招 标 文 件

项目编号：2019-026S

项目名称：盐城工业职业技术学院网络安全实验室建设项目

盐城工业职业技术学院

江苏双清工程造价咨询有限公司

2019 年 8 月 9 日

总 目 录

第一章　招标公告（征求意见稿）

根据盐城工业职业技术学院下达的采购计划，江苏双清工程造价咨询有限公司受盐城工业职业技术学院的委托，决定就其所需的盐城工业职业技术学院网络安全实验室建设项目进行公开招标采购，现欢迎符合相关条件的合格供应商投标。

一、招标项目名称及编号

项目名称：盐城工业职业技术学院网络安全实验室建设项目

标书编号：2019-026S

二、招标项目（简要说明）及预算金额

本项目主要内容为盐城工业职业技术学院网络安全实验室建设项目所需的硬件设备、软件研发、采购、安装、调试、培训、验收、维保、售前及售后等伴随服务，详情见招标文件项目需求部分，招标人保留适当变更的权利。

预算价约 1300 万元；投标人的投标报价不得超过预算价。

三、供应商资格要求

（一）符合政府采购法第二十二条第一款规定的条件，并提供下列材料：

1、法人或者其他组织的营业执照等证明文件，自然人的身份证明；

2、上一年度的财务报表（成立不满一年不需提供）；

3、依法缴纳税收和社会保障资金的相关材料；

4、具备履行合同所必需的设备和专业技术能力的书面声明；

5、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；

（二）其他资格条件：

1、未被“信用中国”网站（www.creditchina.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重失信行为记录名单。

（三）本项目不接受联合体投标。

四、招标文件提供信息、意见征集

招标公告发布媒体：“盐城市政府采购网”和“盐城工业职业技术学院招标采购网”

本招标公告发布后凡具备上述资格要求，并自愿参加本项目投标的申请人请在“盐城市政府采购网”、“盐城工业职业技术学院招标采购网”上自行下载招标文件。

各投标人对招标文件有优化建议的请于 2019 年 8 月 20 日 18 时前以书面形式（加盖单位公章）向招标代理机构提出（或将加盖公章的书面材料扫描件发送至 310920981@qq.com 邮箱，联系人：尤鸿望，联系电话：13770089996，地址：盐城市紫薇广场 C 区 7 楼），逾期不再受理。未提供建议的视为认可招标文件所有条款。

注：本次发布的招标公告为征集意见稿，招标人将结合投标人提出的优化建议调整到位后发布正式招标公告，请及时关注“盐城市政府采购网”、“盐城工业职业技术学院招标采购网”发布的招标信息。

五、现场踏勘

时间：2019 年 8 月 9 日至 2019 年 8 月 20 日

地点：盐城工业职业技术学院

联系人：王老师

联系电话：15851766858

六、本次招标联系事项

（一）采购人项目联系人：王老师，联系电话：15851766858 ；

采购人地址：盐城工业职业技术学院；

（二）采购代理机构联系人：尤鸿望， 联系电话：0515-88200316；

采购代理机构联系地址：盐城市紫薇广场 C 区 7 楼。

七、本次招标投标保证金

本次投标收取保证金。本次投标保证金金额为人民币贰拾陆万元整，投标保证金必须在投标文件接收截止时间前与投标文件一起送达投标文件接收地点（不要密封在响应文件中）。

投标保证金必须采用有效银行本票或银行汇票，不接受电汇、转账、现金、现金交款单、支票或其他形式的保证金。各投标人须在投标文件接收截止时间前将投标保证金从投标人本单位的基本账户上汇出（不入账），以投标人汇出资金的银行日期为准，且保证金汇出单位必须与投标人名称一致，收款人名称：江苏双清工程造价咨询有限公司，开户行：中国银行股份有限公司盐城分行，账号：513158208001。投标文件接收截止时间前，各投标人将有效银行本票（或银行汇票）原件和人民银行基本账户开户许可证复印件（或“基本存款账户信息”证明材料）带至开标现场交工作人员核验，未按上述要求交纳投标保证金的，将被视为非响应性投标而予以拒绝。

投标保证金退还方式：未中标人的投标保证金现场退还，中标人的投标保证金在签订合同并交纳招标代理服务费后，凭合同原件及交费凭证至招标代理机构财务部退还。

盐城工业职业技术学院

江苏双清工程造价咨询有限公司

2019 年 8 月 9 日

第二章　投标人须知

一、总则

1、招标方式

1.1 本次招标采取公开招标方式，本招标文件仅适用于招标公告中所述项目。

2、合格的投标人

2.1 满足招标公告中供应商的资格要求的规定。

2.2 满足本文件实质性条款的规定。

3、适用法律

3.1 本次招标及由此产生的合同受中华人民共和国有关的法律法规制约和保护。

4、投标费用

4.1 投标人应自行承担所有与参加投标有关的费用，无论投标过程中的做法和结果如何，采购人及采购代理机构在任何情况下均无义务和责任承担这些费用。

4.2 本项目中标人与采购人签订合同前，须向采购代理机构支付招标代理服务费，收费标准按中标价的 1.5%×42%计取（如低于 3000 元的直接按 3000 计取）；上述费用由各投标人在投标时自行综合考虑分摊含进投标报价中，且不得单列，采购人不再承担上述费用。

5、招标文件的约束力

5.1 投标人一旦参加本项目采购活动，即被认为接受了本招标文件的规定和约束，并且视为自招标公告期限届满之日起知道或应当知道自身权益是否受到了损害。

6、招标文件的解释

6.1 本招标文件由采购人或采购代理机构负责解释。

二、招标文件

7、招标文件构成

7.1 招标文件有以下部分组成：

（1）招标公告

（2）投标人须知

（3）合同条款及格式

（4）项目需求

（5）评标方法与评标标准

（6）投标文件格式

请仔细检查招标文件是否齐全，如有缺漏请立即与采购人或采购代理机构联系解决。

7.2 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。按招标文件要求和规定编制投标文件，并保证所提供的全部资料的真实性，以使其投标文件对招标文件作出实质性响应，否则其风险由投标人自行承担。

8、招标文件的询问

8.1 任何要求对招标文件进行询问的投标人，应在投标截止日期**十日**前按招标公告中的通讯地址，向采购代理机构或采购人提出。

9、招标文件的修改

9.1 在投标截止时间三天前，采购人可以对招标文件进行修改。

9.2 采购人有权依法推迟投标截止日期和开标日期。

9.3 招标文件的修改将在“盐城市政府采购网”和“盐城工业职业技术学院招标采购网”公布，补充文件将作为招标文件的组成部分，并对投标人具有约束力。

三、投标文件的编制

10、投标文件的语言及度量衡单位

10.1 投标人提交的投标文件以及投标人与采购人或采购代理机构就有关投标的所有来往通知、函件和文件均应使用**简体中文**。

10.2 除技术性能另有规定外，投标文件所使用的度量衡单位，均须采用国家法定计量单位。

11、投标文件构成

11.1 投标人编写的投标文件应包括资信证明文件、投标配置与分项报价表、供货一览表、技术参数响应及偏离表、商务条款响应及偏离表、技术及售后服务承诺书、投标函、开标一览表等部分；

11.2 投标人应将投标文件按顺序装订成册，并编制投标文件资料目录。

12、证明投标人资格及符合招标文件规定的文件

12.1 投标人应按要求提交资格证明文件及符合招标文件规定的文件。

12.2 投标人应提交证明其有资格参加投标和中标后有能力独立履行合同的文件。

12.3 投标人除必须具有履行合同所需提供的货物以及服务的能力外，还必须具备相应的财务、技术方面的能力。

12.4 投标人应提交根据合同要求提供的证明产品质量合格以及符合招标文件规定的证明文件。

12.5 证明投标人所提供货物与招标文件的要求相一致的文件可以是手册、图纸、文字资料和数据。

13、供货一览表和投标配置与分项报价表

13.1 投标人应按照招标文件规定格式填报供货一览表、投标配置与分项报价表，在表中标明所提供的设备品牌、规格、型号、原产地、主要部件型号及其功能的中文说明和供货期。每项货物和服务等只允许有一个报价，任何有选择的报价将不予接受(如有备选配件，备选配件的报价不属于选择的报价)。

13.2 标的物

采购人需求的货物供应、安装，调试及有关技术服务等。

13.3 有关费用处理

招标报价采用总承包方式，投标人的报价应包括所投产品费用、安装调试费、测试验收费、培训费、运行维护费用、税金、国际国内运输保险、报关清关、开证、办理全套免税手续费用及其他有关的为完成本项目发生的所有费用，招标文件中另有规定的除外。

13.4 其它费用处理

招标文件未列明，而投标人认为必需的费用也需列入报价。

13.5 投标货币

投标文件中的货物单价和总价无特殊规定的采用人民币报价，以元为单位标注。招标文件中另有规定的按规定执行。

13.6 投标配置与分项报价表上的价格应按下列方式分开填写：

13.6.1 项目总价：包括买方需求的货物价格、质量保证费用、培训费用及售后服务费用，项目在指定地点、环境交付、安装、调试、验收所需费用和所有相关税金费用及为完成整个项目所产生的其它所有费用。

13.6.2 项目单价按投标配置及分项报价表中要求填报。

14、技术参数响应及偏离表、商务条款响应及偏离表及投标货物说明

14.1 对招标文件中的技术与商务条款要求逐项作出响应或偏离，并说明原因；

14.2 提供参加本项目类似案例简介；

14.3 培训计划；

14.4 详细阐述所投货物的主要组成部分、功能设计、实现思路及关键技术；

14.5 投标人认为需要的其他技术文件或说明。

15、服务承诺及售后服务机构、人员的情况介绍

15、1投标人的服务承诺应按不低于招标文件中商务要求的标准。

15、2 提供投标人有关售后服务的管理制度、售后服务机构的分布情况、售后服务人员的数量、素质、技术水平及售后服务的反应能力。

16、投标函和开标一览表

16.1 投标人应按照招标文件中提供的格式完整、正确填写投标函、开标一览表。

16.2 开标一览表中的价格应与投标文件中投标配置与分项报价表中的价格一致，如不一致，不作为无效投标处理，但评标时按开标一览表中价格为准。

17、投标保证金

17.1 投标人提交的投标保证金必须在投标截止时间前送达，并作为其投标的组成部分。

17.2 在开标时，对于未按要求提交投标保证金的投标无效，采购人或采购代理机构拒绝接收其投标文件。

17.3 投标人在投标截止时间前撤回已提交的投标文件的，采购人或者采购代理机构应当自收到投标人书面撤回通知之日起 5 个工作日内，退还已收取的投标保证金，但因投标人自身原因导致无法及时退还的除外。

未中标的投标人的投标保证金，将在中标通知书发出之日起 5 个工作内退还，不计利息。

17.4 签订合同时，中标人须向采购人交纳履约保证金，于合同履行后无息退还。

17.5 下列任何情况发生时，投标保证金将不予退还：

（1）投标人在投标有效期内撤回其投标；

（2）投标人提供的有关资料、资格证明文件被确认是不真实的；

（3） 投标人之间被证实有串通（统一哄抬价格）、欺诈行为；

（4） 投标人被证明有妨碍其他人公平竞争、损害采购人或采购代理机构或者其他投标人合法权益的；

18、投标有效期

18.1 投标有效期为规定的开标之日后六十（60）天。投标有效期比规定短的将被视为非响应性投标而予以拒绝。

18.2 在特殊情况下，采购人于原投标有效期满之前，可向投标人提出延长投标有效期的要求。这种要求与答复均应采用书面形式。投标人可以拒绝采购人的这一要求而放弃投标，采购人或采购代理机构在接到投标人书面答复后，将在原投标有效期满后五日内**无息退还其投标保证金**。同意延长投标有效期的投标人既不能要求也不允许

修改其投标文件。第 16 条有关投标保证金的规定在延长期内继续有效，同时受投标有效期约束的所有权利与义务均延长至新的有效期。

19、投标文件份数和签署

19.1 投标人应严格按照招标公告和招标文件要求的份数准备投标文件，每份投标文件须清楚地标明“正本”或“副本”字样。一旦正本和副本不符，以正本为准。

19.2 投标文件正本中，招标文件要求必须提供原件的按照要求提供，文字材料需打印或用不褪色墨水书写。投标文件的正本须经法定代表人或授权委托人（被授权人）签署和加盖投标人公章。 本采购文件所表述（指定）的公章是指法定名称章，不包括合同专用章、业务专用章等印章。

19.3 除投标人对错处做必要修改外，投标文件不得行间插字、涂改或增删。如有修改错漏处，必须由投标文件签署人签字或盖章。

四、投标文件的递交

20、投标文件的密封和标记

20.1 投标人应将投标文件正本和所有副本密封，不论投标人中标与否，投标文件均不退回。

20.2 密封的投标文件应：

20.2.1 注明投标人名称，如因标注不清而产生的后果由投标人自负。按招标公告中注明的地址送达；

20.2.2 注明投标项目名称、标书编号及包号。

20.2.3 未按要求密封和加写标记，采购人或采购代理机构对误投或过早启封概不负责。对由此造成提前开封的投标文件，采购人或采购代理机构将予以拒绝，作无效投标处理。

21、投标截止日期

21.1 采购人或采购代理机构收到投标文件的时间不得迟于招标公告中规定的截止时间。

21.2 采购人有权通过修改招标文件酌情延长投标截止日期，在此情况下，投标人的所有权利和义务以及投标人受制的截止日期均应以延长后新的截止日期为准。

22、迟交的投标文件

22.1 采购人或采购代理机构拒绝接收在其规定的投标截止时间后递交的任何投标文件。

23、投标文件的修改和撤回

23.1 投标人在递交投标文件后，可以修改或撤回其投标文件，但这种修改和撤回，必须在规定的投标截止时间前，以书面形式通知采购人，修改或撤回其投标文件。

23.2 投标人的修改或撤回文件应按规定进行编制、密封、标记和发送，并应在封套上加注“修改”或“撤回”字样。上述补充或修改若涉及投标报价，必须注明“最后唯一报价”字样，否则将视为有选择的报价。修改文件必须在投标截止时间前送达采购人或采购代理机构。

23.3 在投标截止时间之后，投标人不得对其投标文件作任何修改。

23.4 在投标截止时间至招标文件中规定的投标有效期满之间的这段时间内，投标人不得撤回其投标，否则其投标保证金将不予退还。

五、开标与评标

24、开标

24.1 采购人或采购代理机构将在招标公告中规定的时间和地点组织公开开标。投标人应委派携带有效证件的代表准时参加，参加开标的代表需签名以证明其出席。

24.2 开标仪式由采购人组织，采购人代表、公证员（必要时）、监管代表、投标人代表等参加。

24.3 按照规定同意撤回的投标将不予开封。

24.4 开标时请监委或投标人代表查验投标文件密封情况，确认无误后，采购代理机构当众拆封宣读每份投标文件中“开标一览表”的内容，未列入开标一览表的内容一律不在开标时宣读。开标时未宣读的投标报价信息，不得在评标时采用。

24.5 采购人将指定专人负责开标记录并存档备查，各投标人需仔细核对开标记录相关内容并签字确认。

24.6 投标人在报价时不允许采用选择性报价，否则将被视为无效投标。

25、资格审查

25.1 依据法律法规和招标文件的规定，开标结束后，由采购人对投标文件中的资格证明文件进行审查。资格审查的结论，采购人以书面形式向评委会进行反馈。未通过资格审查的投标人，由采购人告知未通过资格审查的原因。

采购人在进行资格性审查的同时，将在“信用中国”网站（www.creditchina.gov.cn）对投标人是否被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重失信行为记录名单情况进行查询，以确定投标人是否具备投标资格。查询结果将以网页打印的形式留存并归档。

