测和一次复测。
实施内容	依据初测初稿、《安全漏洞扫描报告》、提出安全建设整改建议，形成初测终稿（即《差距分析测评报告》和《安全整改建议》）
建设标准	满足以下标准： 信息安全技术 网络安全等级保护实施指南（GB/T25058-2019） 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 网络安全等级保护设计技术要求（GB/T25070-2019） 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） 信息安全技术 网络安全等级保护定级指南（GB/T22240-2020）

5. 机房环境

类别	功能及技术描述
吊顶	铝合金微孔板 61 ㎡
墙面	包括现有房间墙面修复和涂料、不锈钢地脚线、防尘处理。增加不锈钢隔断（原隔断拆除）
防火门	甲级钢制防火门 2 套
照明	包含 8 套 LED 平板灯、照明配电箱、灯具墙面插座、开关、应急照明等
地板	配合房间内现有地板提供地板修复，将现储藏间地板扩容、增加门口踏步
配电箱	机房总输入配电箱 1 套、连接机房一级配电箱，UPS 输出，改造现有机柜为市电和 UPS 电源冗余输出及配套电缆和 PDU 等，提供防雷接地相关实施工作和辅材
门禁	提供人脸识别门禁系统 1 套
空调	提供工业空调 1 套，并且根据新的机房机柜拜访位置调整现有空调设施。
信息点标记	将现有办公区信息点进行标记、与机房配线端进行核对、巡线、标签。
机柜设备整理	将现有机柜内服务器、网络和安全设备、配线架等进行梳理、按照 IT 系统管理规范进行梳理、调整、增加机柜、机柜 重新定位、标记和线缆连接。
动环监控系统	提供 1 套动力环境监测系统，提供漏水监测、温度和湿度监控、UPS 监测模块、提供远程图形界面

3.实施需求

3.1 项目实施要求

项目实施不能影响企业正常运转，工作时间由甲乙双方共同确定。

项目实施期间需定期召开工作例会。项目实施过程的重大问题向甲方项目组进行汇报。

严格进行项目管理，各阶段都应提交相应的计划、设计，并经甲方认可后方可进行下阶段工作，应确保人力、物力的定量投入，定期向甲方提交项目进展情况报告。

3.2 进度要求

投标人应根据自己的实际解决方案及能力综合分析，提供相应的实施计划安排。

1）提供实施团队成员名单。

2）合同签定后确定项目经理，在项目结束前不允许更换，如需更换需提前5-7 个工作日书面提交申请，招标人面试同意后方可更换。

3）给出项目实施的进度表。

4.售后服务

本项目要求投标人提供所有软硬件设备不少于三年的质保服务。服务内容如下：

定期巡检：每个质保年度对本项目进行巡检，并出具巡检报告。

远程支持：提供 7×24 小时电话和邮件技术支持。

现场支持：投标人自接到招标人设备故障通知后，须派工程师于 4 小时内到达指定现场，并到达现场直至故障解决为止。

升级服务：投标人需在必要时对本项目产品的软硬件进行固件升级和系统 BUG 修复，以保证系统稳定运行。

5.培训要求

投标人需针对本项目建设所涉及软硬件系统进行培训。培训要求包括以下方面。

5.1 培训内容

5.1.1 系统设计宣贯培训

针对系统结构、信息安全使用等方面，对系统运维人员进行培训。

5.1.2 系统运维及使用培训

针对系统运及系统日常使用情况的培训，以确保日常维护人员及管理人员的

正确使用，时间不少于 1 天。

5.2 培训方式要求

需提供详细的培训方案和培训承诺。培训方案主要包括培训内容、培训计划、培训对象和培训资料等几个方面，并按照上述要求进行详细说明。

5.2.1 培训日期

进行有针对性的专门的技术培训，包括操作使用、日常维护、简单故障处理等内容，确定培训时间。

5.2.2 培训对象

培训对象主要分为技术维护人员，具体培训人员数量依据实际操作情况决定。

5.2.3 培训目的及内容

培训目的应使系统的操作人员对项目软硬件设备功能有清晰的了解；能够正确使用相关系统；能够应对一般故障的紧急处理；掌握常见的故障判断、原因分析、日常检查等。

针对技术维护人员的培训除了要具备操作人员的技能外，还要包括理论讲解和实际操作，使有关技术人员能够熟悉系统情况，充分掌握相关系统功能，熟练操作和使用系统，可以设置系统参数，并能明确判断故障原因，独立处理一般故障，恰当地维护系统。

