附件1：

招 标 文 件

项目编号：ZC-AZB16202

项目名称：劳动关系学院校园网络安全与管理建设采购项目

中共中央直属机关采购中心

2016 年 9 月

**目 录**

 第一章 专用部分 1

 第一部分 投标邀请 2

 第二部分 招标基本信息 5

 第三部分 投标内容及格式要求 6

 第四部分 符合性审查项及评分标准 27

 第五部分 技术规格及要求 31

 第二章 通用部分 32

 第一部分 投标人须知 33

 第二部分 合同条款及格式 43

**第一章 专用部分**

**第一部分 投标邀请**

中共中央直属机关采购中心受中国劳动关系学院委托，就劳动关系学院校园网络安全与管理建设采购项目(项目编号：ZC-AZB16202)进行国内公开招标。现邀请合格的投标人提交符合招标文件要求的投标文件。

1. **项目概述**
	1. 招标内容：本项目所采购设备用于中国劳动关系学院校园网络安全与管理建设。采购标的、数量以及技术要求等详见招标文件技术要求部分。
	2. 采购预算：本项目预算为：310万元，超过预算的投标将作为无效投标处理。
	3. 本项目不分包。

本项目为非专门面向中小企业采购项目。

* 1. 本项目不接受进口产品的投标，进口产品是指“通过中国海关报关验放进入中国境内且产自关境外的产品”。
	2. 本项目不涉及节能强采产品。
1. **投标人必须符合的条件**

投标人应具备《中华人民共和国政府采购法》第二十二条规定的条件，且符合、承认并承诺履行招标文件各项规定的国内法人和其他组织（不包括在港澳台地区注册成立的法人和其它组织）。

同时还应具有以下特定条件的：

　　1、本项目不接受联合体投标。

　　2、受托为劳动关系学院校园网络安全与管理建设采购项目整体采购项目或其中分项目的前期工作提供设计、编制规范、进行管理等服务的供应商，及其附属机构（单位），不得参加劳动关系学院校园网络安全与管理建设采购项目的投标。

　　3、单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

1. **获取招标文件的时间和办法**

2016年09月22日至2016年10月09日，登录“中国政府采购网中直采购频道”（zzcg.ccgp.gov.cn）免费下载招标文件。**未通过中直采购频道下载招标文件的投标人，其递交的投标文件将被作为无效投标处理。联合体投标的应当由联合体代表下载招标文件。**

1. **投标文件递交时间、地点**

投标文件递交时间：2016年10月09日至2016年10月13日（北京时间）

投标文件递交地点：中新大厦（北京市西城区新风街一号院甲6号楼）一层电子投标文件递交室

投标截止时间：2016年10月13日09时00分（北京时间），截至此时间未完成递交的投标文件予以退回，此后递交的投标文件不予接收。

1. **开标时间、地点**

开标时间：2016年10月13日09时00分（北京时间）

开标地点：中新大厦（北京市西城区新风街1号院甲6号楼）开标室

**特别提醒：**本项目采用电子化招投标。中直机关集中采购电子化平台集成北京数字认证股份有限公司数字证书系统，投标人须使用该公司发放的数字认证证书对投标文件进行签封、加密、递交及开标时解密等相关招投标事宜，具体要求和操作程序详见招标文件投标人须知部分。申请办理数字认证证书的方式详见：<http://help.bjca.org.cn/support/client/zzcg-ccgp/index.htm>。

投标人下载电子招标文件同时须在“中国政府采购网中直采购频道”的“资料下载”栏目中，免费下载“全流程电子化投标客户端”，并使用该客户端制作电子投标文件，制作完成后，导出扩展名为“.file”的电子投标文件；

投标人请于投标文件递交时间内的每天8：00至 17：00，或开标当天8：00至投标截止时间，携带存储在光盘内的电子投标文件到投标文件递交地点，通过终端使用**用户名和密码**登陆电子化平台后，使用**数字认证证书**将电子投标文件上传至电子化平台。因电子文件递交需要一定的时间，请供应商安排充足时间递交文件。

除上述方式之外，招标方不接受投标人以纸质文件以及其他任何方式（包括但不限于：邮寄、传真、电子邮件等）提交的投标文件。

1. **联系方式**

**采购人：**中国劳动关系学院

联系方式：88561877

地 址：北京市海淀区增光路45号

**采购中心：**

项目联系人：薛宗伟

电　　话：010-82273286

系统技术支持电话：010-82273275 010-82273269

地 址：北京市西城区新风街1号院甲6号楼

邮政编码：100088

**第二部分 招标基本信息**

* + 1. 项目编号：ZC-AZB16202
		2. 项目名称：劳动关系学院校园网络安全与管理建设采购项目
		3. 采购人：中国劳动关系学院
		4. 报价要求：本项目预算为：310万元，超过预算的投标将作为无效投标处理。

投标报价应包含系统集成、制造货物、运输、保险、安装、调试、备品备件、培训、保修、包装、验收费用及其它相关费用。

* + 1. 资金来源：财政性资金
		2. 交货要求：交货时间及交货地点：签订合同后30天内，采购人指定地点：北京市海淀区增光路45号。
		3. 投标有效期：开标之日起90个日历日。如果中标，有效期自动延长至合同履行完毕。
		4. 投标保证金要求：

本项目不收取投标保证金。

* + 1. 评标委员会组成：

评标委员会成员共7名，其中有关技术、经济等方面的专家5名，采购人代表2名。

* + 1. 评分办法：本项目采用综合评分法。

**第三部分 投标内容及格式要求**

一、投标声明函

**致：中共中央直属机关采购中心：**

* 1. 我方承诺，我方完全具备《政府采购法》第二十二条第一款规定的条件以及本项目招标文件规定的投标人须满足的特定条件。
	2. 我方承诺按照本项目招标文件和相关技术标准的条件，提供货物及相关服务，并承担因货物质量或服务等引起的一切责任。
	3. 我方对该项目招标文件（包括修改文件及有关附件）完全理解，并承诺在发生争议时，不会以对招标文件存在误解、不明为由，向贵中心行使任何法律上的抗辩权。
	4. 我方投标文件有效期为自开标日起 个日历日，若中标，则投标有效期自动延续至合同履行完毕。
	5. 我方承诺接受招标文件规定的付款方式。
	6. 我方投标文件和你方的中标通知书、招标文件将成为约束双方的合同文件组成部分，若招标文件存在要求，而本投标文件没有拒绝亦没有涉及的情形下，我方接受招标文件的有关约束，并同意将招标文件对投标人的要求作为投标人合同义务的组成部分。
	7. 我方承诺投标文件中所有的资料及所作各项承诺均真实准确，所提交的营业执照副本复印件已依法履行相应的年度报告登记公示手续（或所提交的《事业单位法人证书》副本复印件/《社会团体法人登记证书》复印件/《民办非企业单位登记证书》复印件已经国家主管部门年检），不存在任何虚假之处，否则，评标委员会可将我方的投标文件按照无效投标文件处理，即使我方中标，中标结果无效，对于因此给其他投标人及你方和采购人造成的全部损失，我方同意无条件予以赔偿。
	8. 我方委托授权 (身份证号: ，联系电话： )作为我方的代理人参加本项目投标，负责提交投标文件以及其它相关资料，参加开标，接受质询并予以澄清，签署、接受招投标过程中的各种法律文件，办理投标过程中的其他相关事务。
	9. 我方将严格遵守《中华人民共和国政府采购法》，若存在违法违规行为，将承担相应的法律后果。

法定代表人签字或盖章：

 数字认证证书电子签章：

日期：

 **特别提醒：为确保电子投标文件的合法性、安全性和完整性，本《投标声明函》 填写完成后须先进行打印，经法定代表人或盖章签字后扫描上传并加盖数字认证证书电子签章。电子签章后，文档不应再修改，否则签章无效；如需修改，请修改后重新签章。**

二、开标一览表

报价合计（大写）:

报价合计: 元

注：

 1、所报价格须用人民币元表示。

 2、报价合计应与《分项报价表》中“合计”一致。如因不一致而产生的不利后果，均由投标人自行承担。

三、分项报价表

**分项报价表**

 项目编号：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名 称** | **数量** | **单位** | **所投产品品牌及型号** | **单价** | **小计** |
| 1 | 安全漏洞扫描设备 | 1  | 台 |  |  |  |
| 2 | Web应用防火墙 | 1  | 台 |  |  |  |
| 3 | 安全运维审计设备 | 1  | 台 |  |  |  |
| 4 | 安全动态主机配置协议设备 | 4  | 台 |  |  |  |
| 5 | 安全虚拟专用网络设备 | 1  | 台 |  |  |  |
| 6 | 安全域名解析设备 | 6  | 台 |  |  |  |
| 7 | 安全运维管理系统 | 1  | 套 |  |  |  |
| 8 | 门禁控制器 | 1 | 台 |  |  |  |
| 9 | 电磁锁 | 1 | 个 |  |  |  |
| 10 | 读卡器 | 1 | 个 |  |  |  |
| 11 | IC卡 | 10 | 张 |  |  |  |
| 12 | 出门按钮 | 1 | 个 |  |  |  |
| 13 | 监控摄像头 | 6 | 个 |  |  |  |
| 14 | 硬盘录像机 | 1 | 台 |  |  |  |
| 15 | 无线传输交互系统 | 1 | 套 |  |  |  |
| 16 | 线缆辅材 | 1 | 项 |  |  |  |
| 17 | 光跳线 | 20 | 根 |  |  |  |
| 18 | 千兆多模光模块 | 10 | 个 |  |  |  |
| **合计** |  |

注：

1. 所报价格系用人民币元表示，保留整数。
2. 合计价格与《开标一览表》中“报价合计”必须一致。

其他相关费用应包括根据合同或其它原因应由投标人支付的税款和应由投标人负担的相关费用。

四、非进口产品

非进口产品声明函

 我方承诺就 （项目名称、编号） 所投 产品为非进口产品，我方保证上述内容的真实性，并承担由此引起的一切责任。

特此声明。

企业名称（盖章）：

 日　期：

五、营业执照

经国家主管部门年检或依法履行年度报告登记公示手续，且在有效期内的营业执照副本原件扫描件/《事业单位法人证书》副本原件扫描件/《社会团体法人登记证书》原件扫描件/《民办非企业单位登记证书》原件扫描件。

六、没有重大违法记录的声明

没有重大违法记录的声明（参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明）

七、财务状况报告

财务状况报告：投标人为法人的，须提供经审计的上年度财务状况报告或基本账户的银行资信证明；其他组织和自然人，可以提供银行资信证明。投标人也可以提供财政部门认可的政府采购专业担保机构出具的投标担保函。

八、依法缴纳税收和社会保障资金的相关材料

依法缴纳税收和社会保障资金的相关材料：投标人依法缴纳近半年内任意一个月税收的相关凭证；投标人依法缴纳近半年内任意一个月社会保险的相关凭证。

九、中国信息安全认证中心出具的有效认证证书

所投Web应用防火墙等安全产品应提供中国信息安全认证中心出具的有效认证证书。

十、所投产品三年原厂售后服务承诺函

所投安全漏洞扫描系统、Web应用防火墙、安全运维审计设备、安全动态主机配置协议设备、安全虚拟专用网络设备、安全域名解析设备、安全运维管理系统、无线传输交互系统需要提供三年原厂售后服务承诺函（含软件免费升级）。