接受联合体的项目，两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，联合体成员存在不良信用记录的，视同联合体存在不良应用记录。

合格投标人不足 3 家的，不得评标。

26、评标委员会

26.1 资格审查通过后，采购人将组织评标委员会（以下简称评委会）进行评标。

26.2 评委会由采购人代表和有关技术、经济等方面的专家组成，且人员构成符合政府采购有关规定。

26.3 评委会独立工作，负责评审所有投标文件并确定中标侯选人。

27、评标过程的保密与公正

27.1 公开开标后，直至签订合同之日止，凡是与审查、澄清、评价和比较投标的有关资料以及授标建议等，采购人、评委均不得向投标人或与评标无关的其他人员透露。

27.2 在评标过程中，投标人不得以任何行为影响评标过程，否则其投标文件将被作为无效投标文件。

27.3 在评标期间，采购人将设专门人员与投标人联系。

27.4 采购人和评标委员会不向落标的投标人解释未中标原因，也不公布评标过程中的相关细节。

27.5 采用综合评分法的项目，未中标的投标人如需了解自己的评审得分及排序情况，可向采购人提出申请。

28、投标的澄清

28.1 评标期间，为有助于对投标文件的审查、评价和比较，评委会有权以书面形式要求投标人对其投标文件进行澄清，但并非对每个投标人都作澄清要求。

28.2 接到评委会澄清要求的投标人应派人按评委会通知的时间和地点做出书面澄清，书面澄清的内容须由投标人法人或授权代表签署，并作为投标文件的补充部分，但投标的价格和实质性的内容不得做任何更改。

28.3 接到评委会澄清要求的投标人如未按规定做出澄清，其风险由投标人自行承担。

29、对投标文件的评审

29.1 符合性检查：依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求作出响应。

29.2 在详细评标之前，评委会将首先审查每份投标文件是否实质性响应了招标文件的要求。实质性响应的投标应该是与招标文件要求的全部条款、条件和规格相符，没有重大偏离或保留的投标。

所谓重大偏离或保留是指与招标文件规定的实质性要求存在负偏离，或者在实质上与招标文件不一致，而且限制了合同中买方和见证方的权利或投标人的义务，纠正这些偏离或保留将会对其他实质性响应要求的投标人的竞争地位产生不公正的影响。是否属于重大偏离由评委会按照少数服从多数的原则作出结论。认定评委决定投标文件的响应性只根据投标文件本身的内容，而不寻求外部的证据。

29.3 如果投标文件实质上没有响应招标文件的要求，评委会将按无效投标处理，投标人不得通过修改或撤销不合要求的偏离或保留而使其投标成为实质性响应的投标。

29.4 评委会将对确定为实质性响应的投标进行进一步审核，看其是否有计算上或累加上的算术错误，修正错误的原则如下：

（1）投标文件中开标一览表内容与投标文件中相应内容不一致的，以开标一览表为准。

（2）大写金额和小写金额不一致的，以大写金额为准。

（3）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价。

（4）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上错误的，按照前款规定的顺序修正。

29.5 评委会将按上述修正错误的方法调整投标文件中的投标报价，调整后的价格应对投标人具有约束力。如果投标人不接受修正后的价格，则其投标将被拒绝，其投标保证金不予退还。

29.6 评委会将允许修正投标文件中不构成重大偏离的、微小的、非正规的、不一致的或不规则的地方，但这些修改不能影响任何投标人相应的名次排列。

29.7 提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

非单一产品采购项目，采购人根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前两款

规定处理。(87 号令第 31 条)

30、无效投标条款和废标条款

30.1 无效投标条款

30.1.1 未按要求交纳投标保证金的；

30.1.2 未按照招标文件规定要求密封、签署、盖章的；

30.1.3 投标人在报价时采用选择性报价；

30.1.4 投标人不具备招标文件中规定资格要求的；

30.1.5 投标人的报价超过了采购预算或最高限价的；

30.1.6 未通过符合性检查的；

30.1.7 不符合招标文件中规定的其他实质性要求和条件的；

30.1.8 投标人串通投标；

30.1.9 投标文件含有采购人不能接受的附加条件的。

30.1.10 评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

30.1.11 其他法律、法规及本招标文件规定的属无效投标的情形。

30.2 废标条款：

30.2.1 符合专业条件的供应商或者对招标文件作实质响应的供应商不足三家的；

30.2.2 出现影响采购公正的违法、违规行为的；

30.2.3 因重大变故，采购任务取消的；

30.2.4 评标委员会认定招标文件存在歧义、 重大缺陷导致评审工作无法进行。

30.3 投标截止时间结束后参加投标的供应商不足三家的处理：

30.3.1 如出现投标截止时间结束后参加投标的供应商或者在评标期间对招标文件做出实质响应的供应商不足三家情况，按财政部第八十七号令第四十三条的规定执行。

六、定标

31、确定中标单位

31.1 评委会根据本招标文件规定评标方法与评标标准向采购人推荐出中标候选人。

31.2 采购人应根据评委会推荐的中标候选人确定中标供应商。

31.3 采购人将在“盐城市政府采购网”和“盐城工业职业技术学院招标采购网”发布中标公告，公告期限为 1 个工作日。

31.4 若有充分证据证明，中标供应商出现下列情况之一的，一经查实，将被取消中标资格：

31.4.1 提供虚假材料谋取中标的；

31.4.2 向采购人行贿或者提供其他不正当利益的；

31.4.3 恶意竞争，投标总报价明显低于其自身合理成本且又无法提供证明的；

31.4.4 属于本文件规定的无效条件，但在评标过程中又未被评委会发现的；

31.4.5 与采购人或者其他供应商恶意串通的；

31.4.6 采取不正当手段诋毁、排挤其他供应商的；

31.4.7 不符合法律、法规的规定的。

31.5 有下列情形之一的，视为投标人串通投标，投标无效：

31.5.1 不同投标人的投标文件由同一单位或者个人编制。

31.5.2 不同投标人委托同一单位或者个人办理投标事宜。

31.5.3 不同投标人的投标文件载明的项目管理成员或者联系人员为同一人。

31.5.4 不同投标人的投标文件异常一致或者投标报价呈规律性差异。

31.5.5 不同投标人的投标文件相互混装。

31.5.6 不同投标人的投标保证金从同一单位或者个人的账户转出。

32、质疑处理

32.1 参加投标人认为招标文件、采购过程和中标结果使自己的权益受到损害的，可以在知道或应知其权益受到损害之日起七个工作日内，以书面形式向采购人或采购代理机构提出质疑。上述应知其权益受到损害之日，是指：

32.1.1 对可以质疑的招标文件提出质疑的，为收到招标文件之日或者招标文件公告期限届满之日；

32.1.2 对采购过程提出质疑的，为各采购程序环节结束之日；

32.1.3 对中标结果提出质疑的，为中标结果公告期限届满之日。

32.2 质疑必须按《政府采购法》、《政府采购法实施条例》及《江苏省政府采购供应商监督管理暂行办法》的相关规定提交，未按上述要求提交的质疑函（含传真、电子邮件等）采购人或采购代理机构有权不予受理。

32.3 未参加投标活动的供应商或在投标活动中自身权益未受到损害的供应商所提出的质疑不予受理。

32.4 质疑函应当包括下列内容：

32.4.1 质疑投标人的名称、地址、邮编、联系人、联系电话；

32.4.2 具体的质疑事项及明确的请求；

32.4.3 认为自己合法权益受到损害或可能受到损害的相关证据材料；

32.4.4 提起质疑的日期；

32.4.5 质疑函应当署名：质疑人为自然人的，应当由本人签字并附有效身份证明；质疑人为法人或其他组织的，应当由法定代表人签字并加盖单位公章。（质疑人为联合体的，则联合体各方法定代表人均须签字并加盖单位公章），未按要求签字和盖章的为无效质疑，采购人或采购代理机构将不予受理)。质疑人委托代理质疑的，应当向采购人或采购代理机构提交授权委托书，并载明委托代理的具体权限和事项。

32.5 采购人或采购代理机构收到质疑函后，将对质疑的形式和内容进行审查，如质疑函内容、格式不符合规定，采购人或采购代理机构将告知质疑人进行补正。

32.6 质疑人应当在法定质疑期限内进行补正并重新提交质疑函，拒不补正或者在法定期限内未重新提交质疑函的，为无效质疑，采购人或采购代理机构有权不予受理。

32.7 对于内容、格式符合规定的质疑函，采购人应当在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复的内容不得涉及商业秘密。

32.8 投标人提出书面质疑必须有理、有据，不得恶意质疑或提交虚假质疑。否则，一经查实，采购人有权依据政府采购的有关规定，报请政府采购监管部门对该投标人进行相应的行政处罚，并扣减其诚信记录分。

33、中标通知书

33.1 中标结果确定后，采购人将向中标供应商发出中标通知书。

33.2 中标通知书将是合同的一个组成部分。对采购人和中标供应商均具有法律效力。中标通知书发出后，采购人改变中标结果的，或者中标供应商放弃中标项目的，应当依法承担法律责任。

七、合同签订相关事项

34. 签订合同

34.1 中标供应商应按中标通知书规定的时间、地点，按照招标文件确定的事项与采购人签订政府采购合同，且不得迟于中标通知书发出之日起三十日内，否则投标保证金将不予退还，由此给采购人造成损失的，中标供应商还应承担赔偿责任。

34.2 招标文件、中标供应商的投标文件及招标过程中有关澄清、承诺文件均应作为合同附件。

34.3 签订合同后，中标供应商不得将货物及其他相关服务进行转包。未经采购人

同意，中标供应商也不得采用分包的形式履行合同，否则采购人有权终止合同，中标供应商的履约保证金将不予退还。转包或分包造成采购人损失的，中标供应商应承担相应赔偿责任。

35、货物和服务的追加、减少和添购。

35.1 政府采购合同履行中，采购人需追加与合同标的相同的货物和服务的，在不改变合同其他条款的前提下，可以与中标供应商协商签订补充合同，但所有补充合同的采购金额不超过原合同金额 10%。

35.2 采购结束后，采购人若由于各种客观原因，必须对采购项目所牵涉的货物和服务进行适当的减少时，在双方协商一致的前提下，可以按照招标采购时的价格水平做相应的调减，并据此签订补充合同。

36、履约保证金

在签订合同时，须向采购人交纳履约保证金，于合同履行后无息退还。履约保证金用以约束成交供应商在合同履行中的行为，弥补合同执行中由于自身行为可能给采购人带来的各种损失。

第三章　合同条款及格式

以下为中标后签定本项目合同的通用条款，中标供应商不得提出实质性的修改，关于专用条款将由采购人与中标供应商结合本项目具体情况协商后签订。

政府采购合同

项目名称：盐城工业职业技术学院网络安全实验室建设项目

项目编号：2019-026S

甲方：盐城工业职业技术学院

乙方：

甲、乙双方根据盐城工业职业技术学院网络安全实验室建设项目公开招标的结果，签署本合同。

一、项目内容

1.1 项目名称：盐城工业职业技术学院网络安全实验室建设项目。

1.2 型号规格及数量等内容：详按项目需求。

二、合同金额

2.1 本合同金额为（大写）：_____元（_____元）人民币或其他币种。

2.2 合同金额为完成本项目所需的硬件设备、软件研发、安装、调试和培训费用等交付使用前的全部费用，包括但不限于所有研发成本、制造采购成本、附件、配件、备品备件及专用工具费、运输费、保险费、培训费、安装、调试、技术研发费用、验收费用、维保费、其他费用（如包装费、仓储费、保管费、资料费、使用耗材等以及完成本项目所需要的其他费用）、管理费、利润、风险费用、规费、招标代理费、国家对乙方征收的各种税费等涉及到的所有费用。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供使用货物和服务的有关技术资料。

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、接受本合同货物和服务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 乙方保证所交付的货物和服务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

6.1 乙方交纳人民币_____元作为本合同的履约保证金（合同金额的 5%）。

七、转包或分包

7.1 本合同范围的货物和服务，应由乙方直接供应，不得转让他人供应；

7.2 除非得到甲方的书面同意，乙方不得部分分包给他人供应。

7.3 如有转让和未经甲方同意的分包行为，甲方有权给予终止合同。

八、质保期

8.1 质保期不少于三年，具体按投标承诺执行。（自交货验收合格之日起计）

九、交货期、交货方式及交货地点

9.1 交货期：合同签订后 60 日历天内完成招标范围内的供货、安装、调试；试运行正常半年后验收。

9.2 交货方式：送货上门

9.3 交货地点：盐城工业职业技术学院校内甲方指定地点

验收：由甲方组织相关部门根据技术要求和相关规范验收。

十、货款支付

10.1 付款方式：项目整体安装、调试、培训结束后进行初验，初验合格后付总价的 50%；试运行半年后进行项目整体验收，验收合格后付总价的 20%；合同签订两年后根据配套服务完成与售后服务情况付总价的 20%;合同签订三年后根据配套服务完成与售后服务情况付总价的 10%。

10.2 乙方向甲方出具的货物税务发票必须是正式合法的，且应保证本项目的软件和硬件系统在甲方使用时不受第三方的指控。

十一、税费

11.1 本合同执行中相关的一切税费均由乙方负担。

十二、质量保证及售后服务

12.1 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品和服务。

12.2 乙方提供的货物和服务在质量期内因本身的质量问题发生故障，乙方应负责

免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴ 更换：由乙方承担所发生的全部费用。

⑵ 贬值处理：由甲乙双方合议定价。

⑶ 退货处理：乙方应退还甲方支付的合同款，同时应承担该货物和服务的直接费用（运输、保险、检验、货款利息及银行手续费等）。

12.3 在质保期内，乙方应对货物和服务出现的质量及安全问题负责处理解决并承担一切费用，并在接到报修通知后 2 小时内响应，4 小时内到达现场（含节假日），24 小时内解决故障，24 小时内不能解决问题应提供备用方案。

12.4 乙方须向甲方免费提供培训服务，确保使用者完全会使用及操作为止。

12.5 质保期内，乙方免费提供系统升级服务。

12.6 乙方提供的设备或产品必须是原装全新、符合招标文件规定技术参数、具有中国有关部门注册或检验或商检及生产厂家质量合格证明的设备和产品。

12.7 乙方提供设备的现场安装调试并达到投标书指标要求的技术性能，并同时在现场对用户进行操作培训。

12.8 设备在调试通过后提供保修服务，整机质保期从验收合格之日起计；在保修期内，所有服务及配件全部免费。保修期外，提供售后服务。

12.9 培训：安装调试合格后，由乙方工程师为甲方操作人员做现场基本操作培训；保证实验人员能够对该实验设备全面地了解，增强使用和维护设备的技能，销售方除了向用户补充完善整个设备的技术说明、操作说明和相关的文档之外，还应负责组织对现场设备使用人员进行全面高质量的培训。培训的目的：使管理和使用设备的人员不仅对设备有足够的认识，而且能完全胜任所承担的工作，确保设备安全可靠地运行并测试获得理想数据。具体详按乙方投标承诺执行。

12.10 乙方提供免费电话，为用户提供免费的电话咨询及技术服务。

12.11 乙方所提供的货物开箱后，发现有任何问题（包括外观损伤），必须以使用方能接受的方式加以解决。

十三、调试和验收

13.1 甲方对乙方提交的货物和服务依据招标文件上的技术规格要求和国家有关质量标准进行现场初步验收，外观、说明书符合招标文件技术要求的，给予签收，初步验收不合格的不予签收。交付后，甲方需在五个工作日内验收。

13.2 乙方交付前应对产品作出全面检查和对验收文件进行整理，并列出清单，作为甲方验收和使用的技术条件依据，检验的结果应一并交甲方。

13.3 甲方对乙方提供的货物和服务在使用前进行调试时，乙方需负责安装并培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验收。