培训结合本项目设备的安装与调试，以授课教学为基础，结合实际系统，在现场进行。

培训内容应该包括原理、操作、应急处理和维护等。

第五章 附件

附件一：投标报价表及分项报价表

投标报价表

序号	投标分项	投标价	项目建设周期	备注
1	日志审计系统			
2	数据库审计系统			
3	服务器防护系统			
4	等保测评服务			
5	机房环境整改			
	总计	小写金额：人民币_____元 大写金额：人民币_____元		
	其中	软硬件产品金额为¥_____元（大写：_____） 服务工作金额为¥_____元（大写：_____） 其余____工作金额为¥_____元（大写：_____）		

以上报价均包含招标文件第四章规定的为完成本期项目的全部费用。

投标人：（盖章）

投标人法人代表或委托代理人（签章）：

日　期：　　年　月　　日

注：所有要求签字、盖章的地方须由法定代表或授权代表签字、盖章；“投标书”中的投标报价表应与投标分项报价表一致，若不一致，将以“投标报价表”上合计大写金额数为准；投标报价金额均以人民币表示。

投标分项报价表

投标分项：

序号	产品名称	品牌/型号	配置参数	数量	单价	金额	税率	备注
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
	投标分项合计价：￥_____元（大写：_____）							
	软硬件产品金额为¥_____元（大写：_____） 服务工作金额为¥_____元（大写：_____） 其余____工作金额为¥_____元（大写：_____）							

注：（1）此表中报价按《投标报价表》中分项项目：日志审计系统、数据库审计系统、服务器防护系统、等保测评服务、机房环境整改 5 个部分进行详细报价。
（2）备注说明为：软硬件产品，服务工作、其余____工作三类。
（3）软件系统可不写品牌和型号。

投标人：（盖章）

投标人法人代表或委托代理人（签字）：
日　期：

附件二：投标人法定代表授权书（格式）

投标人法定代表人授权书

项目名称：北人智能装备科技有限公司_____项目

日期：

致：北人智能装备科技有限公司

〔投标人名称〕，为合法注册和营业企业，注册地址_____。

本人（授权人姓名）特授权（被授权人姓名）（身份证号：　　）代表我公司全权办理针对上述项目提交投标文件、办理投标事宜、签署相关文件以及中标后代表我公司与贵公司签订合同等具体工作。

我公司对被授权人签署的全部文件承担全部责任。

授权人签名：　　被授权人签名：

职务：　　职务：

投标人公章：

被授权人身份证复印件附后

附件三：投标人承诺函（格式）

投标人承诺函

项目名称：

北人智能装备科技有限公司_____项目

日期：

致：

本公司荣幸地参与上述项目的投标，并在此作如下承诺，本公司：

1. 完全理解招标文件的一切规定和要求。
2. 以合法的、正当的方式竞标，不采取非正当的违反法律规定的竞争方式。
3. 向贵公司提供最优惠的价格，不以任何方式向任何人提供佣金等以干扰定标。
4. 按照招标文件的要求向贵公司提交下列文件：

（1）投标报价表；

（2）贵公司招标文件中要求提交的其它文件或资料。

5. 若中标，我方将按照招标文件的具体规定与贵公司签订合同，并且严格履行合同义务，为贵公司提供优质的服务。如果在合同执行过程中，发生服务质量问题，我方一定按贵公司要求尽快解决，并承担相应的责任。
6. 在整个招标过程中，我方若有违规行为，贵方可按招标文件之规定给予惩罚，我方完全接受。
7. 若中标，本承诺函将成为投标文件及合同不可分割的一部分，具有同等的法律效力。