十一、标★号的指标能否满足招标文件要求

详细说明标★号的指标能否满足招标文件要求。

十二、应用案例

提供近三年同类项目合同，300万以上的成功案例（须提供合同首页、合同金额和签字所在页原件扫描件）。

十三、计算机系统集成资质

计算机信息系统集成或计算机信息系统集成及服务资质

十四、国家信息安全测评信息安全服务资质

提供中国信息安全测评中心颁发的国家信息安全测评信息安全服务资质。

十五、项目组成员配备情况

项目组成员配备情况

十六、中小企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）的规定，本公司为\_\_\_\_\_\_（请填写：中型、小型、微型）企业。即，本公司同时满足以下条件：

　　1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）规定的划分标准，本公司为 （请填写：中型、小型、微型）企业。

　　2.本公司参加\_\_\_\_\_\_单位的\_\_\_\_\_\_项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他\_\_\_\_\_\_（请填写：中型、小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

　　本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

备注：投标人若不提供本声明函的，将不能享受政府采购扶持中小微型企业的政策。

监狱企业证明函

本公司郑重声明，根据《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，本公司为监狱企业。

 省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）（盖章）：日 期：

备注：投标人若不提供监狱企业证明函的，将不能享受政府采购扶持监狱企业的政策。

十七、产品选型

货物主要技术指标和运行性能的详细说明（须对技术需求中的产品技术指标逐条进行应答，说明正负偏离情况） 及整体方案

十八、服务部分

服务及培训方案。

**第四部分 符合性审查项及评分标准**

一、投标人须提供下列各项资料，且所提供的资料满足招标文件要求，有任意一项未提交或不满足的，经评标委员会半数以上成员一致同意，其投标将被按照无效投标处理，经评标委员会认定的无效投标文件不得进入详细评审：

 1.投标声明函

 2.开标一览表

 3.分项报价表

 4.非进口产品声明函

 5.营业执照

 6.没有重大违法记录的声明

 7.财务状况报告

 8.依法缴纳税收和社会保障资金的相关材料

 9.中国信息安全认证中心出具的有效认证证书

 10.所投产品三年原厂售后服务承诺函

 11.标★号的指标能否满足招标文件要求

二、评分标准

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目 | 评审因素 | 分值 | 对应的投标格式 |
| 第一部分 商务部分 | 1.投标人应用案例 | 提供近三年同类项目合同，300万以上的成功案例，提供1个得2分，最高得6分； | 0～6 | 应用案例  |
| 2.计算机系统集成资质 | 二级及以上资质者得3分，三级得1分，其它不得分。 | 0～3 | 计算机系统集成资质  |
| 3.国家信息安全测评信息安全服务资质 | （安全工程类一级）或以上者得2分，不提供不得分； | 0～2 | 国家信息安全测评信息安全服务资质  |
| 第二部分 项目组成员 | 1.项目组成员配备情况 | 项目组成员需提供相应证明文件及2014年以来的社会保险缴纳证明：1、项目经理具有高级项目经理证书，得2分，否则0分；2、项目组配备国家信息安全测评注册信息安全专业人员，每配备1名得1分，最多得2分。 | 0～4 | 项目组成员配备情况  |
| 第三部分 产品选型 | 1.技术性能指标 | 满足招标文件要求的全部技术指标得38分。标⊙为重要指标项，每有一项不满足扣5分，扣完为止；其他指标每有一项不满足扣3分，扣完为止。 | 0～38 | 产品选型 |
| 第四部分 服务部分 | 1.所承诺服务满足招标文件要求情况 | 所承诺服务内容满足招标文件要求情况：满足一条得2分，满分10分。 | 0～10 | 服务部分 |
| 2.质保期 | 所投系统及硬件设备产品质保期高于招标文件要求，所有设备质保期多1年得2分，最多4分。 | 0～4 |
| 3.驻场服务 | 满足招标文件要求（提供驻场人员相关资质证明材料）得3分，否则0分 | 0～3 |
| 第五部分 报价分 | 1.价格 | （1）满足招标文件要求且投标价格最低的投标报价为评标基准价，其投标人的报价分为最高分30分；（2）其他投标人的报价分按以下公式计算：报价得分=(评标基准价／投标报价)×价格权值×100；（3）小型、微型企业价格折扣率作为非专门面向小型、微型企业的采购项目，其中小型、微型企业参与投标的，对其产品价格给予 6%（幅度为6%-10%） 的扣除，用扣除后的价格参与评审。（4）监狱企业视同小型、微型企业。 | 0～30 |  |

**第五部分 技术规格及要求**

详见附件：

技术需求.doc

**第二章 通用部分**

**第一部分 投标人须知**

* + - 1. 总则
1. **适用范围及编制依据**
	1. 本招标文件仅适用于本项目投标邀请中所叙述的招标项目。
	2. 本招标文件依据《中华人民共和国政府采购法》、《政府采购货物和服务招标投标管理办法》、《电子签名法》等有关法律法规及规定编制。
2. **定义**
	1. “采购中心”指中共中央直属机关采购中心，为本次招标的组织者。
	2. “采购人”指本项目的委托单位。
	3. “投标人”指按本文件规定领取招标文件并在采购中心登记备案的，且响应招标文件要求，向采购中心提交投标文件的供应商。
	4. “招标方”指采购人和采购中心。
	5. “货物”指本文件中所述所有货物及相关服务。
	6. “日”指日历日。
	7. “电子化平台”指在采购中心设置、运行的计算机信息系统，该系统在采购中心局域网用于接收投标人的电子投标文件、完成开标、评标等活动，在互联网用于供应商下载招标文件。
	8. “数字认证证书”指北京数字认证股份有限公司颁发的用于证明投标人身份的单位电子签名认证证书（非个人证书）。
	9. “投标客户端”指采购中心提供的用于投标人编制投标文件的软件，该软件在“中国政府采购网中直采购频道”的“资料下载”栏目中，由投标人自行免费下载。
3. **投标费用**

投标人应承担所有与本次投标有关的费用，不论投标的结果如何，招标方在任何情况下均无义务和责任承担这些费用。

## 招标文件说明

1. **招标文件的法律效力**

本招标文件阐明了投标人所需提供的货物及服务的范围和招标投标的程序，是本次招标活动具有法律效力的文件。投标人应认真阅读招标文件中所有的事项、格式条款和规范等要求，否则，出现的相关不利后果，由投标人自行承担相关风险。

1. **招标文件的澄清、修改**
	1. 在投标截止时间15日前，采购中心可以根据需要对招标文件进行澄清、修改。澄清文件作为招标文件的组成部分，与招标文件具有同等法律效力。
	2. 对招标文件进行澄清、修改的，将依法发布公告，并以短信、电子邮件或传真等形式通知所有已领取招标文件的投标人，投标人未填写手机联系方式、电子邮箱或相关信息不准确的，后果由投标人自行承担。
	3. 招标文件进行澄清、修改的，投标人须重新下载澄清、修改后的招标文件，并按照澄清、修改后的招标文件编制投标文件，投标人因未重新下载澄清、修改后的招标文件并编制投标文件，由此可能引起的投标文件递交失败、解密失败、内容缺失等相关后果由投标人自行承担。
	4. 当招标文件和澄清文件在同一内容的表述上不一致时，以最后发出的文件为准。

## 投标文件编写

1. **编制投标文件的工具和语言**
	1. 投标人应当通过自备的计算机使用投标客户端编制电子投标文件，投标人提交的电子投标文件以及相关资料均应当使用中文简体字。
	2. 安装和使用投标客户端需要具备的计算机软硬件环境：
		1. 硬件要求:

处理器：双核，1000 MHz以上主频

内存：1G B或以上

硬盘：40G以上

显示器分辨率：1024\*768或以上

USB接口：至少一个USB2.0接口

* + 1. 软件要求:

操作系统： Microsoft Windows XP简体中文版、Microsoft Windows 7简体中文版、Microsoft Windows 8简体中文版

文档编辑软件：32位 MicrosoftOffice 2003 或以上

浏览器要求：IE浏览器6.0及以上版本

1. **计量单位**

计量单位应当使用中华人民共和国法定计量单位，招标文件的技术要求中另有规定的除外。

1. **投标报价**
	1. 投标总价包括投标人为完成本项目所发生的一切费用，估算错误或漏项的风险由投标人自行承担。
	2. 投标人对每包只能有一个不可变更的报价。任何有选择的报价或包含价格调整要求的投标，将被作为无效投标处理。
	3. 最低报价不能作为中标的保证。
2. **投标货币**

投标人应以人民币填报投标报价，合同履行时采购人亦以人民币支付。

1. **投标有效期**
	1. 投标人投标有效期短于招标文件规定期限的，将被视为非响应投标而按照无效投标处理。
	2. 在特殊情况下，在原投标有效期期满之前，采购中心可以要求投标人延长投标有效期。这种要求与答复均应以书面形式进行。在此种情况下，投标人不得修改投标文件的其它内容。投标人不同意延长投标有效期的，将被按照无效投标处理。
2. **投标文件的式样和签署**
	1. 投标文件编制完成后应通过投标客户端使用数字认证证书加密和签章。没有加密的投标文件将被拒绝接收。
	2. 因投标文件字迹模糊或表达不清所引起的不利后果由投标人自行承担。

## 投标文件的递交

1. **投标文件的递交**
	1. 投标人应自行携带数字认证证书、加密后的电子投标文件，及招标文件要求的其他材料，按照投标邀请中的时间，到达投标地点，自行通过在投标地点设置的计算机终端登陆电子化平台，使用数字认证证书将经加密的电子投标文件通过移动存储介质（光盘）上传至电子化平台。上传成功后，电子化平台将予以记录并提供上传成功的回执。
	2. 截至投标截止时间，投标人未完成电子投标文件传输的，视为其撤回投标文件。
	3. 投标截止时间后电子化平台拒绝接收投标文件。
	4. 递交完成后至开标前，投标人不能对数字证书更新、续费，否则可能引起的投标文件解密失败等相关后果由投标人自行承担。
2. **投标截止时间的延长**

采购中心可以视采购具体情况，于投标截止时间3日前延长投标截止时间和开标时间，并将以书面形式通知所有领取招标文件的投标人和在中国政府采购网发布变更公告。

1. **投标文件的撤回、修改和补充**
	1. 投标人在投标截止时间前可通过电子化平台撤回其已成功递交的电子投标文件，电子化平台将予以记录并提供撤回回执。
	2. 如果在投标截止时间前需要对已经成功递交的电子投标文件进行修改、补充的，投标人应当使用自备的计算机和“投标客户端”重新制作并导出完整的电子投标文件，并按要求重新上传至电子化平台。
	3. 电子化平台以投标人最后上传成功的投标文件为准。

## 开标

1. **开标**
	1. 采购中心将在规定的时间和地点组织开标活动。开标活动由采购中心主持。
	2. 投标人应当委派投标代表参加开标活动，否则，由此产生的不利后果由投标人自行承担。
	3. 开标时，投标人委派的投标代表应当使用与制作投标文件时同一数字认证证书对投标文件进行解密。在场所有供应商解密完成后，采购中心工作人员将进行开封报价。
	4. 在开封报价之后，因投标人原因造成投标文件未解密的，视为撤销其投标文件；因投标人之外的原因造成投标文件未解密的，视为撤回其投标文件，投标人有权要求责任方赔偿因此遭受的直接损失。
	5. 开标时，部分投标人投标文件未解密的，开标可以继续进行。若解密成功的投标人不足三家，该项目或该包按废标处理。
	6. 解密失败应急措施: 为应对现场开标时非人为因素造成的解密电子投标文件失败的情况，请投标供应商将投标客户端系统导出的未签名加密电子版投标文件（.xbid格式电子文件）刻录于不可擦写的光盘上以作备用，此光盘上须有法人或授权代表手写签字，并密封于信封中，在开标当天文件递交截止时间前交予采购中心开标现场工作人员。若开标过程中，已加密电子投标文件解密失败，可现场由采购中心工作人员将光盘中的投标文件（.xbid格式电子文件）导入系统，继续开标。此解密失败应急措施仅适用于非供应商原因造成的解密失败情况。若供应商开标前没有提交密封于信封中的光盘，或光盘中刻录的数据有误，则解密失败时，视为供应商撤回投标文件。
	7. 开标过程中，如遇不可抗力或意外事件等情况，采购中心将暂时中断开标程序并依法处理后续事宜。