13.4 对技术复杂的货物和服务，甲方可请国家认可的专业检测机构参与初步验收及最终验收，并由其出具质量检测报告。

13.5 验收时乙方必须在现场，验收完毕后作出验收结果报告；验收费用由甲乙双方协商解决。

13.6 甲方根据国家有关规定、采购文件、乙方的响应文件以及合同约定的内容和验收标准进行验收。验收情况作为支付货款的依据。如有质疑，以相关质量技术检验检测机构的检验结果为准，如产生检验费用，则该费用由过失方承担。

要求乙方对设备及各类相关文档进行确认和验收，以保障系统达到验收标准。验收内容包括：

(1)对设备的详细数量进行到货签收确认；

(2)对设备安装、调试，运行报告进行确认；

(3)对项目交付文档进行移交和确认；

以上确认无误后，乙方应和甲方共同确认设备运行符合技术规范后，完成软件测试验收，并签署验收报告。

十四、货物包装、发运及运输

14.1 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

14.2 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

14.3 乙方在货物发运手续办理完毕后 24 小时内或货到甲方 48 小时前通知甲方，以准备接货。

14.4 货物和服务在交付甲方前发生的风险均由乙方负责。

14.5 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需通知甲方货物已送达。

十五、违约责任

15.1 甲方无正当理由拒收货物和服务的，甲方向乙方偿付拒收货款总值的百分之五违约金。

15.2 甲方无故逾期验收和办理合同款支付手续的，甲方应按逾期付款总额每日万分之五向乙方支付违约金。

15.3 乙方逾期交付货物和服务的，乙方应按逾期交货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中扣除。逾期超过约定日期 10 个工作日不能交货的，甲方可解除本合同。乙方因逾期交货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总值 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。

15.4 乙方所交的货物和服务品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准的，甲方有权拒收该货物和服务，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物和服务的，甲方可单方面解除合同。

十六、不可抗力事件处理

16.1 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。

16.2 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。

16.3 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。

十七、诉讼

17.1 双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向合同签订地法院起诉，合同签订地在此约定为盐城市。

十八、合同生效及其它

18.1 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。

18.2 本合同未尽事宜，遵照《合同法》有关条文执行。

18.3 本合同正本一式二份，副本一式六份，具有同等法律效力。

甲方：	乙方：
地址：	地址：
法定代表人或授权代表：	法定代表人或授权代表：
采购单位负责人：	
联系电话：	联系电话：

签订日期：　　年　月　日

第四章 项目需求

一、项目概况

（一）项目背景

当前，网络安全形势日益严峻，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临风险与挑战。习近平总书记指出：“没有网络安全就没有国家安全”。“培养网信人才，要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院。”

据相关调研报告显示，我国网络安全人才总需求量超过 70 万人，相关行业每年还以 1.5 万人的速度递增，预计 2020 年相关人才需求将增长到 140 万，但我国高等教育近年培养的信息安全专业人才仅 3 万余人，网络安全人才需求缺口巨大。

2016 年 6 月中央网信办、国家发改委、教育部等联合印发《关于加强网络安全学科建设和人才培养的意见（中网办发文〔2016〕4 号）》，提出“加强网络安全学院学科建设和人才培养”8 条意见。网络安全人才培养已被列为国家发展大战略。2019 年，国家相继出台了《国家职业教育改革实施方案》（“职教二十条”）、《建设产教融合型企业实施办法(试行)》等文件，为破解长期制约我国职业教育体制机制发展的难题指明了方向。

为策应国家网络强国战略，培养紧缺型网络安全技术技能人才，实现学校转型升级发展。盐城工业职业技术学院决定通过公开招标方式选择国内知名网络安全厂商参与学校的网络安全产业学院建设。

（二）项目总体要求

1、本项目招标是以产教融合为目的，与中标供应商共建网络安全学院。投标人应为国内知名网络安全行业从业企业，并以书面授权的方式授予校方挂牌“企业品牌+网络安全学院”，期限不少于 5 年。

2、投标人除按招标采购清单要求完成实验实训等环境建设外，应能与校方建立产教融合合作关系，在后续的合作中参与人才培养方案、专业与课程设置等方案的制定，共同进行精品在线开放课程开发、课程资源库建设、教学方案制定、物理场景定向授课、演练题库更新等一系列的教学资源建设服务内容。

3、本次招标建设的实验实训等环境，应能支持不少于 5 个信息（网络）安全方面的专业开设，以满足网络空间安全专业群建设需求。

4、本项目共建设一个数据中心、四个实验室（满足 200 个学生同时实验需要）与一个科普基地。供应商应根据招标文件载明的现场踏勘联系方式联系索取平面图并进行现场踏勘，设计与项目相适应的室内装潢效果图与施工图。

二、采购清单

序号	名目	设备名称	数量	单位	备注
1	实验室数据中心	实验实训系统主控服务器	3	台	
2		实验实训系统从属支撑服务器	6	台	
3		攻防演练系统支撑服务器	4	台	
4		云计算实验室控制节点服务器	1	台	
5		云计算实验室云计算节点服务器	5	台	
6		网络安全职业技能认证考试系统支撑服务器	2	台	
7		态势感知大数据安全支撑服务器	1	台	
8		流量探针服务器	4	台	
9		态势感知资产探测支撑服务器	1	台	
10		服务器机柜	5	台	
11		电气系统分项工程	1	套	
12		接地系统分项工程	1	套	
13		UPS 系统分项工程	1	套	
14		环境监控系统	1	套	
15		路由器	1	台	
16		中心交换机	1	台	
17		接入交换机	1	台	
18	网络安全综合实验室	云实验管理系统	1	套	
19		教学管理系统	1	套	
20		学情管理系统	1	套	
21		题库管理系统	1	套	
22		项目实训管理系统	1	套	
23		虚拟仿真系统	1	套	
24		虚实结合管理系统	1	套	
25		安全攻防演练系统	1	套	
26		防火墙安全实训设备	4	台	
27		入侵防御安全实训设备	1	台	
28		入侵检测实训设备	1	台	
29		网站防火墙实训设备	1	台	
30		VPN 实训设备	1	台	
31		日志审计实训设备	1	台	
32		漏洞扫描设备实训设备	1	台	
33		网络机柜	2	台	
34		接入交换机	4	台	
35		可视化大屏	2	台	
36	网络安全职业认证考试平台	认证考试平台	1	套	
37	云计算安全实验室	云基础架构平台软件	1	套	
38		实训系统	1	套	
39		网络机柜	1	台	
40		接入交换机	2	台	
41	网络安全态势感知实验室	入侵检测模块	1	套	
42		事件还原模块	1	套	
43		行为预判模块	1	套	

44		可视化分析模块	1	套	
45		脱敏数据	1	套	
46		可视化大屏	2	台	
47		资产测绘模块	1	套	
48		漏洞感知模块	1	套	
49		可视分析模块	1	套	
50		漏洞插件库	1	套	
51		资产探测平台脱敏数据	1	套	
52		网络机柜	1	台	
53		接入交换机	2	台	
54	网络安全科普基地	政策法规功能区	1	套	
55		网络攻击体验区	1	套	
56		安全案例功能区	1	套	
57		交互体验功能区	1	套	
58		辅助设备与服务	1	套	
59	网络安全综合教学实验实训课程资源	《网络安全导论》课程资源包	1	套	
60		《信息安全技术》课程资源包	1	套	
61		《操作系统安全》课程资源包	1	套	
62		《网络协议安全》课程资源包	1	套	
63		《网络攻防原理与实践》课程资源包	1	套	
64		《Web 安全原理与实践》课程资源包	1	套	
65		《网络渗透测试实践》课程资源包	1	套	
66		《网络安全等级保护》课程资源包	1	套	
67		《代码审计与实践》课程资源包	1	套	
68		《信息安全管理》课程资源包	1	套	
69		《企业安全体系与实践》课程资源包	1	套	
70	云计算教学实验实训课程资源	《云计算导论》课程资源包	1	套	
71		《KVM 虚拟化技术基础与实践》课程资源包	1	套	
72		《云平台技术应用与开发》课程资源包	1	套	
73		《云计算综合实训》课程资源包	1	套	
74		《云计算与云安全》课程资源包	1	套	
75	配套服务	品牌使用授权	1	套	
76		升级、维护	1	套	
77		定制专业人才培养方案	1	套	
78		招生推广服务	1	套	
79		师资培训服务	1	套	
80		专业教学服务	1	套	
81		大学生竞赛服务	1	套	
82		企业职业认证考试与社会培训	1	套	
83		课程资源库开发服务	1	套	
84		就业服务	1	套	
85		教学管理支撑服务	1	套	
86		室内装潢设计	1	套	中标后提供全套设计图纸

四、技术规格、参数及服务要求

4.1 实验室数据中心

序号	项目名称	招标要求的技术指标	数量	单位
1	实验实训系统主控服务器	规格：2U 机架式，配导轨套件； CPU：配置≥2 颗 Intel E5-2630v4 十核处理器（主频 2.2GHz）； 内存：配置≥32GB*4 DDR4 REEC，基于后期扩展，最大支持≥8 根内存插槽； 硬盘：配置≥600GB*2 SAS 10K RPM 12Gb/s ，至少配置 480GB SSD 6Gb/s，至少配置 3 块 8T SATA(3.5 英寸硬盘满配盘托)； RAID：1GB 缓存 12Gb/S RAID 控制器，支持 RAID0,1,5,6,10,50,60，带超级电容； 网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能； 电源：至少配置白金效率 500W 交流电源； 管理：支持 IPMI 2.0 标准，配置 KVM over IP（允许从任何地点通过网络访问、安装、配置和控制远端服务器）及虚拟媒体功能，提供 1 个管理专用的 1000Mb 以太网口（RJ45 接口）。 系统：CentOS(定制版)。	3	台
2	实验实训系统从属支撑服务器	规格：2U 机架式，配导轨套件； CPU：配置≥2 颗 Intel E5-2630v4 十核处理器（主频 2.2GHz）； 内存：配置≥32GB*8 DDR4 REEC，基于后期扩展，最大支持≥8 根内存插槽； 硬盘：配置≥600GB*2 SAS 10K RPM 12Gb/s ，至少配置 480GB SSD 6Gb/s； RAID：1GB 缓存 12Gb/S RAID 控制器，支持 RAID0,1,5,6,10,50,60，带超级电容； 网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能； 电源：至少配置白金效率 500W 交流电源； 管理：支持 IPMI 2.0 标准，配置 KVM over IP（允许从任何地点通过网络访问、安装、配置和控制远端服务器）及虚拟媒体功能，提供 1 个管理专用的 1000Mb 以太网口（RJ45 接口）。 系统：CentOS(定制版)。	6	台
3	攻防演练系统支撑服务器	规格：2U 机架式，配导轨套件； CPU：配置≥2 颗 Intel E5-2630v4 十核处理器（主频 2.2GHz）； 内存：配置≥32GB*4 DDR4 REEC，基于后期扩展，最大支持≥8 根内存插槽； 硬盘:配置≥600GB*2 SAS 10K RPM 12Gb/s 至少配置 1T HDD 硬盘,至少配置 1T*2 PCIe 硬盘 ； RAID：1GB 缓存 12Gb/S RAID 控制器，支持 RAID0,1,5,6,10,50,60，带超级电容； 网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能； 电源：至少配置白金效率 500W 交流电源。	4	台
4	云计算实验室控制节点服务器	规格：2U 机架式，配导轨套件； CPU：配置≥1 颗 Intel E5-2630v3 八核处理器（主频 2.4GHz）； 内存：配置≥32GB REEC，基于后期扩展，最大支持≥8 根内存插槽； 硬盘：至少配置 2 块 300GB SAS 15000RPM 6.0Gb/s； RAID：1GB 缓存 6Gb RAID 控制器，支持 RAID0,1,10,5； 网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能；	1	台

		电源：配置白金效率 500W 电源； 管理：支持 IPMI 2.0 标准，配置 KVM over IP（允许从任何地点通过网络访问、安装、配置和控制远端服务器）及虚拟媒体功能，提供 1 个管理专用的 1000Mb 以太网口（RJ45 接口）。		
5	云计算实验室云计算节点服务器	规格：2U 机架式，配导轨套件； CPU：配置≥2 颗 Intel Xeon E5-2630v4 十核处理器（主频 2.2GHz）； 内存：配置≥192GB REEC，基于后期扩展，最大支持≥8 根内存插槽硬盘：至少配置 2 块 240G SSD+2 块 2TB SATA； RAID：1GB 缓存 6Gb RAID 控制器，支持 RAID0,1,10,5； 网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能。 电源：配置白金效率 500W+1 冗余电源；风扇：具备精准气流管理系统，根据环境温度、组件温度、气压，精确控制风量；I/O 扩展：基于应用，支持≥8 个 PCIE3.0 插槽，支持≥2 个 GPU 扩展； 管理：支持 IPMI 2.0 标准，配置 KVM over IP（允许从任何地点通过网络访问、安装、配置和控制远端服务器）及虚拟媒体功能，提供 1 个管理专用的 1000Mb 以太网口（RJ45 接口）。	5	台
6	网络安全职业技能认证考试系统支撑服务器	规格：2U 机架式，配导轨套件； CPU：配置≥2 颗 Intel E5-2630v4 十核处理器（主频 2.2GHz）； 内存：配置≥32GB*4 DDR4 REEC，基于后期扩展，最大支持≥8 根内存插槽； 硬盘：配置≥600GB*2 SAS 10K RPM 12Gb/s，配置≥1T*2 SATA 硬盘； RAID：1GB 缓存 12Gb/S RAID 控制器，支持 RAID0,1,5,6,10,50,60，带超级电容； 网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能； 电源：至少配置白金效率 500W 交流电源。	2	台
7	态势感知大数据安全支撑服务器	规格：2U 机架式，配导轨套件； CPU：配置≥2 颗 Intel E5-2630v4 十核处理器（主频 2.2GHz）； 内存：配置≥32GB*2 DDR4 REEC，基于后期扩展，最大支持≥8 根内存插槽； 硬盘：配置≥600GB*2 SAS 10K RPM 12Gb/s 配置≥6T*3 SATA 硬盘； RAID：1GB 缓存 12Gb/S RAID 控制器，支持 RAID0,1,5,6,10,50,60，带超级电容； 网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能； 电源：至少配置白金效率 500W 交流电源。	1	台
8	态势感知资产探测支撑服务器	规格：2U 机架式，配导轨套件； CPU：配置≥2 颗 Intel E5-2630v4 十核处理器（主频 2.2GHz）； 内存：配置≥32GB*2 DDR4 REEC，基于后期扩展，最大支持≥8 根内存插槽； 硬盘：配置≥600GB*4 SAS 10K RPM 12Gb/s 配置≥2T*3 SATA 硬盘； RAID：1GB 缓存 12Gb/S RAID 控制器，支持 RAID0,1,5,6,10,50,60，带超级电容； 网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能； 电源：至少配置白金效率500W交流电源。	1	台
9	流量探针服务器	规格：2U 机架式，配导轨套件； CPU：配置≥2 颗 Intel E5-2630v4 十核处理器（主频 2.2GHz）； 内存：配置≥32GB*4 DDR4 REEC，基于后期扩展，最大支持≥8 根内存插槽； 硬盘：至少配置 600GB SAS 10K RPM 12Gb/s 配置≥2T*3 SATA 硬盘； RAID：1GB 缓存 12Gb/S RAID 控制器，支持 RAID0,1,5,6,10,50,60，带超级电容；	4	台