法定代表人或授权代表（签字）：

投标人（盖章）：

附件四：

近三年类似项目的业绩

单　位			
项　目 名 称			
规　模			
完成日期 （年/月/日）			
项目主要情况			
…			

提供 2019 年 1 月 1 日-2021 年 12 月 31 日期间成功实施的 100 万以上投标人直签客户同类案例（网络安全），须提供项目合同复印件，包括但不限于：合同首尾页、合同金额、项目内容、双方签字页。

投标人：_____（单位全称）（盖章）_____

法定代表人或授权代表：_____（签字）_____

日　　期：　　年　　月　　日

附件五：

投标人关于资格的声明函

项目名称：

日期：

致：北人智能装备科技有限公司

我公司愿意针对上述项目进行投标。投标文件中所有关于投标人资格的文件、证明、陈述均是真实的、准确的。若有不实或者违背，我公司承担由此而产生的一切责任和后果。

特此声明。

法定代表人或授权代表（签字）：

投标人（盖章）：

附件六：

安全免责声明

我公司承诺自承接该项目之日起，派往项目现场前，我公司将对进场人员进行安全教育，并要求其遵守贵公司及项目现场安全管理规定，若进场人员以及设备发生人身伤亡和/或财产损失，相关损失及责任由我公司全权承担，与招标方无关。

法定代表人或授权代表（签字）：

投标人（盖章）：

投标日期：

附件七：关键项目响应表

关键项目技术响应表

项目	类别	功能及技术描述	是否响应	方案响应有无增减	说明
	日志审计系统				
1	**日志审计：性能要求**	★1U 机架式设备，不少于 6 个千兆电口，存储容量不少于 4TB。支持 50 个日志源授权。包含日志收集、存储、查询、统计分析等功能。综合采集处理均值 5000EPS。			
2	**日志审计：数据采集**	★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；			
3	**日志审计：数据存储**	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；			
4	**日志审计：数据查询**	支持为不同类型日志设置不同的查询条件和显示条件；			
5	**日志审计：数据查询**	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；			
6	**日志审计：告警管理**	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；			
7	**日志审计：日志源管理**	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；			
8	**系统管理**	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。			
9	**系统管理**	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；			
10	**《计算机信息系统安全专用产品销售许可证》**	★所提供的产品检验报告须符合《信息安全技术 日志分析产品安全技术要求 GA/T 911-2019》检验规范，增强级；			
11	**IT 产品信息安全认证证书**	★所提供的产品获得中国信息安全认证中心颁发的《IT 产品信息安全认证证书》，需符合《日志采集与分析产品安全技术要求》，并提供完整的检测报告复印件；			
12	**IPv6 Ready**	★所提供的产品获得全球 IPv6 论坛 IPv6 Ready			

	Logo 认证	Logo 委员会颁发的 IPv6 Ready Logo 认证证书；			
13	**计算机软件著作权登记证书**	★所提供的产品获得国家版权局计算机软件著作权登记证书			
14	**TL9000 认证**	TL9000 电讯业质量管理体系认证			
15	**安全开发二级及以上**	中国信息安全测评中心颁发的《安全开发资质认证二级及以上》			
16	**CISP 培训机构**	信息安全测评中心颁发证书的 CISP 培训机构			
17	**涉甲级资质**	国家保密局颁发的涉及国家秘密的计算机信息系统集成资质证书（甲级）包含（系统集成、软件开发、运行维护）			
	数据库审计系统				
18	**性能要求**	★1U 机箱， 不少于 6 个千兆电口，不少于 1TB 存储空间，单电源；审计能力 100Mbps，SQL 处理数 1000 条/秒。含 3 应用识别库。			
19	**数据库类型**	★支持 Oracle、SQLServer、MySQL 等数据库系统			
		支持 KingBase、DaMeng、Oscar、GBase、Inspur_KDB、Highgo、GaussDB 等国内主流数据库系统			
20	**主流业务协议审计**	★支持 HTTP、Telnet、FTP、SMTP、IMAP、POP3 的审计			
21	**主流业务协议审计查询**	HTTP 协议支持按 HTTP 访问域、URL、请求类型、请求文件、Cookie、返回码等 34 个分项作为查询和统计的条件			
		Telnet 协议支持按 telnet 命令、返回信息等 20 个分项作为查询和统计的条件			
		FTP 协议支持按 ftp 命令、传输文件信息、ftp 用户名、密码等 23 个分项作为查询和统计条件			
		邮件协议支持按邮件主题、附件、发送 ip 等 24 个分项作为查询和统计的条件			
22	**数据库监控**	支持依据数据库实例监控各个数据的数据库类型、活跃会话数、总会话数、负载等信息			
		支持依据数据库实例监控各个数据库的连接池、缓冲区、表空间、死锁、CPU、内存、硬盘等信息，可自定义告警阈值进行健康评估			
		支持自定义时间条件进行各个数据库的会话趋势、SQL 操作趋势、安全趋势、访问源趋势的			