## 评标

1. **评标**
	1. 本评标办法仅适用于本项目评标。
	2. 评标原则和纪律：

 （1）客观、公平、公正和诚实信用；

 （2）依据法律和招标文件规定科学、合理评标，择优推荐中标候选人；

 （3）独立评审，禁止任何有失公平、公正的串通行为；

 （4）反不正当竞争；

 （5）恪守保密义务，凡与审查、澄清、评价和比较投标的有关资料以及授标意见等，不得向投标人及与评标无关的其他人员泄露。

* 1. 本项目评标工作分为符合性与完整性评审、详细评审两个阶段。
	2. 符合性与完整性评审
		1. 评标委员会应当根据招标文件规定，对投标文件进行符合性、完整性评审。
		2. 评标委员会对投标文件中的明显错误，有权按以下原则处理：

 （1）开标一览表内容与投标文件中分项报价表内容不一致的，以开标一览表为准，评标委员会有权要求投标人根据开标一览表对分项报价表进行澄清、说明或修正。对于拒不按要求修正的，将作为无效投标处理；

 （2）如果用数字表示（小写）的金额和用文字表示（大写）的金额不一致，应以大写表示的金额为准；

 （3）当投标单价与数量的乘积和投标总价不一致时，以单价为准，并修正总价。如单价金额小数点明显错位的，应以总价为准，修正单价；

 （4）对明显且可以推知其原义的笔误，依据其原义进行修正；

* + 1. 投标的澄清

 （1）评标委员会有权要求投标人对投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误等内容作必要的澄清、说明或者补正。该要求应当采用书面形式提出。

 （2）投标人必须按照评标委员会通知的内容和时间做出书面答复，该答复应加盖投标人公章，并经法定代表人或投标人代表的签字确认，作为投标文件的组成部分。澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。投标人拒不按照要求对投标文件进行澄清、说明或者补正的，将作为无效投标处理。

* 1. 详细评审
		1. 评标委员会只对通过了符合性与完整性评审的投标文件进行详细评审。评标委员会按照评分标准进行评标计分。所有评委给每一投标人的评分的算术平均值为该投标人的最终得分。最终得分非整数的，保留至小数点后两位，小数点后第三位按照四舍五入的规则计算
		2. 评标委员会对投标人得分按照从高到低进行排序，得分相同的投标人，报价低者排名在前，得分相同且投标报价相同的，按技术指标优劣顺序排列。
	2. 推荐中标候选人和确定中标人
		1. 评标委员会向招标方出具书面评标报告，并推荐综合得分排名前三位的合格投标人作为中标候选人。
		2. 采购人根据评标委员会提出的书面评标报告，依据本文件及相关法律法规确定中标人。

## 合同授予

1. **定标**
	1. 采购人根据评标委员会出具的评审报告，确定综合评分排名第一的中标候选人为中标人。如果中标人放弃中标或出现中标无效的情形，采购人有权递补确定排名在其下一位的中标候选人为中标人，以此类推。
	2. 中标人如果放弃中标，招标方有权依照法律规定追究其相应的法律责任。
2. **中标通知书**
	1. 采购人确定中标人后，采购中心将向中标人发出中标通知书，并将中标结果依法公告。采购中心对投标人未中标的原因不予解释。
	2. 中标通知书是合同的组成部分。
3. **签订合同**
	1. 中标人应当在中标通知书发出之日起30日内与采购人签订合同，由于中标人自身原因未及时签订合同的，招标方可以视为中标人放弃中标，中标人应当承担相应法律后果。在此种情况下，采购人可以按中标候选人顺序将标授予下一个中标候选人。
	2. 招标文件、中标人的投标文件及其双方确认的澄清文件等，均为有法律约束力的合同组成部分。
	3. **招标文件所附《合同条款及格式》是采购人与中标人签订合同的基本条款，投标人应认真阅读，在没有实质性违反招标文件及投标文件的前提下，采购人有权在合同签订前对合同条款进行适当修改、增加、删除，中标人不得以此为由拒绝签订合同。对此，请投标人参加投标前慎重考虑相关商业风险**。

## 质疑与投诉

1. **投标人质疑**
	1. 按照《中华人民共和国政府采购法》及相关规定，若投标人认为采购文件、采购过程和中标结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购中心或采购人提出质疑。
	2. 质疑书应当包括以下主要内容：被质疑项目名称、项目编号、包号、中标公告发布时间、质疑事项、证据材料、法律依据（具体条款）、有效联系方式（包括手机、传真号码）等。
	3. 质疑书必须有法定代表人签字或盖章，并加盖投标人公章。若授权代表签章，必须附法定代表人针对当次质疑的特别授权，且公章不得以合同章或其他印章代替。
	4. 有下列情形之一的，属于无效质疑，采购中心可不予受理：
2. 未在法定期限内提出质疑的；
3. 质疑未以书面形式提出，或质疑书内容不符合本须知20.2条要求的；
4. 质疑书没有法定代表人本人签章，或未提供法定代表人签章的特别授权，或未加盖单位公章的；
5. 其它不符合受理条件的情形。
	1. 采购人或采购中心将在收到书面质疑后7个工作日内作出答复，并以书面形式通知质疑投标人和其他有关投标人，但答复的内容不涉及商业秘密。
6. **投标人投诉**

质疑投标人对采购人或采购中心的答复不满意以及采购人或采购中心未在规定的时间内做出答复的，可以在答复期满后15个工作日内向财政部投诉。

## 其他事项

1. **废标**

本项目出现《政府采购法》第三十六条规定的废标情形时，招标方有权宣布废标，招标方对受影响的投标人不承担任何责任，但因招标方出现影响采购公正的违法、违规行为引起的废标情形除外。如果项目分包，将以包为单位执行。

1. **履约保证金**

按照合同约定执行。

1. **履约监管**

**为保障国有资金的使用效益，促进中标供应商严格履约，采购中心将对本项目的履约情况进行跟踪督查。中标供应商在项目实施过程中，如存在供货进度、数量、质量、安全等违约情况，除采购人可依据采购合同追究其民事责任外，采购中心有权将中标供应商的违约情况报告财政部。**

1. **中标服务费**

 本次招标不收取中标服务费，请投标人在报价时充分考虑这一因素。

1. **信用担保**

根据《财政部关于开展政府采购信用担保试点工作的通知》（财库[2011]124号），明确中国投资担保有限公司作为中央本级试点专业担保机构，投标人可以自愿选择是否采用该公司提供的投标担保、履约担保和融资担保服务。中国投资担保有限公司联系电话：010- 88822589 / 2656，地址：北京市海淀区西三环北路100号光耀东方写字楼19F，邮编：100048，网址：<http://www.guaranty.com.cn>。

1. **数字认证证书办理**

申请办理数字证书的方式详见：<http://help.bjca.org.cn/support/client/zzcg-ccgp/index.htm>。

1. **其他**

 本部分未涉及的事项请参见招标文件其他部分。

**第二部分 合同条款及格式**

## 合同条款

1. **本合同对下列术语定义为：**
	1. “合同”系指甲乙双方签署的、合同格式中载明的甲乙双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。
	2. “合同价”系指根据本合同规定乙方在正确地完全履行合同义务后甲方应支付给乙方的价款。
	3. “货物”系指乙方根据合同规定须向甲方提供的由招标项目产生的所有成果。
	4. “服务”系指根据合同规定乙方承担与供货有关的辅助服务，如运输、保险以及其它的伴随服务，例如安装、调试、提供技术援助、培训和合同中规定乙方应承担的其它义务。
	5. “合同条款”系指本合同条款。
	6. “甲方”系指购买货物和服务的采购人。
	7. “乙方”系指提供货物和服务的中标人。
	8. “项目现场”系指本项目招标文件《招标基本信息》中指明的交货地点。
	9. “天”指日历天数。
2. **适用性**

本合同条款适用于没有被本合同其他组成部分所取代的范围。

1. **标准**
	1. 本合同下交付的货物应符合本项目招标文件《技术规格及要求》所述的标准。如果没有提及适用标准，则应符合中华人民共和国有关机构发布的最新版本的标准。
	2. 除非技术规格另有规定外，计量单位均采用中华人民共和国法定计量单位。
2. **使用合同文件和资料**
	1. 未经甲方事先书面同意，乙方不得将由甲方或甲方委托的第三方提供的有关合同或合同条文、规格、计划或其他书面资料以及其获悉的甲方国家秘密、商业秘密、内部工作信息（上述资料及信息以下合称保密信息）向与履行本合同无关的任何第三方披露、泄露或许可该第三方使用。如乙方因履行本合同需要向第三方披露上述保密信息，乙方应注意保密并将披露限于履行合同必须的范围，并保证该第三方亦履行上述保密义务。乙方上述保密义务不因本合同的终止而结束，直至上述保密信息非因乙方原因已为社会公众所知悉。
	2. 没有甲方事先同意，除了履行本合同外，乙方不应使用合同条款第4.1所列举的任何保密信息。
	3. 除了合同本身以外，合同条款第4.1条所列举的任何文件是甲方的财产。如果甲方有要求，乙方在完成合同后应将这些文件全部复制件还给甲方。
	4. 乙方未按照上述约定严格履行保密义务的，应当向甲方支付合同总价10%的违约金，于此情形下，甲方还有权提前解除合同。
3. **权利保护**

乙方保证，其向甲方销售货物的行为合法有效，甲方在中华人民共和国使用该货物或货物的任何一部分时，免受任何第三方提出侵犯其著作权、专利权、商标权、专有秘密等知识产权及其他权利的起诉。

1. **履约保证金**
	1. 乙方应按照本项目招标文件规定的期限和数额提交履约保证金。
	2. 履约保证金作为乙方履行本合同义务的保证，如乙方不能全面、适当地履行本合同义务，则甲方有权直接从履约保证金中扣除其所遭受的全部损失，或者根据本合同中关于违约责任的约定扣除乙方应当支付的全部违约金。
	3. 履约保证金应采用人民币，并采用下述方式之一提交：
2. 银行保函