		网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能，至少配置万兆网卡 1 个； 电源：至少配置白金效率500W交流电源。		
10	服务器机柜	标准 42U 机柜，尺寸：600*1100*2000mm，承重≥1200KG。颜色：黑色；材质：立柱、横梁、方孔条采用不小于 1.5mm 厚高强度热镀锌钢板，侧门、后门、前门采用≥1.2mm 厚高强度热镀锌钢板；防火等级 IP20,。网孔门板开孔均匀，支持通风率大于等于 67%，前后门均采用机械门锁，具有高可靠性接地功能，随机配件配齐。	5	台
11	电气系统分项工程	1、UPS 一体化精密配电柜：（1） 外形尺寸与服务器机柜一致；（2）产品符合 GB 7251.1-2005，并提供 3C 认证；（3）输入电压：380/400/415V（-10%~+20%）；（4）开关元器件采用施耐德/ABB 元器件；（5）与 UPS 集成一体化设计；（6）防雷：B 级防雷 30KA；（7）附件：LCD 屏幕、多功能电量仪、指示灯、铜排等；（8）接入动环监控系统。 2、机柜专用 PDU：铝合金材质，额定输入电压：220-250V，额定电流：16A；8 位。	1	套
12	接地系统分项工程	接地端子箱：尺寸：330*230*120mm，同流容量 200KA/接线柱 10 个；静电泄漏网、等电位地网、浪涌保护器	1	套
13	UPS 系统分项工程	1、UPS 不间断主机：兼容单进单出、三进单出及三进三出，20KVA 机架式 UPS；电池节数 24-40 节可调。 2、密封阀式铅酸蓄电池：（1）容量：12V100AH 阀控铅酸免维护蓄电池；（2）电池设计寿命≥10 年；（3）防火性能：蓄电池外壳须采用 ABS 阻燃壳体制造；（4）与 UPS 主机同品牌。 3、电池柜：整机磷化喷塑，耐磨防蚀。可拆装式全开放结构。优质金属成型，受力均匀。封闭式电池柜，内置 12V100AH 电池 32 节。	1	套
14	环境监控系统	机房动力环境监控主机、温湿度传感器、市配电柜（三相电量仪）电压电流监控、普通空调监控、UPS 监控、门磁/人体红外感应。	1	套
15	路由器	支持网络协议：PPP，CHAP，PAP，MS-CHAP，PPPoE，DHCP 客户端，DHCP 服务器，NAPT，NTP，DDNS； 广域网接口≥2 个 10/100/1000M WAN 口（电口和光口复用），局域网接口≥8 个 10/100/1000M LAN 口； 配置 1 个 USB 接口、1 个 Console 口； 功能参数：内置防火墙、Qos 支持、VPN 支持； 网络管理：基于 Web 的用户管理接口(远程管理/本地管理)、HTTPS 远程管理、命令行 CLI； 流量监控：基于物理端口的流量统计；基于 IP 的流量统计，支持自动排序功能；基于 IP 的 NAT 链接数统计； 系统服务：ALG；端口触发；UPnP；虚拟服务器；DMZ 主机；VPN 透传(PPTP、L2TP、IPSec)； 故障诊断：Ping/Traceroute；设备自检；故障信息一键导出。	1	台
16	中心交换机	传输速率:10/100/1000Mbps,交换方式:存储-转发,背板带宽≥336Gbps/3.36Tbps,包转发率≥51Mpps/108Mpps； MAC 地址表:支持黑洞 MAC 地址，支持设置端口 MAC 地址学习最大个数； 端口描述≥24 个 10/100/1000Base-T 以太网端口，≥4 个 1000Base-X SFP 千兆以太网端口； 控制端口:1 个 Console 口； 功能特性: 网络协议:支持 STP/RSTP/MSTP 协议，支持 STP Root Protection，支持 RRPP； 路由协议：支持 IPv4/IPv6 静态路由，支持 RIP/RIPng，OSPFV1/V2/V3； 网络管理:支持命令行接口(CLI)配置,支持 Telnet 远程配置,支持通过 Console 口配置；	1	台

		安全特性：支持用户分级管理和口令保护，支持 SSH2.0； 镜像：支持端口镜像，支持流镜像。		
17	接入交换机	传输速率:10/100/1000Mbps,交换方式:存储-转发,背板带宽≥96Gbps,包转发率≥71.4Mpps； 端口描述≥48个10/100/1000Mbps自适应以太网端口； 功能特性: 网络标准:IEEE 802.3，IEEE 802.3u，IEEE 802.3x，IEEE 802.3ab； 电源电压:AC 100-240V，50-60Hz。	1	台

4.2 网络安全综合实验室

序号	项目名称	招标要求的技术指标	数量	单位
1	云实验管理系统	B/S 架构，包含课程管理、学生管理、虚拟环境管理、实验工具、知识库、项目实训等功能。	1	套
		★支持同时并发 200 个用户使用，支持同时仿真不少于 400 台设备，操作应无卡顿。多个学生使用相同实验环境学习，实验环境内设备每个设备都有独立 IP。**（提供功能截图加盖投标人公章并现场功能演示）**		
		在线实训模块-平台提供在线学习实训功能，用户可以通过提供的功能进行信息安全知识学习、培训、实训、实验及考核。		
		资源状态监控模块-支持系统整体资源状态监控，展现系统整体内存、硬盘的使用情况和资源占用的百分比显示。同时，可监控不同子系统的资源使用情况并对不同部分进行资源限额。		
		★**用户管理模块**-支持用户对头像、密码、性别、生日、城市、邮箱、签名等信息进行管理维护，支持账号的批量导入，同时支持可对学生进行批量导出，也可根据角色导出不同类型的用户。批量导入时支持直接通过导入模板创建不同角色的用户。**（提供功能截图加盖投标人公章并现场功能演示）**		
		实验管理模块-支持实验标准模式和扩展模式两种模式；拓展模式下老师可结合时下热点漏洞和教学倾向自行配置实验环境。		
		★支持实验手册和实验拓扑同屏显示，方便学生做实验，实验手册支持拖拽放大缩小，提供一键启动、一键关停、标靶单独重启、多次延时功能。**（提供功能截图加盖投标人公章并现场功能演示）**		
		平台支持学生学习实验报告撰写功能，对于已经提交的实验报告支持重复提交。		
		集群统一管理模块-支持设备的集群统一管理：平台可动态增加、移除计算资源；增加计算资源后，平台内的可用 CPU 数量和内存容量会自动动态增加。		
		平台可动态增加、移除存储资源；增加存储资源后，平台内的可用存储容量会自动动态增加，在平台上新增课件及实验场景时，存储资源可即时同步，无需手动进行更新；平台可自动对资源按性能进行自动调度及负载均衡，不需要设置任何的阈值。		
2	教学管理系统	**方案管理模块**-要求教学资源支持快速复制和重复利用，老师自己创建全新的人才培养方案，也可以系统提供的方案内容为基础进程继承创建，要求支持方案内部支持课程的先后排序，系统提供配套教学资源，提供职业教育、知识短训、就业培训多种类型。	1	套
		教师事务管理模块-平台支持对教师事务功能，用于存放需要教师处理的事务，可以根据时间、组织架构、教学计划等进行待处理事情的查看，事务内容包含课程备课、练习、随堂练习、项目实训、技能评测等内容学生的完成情况和提交情况。		

		教学计划模块-平台提供教学计划功能，教师可设置教学计划，一个教学计划由多个时间块组成，每个时间块可以包含多个课程资源，教师可对课程资源进行创建、修改、删除，资源内容包含培训视频、实验操作环境、实验手册、实验报告、项目实训、技能测评。		
		平台支持针对班级进行教学计划的下发，也可以根据实际教学情况进行定制化教学计划的下发，可对课程进行详细制定，包括班级、计划名称等。		
		课程管理模块-教员创建课程时，教员可选择所建课程的访问模式，包含公开和不公开两种模式，其中公开模式下所有学员及教员均可使用和查看。		
		考核管理模块-平台可提供不少于 1000 道理论题目和不少于 200 道 CTF 竞赛题目，支持单选、多选、判断、实验靶场，其中技能题目需要包含附件题、本地操作类型题目、综合网络渗透等多种题目形式。		
		考试统计模块-支持设置考试题目是否显示，提供每场考试按分数段进行统计，并可导出考试成绩，每场考试平台可出具错误题目的统计，包含出错题目以及出错学员，且支持按不同分数段进行人数统计；		
		教学统计模块-平台需提供统计及分析功能，包含课程资源数量、题库数量、实训项目数量等信息。平台提供学生学习能力分析，可通过分析报告了解学生知识掌握情况，老师可通过数据分析了解学生的整体情况以及每个知识点学生的掌握情况，便于定向辅导。		
3	学情管理系统	**学习模式模块**-支持教学、自学两种模式，教学模式下学生需按照教师规定的教学任务进行学习，自学模式下除教师的教学任务之外，可自由选择课程学习。	1	套
		学习统计模块-支持对学员提供自学统计功能，学员可实时查看自己对自学选课的学习掌握情况以及课程的学习进度，并通过测试记录对学员能力进行展示。		
		学习追踪模块-支持对学员提供学习跟踪功能，学员可实时查看自己对自学选课的学习掌握情况以及课程的学习进度，平台需记录学员操作日志，包含学习课程、实验内容、考试名称、考试时间等。		
		▲随堂练习模块-平台学习支持实验实操机制和随堂练习功能，教员可查看每个班级的学习进度、实验进度、练习进度以及课表，学生、教师可通过测试成绩记录对学生在培训方案中的知识掌握情况进行分析，同时学生可查看自己的学习记录等。**（提供功能截图加盖投标人公章）**		
		考试查看模块-支持学员对未开始考试、正在进行考试、已结束考试的考试名称、题目类型等信息进行查看。		
4	题库管理系统	**题库分类模块**-题库支持题目分类功能，用户可自定义分类，支持题目内容搜索功能，支持题目的创建，支持试题导出功能。	1	套
		试卷管理模块-支持试卷模板功能，可将题库中的题目挑选完成后组成试卷，用于考试时选择跟引入。		
		支持自动组卷和手动组卷两种组卷方式，自动组卷只需指定知识结构下各类题目数量、题目分值即可快速形成考核试卷。		
5	项目实训管理系统	平台支持项目实训，项目实训以实际的项目开展方式为基础，支持 WEB 安全、渗透测试、代码审计、内网渗透、反序列化、信息收集等多个方面的实训项目。	1	套
		▲项目管理模块-要求系统支持项目简介与项目课程大纲，项目简介至少包括核心内容、实验环境等信息；课程大纲以流程形式显示课程模块，可以点击展开模块显示具体实验课程。**（提供功能截图加盖投标人公章）**		
		项目分组管理-要求项目实训以项目团队的方式模拟一个完整项目的实际工作方式对学生进行项目实训演练；		
		项目流程管理模块-要求系统支持对项目流程的完整模拟，提供项目实训、技能测试等内容学生的完成情况和提交情况。		

6	虚拟仿真系统	**虚拟仿真模板**-虚拟化设备支持包括网络设备、基础服务器、web 服务器、数据库、PC 终端、武器库等实验室母版和模板镜像系统，母版为基础镜像，模板集成测试环境，支持虚拟机模板和母版的管理功能。	1	套
		★镜像管理模块-支持用户根据历史镜像选择文件形式生成自己的镜像，生成后系统自动纪录镜像的状态、大小等信息，可对系统镜像资源的查询，查询支持镜像名称的关键字查询方式，支持镜像的分类管理。**（提供功能截图加盖投标人公章并现场功能演示）**		
		虚拟机管理模块-支持虚拟化机的自动安装和快速克隆功能,可查看对虚拟化设备使用情况的查看，包含所属课程（项目）、操作人、操作状态等操作详情。		
		▲支持虚拟机镜像模板的管理功能，可对模板信息进行编辑，包含模板名称、描述信息等，支持虚拟机模板在线启动查看，启动时可动态设置 CPU 数量及内存大小。**（提供功能截图加盖投标人公章）**		
		支持虚拟机一键启动校验，记录拓扑内虚拟机的启动情况，对于启动异常的虚拟机设备给与提示。		
		实验操作管理模块-学员进行实验时，平台需支持学员电脑直接对目标环境的访问以及通过 web 虚拟桌面的方式进行操作两种实验形式。		
7	虚实结合管理系统	**★拓扑管理模块**-平台支持自定义网络拓扑功能，可通过名称、ID 等方式模糊查询标靶单元，支持以拓扑拖拽形式选择标靶单元进行组建，提供拓扑图、显示、放大显示、鼠标缩放等拓扑查看功能。**（提供功能截图加盖投标人公章并现场功能演示）**	1	套
		系统提供拓扑的管理功能，可实现创建拓扑、修改拓扑、删除拓扑。		
		系统支持可视化视图，可视化视图场景化的实验操作模式体验，可形象展示设备详情以及网络连接情况，可视化视图贯穿实验、项目等实操环节；支持拓扑内标靶的检索、快速预览和重复利用。		
		★拓扑配置模块-单机实验及网络实验课时添加支持自定义网络拓扑，可对拓扑中的元素进行镜像模板、CPU、内存、磁盘、是否可见等参数信息进行配置。同时支持共享元素，可通过域名或 IP，实现共享访问。可灵活自定义拓扑的链路连接结构。在外部环境中可使用图形化和命令行远程工具连接拓扑环境中的虚拟机。**（提供功能截图加盖投标人公章并现场功能演示）**		
		拓扑展现模块-物理设备创建完成后在实验拓扑环境中显示，并支持实验环境中资产拖拽。		
		设备管理模块-平台支持外置物理安全设备的接入，包含防火墙、IPS、IDS、VPN、WAF，提供自定义设备管理功能，包含设备名称、分类、串口端口、所属小组等基本信息。		
		资产管理模块-平台支持所添加的真实设备资产的设备名称、设备类型、设备图标、设备面板、设备描述、账号、密码等信息修改。		
		实验监控模块-支持实验以小组形式下发，支持教师监控功能，教师可远程监控学员正在进行的实验操作。		
		环境还原模块-提供目标环境还原接口，教师可通过 webconsole 的方式对目标环境进行还原。		
8	安全攻防演练系统	能够支持不少于 1000 人同时在线选择题、技能题，不少于 60 支队伍的 CTF 夺旗、擂台对抗和红蓝对抗。	1	套
		用户管理模块-提供管理员、教师、学生等用户角色；管理员可对账户进行批量操作，包括导入、新增、删除和修改等。		
		赛事公告模块-提供全面的竞赛过程管理功能，管理员可对竞赛过程中竞赛行为进行监控和管理。支持对比赛开始时间、比赛时长等进行配置，提供系统提供减分功能，管理员可根据竞赛规则对违规竞赛人员进行减分操作，提供扣分提示开		