		图表展示			
		支持自定义审计精确到秒级的流入流出总流量趋势、总体新建与并发会话数趋势、总体资源占用率趋势			
23	**SQL 操作统计**	支持各类 SQL 操作数量以及占比情况			
24	**应用流量监听**	支持审计各个应用协议的流量大小和数据包数量，并以图表形式进行排名；			
25		支持自定义时间查看各个协议审计的流量趋势图，直观展示应用流量的监听情况			
26	**设备运行状态**	支持首页直观展示数据库审计系统的运行情况，比如并发连接数、每秒新建连接速率、版本号、运行时间以及 CPU、内存、硬盘等资源占用情况			
27	**数据库攻击行为审计**	★支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为，利用漏洞攻击等行为进行审计，并进行实时报警			
28	**SQL 错误统计**	多个维度展示错误占比及趋势，从源 IP 维度以柱状图展示 SQL 错误数（TOP10）			
29	**SQL 错误分析**	以列表形式给出出错原因、出错信息以及解决办法			
30	**SQL 效率分析**	★以饼图展示正常 SQL 与慢 SQL 占比情况、TOP10 慢 SQL 的详细分析：TOP 排名信息、事件 ID、数据库名、目的 ip、协议类型、源 ip、sql 响应时间、操作类型、具体 sql 语句等要素			
31	**会话回放**	支持会话回放功能,并至少支持 0.5 倍速、1 倍速、1.5 倍速、2 倍速、4 倍速五级播放速度调节			
32	**翻译功能**	实现对 SQL 语句报警内容自定义成中文自然语言的描述功能，便于非技术人员理解报警内容；			
33	**数据查询**	支持基于数据库时间、源/目的 IP、数据库名、应用协议、数据库表名、字段值、预处理 SQL、SQL 关键词、数据库返回码、SQL 响应时间、数据库操作类型、影响行数等条件的审计查询。			
		边查询边统计机制，页面采用异步加载技术，保障查询和统计效率			
		查询方式支持精确查询与模糊查询两种模式，并支持自定义保存当前查询条件，为后续查询提高便捷			
34	**复杂 SQL 审计能力**	支持超长 SQL 语句审计，至少不低于 2M			
		支持嵌套 SQL 语句的审计			
		准确审计绑定变量的 SQL 语句			