由甲方可接受的在中华人民共和国境内注册和营业的银行总行或省、直辖市级分行出具，其格式采用招标文件提供的格式或其他甲方可接受的格式；

1. 银行汇票或支票；
2. 中国投资担保有限公司政府采购履约担保函。
	1. 如果乙方能按约全面履行合同义务，甲方将在质量保证期满后三十（30）天内退还乙方履约保证金（不计利息）。
3. **检验、测试与安装、调试和验收**
	1. 甲方或其代表应有权检验和/或测试货物，以确认货物是否符合合同规格的要求，并且不承担额外的费用。合同条款和技术规格将说明甲方要求进行的检验和测试，以及在何处进行这些检验和测试。甲方将及时以书面形式把进行检验和/或甲方测试代表的身份通知乙方。
	2. 检验和测试可以在乙方或制造厂的所在地、交货地点和/或货物的最终目的地进行。如果在乙方或制造厂的所在地进行，乙方应免费为甲方的检验人员提供工作条件，包括但不限于必要的技术资料、检测工具和仪器。
	3. 如果任何被检测或测试的货物不能满足规格的要求，甲方可以拒绝接受该货物，乙方应更换被拒绝的货物，或者免费进行必要的修改以满足规格的要求。乙方因更换货物导致延期交货的，应当承担延期交货的违约责任。
	4. 甲方在货物到达最终目的地后对货物进行检验、测试及必要时拒绝接受货物的权利将不会因为货物在从乙方或制造厂启运前通过了甲方或其代表的检验、测试和认可而受到限制或放弃。
	5. 在交货前，乙方或制造厂应对货物的质量、规格、性能、数量和重量等进行详细而全面的检验，并出具一份证明货物符合合同规定的检验证书，但该检验证书不能作为有关质量、规格、性能、数量或重量的最终检验。制造厂检验的结果和细节应附在质量检验证书后面。
	6. 依据合同条款第7条的约定进行检测验收后，并不证明该产品无任何质量瑕疵，且不因此免除乙方在本合同项下的保证义务或其他义务。
	7. 场地环境
4. 货物到达安装现场后，乙方按有关技术规程的规定负责存放和保管，如乙方有特殊要求，应向甲方及早提出。
5. 对于所有货物，乙方的货物安装工程师在到现场安装之前，应针对货物安装前对安装现场的具体要求与甲方进行协商确定。
	1. 安装调试
6. 乙方应按照甲方的工期要求，负责在货物到达交货地点后，在甲方规定的期限内和指定的现场将货物安装、调试、试运行完毕。
7. 乙方应提供全部安装、调试过程中所需的特殊工具和易损件，并自带专用仪器仪表。乙方还应提供与安装工程有关的所有材料、设备和人工。
8. 乙方应在现场对设备进行调试和试运行，以检验其设计制作质量、操作可靠性和功能完备性等的情况。试运行应在甲方工程师的监督下进行。
	1. 最终验收
9. 乙方将货物安装、调试完毕后应立即书面通知甲方进行最终验收，甲方将在接到中标人书面通知起10个工作日内进行最终验收，如果货物性能测试结果能满足合同、招标文件以及国家有关规定的要求，则认为本合同中签署的全部货物的性能测试是成功的。
10. 如果性能测试不合格，乙方工程师应以书面形式向甲方说明失败的原因，排除故障后重新测试。如测试次数超过3次或合同规定的期限，甲方有权拒绝验收，并按乙方违约处理。甲方除有权没收乙方的履约保证金外，还有权追索因乙方造成工期延误而给甲方造成的经济损失。
11. **包装要求**

乙方应提供货物运至合同规定的最终目的地所需要的包装，以防止货物在运转中损坏或变质。这类包装应采取防潮、防晒、防锈、防腐蚀、防震动及防止其它损坏的必要保护措施，从而保护货物能够经受多次搬运、装卸及长途运输。乙方应承担由于其包装或其防护措施不妥而引起的货物锈蚀、损坏和丢失的任何损失的责任和费用。

1. **装运标记**
	1. 乙方应在每一包装箱的相邻四面用不可擦除的油漆和明显的中文字样做出以下标记：
2. 收货人
3. 合同号
4. 发货标记
5. 收货人编号
6. 目的地
7. 货物名称、品目号和箱号
8. 毛重／净重（用公斤表示）
9. 尺寸（以长×宽×高用厘米表示）
	1. 如果单件包装箱重量在2吨（t）或2吨（t）以上，乙方应在包装箱的两侧用中文和适当的运输标记标注“重心”和“吊装点”，以便装卸和搬运。根据货物的特点和运输的不同要求，乙方应在包装箱上清楚地标注“小心轻放”、“此端朝上，请勿倒置”、“保持干燥”等字样和其他适当的标志。
10. **运输和保险**
	1. 乙方负责办理将货物运抵招标文件规定的交货地点，包括合同规定的保险和储存在内的一切事项，有关费用应包括在合同总价中，并且，乙方应承担货物在途期间以及装卸过程中可能发生的毁损、灭失的法律风险。
	2. 乙方负责办理货物在运抵过程中的全程保险，并以货物发票金额的百分之一百一十（110%）为货物办理“一切险”。
11. **伴随服务**
	1. 甲方有权要求乙方提供下列服务中的任一或所有服务，包括本招标文件规定的附加服务（如果有的话）：
12. 实施或监督所供货物的安装和/或试运行；
13. 提供货物安装和/或维修所需的工具；
14. 为所供货物的每一适当的单台设备提供详细的操作和维护手册；
15. 在双方商定的一定期限内对所供货物实施运行或监督或维护或修理，但前提条件是该服务并不能免除乙方在合同保证期内所承担的义务；
16. 在乙方或制造厂和/或在项目现场就所供货物的安装、试运行、运行、维护和/或修理对甲方人员进行培训。
	1. 乙方应提供本项目招标文件中规定的所有服务。为履行要求的伴随服务的报价或双方商定的费用已经包括在合同价中。
17. **备品备件**
	1. 乙方应按照本项目招标文件、投标文件中的规定提供所需的备品备件。
	2. 在备品备件停止生产的情况下，乙方应事先将要停止生产的计划通知甲方，使甲方有足够的时间采购所需的备品备件；
	3. 在备品备件停止生产后，如果甲方要求，乙方应免费向甲方提供备品备件的蓝图、图纸和规格。
18. **保证**
	1. 乙方应保证合同项下所供货物是全新的、未使用过的。乙方进一步保证，合同项下提供的全部货物没有设计、材料或工艺上的缺陷，或者没有因乙方的行为或疏忽而产生的缺陷。如乙方提供的货物存在技术缺陷或事故隐患造成甲方或任何第三方人身、财产损害的，乙方应当对该损害承担全部法律责任。如由于乙方的违约行为造成甲方损失的，乙方还应当赔偿甲方的全部损失。
	2. 本保证应持续有效。质量保证期及免费维修保养服务期限按本项目招标文件、投标文件规定执行**。**
	3. 甲方应尽快以书面形式通知乙方保证期内所发现的质量问题。
	4. 乙方在收到甲方通知后应在本项目招标文件、投标文件规定的时限内将出现质量问题的货物免费维修或更换完毕。
	5. 如果乙方未在本项目招标文件、投标文件规定的时限内将出现质量问题的货物免费维修或更换完毕，视为乙方恶意违约，在此种情况下，甲方可采取必要的补救措施，但其风险和费用将由乙方承担，甲方凭维修通知及维修单位出具的发票即可向乙方索赔而无需提供该项维修责任形成原因的证据。甲方根据合同规定对乙方行使的其他权力不受影响。
19. **索赔**
	1. 如果本合同项下的货物不符合约定的标准及/或乙方保证的，甲方有权在合同条款第13条或合同的其他条款规定的检验、安装、调试和质量保证期内提出索赔要求，乙方应按照甲方同意的下列一种或几种方式结合起来解决索赔事宜：
20. 如甲方决定退货，则乙方应将其向甲方收取的全部价款退还甲方，并承担甲方由此发生的一切损失和费用，包括利息、银行手续费、运费、保险费、检验费、仓储费、装卸费以及为看管和保护退回货物所需的其它必要费用；
21. 根据货物的偏差情况、损坏程度以及甲方所遭受损失的金额，降低货物的价格；
22. 用符合合同规定的规格、质量和性能要求的新零件、部件和／或设备来更换有缺陷的部分和／或修补缺陷部分，乙方应承担一切费用和风险并负担甲方蒙受的全部直接损失费用。同时，乙方应按合同条款第13条规定，相应延长修补和／或更换件的质量保证期。
	1. 如果在甲方发出索赔通知后10天内，乙方未作答复，上述索赔应视为已被乙方接受。如乙方未能在甲方发出索赔通知限定的期限内或甲方同意的延长期限内，按照甲方同意的上述规定的任何一种方法解决索赔事宜，甲方将从应付货款或从乙方开具的履约保证金中扣回索赔金额。
23. **付款**
	1. 本合同以人民币付款。
	2. 乙方应按照双方签订的合同规定交货。交货后乙方应把下列单据提交给甲方，甲方按合同规定审核后付款：
24. 发票；
25. 全部工程技术资料；
26. 制造厂家出具的质量检验证书和数量证明书；
27. 由买卖双方签字的验收证书。
	1. 甲方付款方式和条件：

 甲方将按照本项目招标文件规定的时间和方式向乙方支付合同价款。

1. **价格**

乙方在本合同项下提交货物和履行服务的价格在合同中给出。

1. **合同修改**

本合同履行过程中，甲方需追加与合同标的相同的货物或服务的，在不改变合同其他条款的前提下，可以与乙方协商签订补充合同，但所有补充合同的采购金额不超过原合同采购金额的百分之十。甲乙双方均不得擅自变更合同，但是如果合同继续履行将损害国家利益和社会公共利益的，双方应当变更合同，有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。

1. **转让和分包**
	1. 乙方不得部分转让或全部转让其享有的合同权利及应履行的合同义务。
	2. 未经甲方书面同意，乙方不得将本合同项下应由乙方履行的义务和工作分包给第三方完成。甲方同意分包的，乙方仍应当就分包项目向甲方负责，接受分包的第三方就分包项目承担连带责任。
	3. 乙方违反合同约定转让合同权利、义务或者分包的，乙方应当向甲方支付合同总价30%的违约金，并且，于此情形下甲方有权决定提前解除合同。
2. **乙方履约延误**
	1. 乙方应按照招标文件中规定的交货时间交货和提供服务。
	2. 在履行合同过程中，如果乙方及其分包人遇到妨碍按时交货和提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的时间和原因通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延长交货时间以及是否收取延期交付违约金。
3. **延期交付违约金**

除遇到合同规定的不可抗力情况外，如果乙方没有按照合同的时间交货和提供服务，甲方应在不影响合同项下的其他补救措施的情况下，有权从合同款项中扣除乙方应当支付的违约金。每延误一天的，乙方应当按迟交货物或服务的费用的百分之零点零肆(0.04％)向甲方支付违约金，直至实际交付为止。延期交付超过 30日时，甲方有权根据合同条款第21条的规定解除合同，甲方因此解除合同的，乙方应当支付合同价格 30 % 的违约金作为赔偿。

1. **违约解除合同**
	1. 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可向乙方发出书面违约通知书，提出解除合同。
2. 乙方延期交付达到约定的合同解除情形。
3. 如果乙方未能履行合同规定的其它任何义务达到合同约定的甲方有权解除合同的情形或者因此导致合同目的无法实现的。
4. 如果甲方认为乙方在本合同的竞争和实施过程中有腐败和欺诈行为。为此目的，定义下述条件：
	1. “腐败行为”是指提供、给予、接受或索取任何有价值的物品来影响相关人员在采购过程或合同实施过程中的行为。
	2. “欺诈行为”是指为了影响采购过程或合同实施过程而恶意隐瞒或谎报事实，损害甲方利益的行为。
5. **不可抗力**
	1. 签约双方任何一方由于不可抗力事件的影响而不能执行合同时，履行合同的期限应予以延长，其延长的期限应相当于事件所影响的时间。不可抗力事件系指买卖双方在缔结合同时所不能预见的，并且它的发生及其后果是无法克服的事件，诸如战争、严重火灾、洪水、台风、地震等。
	2. 受影响的一方在不可抗力事件发生后尽快用书面形式通知对方，并于不可抗力事件发生后十四（14）天内将有关当局出具的证明文件用特快专递或挂号信寄给对方审阅确认。一旦不可抗力事件影响持续超过一百二十（120）天以上，双方应通过友好协商在合理的时间内达成进一步履行合同的协议。
	3. 因合同一方迟延履行合同后发生不可抗力的，不能免除迟延履行方的相应责任。
6. **因破产解除合同**