		关功能。		
		竞赛管理模块--提供全面的竞赛过程管理功能，管理员可对竞赛过程中竞赛行为进行监控和管理。支持对比赛开始时间、比赛时长等进行配置，提供系统提供减分功能，管理员可根据竞赛规则对违规竞赛人员进行减分操作，提供扣分提示开关功能。		
		CTF 模块-提供解题思路开关服务，服务开启系统提供解决思路，在提交错误 Flag 情况下支持智能推荐相关课程；CTF 平台管理支持支持编辑、删除、批量删除、筛选等操作；支持关键字模糊搜索 CTF 题目；支持开启关闭 Write-up，关闭之后前台用户无法查看 CTF 题目解题思路。		
		▲擂台对抗系统-1.要求提供擂主靶机设计功能，支持对靶机的网络名称、网络地址、网关 IP、分配地址池、DNS 域名解析服务、连接设备等参数的编辑；支持是否对攻擂选手显示拓扑图，该功能的开启可帮助夺擂者获取对应靶机的 IP 地址便于夺擂；要求支持现场演示； 2.支持夺擂操作区包括擂主拓扑查看、倒计时显示、Flag 提交等功能；要求拓扑显示攻陷状态、运行状态、擂主服务器的 IP；要求系统提供夺擂通道支持投诉、举报方式、比赛规则的说明，同时具有放大、缩小和隐藏的功能；支持得分排行榜功能显示该队伍的得分情况； 3.擂台系统的工作流程顺序为管理员创建第一轮比赛擂主队伍，擂主队伍对比赛环境进行设定，设定完毕后提交管理员进行审核，管理员进行审核后可设置比赛是否开始，比赛开始后，其他队伍可查看到擂主设定的比赛环境，并进行比赛。**（提供功能截图加盖投标人公章）**		
		▲红蓝对抗系统-要求比赛界面显示竞赛名称、比赛倒计时、服务监控状态、比赛信息、通知栏、靶机信息、排行榜、Flag 提交窗口；比赛信息包括所属队伍、队员名称、开始时间、比赛限时；通知栏实时显示比赛信息；服务监控支持显示未开启、服务正常、服务异常、被攻陷等状态；排行榜信息支持滚动显示队伍名称、总分、攻击分、防守分、奖惩分等。**（提供功能截图加盖投标人公章）**		
		分数管理模块-管理员可通过裁判操作界面进行对发现的恶意攻击情况进行扣分及公告，同时对比赛中的表现良好的队伍进行分数后台添加。		
		大屏展示模块-提供生动、形象的展示界面，主要分为竞赛人员答题界面和竞赛过程展示界面：竞赛过程展示页面支持中国地图展示、世界地图展示、排名展示与流量展示。		
		1、竞赛人员在答题界面能够实时查看个人排名、得分情况、比赛公告、比赛时间等相关比赛信息。		
		2、竞赛过程展示界面能够实时显示竞赛所有竞赛人员的得分、排名、时间等竞赛信息。		
		3、提供竞赛过程中的攻防行为形象展示，如动态的射线显示队伍之间的攻击行为、不同颜色射线块显示不同队伍等；系统根据竞赛人员的答题情况进行统计分析，最后以竞赛能力进度条的方式展示。		
9	防火墙安全实训设备	硬件要求：1U 标准机架式设备，配备≥5 个千兆电口、≥4 个 COMBO 接口，提供 USB 接口，配置双冗余交流电源，符合国家标准 GB/T 17626.5：2008 第三级及以上标准，并提供检测报告，采用 64 位 MIPS 多核架构，采用自主知识产权的 64 位多核并行安全操作系统。 性能要求：吞吐量≥4Gbps，AV 吞吐量≥700Mbps， IPS 吞吐量≥1Gbps，IPsec VPN 吞吐率≥1Gbps；最大并发连接数≥200 万；最大 IPsec VPN 隧道数≥2000，每秒新建会话≥5 万，SSL VPN 并发用户数可扩展到至 1000 个；最大支持的虚拟防火墙个数≥10 个； 功能要求： 1、支持 OSPF、BGP 和 RIP 路由协议，内置运营商路由条目；支持非等价链路的智能链路负载均衡，包括出站动态探测、TCP Track、入站 SmartDNS；支持透明、路由、混合三种工作模式，支持双向 NAT、动态地址转换和静态地址转换，并且	4	台

		提供网段间的双向静态一对一地址转换功能；支持按照应用、时间、用户账号、IP 地址、服务端口、物理端口等方式对数据进行访问控制，要求能主动屏蔽恶意地址，以用于提前免疫包括病毒网站或者攻击源地址的攻击。 2、支持智能 DNS 功能，使外网访问内部服务器的流量可以在多条链路上实现智能分担，支持智能链路负载均衡技术，可动态探测链路响应速度并选择最优链路进行数据转发，支持基于应用的自动链路选择，即根据应用类型来选择将会话路由到不同链路上。 3、支持虚拟化技术，包括虚拟交换机、虚拟路由器，虚拟防火墙，支持抵御各种 DDOS 攻击，威胁防护功能可以呈现全球威胁防护地图。 4、提供开发云运维管理平台软件，实现手机 APP 实时管理和监控设备运行状况，日志存储功能。 5、支持AlgoSec和FireMon主流防火墙管理系统，并提供AlgoSec和FireMon官网证明材料。支持通过SYSLOG、二进制格式记录NAT日志。		
10	入侵防御安全实训设备	硬件要求：1U 标准机架式设备，专业 IPS 设备，非下一代防火墙或者 UTM 设备，单电源，标配 4 个 GE 接口，支持硬件 bypass，配备 1 个扩展插槽，1T 硬盘。 性能要求：整体吞吐≥2.5Gbps，IPS 吞吐量≥900Mbps，最大并发连接数≥100 万，可扩展至 200 万，HTTP 最大并发连接≥100 万，HTTP 每秒新建会话≥1 万。 入侵防御功能：基于状态、精准的高性能攻击检测和防御，实时攻击源阻断、IP 屏蔽、攻击事件记录；支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御；支持 HTTP Get、Head、Put、Post 等多种协议方法检查；提供预定义入侵防御配置模板，支持自定义入侵防御特征 -依据 IP、TCP、UDP、IGMP、ICMP 等网络层的各项参数设置特征，全面设置 TCP/IP 应用层的特征比对内容，不受通信协议的限制，支持跨数据包检测机制，包括：比对位移(matching offset)、比对长度(matching depth)、比对距离(matching distance)、比对范围(within)，支持基于流的数据包(stream-based)比对技术；提供 7800 多种特征的攻击检测和防御，特征库支持网络实时更新，包含 3 年 IPS 特征库升级服务。 WEB 防护功能：系统具备对网站外链防护功能，系统具备对 CC 攻击的检测和防御能力，系统具备对跨站脚本攻击的检测和防御能力，系统具备对 SQL 注入攻击的检测和防御能力，可以对 Web 服务系统提供保护。 报表功能：支持报表，报表需要包含多视角,提供安全风险概览、安全风险详情、威胁类型、网络流量分析、系统运行状况不同维度报表，丰富的威胁日志内容，包含 CVE-ID、漏洞描述信息和解决方案。	1	台
11	入侵检测实训设备	硬件要求：1U 标准机架式设备，专业 IDS 设备，单电源，标配 4 个 GE 接口，支持硬件 bypass，配备 1 个扩展插槽，1T 硬盘。 性能要求：整体吞吐≥2.5Gbps，IPS 吞吐量≥900Mbps，最大并发连接数≥100 万，可扩展至 200 万，HTTP 最大并发连接≥100 万，HTTP 每秒新建会话≥1 万。 入侵检测功能：基于状态、精准的高性能攻击检测，实时攻击源、攻击事件记录；支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测；支持 HTTP Get、Head、Put、Post 等多种协议方法检查；提供预定义入侵检测配置模板，支持自定义入侵检测特征 -依据 IP、TCP、UDP、IGMP、ICMP 等网络层的各项参数设置特征，全面设置 TCP/IP 应用层的特征比对内容，不受通信协议的限制，支持跨数据包检测机制，包括：比对位移(matching offset)、比对长度(matching depth)、比对距离(matching distance)、比对范围(within)，支持基于流的数据包(stream-based)比对技术；提供 7800 多种特征的攻击检测，特征库支持网络实时更新，包含 3 年 IPS 特征库升级服务。 WEB 攻击检测：系统具备对网站外链检测功能，系统具备对 CC 攻击的检测能力，系统具备对跨站脚本攻击的检测能力，系统具备对 SQL 注入攻击的检测能力，可以对 Web 服务系统提供保护。 报表功能：支持报表，报表需要包含多视角,提供安全风险概览、安全风险详情、	1	台

		威胁类型、网络流量分析、系统运行状况不同维度报表，丰富的威胁日志内容，包含 CVE-ID、漏洞描述信息和解决方案。		
12	网站防火墙实训设备	硬件要求：1U 标准机架式设备，产品为专业的 WEB 应用防护系统产品，单电源；1 个 RJ45 串口，2 个 USB 口，配置 6 个千兆电口含 1 个 MGT 口及 1 个 HA 口，配置 1 个扩展插槽，可扩展 IOC-W-4GE-B-L，IOC-W-4SFP-L； 整机吞吐 5Gbps，HTTP 应用吞吐量 600Mbps，TCP 并发连接 50 万，HTTP 并发连接 10 万，HTTP 新建连接 6000；硬盘大于 1TB。 功能要求： 系统具备 DDoS 攻击防御能力，系统具备注入攻击防御能力，可以对 SQL 注入、LDAP 注入、SSI 指令注入、Xpath 注入、命令注入、远程文件包含以及其他注入进行防御，系统具备跨站攻击防御能力，可以对 XSS 和 CSRF 攻击进行防御，系统具备信息泄露防御能力，可以防止服务器错误、数据库错误、Web 目录内容、程序代码、关键字等信息的泄露，需提供相关截图证明；系统具备保护 Cookie 安全能力，可以防止 Cookie 被恶意篡改、Cookie 被恶意劫持，系统具备 Web 访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御，系统具备特殊漏洞攻击防御能力，可以对针对 Web 服务器、Web 框架、Web 应用程序的漏洞攻击进行防御，系统具备防御资源非法访问能力，可以对非法上传、非法下载和盗链攻击进行防御，系统具备恶意软件防御能力，可以对 Web Shell、木马攻击等进行防御； 支持 IPv4、IPv6 双栈部署，可同时添加 IPv4 和 IPv6 地址为保护站点； 网页防篡改支持学习模式和保护模式两种运行模式，支持自定义防护的静态网页类型，支持内置同步引擎同步服务器内容并建立基线，支持篡改监控和正常修改监控，支持篡改内容取证；网络层安全防护支持整机 Flood 攻击防护（Syn Flood、UDP Flood、ICMP Flood 等）、扫描/欺骗攻击防护、DoS 攻击防护、代理攻击防护等；部署模式支持透明串接部署，支持反向代理部署，支持单臂部署模式，支持牵引部署模式，含 PBR 回注和跨接回注；高可用支持 HA-AP 双机热备功能，通过内置或外置的组件，支持断电 Bypass 功能，所有标配业务电口都支持硬件 Bypass 功能；应用加速支持 Web Cache 功能，支持 SSL 卸载；负载均衡支持 SLB，支持加权轮询、最少连接以及 IP Hash 算法；报表功能需要包含多视角，提供安全风险概览、站点风险详情、攻击类型详情、站点篡改分析、站点访问量、网络层攻击汇总、系统运行状况不同维度报表，需要提供截图证明；特征库可以通过人工或者自动方式进行升级，升级过程中不需重启设备，并能保持原有会话连接不中断。	1	台
13	VPN 实训设备	硬件要求：1U 标准机架式设备，配备≥9 个千兆电口，支持双冗余交流电源，符合国家标准 GB/T 17626.5：2008 第三级及以上标准，并提供检测报告，采用 64 位 MIPS 多核架构，采用自主知识产权的 64 位多核并行安全操作系统。 性能要求： IPsec VPN 吞吐率≥600Mbps；最大并发连接数≥40 万；最大 IPsec VPN 隧道数≥1000，每秒新建会话≥1.2 万，SSL VPN 并发用户数可扩展到至 500 个； 功能要求： 1、支持 OSPF、BGP 和 RIP 路由协议，内置运营商路由条目；支持非等价链路的智能链路负载均衡，包括出站动态探测、TCP Track、入站 SmartDNS；支持透明、路由、混合三种工作模式，支持双向 NAT、动态地址转换和静态地址转换，并且提供网段间的双向静态一对一地址转换功能；支持按照应用、时间、用户账号、IP 地址、服务端口、物理端口等方式对数据进行访问控制，要求能主动屏蔽恶意地址，以用于提前免疫包括病毒网站或者攻击源地址的攻击。 2、IPSec VPN 严格遵循 RFC 国际标准，可于主流 VPN 厂商互通，支持 DH 组的秘钥交换方式，支持 group 1、2、5、14、15、16 等类型，提供产品界面截图有效。 3、SSL VPN 支持 32 位和 64 位 Windows 2000/2003/XP/Vista/Windows 7/Windows 8/IOS/Android 操作系统 VPN 接入，支持对登录 SSL VPN 的用户端系统进行端点安全检查，至少包括文件路径、运行进程、安装服务、运行服务、防火墙、防间	1	台

		谍软件、防病毒软件、自动更新、注册表键值、系统版本、系统补丁、浏览器版本、浏览器安全级别设置等方面，提供产品界面截图有效。 4、提供开发云运维管理平台软件，实现手机 APP 实时管理和监控设备运行状况，日志存储功能。 5、支持 AlgoSec 和 FireMon 主流防火墙管理系统，并提供 AlgoSec 和 FireMon 官网证明材料。支持通过 SYSLOG、二进制格式记录 NAT 日志。		
14	日志审计实训设备	硬件要求：1U 标准机架式设备，专业的网络安全审计系统，收集存储网络行为、流量分析及网络安全日志内容，收集并存储服务器，交换机和现有的网络安全设备的日志，实现对所有网络访问行为的安全审计及统计分析、报表管理，实现对防火墙/IPS 设备的状态监测、性能分析等功能，配置 2 个 10/100/1000Base-T 接口，单电源。 性能要求：二进制 NAT 日志处理速度不少于 30,000EPS；syslog 日志处理速度不少于 3000EPS；在线日志查询速度＜20s；存储空间≧2TB（RAID0）。 支持日志类型：支持 NAT 日志包括时间、用户名、MAC、转换前后 IP、端口等元素；支持 NAT444 日志包括时间、转换后 IP/端口、源 IP/端口、第一个/最后一个源端口、协议类型等元素；支持安全网关、IPS 设备以及防病毒设备的攻击日志、入侵防御日志、病毒日志等。全面支持 Syslog、SNMP 日志协议，可以覆盖主流硬件设备、服务器、交换机、主机及应用，保障日志信息的全面收集。实现信息资产（网络设备、安全设备、主机）的日志获取，并通过预置的解析规则实现日志的解析、过滤及聚合。 日志备份：支持手动、自动方式的日志导入、导出，支持单独导出 NAT 日志、会话日志、安全功能日志等；支持 SFTP 日志转存；支持查询匹配条目导出。 监控：支持监控磁盘使用情况、日志接收情况；支持定制条件邮件告警； 管理：支持多用户并发登陆；支持本地/远程系统升级。	1	台
15	漏洞扫描设备实训设备	硬件要求：1U 标准机架式设备，配备≥6 个千兆电口、≥4 个 USB 接口、1 个 RJ45 串口、1 个 DB9 串口、单电源。系统漏洞扫描（支持 512 个扫描对象范围）；单个扫描任务最多包含 2048 个 IP 地址（8 个 C 类网段）；最大允许并发扫描 80 个主机；最大允许 5 个扫描任务并发。 功能参数： 能够对主流的操作系统、应用服务、数据库和网络设备四个方面进行漏洞扫描和分析。系统漏洞知识库的检测脚本大于 82000 多条。支持智能服务识别、授权登录扫描、安全优化扫描等技术。包括资产探测管理、系统漏洞扫描、弱口令猜解、漏洞大屏展示等功能。系统提供了详细的漏洞描述和对应的修补措施及安全建议，方便用户全面发现信息系统中存在的安全漏洞，防患于未然。 支持系统漏洞扫描，系统漏洞知识库的检测脚本大于 82000 多条。支持智能服务识别、授权登录扫描、安全优化扫描等技术。 支持弱口令扫描，支持 SSH、TELNET、SMB、RDP、FTP、POP3、SMTP、SNMP、REDIS、ORACLE、MSSQL、MYSQL、RTSP、SIP、S7-300、VNC 等 20 多种协议；支持恶意代码检测，支持木马后门的离线检查，支持网站恶意代码的离线检查；支持资产探测管理，每周至少升级一次，报表格式支持 HTML、DOC、PDF、XML 等；支持脆弱性大屏展示，支持通过大屏展示各类漏洞地理分布情况，资产统计，漏洞统计，最新漏洞，风险趋势等。	1	台
16	网络机柜	容量：12U，门及门锁：有，材料及工艺：SPC 优质冷轧钢，脱脂静电喷塑 标准符合 ANSI/EIA RS-310-D，IEC297-2DIN41491PART1，DIN41494； PART7GB/T3047.2-92 标准，兼容 EISI 材料及工艺　SPC 优质冷轧钢，脱脂静电喷塑 外观参数（长*宽*深）：700mm*550mm*450mm 标准标配：托盘×1，12U 立柱×4，脚轮×4	2	台