		有效分割、准确审计主流数据库协议的多 SQL 语句			
35	**版本回滚**	支持历史版本回退功能，系统内建历史版本库不少于 3 个			
36	**操作系统**	安全操作系统采用冗余设计，可在设备命令行启动过程中选择主备系统			
37	**云检测**	支持云检测，可对本单位部署的同一品牌的多台审计或者多类型安全设备（版本号、序列号、型号、运行时长、CPU 和内存占用、并发和新建连接数、设备流量等）进行远程统一检测，保障各设备的安全稳定运行			
38	**系统抓包**	支持抓包工具（可配置抓包个数、源和目的 IP、协议等）、系统巡检、网络诊断、规则库升级			
39	**一键巡检**	支持系统本身主要运行功能服务模块的运行状态巡检，保证系统安全稳定运行			
40	**配置与策略**	支持系统配置文件和系统策略的密文导入导出，不可设置为明文			
41	**安全浏览器管理**	支持红莲花、密信等安全浏览器登录管理设备，该类浏览器支持国密算法 SM2/SM3/SM4，安全性非常高			
42	**系统登录连接数设置**	支持 webui/ssh/telnet 方式登录系统的最大连接数设置			
43	**日志外发**	支持 Syslog、SNMP、kafka 等方式外发日志			
44	**磁盘管理**	支持手动、自动方式的磁盘清理，可根据剩余空间、保存时限等条件灵活设置，磁盘空间占用情况的检查频率可灵活设置：10min、30min、1h、3h、6h、24h 等时长 ），支持存储外发。			
45	**告警级别**	支持告警级别划分，至少分为七类，例如：紧急、警告、一般等级别，以便运维人员作出不同响应			
46	**报表模板**	支持等保、萨班斯法案报表模板以及自定义报表，可以按日、周、月等周期自动生成报表			
47	**《计算机信息系统安全专用产品销售许可证》**	★《计算机信息系统安全专用产品销售许可证》，证书类别必须为：数据库安全审计类（增强级）			
48	**IPV6 认证中心证书**	★所提供的产品获得全球 IPv6 论坛 IPv6 Ready Logo 委员会颁发的 IPv6 Ready Logo 认证证书；			
49	**信息技术产品安全测评证书**	信息技术产品安全测评证书，级别：EAL3+			
50	**中国国家信息安全产品**	中国国家信息安全产品认证证书，增强级			

	认证证书				
51	**TL9000 认证**	TL9000 电讯业质量管理体系认证			
52	**安全开发二级及以上**	中国信息安全测评中心颁发的《安全开发资质认证二级及以上》			
53	**CISP 培训机构**	信息安全测评中心颁发证书的 CISP 培训机构			
54	**涉甲级资质**	国家保密局颁发的涉及国家秘密的计算机信息系统集成资质证书（甲级）包含（系统集成、软件开发、运行维护）			
	服务器安全防护系统				
55	**操作系统兼容性**	支持 windows/linux 主流操作系统，包括但不限于以下的操作系统：Windows Server 2003 SP2（x86/x64）、Windows Server 2008（x86/x64）、Windows Server 2012、Windows Server 2016、Windows Server 2019；			
		RedHat 4.3~RedHat 5.11（x86/x64）、RedHat 6.0~RedHat 6.7（x86/x64）、RedHat 7.0~RedHat 7.2 RedHat8.0 ；			
		CentOS 4.3~CentOS 5.11（x86/x64）、CentOS 6.0~CentOS 6.10（x86/x64）、CentOS 7.0~CentOS 7.6、Centos8.0；			
		Ubuntu10.0 以上；			
		Suse 10~Suse 10 sp3、Suse 11~Suse 11 sp3、Suse12；中标麒麟、红旗 Redflag3~4；			
56	**产品安全机制**	客户端具有反逆向、反调试功能、自保护功能，客户端和管理中心通信采用安全的加密机制			
		支持自我防护技术，即使客户端被意外关闭，防护依然有效			
57	**风险发现**	支持服务器系统级、数据库、中间件、应用级的弱口令、口令复用扫描，并可对扫描的结果进行修复验证，还可对口令风险的扫描任务进行设置，包括任务名称、目标服务器、扫描类型、扫描所用字典、执行周期等方式。			
58	**基线检查**	支持 CIS、等级保护二级、三级检查，系统内置官方等保 2.0 的二级、三级基线模板，满足等保二级及等保三级要求，同时支持用户自定义基线检查任务。并支持基线检查结果的图形化统计，包括：合规率、问题项 TOP5、风险服务器 TOP5 等维度的统计，并可导出基线检查报告。			