如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方，提出解除合同，甲方有权将已收货物退还乙方，合同解除前如果乙方只提供了部分货物且该部分货物可以满足甲方采购货物最终要实现的目的的，甲方仅就该部分货物支付相应的货物，并有权不支付乙方未履行合同义务部分相对应的合同价款。该合同将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权利。

1. **争议的解决**
	1. 因执行本合同所发生的或与本合同有关的一切争议，双方应通过友好协商解决。如果协商不能解决，双方确定通过向本合同签订地有关人民法院提起诉讼方式解决争议。
2. **合同语言**

本合同语言为简体中文。双方交换的与合同有关的信函均用简体中文书写。

1. **适用法律**

本合同应按照中华人民共和国的现行法律进行解释。

1. **通知**
	1. 本合同一方给对方的通知应用书面形式送到合同中规定的对方的地址。
	2. 通知以送到日期或通知书的落款日期为生效日期，两者中以晚的一个日期为准。
2. **税款**

本合同项下乙方所提供的货物和服务的所有税费均已包含于合同价格，甲方不再另行支付。按照中华人民共和国税法和有关部门的规定，乙方需交纳的与本合同有关的一切税费均应由乙方负担。

1. **合同生效及其他**

本合同以双方法定代表人或授权代表签字、加盖双方单位印章并且甲方收到乙方提交的履约保证金后生效。

## 合同格式

 （以下简称“甲方” ）为一方和 （以下简称“乙方” ）为一方同意按下述条款和条件签署本合同（以下简称“合同” ）：

1. **合同文件**

本合同所附下列文件是构成本合同不可分割的部分：

1. 合同条款及附表
2. 投标人提交的投标声明函和报价表
3. 技术规格（包括图纸，如果有的话）
4. 澄清函及有关文件
5. 中标通知书
6. 招标文件
7. 投标文件
8. **合同范围和条件**

本合同的范围和条件应与上述合同文件的规定相一致。

1. **货物及数量**

本合同所提供的货物及数量详见招标文件和投标文件。

1. **合同金额**

根据上述合同文件要求，合同的总金额为 元人民币，分项价格在报价表中有明确规定。

1. **付款条件**

本合同货物的付款条件在合同条款中有明确规定。

1. **交货时间和交货地点**

本合同货物的交付时间和交货地点在本项目招标文件中有明确规定。

1. **合同生效**

本合同经双方法定代表人或授权代表签字、加盖双方单位印章并且甲方收到乙方提交的履约保证金后生效。

1. **其它**

本合同一式 份，其中甲方 份，乙方 份，采购中心**一**份。本合同签订于 。

**甲方名称（盖章） 乙方名称（盖章）**

**甲方代表签字： 乙方代表签字：**

签订地点： 签订日期： 年 月 日

履约保证金保函（样式）

开具日期：

**致：（甲方名称）**

 号合同履约保函

本保函作为贵方与（乙方名称）（以下简称乙方）于 年 月 日就 项目（以下简称项目）项下提供（货物名称）（以下简称货物）签订的 （合同号）号合同的履约保函。

（出具保函银行名称）（以下简称银行）无条件地、不可撤消地具结保证本行、其继承人和受让人无追索地向贵方以人民币支付总额不超过（货币数量），即相当于合同价格的 %，并以此约定如下：

1. 只要贵方确定乙方未能忠实地履行所有合同文件的规定和双方此后一致同意的修改、补充和变动，包括更换和/或修补贵方认为有缺陷的货物（以下简称违约），无论乙方有任何反对，本行将凭贵方关于乙方违约说明的书面通知，立即按贵方提出的累计总额不超过上述金额的款项和按贵方通知规定的方式、时间付给贵方，本行放弃行使抗辩权。
2. 本保函项下的任何支付应为免税和净值。对于现有或将有的税收、关税、收费、费用扣减或预提税款，不论这些款项是何种性质和由谁征收，都不应从本保函项下的支付中扣除。
3. 本保函的条款构成本行无条件的、不可撤销的直接责任。对即将履行的合同条款的任何变更、贵方在时间上的宽限、或由贵方采取的如果没有本款可能免除本行责任的任何其它行为，均不能解除或免除本行在本保函项下的责任。
4. 本保函在贵方与乙方签订的合同全部履行完毕前（含质量保证期）完全有效。

谨启

出具保函银行名称

签字人姓名和职务

签 字 人 签 名

公 章

一、总体要求

1. 本部分内容是根据本项目实际情况制定的。
2. 投标人必须仔细阅读本部分的全部条款。对本部分中存在的任何疑问、遗漏或相互矛盾之处，或是对于相关要求不清楚，认为存在歧视、限制的情况，投标人可以向采购中心寻求书面澄清。
3. 本部分所列明的工艺、材料和设备的标准以及参照的品牌或分类号仅起说明作用，并没有任何限制性，投标人在投标中可以选用替代标准，品牌或分类号，但这些替代应当等于或优于文件技术要求。
4. 付款方式：
	* 1. 合同生效后**7**天内，采购人向中标供应商支付合同总金额的**30**%；
		2. 中标供应商将合同货物安装、调试、试运行完成，经采购人最终验收签发最终验收证书后30天内，采购人向中标供应商支付合同总金额的65%；
		3. 合同生效一年后**30**天内，采购人向中标供应商支付合同总金额的5%。

二、项目概述

中国劳动关系学院是中华全国总工会所属，重点培养劳动关系和工会等领域从事协调劳动关系、工会工作、劳动法律、经济管理、公共管理等方面人才的普通高等学校，学院有北京、河北涿州两个校区。

我校校园局域网络分为北京和涿州两个部分,两个局域网络都有各自的互联网出口，之间通过两条共1.6G的点对点线路进行连接，用来传输服务器和一卡通等数据；北京校区和涿州校区目前各采用两台型号为H3C S7506E交换机通过IRF虚拟化作为校园有线网和无线网的核心交换机；

校园服务器区为校园网提供业务支持，包括动态主机配置协议、域名解析、校园卡等业务，两校区网络拓扑结构如下：



三、项目建设目标

为了实现数字化校园建设的总目标，本项目作为其子项目，为建成后的数字化校园平台提供安全保证。

随着网络技术的高速发展，高校网络建设一直走在网络发展的前端。而近几年来，网络的安全问题日益突出，黑客攻击、网络病毒等等已经屡见不鲜，而且一次比一次破坏力大，对网络安全造成的威胁也越来越大，一旦网络存在安全隐患，遭受重大损失在所难免。

随着我校网络规模的急剧膨胀，网络用户的快速增长，一方面校园网已从早先教育、科研的试验网的角色已经转变成教育、科研和服务并重的网络，校园网在学校的信息化建设中已经在扮演了至关重要的角色，作为数字化信息的最重要传输载体，如何保证校园网络能正常的运行不受各种网络黑客的侵害就成为不可回避的一个紧迫问题；另一方面，高校是思想政治和意识形态的重要阵地，确保学生的身心健康，使他们具备一个积极向上的意识形态，必须使学生尽可能少地接触网络上的不良信息。因此，解决网络安全问题刻不容缓。

根据信息安全体系建设的目标，分析我校各信息系统实际安全需求，结合业务信息的实际特性，并依据《信息安全技术信息系统安全等级保护基本要求》、《安全设计技术要求》等相关标准规范，建立符合我校实际业务需求的信息安全保障体系。一个完整的信息安全保障体系应该是安全管理和安全技术实施的结合，两者缺一不可。针对我校实际情况，本次着重对动态主机配置协议、域名转换等设备进行优化，提升学校网络整体使用感受，保障整体网络系统的顺畅运行。同时基于我校教师远程访问校园网资源的需求，本次基于公网建设虚拟专用网络，为师生提供远程访问的接口，提升校园网资源利用率。同时对学校网站、整体业务系统进行加固，规范信息系统管理流程，从物理空间、虚拟空间多方面加强学校整体信息系统的安全性。

总体设计上应遵循稳定可靠、技术领先、经济实用、操作简单、维护简便、方便扩展和升级的基本原则，达到系统稳定、功能完善、拓展性强的应用效果。系统设计和设备选型注重技术成熟、功能实用、性价比高等特点。系统建设注重细节，力争做到全面规划、统一实施、注重应用、节约成本，充分保证用户的利益，并支持未来的扩展和升级。

四、项目建设内容

## 4.1设计要求

项目设计需要充分考虑我校两个校区的网络拓扑和实际网络需求，参考国家信息系统安全等级保护的相关文件，利于我校未来进行等级保护定级、整体建设需要考虑与我校原有设备的对接，与近期新建项目的兼容性，以及未来建设的可扩展性，本次项目主要包括内容有：

1、在整个网络系统内部署一台安全漏洞扫描设备，针对网络系统、业务服务器的安全漏洞进行扫描和预警，提高整个信息系统的安全性。

2、在DMZ区到下一代防火墙之间增加Web应用防火墙，对4-7层应用进行保护，节约防火墙性能，提供更有针对性的防护，设备选型需要考虑与现有防火墙的对接，安全策略配置，保障服务器业务不中断，提升学校网页、应用安全性。

3、利用专门的安全设备加固学校业务系统，对服务器区进行运维安全审计，提高服务器区的安全性，防止业务系统因为遭受攻击而中断服务。

4、本次建设针对学校动态主机配置协议速度缓慢的情况，考虑增加4台安全动态主机配置协议设备，提升学校内部网络自动分配IP地址的速度，省去师生手动输入地址的繁琐操作，设备需与现有动态主机配置协议系统对接，平滑过渡，提升性能同时保障整体的高可用性。

5、建设学校虚拟专用网络，利用公用网络上建立专用网络，进行加密通讯。虚拟专用网络设备通过对数据包的加密和数据包目标地址的转换实现远程访问。要求同时支持IPSec和SSL 两类协议。为学校校外用户访问校园网，提供安全远程接入路径，防止有不法分子恶意加载链接，并且阻隔黑客攻击。为了更好的支持虚拟专用网络，设备采取单臂模式，减少对主干链路的影响。设备需保留性能扩展能力，便于以后按需扩展。

6、针对学校域名解析设备性能不足的情况，考虑增加6台安全域名解析设备，增强校园网络的地址解析能力，提高网络访问响应速度，改善用户使用体验，设备需要和学校现有服务器系统实现无缝对接，对接过程中需要确保整个信息系统平稳运行，业务不中断。

7、升级学校现有网络运维管理平台，增加本次项目相应的设备管理授权，要求可以和原有管理平台、IT运维管理系统、资产管理系统进行无缝对接，保障学校业务的连续性。

8、学校原有核心机房进行安全改造施工，投标方需提供施工所需的人工、辅材、运输、搬迁等。

## 4.2设备材料清单

**本工程所需要的设备和材料清单如下：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **单位** | **型号及技术规格** |
| 1 | 安全漏洞扫描设备 | 1  | 台 | 详见4.3.1技术参数及配置要求 |
| 2 | Web应用防火墙 | 1  | 台 | 详见4.3.2技术参数及配置要求 |
| 3 | 安全运维审计设备 | 1  | 台 | 详见4.3.3技术参数及配置要求 |
| 4 | 安全动态主机配置协议设备 | 4  | 台 | 详见4.3.4技术参数及配置要求 |
| 5 | 安全虚拟专用网络设备 | 1  | 台 | 详见4.3.5技术参数及配置要求 |
| 6 | 安全域名解析设备 | 6  | 台 | 详见4.3.6技术参数及配置要求 |
| 7 | 安全运维管理系统 | 1  | 套 | 详见4.3.7技术参数及配置要求 |
| 8 | 门禁控制器 | 1 | 台 | 详见4.3.8技术参数及配置要求 |
| 9 | 电磁锁 | 1 | 个 |
| 10 | 读卡器 | 1 | 个 |
| 11 | IC卡 | 10 | 张 |
| 12 | 出门按钮 | 1 | 个 |
| 13 | 监控摄像头 | 6 | 个 |
| 14 | 硬盘录像机 | 1 | 台 |
| 15 | 无线传输交互系统 | 1 | 套 |
| 16 | 线缆辅材 | 1 | 项 |
| 17 | 光跳线 | 20 | 根 | LC-LC接口，长度2米 |
| 18 | 千兆多模光模块 | 10 | 个 | 850nm波长千兆SFP光模块 |