17	接入交换机	传输速率:10/100/1000Mbps,交换方式:存储-转发,背板带宽≥96Gbps,包转发率≥71.4Mpps 端口描述≥48 个 10/100/1000Mbps 自适应以太网端口 功能特性: 网络标准:IEEE 802.3，IEEE 802.3u，IEEE 802.3x，IEEE 802.3ab 电源电压:AC 100-240V，50-60Hz	4	台
18	可视化大屏	80 寸展示大屏，,屏幕分辨率:超高清 4K,HDR 显示:支持，背光源：LED，背光方式：直下式，支持格式（高清）：2160p，核心参数：CPU4 核，运行内存：至少 2GB，存储内存：至少 8GB，端口参数：支持 USB2.0 接口、支持 HDMI2.0 接口，单屏尺寸（宽*高）mm：至少 1686x970。	2	台

4.3 网络安全职业认证考试平台

序号	产品名称	招标要求的技术指标	数量	单位
1	认证考试平台	▲投标人根据各自企业情况提供企业职业认证考试系统的功能模块与职业认证方式。**（提供功能截图加盖投标人公章，至少包括认证证书、客观试卷、实操试卷、认证考试报告、认证考生报告等五项）**	1	套

4.4 云计算安全实验室

序号	产品名称	招标要求的技术指标	数量	单位
1	云基础架构平台软件	1、平台支持基于 Docker 容器开放式云平台架构和基于 OpenStack 的云平台架构的混合架构模式。基于 Docker 容器开放式云平台架构优势：更高效的利用系统资源、秒级、甚至毫秒级的启动时间、更轻松的迁移、更轻松的维护和扩展；基于 OpenStack 的云平台架构优势：实现对内部的虚拟机资源分配管理，虚拟机在线迁移和冷迁移实现。 2、镜像管理功能：支持显示 OpenStack 和 Docker 镜像列表、能从 Docker 容器创建新镜像、要求能够从 Dockerfile 构建镜像、从 registry 下载镜像、能将 OpenStack 镜像和 Docker 镜像上传到镜像仓库、能够删除 Docker 镜像和 OpenStack 镜像、支持修改镜像支持使用 Dockerfile 构建镜像。 3、配额调度：启动/停止/重启容器和 OpenStack 虚拟机、暂停/恢复容器、删除容器和 OpenStack 虚拟机、重置 OpenStack 虚拟机密码、限制虚拟机、容器对 CPU 的使用、限制虚拟机、容器对内存的使用、限制容器对 Block IO 的使用、限制虚拟机对根磁盘的使用。支持私有 Docker Registry，用户可在本地搭建私有 Docker Registry。 4、支持认证、授权、访问控制、API 注册和发现等机制。 5、支持维护 Docker、OpenStack 集群状态，比如故障检测、自动扩展。 6、支持 OpenStack 虚拟机管理器的概述。 7、支持维护容器、OpenStack 虚拟机的生命周期，支持 Volume 和网络管理。 8、支持 OpenStack 虚拟机的冷迁移、热迁移。 9、支持负载均衡。 10、可提供教学所需的镜像资源。 11、Docker 支持秒级创建容器资源。	1	套

2	实训系统	1、院校内组织机构管理：系统支持根据院校自身管理机构进行院校内组织机构的管理，管理层级满足院校-二级院校-系-专业或者院校-二级院校--专业等多种方式进行组织机构管理。 2、院校内角色自定义：系统支持根据院校自身管理进行相应角色定义及角色权限定义。 3、用户管理及班级管理：系统支持按照当前登录人员所处院内组织机构及角色进行用户的分级管理，以及各个专业的班级分级分域管理；支持学生的批量导入功能。 4、支持课程分类及知识标签可定义：系统支持课程分类、知识标签的自定义功能，院校可以按照自身知识体系、课程分类进行设置。 5、实训课程自定义管理：实训课件定义实现标准化，支持根据自定义添加实训内容，包括编辑实训内容、实训章节定义、选择实训环境、判分准则、实训课件上传附件(PDF/视频)等操作。 6、支持顺序连续进行实验和非连续实验定义：系统支持根据不同课程资源及内容，支持课程按照顺序连续进行实验或者非连续由实验者进行选择实验进行实验，以便于支持对知识类或者案例类实验课程进行不同的实验管理方式。 7、支持实训环境定义：系统支持为课程设置实训环境，系统内嵌部署课程技能实训所需的实训环境，在课程定义时进行实训环境定义，学员实训时按照实验定义对实验环境进行分配或加载，保障整体实验资源的高效利用。系统支持按照实验或者课程设置不同的实验环境，可以在同一门课程中，按照不同实验内容，对某些实验特殊要求进行实验环境定义。 8、开课：支持开课老师与授课老师分离，开课时可以选择自己或者其他老师进行授课。开课可以按照教学班进行开课，开课过程中可以选择一个行政班进行教学，也可以支持选择多个行政班级进行大班制教学。 9、实验环境管理：系统支持开课老师或者授课老师对自己教学班进行实验环境管理，支持自己教学班学生的实验环境进行开机、关机、重启等功能。 10、实验报告管理：系统支持开课老师或者授课老师对自己教学班进行实验报告查阅、评语及评分等功能。 11、教师实验功能：系统支持开课老师及授课老师对自己参与的课程进入实验功能，并进行实验。 12、学生实验功能：学生按照课程开设要求进入自己教学班所分配课程中进行实验。 13、实验辅助功能：当实验中存在多台虚拟机时，可以进行虚拟机切换；实验过程支持向虚拟机上传文件、下载文件、虚拟机截屏、粘贴板、重置实验等功能。 14、实验报告提交：在实验界面支持实训操作的同时提交实训报告。 15、实验报告自动判分功能：系统支持按照实验自动评分，对完成在线实训课程的实验结果，通过判分服务，自动判定学生操作的成绩，教师可以接受系统自动评分结果，也可以手动进行评分。 15、我的实验及报告：系统支持实验者自身查看实验及报告功能，对于已完成的实验，实验者可查看自己提交的实验报告及教师评语、评分；对于正在进行实验，实验者可以进行继续实验、重新实验以及释放实验资源功能。 16、我的实验环境：系统支持实验者对自身占用的实验环境进行管理，包括开机、关机、重启、重置密码等功能。 17、提供学生个人中心页面，支持对个人资料、密码等进行修改；支持最近未完成的实验进行展现，可以快速进入上一个尚未完成的实验；支持查看近期自身学习时长，展现方式支持最近一周、最近 2 周、最近一月多种查看方式。 18、学生个人中心支持查看学生个人所需学习的课程信息，支持更多快速进入我的课程查看更多课程信息；支持查看个人正在进行或已完成的实验信息，支持更多快速进入我的实验及报告查看更多实验及报告功能；支持查看个人正在占用的虚拟机资源信息，可以进行开机、关机、重启、重置密码等功能，系统支持点击更多快速进入我的实验环境查看更多实验环境功能。	1	套

		19、教师个人中心支持对个人资料、密码等进行修改；教师个人中心支持最近未完成的实验进行展现，可以快速进入上一个尚未完成的实验. 20、班级中心：系统支持教师按照班级对各班级开展的课程进行查看，并对该课程各实验报告、实验环境等进行查看。 21、课程中心：系统支持教师按照课程对该课程开课班级进行查看，并对该课程各实验报告、实验环境等进行查看。 22、课堂管理：系统支持按照班级、实验对课程实验情况进行实验进度查看，可以对具体实验进展，已完成学生、未完成学生进行查看。		
3	网络机柜	容量：12U，门及门锁：有，材料及工艺：SPC 优质冷轧钢，脱脂静电喷塑 标准符合 ANSI/EIA RS-310-D，IEC297-2DIN41491PART1，DIN41494；PART7GB/T3047.2-92 标准，兼容 EISI 材料及工艺　SPC 优质冷轧钢，脱脂静电喷塑 外观参数（长*宽*深）：700mm*550mm*450mm 标准标配：托盘×1，12U 立柱×4，脚轮×4	1	台
4	接入交换机	传输速率:10/100/1000Mbps,交换方式:存储-转发,背板带宽≥96Gbps,包转发率≥71.4Mpps 端口描述≥48 个 10/100/1000Mbps 自适应以太网端口 功能特性: 网络标准:IEEE 802.3，IEEE 802.3u，IEEE 802.3x，IEEE 802.3ab 电源电压:AC 100-240V，50-60Hz	2	台

4.5 网络安全态势感知实验室

序号	项目名称	招标要求的技术指标	数量	单位
1	入侵检测模块	▲至少 19 种 web 漏洞（ PHP 代码执行、扫描器漏洞探测、XSS 跨站脚本、PYTHON 代码执行、SQL 注入攻击等）、常规渗透入侵、内网横向渗透等各类黑客攻击和恶意流量进行实时检测及报警，实时响应准确率 99.5%以上，并能够检测出系统中受控的服务器，定位出当前企业受影响的业务模块。**（提供功能截图加盖投标人公章）**	1	套
2	事件还原模块	▲面对善于用不同身份和地址进行攻击的黑客，将多条攻击告警分析汇总，做攻击事件还原（支持精细化规则至少 65 条，例如读取/etc/passwd 文件、执行 ipconfig 命令、执行 netstat 命令等），这对事后的审计、溯源、取证有极大的帮助，同时基于攻击成功事件的数据下钻能力，可做到威胁狩猎、攻击者画像、APT 感知、入侵事件还原、渗透测试监控，达到实时反馈安全问题的目标。**（提供功能截图加盖投标人公章）**	1	套
3	行为预判模块	基于对攻击链深入的理解，通过观察成功入侵动作在攻击链的位置信息，能预测该入侵事件的下一步动作，感知当前区域的成功攻击情况，真实刻画该区域的安全态势。提供决策参考，以便及时做出调整和防御动作，早一步扼杀黑客的攻击，避免造成严重的财产损失和进一步的敏感信息泄露。	1	套
4	可视化分析模块	对流量数据监测分析，是通过数据间的关联关系，识别并还原整个攻击过程，通过攻击链理论能够识别当前攻击所处的环节，追踪定位攻击发起的时间、攻击利用的位置、攻击源相关的信息，通过攻击链能够完整的还原整个攻击过程，系统可视化展示事件的信息侦查、攻击入侵、命令控制、横向渗透、数据外泄、痕迹清理整个攻击过程，并统计主流的攻击方式、攻击源、被攻击资产，实时展示告警趋势图，用户可一目了然知道自己网络资产安全现状。	1	套
5	脱敏数据	以大数据为基础的流量入侵感知平台脱敏数据。	1	套

6	可视化大屏	80 寸高清液晶显示大屏 HDR 显示：支持、背光源：LED、背光方式：直下式、支持格式：1080p。	2	台
7	资产测绘模块	多维度描述空间资产，全面自主发现联网资产，可覆盖 IPv4 ->端口 ->服务 ->产品组件->设备身份信息 ->实际物理信息->设备使用者（公司、企业）->市区、省份、国家->全球。	1	套
8	漏洞感知模块	监测数字资产中的脆弱性资产，发现、感知、响应重大漏洞，级联响应，漏洞扫描 ->漏洞检测 ->脆弱性资产->影响范围 ->漏洞处置。	1	套
9	可视分析模块	资产可视化分析，帮助决策，地域分析、行业分析，实现资产定位可视化、资产统计可视化、资产报表可视化。	1	套
10	漏洞插件库	▲提供目前最新的插件至少 254 个，准确率 99.99%，误报率低于 0.01%，能够对内网进行漏洞验证和发现。帮助企业建立健全资产管理合规性流程、监控资产设备使用规范、发现内部的违规性行为。**（提供功能截图加盖投标人公章）**	1	套
11	资产探测平台脱敏数据	以大数据为基础的资产探测平台脱敏数据。	1	套
12	网络机柜	容量：12U，门及门锁：有，材料及工艺：SPC 优质冷轧钢，脱脂静电喷塑 标准符合 ANSI/EIA RS-310-D，IEC297-2DIN41491PART1，DIN41494；PART7GB/T3047.2-92 标准，兼容 EISI 材料及工艺　SPC 优质冷轧钢，脱脂静电喷塑 外观参数（长*宽*深）：700mm*550mm*450mm 标准标配：托盘×1，12U 立柱×4，螺母若干，脚轮×4	1	台
13	接入交换机	传输速率:10/100/1000Mbps,交换方式:存储-转发,背板带宽≥96Gbps,包转发率≥71.4Mpps 端口描述≥48 个 10/100/1000Mbps 自适应以太网端口 功能特性: 网络标准:IEEE 802.3，IEEE 802.3u，IEEE 802.3x，IEEE 802.3ab 电源电压:AC 100-240V，50-60Hz	2	台

4.6 网络安全科普基地

序号	项目名称	招标要求的技术指标	数量	单位
1	政策法规功能区	1、习近平总书记的网络安全观，不少于 2 个栏目； 2、《中华人民共和国网络安全法》总则及附则，不少于 3 个栏目。	1	套
2	网络攻击体验区	1、至少配置服务器*2，规格：2U 机架式，配导轨套件； CPU：配置≥2 颗 Intel E5-2630v4 十核处理器（主频 2.2GHz）； 内存：配置≥32GB*2 DDR4 REEC，基于后期扩展，最大支持≥8 根内存插槽； 硬盘：配置≥600GB*2 SAS 10K RPM 12Gb/s，配置≥44T SATA*3(Raid 5)硬盘； RAID：1GB 缓存 12Gb/S RAID 控制器，支持 RAID0,1,5,6,10,50,60，带超级电容； 网络接口：配置双口千兆以太网控制器，支持虚拟化、网络加速、负载均衡、冗余等高级功能； 电源：至少配置白金效率 500W 交流电源。 2、态势感知全国入侵感知展示，面对基于 HTTP 的应用层攻击/Web 漏洞利用/常规渗透入侵/服务器控制/内网横向渗透，应用机器学习和大数据技术识别技术，能够集中监测、分析全网的流量信息，识别已经发生或者正在发生的攻击，定位入侵行为、追溯攻击源、实时响应、阻断入侵、降低损失。 3、城市安全展示，城市安全利用智能终端，采集数据和信息，经过智能化的分析，感知城市安全风险。 4、全球网络安全态势展示，不少于 2 个栏目。	1	套