59	**病毒查杀**	采用主动的方式进行自动化病毒查杀，可支持 Bitdefender、ClamAV、Qowl 等多引擎技术识别并查杀最新病毒；可支持病毒文件自动隔离、自动删除、不处理三种方式。并可将病毒查杀的结果导出报告			
60	**威胁总览**	支持统计并展示服务器的可疑威胁及告警信息，包括：可疑威胁事件统计、可疑威胁分布、可疑问些趋势，以及具体的威胁事件列表，并可对威胁事件进行研判，还可将威胁事件导出为 EXCEL 格式的报告			
61	**防恶意扫描**	以攻击者视角、受害者视角展示恶意扫描的事件，包括：服务器名称、负责人、所属部门、操作地址、最近发生时间、受害 IP、攻击 IP 等信息，并可将事件加入黑名单或白名单，还可对受害的 IP 进行防端口扫描、屏蔽扫描器等设置			
62	**暴力破解检测**	对暴力登录系统的账号和 IP 进行自动发现并上报暴力破解入侵事件，支持对 RDP、SSH、FTP 等服务的暴力破解行为进行检测拦截，支持设定暴力破解行为的请求范围、失败次数，针对暴力破解的 IP 支持设定锁定时长。			
63	**异常登陆监测**	以违规登录、可疑登录的视角，对异常登录行为进行监控及告警，包括：登录账号、来源 IP、登录区域、服务器 IP、操作系统等，并可进行登陆规则的设置，以及告警设置			
64	**后门检测**	支持对操作系统、文件、软件中存在的后门进行检测，包括：发现时间、后门名称、后门类型、风险等级、服务器名称、服务器 IP、操作系统等，并可进行隔离、删除、加白、下载等操作，并提供后门的详情信息			
65	**Webshell 检测**	自动识别web服务目录,并实时进行webshell后门的扫描，包括：危险级别、文件路径、文件代销、文件 MD5、文件修改时间、webshell 发现时间、感染服务器等信息。			
66	**反弹 shell 检测**	可实时发现反弹 shell 等危险的反链操作风险，包括：发起连接主机、服务器名称、服务器别名、AgentID、服务器 IP、操作系统等信息，并支持事件的上报和阻断。			
67	**性能监控**	支持对服务器主机的 CPU 利用率、内存使用率、磁盘使用率进行监控，支持展示近 1 小时、近半天、近 1 天、近 7 天、近 1 个月、近 1 年的监控数据			
		支持对自身 Agent 的 CPU 利用率、内存使用			

		率进行监控，支持展示近 1 小时、近半天、近 1 天、近 7 天、近 1 个月、近 1 年的监控数据			
		支持对当前的客户端性能、服务器主机性能监控数据进行导出			
68	**报表生成下载**	支持各类日志、安全报表、资产报表、事件报表、功能状态报表的综合下载导出，并可根据实际情况对报表内容进行自定义导出			
69	**产品后台管理**	支持展示客户端的安装时间、当前客户端版本、最新客户端版本、启动时间、结束时间、更新状态进行展示			
		支持批量对客户端的版本进行更新			
		支持离线安装、命令安装客户端，采用命令安装时支持设置代理地址、默认端口、安装路径、磁盘检测、是否允许覆盖安装等参数			
70	**账号管理**	支持创建子账号，创建账号时支持配置其角色、上级账户、绑定服务器，支持添加归属人、手机号、邮箱、备注等附属信息			
71	**资质要求**	产品拥有自主知识产权，具有国家版权局颁发的“计算机软件著作权登记证书”			
		产品拥有公安部颁发的销售许可证			
	机房环境				
72	防火门	甲级钢制防火门 1 套			
73	配电箱	机房总输入配电箱 1 套、连接机房一级配电箱，UPS 输出，改造现有机柜为市电和 UPS 电源冗余输出及配套电缆和 PDU 等，提供防雷接地相关实施工作和辅材			
74	门禁	提供人脸识别门禁系统 1 套			
75	空调	提供工业空调 1 套，并且根据新的机房机柜拜访位置调整现有空调设施。			
76	信息点标记	将现有办公区信息点进行标记、与机房配线端进行核对、巡线、标签。			
77	机柜设备整理	将现有机柜内服务器、网络和安全设备、配线架等进行梳理、按照 IT 系统管理规范进行梳理、重新定位、标记和线缆连接。			
78	动环监控系统	提供 1 套动力环境监测系统，提供漏水监测、温度和湿度监控、UPS 监测模块、提供远程图形界面			

注：本表内容是主要评分项，详细要求以技术要求为准，★号内容为否决项。