**注意：以下设备或系统技术要求中，**

**标带“**★**”号为重要项，不满足按无效投标处理；以下指标带“⊙”号为较重要项，如不满足按负偏离处理。**

## 4.3安全设备和系统技术要求

**★注：安全漏洞扫描系统、Web应用防火墙、安全运维审计设备、安全动态主机配置协议设备、安全虚拟专用网络设备、安全域名解析设备、安全运维管理系统、无线传输交互系统需要提供三年原厂售后服务承诺函（含软件免费升级）；**

**4.3.1安全漏洞扫描系统**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ★设备配置要求 | 千兆以太网电口≥6个，千兆光口≥2个； |
| 支持2个扩展槽位，最大支持16GE接口能力； |
| 所有固化端口均可作为扫描端口，即端口全放开授权，不允许后续增收授权费用； |
| ★产品性能 | 授权扫描IP数量≥512； |
| 并发IP数：≥200； |
| 并发任务数≥6； |
| ★特征库 | 漏洞库≥10000种；漏洞库能够保证定期升级； |
| 漏洞库支持手动升级和自动升级，支持本地升级和在线升级； |
| 主机漏洞扫描 | 支持扫描主流操作系统、数据库、网络设备的漏洞，并在漏洞库列表中体现； |
| 能够扫描主流虚拟机管理系统的安全漏洞，如：VMWareESX/ESXi等； |
| 支持Windows补丁扫描； |
| 支持web服务漏洞检测，包括Apache、Tomcat、Jboss、Microsoft-IIS等服务器漏洞检测； |
| 支持SMTP漏洞扫描，如SendMail等主流邮件服务器的漏洞扫描； |
| 支持对知名和自定义主机端口扫描； |
| 支持FTP漏洞扫描，如支持Serv-U、VsFTP、ProFTPD服务器等； |
| 支持弱口令扫描：可根据预定义弱口令字典，利用FTP、Telnet、SMTP、SSH、SMB、POP3、MySQL、SQL Server等协议进行弱口令扫描探测， |
| 支持数据库扫描，包括MySQL、Sybase、Oracle等； |
| 提供专门针对DNS服务的安全漏洞的检测； |
| 支持常见应用软件漏洞扫描，如IE、Chrome、Adobe等常用应用软件漏洞扫描； |
| 支持针对Windows、Unix/Linux、数据库、DNS检测等不同的扫描目标定义不同的扫描策略； |
| 支持单个扫描任务，可同时扫描资产树中不同资产组； |
| 支持对扫描任务进行优先级划分； |
| ★安全基线检查 | 支持对主机系统（如Windows、Linux等系统）进行安全评估，准确发现信息系统中存在的安全漏洞和配置隐患； |
| 扫描方式 | 支持定时扫描（定期扫描可细化到每天、每周、每月）； |
| 支持手动扫描； |
| 扫描对象 | 支持多个域名/IP设置扫描对象； |
| 支持子域名/URL设置扫描对象； |
| 支持多个扫描对象扫描； |
| ⊙支持IPv6； |
| 系统管理 | 支持ICP备案提醒； |
| 支持HTTPS； |
| 支持管理分级管理； |
| 报表分析 | 可选择不同时段的扫描结果进行比对； |
| 根据漏洞严重级别、漏洞名和漏洞数量等统计排序前10的漏洞； |
| 报表模板丰富，支持针对资产组的风险分析，支持不同资产组之间的对比分析； |
| 提供详细的漏洞报告； |
| 统计分析：提供基于漏洞类型、服务器、事件的统计分析，直观展示总体漏洞分布与趋势； |
| 报表导出：支持PDF、CSV、EXCEL、HTML、XML导出； |
| 产品资质 | 提供国家保密局《涉密信息系统产品检测证书》； |
| 提供中国信息安全认证中心《中国国家信息安全产品认证证书》（增强级）； |

**4.3.2 Web应用防火墙**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★产品规格 | 设备高度不超过2U。 |
| 串口：≥1个RJ45。 |
| 管理口：≥2个GE。 |
| USB口：≥2个。 |
| 千兆光口插槽：≥4个。 |
| 万兆插槽：≥2个，配置相应数量的原厂光模块。 |
| 应用层吞吐量：≥6Gbps。 |
| 网络吞吐量：≥8Gbps。 |
| 冗余双电源 |
| 防护功能要求 | ★支持HTTP 0.9/1.0/1.1，完全解析HTTP事务。 |
| 支持对HTTP协议的异常元素、异常参数、非法编码和解码的灵活控制与处理。 |
| 支持HTTP访问控制功能，可以提供针对HTTP元素和客户端的组合访问控制策略。 |
| 支持根据用户配置的服务器信息，自动生成一套安全解决方案。 |
| ★支持对Web服务器、数据库、开发语言的基础防护，包括了Apache、IIS、Tomcat、Nginx、Weblogic等Web服务器类型，SQL Server、Oracle、Mysql等数据库类型，PHP、ASP、Java、.Net等开发语言的深入防护。 |
| ⊙支持对注入、XSS、SSI指令、路径穿越及远程文件包含的攻击防护。 |
| 支持CSRF（跨站请求伪造）防护。 |
| 支持爬虫防护，实现对100种以上的爬虫特征进行识别和阻断，防止页面因爬虫而引起信息泄露等问题。 |
| 支持盗链防护，可采用Referer和Cookie算法，有效识别网页盗链行为，避免用户网页资源被滥用。 |
| ⊙支持通过规则库防护Web扫描，支持以统计算法分析扫描行为的扫描防护。 |
| 支持Cookie安全机制。 |
| 支持敏感关键字自定义功能。 |
| 可以根据文件大小、MIME类型及文件扩展名灵活定义下载限制策略，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等）。 |
| 支持URL ACL。对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE等。 |
| ★支持对SSL（HTTPS）加密会话进行分析。 |
| ⊙支持对安全策略的一键式例外配置。 |
| 提供网页篡改防护以及服务器侧恶意代码过滤功能。 |
| 日志与报表要求 | 支持不同安全事件类型以不同的颜色区分。 |
| 支持基于时间、IP、端口、动作、事件类型、URI、方法等条件的日志查询。 |
| 支持在安全日志中带有客户端真实IP地址，便于IP溯源。 |
| 支持日志分时段导出、全部导出或者清空。 |
| 支持提供PCI-DSS符合性报表。 |
| 管理功能要求 | 支持标准SNMP trap和Syslog接口。 |
| 支持与时间服务器同步。 |
| 系统应提供配套的集中管理平台，实现设备的集中管理功能，可对管理范围内的所有引擎设备进行统一的状态监控、策略配置、系统升级和日志报表管理。 |
| 产品资质 | ★提供中国信息安全认证中心的《中国国家信息安全产品认证证书》。 |
| 提供中国信息安全测评中心《国家信息安全测评信息技术产品安全测评证书》（EAL3）。 |

**4.3.3 安全运维审计设备**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★产品规格 | 采用物理旁路模式部署方式。 |
| B/S架构，采用HTTPS方式远程安全管理，无需安装客户端。 |
| 千兆电口≥4个。 |
| 系统自带内部存储，存储空间≥2T。 |
| 并发访问 | 图形并发：≥100个。字符并发：≥300个。 |
| ★授权可管理设备 | 数量≥100台。 |
| 用户角色 | 具有用户多角色划分功能，如堡垒机管理员、设备管理员、普通用户、审计管理员等，对各类角色需要进行细粒度的权限管理。 |
| 身份认证 | 主帐号登录堡垒机应支持本地静态密码认证，LDAP认证、RADIUS认证、证书认证等身份认证方式。 |
| 设备访问授权 | 身份认证之外，需要更高级管理员授权才能对设备进行运维操作。 |
| 命令执行授权 | 对特定命令的执行需要更高级管理员授权才能执行。 |
| ⊙目标设备登录方式 | 支持自动登录目标设备功能，运维人员不必知道目标设备帐号及密码，无需进行二次登录认证，实现单点登录。 |
| 支持手工登录目标设备，运维人员每次通过堡垒机登录目标设备都需要手工输入目标设备用户名密码。 |
| 支持运维人员半自动登录目标设备，即第一次登录目标设备时运维人员需手工输入目标设备帐号和密码并允许堡垒机保存该帐号密码，运维人员就可以自动登录目标设备。 |
| ⊙主账号关联 | 支持以首页中的主账号为基准，支持直接查询并编辑与该主账号相关的策略。 |
| 支持以首页中的设备为基准，支持直接查询该主账号有权限运维的所有设备。 |
| 支持以首页中的设备为基准，支持直接查询该主账号的所有审计信息。 |
| ⊙设备关联 | 支持以首页中的设备为基准，支持直接查询并编辑与该设备相关的策略。 |
| 支持以首页中的设备为基准，支持直接查询有权限运维该设备的所有普通用户。 |
| 支持以首页中的设备为基准，支持直接查询该设备的所有审计信息。 |
| 目标设备分组展示 | 用户登录堡垒机后可在首页分组显示该用户有权限管理的目标设备，分组依据应支持按部门、按设备类型、按业务类型分组。 |
| ⊙账号维护 | 支持批量导入用户帐号信息。 |
| ⊙设备维护 | 支持批量导入目标设备信息。 |
| 自动修改从账号密码 | 支持定期自动修改目标设备密码功能。 |
| 特权密码代填 | 支持自动填写特权密码，从普通管理模式进入到特权模式。 |
| 实时监控 | ⊙支持实时监控通过SSH、SFTP、RDP、VNC 、Telnet、FTP等协议的操作行为；对监控到的非法操作，可实时手工切断。 |
| 静态路由 | 可添加静态路由信息，部署于复杂的网络环境。 |
| 支持的协议 | 字符型远程操作协议：SSH(V1、V2)、TELNET。 |
| 图形化远程操作协议：RDP、VNC、X11，其支持文件共享。 |
| 文件传输协议：FTP、SFTP。 |
| 支持Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、PostgreSQL等数据库。 |
| 支持HTTP、HTTPS操作审计。 |
| 应用发布 | 可通过应用发布的方式进行协议扩展，无需定制即可支持其他通用及专有的运维客户端程序。 |
| 支持的设备访问方式 | Web访问方式:支持通过审计系统的Web页面直接访问设备。 |
| ⊙客户端访问方式：支持通过SecurCRT等常用的命令行客户端工具登录堡垒机并访问目标设备。 |
| 登录菜单访问：客户端访问审计系统即可显示用户能访问的资源菜单，用户通过字符菜单或图形菜单选择方式直接访问设备。 |
| 操作行为记录 | Telnet、SSH审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议类型、事件等级及操作内容回放。 |
| RDP、VNC、HTTP、HTTPS等协议审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议/应用类型、事件等级、操作内容等；支持操作内容录像回放。 |
| 数据库运维操作审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、应用类型、事件等级、操作内容等；支持操作内容录像回放。 |
| 文件操作审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议类型、事件等级、操作内容（如对文件的上传、下载、删除、修改等操作等）。 |
| 产品资质 | 提供国家保密局涉密信息系统产品认证。 |
| 提供中国信息安全测评中心《国家信息安全测评信息技术产品安全测评证书》（EAL3）。 |