3	安全案例功能区	结合云安全技术与全国网民的举报线索，通过关联串并、大数据分析、自动化挖掘等技术手段将数据推送给相应管辖警方实施打击。提供舆情、电信诈骗、账户安全、木马、病毒等实际生活安全案例，不少于 5 个栏目。	1	套
4	交互体验功能区	1、病毒木马大挑战，通过定制靶场，体验者可亲手释放出一种病毒，并可观看病毒运行全过程，并可尝试对病毒进行挑战，体验遭遇网络病毒场景。 2、通过定制靶场，体验者可以扮演一个黑客的角色，通过挖掘的漏洞对目标靶机进行控制，进行植入木马病毒，体验黑客文化场景。 3、手机恶意充电桩，平时看到的很多公共场合的免费手机充电桩是否可以放心使用，当使用者的手机接入公共场所的充电桩，一些恶意充电桩会诱导用户开启 USB 调试，从而获得手机的完全控制权，进而恶意盗取用户的照片、个人信息甚至是支付密码。此展项将展示手机充电桩可能发生的危害，以此对大家进行安全意识提醒。 4、IOT 全线硬件产品，包含手机、行车记录仪、儿童手表、摄像机、路由器、扫地机器人、智能音箱、智能门铃等。	1	套
5	辅助设备与服务	1、≥80寸*2 展示大屏，屏幕分辨率:超高清4K，HDR显示:支持，背光源：LED，背光方式：直下式，支持格式（高清）：2160p，核心参数：CPU4核，运行内存：至少2GB，存储内存：至少8GB，端口参数：支持USB2.0接口、支持HDMI2.0接口，单屏尺寸（宽*高）mm：至少1686x970。 2、≥55寸*2 展示大屏，屏幕分辨率:超高清4K，HDR显示:支持，背光源：LED，背光方式：直下式，支持格式（高清）：2160p，核心参数：CPU4核，运行内存：至少2GB，存储内存：至少8GB，端口参数：支持USB2.0接口、支持HDMI2.0接口，单屏尺寸（宽*高）mm：至少1241x721。 3、≥16寸*2 笔记本电脑，CUP:英特尔酷睿i7处理器，内存8G，显存2G、硬盘500G、背光键盘、全面屏、超高清屏（2K/3k/4K)。 4、至少配置2套IOT产品展示台，直径高度规格至少1000mm*高度900mm。 5、至少配置2套操作体验台，长宽规格至少1400mm*600mm。 6、强弱电改造，根据基地展示点位进行强弱电施工（暗线）**（投标人提供强弱电施工图）。** 7、内饰施工，包括400平米空间的墙壁粉饰、展板印刷及安装等施工**（投标人提供效果图及施工图）。**	1	套

4.7 课程资源

4.7.1 网络安全综合教学实验实训课程资源

序号	课程名称	内容要求	课时要求
1	《网络安全导论》课程资源包	《网络安全导论》课程资源包内容包括：信息安全要素、安全问题剖析、重大网络安全事件分析、典型网络攻击手段分析、企业安全风险分析、典型信息安全诈骗手段剖析、网络安全意识培养、典型网络对抗工具思路与方法以及 CTF 比赛入门等内容。通过学习，初步认识网络信息安全，了解信息安全带来的危害、了解网络对抗的典型工具思路和方法，并了解 CTF 比赛的相关知识。包含配套实验实践内容，通过对密码破解、ms08-067 漏洞利用、ms17-010 漏洞利用以及网络监听等实验，深刻理解网络安全的重要性。	不少于 48 课时

2	《信息安全技术》课程资源包	《信息安全技术》课程资源包内容包括：常见密码学基础知识、典型网络攻击技术、常见安全防护系统、防病毒技术、软件保护技术、数据备份恢复技术以及等。通过本课程的学习，初步了解密码学的概念框架，掌握基本的网络攻击技术、了解常用的网络安全防护系统，建立起基本的网络安全技术知识体系。包含配套实验实践内容，信息安全技术实践环节：凯撒密码算法开发与验证、DES 加密算法开发验证、SHA 算法开发验证、MD5 算法开发验证以及数据加密工具使用。	不少于 48 课时
3	《操作系统安全》课程资源包	《操作系统安全》课程资源包内容包括：网络安全方向的学科基础课。主要内容包括操作系统的安全机制、安全操作系统模型、密码安全策略、安全审计策略、用户账户管理策略、访问权限管理、补丁管理、防火墙策略管理、服务进程管理等以及对操作系统的典型攻击分析。通过本课程学习，深入了解操作系统面临的各种安全威胁，熟悉操作系统加固的典型方法和工具。包含配套实验实践内容，典型操作系统 Windows、Linux 等系统账户安全配置、操作系统访问权限管理、操作系统安全审计管理、操作系统访问控制管理、数据加密、操作系统安全加固及备份恢复。	不少于 48 课时
4	《网络协议安全》课程资源包	《网络协议安全》课程资源包内容包括：网络安全方向的专业基础课。主要内容包括以太网技术、ARP 协议、RARP 协议、IP 协议、ICMP 协议、IGMP 协议、TCP 协议、UDP 协议以及应用层协议等网络报文格式及工作原理、安全特性分析及 IPv6 协议等内容。包含配套实验实践内容，利用 wireshark 捕获并分析 IP 报文、ARP 缓存查看、TCP 连接建立过程分析、UDP 报文分析、HTTP 报文分析。	不少于 64 课时
5	《网络攻防原理与实践》课程资源包	《网络攻防原理与实践》课程资源包内容包括：信息搜集技术、网络扫描技术、网络监听技术、口令破解技术、典型木马攻防技术、网络跳板技术、缓冲区溢出攻击技术、网络攻击痕迹清除技术以及典型网络攻击的安全防护方法等。通过本课程学习，深入了解网络攻击的基本过程及工具方法，从攻击的角度，深入理解防护策略。包含配套实验实践内容，Nmap 网络扫描、wireshark 网络监听、windows 登录密码破解、木马的配置与远程控制、获取网站 webshell。	不少于 64 课时
6	《Web 安全原理与实践》课程资源包	《Web 安全原理与实践》课程资源包内容包括：SQL 注入攻击、XSS 攻击、CSRF 攻击、文件解析与上传工具、文件包含攻击、WEB 远程命令执行漏洞原理与利用、逻辑漏洞原理及利用、敏感信息泄露漏洞原理与利用、WAF 防火墙技术以及 WEB 框架漏洞分析等。通过本课程的学习，深入理解 WEB 安全面临的各种威胁，并掌握 WEB 渗透攻击的常用工具方法以及防护技术。包含配套实验实践内容，网站 SQL 注入攻击实验、网站文件上传实验、远程命令执行漏洞分析、WEB 框架漏洞分析等。	不少于 64 课时
7	《网络渗透测试实践》课程资源包	《网络渗透测试实践》课程资源包内容包括：网络渗透环境构建、渗透工具利用、信息搜集技术、主要阶段的网络渗透原理与实践以及网络渗透的防护策略。通过本课程学习，深入了解网络渗透的基本过程及工具方法，从攻击的角度，深入理解防护策略。包含配套实验实践内容，Google Hacking 搜集信息、Nmap 扫描目标、OS 指纹识别、密码破解、漏洞利用及提权、内网渗透与横向移动。	不少于 64 课时
8	《网络安全等级保护》课程资源包	《网络安全等级保护》课程资源包内容包括：网络安全等级保护相关的法律法规及标准、网络安全等级保护工作主要内容、网络安全等级保护基本要求、设计技术要求和测评要求（安全通用要求及扩展要求）主要内容解读、网络系统等级保护测评实践（包括定级、备案、建设整改和监督检查）以及网络系统安全加固及安全运维。包含配套实验实践内容，结合等级保护相关要求，对网络信息系统进行模拟定级、备案、安全设计并进行测评。	不少于 48 课时

9	《代码审计与实践》课程资源包	《代码审计与实践》课程资源包内容包括：代码审计原理与方法、代码审计工具使用、web 代码审计原理与实践、php 代码审计原理与实践等。通过本课程的学习能够了解代码审计的基本概念、原理与方法，能够使用常见的代码审计工具对 web 漏洞进行代码审计，并且能够针对性的进行代码安全加固。包含配套实验实践内容，对 windows 下的 PE 文件进行反编译、PE 文件脱壳、静态分析反编译代码、动态跟踪调试代码执行过程、栈溢出跟踪分析。	不少于 64 课时
10	《信息安全管理》课程资源包	《信息安全管理》课程资源包内容包括：网络安全等级确定、网络安全风险分析、等级保护目标与措施、网络安全人员管理、网络安全策略管理、机构人员管理、安全运维管理与法律法规。包含配套实验实践内容，结合等级保护基本要求及测评要求，对网络信息系统进行安全设计、部署相关安全措施、对安全策略进行管理、制定相关的管理制度。	不少于 48 课时
11	《企业安全体系与实践》课程资源包	《企业安全体系与实践》课程资源包内容包括：业务网纵深防御体系建设、业务网安全加固、企业威胁情报、态势感知系统建设、办公网数据防泄露、办公网准入系统和安全加固、蜜罐与攻击欺骗。	不少于 64 课时
备注：网络安全综合教学实验实训课程资源包含但不限于以上内容。资源内容包括：课程大纲、讲义、教学 ppt、实验指导书、试题库、实训实验的教学及实操资源。			

4.7.2 云计算教学实验实训课程资源

序号	课程名称	内容要求	课时要求
1	《云计算导论》课程资源包	课程内容涵盖云计算的基本概念、云服务、云计算数据处理技术、虚拟化技术、云计算管理平台相关技术及云计算典型应用案例等知识的介绍和讲解，课程资源包含教学大纲，章节内容及对应知识点，包含配套 PPT、实验指导书等内容；该课程包含教学大纲，章节内容及对应知识点，必须提供 PPT、实验指导书、源码。	不少于 48 总学时
2	《KVM 虚拟化技术基础与实践》课程资源包	课程内容涵盖虚拟化概述、虚拟化实现技术架构、构建 KVM 环境、QEMU 核心模块配置、KVM 高级功能详解、虚拟化管理工具介绍与讲解；课程资源包含教学大纲，章节内容及对应知识点，包含配套 PPT、实验指导书等内容；具体实验内容包含且不限于： Ubuntu 系统环境准备、KVMQEMU 的虚拟化环境的搭建、制作虚拟机镜像、启动运行第一个虚拟机、虚拟机迁移等内容；该课程包含教学大纲，章节内容及对应知识点，必须提供 PPT、实验指导书、源码。	不少于 48 总学时
3	《云平台技术应用与开发》课程资源包	课程内容涵盖云平台、云平台架构、云平台管理、开源平台 openstack 虚拟化管理工具 libvirt、虚拟化管理工具 virsh、云管理平台综合应用；课程资源包含教学大纲，章节内容及对应知识点，包含配套 PPT、实验指导书等内容；具体实验内容包含且不限于：系统安装与网络基础配置、Keystone 安装与配置、nova 的安装与配置、glance 安装与配置、镜像的创建与管理、cinder 的安装与配置、Quantum 安装与配置、Horizon 的安装与 Openstack 的使用、Libvirt 工具的安装与使用、virt-manage 应用实践、基于 opnstack 云平台的系统设计；该课程包含教学大纲，章节内容及对应知识点，必须提供 PPT、实验指导书、源码。	不少于 48 总学时
4	《云计算综合实训》课程资源包	提供云计算综合实训,实训内容主要包含 KVM/Qemu 虚拟环境搭建、虚拟机迁移、虚拟化管理工具安装及使用、Openstack 平台的配置与安装、虚拟化管理工具的安装与使用、虚拟化应用实践、虚拟化管理工具的安装与使用、虚拟化应用实践、基于 openstack 云平台的系统设计、基于 KVM 的虚拟化服务器及虚拟化云桌面系统设计等。	不少于 48 总学时

5	《云计算与云安全》课程资源包	云计算与云安全课程资源包含云计算与云安全课程大纲、讲义、教学 ppt、实验指导书、试题库、实训实验的教学及实操资源；介绍云安全管理系统的基本知识、结构、配置方法及云安全管理系统的技术理念。云计算与云安全课程资源至少覆盖以下内容： 云平台工单管理、云平台权限管理、云平台报表管理、云平台健康管理、云平台用户中心配置、云平台日志消息管理、云平台资源协作管理、云平台网络管理、云平台路由器基本操作、云平台公网 IP 管理、云平台安全组管理、云平台服务编排管理、云平台虚拟机创建/删除与恢复、云平台虚拟机基础配置升级、云平台虚拟机资源分配、云安全管理平台基本使用管理、云安全管理平台用户管理、云安全管理平台订单服务、云安全管理平台日志管理、云安全管理平台日志记录与审计、虚拟化安全管理系统 Linux 客户端安装及卸载、虚拟化安全管理系统 Windows 客户端安装及卸载、虚拟化安全管理系统账号管理、虚拟化安全管理系统基础设置、虚拟化安全管理系统升级管理、虚拟化安全管理系统主机病毒查杀、虚拟化安全管理系统主机 Webshell 扫描、虚拟化安全管理系统主机安全基线、虚拟化安全管理系统主机的防暴力破解、虚拟化安全管理系统的防火墙策略、虚拟化安全管理系统入侵防护操作、虚拟化安全管理系统黑白名单的添加、虚拟化安全管理系统分组策略管理、虚拟化安全管理系统主机日志分析、虚拟化安全管理系统日志与报表管理、虚拟化安全管理系统主机定时查杀策略配置、虚拟化安全管理系统数据备份与恢复。	不少于 48 总学时
备注：云计算教学实验实训课程资源包含但不限于以上内容。资源内容包括：课程大纲、讲义、教学 ppt、实验指导书、试题库、实训实验的教学及实操资源。			

4.8 配套服务

序号	项目名称	招标要求的技术指标
1	品牌使用授权	★投标人以书面授权的方式授予校方挂牌“企业品牌+网络安全学院”，期限不少于 5 年。 **投标人提供的品牌须满足：** 1、投标人自有品牌，提供投标人授权书； 2、投标人母公司品牌，提供子母公司证明材料与母公司出具的品牌使用授权书； 3、投标人所投本项目设备与系统占比超过 70%的品牌，提供所投产品占比说明与品牌持有人出具的品牌使用授权书。 **（投标人除根据以上情形提供相关文件外，还需提供品牌及其持有人证明材料）**
2	升级、维护	▲1.投标人针对本项目所采购的实验实训平台提供不少于 3 年的免费升级服务，3 年后年升级费用应不高于中标相应项价格的 5%。**（须在投标文件服务承诺项中进行承诺）** 2.服务商提供 3 年完整的售后服务,包含维修服务、巡检巡修、零备件支持、软件系统升级等。服务商需根据学校要求在现场或安装地点（或指导用户）进行产品的安装调试工作。按产品维修计划和服务项目所规定的维修类别进行的服务工作，向用户提供产品说明书、使用说明书、维修手册等有关技术文件。 3.产品在原厂商规定的质保期内必须免费提供包修、包换、包退服务；3 年服务期内设备故障报修的应急响应时间：2 小时内响应，4 小时内到达现场（含节假日）。**（须在投标文件服务承诺项中进行承诺）**
3	定制专业人才建设方案	▲供应商须协助学校完成网络空间安全专业群建设，协助完成专业类别包括但不限于：大数据安全专业、物联网安全专业、web 安全与安全开发专业等。**（须在投标文件服务承诺项中进行承诺）**
4	招生推广服务	供应商在投标文件中列举协助学校招生的支持方式。