**4.3.4 ：安全动态主机配置协议设备**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★硬件架构 | 动态主机配置协议软件必须为自主研发软件，不能采用开源软件BIND软件。 |
| ★性能指标 | LPS指标：≥500，可以自动关闭日志提高性能，可扩展域名解析功能。 |
| 硬盘：≥500G。 |
| ★接口数量 | 千兆电口：≥6个10/100/1000M自适应电口。万兆光口：≥2个万兆光口，配备相应数量的原厂万兆光模块。 |
| 高可用性 | 主备多管理中心，HA双机互为备份，能实现双网卡主备/负载，能实现健康检测、宕机切换（Ping、TCP、HTTP、HTTPs多种策略）能实现动态主机配置协议 Failover，灵活的手动接管设置。 |
| 能实现双网卡互为主备及负载均衡，提供交流冗余电源。 |
| 软件功能要求 | ★系统支持IPv6核心协议及互通性操作。 |
| 可视化中文界面：用户输入、报表、管理界面、告警事件的信息等均能实现中文界面。 |
| 能实现同Radius、TACACS+、LDAP认证方式对接。 |
| ⊙可通过中央管理器进行全部功能GUI管理（https），支持通过图形界面进行地图展示，主管理中心、备管理中心、节点设备拓扑展示。 |
| 能实现SNMP V2/V3 、SFTP、Syslog，、TFTP文件管理。 |
| ⊙能实现本地策略，基于域名/IP/IP段/IP全地址的解析限速，防范缓存中毒、域名劫持等主要的域名安全威胁。 |
| 能实现动态主机配置协议指纹，临时授权、地址回收、动态主机配置协议v6,共享网络配置，灵活、丰富的Option设置、Option精细下发。 |
| 能实现基于MAC、指纹、Option的访问控制，地址池的自定义属性、手动清除租约。 |
| 能实现手动地址、僵尸地址、固定地址和预留地址管理，地址类型一键转换,全局搜索。 |
| 探测网络，IP和网络变化探测和审计\探测设备，获取如交换机内的IP、MAC等信息拓展。 |
| ⊙能实现MAC管理、网络管理的自定义属性设置,基于视图的失败转发，定期数据备份，配置回滚。 |
| 能实现统一下发升级文件，不同节点按需完成升级；故障设备的即时替换，数据配置一键恢复。 |
| 图形化统计报表，LPS、指纹等统计，全节点的总体统计。 |
| 用户操作日志，系统日志，告警阈值设置，日志告警，多种方式发送告警信息。 |
| 多用户/多角色/多权限，域名解析授权管理，可基于view授权，可基于zone授权。 |
| ⊙可基于权威记录授权，集中或分布管理，动态主机配置协议授权管理，可基于网络授权，可基于地址池授权,要求能实现多角色管理和授权。 |
| 产品资质 | 提供中国信息安全测评中心《国家信息安全测评信息技术产品安全测评证书》。 |

**4.3.5 ：安全虚拟专用网络设备**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★硬件标准 | 设备高度不超过2U。 |
| 千兆电口：≥6个。 |
| 万兆光口：≥2个，配备相应数量的原厂万兆光模块。 |
| 流缓存硬盘容量：≥500G。 |
| 内存：≥2G。 |
| CF卡：≥1G。 |
| 性能指标 | 防火墙代理并发会话数目：≥600000 。  |
| 吞吐量：≥1.5Gbps。 |
| SSL最大加密流量：≥200M。  |
| ★SSL理论并发用户：≥800人。  |
| ⊙SSL理论新建用户数（个/秒）：≥90。  |
| ⊙IPSec理论并发会话数：≥3600。  |
| IPSec最大加密流量：≥85M。 |
| IPSec理论并发隧道数：≥400。 |
| 部署方式 | 支持网关模式、单臂模式部署两种方式。 |
| 基本特性 | 专业虚拟专用网络设备，采用标准SSL、TLS 协议，同时支持IPSec 虚拟专用网络、SSL虚拟专用网络两种虚拟专用网络，非插卡或防火墙带虚拟专用网络模块设备。 |
| ★支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用。 |
| ★支持PC终端使用包括Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；支持Windows、IOS、Android、塞班、黑莓等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入，或通过PPTP、L2TP 虚拟专用网络方式接入。 |
| 产品可支持中国国家标准的商用密码算法，包括：SM1，SM2、SM3、SM4。（提供所投产品生产厂家的商用密码生产、销售、型号三证） |
| 终端安全 | 产品必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。 |
| 支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问。 |
| 权限、服务器安全 | 产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权。  |
| 产品应具有角色授权机制，支持在用户组的基础上，根据角色的不同，组合关联不同的资源权限。 |
| 支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，虚拟专用网络资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统。  |
| 支持关键文件保护功能，可针对特定应用关键文件进行锁定，防止用户进行篡改进行越权。 |
| 针对服务器地址保护方面，可支持SSLVPN资源列表界面上的用户授权资源隐藏；针对B/S应用，可进行URL地址伪装，防止服务器真实IP地址泄露。 |
| 稳定性、可扩展性、高速性 | 支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度。 |
| 支持针对移动APP的虚拟专用网络安全代码的自动封装，实现App应用的安全加固。 |
| 支持HTP快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议。 |
| 支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。 |
| ⊙支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式。 |
| 移动智能终端支持 | 产品必须支持远程应用发布功能，可以无需二次开发，即把Windows应用发布到移动智能终端中，也可以支持无需开发，将C/S资源Web化。 |
| 产品必须支持对终端服务器的实时监测，包括服务器综合状态、CPU使用率、内存使用率、磁盘I/O、远程应用会话数、服务器当前会话数。 |
| 产品应该支持企业级“云盘”（又名“网盘”、“文件共享”）功能，即可以通过手机、PC、IPAD的客户端，将数据、文件同步到云端或和分享到终端。 |
| 能够支持分享给他人。 |
| 远程应用发布必须支持应用权限控制项，不得通过远程应用访问任何未经授权的windows资源，至少应该包括：未经授权的应用程序、注册表、任务管理器、资源管理器、控制面板、cmd命令提示行、Win+R运行命令行、管理选型、映射网络驱动器选型、断开网络驱动器选型、回收站、网上邻居等。并支持隐藏本地原有磁盘，仅提供公共磁盘。 |
| 支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性，针对图像数据，服务端必须支持有损压缩算法；服务端必须能够支持过滤动态内容(gif/flash/video)以减少传输流量，且根据客户需要配置。 |
| 产品资质 | ★提供公安部颁发的《计算机信息系统安全专用产品销售许可证》。 |
| 提供公安部信息安全产品检测中心颁发的《GA/T 686-2007信息安全技术 虚拟专用网安全技术要求》三级或三级以上检测报告。 |

**4.3.6 安全域名解析设备**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| ★硬件标准 | 域名解析软件必须为自主研发软件，不能采用开源软件BIND软件。 |
| ★性能指标 | QPS指标：≥10万 ，可以实现QPS自动关闭日志，提高性能。 |
| 硬盘：≥500G。 |
| ★端口数量 | 千兆电口：≥6个10/100/1000M自适应电口, 万兆光口：≥2个万兆光口，配备相应数量的原厂万兆光模块。 |
| 高可用性 | 系统具备设备级、系统级、软件功能级冗余备份方案，能实现HA部署，来保护其安全、可靠运转。 |
| 能实现双网卡互为主备及负载均衡，提供交流冗余电源。 |
| 软件功能要求 | ★系统支持IPv6核心协议及互通性操作。 |
| 可视化中文界面：用户输入、报表、管理界面、告警事件的信息等均中文界面。 |
| 能实现分层次的多级部署，采用HTTPS协议下的WEB方式登陆和管理，通过中央管理设备上的统一集中式管理界面完成所有域名解析服务的配置，并可分配不同权限 。 |
| 能实现智能解析、基于视图的存根区、转发区和重定向。 |
| 必须实现安全加强，以更好的抵御和防范DOS和缓存攻击等主要的域名安全威胁。包括：能实现0x20，对外查询端口高度随机，对外并发查询数量限制，相同IP的并发查询限制，DNSSEC、EDNS等协议或算法机制。 |
| 能实现View备注、View禁用、健康检查、多区多视图、资源记录的批量修改。 |
| 能实现以区文件格式批量导入解析记录、增量导入、共享记录、A记录和ptr（反向记录）的联动、视图间的区拷贝。 |
| 能实现IDN（中文域名等），方便企业定制中文的内部域名体系和访问IDN外部网站。 |
| 能实现对域名解析所有数据的全局搜索，模糊搜索；域名解析查询限速，能实现DNS64和DNSSEC平滑部署。 |
| 能实现时间同步，域名解析系统可作为NTP服务器和NTP客户端，NTP服务器可选择性配置域名和IP地址。 |
| ⊙要求具有丰富的域名解析解析日志及统计报告，所有节点域名解析解析实时展示和统计，帮助网络管理员跟踪和快速解决与 域名解析配置有关的问题。统计CPU、内存、硬盘利用率、包括QPS、Top域名、Top IP 、解析记录统计、Ip\域名限速。 |
| 要求能实现中文图形化方式的全局所有子节点监控，包括：服务器性能、运行状态等。 |
| 可设定报警阈值，发生问题时可实时触发故障报警，要能能实现邮件、SNMP接口和URL回调等报警方式。 |
| ⊙要求能实现多角色管理和授权、账户保护功能（多次登陆失败则10分钟内禁止登陆）。能实现同Radius、TACACS+、LDAP认证，产品可拓展动态主机配置协议\IPAM功能。 |
| 产品资质 | 提供中国信息安全测评中心《国家信息安全测评信息技术产品安全测评证书》。 |
| ★提供公安部颁发的《计算机信息系统安全专用产品销售许可证》。 |

**4.3.7 安全运维管理系统**

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 功能参数 | ★要求支持纯IPV4、IPV6网络环境，以及IPV4/IPV6双栈网络环境。 |
| ⊙要求以物理拓扑图方式显示分区中设备和线路的连接关系，实时显示设备、线路的状态及性能参数，拓扑图数据刷新时间最短为10秒。 |
| 要求在拓扑图连线上直接显示流量数据，支持流量、单播包、广播包、错包、丢包、负荷、线速、广播包比例和峰值显示选择；连线箭头显示流量方向，支持双向、离心、向心和循环显示选择。 |
| 要求以星型拓扑图方式同时显示分区中服务器及其服务端口、网络连接的实时状态及运行参数。 |
| 要求自动生成终端档案、实时快照和接入日志。终端信息包括IP地址、MAC地址、上连设备端口、计算机名、域组、用户登录名、分区和最近出现时间；提供方便的终端查询功能；接入日志提供终端交换机端口的流量数据。 |
| 要求自动生成交换机与计算机终端连接关系拓扑图，实时显示交换机端口及终端的状态及参数。 |
| 能够提供设备CPU利用率排序表。 |
| ★要求系统支持应用URL监测，可以对WEB服务进行监控，支持HTTP协议和HTTPS协议。监测指定Web服务，可以指定端口。如果服务出现异常可以进行报警。 |
| ⊙要求自动发现无线AP的相关信息，监控AP的在线状态，并能维护AP所在位置、负责人等相关信息。要求自动发现接入的移动终端，监控移动终端的在线状态，并能维护移动终端的使用人、所属部门等相关信息。 |
| 要求支持单条和批量添加PING目标，PING目标可以是IP或者URL。 |
|  | ⊙提供IPV6网管认证证书。 |
| 要求本次提供运维平台可以与学校现有IT运维管理系统、资产管理平台进行对接 |
| 提供软件著作权登记证书复印件加盖原厂公章。 |

**4.3.8 机房物理安全防护**

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 门禁控制器 | 单门双向智能门禁控制器，可以独立使用，支持与学校一卡通系统对接。 |
| 电磁锁 | 单门门禁电磁锁，12V电源控制，最大闭合力≥250kg。 |
| 读卡器 | 门禁读卡器，识别距离不小于1.5cm。 |
| IC卡 | 非接触式IC卡。 |
| 出门按钮 | 门禁出门按钮，塑料材质。 |
| 监控摄像头 | 200万像素1/3寸 CMOS ICR日夜型半球网络摄像机、1/3寸自动变焦镜头，角度调整：水平:0°~355°,垂直:0°~65°；1个 RJ45 10M / 100M 自适应以太网口。 |
| 硬盘录像机 | 音视频输入/输出路数 32路 音视频接口 HDMI/VGA输出1路、音频输出1路 网络接口 2个，RJ45 10M/100M/1000M自适应以太网口 其它接口 语音对讲输入1路；串行接口2个；USB接口3个；报警输入16路报警输出4路 视频制式 PAL 视频编码方式 H.264 最大硬盘数量 8个SATA接口 配置8块3T专用监控硬盘 |
| 无线传输交互系统 | 设备接口：USB/VGA/HDMI/3.5mm音频；驱动程序免安装，随时随用方便快捷；支持电脑音视频信号无线传输,支持USB触控信号回传,支持VGA和HDMI视频信号同时输出,电脑端无需外接任何硬件设备即可实现无线传输,连续波辐射骚扰抗扰度：≥3V/m；需提供国家电子计算机质量监督检验中心的检测报告及产品电磁兼容性检验证书；★无线传输交互系统需提供原厂商三年售后服务承诺函。 |
| 线缆辅材 | 提供系统实施所需要的线缆包含，电源线、网线、光纤线缆及相应的布设工程，相关线缆长度需要投标方亲自去现场确定，并提供相关实施方案。 |
| 布线要求 | 本次机房监控系统需要与现有监控系统平台对接，本次项目实施需要包含终端设备上联到原有监控中心的布线工程。 |

## 4.4项目施工要求

**4.4.1 项目建设目标**

本次项目施工中北京校区综合楼核心机房及涿州校区核心机房涉及到原有服务器机柜的更换移位等工作，现有核心设备业务较为集中，设备间连线较为复杂，光缆配线架较为分散，机柜的移机割接工作要避开正常工作时间，同时保证校内业务不能中断。

施工方在设备机柜移机割接前要求与老师充分沟通，对设备移机割接工作时间，工作量进行讨论。

**4.4.2项目施工要求**

在施工过程中必须严格执行国家有关安全施规程，认真贯彻“安全为了施工，施工必须安全”及“预防为主”的方针，加强安全施工的科学 管理，建立安全施工责任制，做到谁施工、谁负责、强化安全教育和安全检查，落实安全措施，确保施工人员的安全、施工设备的安全、已施工完工工程的安全，杜绝事故的发生。

1、 针对本工程的安全施工制度，并组织施工人员学习，严格遵守；设立安全检察员负责施工安全工作。

2、 现场施工人员，在任何情况下不得违章指挥或违章施工，并遵守如下纪律：

 1） 进入施工现场必须戴安全帽，并正确使用个人劳保防护用品。

 2） 禁止酒后上岗作业，特种作业人员无操作合格证者，不准上岗作业。

 3） 现场施工人员应自觉服从实施组长和项目监理方监护检查。

 4） 现场施工人员应自觉遵守施工现场和项目监理方安全治安方面的管理要求。

3、 施工中产生的有危害施工安全的孔洞必须加以处理，防止有关事故的发生。

4、 施工现场所使用的有关工具应注意安全放置，杜绝由于使用和放置不当而造成的事故。

5、 对有关需现场制作且制作时干扰较大的加工作业应尽量远离公共区域。

6、 加强现场施工用电管理，对有关设备和线路应做到经常的检查和维护，分析技术难点。

**4.4.3项目服务要求**

**设备移机割接工作暂安排在每天晚上23:00至次日7:00之间进行。**

**在移机割接前提供详细的割接方案，在移机割接过程中，施工方需委派1名高级项目经理（信息系统集成及服务项目管理人员-高级项目经理）、2名网络调试高级工程师、2名中国信息安全测评中心注册信息安全专业人员（CISP）提供现场服务，在施工中软硬件相互配合，符合国家信息系统安全等级保护标准，保证校内业务不中断。每次机柜移机割接完成后，需要至少1名高级项目经理及1名现场工程师驻留在学校6小时以上进行业务保障。**

五、售后服务要求

1. 投标人需提供所有设备和系统3年免费质保，自竣工验收合格并签署验收文件后开始计算，在质保期内，投标人应保证所有设备无故障开机运行，如达不到要求，质保期应顺延。
2. 对质保期内的维修服务，质保期内中标供应商须为最终用户提供技术支持服务热线（7\*24 小时），中标人应在接到招标人通知后2小时内赶到现场，无偿负责系统的调试或更换已损坏的零部件；质保期以后的维修服务，中标人应做到在招标人发出维修通知后4小时内赶到现场进行维修，更换已损坏的零部件，要求第二个工作日内修复，否则提供备机。
3. 投标人应在投标文件中声明其售后服务承诺内容、售后服务方式和能力，并提供售后服务人员名单及联系方法。
4. 提供培训，培训内容包括项目所涉及产品（包括软硬件）的基本原理、系统组成、日常操作、日常维护、一般故障处理等内容。培训地点：招标人所在地,时间:不少于3天,人次：5人。
5. 要求提供不少于3名工程师两个月驻场服务。

附件2：

中标标的内容及售后服务承诺

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名 称** | **数量** | **单位** | **所投产品品牌及型号** | **单价** | **小计** |
| 1 | 安全漏洞扫描设备 | 1 | 台 | 迪普 DPtech Scanner1000-GS | ¥135,000.00 | ¥135,000.00 |
| 2 | Web应用防火墙 | 1 | 台 | 绿盟 WEB应用防护系统 V6.0 | ¥280,000.00 | ¥280,000.00 |
| 3 | 安全运维审计设备 | 1 | 台 | 绿盟 安全审计系统 V5.6 | ¥160,000.00 | ¥160,000.00 |
| 4 | 安全动态主机配置协议设备 | 4 | 台 | ZDNS T5100H | ¥155,000.00 | ¥620,000.00 |
| 5 | 安全虚拟专用网络设备 | 1 | 台 | 深信服 VPN-4050-TJ02 | ¥270,000.00 | ¥270,000.00 |
| 6 | 安全域名解析设备 | 6 | 台 | ZDNS T5100H-D | ¥155,000.00 | ¥930,000.00 |
| 7 | 安全运维管理系统 | 1 | 套 | 基线天成 基线网络管理系统 V2.0 | ¥50,000.00 | ¥50,000.00 |
| 8 | 门禁控制器 | 1 | 台 | 宇川 YC-C10 | ¥1,650.00 | ¥1,650.00 |
| 9 | 电磁锁 | 1 | 个 | 莹德佳 JDY280 | ¥400.00 | ¥400.00 |
| 10 | 读卡器 | 1 | 个 | 宇川 YC-M190 | ¥600.00 | ¥600.00 |
| 11 | IC卡 | 10 | 张 | 宇川 YC-C01 | ¥20.00 | ¥200.00 |
| 12 | 出门按钮 | 1 | 个 | 莹德佳 JDY86 | ¥50.00 | ¥50.00 |
| 13 | 监控摄像头 | 6 | 个 | 海康威视 DS-2CD2120XY-I/BC | ¥850.00 | ¥5,100.00 |
| 14 | 硬盘录像机 | 1 | 台 | 海康威视 DS-8608N-E8/BC | ¥15,000.00 | ¥15,000.00 |
| 15 | 无线传输交互系统 | 1 | 套 | 中航奥特 WID515 | ¥3,000.00 | ¥3,000.00 |
| 16 | 线缆辅材 | 1 | 项 | 康邦科技定制 | ¥3,000.00 | ¥3,000.00 |
| 17 | 光跳线 | 20 | 根 | 山泽 GQ-8017 | ¥50.00 | ¥1,000.00 |
| 18 | 千兆多模光模块 | 10 | 个 | 华三 SFP-GE-SX-MM850-A | ¥1,500.00 | ¥15,000.00 |
| 合计 | ¥2,490,000.00 |

**售后服务承诺**

**针对于本项目我公司在此承诺所投产品提供5年的原厂质保服务**

**一、安装调试服务**

1. 我公司将针对该系统成立专门的项目实施小组，在系统实施的各个阶段（系统需求分析、系统设计、系统运行与维护等阶段）为最终用户作好系统实施各个环节的协调及服务支持工作。
2. 我公司将为用户提供现场的技术支持与服务，参与系统的最终调试和优化工作，以保证应用系统以良好的状态运行。
3. 在系统投入正常运行后，为了确保该系统的正常健康运行和及时解决系统运行过程中出现的实际问题，我公司将定期到用户现场进行指导，完成系统进一步调试优化和系统维护工作。
4. **5年内对软硬件设备每季度现场维护一次，学校重大活动提供1名技术人员负责现场服务。**
5. **常规的技术支持和版本升级。项目投入正式运行后，我公司将提供五年的免费技术支持，时间从项目验收结束后开始计算；在质保期内，保证所有设备无故障开机运行，如达不到要求，质保期顺延。我公司提供远程软件调试、诊断服务，同时将采用电话、传真、Internet等灵活、多样的通信手段，提供24小时的响应服务，保证在任何时候用户都能及时找到技术支持小组的工程师，质保期内，技术服务人员2小时到现场解决，无偿负责系统的调试或更换已损坏的零部件。质保期以后的维修服务，中标人应做到在招标人发出维修通知后4小时内赶到现场进行维修，更换已损坏的零部件，要求第二个工作日内修复，否则提供备机。**
6. **现场重大技术问题解决服务。实施结束并投入试运行后，如遇到重大的技术问题，我公司将安排现场维护人员立即着手解决问题，同时公司内部的系统维护支持小组成员将在2小时内赶到用户现场，解决技术问题，确保项目的顺利实施和系统正常健康运行。**

**二、技术支持与服务计划**

1. 根据我公司向最终用户所提供的主机设备、应用软件等的种类及其应用范围，以及最终用户的需求，向最终用户提供全方位的、有效的、及时的技术支持和服务。
2. 我公司负责指导和实施向最终用户所提供的各类软、硬件产品的现场安装、调试及开通。
3. 为了提供快速的服务响应和长期向最终用户提供技术支持，我公司指定有经验的技术人员为最终用户提供服务。试运行期间，若我公司所提供的硬件或软件出现问题时，我公司指定有经验的技术人员在现场免费进行维护。
4. 建立最终用户技术支持档案，定期上门跟踪服务。
5. **我公司对其所提供的软件产品提供五年的免费技术支持和一年的版本更新升级，硬件产品根据生产厂家保修服务条款给予保修。**
6. **本次项目我方提供5人次为期10天的技术培训，包括项目所涉及产品（包括软硬件）的基本原理、系统组成、日常操作、日常维护、一般故障处理等内容，具体情况见培训方案部分。**
7. **本次项目我方提供3名驻场工程师进行为期两个月的驻场服务。**