5	师资培训服务	▲1.师资培训总体要求：为校方培训能够承担专业课教学与实验实训的师资不少于 10 名，课程涵盖专科阶段信息安全与管理、云计算技术专业的所有核心专业课。**（须在投标文件服务承诺项中进行承诺）** 2.供应商在投标文件提供培训方案，培训类别不限于专业课程培训、教学方法培训等；报价费用应包含住宿、培训费。
6	专业教学服务	★供应商不少于 40 门专业理论与实践教学服务，不于少 2 人 2 年驻校。2019 年（秋）须承担：云基础架构技术及应用、网络存储技术及应用、网络协议分析、操作系统安全、网络协议安全、网络攻防原理与实践、Web 安全原理与实践等七门专业课教学。报价费用应包含所派驻人员产生的所有费用。 1.投标人派驻校方承担教学任务的工程应有较高的师德师风与专业技术水平，因派驻人员原因给校方造成不良影响的，供应商须承担赔偿责任； 2.课程教学支持的内容包括：结合实训实验设备开发所需要的实训的案例、PPT 课件、教师手册和试题库。 **（须在投标文件服务承诺项中进行承诺）**
7	大学生竞赛服务	▲1、供应商须每年协助学校举办 1 次校内网络攻防大赛；三年内协助学校承办省级大学生网络攻防大赛 1 次。**（须在投标文件服务承诺项中进行承诺）** 2、赛前辅导服务，针对学校学生参加省赛、行业赛、国赛等网络信息安全类比赛时，供应商须进行赛前辅导，辅导周期不少于 30 天。并选拔优秀学员，协助校方组建网安俱乐部。
8	企业职业认证考试与社会培训	1.供应商须已建立企业职业技能证书认证体系，认证体系包括服务商企业安全认证体系或供应商与国家合作的技能认证体系；能够颁发企业职业技能证书； ▲2.提供面向校内相关专业学生至少一次免费认证考试机会，对未通过的补考与社会人员考试进行报价说明；**（须在投标文件服务承诺项中进行承诺）** 3. 供应商须面向学校在校师生提供认证培训服务，供应商对认证考试成绩优异者提供的实习就业名额，保障学生就业； ▲4、供应商基于实验室在校内设立社会培训中心，帮助学校开展对外社会培训推广，例如：导入网安行业认证培训体系、市场推广、招收社会学员等工作内容，三年建设期内引进的社会培训不少于 600 人次。**（须在投标文件服务承诺项中进行承诺）**
9	课程资源库开发服务	1.投标人须每半年一次与网络空间安全专业群的各专业带头人进行特色教材开发以及学术、论文发表。 ▲2.投标人须对以教学配套的网络安全软硬件设备为依托，定制开发精品课程不少于 6 门。内容须涵盖：课程大纲、讲义、教学 ppt、实验指导书、试题库、实训实验的教学及实操资源。**（须在投标文件服务承诺项中进行承诺）**
10	就业服务	▲1.供应商须每年提供不少于 200 人次的学生就业服务。 ▲2.供应商须每半年组织一次校内专场招聘会。 ▲3.供应商须每年供一份企业用人需求名单。名单中包含企业名称、规模、当年需求数量、本/专科应届就业薪资、特殊要求。**（以上 1-3 项须在投标文件服务承诺项中进行承诺）** 供应商设有专门的校企合作部为学生提供全面、完善的就业支持服务，其中包括就业指导服务、实习就业推荐服务、定向人才培养服务等。就业指导实训服务有助于学生提高和掌握综合就业实践能力，从容面对各种招聘考核，使学生在面试中更具竞争力；实习就业推荐服务能极大地提高学生就业率和专业对口率，保障学生就业质量；定向人才培养服务，为学生提供优质企业的就业岗位，通过定岗实训综合实力，更好的在企业中发展。 4.供应商已建就业服务平台。系统主要功能包括： （1）招聘企业信息注册、开放使用权限，完善个人信息。 （2）招聘企业录入招聘启事，学生可以通过就业服务平台投递简历，并预约面试等功能。 （3）就业企业信息库管理，系统记录了所有合作企业的地址以及联系方式。

11	教学管理服务	供应商提供教学运行管理平台，系统功能如下： 1.系统管理：对系统用户、进行管理授权； 2.院校数据：对学校、专业、班级、学生等基本信息进行管理，对校历进行管理； 3.教务管理功能：录入专业的培养计划、各班级配备师资，课程表，能对教师的资料反馈进行时效性以及量化的考核工作，如：是否及时提交授课资料、课时统计等内容；教师满意度调查模块的发起、进度监督、结果统计；对教学资料进行档案性查询； 4.教学工作：教师对课程考核方案、教学进度、授课资料等内容进行提交、反馈，对课程表进行查询； 5.流程审批：对教学服务计划、课程考核方案等内容进行流程化审批； 6.供应商以现场操作演示的方式展现教务管理系统的相关使用与部分功能； 7.提供不少于 20 个账号 3 年的授权使用。
12	装潢设计	★投标人根据招标文件提供的数据中心、四个实验室与一个科普基地平面图至现场勘察，设计与本项目相适应并体现企业文化的室内平面布置图、装潢效果图与施工图，并对装潢主要材料提出建议。**（本项要求现场效果图演示，并在中标后提供全套图纸）**
13	其他	投标人提供的与网络安全人才培养相关的其他服务项。
备注：以上配套服务要求，投标人根据自身情况逐项进行响应报价。		

第五章评标方法与评标标准

一、评标方法与定标原则

评标采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

二、评标标准

本项目评分总分值为100分。

序号	评审因素	评分标准说明		分值
1	价格部分（30分）	采用低价优先法计算，即满足招标文件要求且投标报价最低的投标报价为评标基准价，其价格为满分30分，其他投标人的报价统一按照下列公式计算：投标报价得分 = （评标基准价/投标报价）×30，计算分数时四舍五入取小数点后两位。		30
2	技术部分（54分）	方案述标	投标人根据对项目的整体理解和把握，结合学校的实际情况，介绍项目的应标方案。内容包括：目标、中长期规划、进度安排、组织架构、人员配备、工具配备、项目管理计划等。 (配套服务之其他服务方案，在此评分项由评委根据情况一并打分) 优7-8分，良5-6分，一般2-3分，差0分。	8
		技术响应	投标产品与招标文件规定的技术参数和要求的满足程度（▲为重要技术参数，不满足1项扣1分；无标注技术参数为一般参数，不满足1项扣0.5分）。	16
			系统演示，标准如下： 网络安全综合实验室★参数功能演示，评委根据每项情况综合打分，每项参数功能演示优得1分，良得0.5分，其余得0分。	6
		品牌授权	投标人以书面授权的方式授予校方挂牌“企业品牌+网络安全学院”，期限不少于5年。评委结合品牌与投标人关系以及品牌影响力价值打分。 高5-6分，中3-4分，一般1-2分，无价值0分。	6
		师资培训	投标人提供详细的师资培训方案，要能实现老师能独立解决网络安全专业教学相关领域的技术问题，能组织教学改革、制定人才培养方案、构建课程体系、进行课程开发的能力。 评委根据结合情况综合打分。 总体评价:优3分，良2分，一般1分,差0分。	3
		专业群建设	投标人提供网络安全专业群建设与相关专业人才培养方案,评委根据结合情况综合打分。总体评价：优1.5分，良1分，一般0.5分,差0分。	1.5分
		招生	投标人提供协助学校的招生方案。评委根据结合情况综合打分。 总体评价:优1.5分，良1分，一般0.5分,差0分。	1.5分
		学生就业	投标人提供学生就业方案，包含可行可靠的就业途径,服务期内就业岗位的数量保障等。评委根据结合情况综合打分。 总体评价:优1.5分，良1分，一般0.5分,差的0分。	1.5分

		认证体系	投标人面向学生提供“1+X”证书的认证体系支持方案。评委根据结合情况综合打分。 总体评价:优 1.5 分，良 1 分，一般 0.5 分,差的 0 分。	1.5 分
		社会培训	投标人为学校引入社会培训资源方案。评委根据情况综合打分。 总体评价:优 1.5 分，良 1 分，一般 0.5 分,差的 0 分。	1.5 分
		课程资源库及开发	投标人提供包括但不限于采购清单所列的课程资源，并协助学校定制开发在线开放精品课程方案。内容须涵盖：课程大纲、讲义、教学 ppt、实验指导书、试题库、实训实验的教学及实操资源。评委根据投标人提供的课程资源数量、开发精品课程门数与方案情况综合打分。 总体评价:优 3 分，良 2 分，一般 1 分,差的 0 分。	3 分
		大学生竞赛	投标人提供协助学校组织校内大学生参加各类大赛并争取各级别赛项的承办方案。 评委根据结合情况综合打分。 总体评价:优 1.5 分，良 1 分，一般 0.5 分,差 0 分。	1.5 分
		设计效果图	投标人根据招标文件中的数据中心、三个实验室与科普基地平面图并至现场勘察，设计相应的效果图、施工图及设计方案说明。评委根据结合情况综合打分。 总体评价:优 3 分，良 2 分，一般 1 分,差 0 分。	3
3	商务资信部分（16 分）	资质	投标人取得以下任一资质得 1 分，本项评分上限为 4 分： 1.中国信息安全测评中心颁发的 CNNVD 二级以上技术支撑单位证书； 2.国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位； 3.投标人具有通信网络安全服务能力评定证书-安全培训一级以上； 4.投标人具有 ISCCC 信息安全服务类资质（包括：安全运维服务、应急处理、风险评估、信息系统安全集成服务）； 5.中国信息安全测评中心颁发的 CISP 授权培训机构证书或 NISP 国家信息安全水平考试授权运营中心资质证书； 6.投标人建有安全技术国家工程实验室； 7.投标人具有中国反网络病毒联盟白名单甲级单位资质； 8.投标人为网络安全类组织成员单位之一的（包括：中国互联网网络安全威胁治理联盟成员、CNVD 国家漏洞库技术组成员、中国反网络病毒联盟成员）。 **（以上相关证明材料需提供证书复印件加盖公章，无相关证明不得分）**	4
		案例	投标人提供自 2016 年 7 月 1 日以来，已签订网络安全实验室建设或网络安全工程项目合同，每提供一个单体合同总额 1000 万元以上合同得 2 分，单体合同总额 2000 万元以上合同得 4 分，不提供不得分。 **（提供相关证明材料复印件加盖公章，无相关证明不得分）**	4
		升级维护	1.投标人针对本项目所采购的实验实训平台提供基本的 3 年免费升级服务，每增加一年免费升级服务得 1 分，最多得 2 分； 2.售后服务保障标准 3 年质保，每增加一年得 1 分，最多得 2 分。	4
		专业教学	投标人自 2019 年（秋）第一学期起提供不少于 40 门专业理论与实践教学服务，不少于 2 人 2 年驻校外。根据投标人提供派驻人员个人资质证书与增加的驻校教学服务时长，由评委综合打分。 优 4 分，良 3 分，一般 2 分,差 0 分。	4

说明：

1、资质、合同等材料因复印件不清及合同复印件价格被遮挡所引起的后果由投标人自行负责。

2、加★ 为实质性响应项，负偏离或只满足部分的，按无效投标处理。

3、技术响应分低于 10 分的，按无效投标处理。

4、演示环节现场只提供电源接口，其余所有演示设备及网络等均由各投标人自行准备，演示时长不得超过 20 分钟。

5、方案述标时长不得超过 10 分钟。

6、若供应商提供虚假资料，一经查实取消其中标候选人资格，并向相关主管部门汇报。

7、中标人不得转包、分包，如果发现有转包、分包情况，则取消其中标候选人资格，并向相关主管部门汇报。

第六章　投标文件格式

（正或副本）

投　标　文　件

项 目 名 称：

招 标 编 号：

投标人名称 ：

日　　期 ：

评分索引表

评分项目	在投标文件中的页码位置

投标主要文件目录

一、资信证明文件要求

1、实质性资格证明文件目录

文件 1　法人或者其他组织的营业执照等证明文件，自然人的身份证明（复印件）

文件 2　上一年度财务状况报告（复印件，成立不满一年不需提供）

文件 3　依法缴纳税收和社会保障资金的相关材料（复印件）

文件 4　具备履行合同所必需的设备和专业技术能力证明材料

文件 5 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

文件 6 法人授权书

文件 7　招标文件中规定要求提供的证明材料和投标人认为需要提供的其他材料（招标文件要求提供原件的必须单独封装并与投标文件一起递交，评标结束后原件退回；未要求提供原件的提供复印件，原件自带备查）

具备履行合同所必需的设备和专业技术能力的书面声明

我公司郑重声明：我公司具备履行本项采购合同所必需的设备和专业技术能力，为履行本项采购合同我公司具备如下主要设备和主要专业技术能力：

主要设备有：。

主要专业技术能力有：。

供应商名称（公章）：

日期：_____年月日

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

声　明

我公司郑重声明：参加本次政府采购活动前 3 年内，我公司在经营活动中没有因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

供应商名称（公章）：

授权代表签字：_____

日期：_____年月日

法人授权书

本授权书声明：_____（供应商名称）授权_____（被授权人的姓名）为我方就号项目采购活动的合法代理人，以本公司名义全权处理一切与该项目采购有关的事务。

本授权书于_____年____月____日起生效，特此声明。

代理人（被授权人）：_____

单位名称：_____

授权单位盖章：_____

单位名称：_____

地址：

日期：

二、资格性审查响应对照表（格式）

投标人全称（加盖公章）：

序号	资格性审查响应内容	是否响应 （填是或者否）	投标文件中的 页码位置
1			
2			
3			
4			
5			
6			
7			

三、符合性检查响应对照表（格式）

投标人全称（加盖公章）：

序号	符合性检查响应内容	是否响应 （填是或者否）	投标文件中的 页码位置
1			
2			
3			
4			
5			
6			
7	招标文件中的其他实质性要求		

四、投标函（格式）

致：盐城工业职业技术学院

根据贵方的号招标文件，正式授权下述签字人_____(姓名)代表我方_____（投标人的名称），全权处理本次项目投标的有关事宜。

据此函，_____签字人兹宣布同意如下：

1.按招标文件规定的各项要求，向买方提供所需货物与服务。

2.我们完全理解贵方不一定将合同授予最低报价的投标人。

3.我们已详细审核全部招标文件及其有效补充文件，我们知道必须放弃提出含糊不清或误解问题的权利。

4.我们同意从规定的开标日期起遵循本投标文件，并在规定的投标有效期期满之前均具有约束力。

5.如果在开标后规定的投标有效期内撤回投标或中标后拒绝签订合同，我们的投标保证金可不予退还。

6.同意向贵方提供贵方可能另外要求的与投标有关的任何证据或资料，并保证我方已提供和将要提供的文件是真实的、准确的。

7.一旦我方中标，我方将根据招标文件的规定，严格履行合同的责任和义务，并保证在招标文件规定的时间完成项目，交付买方验收、使用。

8.与本投标有关的正式通讯地址为：

地　　址：

邮　　编：

电　　话：

传　　真：

投标人开户行：

账　　户：

投标人授权代表姓名（签字）：

投标人名称（公章）：

日　　期：_____年____月____日

五、开标一览表（格式）

项目编号	2019-026S
项目名称	盐城工业职业技术学院网络安全实验室建设项目
项目投标报价：（大写），小写：	
质保期：	
项目实施时间（供期或工期）：	
保证金形式：	

填写说明：

1、 开标一览表不得填报选择性报价，否则将作为无效投标；

2、 开标一览表中报价与投标分项明细报价表中不符时时，以开标一览表为准；

供应商名称（公章）：

日期： 年月日

六、投标产品配置及分项报价表（格式）

投标人全称（加盖公章）：

1	2	3	4
货物名称及规格、型号	数量	单价	总价
合计			

法定代表人或授权代表签字：

1、此表可以根据需要自行增减行数。

七、技术参数响应及偏离表（如有）

投标人全称（加盖公章）：

序号	招标要求	投标响应	超出、符合或偏离	原因

法定代表人或授权代表签字：

注：1、按照基本技术要求详细填列。

2、行数不够，可自行添加。

八、商务条款响应及偏离表（如有）

投标人全称（加盖公章）：

项目	招标文件要求	是否响应	投标人的承诺或说明
质保期			
售后技术服务要求(含质保期内产品故障服务响应时限、上门时间、故障修复时限、耗材供应响应时限等)			
交货时间	合同签订后天内		
交货方式			
交货地点			
付款方式			
投标货币			
备品备件及耗材等要求			
其他			

法定代表人或授权代表签字：

九、技术方案

十、品牌使用授权书

授 权 书

兹授权：盐城工业职业技术学院挂牌“_____网络安全学院”，时间：_____年____月____日至_____年____月____日。

授权人：（盖章）

法人代表签字：

年　　月　　日

十一、服务承诺

1、升级、维护：

2、定制专业人才建设方案：

3、招生推广服务：

4、师资培训服务：

5、专业教学服务：

6、大学生竞赛服务 ：

7、企业职业认证考试与社会培训：

8、课程资源库开发服务：

9、就业服务：

10、其他服务承诺：